IBM Systems - iSeries

Lucru în reţea
Serviciile de acces la distanţă (RAS): Conexiunile PPP

Versiunea 5 Ediţia 4

IBM Systems - iSeries

Lucru în reţea
Serviciile de acces la distanţă (RAS): Conexiunile PPP

Versiunea 5 Ediţia 4

Notă

Înainte de a folosi aceste informaţii şi produsul pe care îl suportă, citiţi informaţiile din “Observaţii”, la pagina 67.

Ediţia a şaptea (februarie 2006)

Această ediţie este valabilă pentru i5/OS (număr produs 5722–SS1) Versiunea 5, Ediţia 4, Modificarea 0 şi pentru toate ediţiile şi modificările următoare, până când se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Servicii de acces la distanţă: Conexiuni PPP

Point-to-Point Protocol (PPP) este un standard de Internet pentru transmiterea datelor prin linii seriale.

Este protocolul de conectare cel mai utilizat de ISP-uri (Internet Service Provider). PPP permite calculatoarelor individuale să acceseze reţele care oferă acces la Internet. Serverul IBM iSeries conţine suportul TCP/IP PPP ca parte a conectivităţii WAN (wide-area network).

Puteţi face schimb de date între locaţii folosind PPP pentru a conecta un calculator la distanţă cu serverul dumneavoastră iSeries. Prin PPP, sistemele care sunt conectate la serverul iSeries pot accesa resurse sau alte maşini care fac parte din reţeaua în care se află serverul. De asemenea, puteţi configura serverul iSeries pentru conectarea la Internet folosind PPP. Vrăjitorul Conexiune prin apel telefonic din Navigator iSeries vă poate ghida prin procesul conectării serverului iSeries la Internet sau la o reţea internă.

Ce este nou pentru V5R4

Acest subiect evidenţiază funcţiile modificate la Serviciile de acces la distanţă: Conexiunile PPP pentru V5R4.

Funcţiile modificate

- **Istoric de apeluri**

  Istoricele de apeluri sunt înregistrări importante a datelor care trec spre sau dinspre modem în timpul unei sesiuni PPP. Ele sunt salvate sau şterse în funcţie de parametrul OUTPUT al comenzii STRTCPPTP (Start TCP/IP Point-to-Point) (*ERROR, *PRINT sau *NONE).

  În ediţiile anterioare, fişierele spool ale istoricelor de apeluri se numeau log*nnnnnn*, unde *nnnnnn* era numărul jobului *nnnnnn*/QTCP/QTPPPSSN.

  În V5R4, toate sesiunile PPP rulează în firul de execuţie *nnnnnn*/QTCP/QTPPPCTL. Fişierele spool ale istoricului de apeluri sunt numite CL*mmmmmmmm*, unde *mmmmmmmm* este ID-ul firului de execuţie. Aceasta vă permite să faceţi corespondenţa între mesajele sesiunii din istoricul jobului QTPPPCTL (care are un câmp Thread .... 00000028) cu istoricul de apeluri corespunzător.

- **QTPPPSSN şi QTPPPL2SSN**

  – Joburile QTPPPSSN şi QTPPPL2SSN (L2TP) sunt joburile sesiunii PPP în ediţiile anterioare IBM i5/OS V5R4. Ele sunt pornite şi oprite de comenzile STRTCPPTP şi ENDTCPPTP sau de QTPPPL2TP când este stabilit sau oprit un tunel. Ele pot fi de asemenea pornite sau oprite automat când legăturile sunt pornite sau oprite de protocolul multilink.

    Începând cu V5R4, PPP nu mai foloseşte joburile QTPPPSSN şi QTPPPL2SSn. Sesiunile rulează ca fire de execuţie în QTPPPCTL.

  – În ediţiile anterioare lui i5/OS V5R4, comanda WRKTCPPTP (Work with Point-to-Point TCP/IP Profiles), opţiunea 14 (Work with job) scotea la iveală joburile active ale sesiunii. Ocazional se va porni QTPPPL2TP, dacă nu era nici o sesiune PPP activă pentru profilul L2TP.

    În V5R4, WRKTCPPTP opţiunea 14, aduce la vedere QTPPPCTL, dacă un fir de execuţie sesiune este activ în acel job.

- **Istoricul de mesaje**

  În V5R4, există un nou fişier spool istoric de mesaje pentru mesajele sesiunii. Colectează mesajele de la firul de execuţie al sesiunii, mesajele de la firul iniţial care sunt rezultatul muncii în numele sesiunii şi mesajele de la procesele copii (spawned) într-un singur fişier spool.

  Un fişier spool istoric de mesaje este numit ML*mmmmmmmm*, unde *mmmmmmmm* este ID-ul firului de execuţie. Aceasta vă permite să puneţi în corespondenţă istoricele de apeluri, istoricele de mesaje şi mesajele sesiunii în istoricul jobului QTPPPCTL (care are un câmp Thread .... 00000028).

- **QTPPPCTL şi QTPPPL2TP**

| În V5R4, jobul QTPPPCTL foloseşte mai multe fire de execuţie sistem pentru a rula sesiunea ca fire în loc de procese separate (QTPPPSSN şi QTPPPL2SSN).

| Jobul QTPPPCTL porneşte fire de execuţie pentru o sesiune şi o legătură secundară pentru a înlocui joburile vechi ale sesiunii şi legăturii QTPPPSSN şi QTPPPL2SSN.

| Jobul QTPPPCTL este returnat la API-uri şi la interfaţa grafică (GUI) Navigator iSeries când joburile sesiunii sunt cerute.

| • **Adaptoare Ethernet**

| În V5R4, lista de adaptoare Ethernet care suportă PPPoE se extinde pentru a include tipul 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 şi 573A de adaptoare Ethernet.

| • **PPPoE**

| În V5R4, PPPoE poate partaja acelaşi adaptor cu traficul IPv4 şi IPv6.

Cum puteţi vedea ce este nou sau modificat

Pentru a vă ajuta să vedeţi care sunt modificările tehnice, în aceste informaţii au fost folosite:

- Imaginea  , pentru a marca locul unde încep informaţiile noi sau modificate.
- Imaginea  , pentru a marca locul unde se termină informaţiile noi sau modificate.

Pentru a găsi alte informaţii despre ce este nou sau modificat în această ediţie, vedeţi Memo către utilizatori.

PDF tipăribil

Folosiţi aceasta pentru a vizualiza sau pentru a tipări un PDF cu aceste informaţii.

Pentru a vedea sau a descărca versiunea PDF, selectaţi Serviciile de acces la distanţă: Conexiunile PPP  (aprox. 940 KB).

Alte informaţii

Puteţi de asemenea vizualiza sau tipări oricare din următoarele informaţii:

- Manuale:
  - Găsiţi cele mai noi corecţii temporare de program (PTF-uri) şi cele mai noi informaţii despre configurare pentru PPP şi L2TP prin legătura PPP de pe pagina de bază iSeries server TCP/IP  . Această legătură oferă ultimele informaţii care suplimentează şi înlocuiesc informaţiile conţinute în această colecţie de subiecte.
- IBM Redbooks:
  - Manualul ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  acoperă serviciile şi aplicaţiile TCP/IP.
  - Manualul ITSO Redbook iSeries IP Networks: Dynamic! (SG24-6718)  acoperă serviciile şi aplicaţiile TCP/IP.

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia de lucru proprie pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe PDF în browser (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe opţiunea care salvează fişierul PDF local.
3. Navigaţi până la directorul unde vreţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Aveţi nevoie de Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca gratis o copie de la situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

---

concepte PPP

Puteţi folosi PPP pentru a conecta un server iSeries la reţele de la distanţă, la PC-uri client, la alt iSeries sau la un ISP. Pentru a utiliza pe deplin acest protocol, ar trebui să înţelegeţi capabilităţile şi suportul iSeries pentru acest protocol.

Referinţe înrudite

"Informaţii înrudite pentru PPP" la pagina 65
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Ce este PPP?

Protocolul punct-la-punct (PPP) este un protocol TCP/IP folosit să conecteze un calculator la altul. Calculatoarele utilizează **PPP** (**Point-to-Point Protocol**), pentru a comunica prin reţeaua telefonică sau prin Internet.

O conexiune PPP există atunci când două sisteme sunt conectate fizic printr-o linie telefonică. Puteţi folosi PPP pentru a conecta un sistem la altul. De exemplu, o conexiune PPP stabilită între un sediu central şi un sediu filială permite ambelor sedii să transfere date celuilalt prin reţea.

PPP este un standard Internet. Este cel mai utilizat protocol de conectare de către ISP-uri (furnizori de servicii Internet). Puteţi folosi PPP pentru a vă conecta la ISP-ul dumneavoastră; ISP-ul dumneavoastră vă acordă conectivitate la Internet.

PPP permite interoperabilitatea între software-ul de acces la distanţă al diferiţilor fabricanţi. De asemenea, permite şi ca protocoale multiple de comunicaţie în reţea să folosească aceeaşi linie fizică de comunicaţie.

Următoarele standarde RFC (Request For Comment) descriu protocolul PPP. Puteţi găsi informaţii suplimentare despre RFC-uri la pagina Web RFC Editor.

- RFC1661 Protocol punct-la-punct
- RFC1662 PPP cu framing stil HDLC
- RFC1994 PPP CHAP

Profiluri de conexiuni

Profilurile conexiune punct-la-punct definesc un set de parametri şi resurse pentru conexiuni PPP specifice. Puteţi porni profiluri care folosesc aceste setări de parametri pentru a apela (iniţia) sau pentru a aştepta (recepţiona) conexiuni PPP.

Există două tipuri de profil care vă permit să definiţi un set de caracteristici pentru o conexiune PPP sau un set de conexiuni.

- **Profilurile de conexiune originator** sunt conexiuni punct-la-punct care provin de la serverul iSeries local şi sunt receptate de un sistem la distanţă. Puteţi configura conexiunile care trebuie iniţiate folosind acest obiect.
- **Profilurile de conexiune receptor** sunt conexiuni punct-la-punct care provin de la un sistem la distanţă şi care sunt receptate de serverul iSeries local. Puteţi configura conexiunile care trebuie receptate folosind acest obiect.

Un profil de conexiune specifică modul în care ar trebui să funcţioneze o conexiune PPP. Informaţiile din profilul unei conexiuni răspund acestor întrebări:

- Ce tip de protocol de conexiune veţi folosi? (PPP sau SLIP (Serial Line Internet Protocol))
- Serverul iSeries contactează celălalt calculator prin apel telefonic (originator)? Serverul iSeries aşteaptă primirea unui apel de la celălalt sistem (receptor)?
- Ce linie de comunicaţie va folosi conexiunea?

- Cum ar trebui serverul iSeries să determine adresa IP pe care o va folosi?
- Cum ar trebui serverul iSeries să autentifice un alt sistem? Unde ar trebui să stocheze serverul iSeries informaţiile de autentificare?

Profilul de conexiune este reprezentarea logică a următoarelor detalii ale conexiunii:

- Tip linie şi profil
- Configurări Multilink
- Numere telefonice la distanţă şi opţiuni de apelare
- Autentificare
- Setări TCP/IP: adrese şi rutare IP şi filtrare IP
- Control funcţionare şi personalizare conexiune
- Servere de nume domeniu

Serverul iSeries stochează aceste informaţii de configurare într-un profil de conexiune. Aceste informaţii oferă contextul necesar pentru ca serverul iSeries să stabilească o conexiune PPP cu alt sistem. Un profil de conexiune conţine următoarele informaţii:

- **Tip protocol**. Puteţi opta între PPP şi SLIP. IBM vă recomandă să folosiţi PPP de fiecare dată când este posibil.
- **Selectare mod**. Tipul de conexiune şi modul de operare pentru acest profil de conexiune.

  Tip conexiune specifică tipul de linie pe care se bazează conexiunile şi dacă ele sunt **de apelare** (originator) sau **de răspuns** (receptor). Puteţi selecta dintre aceste tipuri de conexiune:

  – Linie comutată
  – Linie închiriată (dedicată)
  – L2TP (linie virtuală)
  – PPPoE (linie virtuală)

  PPPoE este suportat numai pentru Profiluri conexiune originator.
- **Mod de funcţionare**. Modul de funcţionare disponibil depinde de tipul conexiunii. Vedeţi următoarele tabele:

  Vedeţi următorul tabel pentru Profiluri conexiune originator:

Tabela 1. Moduri de operare disponibile pentru Profiluri conexiune originator

Tip conexiune	Moduri de operare disponibile
Linie comutată	• Apel • Apel-la-cerere (doar apel) • Apel-la-cerere (peer dedicat cu răspuns activat) • Apel la cerere (peer activat la distanţă)
Linie închiriată	Iniţiator
L2TP	• Iniţiator • Iniţiator multi-hop • Apel la distanţă
PPP peste Ethernet	Iniţiator

Vedeţi următorul tabel pentru Profiluri conexiune receptor:

Tabela 2. Moduri de operare disponibile pentru Profiluri conexiune receptor

Tip conexiune	Moduri de operare disponibile
Linie comutată	Răspuns
Linie închiriată	Terminator
L2TP	Terminator (server reţea)

- **Configurare legătură**. Aceasta specifică tipul de serviciu linie folosit de conexiune.

  Aceste opţiuni depind de tipul selecţiei de mod ales. Pentru o linie comutată şi o linie închiriată puteţi alege din următoarele:

  – Linie singulară
  – Pool de linii

  Pentru toate celelalte tipuri de conexiune (închiriată, L2TP, PPPoE) selecţia serviciului liniei este doar Linie singulară.

  Referinţe înrudite

  “Cerinţe software şi hardware” la pagina 32
  Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul dintre calculatoare, serverul iSeries, poate fi originator sau receptor.

Suport politici de grup

Suportul pentru Politici de grup permite administratorilor de reţea să definească politici de grup la nivel de utilizator pentru ajutor în administrarea resurselor şi permite ca politicile de control al accesului să fie atribuite utilizatorilor individuali în momentul deschiderii de sesiuni PPP sau L2TP în reţea.

Utilizatorii pot fi identificaţi ca aparţinând unei anumite clase de utilizatori, iar fiecare clasă va avea propria politică unică. Fiecare Politică de acces de grup unică permite definirea limitelor resurselor ca numărul de legături permis într-un bundle Multilink, atribute ca ″IP forwarding″ şi identificarea setului de reguli filtrare pachete IP de aplicat. Cu suportul pentru Politici de grup, administratorii de reţea pot defini de exemplu un grup Lucru_acasă care permite acestei clase de utilizatori accesul complet la reţea, în timp ce un grup Lucrător_vânzări ar putea fi restricţionat la un set limitat de servicii.

Referinţe înrudite

“Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE” la pagina 11
Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

“Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP” la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Scenarii

Scenariile din acest subiect vă ajută să înţelegeţi cum funcţionează PPP şi cum puteţi implementa un mediu PPP în reţeaua dumneavoastră. Aceste scenarii introduc concepte PPP fundamentale, pe care începătorii şi utilizatorii experimentaţi le pot învăţa înainte de a trece la operaţiile de planificare şi configurare.

Referinţe înrudite

“Informaţii înrudite pentru PPP” la pagina 65
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Exemplu: PPP şi DHCP pe un singur server iSeries

Puteţi afla cum să setaţi serverul iSeries ca un server DHCP pentru un client din LAN şi pentru un client de la distanţă prin apel telefonic.

Clienţii la distanţă, cum sunt clienţii prin apel telefonic, au nevoie adesea de acces la reţeaua unei companii. Clienţii prin apel telefonic pot accesa un server iSeries cu PPP. Pentru a accesa reţeaua, clientul prin apel telefonic va avea nevoie de informaţii IP, la fel ca oricare alt client de reţea ataşat direct. Un server DHCP iSeries poate distribui

informaţii de adresă IP la un client apel telefonic PPP la fel ca la orice client ataşat direct. Următoarea figură arată un angajat de la distanţă care are nevoie să apeleze telefonic în reţeaua companiei pentru a efectua nişte operaţii.

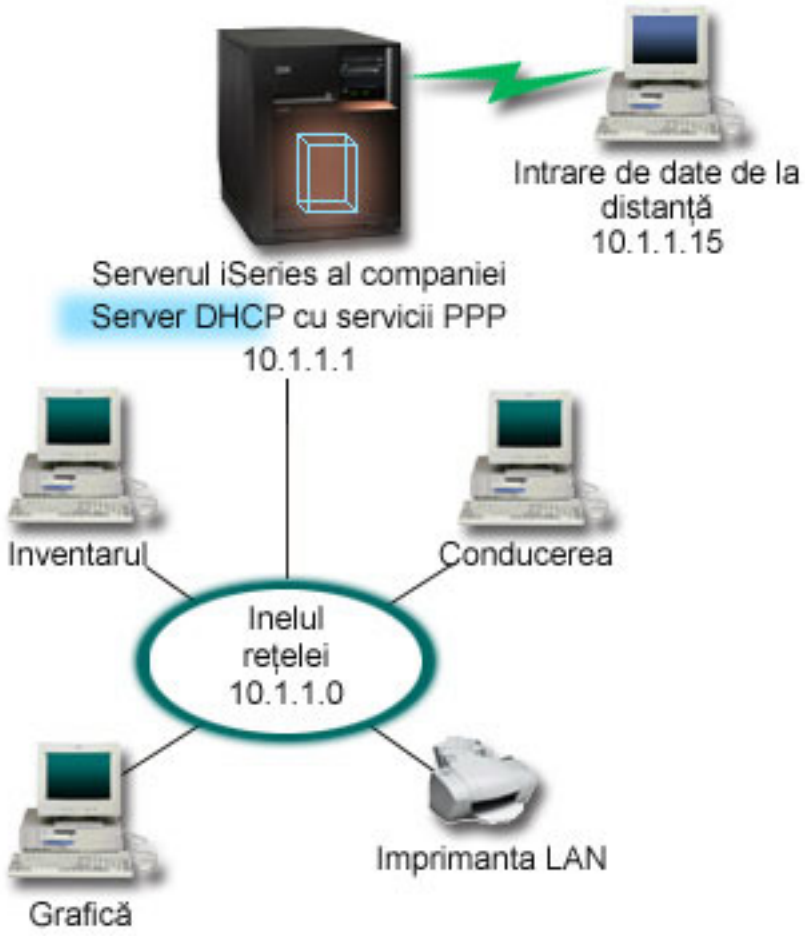


Figura 1. PPP şi DHCP pe un singur server iSeries

Pentru angajatul de la distanţă să devină cu succes parte a reţelei companiei, serverul iSeries trebuie să folosească o combinaţie de RAS (Remote Access Services) şi DHCP. Funcţia Remote Access Services creează capabilitatea de apel telefonic pentru serverul iSeries. Dacă este setată corespunzător, după ce angajatul stabileşte conexiunea prin apel telefonic, serverul PPP îi comunică spune serverului DHCP să distribuie informaţiile TCP/IP către angajat.

În acest exemplu, o singură politică de subreţea DHCP acoperă atât clienţii de reţea de la sediul central, cât şi clienţii prin apel telefonic.

Dacă doriţi ca profilul PPP să delege la DHCP distribuţia de IP, trebuie să faceţi aceasta în profilul PPP. În setările TCP/IP ale profilului de conexiune receptor, trebuie să setaţi metoda de alocare a adresei de la distanţă de la Fixă la DHCP. Pentru a permite clienţilor prin apel telefonic să comunice cu alţi clienţi de reţea cum ar fi imprimanta LAN, trebuie să permiteţi şi înaintarea IP în setările TCP/IP ale profilului şi proprietăţile configuraţiei (stivei) TCP/IP. Dacă setaţi doar înaintarea IP în profilul PPP, serverul iSeries nu va trece mai departe pachetele IP. Trebuie să setaţi înaintarea IP atât pe profil, cât şi în stiva de protocoale.

De asemenea, adresa IP a interfeţei locale din profilul PPP trebuie să fie o adresă IP care se încadrează în definiţia subreţelei din serverul DHCP. În acest exemplu, adresa interfeţei locale PPP trebuie să fie 10.1.1.1. Această adresă va trebui să fie exclusă din pool-ul de adrese al serverului DHCP, aşa încât să nu fie alocată unui client DHCP.

Planificarea setării DHCP pentru clienţii din sediu şi cei PPP

Tabela 3. Opţiunile de configurare globale (se aplică la toţi clienţii serviţi de serverul DHCP)

Obiect		**Valoare**
Opţiuni de configurare	opţiunea 1: Mască subreţea	255.255.255.0
	opţiunea 6: Server nume de domeniu	10.1.1.1
	opţiunea 15: Nume domeniu	mycompany.com
Serverul realizează actualizări DNS?		Nu
Serverul suportă clienţi BOOTP?		Nu

Tabela 4. Subreţea atât pentru clienţii din sediu, cât şi pentru cei prin apel telefonic

Obiect		**Valoare**
Nume subreţea		MainNetwork
Adrese de gestionat		10.1.1.3 - 10.1.1.150
Timpul de închiriere		24 ore (implicit)
Opţiuni de configurare	Opţiuni moştenite	Opţiuni din configuraţia Globală
Adresele de subreţea nu sunt alocate de server		10.1.1.1 (Adresa de interfaţă locală specificată în Setările TCP/IP ale proprietăţilor Profilului de conexiune receptor în Navigator iSeries)

Alte setări

- Setaţi metoda adresei IP de la distanţă la DHCP în profilul de conexiune receptor PPP.
  1. Activaţi conexiunea clientului WAN DHCP cu un server DHCP sau o conexiune releu folosind elementul de meniu Servicii pentru Servicii de acces la distanţă din Navigator iSeries.
  2. Selectaţi să folosiţi DHCP pentru metoda de alocare a adresei IP sub Proprietăţi Setări TCP/IP ale Profilului de conexiune receptor în Navigator iSeries.
- Permiteţi sistemelor de la distanţă să acceseze alte reţele (înaintarea IP) sub Proprietăţi Setări TCP/IP ale Profilului de conexiune receptor în Navigator iSeries Navigator.
- Activaţi înaintarea datagramelor IP sub Proprietăţi de setare ale configuraţiei TCP/IP în Navigator iSeries.

Exemplu: Profil PPP şi DHCP pe servere iSeries diferite

Puteţi afla cum să setaţi două servere iSeries ca serverul DHCP al reţelei şi un agent releu DHCP/BOOTP pentru două reţele şi pentru clienţii de la distanţă care intră prin apel telefonic.

Acest exemplu anterior, PPP şi DHCP pe un singur server iSeries, arată cum să folosiţi PPP şi DHCP pe un singur server iSeries pentru a permite clienţilor prin apel telefonic (dial-in) să acceseze la o reţea. Fie datorită dispunerii fizice a reţelei, fie din motive de securitate, poate să fie mai bine să aveţi serverele PPP şi DHCP separate sau să aveţi un server PPP dedicat fără serviciile DHCP. Următoarea figură reprezintă o reţea care are clienţi prin apel telefonic, dar politicile PPP şi DHCP sunt pe servere diferite.

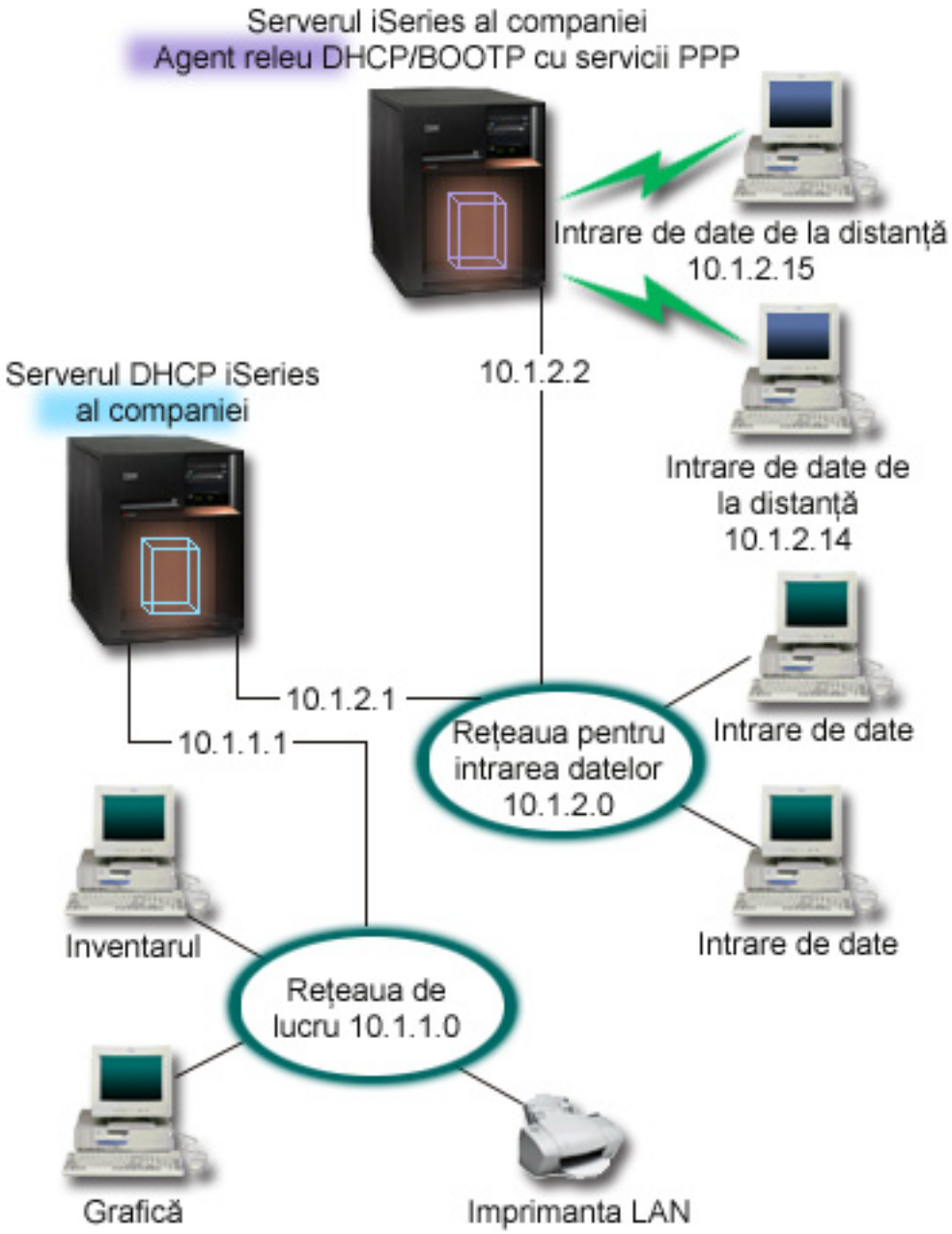


Figura 2. Profil PPP şi DHCP pe servere iSeries diferite

Clienţii de la distanţă de introducere a datelor apelează serverul PPP iSeries. Profilul PPP pe acel server trebuie să aibă o metodă DHCP de alocare a adresei IP de la distanţă, ca şi în exemplul precedent, precum şi înaintarea IP din proprietăţile profilului PPP şi ale stivei TCP/IP. În plus, deoarece serverul acţionează ca un agent releu DHCP, serverul TCP/IP agent releu BOOTP/DHCP trebuie să fie activat. Aceasta permite serverului de acces la distanţă iSeries să treacă pachetele DHCP DISCOVER pe serverul DHCP. Serverul DHCP va răspunde şi va distribui informaţiile TCP/IP clienţilor apel telefonic prin intermediul serverului PPP.

Serverul DHCP este responsabil pentru distribuirea adreselor IP la amândouă reţelele, 10.1.1.0 şi 10.1.2.0. În reţeaua pentru introducere de date, va oferi adrese IP de la 10.1.2.10 la 10.1.2.40 atât clienţilor prin apel telefonic, cât şi clienţilor ataşaţi direct la reţea. Clienţii pentru introducerea datelor au nevoie şi de o adresă de ruter (opţiunea 3) de 10.1.2.1 pentru a comunica cu reţeaua Producţie şi serverul DHCP iSeries trebuie să aibă înaintarea IP activată.

De asemenea, adresa IP a interfeţei locale din profilul PPP trebuie să fie o adresă IP care se încadrează în definiţia subreţelei din serverul DHCP. În acest exemplu, adresa interfeţei locale PPP trebuie să fie 10.1.2.2. Această adresă va trebui să fie exclusă din pool-ul de adrese al serverului DHCP, aşa încât să nu fie alocată unui client DHCP. Adresa IP a interfeţei locale trebuie să fie o adresă la care serverul DHCP să trimită pachetele de răspuns.

