System i

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

Versiunea 6 Ediţia 1

System i

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

Versiunea 6 Ediţia 1

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, citiţi informaţiile din “Observaţii”, la pagina 65.

Această ediţie este valabilă pentru IBM i5/OS (număr de produs 5761–SS1) versiunea 6, ediţia 1, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare, până se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Serviciile de acces la distanţă: Conexiunile PPP 1

Fişierul PDF pentru Serviciile de acces la distanţă 1
Concepte privind PPP 1
Ce este PPP 2
Profilurile de conexiune 2
Suportul pentru politică de grup 4
Scenarii: Accesul de la distanţă folosind conexiuni PPP . . 4
Exemplu: PPP şi DHCP pe un singur System i 4
Scenariu: Profil DHCP şi PPP pe modele diferite System i 6
Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec 9
Scenariu: Conectarea sistemului la un concentrator de acces PPPoE 10
Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră 13
Scenariu: Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem 15
Scenariu: Conectarea reţelei dumneavoastră corporative şi la distanţă cu un modem 18
Scenariu: Autentificarea conexiunilor dial-up cu RADIUS NAS 21
Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP. 23
Scenariu: Partajarea unui modem între partiţii logice utilizând L2TP 26
Detalii scenariu: Partajare unui modem între partiţii logice utilizând L2TP 28
Pasul 1: Configurarea unui profil terminator L2TP pentru orice interfaţă de pe partiţia care deţine modemurile. 28
Pasul 2: Configurarea unui profil originator L2TP pe 10.1.1.74. 29
PAsul 3: Configurarea unui profil de apel la distanţă L2TP pentru 192.168.1.2 30
Pasul 4: Testarea conexiunii 30
Planificarea PPP 31
Cerinţe de software şi hardware 31
Alternative de conexiune 32
Linii telefonice analogice. 32
Serviciul digital şi DDS 33
Switched-56 34
ISDN (Integrated Services Digital Network) . . . 34
Conexiuni T1/E1 şi T1 fracţional 35
Frame relay. 36
Suport L2TP pentru conexiuni PPP. 36
Tunel voluntar 37
Model de tunel obligatoriu - apel de intrare . . 37
Model de tunel obligatoriu - apel la distanţă . . 37
Conexiune multi-hop L2TP 37
Suportul PPPoE (DSL) pentru conexiuni PPP. . . 37
Echipamentul conexiunii 38
Modemuri 38
CSU/DSU 38
Adaptoare terminale ISDN 39
Sugestii pentru adaptorul terminal ISDN . . . 39
Restricţii la adaptoarele terminale ISDN . . . 40
Tratarea adreselor IP 40
Filtrarea pachetelor IP 41
Strategia de gestionare a adreselor IP 41
Autentificarea sistemului 43
CHAP (Challenge Handshake Authentication Protocol) cu MD5 43
EAP (Extensible Authentication Protocol). . . . 44
PAP (Password Authentication Protocol) 44
Privire generală asupra RADIUS 44
Lista de validare 45
Considerente de lăţime de bandă pentru legătură multiplă 45
Configurarea PPP 46
Crearea unui profil de conexiune 46
Tip ptotocol: PPP sau SLIP (Serial Line Internet Protocol) 47
Selecţii mod 47
Linie comutată 48
Linie închiriată. 48
L2TP (linie virtuală) 49
Linie PPPoE 49
Configurarea legăturii. 49
Linie singulară 50
Pool de linii. 50
Suport pentru profil conexiuni multiple . . . 52
Configurarea modemului pentru PPP 54
Configurarea unui modem nou 54
Setarea şirurilor de comenzi pentru modem . . . 55
Exemplu: Configurarea unui adaptor terminal ISDN 55
Asocierea unui modem cu o descriere de linie . . 56
Configurarea unui PC la distanţă 56
Configurarea accesului la Internet prin AT&T Global Network. 57
Vrăjitori de conectare 57
Configurarea unei politici de acces de grup 58
Aplicarea regulilor de filtrare a pachetelor IP la o conexiune PPP 59
Activarea serviciilor RADIUS şi DHCP pentru profiluri de conexiune 60
Gestionarea PPP 60
Setarea proprietăţilor pentru profiluri de conexiune PPP 60
Monitorizarea activităţii PPP 61
Depanarea PPP. 63
Informaţii înrudite pentru Serviciile de acces la distanţă. . 64

Anexa. Observaţii 65

Informaţii despre interfaţa de programare 66
Mărci comerciale 66
Termenii şi condiţiile 67

Serviciile de acces la distanţă: Conexiunile PPP

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

Este protocolul de conectare cel mai utilizat de către furnizorii de servicii Internet (ISP - Internet service Provider). PPP permite calculatoarelor individuale să acceseze reţele. Prin intermediul reţelelor, se obţine acces la Internet. Produsul System i include suport TCP/IP PPP ca parte a conectivităţii sale de reţea de suprafaţă mare (WAN).

Puteţi schimba date între locaţii utilizând PPP pentru a conecta un calculator de la distanţă la platforma dumneavoastră System i. Prin PPP, sistemele de la distanţă care sunt conectate la sistemul dumneavoastră pot accesa resurse sau alte maşini care aparţin aceleiaşi reţele ca şi sistemul dumneavoastră. De asemenea, vă puteţi configura sistemul pentru a vă conecta la Internet utilizând PPP. Vrăjitorul Conexiune prin apel telefonic din System i Navigator vă poate ghida prin procesul de conectare a sistemului la Internet sau la o reţea internă.

Fişierul PDF pentru Serviciile de acces la distanţă

Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

Pentru a vizualiza sau descărca versiunea PDF a acestui document, selectaţi Serviciile de acces la distanţă: Conexiunile PPP (aproximativ 940 KB).

Salvarea fişierelor PDF

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

1. Faceţi clic dreapta pe legătura PDF-ului din browser-ul dumneavoastră.
2. Faceţi clic pe opţiunea de salvare locală a PDF-ului.
3. Navigaţi la directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Pentru a vizualiza sau tipări aceste PDF-uri, trebuie să aveţi instalat pe sistem Adobe Reader. Puteţi descărca o copie gratuită de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Referinţe înrudite

“Informaţii înrudite pentru Serviciile de acces la distanţă” la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Concepte privind PPP

Puteţi utiliza PPP pentru a conecta o platformă System i la reţele la distanţă, PC-uri client, o altă platformă System i sau un furnizor de servicii Internet (ISP). Pentru a folosi întreaga funcţionalitate oferită de acest protocol, ar trebui să înţelegeţi atât capabilităţile sale, cât şi suportul i5/OS existent pentru el.

Referinţe înrudite

“Informaţii înrudite pentru Serviciile de acces la distanţă” la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Ce este PPP

Protocolul punct-la-punct (PPP) este un protocol TCP/IP utilizat pentru a conecta un sistem de calculatoare la altul. Calculatoarele utilizează PPP pentru a comunica prin reţeaua telefonică sau prin Internet.

O conexiune PPP se realizează 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 de filială permite ambelor sedii să transfere date celuilalt prin reţea.

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 pe pagina web RFC Editor.

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

Profilurile de conexiune

Profilurile de conexiune punct-la-punct definesc un set de parametri şi resurse pentru conexiuni Protocol punct-la-punct (PPP) specifice. Puteţi porni profiluri care utilizează aceste setări de parametri pentru apeluri telefonice de ieşire (iniţiatoare) sau