Planificarea setării DHCP pentru DHCP cu un agent releu DHCP

Tabela 5. Opţiunile de configurare globale (se aplică la toţi clienţii serviţi de serverul DHCP)

Obiect		**Valoare**
Opţiuni de configurare	opţiunea 1: Mască subreţea	255.255.255.0
	opţiunea 6: Server nume de domeniu	10.1.1.1
	opţiunea 15: Nume domeniu	mycompany.com
Serverul realizează actualizări DNS?		Nu
Serverul suportă clienţi BOOTP?		Nu

Tabela 6. Subreţea pentru reţeaua Producţie

Obiect		**Valoare**
Nume subreţea		WorkNetwork
Adrese de gestionat		10.1.1.3 - 10.1.1.150
Timpul de închiriere		24 ore (implicit)
Opţiuni de configurare	Opţiuni moştenite	Opţiuni din configuraţia Globală
Adresele de subreţea nu sunt alocate de server		fără

Tabela 7. Subreţea pentru reţeaua Introducere de date

Obiect		**Valoare**
Nume subreţea		DataEntry
Adrese de gestionat		10.1.2.10 - 10.1.2.40
Timpul de închiriere		24 ore (implicit)
Opţiuni de configurare	opţiunea 3: Ruter	10.1.2.1
	Opţiuni moştenite	Opţiuni din configuraţia Globală
Adrese de subreţea care nu sunt alocate de server		10.1.2.1 (Ruter) 10.1.2.15 (Adresa IP a interfeţei locale a clientului de la distanţă de introducerea datelor) 10.1.2.14 (Adresa IP a interfeţei locale a clientului de la distanţă de introducerea datelor)

Alte setări pe serverul iSeries care rulează PPP

- Setarea serverului TCP/IP agent releu BOOTP/DHCP

Obiect	**Valoare**
Adresă interfaţă	10.1.2.2
Pachete releu la adresa de IP a serverului	10.1.2.1

- Setaţi metoda adresei IP de la distanţă la DHCP în profilul de conexiune receptor PPP
  1. Activaţi conexiunea clientului WAN DHCP cu un server DHCP sau o conexiune releu folosind elementul de meniu Servicii pentru Servicii de acces la distanţă din Navigator iSeries

2. Selectaţi să folosiţi DHCP pentru metoda de alocare a adresei IP sub Proprietăţi Setări TCP/IP ale Profilului de conexiune receptor în Navigator iSeries

- Permiteţi sistemelor de la distanţă să acceseze alte reţele (înaintarea IP) sub Proprietăţi Setări TCP/IP ale Profilului de conexiune receptor în Navigator iSeries (pentru a permite clienţilor de la distanţă să comunice cu reţeaua de introducere de date)
- Activaţi înaintarea datagramelor IP sub Proprietăţi Setări TCP/IP ale Profilului de conexiune receptor în Navigator iSeries (pentru a permite clienţilor de la distanţă să comunice cu reţeaua de introducere de date)

Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec

În acest scenariu, aflaţi cum să setaţi o conexiune între o gazdă a filialei şi sediul central care foloseşte L2TP protejat de IPSec. Calculatorul din filială are o adresă IP alocată dinamic, în timp ce calculatorul din sediul central are o adresă IP statică, rutabilă global.

Situaţie

Să presupunem că firma dumneavoastră are o mică filială în alt stat. În orice zi de lucru filiala poate necesita acces la informaţiile confidenţiale de pe un sistem iSeries din intranetul companiei. Compania foloseşte în mod curent o linie închiriată scumpă pentru a oferi filialei acces la reţeaua companiei. Deşi compania doreşte să continue să furnizeze acces securizat la intranet, aţi dori să reduceţi cheltuielile datorate liniei închiriate. Acest lucru poate fi făcut prin crearea unui tunel voluntar L2TP (Layer 2 Tunnel Protocol) care extinde reţeaua companiei, astfel încât filiala apare ca parte a subreţelei companiei. VPN protejează traficul de date prin tunelul L2TP.

Cu un tunel voluntar L2TP, filiala stabileşte un tunel cu serverul reţelei L2TP (LNS) al reţelei companiei. Funcţionalitatea concentratorului de acces L2TP (LAC) se află pe client. Tunelul este transparent ISP-ului clientului de la distanţă, aşa că furnizorul de servicii Internet (ISP) nu este necesar să suporte L2TP. Dacă vreţi să citiţi mai multe despre conceptele L2TP, vedeţi L2TP (Layer 2 Tunnel Protocol).

Important: Acest scenariu arată gateway-urile de securitate ataşate direct la Internet. Absenţa unui firewall este menită să simplifice scenariul. Nu înseamnă că utilizarea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile implicate de fiecare dată când vâ conectaţi la internet.

Obiective

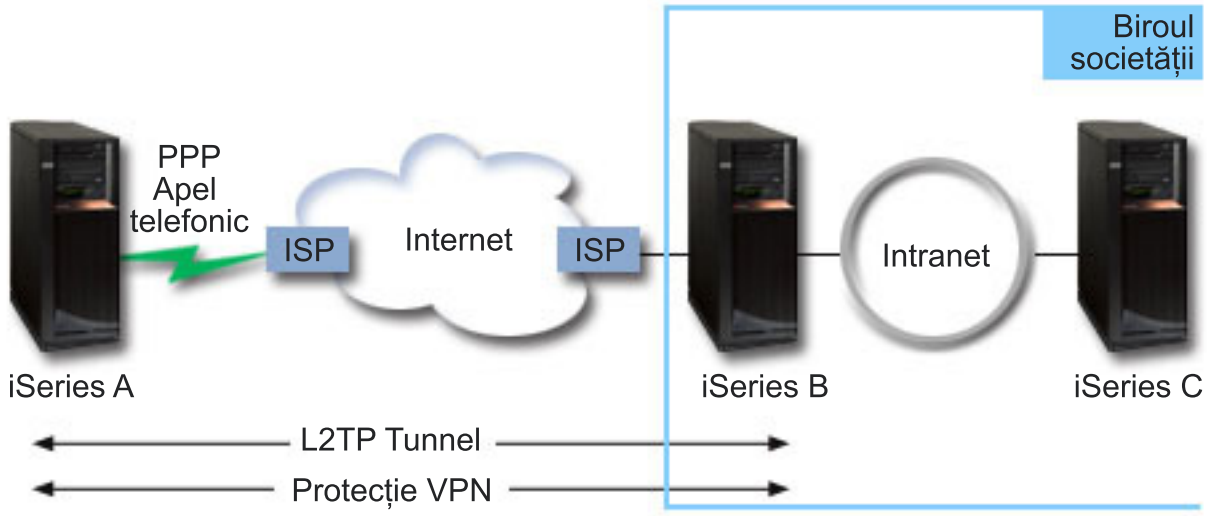
În acest scenariu, un sistem al filialei se conectează la reţeaua companiei printr-un sistem gateway cu un tunel L2TP protejat de VPN.

Principalele obiective ale acestui scenariu sunt:

- Sistemul filialei iniţiază întotdeauna conexiunea la sediul companiei.
- Sistemul fililalei este singurul sistem din reţeaua filialei care are nevoie de acces la reţeaua companiei. Cu alte cuvinte, rolul său este de gazdă, nu de gateway, în reţeaua filialei.
- Sistemul companiei este un calculator gazdă din reţeaua sediului companiei.

Detalii

Următoarea figură ilustrează caracteristicile reţelei pentru acest scenariu:



iSeries-A

- Trebuie să aibă acces la aplicaţiile TCP/IP pe toate sistemele din reţeaua companiei.
- Să primească adresele IP alocate dinamic de la ISP.
- Trebuie configurat să primească suport L2TP.

iSeries-B

- Trebuie să aibă acces la aplicaţiile TCP/IP pe iSeries-A.
- Subreţeaua este 10.6.0.0 cu masca 255.255.0.0. Această subreţea reprezintă punctul final pentru date al tunelului VPN la sediul companiei.
- Se conectează la Internet cu adresa IP 205.13.237.6. Acesta este punctul final al conexiunii. Adică, iSeries-B realizează gestionarea cheilor şi aplică IPSec datagramelor IP de intrare şi ieşire. iSeries-B se conectează la subreţeaua sa cu adresa IP 10.6.11.1.

În termeni L2TP, *iSeries-A* acţionează ca un iniţiator L2TP, în timp ce *iSeries-B* acţionează ca un terminator L2TP.

Task-urile de configurare

Presupunând că configuraţia TCP/IP există deja şi funcţionează, trebuie să efectuaţi următorii paşi:

Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE

Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

Situaţie

Afacerile dumneavoastră cer o conexiune Internet mai rapidă, deci sunteţi interesat de un serviciu DSL (digital subscriber line) cu un ISP local. După o investigaţie iniţială, aflaţi că ISP-ul dumneavoastră foloseşte PPPoE pentru a-şi conecta clienţii. aveţi nevoie să folosiţi conexiunea PPPoE pentru a asigura conexiuni de bandă largă la Internet prin serverul iSeries.

Figura 3. Conectarea serverului iSeries la un ISP cu PPPoE

Soluţie

Puteţi asigura suportul pentru o conexiune PPPoE la ISP prin serverul iSeries. Serverul iSeries foloseşte noul tip de linie virtuală PPPoE, care se leagă la o linie Ethernet fizică, configurată să folosească un adaptor Ethernet de tipul 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 sau 573A. Această linie virtuală suportă protocoale de sesiune PPP printr-un LAN Ethernet conectat la un modem DSL, care oferă gateway-ul spre ISP-ul la distanţă. În acest fel, utilizatorii conectaţi prin LAN pot să beneficieze de acces de mare viteză la Internet folosind conexiunile PPPoE ale serverelor iSeries. După ce s-a stabilit conexiunea dintre iSeries şi ISP, utilizatorii individuali de pe LAN pot accesa ISP-ul prin PPPoE, folosind adresa IP alocată serverului iSeries. Pentru a oferi o securitate sporită, pot fi aplicate reguli de filtrare liniei virtuale PPPoE, pentru a restricţiona un anumit trafic Internet de intrare.

Configuraţie exemplu

1. Configuraţi dispozitivul de conexiune pentru a fi folosit cu ISP-ul dumneavoastră.
2. Configuraţi un profil de conexiune originator pe serverul iSeries.

   Aveţi grijă să introduceţi următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: PPP peste Ethernet
   - **Mod operare**: Iniţiator
   - **Configuraţie legătură**: Linie singulară
3. În pagina General din Proprietăţi profil punct-la-punct nou, introduceţi un nume şi o descriere pentru profilul originator. Acest nume se referă la profilul conexiunii şi la linia PPPoE virtuală.
4. Faceţi clic pe **Conexiune** pentru a deschide pagina Conexiune. Alegeţi **Numele de linie virtuală PPPoE** care corespunde numelui pentru acest profil de conexiune. După ce selectaţi linia, Navigator iSeries va afişa dialogul pentru **proprietăţile liniei**.

   a. Pe pagina General, introduceţi o descriere relevantă pentru linia virtuală PPPoE.

b. Faceţi clic pe **Legătură** pentru a deschide pagina Legătură. Din lista de selecţie Nume linie fizică, alegeţi linia Ethernet pe care o va folosi această conexiune şi faceţi clic pe **Deschidere**. Alternativ, dacă aveţi nevoie să definiţi o nouă linie Ethernet, introduceţi numele liniei şi faceţi clic pe **Nouă**. Navigator iSeries afişează dialogul **Proprietăţile liniei Ethernet**.

| **Notă:** PPPoE necesită un tip de adaptor Ethernet 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 sau
| 573A.

1) Pe pagina General, introduceţi o descriere relevantă pentru Linia Ethernet şi verificaţi dacă definiţia liniei foloseşte resursele hardware cerute.
2) Faceţi clic pe **Legătură** pentru a deschide pagina Legătură. Introduceţi proprietăţile pentru linia Ethernet fizică. Consultaţi documentaţia adaptorului dumneavoastră Ethernet şi ajutorul online pentru informaţii suplimentare.
3) Faceţi clic pe **Altele** pentru a deschide pagina Altele. Specificaţi nivelul de acces şi autorizarea pe care o pot avea alţi utilizatori pentru această linie.
4) Selectaţi **OK** pentru a vă întoarce la pagina cu proprietăţile liniei virtuale PPPoE.

c. Faceţi clic pe **Limite** pentru a defini proprietăţi pentru autentificarea LCP sau faceţi clic pe **OK** pentru a vă întoarce la pagina Conexiune din Profil punct-la-punct nou.
d. Când reveniţi în pagina Conexiune, specificaţi adresarea serverului PPPoE, în funcţie de informaţiile furnizate de ISP.

5. Dacă ISP-ul dumneavoastră cere ca serverul iSeries să se autentifice sau dacă vreţi ca iSeries să autentifice serverul la distanţă, faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare.
6. Faceţi clic pe pagina **Setări TCP/IP** pentru a deschide pagina TCP/IP şi specificaţi parametrii Tratare adresă IP pentru acest profil de conexiune. Setarea care urmează să fie folosită trebuie să fie furnizată de ISP. Pentru a permite utilizatorilor ataşaţi prin LAN să se conecteze la ISP folosind adresele IP alocate serverului iSeries, selectaţi **Ascundere adrese (Travestire totală)**.
7. Faceţi clic pe **DNS** pentru a deschide pagina DNS, introduceţi adresa IP a serverului DNS furnizat de ISP.
8. Dacă vreţi să specificaţi subsistemul care va rula jobul conexiune, faceţi clic pe **Altele** pentru a deschide pagina Altele .
9. Faceţi clic pe **OK** pentru încheierea profilului.

Concepte înrudite

“Suport politici de grup” la pagina 5
Suportul pentru Politici de grup permite administratorilor de reţea să definească politici de grup la nivel de utilizator pentru ajutor în administrarea resurselor şi permite ca politicile de control al accesului să fie atribuite utilizatorilor individuali în momentul deschiderii de sesiuni PPP sau L2TP în reţea.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Referinţe înrudite

“Configurare legătură” la pagina 50
Configurare legătură defineşte tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni.

“Autentificare sistem” la pagina 43
Conexiunile PPP cu un server iSeries suportă mai multe opţiuni de autentificare a clienţilor la distanţă care se conectează prin apel telefonic la iSeries şi a conexiunilor la ISP sau alt server pe care iSeries îl apelează telefonic.

“Tratare adrese IP” la pagina 41
Conexiunile PPP permit mai multe seturi diferite de opţiuni pentru gestiunea adreselor IP în funcţie de tipul de profil conexiune.

“Filtrare pachet IP” la pagina 41
Filtrarea pachetelor IP limitează serviciile pentru un utilizator individual când este logat la o reţea.

Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries

Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

Situaţie

Ca administrator al reţelei companiei, trebuie să întreţineţi atât serverul iSeries, cât şi clienţii din reţea. În loc de a vă deplasa pentru depanarea şi corectarea problemelor, aţi dori să aveţi posibilitatea de a lucra de la o locaţie la distanţă, cum ar fi de acasă. Deoarece compania nu are o conexiune de reţea legată la Internet, aţi putea să vă conectaţi la serverul iSeries folosind o conexiune PPP. În plus, singurul modem pe care îl aveţi în acest moment este modemul ECS (electronic custromer support) 7852-400 şi este necesar să utilizaţi acest modem pentru conexiunea dumneavoastră.

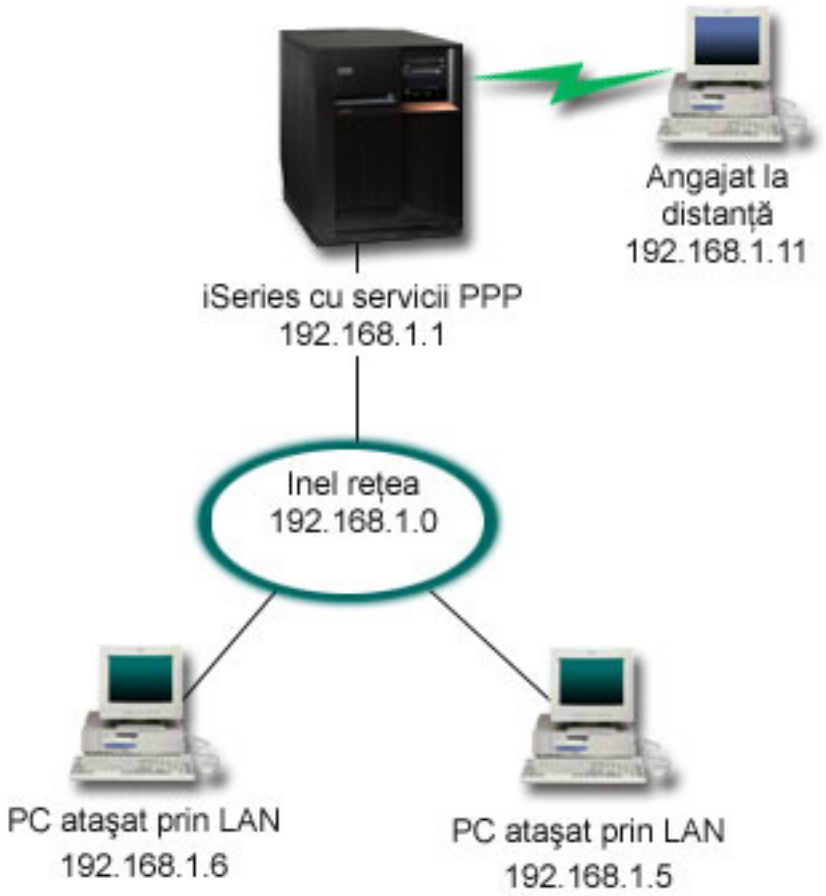


Figura 4. Conectarea clienţilor la distanţă la serverul iSeries

Soluţie

Puteţi folosi PPP pentru conectarea PC-ului de acasă la serverul iSeries folosind propriul modem. Deoarece folosiţi modemul ECS pentru acest tip de conexiune PPP, trebuie să vă asiguraţi că modemul este configurat atât pentru modul sincron, cât şi pentru cel asincron. Această ilustraţie prezintă un server iSeries cu servicii PPP care este conectat la un LAN cu două PC-uri. Cel care lucrează la distanţă se conectează la serverul iSeries prin apel telefonic, se autentifică şi apoi devine parte a reţelei de lucru (192.168.1.0). În acest caz, este mai simplu să atribuiţi o adresă IP statică clientului care se conectează prin linia telefonică.

Cel care lucrează la distanţă foloseşte CHAP-MD5 pentru a se autentifica pe serverul iSeries. iSeries nu poate folosi MS_CHAP, deci trebuie ca un client PPP să aibă configurată utilizarea CHAP-MD5.

Dacă doriţi pentru clienţii dumneavoastră la distanţă un acces la reţeaua companiei aşa cum este arătat mai sus, trebuie să fie activată opţiunea de înaintare (forwarding) IP în stiva TCP/IP şi de asemenea în profilul receptor PPP, iar rutarea IP trebuie configurată corect. Dacă doriţi să limitaţi sau să securizaţi acţiunile pe care clientul la distanţă le poate executa în reţea, puteţi folosi reguli de filtrare pentru a-i trata pachetele IP.

În desenul de mai sus este conectat un singur client, deoarece modemul ECS nu poate lucra decât cu o singură conexiune la un moment dat. Dacă este necesar ca mai mulţi clienţi să fie conectaţi simultan prin apel telefonic, consultaţi secţiunea de planificare pentru considerente hardware şi software.

Configuraţie exemplu

1. Configuraţi Dial-up Networking şi creaţi o conexiune prin linie telefonică pe PC-ul la distanţă.
2. Configuraţi un profil de conexiune receptor pe serverul iSeries.

   Aveţi grijă să introduceţi următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Răspuns
   - **Configuraţie legătură**: ceasta ar putea fi linie singulară sau un pool de linii, în funcţie de mediul dumneavoastră.
3. În pagina General din Proprietăţi profil punct-la-punct nou, introduceţi un nume şi o descriere pentru profilul receptorului.
4. Faceţi clic pe **Conexiune** pentru a deschide pagina Conexiune. Alegeţi **Nume linie** corespunzător sau creaţi unul nou prin tastarea unui nume şi apoi apăsaţi **Nou**.
   a. În pagina General, evidenţiaţi o resursă hardware existentă la care este ataşat adaptorul dumneavoastră 7852–400 şi setaţi Cadre la **Asincrone**.
   b. Faceţi clic pe **Modem** pentru a deschide pagina Modem. În lista de selecţie Nume, alegeţi modemul **IBM 7852–400**.
   c. Faceţi clic pe **OK** pentru revenire la pagina Proprietăţi profil punct-la-punct nou.
5. Faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare.
   a. Selectaţi **Este necesar ca acest server iSeries să verifice identitatea sistemului la distanţă**.
   b. Selectaţi **Autentificare locală folosind o listă de validare** şi adăugaţi un nou utilizator la distanţă în lista de validare.
   c. Selectaţi **Permitere parolă criptată (CHAP-MD5)**.
6. Faceţi clic pe **Setări TCP/IP** pentru a deschide pagina TCP/IP.
   a. Selectaţi adresa IP locală 192.168.1.1.
   b. Pentru adresa IP la distanţă, selectaţi **Adresă IP fixă** cu adresa IP de început 192.168.1.11.
   c. Selectaţi **Permitere ca sistemele la distanţă să acceseze alte reţele**.
7. Faceţi clic pe **OK** pentru încheierea profilului.

Concepte înrudite

“Planificare PPP” la pagina 32
Puteţi citi acest subiect pentru informaţii despre crearea şi administrarea conexiunilor PPP.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Referinţe înrudite

“CHAP-MD5” la pagina 44
Challenge Handshake Authentication Protocol (CHAP-MD5) foloseşte un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul care autentifică şi de dispozitivul la distanţă.

“Configurare legătură” la pagina 50
Configurare legătură defineşte tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni.

“Pool de linii” la pagina 51
Selectaţi acest serviciu linie pentru a configura conexiunea PPP pentru a folosi o linie dintr-un pool de linii. La pornirea conexiunii PPP, serverul iSeries selectează o linie neutilizată din pool-ul de linii. Pentru profiluri cu conectare pe linie telefonică la cerere, serverul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

Scenariu: Conectarea LAN-ului de la birou la Internet cu un modem

Administratorii configurează de obicei reţele care permit angajaţilor să aibă acces la Internet. Ei pot folosi un modem pentru a conecta serverul iSeries la un ISP. Clienţii PC ataşaţi prin LAN pot să comunice cu Internetul folosind serverul iSeries ca gateway.

Situaţie

Aplicaţia pe care o utilizează compania dumneavoastră cere acum ca utilizatorii să acceseze Internetul. Deoarece aplicaţia nu necesită transferul unei cantităţi mari de date, trebuie să puteţi folosi un modem pentru a conecta atât serverul iSeries, cât şi clienţii legaţi prin LAN la Internet. Ilustraţia următoare prezintă un exemplu cu această situaţie.

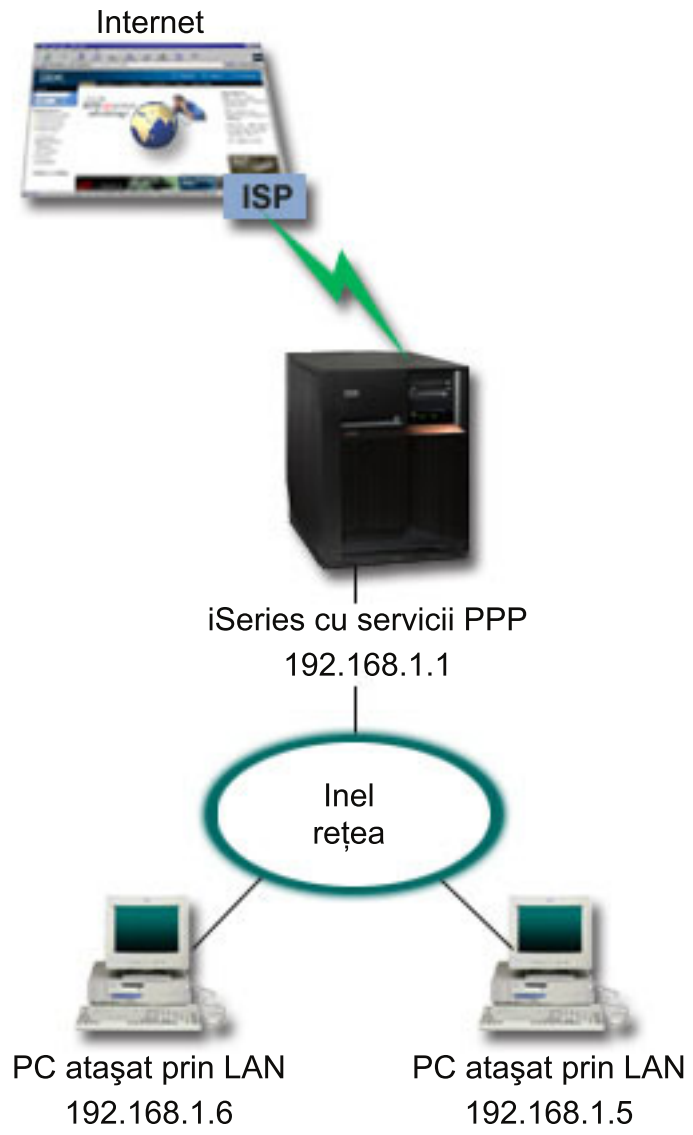


Figura 5. Conectarea LAN-ului de la birou la Internet cu un modem

Soluţie

Puteţi folosi modemul integrat (sau alt modem compatibil) pentru a vă conecta serverul iSeries la ISP. Pentru a stabili conexiunea PPP la ISP, trebuie să creaţi un profil PPP originator pe server.

După realizarea conexiunii între iSeries şi ISP, PC-urile ataşate la LAN pot comunica cu Internetul folosind iSeries ca gateway. În profilul originator, este bine să selectaţi opţiunea Ascundere adresă, astfel încât clienţii LAN, care au adrese IP private, să poată comunica cu Internetul.

Acum, când iSeries şi reţeaua sunt ataşate la Internet, trebuie să înţelegeţi riscurile legate de securitate. Luaţi legătura cu ISP-ul pentru a vă explica politica lor de securitate şi luaţi măsurile necesare pentru a vă proteja serverul şi reţeaua.

În funcţie de modul de utilizare a Internetului, lărgimea de bandă ar putea deveni o problemă. Pentru a afla mai multe despre modul în care vă puteţi creşte lărgimea de bandă a conexiunii, consultaţi secţiunea de planificare.

Configuraţie exemplu

1. Configuraţi un profil de conexiune originator pe serverul iSeries.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Apel telefonic
   - **Configuraţie legătură**: Aceasta ar putea fi linie singulară sau un pool de linii, în funcţie de mediul dumneavoastră.

2. În pagina General din Proprietăţi profil punct-la-punct nou, introduceţi un nume şi o descriere pentru profilul originator.
3. Faceţi clic pe **Conexiune** pentru a deschide pagina Conexiune. Alegeţi Nume linie corespunzător sau creaţi unul nou prin tastarea unui nume şi apoi apăsaţi **Nou**.
   a. În pagina General a proprietăţilor noii linii, evidenţiaţi o resursă hardware existentă. Dacă selectaţi o resursă modem internă, setările pentru tipul de modem şi secvenţa de cadre vor fi selectate automat.
   b. Faceţi clic pe **OK** pentru revenire la pagina Proprietăţi profil punct-la-punct nou.
4. Faceţi clic pe **Adăugare** şi tastaţi numărul de telefon pentru conectarea la serverul ISP. Asiguraţi-vă că aţi inclus prefixele necesare.
5. Faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare, selectaţi **Permite sistemului de la distanţă să verifice identitatea serverului iSeries** . Selectaţi protocolul de autentificare şi introduceţi informaţiile despre nume sau parolă necesare.
6. Faceţi clic pe **Setări TCP/IP** pentru a deschide pagina TCP/IP.
   a. Selectaţi **Atribuit de sistemul la distanţă** pentru adresele IP locale şi la distanţă.
   b. Selectaţi **Adăugare sistem la distanţă ca rută implicită**.
   c. Activaţi **Ascundere adrese** pentru ca adresele IP interne să nu fie rutate pe Internet.
7. Faceţi clic pe **DNS** pentru a deschide pagina DNS, introduceţi adresa IP a serverului DNS furnizat de ISP.
8. Faceţi clic pe **OK** pentru încheierea profilului.

Pentru a folosi profilul de conexiune ca să vă conectaţi la Internet, faceţi clic dreapta pe profilul de conexiune în Navigator iSeries şi selectaţi **Pornire**. Conexiunea este realizată cu succes când starea se schimbă în **Activ**. Reîmprospătaţi pentru a actualiza ecranul.

Notă: De asemenea, trebuie să vă asiguraţi că pe celelalte sisteme din reţeaua dumneavoastră rutarea este definită corect, astfel încât traficul TCP/IP legat de Internet de la aceste sisteme să fie trimis prin serverul iSeries.

Concepte înrudite

“Planificare PPP” la pagina 32
Puteţi citi acest subiect pentru informaţii despre crearea şi administrarea conexiunilor PPP.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Referinţe înrudite

“Pool de linii” la pagina 51
Selectaţi acest serviciu linie pentru a configura conexiunea PPP pentru a folosi o linie dintr-un pool de linii. La pornirea conexiunii PPP, serverul iSeries selectează o linie neutilizată din pool-ul de linii. Pentru profiluri cu conectare pe linie telefonică la cerere, serverul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

“Configurare legătură” la pagina 50
Configurare legătură defineşte tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni.

Scenariu: conectarea reţelei companiei şi a reţelelor la distanţă cu un modem

Un modem permite ca două locaţii la distanţă (cum ar fi sediul central şi o filială) să schimbe date între ele. PPP poate conecta între ele cele două LAN-uri prin stabilirea unei conexiuni între serverul iSeries din sediul central şi alt server iSeries din sediul filialei.

Situaţie

Să presupunem că aveţi reţeaua companiei şi reţeaua unei filiale în două locaţii diferite. În fiecare zi, biroul filialei trebuie să se conecteze cu biroul centralei pentru a face schimb de informaţii din baza de date referitoare la aplicaţiile de culegere a datelor. Cantitatea de date schimbată nu justifică achiziţionarea unei conexiuni fizice de reţea, astfel încât vă decideţi să folosiţi modemuri pentru conectarea celor două reţele.

Figura 6. Conectarea reţelei companiei şi a reţelelor la distanţă printr-un modem

Soluţie

PPP poate conecta cele două LAN-uri prin stabilirea unei conexiuni între fiecare server iSeries, ca în ilustraţia de mai sus. În acest caz, presupuneţi că biroul la distanţă iniţiază conexiunea cu biroul central. Veţi configura un profil originator pe serverul iSeries de la distanţă şi un profil receptor pe serverul din sediul central.

În cazul în care calculatoarele biroului de la distanţă au nevoie să acceseze LAN-ul companiei (192.168.1.0), profilul receptor din biroul central trebuie să aibă activată înaintarea IP (IP forwarding) şi rutarea adreselor IP pentru calculatoare (192.168.2, 192.168.3, 192.168.1.6 şi 192.168.1.5 în acest exemplu). De asemenea, trebuie activată ″IP forwarding″ TCP/IP. Această configuraţie activează comunicaţii TCP/IP de bază intre LAN-uri. Va trebui să luaţi în considerare factori de securitate şi DNS pentru a rezolva numele gazdă între reţelele locale.

Configuraţie exemplu

1. Configuraţi un Profil conexiune originator pe serverul iSeries al sediului la distanţă.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Apel telefonic
   - **Configuraţie legătură**: Aceasta ar putea fi linie singulară sau un pool de linii, în funcţie de mediul dumneavoastră.
2. În pagina General din Proprietăţi profil punct-la-punct nou, introduceţi un nume şi o descriere pentru profilul originator.
3. Faceţi clic pe **Conexiune** pentru a deschide pagina Conexiune. Alegeţi Nume linie corespunzător sau creaţi unul nou prin tastarea unui nume şi apoi apăsaţi **Nou**.
   a. În pagina General a proprietăţilor pentru noua linie, evidenţiaţi o resursă hardware existentă şi setaţi Cadre în **Asincron**.
   b. Faceţi clic pe **Modem** pentru a deschide pagina Modem. Din lista de selecţie Nume, alegeţi modemul pe care îl folosiţi.
   c. Faceţi clic pe **OK** pentru revenire la pagina Proprietăţi profil punct-la-punct nou.
4. Faceţi clic pe **Adăugare** şi tastaţi numărul de telefon pentru a vă conecta pe linie telefonică la serverul iSeries din sediul central. Asiguraţi-vă că aţi inclus prefixele necesare.
5. Faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare şi selectaţi **Permite sistemului de la distanţă să verifice identitatea serverului iSeries**. Selectaţi **Necesită parolă criptată (CHAP-MD5)** şi introduceţi informaţiile despre nume sau parolă necesare.
6. Faceţi clic pe **Setări TCP/IP** pentru a deschide pagina Setări TCP/IP.
   a. Pentru adrese IP locale, selectaţi adresa IP a interfeţei LAN a sediului la distanţă (192.168.2.1) din caseta de selecţie **Utilizare adresă IP fixată**.
   b. Pentru adresa IP la distanţă, selectaţi **Atribuit de sistemul la distanţă**.
   c. În secţiunea de rutare, selectaţi **Adăugare sistem la distanţă ca rută implicită**.
   d. Faceţi clic pe **OK** pentru încheierea profilului iniţiator.
7. Configuraţi un **Profil conexiune receptor** pe serverul iSeries din sediul central.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Răspuns
   - **Configuraţie legătură**: Aceasta ar putea fi linie singulară sau un pool de linii, în funcţie de mediul dumneavoastră.
8. În pagina General din Proprietăţi profil punct-la-punct nou, introduceţi un nume şi o descriere pentru profilul receptorului.

9. Faceţi clic pe **Conexiune** pentru a deschide pagina Conexiune. Alegeţi Nume linie corespunzător sau creaţi unul nou prin tastarea unui nume şi apoi apăsaţi **Nou**.
   a. În pagina General evidenţiaţi o resursă hardware existentă şi setaţi Cadre la **Asincron**.
   b. Faceţi clic pe **Modem** pentru a deschide pagina Modem. Din lista de selecţie Nume, alegeţi modemul pe care îl folosiţi.
   c. Faceţi clic pe **OK** pentru revenire la pagina Proprietăţi profil punct-la-punct nou.
10. Faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare.
   a. Bifaţi **Este necesar ca acest server iSeries să verifice identitatea sistemului la distanţă**.
   b. Adăugaţi un nou utilizator la distanţă în lista de validare.
   c. Verificaţi autentificarea CHAP-MD5.
11. Faceţi clic pe **Setări TCP/IP** pentru a deschide pagina Setări TCP/IP.
   a. Pentru adresele IP locale, selectaţi adresa IP a interfeţei sediului central (192.168.1.1) din caseta de selecţie.
   b. Pentru adresa IP la distanţă, selectaţi **Pe baza ID utilizator al sistemului la distanţă**. Va apare dialogul **Adrese IP definite de nume utilizator**. Faceţi clic pe **Adăugare**. Completaţi câmpurile nume utilizator, adresă IP şi mască subreţea pentru Apelant. În scenariul nostru, ar putea fi indicate următoarele:
      - Nume utilizator apelant: Locaţie_la_distanţă
      - Adresă IP: 192.168.2.1
      - Mască subreţea: 255.255.255.0

      Faceţi clic pe **OK** şi apoi apăsaţi din nou **OK** pentru a reveni la pagina Configurări TCP/IP.
   c. Selectaţi **Înaintare IP** pentru a activa alte sisteme din reţea pentru utilizarea acestui server iSeries ca gateway.
12. Faceţi clic pe **OK** pentru încheierea profilului receptor.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Referinţe înrudite

“Configurare legătură” la pagina 50
Configurare legătură defineşte tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni.

“Pool de linii” la pagina 51
Selectaţi acest serviciu linie pentru a configura conexiunea PPP pentru a folosi o linie dintr-un pool de linii. La pornirea conexiunii PPP, serverul iSeries selectează o linie neutilizată din pool-ul de linii. Pentru profiluri cu conectare pe linie telefonică la cerere, serverul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

Scenariu: Autentificarea conexiunilor apel telefonic cu RADIUS NAS

Rulând NAS (Network Access Server) pe serverul iSeries, cererile de autentificare de la clienţii prin apel telefonic pot fi rutate la un server RADIUS separat. Dacă este autentificat, RADIUS poate de asemenea controla adresele IP ale utilizatorului.

Situaţie

Reţeaua companiei dumneavoastră are utilizatori la distanţă ce se conectează la două servere iSeries dintr-o reţea distribuită cu conectare prin apel telefonic. Aveţi nevoie de o modalitate de a centraliza autentificarea service-ul şi contabilizarea, astfel încât un singur server să poată trata cererile de validare a ID-urilor de utilizator şi a parolelor şi să determine care adrese IP le sunt atribuite.

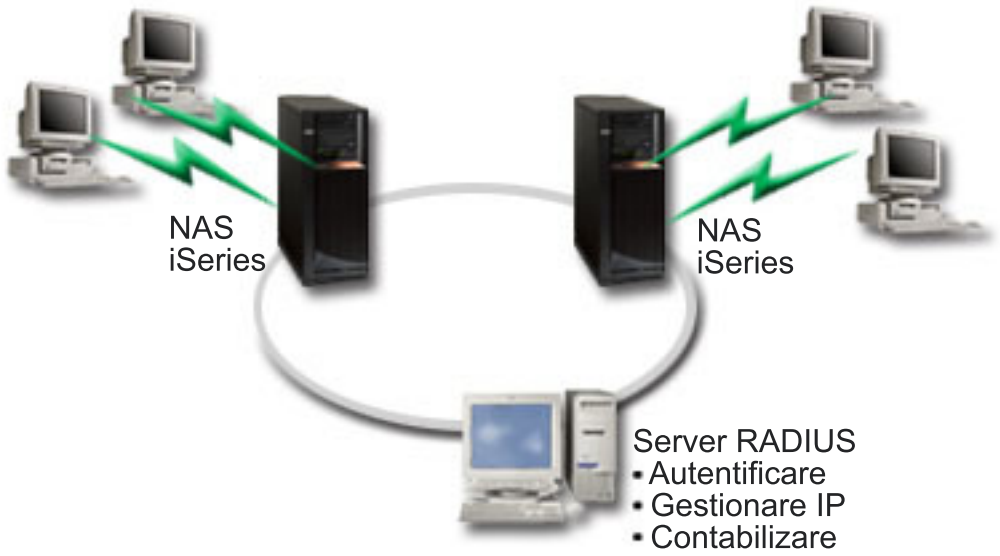


Figura 7. Autentificaţi conexiunile apel telefonic cu un server RADIUS

Soluţie

Când utilizatorii încearcă să se conecteze, serverul NAS ce rulează pe serverele iSeries expediază informaţiile de autentificare la un server RADIUS din reţea. Serverul RADIUS, care întreţine toate informaţiile de autentificare pentru reţeaua dumneavoastră, procesează cererile de autentificare şi răspunde. Dacă utilizatorul este validat, serverul RADIUS poate fi de asemenea configurat să aloce adresa IP peer şi poate activa contabilizarea pentru a urmări activitatea şi funcţionarea utilizatorilor. Pentru suport RADIUS, trebuie să definiţi serverul NAS RADIUS pe iSeries.

Configuraţie exemplu

1. În Navigator iSeries, expandaţi **Reţea**, faceţi clic dreapta pe **Servicii de acces la distanţă** şi selectaţi **Servicii**.
2. În fişa RADIUS, selectaţi **Activare conexiune RADIUS NAS** şi **Activare RADIUS pentru autentificare**. În funcţie de soluţia RADIUS, puteţi de asemenea alege ca RADIUS să trateze contabilizarea conexiunilor şi configurarea adreselor TCP/IP.
3. Faceţi clic pe butonul **Setări RADIUS NAS**.
4. Pe pagina General, introduceţi o descriere pentru acest server.
5. Pe pagina Server autentificare (şi opţional Server contabilizare), apăsaţi pe **Adăugare** şi introduceţi următoarele informaţii:
   a. În caseta Adresă IP locală, introduceţi adresa IP pentru interfaţa iSeries folosită pentru conectare la serverul RADIUS.
   b. În caseta Adresă IP server, introduceţi adresa IP pentru serverul RADIUS.
   c. În caseta Parolă, introduceţi parola folosită pentru a identifica serverul iSeries pentru serverul RADIUS.
   d. În caseta Port, introduceţi portul de pe iSeries folosit pentru a comunica cu serverul RADIUS. Valorile implicite sunt portul 1812 pentru serverul de autentificare sau portul 1813 pentru serverul de contabilizare.
6. Faceţi clic pe **OK**.
7. În Navigator iSeries, expandaţi **Reţea → Servicii de acces la distanţă**.
8. Selectaţi profilul conexiune care va folosi serverul RADIUS pentru autentificare. Serviciile RADIUS sunt aplicabile doar pentru profiluri conexiune Receptor.
9. În pagina Autentificare, selectaţi **Este necesar ca acest server iSeries să verifice identitatea sistemului la distanţă**.
10. Selectaţi **Autentificare la distanţă folosind server RADIUS**.

11. Selectaţi protocolul de autentificare. (PAP sau CHAP-MD5) Acest protocol trebuie folosit şi de serverul RADIUS.
12. Selectaţi **Folosire RADIUS pentru editarea şi contabilizarea conexiunii** .
13. Faceţi clic pe **OK** pentru a salva modificările profilului de conexiune.

Trebuie de asemenea să setaţi serverul RADIUS, incluzând suport pentru protocolul de autentificare, parole şi informaţii de contabilizare. Consultaţi vânzătorul dumneavoastră RADIUS pentru mai multe informaţii.

Când utilizatorii se conectează folosind acest profil de conexiune, iSeries va expedia informaţiile de autentificare serverului RADIUS specificat. Dacă utilizatorul este validat, conexiunea va fi permisă şi va folosi orice restricţii de conexiune specificate în informaţiile utilizatorului de pe serverul RADIUS.

Operaţii înrudite

"Activarea serviciilor RADIUS şi DHCP pentru profiluri conexiune" la pagina 61
Pentru a activa serviciul RADIUS sau DHCP pentru profilurile de conexiune receptor PPP, urmaţi aceşti paşi:

Referinţe înrudite

"Autentificare sistem" la pagina 43
Conexiunile PPP cu un server iSeries suportă mai multe opţiuni de autentificare a clienţilor la distanţă care se conectează prin apel telefonic la iSeries şi a conexiunilor la ISP sau alt server pe care iSeries îl apelează telefonic.

"Privire generală asupra RADIUS" la pagina 45
RADIUS (Remote Authentication Dial In User Service) este un protocol standard de Internet care oferă servicii de autentificare centralizată, contabilizare şi administrare IP pentru utilizatorii cu acces la distanţă dintr-o reţea distribuită cu conectare prin apel telefonic.

Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP

Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Situaţie

Reţeaua dumneavoastră are mai multe grupuri de utilizatori distribuiţi şi fiecare din ei are nevoie de acces la resurse diferite din LAN-ul companiei. Un grup de utilizatori are nevoie de acces la baza de date şi încă alte câteva aplicaţii, în timp ce o persoană are nevoie de acces apel telefonic (dial-up) la servicii HTTP, FTP şi Telnet, dar din motive de securitate nu trebuie să îi fie permis accesul la alt trafic sau alte servicii TCP/IP. Definirea detaliată a atributelor conexiunii şi a permisiunilor pentru fiecare utilizator ar mări eforturile dumneavoastră şi furnizarea restricţiilor de reţea pentru toţi utilizatorii acestui profil conexiune nu ar oferi destul control. Aţi prefera un mod de a defini setările şi permisiunile conexiunii pentru mai multe grupuri distincte de utilizatori care apelează acest server frecvent.

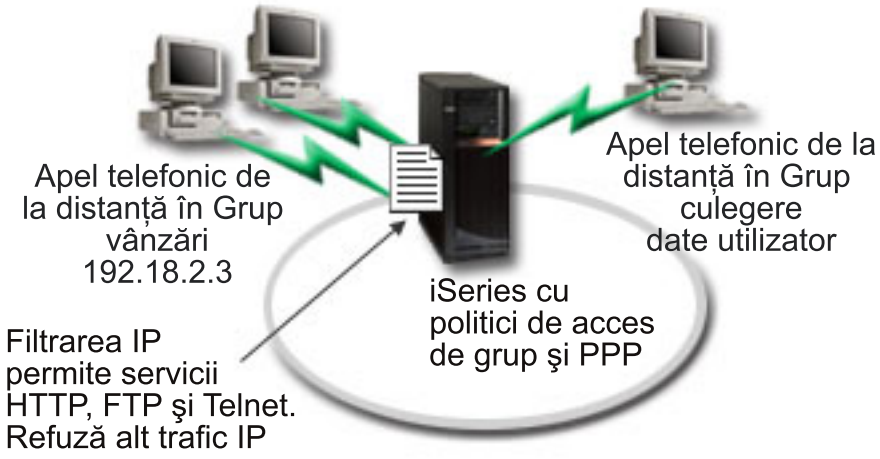


Figura 8. Aplicaţi setările de conexiune la conexiunile dial-up pe baza setărilor politicii de grup.

Soluţie

Trebuie să aplicaţi restricţii de filtrare IP unice asupra a două grupuri diferite de utilizatori. Pentru a realiza aceasta, veţi crea politici de acces de grup şi reguli de filtrare IP. Politicile de acces de grup fac referinţă la regulile de filtrare IP, deci trebuie să creaţi mai întâi regulile de filtrare. În acest exemplu, trebuie să creaţi un filtru PPP pentru a include reguli de filtrare IP pentru Politica de acces de grup ″IBM Business Partner″. Aceste reguli de filtrare vor permite serviciile HTTP, FTP şi Telnet, dar vor restricţiona accesul la alte servicii şi trafic TCP/IP prin serverul iSeries. Acest scenariu arată numai regulile de filtrare necesare pentru grupul vânzări; însă puteţi de asemenea să setaţi filtre similare pentru grupul ″Intrare date″.

În final, trebuie să creaţi politicile de acces de grup (câte una pentru fiecare grup) pentru a defini grupul dumneavoastră. Politicile de acces de grup vă permit să definiţi atribute conexiune comune pentru un grup de utilizatori. Adăugând o Politică de acces de grup la o Listă de validare de pe serverul iSeries, puteţi aplica aceste setări de conexiune în timpul procesului de autentificare. Politica de acces de grup specifică mai multe setări pentru sesiunea utilizatorului, inclusiv capacitatea de a aplica reguli filtru IP care vor restricţiona adresele IP şi serviciile TCP/IP disponibile unui utilizator în timpul sesiunii sale.

Configuraţie exemplu

1. Creaţi identificatorul filtru PPP şi filtrele reguli pachet IP care specifică permisiunile şi restricţiile pentru această politică de acces de grup.
   a. În Navigator iSeries, expandaţi **Reţea → Servicii de acces la distanţă**.
   b. Faceţi clic pe **Profiluri de conexiune receptor** şi selectaţi Politici de acces de grup.
   c. Faceţi clic dreapta pe un grup predefinit în panoul din dreapta şi selectaţi **Proprietăţi**.

      Notă: Dacă doriţi să creaţi o nouă politică de acces de grup, faceţi clic-dreapta pe Politică de acces de grup şi selectaţi **Politici noi de acces de grup**. Finalizaţi fişa General. Apoi selectaţi fişa Setări TCP/IP şi continuaţi cu pasul e de mai jos.
   d. Selectaţi fişa Setări TCP/IP şi apăsaţi pe **Avansat**.
   e. Selectaţi **Foloseşte reguli pachet IP pentru această conexiune** şi apăsaţi **Editare fişier reguli**. Aceasta va porni Editorul de reguli pachet IP şi va deschide fişierul de reguli pachet pentru filtre PPP.
   f. Deschideţi meniul **Inserare** şi selectaţi **Filtre** pentru a adăuga seturi de filtre. Folosiţi fişa General pentru a defini seturile de filtre şi fişa Servicii pentru a defini serviciul pe care îl permiteţi, ca HTTP. Următorul set filtru, ″services_rules″, va permite serviciile HTTP, FTP şi Telnet. Regulile de filtrare includ o instrucţiune implicită de refuzare, care restricţionează orice serviciu TCP/IP sau trafic IP care nu este permis în mod specific.

Notă: Adresele IP din următorul exemplu sunt rutabile global şi au doar scopul de exemplu.

```
###Următoarele 2 filtre vor permite traficul HTTP (browser web) din & spre sistem.

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

###Următoarele 4 filtre vor permite traficul FTP din & spre sistem.

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
###Următoarele 2 filtre vor permite traficul telnet din & spre sistem.

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. Deschideţi meniul **Inserare** şi selectaţi **Interfaţă filtru**. Folosiţi interfaţa filtru pentru a crea un identificator filtru PPP şi includeţi seturile filtru pe care le-aţi definit.

   1) În fişa General, introduceţi permitted_services pentru identificatorul de filtru PPP.

   2) În fişa Seturi filtru, alegeţi setul filtru **services_rules** şi apăsaţi pe **Adăugare**.

   3) Faceţi clic pe OK. Următoarea linie va fi adăugată la fişierul de reguli:

```
###Următoarea declaraţie leagă (asociază) setul filtru 'services_rules' cu
ID-ul filtru PPP "permitted_services". Acest ID filtru PPP
poate fi aplicat apoi interfeţei fizice asociate cu un profil conexiune PPP
sau Politică de acces de grup.

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

h. Salvaţi schimbările şi ieşiţi. Dacă trebuie să anulaţi aceste schimbări mai târziu, folosiţi interfaţa pe bază de caractere pentru a introduce comanda: RMVTCPTBL *ALL Aceasta va înlătura toate regulile de filtru şi NAT de pe server.

i. În dialogul **Setări TCP/IP avansate**, lăsaţi goală caseta Identificator filtru PPP şi apăsaţi pe **OK** pentru a ieşi. Ulterior ar trebui să aplicaţi identificatorul filtru pe care tocmai l-aţi creat unei Politici de acces de grup, nu acestui profil conexiune.

2. Definiţi o nouă Politică de acces de grup pentru acest grup utilizatori.

   a. În Navigator iSeries, expandaţi **Reţea → Servicii de acces la distanţă → Profiluri conexiune receptor**.

   b. Clic dreapta pe icoana Politică de acces de grup şi selectaţi Politică de acces de grup nouă. Navigator iSeries va afişa dialogul Definiţie nouă politică de acces de grup.

   c. În pagina General, introduceţi un nume şi o descriere pentru Politica de acces de grup.

   d. Pe pagina Setări TCP/IP:

- Selectaţi **Foloseşte reguli pachet IP pentru această conexiune** şi selectaţi identificatorul filtru PPP **permitted_services**.

e. Selectaţi **OK** pentru a salva Politica de acces de grup.

3. Aplicaţi Politica de acces de grup utilizatorilor asociaţi acestui grup.
   a. Deschideţi Profil conexiune receptor care controlează aceste conexiuni apel telefonic (dial-up).
   b. Pe pagina Autentificare a Profilului conexiune receptor, selectaţi lista de validare care conţine informaţia de autentificare a utilizatorilor şi apăsaţi pe **Deschidere**.
   c. Selectaţi un utilizator din grupul Vânzări asupra căruia vreţi să aplicaţi Politica de acces de grup şi apăsaţi pe **Deschidere**.
   d. apăsaţi pe **Aplică o politică de grup utilizatorului** şi selectaţi Politica de acces de grup definită la pasul 2.
   e. Repetaţi pentru fiecare utilizator Vânzări.

Concepte înrudite

“Configurarea unei politici de acces de grup” la pagina 59
Folderul **Politici de acces grup** de sub Profiluri de conexiune receptor oferă opţiuni pentru configurarea parametrilor conexiunilor punct-la-punct care se referă la un grup de utilizatori la distanţă. Acest lucru este valabil numai pentru acele conexiuni punct-la-punct iniţiate de un sistem la distanţă şi care sunt recepţionate de sistemul local.

“Suport politici de grup” la pagina 5
Suportul pentru Politici de grup permite administratorilor de reţea să definească politici de grup la nivel de utilizator pentru ajutor în administrarea resurselor şi permite ca politicile de control al accesului să fie atribuite utilizatorilor individuali în momentul deschiderii de sesiuni PPP sau L2TP în reţea.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

“Aplicarea regulilor de filtrare pachet IP unei conexiuni PPP” la pagina 60
Puteţi folosi un fişier cu reguli de pachet pentru a restricţiona accesul unui utilizator sau al unui grup la adrese IP din reţeaua dumneavoastră.

Referinţe înrudite

“Listă de validare” la pagina 46
O listă de validare este folosită pentru a păstra informaţiile ID utilizator şi parolă despre utilizatorii la distanţă.

“Autentificare sistem” la pagina 43
Conexiunile PPP cu un server iSeries suportă mai multe opţiuni de autentificare a clienţilor la distanţă care se conectează prin apel telefonic la iSeries şi a conexiunilor la ISP sau alt server pe care iSeries îl apelează telefonic.

Informaţii înrudite

IP packet rules (Filtering and NAT)

Scenariu: Partajarea unui modem între partiţiile logice folosind L2TP

Aţi configurat Ethernet virtual peste patru partiţii logice. Folosiţi acest scenariu pentru a activa partiţiile logice selectate să partajeze un modem. Aceste partiţii logice vor folosi modemul partajat pentru a accesa un LAN extern.

Situaţie

Sunteţi administratorul de sistem pentru o companie de dimensiune medie. Este timpul să actualizaţi echipamentul de calcul, dar aţi vrea să faceţi mai mult decât atât, aţi vrea să vă modernizaţi hardware-ul. Începeţi procesul prin consolidarea lucrului a trei servere mai vechi într-un singur server nou iSeries. Creaţi trei partiţii logice pe serverul iSeries. Noul server iSeries vine cu un modem intern 2793. Acesta este singurul procesor de intrare/ieşire (IOP) pe care-l aveţi care suportă PPP. Aveţi de asemenea, un modem vechi pentru suportul de client electronic (ECS) 7852-400.

Soluţie

Mai multe sisteme şi partiţii pot partaja aceleaşi modem-uri pentru conexiunile cu apelare telefonică, eliminând nevoia ca fiecare sistem sau partiţie să aibă modemul său. Acest lucru este posibil folosind tunelurile L2TP şi configurând profiluri L2TP care permit apeluri de ieşire. În reţeaua dumneavoastră, tunelurile vor funcţiona peste o reţea virtuală Ethernet şi peste o reţea fizică. Linia fizică conectează la un alt server din reţea, care de asemenea partajează modem-uri.

Detalii

Următoarea figură ilustrează caracteristicile reţelei pentru acest scenariu:

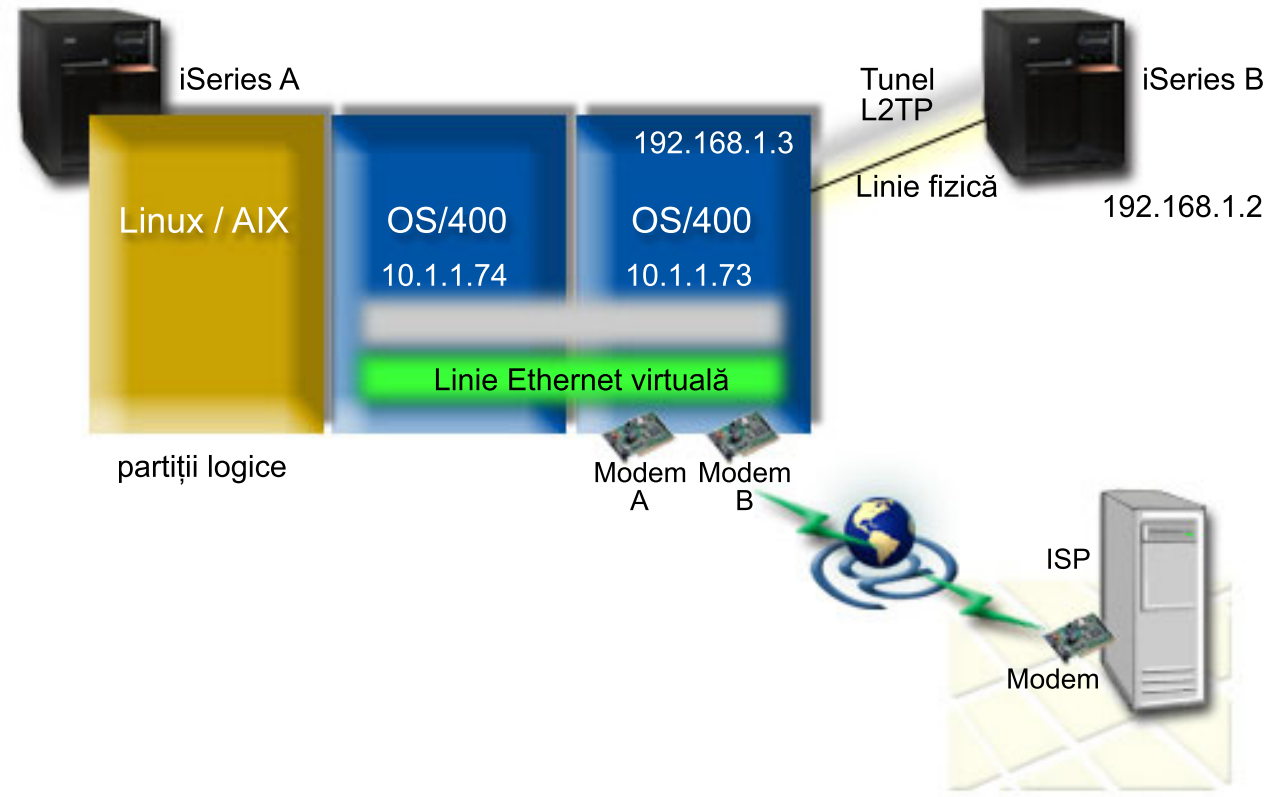


Figura 9. Mai multe sisteme care partajează acelaşi modem pentru conexiunile apel telefonic

Cerinţe preliminare şi presupuneri

Cerinţele de setare pentru iSeries-A includ:

- i5/OS V5R3 sau mai nouă, instalat pe partiţia care deţine modemurile capabile ASYNC
- Hardware care să vă permită partiţionarea.
- iSeries Access pentru Windows şi Navigator iSeries (Componenta Configurare şi service a Navigatorului iSeries), V5R3 sau mai nouă
- Aţi creat cel puţin două partiţii logice (LPAR) pe server. Partiţia care deţine modem-ul trebuie să aibă instalat i5/OS V5R3 sau mai nou. Celelalte partiţii pot avea instalat OS/400 V5R2, V5R3, Linux sau AIX. În acest scenariu, partiţiile folosesc fie sistemele de operare i5/OS, fie Linux.
- Aveţi creat Ethernet virtual pentru a comunica între partiţii. Vedeţi următorul scenariu: Crearea unei reţele Ethernet virtuale pentru comunicaţiile între partiţii.

Cerinţelele de setare pentru iSeries-B includ:

- iSeries Access pentru Windows şi Navigator iSeries (Componenta Configurare şi service a Navigatorului iSeries), V5R2 sau mai nouă

Informaţii înrudite

Partiţiile logice

Detalii scenariu: Partajarea unui modem între partiţiile logice folosind L2TP

După ce aţi terminat cu cerinţele preliminare, sunteţi gata să începeţi configurarea profilurilor L2TP.

Pasul 1: Configurarea unui profil terminator L2TP pentru orice interfaţă de pe partiţia care deţine modemul:

Urmaţi aceşti paşi pentru a crea un profil terminator pentru orice interfaţă:

1. În Navigator iSeries, expandaţi *serverul* → **Reţea** → **Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Profiluri de conexiune recepţie** şi selectaţi **Profil nou**.
3. Selectaţi următoarele opţiuni în pagina Setare şi faceţi clic pe **OK**:
   - **Tip protocol**: PPP
   - **Tip conexiune**: L2TP (linie virtuală)
   - **Mod de operare**: Terminator (server de reţea)
   - **Tip de serviciu linie**: Linie singulară
4. Pe fişa **Profil nou - General**, completaţi următoarele câmpuri:
   - **Nume**: toExternal
   - **Descriere**: Conexiune receptor pentru apelare în exterior
   - Selectaţi **Pornire profil cu TCP**.
5. Pe fişa **Profil nou - Conexiune**, completaţi următoarele câmpuri.
   - **Adresa IP a punctului final tunel local**: ANY
   - **Nume linie virtuală**: toExternal. Această linie nu are interfeţe fizice asociate. Linia virtuală descrie caracteristici diverse ale acestui profil PPP. Se deschide fereastra Proprietăţi linie L2TP. Faceţi clic pe fişa **Autentificare** şi introduceţi numele de gazdă al serverului. Faceţi clic pe **OK** pentru a vă întoarce la fişa Conexiune din fereastra Proprietăţi profil nou.
6. Faceţi clic pe **Permite stabilirea de apeluri către ieşire**. Apare dialogul **Proprietăţi apel telefonic de ieşire**.
7. Pe pagina Proprietăţi apel telefonic de ieşire, selectaţi un tip de serviciu linie.
   - **Tip de serviciu linie**: Pool de linii
   - **Nume**: dialOut
   - Faceţi clic pe **Nou**. Apare dialogul **Proprietăţi pool nou de linii**.
8. În fereastra Proprietăţi pool nou de linii, selectaţi liniile şi modemurile la care permiteţi apelurile telefonice de ieşire şi faceţi clic pe **Adăugare**. Dacă aveţi nevoie să definiţi aceste linii, selectaţi **Linie nouă**. Interfeţele pe partiţiile care deţin aceste modemuri, vor încerca să folosească orice linie care este deschisă pentru acest pool de linii. Apare dialogul Proprietăţi linie nouă.
9. La fişa **Proprietăţi linie nouă - General**, introduceţi informaţii în următoarele câmpuri:
   - **Nume**: linie1
   - **Descriere**: prima linie şi primul modem pentru pool de linii (modem intern 2793)
   - **Resursă hardware**: cmn03 (port comunicaţii)
10. Acceptaţi valorile implicite la celelalte fişe şi faceţi clic pe **OK** ca să vă întoarceţi la fereastra Proprietăţi pool nou de linii.
11. În fereastra Proprietăţi pool nou de linii, selectaţi liniile şi modemurile la care permiteţi apelurile telefonice de ieşire şi faceţi clic pe **Adăugare**. Verificaţi dacă modemul 2793 este selectat pentru pool.
12. Selectaţi **Linie nouă** din nou pentru a adăuga modemul ECS 7852-400. Apare dialogul Proprietăţi linie nouă.
13. La fişa **Proprietăţi linie nouă - General**, introduceţi informaţii în următoarele câmpuri:

- **Nume**: linie2
- **Descriere**: a doua linie şi al doilea modem pentru pool de linii (modem extern ECS 7852-400)
- **Resursă hardware**: cmn04 (port comunicaţii)
- **Cadre**: Asincron

14. La fişa **Proprietăţi linie nouă - Modem**, selectaţi modemul extern (7852–400) şi faceţi clic **OK** ca să vă întoarceţi la fereastra Proprietăţi pool nou de linii.
15. Selectaţi orice altă linie disponibilă pe care vreţi să o adăugaţi la pool-ul de linii şi faceţi clic pe **Adăugare**. În acest exemplu, verificaţi că cele două noi modemuri adăugate mai sus sunt listate sub câmpul *Linii selectate pentru pool* şi faceţi clic pe **OK** să vă întoarceţi la fereastra Proprietăţi apel telefonic de ieşire.
16. În fereastra Proprietăţi apel telefonic de ieşire, introduceţi Numerele de apel implicite şi faceţi clic pe **OK** pentru a vă întoarce la fereastra Proprietăţi profil PPP nou.

    Notă: Aceste numere pot fi cele ale ISP-ului dumneavoastră care va fi apelat frecvent de celelalte sisteme folosind aceste modemuri. Dacă pe celelalte sisteme se specifică un număr de telefon de *PRIMARY sau *BACKUP, numerele reale apelate vor fi cele specificate aici. Dacă celelalte sisteme specifică un număr de telefon real, atunci va fi folosit numărul de telefon.
17. În fişa **Setări TCP/IP**, selectaţi următoarele valori:
    - **Adresă IP locală**: Fără
    - **Adresă IP de la distanţă**: Fără

    Notă: Dacă folosiţi profilul şi pentru a termina sesiunile L2TP, trebuie să alegeţi adresa IP locală care reprezintă serverul iSeries. Pentru adresa IP de la distanţă, puteţi selecta un pool de adrese care este în aceeaşi subreţea ca şi serverul. Toate sesiunile L2TP vor primi adresele lor IP din acest pool. Pentru alte consideraţii, vedeţi Suport profil conexiuni multiple.
18. În fişa **Autentificare**, acceptaţi toate valorile implicite.

Aţi terminat de configurat un profil terminator L2TP pe partiţia cu modemurile. Următorul pas este să configuraţi un profil originator - apel telefonic la distanţă L2TP pentru 10.1.1.74.

Pasul 2: Crearea unui profil originator L2TP pe 10.1.1.74:

Urmaţi aceşti paşi pentru a crea un profil originator L2TP:

1. În Navigator iSeries, expandaţi **10.1.1.74 → Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Profiluri de conexiune originator** şi selectaţi **Profil nou**.
3. Selectaţi următoarele opţiuni în pagina Setare şi faceţi clic pe **OK**:
   - **Tip protocol**: PPP
   - **Tip conexiune**: L2TP (linie virtuală)
   - **Mod de operare**: Apel telefonic de la distanţă
   - **Tip de serviciu linie**: Linie singulară
4. Pe fişa **General**, completaţi următoarele câmpuri:
   - **Nume**: toModem
   - **Descriere**: conexiunea originator care duce la partiţia care deţine modemul
5. Pe fişa **Conexiune**, completaţi următoarele câmpuri:

   Nume linie virtuală: toModem Această linie nu are interfeţe fizice asociate. Linia virtuală descrie caracteristici diverse ale acestui profil PPP. Se deschide fereastra Proprietăţi linie L2TP.
6. În fişa **General**, introduceţi o descriere pentru linia virtuală.
7. În fişa **Autentificare**, introduceţi numele gazdei locale a partiţiei şi faceţi clic pe **OK** pentru a vă întoarce la pagina Conexiune.
8. În câmpul **Numere de telefon de la distanţă**, adăugaţi *PRIMARY şi *BACKUP. Aceasta permite profilului să folosească aceleaşi numere de telefon ca şi profilul terminator de pe partiţia care deţine modemul.

9. În câmpul **Adresa IP sau numele de gazdă punct final tunel de la distanţă**, introduceţi adresa punctului final tunel de la distanţă (10.1.1.73).
10. În fişa **Autentificare**, selectaţi **Permite sistemului de la distanţă să identifice serverul iSeries** .
11. Sub Protocolul de autentificare de folosit, selectaţi **Cerere parolă criptată (CHAP-MD5)**. Implicit este selectat şi **Permite protocolul de autentificare extins**.

    Notă: Protocolul trebuie să se potrivească cu protocolul pe care-l foloseşte serverul la care se sună.
12. Introduceţi numele utilizatorului şi parola.

    Notă: Numele utilizatorului şi parola trebuie să se potrivească cu un nume de utilizator şi parolă valide de pe serverul unde apelaţi.
13. Mergeţi la fişa **Setări TCP/IP** şi verificaţi câmpurile necesare:
    - **Adresa IP locală**: Alocată de sistemul de la distanţă
    - **Adresa IP de la distanţă**: Alocată de sistemul de la distanţă
    - **Rutare**: Nu este necesară rutare suplimentară
14. Faceţi clic pe **OK** pentru a salva profilul PPP.

Pasul 3: Configurarea unui profil de apel telefonic la distanţă L2TP pentru 192.168.1.2:

Repetaţi pasul 2. Dar, modificaţi adresa de punct final tunel de la distanţă la 192.168.1.3 (interfaţa fizică la care se conectează iSeries B).

Notă: Acestea sunt adrese IP fictive şi sunt folosite doar pentru exemplificare.

Pasul 4: Testarea conexiunii:

După ce aţi terminat de configurat ambele servere, trebuie să testaţi conectivitatea pentru a vă asigura că sistemele partajează modemul pentru a ajunge la reţele externe. Pentru a face aceasta, urmaţi aceşti paşi:

1. Asiguraţi-vă că profilul terminator L2TP este activ.
   a. În Navigator iSeries, expandaţi **10.1.1.73 → Reţea → Servicii de acces la distanţă → Profiluri conexiune receptor**.
   b. În panoul din dreapta, găsiţi profilul cerut (toExternal) şi verificaţi câmpul **Stare** şi vedeţi dacă este *Activ*. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.
2. Porniţi profilul de apel de la distanţă pe 10.1.1.74.
   a. În Navigator iSeries, expandaţi **10.1.1.74 → Reţea → Servicii de acces la distanţă → Profiluri conexiune originator**.
   b. În panoul din dreapta, găsiţi profilul cerut (toModem) şi verificaţi câmpul **Stare** şi vedeţi dacă este *Activ*. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.
3. Porniţi profilul de apel de la distanţă pe iSeries B.
   a. În Navigator iSeries, expandaţi **192.168.1.2 → Reţea → Servicii de acces la distanţă → Profiluri conexiune originator**.
   b. În panoul din dreapta, găsiţi profilul creat şi verificaţi câmpul **Stare** şi vedeţi dacă este *Activ*. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.
4. Dacă este posibil, faceţi ping la ISP sau altă destinaţie pe care aţi apelat-o telefonic, pentru a verifica dacă sunt active ambele profiluri. Veţi încerca ping de la ambele 10.1.1.74 şi 192.168.1.2.
5. Ca o alternativă, puteţi verifica şi Starea conexiunii.
   a. În Navigator iSeries, expandaţi *serverul necesar (cum ar fi 10.1.1.73)* **→ Reţea → Servicii de acces la distanţă → Profiluri conexiune originator**.
   b. În panoul din dreapta, faceţi clic-dreapta pe profilul creat şi selectaţi **Conexiuni**. Pe fereastra Stare conexiune puteţi vedea profilurile care sunt active, inactive, în curs de conectare sau altele.

Planificare PPP

Puteţi citi acest subiect pentru informaţii despre crearea şi administrarea conexiunilor PPP.

Referinţe înrudite

"Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries" la pagina 14
Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

"Scenariu: Conectarea LAN-ului de la birou la Internet cu un modem" la pagina 16
Administratorii configurează de obicei reţele care permit angajaţilor să aibă acces la Internet. Ei pot folosi un modem pentru a conecta serverul iSeries la un ISP. Clienţii PC ataşaţi prin LAN pot să comunice cu Internetul folosind serverul iSeries ca gateway.

"Informaţii înrudite pentru PPP" la pagina 65
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Cerinţe software şi hardware

Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul dintre calculatoare, serverul iSeries, poate fi originator sau receptor.

Serverul iSeries trebuie să îndeplinească următoarele cerinţe preliminare pentru a putea fi accesat de sistemele la distanţă.

- Navigator iSeries cu suport TCP/IP.
- Unul din cele două profiluri de conexiune:
  - Un Profil conexiune originator pentru tratarea conexiunilor PPP care trebuie expediate
  - Un Profil conexiune receptor pentru tratarea conexiunilor PPP care trebuie primite
- O consolă staţie de lucru PC pe care este instalat iSeries Access pentru Windows 95 sau mai nou cu Navigator iSeries.
- Un adaptor instalat

  Puteţi alege unul din următoarele adaptoare:
  - 2699*: IOA două linii WAN
  - 2720*: IOA PCI WAN/Twinax
  - 2721*: IOA PCI două linii WAN
  - 2745*: IOA PCI două linii WAN (înlocuieşte IOA 2721)
  - 2742*: IOA două linii (înlocuieşte IOA 2745)
  - 2771: IOA două linii WAN, cu un modem integrat V.90 la portul 1 şi o interfaţă standard de comunicaţii la portul 2. Pentru a folosi portul 2 al adaptorului 2771, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător.
  - 2772: IOA cu două porturi WAN cu modem integrat V.90
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A: Adaptor Ethernet pentru conexiuni PPPoE.
  - 2793*: IOA cu două porturi WAN, cu un modem integrat V.92 la portul 1 şi o interfaţă standard de comunicaţii la portul 2. Pentru a folosi portul 2 al adaptorului 2793, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător. Acesta înlocuieşte IOA model 2771.
  - 2805: IOA cu patru porturi WAN, cu un modem analog V.92 integrat. Acesta înlocuieşte modelele 2761 şi 2772.

  * Aceste adaptoare cer un modem V.90 extern (sau mai sus) sau adaptor terminal ISDN şi un cablu RS-232 (EIA 232) sau compatibil.
- Unul din următoarele, în funcţie de tipul de conexiune şi linie:
  - modem intern sau extern sau CSU (channel service unit)/DSU (data service unit)
  - adaptor terminal ISDN (integrated services digital network)

- Dacă doriţi să vă conectaţi la Internet, trebuie să aveţi şi un cont pentru conectarea pe linie telefonică cu un ISP (Furnizor de servicii Internet). ISP ar trebui să vă ofere numerele de telefon şi informaţiile necesare pentru conectarea la Internet.

  Referinţe înrudite

  “Profiluri de conexiuni” la pagina 3
  Profilurile conexiune punct-la-punct definesc un set de parametri şi resurse pentru conexiuni PPP specifice. Puteţi porni profiluri care folosesc aceste setări de parametri pentru a apela (iniţia) sau pentru a aştepta (recepţiona) conexiuni PPP.

  “Modemuri” la pagina 39
  Pentru conexiuni PPP pot fi folosite atât modemuri interne, cât şi externe.

  “CSU/DSU” la pagina 39
  Un CSU (Channel Service Unit) este un dispozitiv care conectează un terminal la o linie digitală. Un DSU (Data Service Unit) este un dispozitiv care realizează funcţii de protecţie şi diagnostic pentru o linie de telecomunicaţii. În mod obişnuit, cele două dispozitive formează o singură unitate, CSU/DSU.

  “Adaptoare terminale ISDN” la pagina 39
  ISDN oferă o conexiune digitală care permite comunicarea folosind orice combinaţie de voce, date şi secvenţe video, împreună cu alte aplicaţii multimedia.

Alternative conexiune

PPP poate transmite datagrame prin legături punct-la-punct seriale.

PPP permite interconectarea de echipamente ale mai multor fabricanţi şi protocoale multiple prin standardizarea comunicaţiilor punct-la-punct. Nivelul de legătură de date din PPP foloseşte cadre stil HDLC (High-level Data Link Control) pentru încapsularea datagramelor în legăturile de telecomunicaţie punct-la-punct sincrone şi asincrone.

În timp ce PPP suportă o mare varietate de tipuri de legături, SLIP (Serial-Line Internet Protocol) suportă doar tipuri de legături sincrone. SLIP este folosit în general numai pentru legături analogice. Companiile locale de telefoane oferă servicii de telecomunicaţii tradiţionale într-o scală crescătoare a capacităţilor şi costurilor. Aceste servicii folosesc facilităţile existente de voce ale companiei de telefoane între client şi sediul central.

Legăturile PPP stabilesc o conexiune fizică între o gazdă locală şi una la distanţă. Legăturile cu conectare oferă lărgime de bandă dedicată. Aceste conţin şi o varietate de protocoale şi rate de date. Cu legăturile PPP, puteţi opta între următoarele alternative de conectare:

Linii telefonice analogice

Conexiunea analogică, care foloseşte modemuri pentru transportarea datelor prin linii închiriate sau comutate, stă la baza PPP.

Liniile închiriate sunt conexiuni permanente între două locaţii specificate, în timp ce liniile comutate sunt linii telefonice pentru voce obişnuite. Cele mai rapide modemuri actuale operează la o rată necomprimată de 56 kbps. Totuşi, din cauza raportului semnal-zgomot din circuitele telefonice cu voce necondiţionată, această rată nu poate fi atinsă de obicei.

Pretenţiile fabricanţilor de modemuri cu rate bps (bit-per-secundă) mai mari se bazează de obicei pe algoritmul de compresie a datelor (CCITT V.42bis) utilizat de aceste modemuri. Deşi V.42bis are potenţialul de a duce la o reducere de patru ori a volumului datelor, compresia depinde de date şi uneori atinge chiar şi 50%. Datele deja comprimate sau criptate pot chiar să crească când este aplicat V.42bis. X2 sau 56Flex extind rata bps la 56 Kbps pentru liniile telefonice analogice. Aceasta este o tehnologie hibridă care necesită ca un capăt al legăturii PPP să fie digital în timp ce celălalt trebuie să fie analog. În plus, rata de 56 Kbps este valabilă doar când transferaţi date de la capătul digital al legăturii la cel analogic. Această tehnologie este potrivită pentru conexiuni cu ISP dacă capătul digital al legăturii şi hardware-ul se află la locaţia lor. În mod obişnuit, vă puteţi conecta la un modem analog V.24 printr-o interfaţă serială RS-232 cu un protocol asincron la rate de până la 115,2 Kbps.

Standardul V.90 a rezolvat problema compatibilităţii K56flex/x2. Standardul V.90 este rezultatul unui compromis între taberele x2 şi K56flex din industria modemurilor. Prin vizualizarea reţelei telefonice comutate publice ca reţea digitală, tehnologia V.90 poate accelera datele de pe Internet la un calculator la viteze de până la 56 Kbps. Tehnologia V.90 diferă de alte standarde deoarece aceasta criptează datele digital în loc de a le modula aşa cum fac modemurile analogice. Transferul datelor este o metodă asimetrică, astfel că transmisiile ascendente (de obicei apăsarea tastelor şi comenzi mouse de la un calculator la locaţia centrală, care necesită o lărgime de bandă mai mică) continuă la ratele convenţionale de până la 33.6 Kbps. Datele de la un modem sunt transferate ca o transmisie analogică care oglindeşte standardul V.34. Doar transferul de date descendent beneficiază de viteza înalte V.90.

Standardul V.92 îmbunătăţeşte V.90 permiţând viteze ascendente de până la 48 Kbps. În plus, timpii de conectare pot fi reduşi mulţumită îmbunătăţirilor aduse la procesul hand-shaking şi modem-urile care suportă o caracteristică ″hold″ pot rămâne acum conectate în timp ce linia telefonică acceptă apeluri sau foloseşte apel în aşteptare.

Servicii digitale şi DDS

Puteţi folosi cu PPP serviciul digital şi DDS (Digital Data Services).

Serviciu digital

Prin serviciul digital, datele sunt transmise de la calculatorul emitentului la sediul central al companiei telefonice, la furnizorul de la distanţă, la sediul central şi apoi la calculatorul receptorului în format digital. Semnalul digital oferă o lărgime de bandă mult mai mare şi o siguranţă sporită faţă de cel analogic. Un sistem cu semnal digital elimină multe din problemele cu care au de a face modemurile analogice, cum sunt zgomotul, calitatea variabilă a liniei şi atenuarea semnalului.

DDS (Digital Data Services)

DDS (Digital Data Services) este cel mai rudimentar dintre serviciile digitale. Legăturile DDS sunt conexiuni închiriate, permanente, care rulează la rate fixate de până la 56Kbps. Acest serviciu mai este numit în mod frecvent DS0.

Vă puteţi conecta la DDS folosind o casetă specială numită *CSU/DSU (Channel Service Unit/Data Service Unit)*, care înlocuieşte modemul din scenariul analogic. DDS are limitări fizice care se referă în principal la distanţa dintre CSU/DSU şi sediul central al companiei telefonice. DDS funcţionează cel mai bine când distanţa este mai mică de 9000 m (30000 picioare). Companiile telefonice pot face adaptări pentru distanţe mai mari prin derivaţii ale semnalului, dar acest serviciu este mai scump. DDS este cel mai potrivit pentru conectarea a două locaţii care sunt deservite de acelaşi sediu central. Pentru conexiuni între distanţe mari care se întind între mai multe sedii centrale, cheltuielile datorate distanţei vor face DDS inaplicabil. În aceste cazuri, Switched-56 poate fi o soluţie mai bună. În mod obişnuit, vă puteţi conecta la un DDS CSU/DSU prin interfaţa serială V.35, RS449 sau X:21 cu un protocol sincron la rate de până la 56Kbps.

Referinţe înrudite

“CSU/DSU” la pagina 39
Un CSU (Channel Service Unit) este un dispozitiv care conectează un terminal la o linie digitală. Un DSU (Data Service Unit) este un dispozitiv care realizează funcţii de protecţie şi diagnostic pentru o linie de telecomunicaţii. În mod obişnuit, cele două dispozitive formează o singură unitate, CSU/DSU.

“Switched-56”
Când nu aveţi nevoie de o conexiune permanentă, puteţi economisi bani folosind serviciul digital comutat, care este numit de obicei *Switch-56 (SW56)*.

Switched-56

Când nu aveţi nevoie de o conexiune permanentă, puteţi economisi bani folosind serviciul digital comutat, care este numit de obicei *Switch-56 (SW56)*.

O legătură SW56 este similară setării DDS (Digital Data Services) prin faptul că DTE (data terminal equipment) se conectează la serviciul digital prin intermediul CSU/DSU. Totuşi, un CSU/DSU SW56 include un dispozitiv de la care se introduce numărul de telefon al gazdei la distanţă. SW56 vă permite să realizaţi conexiuni digitale prin apel telefonic

la oricare utilizator SW56 de oriunde din ţară sau din lume. Un apel SW56 este transportat în reţeaua digitală la distanţă ca şi un apel vocal digitalizat. SW56 foloseşte aceleaşi numere de telefon ca şi sistemul telefonic local, iar taxele de utilizare sunt aceleaşi ca şi pentru apeluri vocale. SW56 este doar în reţelele nord americane şi este limitat la canale singulare care pot transporta doar date. SW56 este o alternativă pentru locurile unde ISDN nu este disponibil. În mod obişnuit, vă puteţi conecta la un SW56 CSU/DSU prin interfaţa serială V.35 sau RS449 cu un protocol sincron la rate de până la 56Kbps. Cu o unitate de apelare/răspuns V.25bis, controlul datelor şi al apelului se face printr-o singură interfaţă serială.

Referinţe înrudite

"Servicii digitale şi DDS" la pagina 34
Puteţi folosi cu PPP serviciul digital şi DDS (Digital Data Services).

"ISDN (Integrated Services Digital Network)"
ISDN (Integrated Services Digital Network) oferă conectivitate digitală comutată capăt-la-capăt (end-to-end). Totuşi, spre deosebire de alte servicii, ISDN poate transporta atât voce, cât şi date prin aceeaşi conexiune.

ISDN (Integrated Services Digital Network)

ISDN (Integrated Services Digital Network) oferă conectivitate digitală comutată capăt-la-capăt (end-to-end). Totuşi, spre deosebire de alte servicii, ISDN poate transporta atât voce, cât şi date prin aceeaşi conexiune.

Există mai multe tipuri de servicii ISDN, dintre care BRI (Basic Rate Interface) este cel mai folosit. BRI este format din două canale B de 64 Kbps pentru transportul datelor client şi un canal D pentru transportul datelor de semnalizare. Cele două canale B pot fi legate pentru a obţine o rată combinată de 128 Kbps. În unele zone, compania telefonică poate limita fiecare canal B la 56 Kbps sau la 112 Kbps în combinaţie. Există şi o restricţie fizică, aceea că localizarea clientului trebuie să fie la cel mult 5400 m (18000 de picioare) de comutatorul sediului central. Această distanţă poate fi extinsă prin repetoare. Vă puteţi conecta la ISDN cu un dispozitiv numit adaptor terminal. Cele mai multe adaptoare terminale au o unitate integrată de sfârşit de reţea (NT1) care permite conexiunea directă la o mufă de telefon. În mod obişnuit, adaptoarele terminale se conectează la calculatorul dumneavoastră printr-o legătură asincronă RS-232 şi folosesc setul de comenzi AT pentru configurare şi control, asemănător cu modemurile analogice convenţionale. Fiecare marcă are propria extensie de comenzi AT pentru setarea parametrilor unici pentru ISDN. În trecut, existau multe probleme de interoperabilitate între diferitele mărci de adaptoare terminale ISDN. Aceste probleme apăreau în mare parte din cauza varietăţii protocoalelor de adaptare a ratei care erau în V.110 şi V.120 ca şi schemele de legare pentru cele două canale B.

În prezent, s-a optat pentru protocolul PPP sincron cu PPP Multilink pentru legarea a două canale B. Unii fabricanţi de adaptoare terminale integrează capacitatea V.34 (modem analogic) în adaptoarele lor terminale. Aceasta permite clienţilor cu o singură linie ISDN să folosească atât apeluri ISDN cât şi analogice convenţionale profitând de capacităţile de simultaneitate voce/date ale serviciilor ISDN. Noua tehnologie permite adaptorului terminal şi operarea ca parte server digital pentru clienţi 56K(X2/56Flex).

În mod obişnuit, aveţi nevoie să vă conectaţi la un adaptor terminal ISDN printr-o interfaţă serială RS-232 folosind un protocol asincron cu rate de până la 230,4 Kbps. Însă rata maximă în bauzi a serverului iSeries pentru comunicaţii asincrone peste RS-232 este de 115,2 Kbps. Din păcate, aceasta restricţionează rata maximă de transfer în octeţi la 11,5 kiloocteţi/sec, în timp ce adaptorul terminal cu multi-linking este capabil de 14/16 kiloocteţi necomprimaţi. Unele adaptoare terminale suportă comunicaţii sincrone peste RS-232 la 128 Kbps, dar rata maximă a serverului iSeries pentru comunicaţii sincrone peste RS-232 este de 64 Kbps.

Serverul iSeries este capabil de rulare asincronă peste V.35 la rate de până la 230,4 Kbps, dar producătorii de adaptoare terminale nu oferă în general o astfel de configuraţie. Convertoarele de interfaţă care convertesc RS-232 în interfaţa V.35 ar putea fi o soluţie rezonabilă a problemei, dar această abordare nu a fost evaluată pentru serverul iSeries. O altă posibilitate este de a utiliza adaptoarele terminale cu protocolul sincron interfaţă V.35 la rata de 128 Kbps. Deşi această clasă de adaptoare terminale există, se pare că nu sunt multe oferte de PPP Multilink sincron.

Referinţe înrudite

"Switched-56" la pagina 34
Când nu aveţi nevoie de o conexiune permanentă, puteţi economisi bani folosind serviciul digital comutat, care este numit de obicei *Switch-56 (SW56)*.

“Adaptoare terminale ISDN” la pagina 39
ISDN oferă o conexiune digitală care permite comunicarea folosind orice combinaţie de voce, date şi secvenţe video, împreună cu alte aplicaţii multimedia.

T1/E1 şi T1 fracţional

T1/E1 şi T1 fracţional sunt două alternative de conexiune validă.

T1/E1

O conexiune T1 uneşte 24 de canale multiplexate cu diviziunea timpului (TDM) de 64 Kbps (DS0) într-un circuit de cupru cu 4 fire. Aceasta creează o lărgime totală de bandă de 1,544 Mbps. Un circuit E1 în Europa şi alte părţi ale lumii uneşte 32 de canale de 64 Kbps într-un total de 2,048 Mbps. TDM permite ca mai mulţi utilizatori să partajeze un mediu de transmisie digital prin folosirea porţiunilor de timp prealocat. Multe PBX (private branch exchanges) digitale profită de serviciul T1 pentru a importa multiple circuite de apel printr-o singură linie T1 în loc de a avea 24 de perechi de fire rutate între PBX şi compania telefonică. Este important de remarcat faptul că T1 poate fi partajat între voce şi date. Un serviciu telefonic poate interveni asupra unui subset din cele 24 de canale ale unei legături T1, de exemplu, lăsând canalele rămase pentru conectarea la Internet. Un dispozitiv multiplexor T1 este necesar pentru administrarea celor 24 de canale atunci când un trunchi T1 este partajat de servicii multiple. Pentru o singură conexiune numai pentru date, circuitul poate fi rulat fără a se face TDM asupra semnalului. În consecinţă, se poate folosi un dispozitiv CSU/DSU mai simplu. În mod obişnuit, vă puteţi conecta la un multiplexor sau CSU/DSU T1/E1 prin interfaţa serială V.35 sau RS 449 cu protocol sincron la rate care sunt multiplu de 64 Kbps până la 1,544 Mbps sau 2,048 Mbps. Multiplexorul sau CSU/DSU oferă temporizarea în reţea.

T1 fracţional

Cu FT1 (Fractional T1), un client poate închiria orice submultiplu de 64 Kbps al unei linii T1. FT1 este util atunci când costul T1 dedicat este prohibitiv pentru lărgimea de bandă efectivă pe care o foloseşte clientul. Cu FT1, plătiţi doar pentru ceea ce aveţi nevoie. În plus, FT1 are următoarea caracteristică care nu este disponibilă într-un circuit T1 complet: Multiplexarea canalelor DS0 la sediul central al companiei telefonice. Capătul la distanţă al unui circuit FT1 este la un comutator de conectare încrucişată cu acces digital (Digital Access Cross-Connect Switch) care este întreţinut de compania telefonică. Sistemele care partajează acelaşi comutator digital pot comuta canalele DS0. Această schemă este utilizată de ISP care folosesc un singur trunchi T1 de la locaţia lor la comutatorul digital al companiei telefonice. În aceste cazuri, clienţi multipli pot fi serviţi cu serviciul FT1. În mod obişnuit, vă puteţi conecta la un multiplexor sau CSU/DSU T1/E1 prin interfaţa serială V.35 sau RS 449 cu protocol sincron la un multiplu de 64 Kbps. Cu FT1, aveţi pre-alocat un subset al celor 24 de canale. Multiplexorul T1 trebuie să fie configurat să folosească doar porţiunile de timp care sunt atribuite serviciului dumneavoastră.

Frame relay

Frame Relay este un protocol pentru rutarea cadrelor în reţea pe baza câmpului de adresă IP (identificator conexiune pentru legătura de date) din cadru şi pentru administrarea rutei sau a conexiunii virtuale.

Reţelele frame-relay din U.S. suportă rate de transfer al datelor cu viteze T1 (1,544 Mbps) şi T3 (45 Mbps). Vă puteţi gândi la frame relay ca fiind o modaliate de utilizare a liniilor T1 şi T3 existente deţinute de un furnizor de servicii. Majoritatea companiilor telefonice oferă acum servicii Frame Relay pentru clienţii care doresc conexiuni la viteze între 56 Kbps şi T1. (În Europa, vitezele Frame Relay variază între 64 Kbps şi 2 Mbps. În S.U.A., Frame Relay este foarte utilizat deoarece este relativ ieftin. Totuşi, acesta este înlocuit în unele zone de tehnologii mai rapide, cum este ATM (asynchronous transfer mode).

Suport L2TP pentru conexiuni PPP

L2TP (Layer 2 Tunneling Protocol) este un protocol tunel care extinde PPP pentru a suporta un tunel la nivel de legătură între un client L2TP care face o cerere (L2TP Access Concentrator sau LAC) şi un punct final server destinaţie L2TP (L2TP Network Server sau LNS).

L2TP (Layer 2 Tunneling Protocol)

Folosind tuneluri L2TP (Layer 2 Tunneling Protocol), este posibilă separarea locaţiei la care se încheie protocolul de conectare pe linie telefonică de locul de unde este furnizat accesul în reţea. Acest lucru face ca L2TP să mai fie numit şi *Virtual PPP*.

Un ISP (Furnizor de servicii Internet) foloseşte modul de linie virtuală pentru operarea în VPN (reţele private virtuale). Vedeţi Configurarea unei conexiuni L2TP protejate prin VPN pentru a înţelege mai bine modul în care IPSec lucrează cu L2TP.

Aceste figuri ilustrează trei implementări diferite de tunel ale L2TP.

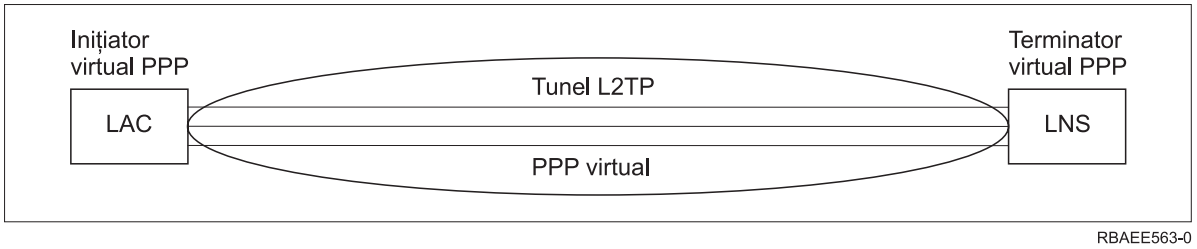


Figura 10. Iniţiator virtual PPP sau terminator virtual PPP

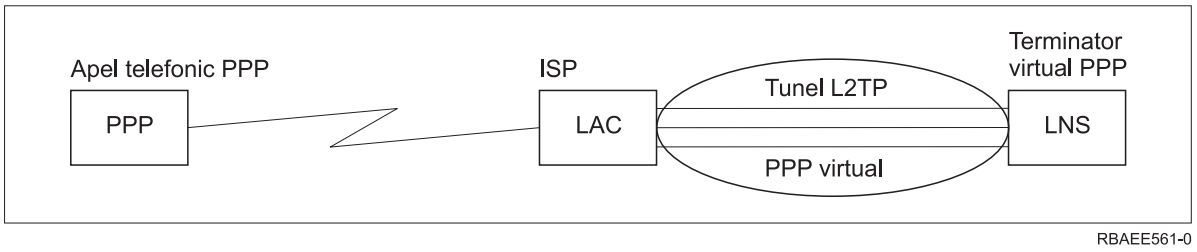


Figura 11. Iniţiator apel telefonic PPP sau terminator virtual PPP

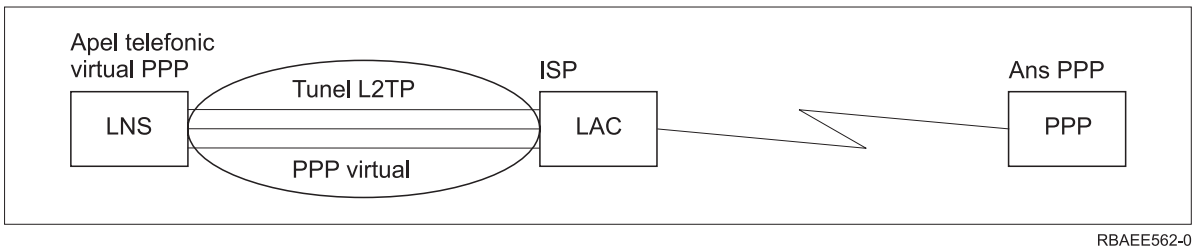


Figura 12. Apel telefonic virtual PPP sau răspuns virtual PPP

Protocolul L2TP este documentat ca Request For Comment standard RFC2661. Informaţii suplimentare despre RFC-uri se găsesc la pagina Web RFC Editor. Un tunel L2TP se poate extinde peste toată sesiunea PPP sau numai peste un segment dintr-o sesiune cu două segmente. Aceasta se poate reprezenta prin patru modele de tunel diferite:

Tunel voluntar:

În modelul tunel voluntar, un tunel este creat de utilizator, de obicei prin folosirea unui client activat L2TP.

Prin urmare, utilizatorul va trimite pachete L2TP la ISP, care le va trimite mai departe la LNS. Pentru tunelul voluntar, ISP nu trebuie să suporte L2TP, iar iniţiatorul tunelului L2TP se află efectiv pe acelaşi sistem ca şi clientul la distanţă. În acest model, tunelul se extinde peste întreaga sesiune PPP de la clientul L2TP la LNS.

Model de tunel obligatoriu - apel de intrare:

În modelul tunel obligatoriu - apel de intrare, un tunel este creat fără acţiuni ale utilizatorului şi fără ca acesta să aibă opţiuni.

Prin urmare, utilizatorul va trimite pachete PPP la ISP (LAC), care le va încapsula în L2TP şi le va transmite într-un tunel la LNS. În cazurile cu tunel obligatoriu, ISP trebuie să fie capabil de L2TP. În acest model tunelul se întinde doar pe segmentul sesiunii PPP dintre ISP şi LNS.

Model de tunel obligatoriu - apel la distanţă:

În modelul cu tunel obligatoriu - apel la distanţă, gateway-ul principal (LNS) iniţiază un tunel la un ISP (LAC) şi instruieşte ISP-ul să apeleze clientul care răspunde PPP.

Acest model este pentru cazurile în care clientul PPP care răspunde de la distanţă are un număr de telefon permanent, stabilit cu un ISP. Acest model ar trebui folosit atunci când o companie cu o prezenţă stabilă pe Internet trebuie să realizeze o conexiune cu un sediu la distanţă care necesită o legătură prin linie telefonică. În acest model tunelul se întinde doar pe segmentul sesiunii PPP dintre LNS şi ISP.

Conexiune multi-hop L2TP:

O conexiune multi-hop L2TP este un mod de redirecţionare a traficului L2TP în numele LAC-urilor şi LNS-urilor client.

O conexiune multi-hop este stabilită folosind un gateway multi-hop L2TP (un sistem care leagă profilurile L2TP terminator şi iniţiator). Pentru stabilirea unei conexiuni multi-hop, gateway-ul multi-hop L2TP se comportă ca un LNS pentru un set de LAC-uri şi în acelaşi timp ca un LAC pentru un anumit LNS. Un tunel este stabilit de la un LAC client la un gateway multi-hop L2TP şi apoi se stabileşte un alt tunel între gateway-ul multi-hop L2TP şi un LNS destinaţie. Traficul L2TP de la LAC client va fi apoi redirecţionat de gateway-ul multi-hop L2TP către LNS destinaţie, iar traficul de la LNS destinaţie va fi redirecţionat la LAC client.

Suport PPPoE (DSL) pentru conexiuni PPP

DSL (digital subscriber line) se referă la o clasă tehnologică folosită pentru a obţine mai multă lărgime de bandă pe cablurile telefonice din cupru existente ce se află între un client şi un furnizor ISP.

DSL permite servicii vocale şi de transmitere a datelor cu viteză mare simultan printr-o singură pereche de fire telefonice din cupru. Vitezele modem-urilor au crescut treptat folosind diferite compresii şi alte tehnologii, dar la maximul de azi (56 kbit/s) ele se apropie de limita teoretică pentru această tehnologie. Tehnologia DSL permite viteze mult mai mari de la un capăt la altul al perechii răsucite de linii de la Biroul central acasă, la şcoală sau la servici. Viteze de până la 2 Megabiţi pe secundă sunt realizabile în unele zone. PPPoE vine de la Protocol punct la punct peste Ethernet (Point to Point Protocol over Ethernet). PPP este de obicei folosit peste comunicaţii seriale cum sunt conexiunile apel telefonic prin modem. Mulţi furnizori de servicii Internet DSL folosesc acum PPP peste Ethernet datorită trăsăturilor sale de logare şi securitate adăugate. Ce este un modem DSL? Un ″modem″ DSL este un dispozitiv care este plasat la oricare capăt al liniei telefonice din cupru pentru a permite unui calculator (sau LAN) să fie conectate la Internet printr-o conexiune DSL. Spre deosebire de o conexiune apel telefonic, de obicei nu necesită o linie telefonică dedicată (un splitter permite liniei să fie împărţită simultan). Deşi modemurile DSL se aseamănă modemurilor analogice convenţionale, ele oferă transfer mult mai ridicat.

Echipamentul conexiunii

Serverele iSeries folosesc modemuri, adaptoare terminale ISDN, adaptoare token-ring, adaptoare Ethernet sau dispozitive CSU/DSU pentru a trata conexiunile PPP.

Acestea sunt cele trei tipuri de echipamente de comunicaţie pe care le puteţi folosi în mediul PPP.

- Modemuri
- CSU/DSU

- Adaptoare terminale ISDN
- Adaptoare Ethernet (pentru conexiuni PPPoE).

Modemuri

Pentru conexiuni PPP pot fi folosite atât modemuri interne, cât şi externe.

Setul de comenzi folosit de un modem este de obicei descris în documentaţia modemului. Comenzile sunt folosite pentru resetarea şi iniţializarea modemului şi pentru a indica modemului să formeze numărul de telefon al sistemului la distanţă. Fiecare model de modem trebuie definit înainte ca acesta să poată fi utilizat cu un profil de conexiune PPP deoarece modele de modem diferite au şiruri de comenzi de iniţializare diferite. Dacă este un modem intern, atunci şirurile modemului sunt deja definite pentru utilizare.

Pe serverul iSeries sunt predefinite multe modele de modemuri, dar pot fi definite şi altele prin Navigator iSeries. Poate fi folosită o definiţie existentă ca bază pentru noul tip care va fi definit. Dacă nu sunteţi sigur de comenzile folosite de modemul dumneavoastră sau dacă nu aveţi acces la documentaţia modemului, începeţi cu definiţia de modem generic Hayes. Definiţiile gata realizate, livrate, nu pot fi modificate. Pot fi însă adăugate comenzi suplimentare şirului de apelare sau comenzii de iniţializare.

Puteţi folosi modemul ECS (electronic customer support) furnizat cu serverul iSeries pentru a stabili conexiuni PPP. Pe sistemele mai vechi, modemul ECS era un modem extern IBM 7852-400. Pe sistemele mai noi, se poate folosi pentru modemul ECS un 2771, un 2793 sau oricare alt modem intern suportat.

Referinţe înrudite

“Cerinţe software şi hardware” la pagina 32
Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul dintre calculatoare, serverul iSeries, poate fi originator sau receptor.

CSU/DSU

Un CSU (Channel Service Unit) este un dispozitiv care conectează un terminal la o linie digitală. Un DSU (Data Service Unit) este un dispozitiv care realizează funcţii de protecţie şi diagnostic pentru o linie de telecomunicaţii. În mod obişnuit, cele două dispozitive formează o singură unitate, CSU/DSU.

Vă puteţi gândi la CSU/DSU ca fiind un modem foarte puternic şi scump. Un astfel de dispozitiv este necesar pentru ambele capete ale unei conexiuni T-1 sau T-3; unităţile de la ambele capete trebuie să fie de la acelaşi fabricant.

Referinţe înrudite

“Cerinţe software şi hardware” la pagina 32
Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul dintre calculatoare, serverul iSeries, poate fi originator sau receptor.

“Servicii digitale şi DDS” la pagina 34
Puteţi folosi cu PPP serviciul digital şi DDS (Digital Data Services).

Adaptoare terminale ISDN

ISDN oferă o conexiune digitală care permite comunicarea folosind orice combinaţie de voce, date şi secvenţe video, împreună cu alte aplicaţii multimedia.

Va trebui să verificaţi dacă adaptorul terminal poate fi folosit pentru serverul iSeries.

Urmaţi aceşti paşi pentru configurarea adaptorului terminal:

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Modemuri** şi selectaţi **Modem nou**.
3. În caseta de dialog **Proprietăţi modem nou**, introduceţi valorile corecte în toate casetele câmp ale fişei General. Asiguraţi-vă că aţi specificat adaptor terminal ISDN ca dispozitiv de comunicare.
4. Selectaţi fişa **Parametri ISDN**.

5. Adăugaţi sau modificaţi proprietăţile ISDN din fişa **Parametri ISDN** pentru a corespunde proprietăţilor necesare pentru adaptorul terminal.

Operaţii înrudite

"Exemplu: Configurarea unui adaptor terminal ISDN" la pagina 56

Referinţe înrudite

"Cerinţe software şi hardware" la pagina 32
Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul dintre calculatoare, serverul iSeries, poate fi originator sau receptor.

"ISDN (Integrated Services Digital Network)" la pagina 35
ISDN (Integrated Services Digital Network) oferă conectivitate digitală comutată capăt-la-capăt (end-to-end). Totuşi, spre deosebire de alte servicii, ISDN poate transporta atât voce, cât şi date prin aceeaşi conexiune.

Recomandări de adaptoare terminale ISDN:

Există alte câteva adaptoare de terminale pe care le puteţi folosi.

Adaptorul terminal ISDN extern (modem-ul ISDN) sugerat este **3Com/U.S. Robotics Courier I ISDN V.Everything** . El suportă conexiuni prin modem analogic V.34, V.90 (X2), V.92 şi Multilink PPP peste ISDN în ambele moduri, de iniţiere şi de răspuns, de pe serverul iSeries. De asemenea, suportă în mod automat CHAP (Challenge Handshake Authentication Protocol) pentru conexiunea PPP ISDN. De asemenea, sunt disponibile următoarele adaptoare terminale ISDN: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA şi ADtran ISU 2x64 Dual Port.

- **Conexiuni care sunt iniţiate de pe serverul iSeries.** Cererilor de identificare CHAP iniţiate de partea receptoare li se răspunde de către adaptorul terminal Courier I, în timpul negocierii PAP (Password Authentication Protocol) cu serverul iSeries. Răspunsurile PAP nu apar în conexiunea ISDN.
- **Conexiuni la care răspunde serverul iSeries.** Courier I necesită autentificarea CHAP de către partea apelantă în cazul în care configurarea pentru răspuns a serverului iSeries face ca serverul iSeries să deschidă autentificarea printr-o cerere de identificare CHAP. Dacă serverul iSeries deschide autentificarea cu PAP, adaptorul terminal Courier I este autentificat cu PAP.

Dacă folosiţi un modem Courier I anterior anului 1999, verificaţi dacă modemul Courier I este conectat la serverul iSeries printr-un cablu V.35, pentru a obţine performanţe maxime de la conexiunea ISDN. O dată cu modemul Courier I este furnizată o interfaţă RS-232 cu cablu de modem V.35; însă versiunile mai vechi ale acestui cablu au un conector V.35 necorespunzător. Contactaţi 3Com/US Robotics Customer Support pentru înlocuire.

Notă: Potrivit 3Com/US Robotics, versiunea V.35 a acestui adaptor terminal nu mai există, deşi unele ar mai putea fi găsite la furnizori terţă parte. Versiunea RS-232 este în continuare recomandată la o performanţa într-o oarecare măsură mai redusă pe serverul iSeries, deoarece conexiunile RS-232 sunt limitate la 115,2 Kb.

Puteţi obţine un V.35 pentru adaptorul RS-232 şi de la Black Box Corporation. Numărul de parte componentă este FA-058.

Aveţi grijă să setaţi viteza liniei V.35 pe serverul iSeries la 230,4 Kbps.

Restricţii la adaptoarele terminale ISDN:

Au fost evaluate următoarele adaptoare terminale din acest subiect. Acestea sunt recomandate numai pentru originea conexiunilor la distanţă ISDN de la serverul iSeries.

3Com Impact IQ ISDN:

Acest adaptor terminal nu este recomandat pentru serverul iSeries din următoarele motive:

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuşi, ar putea suporta conexiuni prin modem analogic V.34 folosind conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.

- Adaptorul terminal nu se poate conecta la serverul iSeries cu viteze mai mari de 115200 bps.
- Adaptorul terminal nu suportă automat CHAP (Challenge Handshake Authentication Protocol). Dacă însă se setează S84=0, se permite realizarea autentificării CHAP pe serverul iSeries.
- Serverul iSeries nu poate determina momentul de încheiere a conexiunii atunci când monitorizează semnalul Data Set Ready de la adaptorul terminal. Aceasta poate duce la o eventuală expunere de securitate a sistemului.

Motorola BitSurfr Pro ISDN:

Acest adaptor terminal nu este recomandat pentru serverul iSeries din următoarele motive:

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuşi, ar putea suporta conexiuni prin modem analogic V.34 folosind conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.
- Adaptorul terminal nu se poate conecta la serverul iSeries cu viteze mai mari de 115200 bps.
- Adaptorul terminal nu suportă automat autentificarea CHAP. Dacă însă se setează @M2=C, se se permite realizarea autentificării CHAP pe serverul iSeries.
- Adaptorul terminal nu permite în mod automat răspunsul la apeluri single-link şi Multilink PPP. Adaptorul terminal originator la distanţă trebuie să fie setat pe acelaşi protocol (single-link sau Multilink) ca şi adaptorul terminal ce răspunde.
- Mecanismul hardware de control al fluxului pentru serverul iSeries nu funcţionează bine cu acest adaptor terminal. Aceasta duce la performanţe degradate când serverul iSeries trimite date printr-o conexiune PPP Multilink.

Tratare adrese IP

Conexiunile PPP permit mai multe seturi diferite de opţiuni pentru gestiunea adreselor IP în funcţie de tipul de profil conexiune.

Referinţe înrudite

“Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE” la pagina 11
Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

Filtrare pachet IP

Filtrarea pachetelor IP limitează serviciile pentru un utilizator individual când este logat la o reţea.

Filtrarea pachetelor poate permite sau refuza accesul pe baza adreselor IP de destinaţie sau porturilor, sau pe baza ambelor. Pot fi aplicate politici diferite prin definirea mai multor seturi de Reguli de filtrare pachet, fiecare având un Identificator de filtru PPP unic. Regulile de filtrare a pachetelor pot fi alocate pentru un profil de conexiune receptor particular sau pot fi alocate folosind o politică de grup care va aplica regulile de filtrare pentru acea categorie de utilizator. Regulile filtru pachet nu sunt definite în PPP, ci sunt definite sub Reguli pachet IP în Navigator iSeries.

În cazul conexiunilor L2TP, trebuie să se folosească VPN cu filtrare IPSec pentru protejarea traficului din reţea.

Referinţe înrudite

“Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE” la pagina 11
Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

Informaţii înrudite

Regulile pachetelor IP

VPN

Strategia de gestionare a adreselor IP

Ar trebui să fiţi familiar cu strategia gestiunii adresei IP din reţeaua dumneavoastră înaintea configurării unui profil conexiune PPP. Această strategie va avea impact asupra multor decizii pe parcursul procesului de configurare inclusiv strategia dumneavoastră de autentificare, consideraţii de securitate şi setări TCP/IP.

Profiluri de conexiune originator:

În mod obişnuit, adresele IP locale şi la distanţă definite pentru un profil originator vor fi definite ca *Atribuit de sistemul la distanţă*. Aceasta permite administratorilor de pe sistemul la distanţă să aibă control asupra adreselor IP care vor fi folosite pentru conexiune. Aproape toate conexiunile la ISP (Furnizori de Internet) vor fi definite în acest mod, deşi mulţi ISP pot oferi adrese IP fixate în schimbul unei taxe suplimentare.

Dacă definiţi adrese IP fixate pentru adresa IP locală sau la distanţă, va trebui să vă fiţi sigur că sistemul la distanţă este definit să accepte adresele pe care le definiţi. O aplicaţie tipică este definirea adresei locale IP ca adresă IP fixată şi cea la distanţă să fie atribuită de către sistemul la distanţă. Sistemul pe care îl conectaţi poate fi definit în acelaşi mod astfel ca le realizarea conexiunii cele două sisteme să schimbe între ele adresele IP ca modalitate de învăţare a adresei IP a sistemului la distanţă. Acest fapt ar putea fi util atunci când un sediu apelează un altul pentru conectivitate temporară.

Un alt aspect este dacă doriţi să activaţi Mascarea adreselor IP. De exemplu, dacă serverul iSeries se conectează la Internet printr-un ISP, atunci aceasta ar putea permite unei reţele ataşate din spatele serverului iSeries să acceseze şi ea Internetul. În principiu, serverul iSeries ascunde adresele IP ale sistemelor din reţeaua din spatele adresei IP locale atribuite de ISP, făcând astfel ca traficul IP să pară ca provenind de la serverul iSeries. Mai există şi alte considerente privind rutarea, atât pentru sistemele din LAN (pentru asigurarea că traficul lor pentru Internet este trimis la serverul iSeries), cât şi pentru serverul iSeries, pe care trebuie să aveţi posibilitatea de a activa caseta ’adăugare sisteme la distanţă ca rută implicită’.

Profiluri de conexiune receptor:

Profilurile conexiune receptor au mult mai multe consideraţii şi opţiuni despre adresa IP decât are profilul conexiune originator. Cum vă configuraţi adresele IP depinde de planul de gestiune al adresei IP pentru reţeaua dumneavoastră, performanţa specifică şi cerinţele funcţionale pentru această conexiune şi planul de securitate.

Adrese IP locale

Pentru un profil receptor singular puteţi defini o adresă IP unică sau puteţi folosi o adresă IP locală existentă pe serverul iSeries. Aceasta va deveni adresa IP care va identifica capătul server iSeries al conexiunii PPP. Pentru profiluri receptor definite pentru a suporta conexiuni multiple în acelaşi timp, trebuie să folosiţi o adresă IP locală existentă. Dacă nu sunt prezente adrese IP locale existente atunci puteţi crea o adresă IP virtuală în acest scop.

Adrese IP la distanţă

Sunt multe opţiuni pentru alocarea adreselor IP la distanţă clienţilor PPP. Următoarele opţiuni pot fi specificate în pagina TCP/IP a profilului conexiune receptor.

Notă: Dacă vreţi ca sistemul la distanţă să fie considerat parte a LAN-ului, trebuie să configuraţi rutarea adresei IP, să specificaţi o adresă IP din intervalul de adrese IP pentru sistemele din LAN şi să verificaţi dacă a fost activată înaintarea (forwarding) IP pentru acest profil de conexiune şi pentru sistemul iSeries.

Tabela 8. Opţiuni alocare adresă IP pentru conexiuni profil receptor

Opţiune	Descriere
Adresă IP fixă	Definiţi singura adresă IP care va fi atribuită utilizatorilor la distanţă în momentul conectării pe linie telefonică. Aceasta este o adresă IP doar pentru gazdă (masca subreţea este 255.255.255.255) şi este numai pentru profiluri receptor conexiune singulară.

Tabela 8. Opţiuni alocare adresă IP pentru conexiuni profil receptor (continuare)

Opţiune	Descriere
Grup de adrese	Definiţi adresa IP de început şi apoi un domeniu al numărului de adrese IP suplimentare care se vor defini. Fiecărui utilizator care se conectează i se atribuie o adresă IP unică din intervalul definit. Aceasta este o adresă IP doar pentru gazdă (masca subreţea este 255.255.255.255) şi este numai pentru profiluri receptor conexiune multiplă.
RADIUS	Adresa IP la distanţă şi masca sa de subreţea vor fi determinate de serverul Radius. Aceasta este valabil doar dacă sunt definite următoarele: • Suportul Radius pentru autentificare şi adresare a fost activat din configurarea serviciilor Server de acces la distanţă. • Este activată autentificarea pentru profilul de conexiune receptor şi este definită autentificarea la distanţă de către Radius.
DHCP	Adresa IP la distanţă este determinată de serverul DHCP direct sau indirect prin retransmisie DHCP. Aceasta este valabilă doar dacă suportul DHCP a fost activat din configuraţia serviciilor Server de acces la distanţă. Aceasta este o adresă IP numai pentru gazdă (masca subreţea este 255.255.255.255).
Pe baza ID-ului utilizator al sistemului la distanţă.	Adresa IP la distanţă este determinată de ID-ul utilizator definit pentru sistemul la distanţă atunci când este autentificat. Aceasta permite administratorului să atribuie diferite adrese IP la distanţă (şi măştile subreţea asociate) utilizatorului care se conectează pe linie telefonică. De asemenea, aceasta permite definirea unor rute suplimentare pentru fiecare dintre aceste ID-uri de utilizator, astfel încât puteţi să vă adaptaţi mediul la un utilizator la distanţă cunoscut. Autentificarea trebuie să fie activată pentru ca această funcţie să fie corectă.
Definiţi adrese IP suplimentare bazate pe ID-ul utilizator al sistemului la distanţă.	Această opţiune permite definirea adreselor IP pe baza ID-ului de utilizator al sistemului la distanţă. Această opţiune este selectată automat (şi trebuie folosită) dacă alocarea adresei IP la distanţă este definită ca fiind **Pe baza ID-ului utilizator al sistemului la distanţă**. Această opţiune este acceptată şi pentru metodele de atribuire a adresei IP pentru adresa IP fixată şi Grupul de adrese. Când un utilizator la distanţă se conectează la serverul iSeries, se face o căutare pentru a determina dacă o adresă IP la distanţă este definită special pentru acest utilizator. Dacă da, acea adresă IP, mască şi set de rute posibile vor fi folosite pentru conexiune. Dacă utilizatorul nu este definit atunci adresa IP va avea valoarea implicită definită Adresă IP fixă sau următoarea adresă IP din grupul de adrese IP.
Permite sistemului la distanţă să-ţi definească propria adresă IP	Această opţiune permite ca un utilizator la distanţă să îşi definească propria adresă dacă negociază aceasta. Dacă nu negociază pentru folosirea propriei adrese IP atunci adresa IP la distanţă va fi determinată de metoda de alocare a adresei IP definită la distanţă. Această opţiune este iniţial dezactivată şi aveţi grijă înainte de activarea ei.
Rutare adresă IP	Clientul cu conectare prin apel telefonic şi serverul iSeries trebuie să aibă rutarea adresei IP configurată corect dacă clientul are nevoie de acces la orice adrese IP din LAN-ul de care aparţine serverul iSeries.

Autentificare sistem

Conexiunile PPP cu un server iSeries suportă mai multe opţiuni de autentificare a clienţilor la distanţă care se conectează prin apel telefonic la iSeries şi a conexiunilor la ISP sau alt server pe care iSeries îl apelează telefonic.

iSeries suportă mai multe metode pentru întreţinerea informaţiilor de autentificare, începând de la simple liste de validare pe iSeries, care conţin listele cu utilizatorii autorizaţi şi parolele asociate, până la suportul pentru serverele RADIUS, care întreţin informaţii de autentificare detaliate pentru utilizatorii reţelei. iSeries suportă de asemenea mai multe opţiuni pentru criptarea ID-ului de utilizator şi parolei, începând de la un simplu schimb de parole şi până la suportul de macerare cu CHAP-MD5. Vă puteţi specifica preferinţele pentru autentificarea sistemului, inclusiv un ID de utilizator şi o parolă care să fie folosite pentru a valida serverul iSeries când apelează în exterior, în fişa **Autentificare** a profilului de conexiune din Navigator iSeries.

Referinţe înrudite

"Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE" la pagina 11
Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

"Scenariu: Autentificarea conexiunilor apel telefonic cu RADIUS NAS" la pagina 22
Rulând NAS (Network Access Server) pe serverul iSeries, cererile de autentificare de la clienţii prin apel telefonic pot fi rutate la un server RADIUS separat. Dacă este autentificat, RADIUS poate de asemenea controla adresele IP ale utilizatorului.

"Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP" la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

CHAP-MD5

Challenge Handshake Authentication Protocol (CHAP-MD5) foloseşte un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul care autentifică şi de dispozitivul la distanţă.

Cu CHAP, ID-ul utilizator şi parola sunt întotdeauna criptate, aşa că el este un protocol mai sigur decât PAP (Password Authentication Protocol). Acest protocol este eficient împotriva playback-ului şi încercărilor de acces prin încercare-şi-eroare (trial-and-error). Autentificarea CHAP poate apare mai mult de o dată în timpul unei conexiuni.

Sistemul care autentifică trimite o cerere de identificare dispozitivului la distanţă care încearcă să se conecteze la reţea. Sistemul la distanţă răspunde cu o valoare care este calculată de un algoritm comun (MD-5) pe care-l folosesc ambele dispozitive. Sistemul de autentificare verifică răspunsul cu propriul calcul. Autentificarea este acceptată când valorile se potrivesc; altfel, conexiunea este încheiată.

Referinţe înrudite

"Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries" la pagina 14
Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

"PAP" la pagina 45
PAP (Password Authentication Protocol) foloseşte un dialog de confirmare pentru a oferi sistemului peer o metodă simplă de stabilire a propriei identităţi.

"EAP"
EAP (Extensible Authentication Protocol) permite modulelor de autentificare terţe să interacţioneze cu implementarea PPP.

EAP

EAP (Extensible Authentication Protocol) permite modulelor de autentificare terţe să interacţioneze cu implementarea PPP.

EAP extinde PPP prin furnizarea unui mecanism suport standard pentru scheme de autentificare cum sunt cartelele cu jeton, Kerberos, Public Key şi S/Key. EAP răspunde cererii în creştere de mărire a autentificării RAS cu dispozitive de securitate de la terţe părţi. EAP protejează VPN-urile securizate de hackeri care folosesc atacuri 'dicţionar' şi ghicirea parolei. EAP îmbunătăţeşte PAP (Password Authentication Protocol) şi CHAP (Challenge Handshake Authentication Protocol).

Cu EAP, informaţiile de autentificare nu sunt incluse în informaţii, ci mai degrabă cu informaţiile. Aceasta permite serverelor la distanţă să negocieze autentificarea necesară înainte de a recepta sau transmite orice informaţie.

Serverul iSeries nu suportă direct EAP. Puteţi totuşi folosi autentificarea la distanţă folosind un server RADIUS care poate suporta unele din schemele suplimentare de autentificare descrise mai sus.

Referinţe înrudite

"PAP"
PAP (Password Authentication Protocol) foloseşte un dialog de confirmare pentru a oferi sistemului peer o metodă simplă de stabilire a propriei identităţi.

"CHAP-MD5" la pagina 44
Challenge Handshake Authentication Protocol (CHAP-MD5) foloseşte un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul care autentifică şi de dispozitivul la distanţă.

PAP

PAP (Password Authentication Protocol) foloseşte un dialog de confirmare pentru a oferi sistemului peer o metodă simplă de stabilire a propriei identităţi.

Dialogul (handshake) are loc la stabilirea legăturii. După ce a fost stabilită conexiunea, dispozitivul de la distanţă trimite sistemului de autentificare o pereche alcătuită din ID-ul de utilizator şi parola. În funcţie de corectitudinea perechii, sistemul de autentificare continuă sau încheie conexiunea.

Autentificarea PAP necesită ca numele şi parola utilizator să fie trimise sistemului la distanţă într-un format text clar. Cu PAP, ID-ul şi parola utilizator nu sunt niciodată criptate, ceea ce face posibilă urmărirea lor şi le face vulnerabile la atacul hackerilor. Din acest motiv, ar trebui să folosiţi CHAP dacă este posibil.

Referinţe înrudite

"CHAP-MD5" la pagina 44
Challenge Handshake Authentication Protocol (CHAP-MD5) foloseşte un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul care autentifică şi de dispozitivul la distanţă.

"EAP" la pagina 44
EAP (Extensible Authentication Protocol) permite modulelor de autentificare terţe să interacţioneze cu implementarea PPP.

Privire generală asupra RADIUS

RADIUS (Remote Authentication Dial In User Service) este un protocol standard de Internet care oferă servicii de autentificare centralizată, contabilizare şi administrare IP pentru utilizatorii cu acces la distanţă dintr-o reţea distribuită cu conectare prin apel telefonic.

Modelul client-server RADIUS are un NAS (Network Access Server - Server de acces la reţea) care operează drept client al unui server RADIUS. Serverul iSeries, care se comportă ca NAS, trimite informaţii despre utilizator şi conexiune unui server RADIUS desemnat, folosind protocolul standard RADIUS definit în RFC 2865.

Serverele RADIUS acţionează asupra cererilor de conectare a utilizatorului recepţionate, autentificând utilizatorul şi apoi returnând toate informaţiile de configurare necesare către NAS, astfel încât NAS (serverul iSeries) să poată furniza servicii autorizate utilizatorului autentificat.

Dacă nu poate fi contactat un server RADIUS, serverul iSeries poate ruta cererile de autentificare la un alt server. Aceasta permite firmelor mari să ofere utilizatorilor un serviciu de conectare prin apel telefonic cu un ID utilizator unic pentru deschidere de sesiuni pentru accesul comun, indiferent de punctul de acces folosit.

Când serverul RADIUS primeşte o cerere de autentificare, cererea este validată, apoi serverul RADIUS decriptează pachetul de date pentru a accesa informaţiile despre nume şi parolă utilizator. Informaţiile sunt transmise sistemului de securitate corespunzător care este acceptat. Acestea pot fi fişierele de parolă UNIX, Kerberos, un sistem de securitate comercial sau chiar un sistem de securitate dezvoltat de client. Serverul RADIUS trimite înapoi serverului iSeries serviciile pe care utilizatorul autentificat este autorizat să le folosească, cum ar fi o adresă IP. Cererile de contabilizare RADIUS sunt tratate de o manieră similară. Informaţiile de contorizare ale utilizatorului la distanţă pot fi trimise unui server de contorizare RADIUS desemnat. Protocolul standard de contorizare RADIUS este definit în RFC 2866. Serverul de contorizare RADIUS acţionează asupra cererilor de contorizare prin înregistrarea informaţiilor din cererea de contorizare RADIUS.

Referinţe înrudite

"Scenariu: Autentificarea conexiunilor apel telefonic cu RADIUS NAS" la pagina 22
Rulând NAS (Network Access Server) pe serverul iSeries, cererile de autentificare de la clienţii prin apel telefonic pot fi rutate la un server RADIUS separat. Dacă este autentificat, RADIUS poate de asemenea controla adresele IP ale utilizatorului.

Listă de validare

O listă de validare este folosită pentru a păstra informaţiile ID utilizator şi parolă despre utilizatorii la distanţă.

Puteţi folosi liste de validare existente sau puteţi să creaţi propriile liste din pagina de autentificare Profil de conexiune receptor. Intrările listă de validare vă cer de asemenea să identificaţi un tip protocol de autentificare pentru a fi asociat cu ID-ul utilizator şi parola. Acesta poate fi **criptat - CHAP-MD5/EAP** sau **necriptat - PAP**.

Consultaţi ajutorul interactiv pentru informaţii suplimentare.

Referinţe înrudite

"Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP" la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Consideraţii lărgime de bandă - Multilink

Adesea, este necesară o lărgime de bandă suplimentară pentru efectuarea anumitor task-uri, dar aceasta nu este necesară tot timpul.

În aceste cazuri, achiziţionarea de hardware specializat şi de linii de comunicaţie costisitoare poate să nu fie justificată. Protocolul PPP Multilink (MP) grupează mai multe legături PPP împreună pentru a forma o singură legătură virtuală sau ″bundle″. Agregarea mai multor legături creşte lărgimea de bandă efectivă totală dintre două sisteme prin folosirea modem-urilor şi liniilor telefonice standard. Puteţi include până la şase legături într-un bundle MP. Pentru a stabili o conexiune Multilink, ambele capete ale legăturii PPP trebuie să suporte protocolul Multilink. Protocolul Multilink este referit ca standard RFC (Request For Comment) RFC1990. Informaţii suplimentare despre RFC-uri se găsesc la pagina Web RFC Editor.

Lărgime de bandă la cerere:

Capacitatea de adăugare şi înlăturare dinamică a legăturilor fizice permite configurarea unui sistem pentru a furniza lărgime de bandă doar când aceasta este necesară. Această abordare este referită în mod comun ca ″Lărgime de bandă la cerere″ şi vă permite să plătiţi pentru lărgimea de bandă suplimentară doar atunci când chiar o folosiţi. Pentru a realiza avantajele ″Lărgimii de bandă la cerere″, cel puţin un peer trebuie să fie capabilă să monitorizeze utilizarea lărgimii de bandă totală în mod curent într-un bundle MP. Legăturile pot fi astfel adăugate sau înlăturate din pachet atunci când utilizarea lărgimii de bandă depăşeste valorile definite prin configurare. Protocolul de alocare a lărgimii de bandă (Bandwidth Allocation Protocol) permite partenerilor să negocieze adăugarea sau înlăturarea legăturilor dintr-un pachet MP. RFC2125 se referă atât la BAP (Bandwidth Allocation Protocol) cât şi la BACP (Bandwidth Allocation Control Protocol) PPP.

Configurare PPP

Înainte de a putea folosi PPP pentru configurarea unei conexiuni punct-la-punct, trebuie să configuraţi mai întâi mediul PPP.

Referinţe înrudite

"Informaţii înrudite pentru PPP" la pagina 65
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Crearea unui profil de conexiune

Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Profilul de conexiune este reprezentarea logică a următoarelor detalii ale conexiunii:

- Tip linie şi profil
- Configurări Multilink
- Numere telefonice la distanţă şi opţiuni de apelare
- Autentificare
- Configurări TCP/IP: rutare şi adrese IP
- Control funcţionare şi personalizare conexiune
- Servere de nume domeniu

Servicii de acces la distanţă, din directorul Reţea, conţine următoarele obiecte:

- **Profilurile de conexiune originator** sunt conexiuni punct-la-punct care provin de la serverul iSeries (sistemul local). Acestea sunt conexiunile PPP pe care le primeşte un sistem la distanţă.
- **Profilurile de conexiune receptor** sunt conexiuni punct-la-punct care trebuie primite şi care provin de la un sistem la distanţă. Acestea sunt conexiuni PPP pe care le primeşte serverul iSeries (sistemul local).
- **Modemuri**

Urmaţi aceşti paşi pentru a crea un profil de conexiune:

1. În Navigator iSeries, selectaţi sistemul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Selectaţi una din următoarele opţiuni:
   - Faceţi clic-dreapta pe **Profiluri conexiune originator** pentru a seta serverul iSeries ca server care iniţiază conexiuni.
   - Faceţi clic-dreapta pe **Profiluri de conexiune receptor** pentru a seta serverul iSeries ca server care permite conexiuni de intrare de la sisteme şi utilizatori de la distanţă.
3. Selectaţi **Profil nou**.
4. Din pagina Configurare profil nou conexiune punct-la-punct, selectaţi tip protocol.
5. Specificaţi selecţiile de mod.
6. Selectaţi configuraţia legăturii.
7. Faceţi clic pe **OK**.

   Apare pagina Proprietăţi profil nou punct-la-punct. Puteţi seta restul de valori care sunt specifice reţelei. Consultaţi ajutorul interactiv pentru informaţii specifice.

   Operaţii înrudite

   “Asocierea unui modem cu o descriere de linie” la pagina 57

   Referinţe înrudite

   “Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE” la pagina 11
   Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

   “Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries” la pagina 14
   Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

   “Scenariu: Conectarea LAN-ului de la birou la Internet cu un modem” la pagina 16
   Administratorii configurează de obicei reţele care permit angajaţilor să aibă acces la Internet. Ei pot folosi un modem pentru a conecta serverul iSeries la un ISP. Clienţii PC ataşaţi prin LAN pot să comunice cu Internetul folosind serverul iSeries ca gateway.

"Scenariu: conectarea reţelei companiei şi a reţelelor la distanţă cu un modem" la pagina 19
Un modem permite ca două locaţii la distanţă (cum ar fi sediul central şi o filială) să schimbe date între ele. PPP poate conecta între ele cele două LAN-uri prin stabilirea unei conexiuni între serverul iSeries din sediul central şi alt server iSeries din sediul filialei.

"Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP" la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Tip ptotocol: PPP sau SLIP (Serial Line Internet Protocol)

Ce tip de protocol ar trebui să alegeţi pentru a face o conexiune punct-la-punct?

PPP este o conexiune la Internet standard. PPP permite interoperabilitatea între software-ul de acces la distanţă al diferiţilor fabricanţi. De asemenea, PPP permite şi ca protocoale multiple de comunicaţie în reţea să folosească aceeaşi linie fizică de comunicaţie.

PPP înlocuieşte SLIP (Serial Line Internet Protocol) ca protocol ales pentru conexiunile punct-la-punct. RFC (Request for Comment) SLIP nu a devenit niciodată un standard Internet din cauza următoarelor deficienţe:

- SLIP nu are un mod standard de definire a adresării IP între cele două gazde. Aceasta înseamnă că nu poate fi folosită o reţea nenumerotată.
- SLIP nu are suport pentru detectarea sau comprimarea erorilor. Detectarea erorilor sau comprimarea erorilor sunt implementate în PPP.
- SLIP nu are suport pentru autentificarea sistemului, în timp ce PPP are o autentificare bidirecţională.

SLIP este folosit şi în prezent, fiind încă suportat pe serverul iSeries. Totuşi, IBM recomandă utilizarea PPP la setarea conectivităţii punct-la-punct. SLIP nu oferă suport pentru conexiuni Multilink. În comparaţie cu SLIP, PPP are o autentificare mai bună. PPP funcţionează mai bine datorită facilităţilor de comprimare.

Notă: Profilurile de conexiune SLIP care sunt definite cu tipuri de linie ASYNC nu mai sunt suportate în această ediţie. Dacă aveţi aceste profiluri de conexiune, trebuie să le migraţi fie la un profil SLIP, fie la unul PPP care folosesc un tip de linie PPP.

Selecţii mod

Selecţiile de mod pentru un profil de conexiune PPP includ selecţii pentru **tip conexiune** şi **mod de operare**. Selecţiile de mod specifică modul în care serverul foloseşte noua conexiune PPP.

Urmaţi aceşti paşi pentru a specifica selecţiile de mod:

1. Selectaţi unul din următoarele tipuri de conexiune:
   - Linie comutată
   - Linie închiriată
   - L2TP (linie virtuală)
   - Linie PPPoE
2. Selectaţi modul de operare potrivit pentru noua conexiune PPP.
3. Înregistraţi tipul de conexiune şi modul de operare selectate. Aveţi nevoie de aceste informaţii atunci când începeţi configurarea conexiunilor PPP.

Linie comutată:

Selectaţi acest tip de conexiune dacă folosiţi unul din următoarele pentru conectarea printr-o linie telefonică: modem (intern sau extern) sau adaptor de terminal ISDN extern

Tipul de conexiune prin linie comutată are următoarele moduri de operare:

Răspuns

Alegeţi acest mod de operare pentru a permite unui sistem la distanţă să se conecteze prin apel telefonic la serverul iSeries.

Apel

Alegeţi acest mod de operare pentru a permite serverului iSeries să se conecteze prin apel telefonic la un sistem la distanţă.

Apel telefonic la cerere (numai apel)

Alegeţi acest mod de operare pentru a permite serverului iSeries să se conecteze automat prin apel telefonic la un sistem la distanţă, atunci când în sistem este detectat traficul TCP/IP. Conexiunea se încheie când transmisia datelor este terminată şi nu mai există trafic TCP/IP pe o anumită perioadă de timp.

Apel telefonic la cerere (peer dedicat capabil de răspuns)

Alegeţi acest mod de operare pentru a permite serverului iSeries să răspundă apelurilor de la un sistem la distanţă dedicat. Acest mod de operare permite de asemenea serverului iSeries să apeleze sistemul la distanţă atunci când este detectat trafic TCP/IP pentru sistemul la distanţă. Dacă ambele sisteme sunt servere iSeries şi dacă ambele folosesc acest mod de operare, traficul TCP/IP circulă între cele două sisteme la cerere, fără a fi nevoie de o conexiune fizică permanentă. Acest mod de operare necesită o resursă dedicată. Peer-ul de la distanţă trebuie să se conecteze pe linie telefonică pentru ca modul de operare să funcţioneze corect.

Apel telefonic la cerere (peer la distanţă activat)

Alegeţi acest mod de operare pentru a permite unui sistem la distanţă să fie apelat sau să i se răspundă. Pentru tratarea apelurilor primite, trebuie să referiţi un profil de răspuns existent dintr-un profil de conexiune PPP care specifică acest mod de operare. Acesta permite unui profil de răspuns să trateze toate apelurile primite de la unul sau mai mulţi parteneri la distanţă şi un profil separat de apel telefonic la cerere pentru fiecare apel trimis. Acest mod de operare nu necesită o resursă dedicată pentru tratarea apelurilor primite de la parteneri la distanţă.

Linie închiriată:

Selectaţi acest tip de conexiune dacă aveţi o linie dedicată între serverul iSeries local şi sistemul la distanţă. Dacă aveţi o linie închiriată, nu aveţi nevoie de un modem sau un adaptor terminal ISDN pentru conectarea celor două sisteme.

O conexiune pe linie închiriată între două sisteme este considerată linie permanentă sau dedicată. Ea este întotdeauna deschisă. Un capăt al conexiunii prin linie închiriată este configurat ca iniţiator, iar celălalt este configurat ca terminator.

Tipul de conexiune prin linie închiriată are următoarele moduri de operare:

Terminator

Alegeţi acest mod de operare pentru a permite unui sistem la distanţă să acceseze serverul iSeries printr-o linie dedicată. Acest mod de operare se referă la un profil răspuns pentru linie închiriată.

Iniţiator

Alegeţi acest mod de operare pentru a permite serverului iSeries să acceseze un sistem la distanţă printr-o linie dedicată. Acest mod de operare se referă la un profil apel telefonic prin linie închiriată.

L2TP (linie virtuală):

Selectaţi acest tip de conexiune pentru a realiza o conexiune între sistemele care folosesc L2TP (Layer Two Tunneling Protocol).

După stabilirea unui tunel L2TP, se face o conexiune PPP virtuală între serverul iSeries şi sistemul la distanţă. Folosind L2TP în conjuncţie cu IP-SEC (IP security), puteţi trimite, ruta şi primi date securizate de pe Internet.

Tipul de conexiune L2TP (linie virtuală) are următoarele moduri de operare:

Terminator

Alegeţi acest mod de operare pentru a permite unui sistem la distanţă să se conecteze la serverul iSeries printr-un tunel L2TP.

Iniţiator

Alegeţi acest mod de operare pentru a permite serverului iSeries să se conecteze la un sistem la distanţă printr-un tunel L2TP.

Apel la distanţă

Alegeţi acest mod de operare pentru a permite serverului iSeries să se conecteze la un ISP printr-un tunel L2TP şi să determine ISP-ul să apeleze un client PPP la distanţă.

Iniţiator multi-hop

Alegeţi acest mod de operare pentru a permite serverului iSeries să stabilească o conexiune multi-hop.

Notă: Profilul Terminator L2TP cu care este asociat acest iniţiator multi-hop trebuie să aibă activată caseta ″Permite conexiune multi-hop″ şi să aibă o intrare în lista de validare PPP care leagă numele de utilizator PPP de profilul iniţiator multi-hop.

Linie PPPoE:

Conexiunile PPPoE (Point-to-Point over Ethernet) folosesc o linie virtuală pentru a trimite date PPP (printr-un adaptor Ethernet) către un modem DSL (Digital Subscriber Line) furnizat de ISP. Modemul este şi el conectat la reţeaua locală bazată pe Ethernet.

Aceasta permite utilizatorilor LAN acces de mare viteză la Internet prin sesiuni PPP folosind serverul iSeries. După ce s-a realizat conexiunea dintre iSeries şi ISP, utilizatorii individuali din LAN pot porni sesiuni unice cu ISP prin PPPoE.

Conexiunile PPPoE sunt folosite doar de profilurile de conexiune originator şi implică un mod de funcţionare Iniţiator şi folosesc doar o linie singulară.

Configurare legătură

Configurare legătură defineşte tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni.

Tipurile de servicii linie depind de tipul de conexiune specificat.

Referinţe înrudite

“Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE” la pagina 11
Multe ISP-uri oferă acces la Internet de mare viteză peste DSL folosind PPPoE (Point-to-Point Protocol over Ethernet). Serverul iSeries se poate conecta la aceşti furnizori de servicii pentru a oferi conexiuni de bandă largă, care păstrează avantajele oferite de PPP.

“Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries” la pagina 14
Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

“Scenariu: Conectarea LAN-ului de la birou la Internet cu un modem” la pagina 16
Administratorii configurează de obicei reţele care permit angajaţilor să aibă acces la Internet. Ei pot folosi un modem pentru a conecta serverul iSeries la un ISP. Clienţii PC ataşaţi prin LAN pot să comunice cu Internetul folosind serverul iSeries ca gateway.

“Scenariu: conectarea reţelei companiei şi a reţelelor la distanţă cu un modem” la pagina 19
Un modem permite ca două locaţii la distanţă (cum ar fi sediul central şi o filială) să schimbe date între ele. PPP poate conecta între ele cele două LAN-uri prin stabilirea unei conexiuni între serverul iSeries din sediul central şi alt server iSeries din sediul filialei.

Linie singulară:

Selectaţi acest serviciu linie pentru a defini o linie PPP care este asociată cu un modem analogic. Această opţiune este de asemenea folosită pentru liniile închiriate unde nu este necesar un modem. Profilul de conexiune PPP foloseşte întotdeauna aceeaşi resursă port de comunicaţii a serverului iSeries.

O linie singulară analogică, dacă este necesar, ar putea fi configurată ca partajată de un profil de răspuns şi unul de apel. Partajarea dinamică a resurselor este o nouă funcţie proiectată pentru a mări capacitatea de funcţionare a resurselor. Până la V5R2, resursele modem erau alocate imediat ce era pornit profilul care le folosea. Aceasta limita utilizatorul la o resursă per sesiune, chiar dacă resursa se afla în stare pasivă, de aşteptare. Acum se aplică noi reguli de partajare atunci când a fost accesată o resursă anume. Sunt două cazuri: primul, un profil de apel a fost pornit înaintea unui profil de răspuns, al doilea un profil de răspuns a fost pornit înaintea unui profil de apel. Se presupune că este activată partajarea resurselor. În primul caz, profilul de apel care a fost pornit se va conecta cu succes. Profilul de răspuns, care a fost pornit al doilea, va aştepta ca linia să devină disponibilă. După ce conexiunea de apel s-a sfârşit, profilul de răspuns va revendica linia şi va porni. În al doilea caz, profilul de răspuns care a fost pornit va aştepta conexiunile de intrare. Dacă nu a fost realizată o conexiune de intrare, profilul de apel, care a fost pornit al doilea, va ″împrumuta″ linia de la profilul de răspuns, care va ″închiria″ linia. Apoi va fi stabilită conexiunea de ieşire. După ce conexiunea s-a sfârşit, profilul apel va returna linia profilului răspuns care va fi din nou gata să accepte conexiuni de intrare. Pentru a activa funcţia de partajare, apăsaţi pe fişa modem pentru o descriere a liniei comutate şi selectaţi **Activează partajarea dinamică a resurselor**.

Serviciul linie singulară este de asemenea folosit pentru tipurile de conexiune L2TP (linie virtuală) şi PPPoE (linie virtuală). Pentru tipurile de conexiuni L2TP (linie virtuală), nu există resurse port de comunicaţii hardware folosite cu linia singulară. Mai degrabă linia singulară folosită cu o conexiune L2TP este *virtuală* prin faptul că nu există hardware PPP fizic care să fie cerut pentru stabilirea tunelului. Linia singulară folosită cu conexiunea PPPoE este de asemenea virtuală prin faptul că oferă un mecanism pentru tratarea unei linii Ethernet fizice ca şi cum ar fi o line PPP care suportă conexiuni la distanţă. Linia virtuală PPPoE este legată de o linie fizică Ethernet şi este folosită pentru a suporta transferul de date protocol PPP peste conexiunea LAN Ethernet către un modem DSL.

Pool de linii:

Selectaţi acest serviciu linie pentru a configura conexiunea PPP pentru a folosi o linie dintr-un pool de linii. La pornirea conexiunii PPP, serverul iSeries selectează o linie neutilizată din pool-ul de linii. Pentru profiluri cu conectare pe linie telefonică la cerere, serverul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

Se poate folosi un pool de linii în loc de a se defini o anumită descriere de linie pentru un profil conexiune. Puteţi specifica una sau mai multe descrieri de linie într-un pool de linii.

Un pool de linii permite de asemenea ca un singur profil de conexiune să trateze fie mai multe apeluri analogice primite, fie un singur apel analogic trimis. Linia se întoarce în grupul de linii atunci când conexiunea PPP se încheie.

Dacă folosiţi grupul de linii pentru a trata simultan mai multe apeluri analogice primite, trebuie să indicaţi numărul maxim de conexiuni recepţionate. Puteţi seta aceasta în fişa Conexiuni a dialogului **Proprietăţi profil nou punct-la-punct** atunci când configuraţi profilul de conexiune. Folosiţi setarea Multilink pentru a folosi grupuri de linii pentru conexiuni singulare cu lărgime de bandă crescută.

Avantaje la utilizarea grupurilor de linii:

- Nu se repartizează o resursă linie unei conexiuni PPP până când aceasta nu porneşte.

  Pentru conexiuni PPP care folosesc o linie specifică, conexiunea se termină dacă linia nu este disponibilă doar dacă partajarea dinamică a resurselor nu este activată. Pentru conexiuni care folosesc un pool de linii, trebuie să fie disponibilă cel puţin o linie din grup atunci când porneşte profilul.

  În plus, dacă resursele erau configurate ca partajate (activare partajarea dinamică a resurselor), este obţinută o disponibilitate suplimentară a resurselor mai ales pentru conexiunile de ieşire.
- Se pot folosi profiluri apel-la-cerere cu grupuri de linii pentru a folosi resursele mai eficient.

Serverul iSeries selectează o linie din pool numai atunci când foloseşte o conexiune prin apel-la-cerere. Alte conexiuni pot folosi aceeaşi linie în alte momente.

- Puteţi porni mai multe conexiuni PPP cu mai puţine resurse pentru suport.

  De exemplu, dacă mediul necesită patru tipuri unice de conexiuni dar la un anumit moment aveţi nevoie doar de două linii, puteţi folosi un pool de linii pentru ca acest mediu să funcţioneze. Puteţi crea patru profiluri de conexiuni apel-la-cerere şi să faceţi astfel încât fiecare profil să refere un pool de linii care conţine două descrieri de linie. Fiecare din linii va fi pentru uzul tuturor celor patru profiluri conexiune, permiţând astfel ca două conexiuni să fie active în orice moment. Prin folosirea unui pool de linii, nu aveţi nevoie să aveţi patru linii separate.

  De asemenea, dacă mediul dumneavoastră este o combinaţie între un Client PPP şi un Server PPP, liniile pot fi partajate (activare partajare dinamică resurse) dacă sunt folosite ca 'linii singulare' sau plasate într-un 'pool de linii'. Profilul care a pornit primul nu va implica resursa decât dacă conexiunea este activă. De exemplu, dacă serverul PPP este pornit şi aşteaptă conexiunile de intrare, el va ″închiria″ o linie pe care o foloseşte pentru clientul PPP care a pornit şi ″împrumutat″ linia partajată de la serverul PPP.

Configurarea unui pool de linii

Pool-urile de linii sunt definite în cadrul unui profil de conexiune. Pentru configurarea unui pool de linii de bază, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi sistemul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Creaţi un profil de conexiune pentru apelare sau pentru primire apeluri. Selectaţi una dintre următoarele opţiuni:
   - Faceţi clic-dreapta pe **Profiluri conexiune originator** pentru a seta serverul iSeries ca server care iniţiază conexiuni.
   - Faceţi clic-dreapta pe **Profiluri de conexiune receptor** pentru a seta serverul iSeries ca server care permite conexiuni de intrare de la sisteme şi utilizatori de la distanţă.
3. Selectaţi **Profil nou**.
4. Pentru un profil originator (apel de ieşire) selectaţi: PPP, Linie comutată şi Mod operare (de obicei apelează). Pentru configuraţia liniei, selectaţi **Pool de linii**. Faceţi clic pe **OK** şi Navigator iSeries deschide fereastra pentru proprietăţile profilului de conexiune.

   Notă: De asemenea, puteţi selecta un pool de linii atunci când creaţi Profiluri de conexiune receptor. Opţiunea Pool de linii poate fi afişată sau nu, în funcţie de următoarele valori de câmp: tip protocol, tip conexiune şi mod operare.
5. În pagina General, introduceţi numele şi descrierea profilului.
6. În pagina Conexiune, introduceţi un nume pentru pool-ul de linii şi faceţi clic pe **Nou**. Aceasta va determina deschiderea dialogului **Proprietăţi pool nou de linii**, în care vor fi afişate toate liniile şi modemurile disponibile pentru sistemul respectiv.
7. Selectaţi liniile pe care doriţi să le utilizaţi şi apoi adăugaţi-le în pool. De asemenea, puteţi să faceţi clic pe **Linie nouă** pentru a defini o nouă linie.
8. Faceţi clic pe **OK** pentru a salva acest pool de linii şi reveniţi la proprietăţi Profil punct-la-punct nou.
9. Completaţi informaţiile necesare despre celelalte pagini (de exemplu Setări TCP/IP sau Autentificare).
10. Profilul de conexiune va desfăşura lista cu linii disponibile (din pool) până la o resursă disponibilă şi va utiliza linia respectivă pentru conexiune. Folosiţi ajutorul din Navigator iSeries pentru asistenţă suplimentară.

Referinţe înrudite

"Scenariu: Conectarea clienţilor dial-in la distanţă la serverul iSeries" la pagina 14
Utilizatorii la distanţă, cum sunt cei care lucrează acasă sau clienţii care se deplasează mult, au nevoie adesea de acces la reţeaua unei companii. Aceşti clienţi pot accesa un server iSeries cu PPP.

"Scenariu: Conectarea LAN-ului de la birou la Internet cu un modem" la pagina 16
Administratorii configurează de obicei reţele care permit angajaţilor să aibă acces la Internet. Ei pot folosi un modem pentru a conecta serverul iSeries la un ISP. Clienţii PC ataşaţi prin LAN pot să comunice cu Internetul folosind serverul iSeries ca gateway.

"Scenariu: conectarea reţelei companiei şi a reţelelor la distanţă cu un modem" la pagina 19
Un modem permite ca două locaţii la distanţă (cum ar fi sediul central şi o filială) să schimbe date între ele. PPP poate conecta între ele cele două LAN-uri prin stabilirea unei conexiuni între serverul iSeries din sediul central şi alt server iSeries din sediul filialei.

Suport pentru profil conexiuni multiple:

Profilurile de conexiune punct-la-punct care suportă mai multe conexiuni vă permit să aveţi un profil de conexiune care manevrează mai multe apeluri de tip digital, analog sau L2TP.

Aceasta va ajută când doriţi ca mai mulţi utilizatori să se conecteze la serverul iSeries, dar nu doriţi să specificaţi un profil de conexiune punct-la-punct separat pentru lucrul cu fiecare linie. Această caracteristică este utilă în special pentru modemul integrat 2805 cu 4 porturi, care permite folosirea a patru linii de pe un singur adaptor.

Pentru liniile analogice cu suport pentru profil de conexiune multiplă, toate liniile din grupul de linii specificat sunt folosite până la numărul maxim de conexiuni. În principiu, se va porni un job profil de conexiune separat pentru fiecare linie definită în grup. Toate joburile profil de conexiune vor aştepta apeluri de intrare pe liniile lor respective.

Adresa IP locală pentru profilurile de conexiuni multiple:

Puteţi folosi adresa IP locală cu profiluri de conexiune multiple, dar aceasta trebuie să fie o adresă IP existentă care este definită pe serverul iSeries. Puteţi folosi lista derulantă Adresă IP locală pentru a selecta o adresă IP existentă. Utilizatorii de la distanţă pot accesa resursele din reţeaua locală dacă alegeţi adresa IP locală a serverului iSeries ca adresa IP locală pentru profilul PPP. De asemenea, trebuie să definiţi adresele IP care sunt în grupul de adrese IP la distanţă pentru a fi în aceeaşi reţea ca şi adresa IP locală.

Dacă nu aveţi o adresă IP locală a serverului iSeries sau nu doriţi ca utilizatorii la distanţă să acceseze LAN-ul, trebuie să definiţi o adresă IP virtuală pentru serverul iSeries. O adresă IP virtuală este de asemenea cunoscută ca o interfaţă fără circuit. Profilurile punct-la-punct pot folosi această adresă IP ca adresă IP locală. Deoarece această adresă IP nu este legată la o reţea fizică, ea va transfera automat traficul către alte reţele care sunt ataşate serverului iSeries.

Pentru a crea o Adresă IP virtuală, urmaţi aceşti paşi:

1. În Navigator iSeries, expandaţi serverul dumneavoastră şi accesaţi **Reţea → > Configuraţie TCP/IP → IPV4 → Interfeţe**.
2. Faceţi clic-dreapta pe **Interfeţe** şi selectaţi **Interfaţă nouă → >IP virtual**.
3. Urmaţi instrucţiunile Vrăjitorului de interfaţă pentru a crea interfaţa IP virtuală. Profilurile de conexiune punct-la-punct pot folosi adresa IP virtuală, după ce aceasta a fost creată. Puteţi folosi lista derulantă din câmpul Adresă IP locală, din pagina Configurări TCP/IP, pentru a folosi adresa IP cu profilul dumneavoastră.

   Notă: Adresa IP virtuală trebuie să fie activă înainte de pornirea profilului de conexiuni multipltiple; altfel, profilul nu va porni. Pentru a activa adresa IP după crearea interfeţei, selectaţi opţiunea de pornire adresă IP atunci când folosiţi Vrăjitorul de interfaţă.

Grupurile de adrese IP la distanţă pentru profilurile de conexiuni multiple:

Puteţi folosi grupuri de adrese IP la distanţă cu profiluri de conexiuni multiple. Un profil tipic punct-la-punct cu o singură conexiune vă va permite să specificaţi doar o adresă IP la distanţă, care este atribuită sistemului apelant, la efectuarea conexiunii. Deoarece acum mai mulţi apelanţi pot să se conecteze simultan, un grup de adrese IP la distanţă este folosit pentru a defini o adresă IP de pornire precum şi intervalul de adrese IP suplimentare care sunt atribuite sistemelor apelante.

Restricţii privind grupul de linii:

Aceste restricţii se aplică atunci când se folosesc grupuri de linii pentru conexiuni multiple:

- O linie nu se poate afla decât într-un singur pool de linii la un moment dat. Dacă înlăturaţi o linie dintr-un pool de linii, ea poate fi folosită într-un alt grup.
- La pornirea unui profil de conexiuni multiple care foloseşte un pool de linii, toate liniile din grupul de linii sunt folosite până la valoarea numărului maxim de conexiuni din profil. Când nu sunt linii deloc, toate noile conexiuni vor eşua. De asemenea, dacă nu sunt linii în grupul de linii şi alt profil porneşte, el se va termina.
- Dacă porniţi un profil conexiune unică ce foloseşte un pool de linii, doar o linie din grupul de linii va fi folosită de către sistem. Dacă porniţi un profil conexiune multiplă care foloseşte acelaşi pool de linii, pot fi folosite orice linii rămase în grup.

Grupuri de adrese IP la distanţă:

Sistemul poate folosi grupurile de adrese IP la distanţă pentru orice profil de conexiune punct-la-punct de răspuns sau de oprire care este folosit cu conexiunile de intrare multiple.

Aceasta include L2TP şi pool-urile de linii cu numărul maxim de conexiuni mai mare de unu. Această funcţie permite sistemului să atribuie o adresă IP unică la distanţă pentru fiecare conexiune de intrare.

Primul sistem ce se va conecta va primi adresa IP definită în câmpul Adresă IP de start. Dacă adresa IP respectivă este deja folosită, este oferită următoarea adresă IP din interval. De exemplu, presupuneţi că adresa IP de început este 10.1.1.1 şi numărul de adrese IP este definit ca 5. Adresele IP din grupul de adrese IP la distanţă vor fi 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 şi 10.1.1.5. Masca subreţea definită pentru adresele grupului de adrese IP la distanţă va fi întotdeauna 255.255.255.255.

Aceste restricţii se aplică atunci când se folosesc pool-uri de adrese IP la distanţă:
- Mai multe profiluri de conexiune pot specifica acelaşi pool de adrese. Dacă însă toate adresele IP din pool sunt utilizate, noile cereri de conexiune sunt refuzate până când se termină o altă conexiune şi devine disponibilă o adresă IP.
- Pentru a aloca adrese IP specifice unor sisteme la distanţă, permiţând în acelaşi timp altor sisteme care apelează să folosească o adresă IP din grup, urmaţi următorii paşi:
  1. Se activează autentificarea sistemului la distanţă din fişa **Autentificare** , astfel încât să poată fi învăţat numele de utilizator al sistemului la distanţă.
  2. Se defineşte un grup de adrese IP la distanţă pentru toate cererile de conectare sosite ce nu necesită o adresă IP specifică.
  3. Se definesc adresele IP la distanţă pentru utilizatori specifici prin activarea **Definire adrese IP suplimentare pe baza ID-ului utilizatorului sistemului la distanţă** şi apoi prin apăsarea **Adrese IP definite după Nume utilizator**.

  Când utilizatorul la distanţă se conectează, serverul iSeries determină dacă este definită o adresă IP specifică pentru utilizatorul respectiv. În acest caz, adresa IP va fi atribuită sistemului la distanţă; altfel, se va returna o adresă IP din grupul de adrese IP la distanţă.

Configurarea modemului pentru PPP

Pentru conexiunile dumneavoastră analogice PPP puteţi folosi un modem extern, intern sau un adaptor terminal ISDN. Un modem vă oferă capacităţile conexiunilor analogice (linii închiriate şi comutate). Pentru serverul iSeries au fost definite descrierile de modem pentru cele mai folosite modemuri.

Referinţe înrudite

“Depanarea PPP” la pagina 64
Dacă aveţi probleme cu conexiunile PPP, puteţi folosi această listă de verificare pentru a strânge informaţii despre eroare. Lista de verificare vă poate ajuta la identificarea simptomelor de eroare şi la rezolvarea problemelor conexiunilor PPP.

Configurare modem nou

În acest subiect aflaţi cum să configuraţi un modem nou.

Pentru a configura un modem nou, urmaţi aceşti paşi:

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Modemuri** şi selectaţi **Modem nou**.
3. În fişa General, introduceţi valorile corecte în toate casetele câmp.
4. Opţional: Selectaţi fişa **Parametri suplimentari** pentru a adăuga alte comenzi de iniţializare necesare pentru modem.
5. Faceţi clic pe **OK** pentru a salva ceea ce aţi introdus şi închideţi pagina Proprietăţi modem nou.

Utilizarea unei descrieri de modem existente

Pentru a determina dacă puteţi folosi o descriere modem existentă , urmaţi aceşti paşi:

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Selectaţi **Modemuri**.
3. Revedeţi lista de modemuri şi aflaţi numele fabricantului, modelul şi data fabricaţiei.

   Notă: Dacă modemul dumneavoastră se află în lista implicită, nu trebuie să mai faceţi nimic.
4. Faceţi clic-dreapta pe descrierea de modem care se potriveşte cu modemul dumneavoastră şi selectaţi **Proprietăţi** pentru a revedea şirurile de comandă.
5. Consultaţi documentaţia modemului pentru a determina şirurile specifice de comandă pentru modemul dumneavoastră.

   Folosiţi proprietăţile implicite ale modemului dacă şirurile de comandă corespund cerinţelor modemului. Altfel, trebuie să creaţi o descriere modem pentru modemul dumneavoastră şi să o adăugaţi în lista de modemuri.

Crearea unei descrieri de modem bazată pe o altă descriere de modem

Pentru a crea o descriere de modem bazată pe o altă descriere de modem, parcurgeţi paşii următori:

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Selectaţi **Modemuri**.
3. Din lista de modemuri, faceţi clic-dreapta pe **Generic Hayes** şi selectaţi **Modem nou pe baza**.
4. Din dialogul **Modem nou**, modificaţi şirurile de comandă pentru a corespunde informaţiilor cerute de modem.

   Referinţe înrudite

   “Setare şir de comenzi modem”

   “Depanarea PPP” la pagina 64
   Dacă aveţi probleme cu conexiunile PPP, puteţi folosi această listă de verificare pentru a strânge informaţii despre eroare. Lista de verificare vă poate ajuta la identificarea simptomelor de eroare şi la rezolvarea problemelor conexiunilor PPP.

Setare şir de comenzi modem

Puteţi găsi şirul de comandă echivalent în manualul pentru utilizator al modemului dumneavoastră. Folosiţi setările recomandate de fabricant din descrierea modem.

Tabela 9. Modemurile definite pe serverul iSeries şi şirurile de comenzi

Proprietate modem	**Şir de comandă corect pentru majoritatea modemurilor**
Resetare modem la valorile implicite de fabrică	AT&F sau AT&Z
Iniţializare modem:	

Tabela 9. Modemurile definite pe serverul iSeries şi şirurile de comenzi (continuare)

Proprietate modem	**Şir de comandă corect pentru majoritatea modemurilor**
Afişare coduri verbale rezultat	Q0 şi V1
Moduri DTR şi CD normal	&C1 şi &D2
Mod echo dezactivat	E0
DSR (Data Set Ready) urmează după Carrier Detect	&S1
Activare control hardware flux (RTS/CTS)	
Activare corecţie erori şi opţional, compresie (V.42/V.42 bis)	
Asigurare că viteza liniei DTE-DCE este activată pentru a rula la fix 115.2 Kbps (sau maximul permis de modem)	
(Opţional) Activare timp de inactivitate dacă modemul suportă această funcţie	
Mod de răspuns modem:	
Răspuns după *n* apeluri	S0=*n* unde *n* = 1 sau 2
Deconectare dacă nu există conectare (carrier) după *m* secunde	S7=*m*
Tip modem Apel telefonic	ATDT pentru apel ton sau ATDP pentru apel puls

Concepte înrudite

"Configurare modem nou" la pagina 55
În acest subiect aflaţi cum să configuraţi un modem nou.

Exemplu: Configurarea unui adaptor terminal ISDN

Următorul exemplu demonstrează cum să configuraţi un adaptor de terminal ISDN.

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Modemuri** şi selectaţi **Modem nou**.
3. În fişa General, introduceţi valorile corecte în toate casetele câmp.
4. **Opţional:** Faceţi clic pe fişa Parametri ISDN pentru a adăuga alte comenzi de iniţializare necesare pentru modem.

   Pentru adaptoare terminale ISDN, comenzile şi parametri din această listă sunt transmişi adaptorului terminal doar în următoarele condiţii:

   - Atunci când comenzile sau parametri din listă sunt fie modificaţi, fie adăugaţi.
   - Ca rezultat al anumitor acţiuni de revenire din eroare pe care le poate efectua serverul iSeries

   În consecinţă, aceste comenzi ar trebui să includă şi să fie limitate la următoarele setări:

   - Setarea tipului de comutare ISDN şi versiune furnizate de compania telefonică locală
   - Setarea numerelor directoarelor şi SPID-uri (service profile identifiers - identificatori profil serviciu) furnizate de compania telefonică locală
   - Setarea TEI (Terminal Entry IDs - identificatori intrare terminal) care ar putea fi furnizaţi de compania telefonică locală
   - Setarea protocolului canal B (PPP asincron-la-sincron)
   - Alte setări modem care au parametri de lungime variabilă ce necesită un început de linie pentru a indica lungimea parametrului
   - Salvarea şi activarea noilor setări pentru a fi restaurate după resetarea lor sau după întreruperea alimentării sistemului.
   - Comanda de probă a stării active a interfeţei *U* (ATD*x*), care permite serverului iSeries să determine când este activată sincronizarea cu comutatorul sediului central ISDN. *x* poate fi oricare din cifrele permise pentru un număr de telefon, incluzând # şi *.

5. Faceţi clic pe **Adăugare** pentru comenzi de modem suplimentare. Acestea pot fi cu sau fără un parametru asociat şi o scurtă descriere în lista de comenzi. Comenzilor specificate fără un parametru asociat li se poate atribui un parametru atunci când modemului i se asociază o descriere linie.
6. Faceţi clic pe **OK** pentru a salva ceea ce aţi introdus şi închideţi pagina Proprietăţi modem nou.

Referinţe înrudite

"Adaptoare terminale ISDN" la pagina 39
ISDN oferă o conexiune digitală care permite comunicarea folosind orice combinaţie de voce, date şi secvenţe video, împreună cu alte aplicaţii multimedia.

Asocierea unui modem cu o descriere de linie

1. În Navigator iSeries selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă → Profiluri conexiune originator sau Profiluri de conexiune receptor**.
2. Selectaţi una din următoarele opţiuni:
   - Pentru gestionarea unui profil de conexiune existent, efectuaţi clic-dreapta pe un profil de conexiune şi selectaţi **Proprietăţi**.
   - Pentru a lucra cu un profil de conexiune nou, creaţi unul nou.
3. Din pagina Proprietăţi profil nou punct-la-punct, selectaţi fişa **Conexiune** şi selectaţi **Nou**.
   - Introduceţi numele pentru configurarea liniei.
   - Selectaţi **Nou** pentru a deschide fereastra Proprietăţi linie nouă.
4. Din fereastra Proprietăţi linie nouă, selectaţi fişa **Modem** şi selectaţi modemul din listă. Modemul selectat va fi asociat cu această descriere de linie. Pentru modem-uri interne definiţia modem corectă ar trebui să fie deja selectată. Pentru mai multe informaţii, consultaţi ajutorul interactiv.

Puteţi configura profiluri de conexiune originator pentru a ″împrumuta″ o linie PPP şi modemul asociate unui profil de conexiune receptor care aşteaptă un apel de intrare. Conexiunea originator va ″returna″ linia şi modemul PPP profilului conexiune receptor când conexiunea s-a încheiat. Pentru a activa această nouă funcţie, selectaţi opţiunea **Activare partajare dinamică de resurse** din fişa Modem a ferestrei de configurare linie PPP. Puteţi configura linii PPP din fişa Conexiune a profilurilor conexiune Receptor şi Originator.

Operaţii înrudite

"Crearea unui profil de conexiune" la pagina 47
Primul pas în configurarea unei conexiuni PPP între sisteme este crearea unui profil de conexiune pe serverul iSeries.

Configurarea unui PC la distanţă

Pentru conectarea la un server iSeries de pe un PC pe care rulează un sistem de operare Windows pe 32 de biţi, verificaţi dacă modemul este instalat şi configurat corespunzător şi asiguraţi-vă că aţi instalat TCP/IP şi Dial-Up Networking pe calculatorul personal.

Consultaţi documentaţia Microsoft Windows pentru informaţii privind modul în care se configurează Dial-up Networking pe PC. Asiguraţi-vă că aţi specificat sau introdus următoarele informaţii:

- Tipul de conexiune prin apel telefonic ar trebui să fie **PPP**.
- Dacă folosiţi parole criptate, asiguraţi-vă că folosiţi MD-5 CHAP (MS-CHAP NU este suportat de serverul iSeries). Unele versiuni de Windows nu suportă CHAP MD-5 direct, dar acesta poate fi configurat cu ajutor suplimentar de la Microsoft.
- Dacă folosiţi parole necriptate (sau nesecurizate), PAP (Password Authentication Protocol) este folosit automat. Orice alt tip de protocol nesecurizat nu va fi suportat de serverul iSeries.
- În mod obişnuit, adresarea IP este definită de sistemul la distanţă sau, în acest caz, serverul iSeries. Dacă intenţionaţi să folosiţi metode alternative de adresare IP (cum ar fi definirea propriilor adrese IP), asiguraţi-vă că serverul iSeries este şi el configurat pentru acceptarea metodei de adresare.
- Adăugaţi adrese IP DNS dacă acestea sunt potrivite mediului dumneavoastră.

Configurarea accesului la Internet prin AT&T Global Network

Când se comunică prin AT&T Global Network, sunt necesare proiluri speciale.

Pentru a accesa acest serviciu, puteţi folosi vrăjitorul Conexiune apel telefonic AT&T Global Network pentru a vă ajuta la configurarea unui profil de conexiune PPP cu apel comutat pentru apelarea AT&T Global Network. Vrăjitorul vă poartă cam prin opt panouri şi necesită cam zece minute pentru terminare. Puteţi anula vrăjitorul în orice moment şi nu sunt salvate nici un fel de date.

Două tipuri de aplicaţii pot folosi conexiunea AT&T Global Network:

- **Mail Exchange**: Vă permite să extrageţi periodic poşta dintr-un cont AT&T Global Network singular şi să o trimiteţi pe serverul iSeries pentru a fi distribuită utilizatorilor Lotus Mail sau utilizatorilor SMTP (Simple Mail Transfer Protocol).
- **Dial-up Networking**: Folosiţi alte aplicaţii de reţea cu conectare prin apel telefonic cu AT&T Global Network, cum este accesul standard Internet.

Întreţineţi profilurile de conexiune AT&T Global Network ca orice alte profiluri de conexiune PPP.

Aveţi nevoie de unul din aceste adaptoare pentru a folosi vrăjitorul Conexiune apel telefonic AT&T Global Network:

- 2699: IOA două linii WAN
- 2720: IOA PCI WAN/Twinax
- 2721: IOA PCI două linii WAN
- 2745: IOA PCI două linii WAN (înlocuieşte IOA 2721)
- 2771: IOA două linii WAN, cu un modem integrat V.90 la portul 1 şi o interfaţă standard de comunicaţii la portul 2. Pentru a folosi portul 2 al adaptorului 2771, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător.
- 2772: IOA cu două porturi WAN cu modem integrat V.90
- 2793: IOA cu două porturi WAN, cu un modem integrat V.92 pe portul 1 şi o interfaţă de comunicaţii standard pe portul 2. Acesta înlocuieşte modelul 2771.
- 2805: IOA cu patru porturi WAN, cu un modem V.92 integrat. Acesta înlocuieşte modelele 2761 şi 2772.

Înainte de a porni vrăjitorul Conexiune apel telefonic AT&T Global Network, trebuie să aveţi aceste informaţii despre mediu:

- Informaţii despre contul AT&T Global Network (număr cont, ID şi parolă utilizator) pentru aplicaţia mail exchange sau dial-up networking.
- Adresele IP ale serverului de poştă şi nume serverului DNS pentru aplicaţia mail exchange.
- Numele modemului care este folosit pentru conexiunea linie singulară.

Pentru a porni vrăjitorul Conexiune apel telefonic AT&T Global Network, urmaţi aceşti paşi:

1. În Navigator iSeries, expandaţi serverul dumneavoastră şi accesaţi **Reţea → > Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Profiluri de conexiune originator** şi selectaţi **Conexiune nouă de apel telefonic AT&T Global Network**.
3. La pornirea vrăjitorului Conexiune apel telefonic AT&T Global Network selectaţi **Ajutor** pentru informaţii despre completarea unui panou.

Vrăjitori de conectare

Puteţi folosi vrăjitori de conexiune pentru a vă ghida la configurarea profilului de conexiune.

Vrăjitor conexiune nouă prin apel telefonic

Acest vrăjitor vă ghidează prin paşii de configurare a unui profil de conexiune prin apel telefonic pentru accesarea furnizorului de servicii Internet sau a intranetului. Ar putea fi nevoie de informaţii de la administratorul reţelei

dumneavoastră sau de la furnizorul dumneavoastră de Internet (ISP) pentru a termina vrăjitorul. Pentru mai multe informaţii despre terminarea vrăjitorului, consultaţi ajutorul interactiv.

Vrăjitorul Conexiune universală IBM

Selectarea acestui vrăjitor vă ghidează prin paşii de configurare a unui profil care poate fi folosit de software-ul Electronic Customer Support pentru conectarea la IBM. Suportul pentru service electronic oferă monitorizarea mediului dumneavoastră unic pentru sistemul server iSeries pentru a vă furniza recomandări de corecţii personalizate pentru sistemul şi situaţia particulară.

Informaţii înrudite

Configurarea conexiunii universale

Configurarea unei politici de acces de grup

Folderul **Politici de acces grup** de sub Profiluri de conexiune receptor oferă opţiuni pentru configurarea parametrilor conexiunilor punct-la-punct care se referă la un grup de utilizatori la distanţă. Acest lucru este valabil numai pentru acele conexiuni punct-la-punct iniţiate de un sistem la distanţă şi care sunt recepţionate de sistemul local.

Pentru a configura o nouă politică de acces grup:

1. În Navigator iSeries selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă → Profiluri conexiune receptor**.
2. Faceţi clic-dreapta pe **Politici de acces grup** şi selectaţi **Politică nouă de acces grup**.
3. În fişa **General**, introduceţi un nume şi o descriere pentru noua politică de acces a grupului.
4. Faceţi clic pe fişa **Multilink** şi setaţi configuraţia Multilink.

   Configuraţia Multilink precizează că vreţi să aveţi linii fizice multiple unite într-un bundle. Numărul maxim de linii dintr-un bundle poate fi între 1 şi 6. Deoarece nu ştiţi tipul setării de linie până ce conexiunea nu este făcută, valoarea implicită este 1. Politica de grup poate fi folosită pentru a extinde sau limita capacităţile protocolului Multilink pentru un utilizator anume.

   Maxim de legături per pachet specifică numărul maxim de legături (sau linii) care doriţi să devină singura linie logică. Numărul maxim de linii nu poate fi mai mare decât numărul liniilor libere atunci când această politică de grup este aplicată unei sesiuni pentru un profil PPP.

   Bifaţi **Necesar protocol de alocare a lărgimii de bandă** dacă doriţi să specificaţi faptul că o conexiune este stabilită doar dacă sistemul la distanţă suportă protocolul BACP (Bandwidth Allocation Protocol). Dacă nu poate fi negociat BACPt, este permisă doar o legătură singulară.
5. Selectaţi fişa **Configurări TCP/IP** pentru a activa una din următoarele setări:

   Permiterea altor sisteme de la distanţă să acceseze alte reţele (înaintarea IP). Această opţiune specifică dacă doriţi ″IP forwarding″. Dacă selectaţi această opţiune, veţi permite serverului iSeries să se comporte ca un ruter pentru această conexiune. Aceasta permite ca datagramele IP (Internet Protocol) care nu sunt destinate serverului iSeries să treacă prin acest sistem către o reţea conectată. Dacă lăsaţi această opţiune neselectată, IP ignoră acele datagrame de la sistemul la distanţă care nu sunt destinate nici uneia dintre adresele locale ale acestui server iSeries.

   Ar putea exista motive de securitate pentru care aţi dori să nu permiteţi înaintarea IP. În schimb, un ISP (furnizor de servicii internet) furnizează înaintarea IP. Observaţi că aceasta va avea efect doar dacă este activată înaintarea datagramelor IP pe tot sistemul, altfel aceasta va fi ignorată chiar dacă este activată. Setarea pentru înaintarea datagramelor IP pe tot sistemul poate fi văzută în fişa **General** din pagina Proprietăţi IPv4.

   Cerere compresie antet TCP/IP (VJ). Această opţiune specifică dacă doriţi ca IP să comprime informaţiile din antet după stabilirea unei conexiuni. Comprimarea duce de obicei la creşterea performanţelor, în special pentru traficul interactiv sau liniile seriale lente. Compresia antetelor foloseşte metoda Van Jacobson (VJ) definită în RFC 1332. Pentru PPP, compresia este negociată la stabilirea conexiunii. Dacă celălalt capăt al conexiunii nu suportă comprimarea VJ, serverul iSeries stabileşte o conexiune care nu foloseşte comprimarea.

   Folosire reguli pachet IP pentru această conexiune. Această opţiune specifică dacă doriţi să aplicaţi o regulă de filtrare pentru această politică de grup. Regulile de filtrare vă permit controlarea traficului IP acceptat de reţea.

Puteţi folosi această componentă de filtrare a pachetului IP pentru protejarea sistemului. Componenta de filtrare a pachetului IP protejează sistemul prin filtrarea pachetelor în funcţie de regulile pe care le specificaţi. Regulile se bazează pe informaţiile din antetul pachetului.

Aplicarea unei politici de grup unui utilizator cu acces la distanţă

Puteţi aplica o politică de grup unui utilizator cu acces de la distanţă după ce aţi completat proprietăţile punct-la-punct pentru un nou profil de conexiune receptor.

Pentru a aplica o politică de grup unui utilizator la distanţă, efectuaţi următorii paşi:

1. Faceţi clic pe **Autentificare** pentru a deschide pagina Autentificare.
2. Selectaţi **Este necesar ca acest server iSeries să verifice identitatea sistemului la distanţă**.
3. Selectaţi **Autentificare locală folosind o listă de validare**.
4. Dacă există o listă de validare, selectaţi-o din listă şi apăsaţi **Deschidere**. Dacă o creaţi pentru prima dată, introduceţi un nume pentru noua listă de validare şi apăsaţi **Nou**.
5. Faceţi clic pe **Adăugare** pentru a adăuga un nou utilizator în lista de validare.
6. În fereastra Adăugare utilizator, specificaţi următoarele informaţii:
   a. Selectaţi protocolul de autentificare pentru care este definit numele utilizatorului.
   b. Introduceţi numele şi parola de utilizator.

      Notă: Din motive de securitate, este recomandat să nu folosiţi aceeaşi parolă pentru un utilizator definit pentru CHAP (Challenge Handshake Authentication Protocol 22314), EAP (Extensible Authentication Protocol) şi PAP (Password Authentication Protocol).

   c. Activaţi **Aplicarea unei politici de grup utilizatorului**, selectaţi o politică de grup din listă şi apăsaţi **Deschidere**.

   Puteţi modifica proprietăţile politicii de grup sau puteţi folosi setările existente.
7. Faceţi clic pe **OK** pentru încheierea configurării şi revenire la pagina Proprietăţi punct-la-punct.

Referinţe înrudite

"Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP" la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Informaţii înrudite

Filtrarea IP şi translatarea adresei de reţea (NAT)

Aplicarea regulilor de filtrare pachet IP unei conexiuni PPP

Puteţi folosi un fişier cu reguli de pachet pentru a restricţiona accesul unui utilizator sau al unui grup la adrese IP din reţeaua dumneavoastră.

Subiectul Regulile de filtrare pachet IP şi NAT din Centrul de informare discută despre modul de creare a regulilor pachet IP pe care să le puteţi referi pentru un profil de conexiune PPP.

Puteţi referi regulile existente de filtrare a pachetelor IP în două moduri:

- Nivel profil de conexiune
  1. La completarea **Proprietăţi punct-la-punct** pentru un **Profil de conexiune receptor**, selectaţi pagina Configurări TCP/IP şi apăsaţi **Avansat**.
  2. Activaţi **Folosire reguli pachet IP pentru această conexiune** şi selectaţi un identificator de filtru PPP din listă.
  3. Faceţi clic pe **OK** pentru a aplica filtrul PPP profilului de conexiune.
- Nivel utilizator

1. Deschideţi o politică de acces grup existentă sau creaţi una nouă.
2. Selectaţi pagina Configurări TCP/IP.
3. Activaţi **Folosire reguli pachet IP pentru această conexiune** şi selectaţi un identificator de filtru PPP din listă.
4. Faceţi clic pe **OK** pentru a aplica filtrul PPP.

Referinţe înrudite

"Scenariu: Gestionarea accesului utilizatorilor la distanţă la resurse folosind Politicile de grup şi filtrare IP" la pagina 24
Politicile de acces de grup identifică grupuri de utilizatori distincte pentru o conexiune şi vă permit să aplicaţi atribute de conexiune comune şi setări de securitate întregului grup. În combinaţie cu filtrarea IP, aceasta vă dau posibilitatea să permiteţi sau restricţionaţi accesul la anumite adrese IP din reţeaua dumneavoastră.

Activarea serviciilor RADIUS şi DHCP pentru profiluri conexiune

Pentru a activa serviciul RADIUS sau DHCP pentru profilurile de conexiune receptor PPP, urmaţi aceşti paşi:

1. În Navigator iSeries, selectaţi serverul dumneavoastră şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Servicii de acces la distanţă** şi selectaţi **Servicii**.
3. Selectaţi fişa **DHCP-WAN**. Aceasta va activa automat DHCP şi va detecta ce server DHCP şi agenţi retransmitere (dacă există) rulează pe sistem.
4. Pentru a activa serviciile RADIUS selectaţi fişa **RADIUS**.
   a. Selectaţi **Activare conexiune RADIUS Network Access Server**
   b. Selectaţi **Activare RADIUS pentru autentificare**.
   c. În funcţie de soluţia RADIUS, puteţi de asemenea alege ca RADIUS să trateze contabilizarea conexiunilor şi configurarea adreselor TCP/IP.
5. Faceţi clic pe butonul **Setări RADIUS NAS** pentru a configura conexiunea cu serverul RADIUS.
6. Faceţi clic pe **OK** pentru a reveni la Navigator iSeries.

Referinţe înrudite

"Scenariu: Autentificarea conexiunilor apel telefonic cu RADIUS NAS" la pagina 22
Rulând NAS (Network Access Server) pe serverul iSeries, cererile de autentificare de la clienţii prin apel telefonic pot fi rutate la un server RADIUS separat. Dacă este autentificat, RADIUS poate de asemenea controla adresele IP ale utilizatorului.

Gestionarea PPP

Puteţi citi despre task-urile de administrare PPP pe care le puteţi efectua pe serverul iSeries.

Referinţe înrudite

"Informaţii înrudite pentru PPP" la pagina 65
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Setarea proprietăţilor pentru profiluri conexiune PPP

La crearea unui profil de conexiune, de obicei selectaţi protocolul, tipul de conexiune şi modul de operare pentru noul profil de conexiune în fereastra Configurare profil de conexiune punct-la-punct.

După introducerea selecţiilor în această fereastră va apare pagina de proprietăţi a profilului de conexiune. Selecţiile specificate în fereastra Configurare profil de conexiune punct-la-punct determină conţinutul şi ordinea fişelor din pagina de proprietăţi a profilului de conexiune. Pagina de proprietăţi este diferită pentru profiluri de conexiune originator şi cele receptor.

Puteţi folosi aceste îndrumări pentru a completa fiecare pagină a ferestrei **Proprietăţi profil punct-la-punct**. Setările pe care le selectaţi în fiecare pagină depind de mediu şi de tipul de conexiune configurată. Ajutorul online din Navigator iSeries descrie fiecare opţiune care apare în fereastră. Puteţi consulta şi exemplele şi procedurile PPP pentru informaţii suplimentare.

Monitorizarea activităţii PPP

Puteţi vizualiza un profil de conexiune şi un istoric de sesiune folosind Navigator iSeries.

Despre joburile conexiunii PPP:

- Există două joburi de control PPP care sunt folosite pentru administrarea joburilor individuale ale conexiunii PPP. Aceste joburi rulează în subsistemul QSYSWRK:
  - QTPPPCTL - Jobul principal de control PPP. Acest job administrează fiecare job al conexiunii PPP.
  - QTPPPL2TP - Server L2TP. Acest job gestionează stabilirea tunelului L2TP şi rulează doar dacă rulează în mod curent un profil L2TP.
- Firele de execuţie PPP ale conexiunii rulează în QTPPPCTL sub numele de utilizator QTCP.
- Joburile pentru conexiuni SLIP rulează în subsistemul QSYSWRK din numele utilizator QTCP. Există două tipuri de nume pentru joburile SLIP:
  - QTPPDIAL*nn* sunt joburi cu transmitere apel unde *nn* este orice număr între 1 şi 99.
  - QTPPANS*nn* sunt joburi cu primire apel unde *nn* este orice număr între 1 şi 99.

Gestionarea profilurilor de conexiune:

1. În Navigator iSeries, expandaţi serverul dumneavoastră şi accesaţi **Reţea → > Servicii de acces la distanţă**. Selectaţi **Profil de conexiune originator** sau **Profil de conexiune receptor**.
2. În coloana Profil, efectuaţi clic-dreapta pe orice nume de profil de conexiune şi selectaţi una din următoarele opţiuni:
   - **Conexiuni** deschide o fereastră pentru a afişa informaţii despre toate conexiunile asociate cu acel profil. Informaţiile pot include datele despre conexiunea curentă, despre conexiunile anterioare sau ambele. Sunt disponibile pentru fiecare conexiune opţiuni pentru a vedea ieşirile joburilor, detaliile conexiunii, istoricele pentru apeluri sau istoricele de mesaje.
   - **Proprietăţi** deschide pagina Proprietăţi pentru a afişa proprietăţile curente ale unei conexiuni.

Vizualizarea informaţiilor despre conexiune:

1. În Navigator iSeries, expandaţi serverul dumneavoastră şi accesaţi **Reţea → > Servicii de acces la distanţă**. Selectaţi **Profil de conexiune originator** sau **Profil de conexiune receptor**.
2. În coloana Profil, efectuaţi clic-dreapta pe orice nume de profil de conexiune care nu are starea Inactiv şi selectaţi **Conexiuni** pentru a vedea informaţii despre conexiune.

   Este arătată fiecare conexiune pentru acest profil (curentă sau anterioară). Câmpul de stare indică starea curentă a conexiunii. Informaţii suplimentare cum sunt ID utilizator pentru utilizatorul conectat, ID fir de execuţie, adrese IP locale şi la distanţă şi numele jobului PPP ar putea fi afişate în funcţie de starea fiecărui job PPP.
3. Pentru a vizualiza ieşirea jobului, detalii despre o conexiune, istoricele de apeluri sau istoricele de mesaje efectuaţi clic-dreapta pe o conexiune pentru a activa butoanele.
4. Pentru a vedea QTPPPCTL, selectaţi **Joburi**. Din fereastra de conexiuni, faceţi clic dreapta pe numele jobului şi selectaţi **Ieşire imprimantă** sau **Istoric job** pentru a afişa informaţiile despre toate firele de execuţie ale conexiunii asociate cu QTPPPCTL.
5. Pentru a vedea detaliile conexiunii, selectaţi **Detalii**. Detaliile nu pot fi afişate decât pentru conexiunile care sunt active în acel moment. Fereastra cu detalii vă va permite să vedeţi informaţii suplimentare despre această conexiune.
6. Pentru a vedea istoricele de apeluri, selectaţi **Istoric de apeluri**.
7. Pentru a vedea istoricele de mesaje, selectaţi **Istoric de mesaje**.

Gestionare ieşire PPP de la serverul iSeries:

Pentru gestionarea ieşirii PPP, tastaţi WRKTCPPTP în linia de comandă a serverului iSeries:

- Pentru gestionarea TUTUROR joburilor PPP active (incluzând joburile QTPPPCTL şi QTPPPL2TP), apăsaţi F14 (Gestionare joburi active).
- Pentru gestionarea tuturor ieşirilor pentru un anumit profil de conexiune, selectaţi **opţiunea 8** (gestionare ieşiri) pentru acel profil.
- Pentru a tipări configurările profilului PPP, selectaţi **opţiunea 6** (Tipărire) pentru acel profil. Apoi folosiţi comanda WRKSPLF pentru a accesa ieşirea tipărită.

Starea conexiunii:

Starea profilului conexiune este afişată în câmpul **Stare** pentru fiecare profil din lista profilurilor conexiune din **Reţea → Servicii de acces la distanţă** după selectarea fie a profilului originator, fie a celui receptor. Starea unei conexiuni individuale este afişată folosind fereastra Conexiuni.

Tabela 10. Descriere stare primară

Descriere stare primară	**Explicaţie**
Aşteaptă cereri de conectare	Profilul receptor gata pentru conectare
Aşteaptă primire apel	Server gata pentru conectare
În curs de conectare	În procesul de conectare cu sistemul la distanţă
Activ/Conexiuni active	Conexiune realizată şi jobul rulează cu succes
Inactiv	În acest moment nu rulează nici un job pentru acest profil de conexiune
Încheiat	Informaţii disponibile
Terminatorul multihop porneşte iniţiatorul multihop	Multihop în desfăşurare
Conexiunea multihop este activă	Multihop conectat cu succes

Tabela 11. Decriere stare secundară

Decriere stare secundară	**Explicaţie**
Iniţializare modem	Iniţializare modem la începutul conexiunii prin apel telefonic
Aşteptare conexiune modem	Serverul PPP în stare de ascultare
APELARE xxx-xxxx	Număr apelat de clientul prin apel telefonic
Apel de intrare detectat	Serverul PPP detectează un apel modem de intrare
Modem conectat	Dialog de confirmare (handshake) PPP completat cu succes
Operaţional	Conexiune PPP activă
Legătură terminată	Conexiune terminată de peer
Oprit	Profil sau job terminat
Eşec autentificare	A eşuat stabilirea conexiunilor PPP din cauza eşuării autentificării
Expirare timp de aşteptare pentru inactivitatea conexiunii	Conexiunile PPP au eşuat să se stabilească datorită expirării timpului de aşteptare activitate
Negociere adrese IP	Conexiunile PPP s-au terminat datorită problemelor de negociere IP
Modem-ul la distanţă nu a răspuns	Conexiunile PPP au eşuat să se stabilească datorită inexistenţei răspunsului de la cealaltă parte
Refuzare protocol	Conexiunile PPP au eşuat datorită eşecului negocierii NCP
Eşec reîncercare	Conexiunea PPP a eşuat să se stabilească datorită numărului depăşit de reîncercări

Tabela 11. Decriere stare secundară (continuare)

Decriere stare secundară	Explicaţie
Confirmare sesiune PPPoE primită de la peer	Negociere PPPoE terminată cu succes
Apel L2TP stabilit	Mesaj tunel L2TP

Depanarea PPP

Dacă aveţi probleme cu conexiunile PPP, puteţi folosi această listă de verificare pentru a strânge informaţii despre eroare. Lista de verificare vă poate ajuta la identificarea simptomelor de eroare şi la rezolvarea problemelor conexiunilor PPP.

Informaţiile curente şi relevante despre corecţiile temporare de program (PTF-uri) şi despre depanare sunt documentate pe pagina de bază iSeries server TCP/IP . iSeries . Această legătură oferă ultimele informaţii care suplimentează şi înlocuiesc informaţiile conţinute în acest subiect.

1. Material necesar pentru suport:
   - Tip gazdă la distanţă, sistem de operare şi nivel
   - Nivel sistem de operare al serverului iSeries
   - Toate fişierele de ieşire sunt salvate într-o coadă de ieşire cu un nume identic cu al profilului.
   - Istoricele de job pentru QTPPPCTL şi QTPPPL2TP (dacă este un profil L2TP)
   - Script conexiune, dacă se foloseşte îm mediul dumneavoastră
   - Starea profilului de conexiune înainte şi după eşuarea conexiunii
2. Material recomandat pentru suport:
   - Descriere linie
   - Profil de conexiune

     Opţiunea 6 din WRKTCPPTP tipăreşte setările profilului.
   - Tip şi model modem
   - Şiruri de comandă modem
   - Urmărire comunicaţii

Manualul ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) acoperă următoarele probleme PPP. De asemenea, oferă şi informaţii detaliate de rezolvare a problemelor.

Tabela 12. Probleme PPP din ITSO Redbook

Problemă	Soluţie
Configurare hardware modem Configurare greşită a comutatoarelor dip şi a altor setări hardware	Asiguraţi-vă că modemul este configurat cu tipul corect de cadre. Acesta poate fi fie *Asincron*, fie *Sincron*. Consultaţi manualul modemului pentru informaţii suplimentare.
Comenzile AT de modem Modemul pe care încercaţi să-l folosiţi nu apare în lista cu modemuri predefinite din Navigator iSeries.	Crearea unui nou modem.
Utilizatori şi parole PPP Obţineţi erori de nume şi parolă utilizator atunci când încercaţi o conexiune PPP.	• Asiguraţi-vă că ID-ul şi parola utilizatorului sunt introduse folosind majuscule sau litere mici, după cum este cazul. • Asiguraţi-vă că protocolul de autentificare folosit de parteneri este acelaşi. • Nu folosiţi PAP la unul din parteneri în timp ce celălalt partener este configurat pentru CHAP.

Tabela 12. Probleme PPP din ITSO Redbook (continuare)

Problemă	Soluţie
Linii PPP pentru pornirea unui profil de conexiune Liniile PPP identificate sunt folosite de aceeaşi resursă hardware.	Nu uitaţi să schimbaţi celelalte linii care folosesc aceeaşi resursă hardware.
Protocol PPP Erorile de conectare pot apare din cauza configurării greşite a protocolului PPP.	Investigarea nivelelor de jos ale protocolului PPP ar putea fi necesară în unele situaţii în care partenerii nu reuşesc să comunice între ei din cauza unei erori de configurare. Dacă istoricul PPP sau istoricul job al jobului PPP nu dau nici o indicaţie despre problemă, puteţi investiga problema folosind funcţia de urmărire a comunicaţiei.

Concepte înrudite

"Configurarea modemului pentru PPP" la pagina 54
Pentru conexiunile dumneavoastră analogice PPP puteţi folosi un modem extern, intern sau un adaptor terminal ISDN. Un modem vă oferă capacităţile conexiunilor analogice (linii închiriate şi comutate). Pentru serverul iSeries au fost definite descrierile de modem pentru cele mai folosite modemuri.

"Configurare modem nou" la pagina 55
În acest subiect aflaţi cum să configuraţi un modem nou.

Referinţe înrudite

"Informaţii înrudite pentru PPP"
Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

Informaţii înrudite pentru PPP

Mai jos sunt listate cărţi IBM Redbooks (în format PDF) şi situri Web care au legătură cu subiectul PPP. Puteţi citi sau tipări oricare din PDF-uri.

IBM Redbooks

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

Site-uri Web

Găsiţi cele mai noi corecţii temporare de program (PTF-uri) şi cele mai noi informaţii despre configurare pentru PPP şi L2TP prin legătura PPP de pe pagina de bază iSeries™ server TCP/IP. Această legătură oferă ultimele informaţii care suplimentează şi înlocuiesc informaţiile conţinute în această colecţie de subiecte.

Salvarea fişierelor PDF

Pentru a salva un PDF pe staţia de lucru proprie pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe PDF în browser (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe opţiunea care salvează fişierul PDF local.
3. Navigaţi până la directorul unde vreţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Aveţi nevoie de Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca gratis o copie de la situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licenţa pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

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

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte), contactaţi departamentul de Proprietate intelectuală al IBM-ului din ţara dumneavoastră sau trimiteţi întrebările în scris la:

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

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE SUBÎNŢELESE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit renunţarea la garanţiile exprese sau deduse în anumite tranzacţii, de aceea aceste clauze pot să nu vi se aplice.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Informaţiile incluse aici sunt modificate periodic; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de site-uri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor site-uri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie faţă de dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile, cu condiţia respectării termenilor şi condiţiilor, iar în unele cazuri cu plata unor taxe.

Programul cu licenţă descris în aceste informaţii şi toate materialele cu licenţă disponibile pentru acesta sunt furnizate de către IBM conform termenilor din Contractul IBM cu Clientul, Contractul de Licenţă IBM pentru Programele Internaţionale, Contractul de Licenţă IBM pentru Codul Maşină, sau orice contract echivalent dintre noi.

Toate datele de performanţă conţinute aici au fost determinate într-un mediu controlat. Prin urmare, rezultatele obţinute în alte medii de operare pot fi semnificativ diferite. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat şi nu există nici o garanţie că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, este posibil ca anumite măsurători să fi fost estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice datele aplicabile pentru mediul lor specific.

Informaţiile în legătură cu produsele non-IBM au fost obţinute de la furnizorii acelor produse, din anunţurile publicate de aceştia sau din alte surse publice disponibile. IBM nu a testat acele produse şi nu poate confirma acurateţea performanţei, compatibilitatea sau orice alte pretenţii legate de produse non-IBM. Întrebările privind capabilităţile produselor non-IBM se pot adresa furnizorilor acelor produse.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţii de afaceri zilnice. Pentru a le ilustra cât mai complet posibil, exemplele includ nume de persoane, companii, mărci şi produse. Toate aceste nume sunt fictive şi orice asemănare cu nume şi adrese utilizate de o întreprindere reală este pur întâmplătoare.

LICENŢĂ DE COPYRIGHT:

Aceste informaţii cuprind exemple de programe de aplicaţie în limbaj sursă, care ilustrează tehnici de programare pe diverse platforme de operare. Puteţi copia, modifica şi distribui aceste programe-eşantion în orice formă fără necesitatea unei plăţi către IBM, în scopul dezvoltării, utilizării, marketingului sau distribuirii programelor de aplicaţie în concordanţă cu interfaţa de programare a aplicaţiei pentru platforma de operare pentru care sunt scrise programele-eşantion. Aceste exemple nu au fost testate complet în toate condiţiile. Prin urmare, IBM nu poate garanta sau sugera că aceste programe vor fi fiabile, practice sau funcţionale.

Fiecare copie sau orice porţiune din aceste programe-eşantion sau orice lucrare derivată trebuie să includă un aviz de copyright, după cum urmează:

© (numele companiei dumneavoastră) (anul). Porţiuni din acest cod sunt derivate din Programe eşantion ale IBM Corp.
© Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vedeţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Informaţii despre interfaţa de programare

Această publicaţie Servicii de acces la distanţă: Conexiunile PPP documentează Interfeţele de programare proiectate care permit clientului să scrie programe pentru a obţine serviciile IBM i5/OS.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

AIX
i5/OS
IBM

| iSeries
|
| Lotus
| OS/400
|
| Redbooks

Linux este marcă comercială a Linus Torvalds în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată, deţinută de The Open Group în Statele Unite şi în alte ţări.

Microsoft, Windows, Windows NT şi emblema Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza lucrări derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit de la IBM.

În afara celor acordate expres prin această permisiune, nu se acordă nici o altă permisiune, licenţă sau drept, explicite sau implicite, pentru aceste publicaţii sau orice informaţii, date, software sau alte elemente pe care le conţin şi care reprezintă o proprietate intelectuală.

IBM îşi păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreţia sa, dacă folosirea publicaţiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât respectând integral legile şi reglementările în vigoare, precum şi legile şi reglementările din Statele Unite privind exportul.

IBM NU OFERĂ GARANŢII DESPRE CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.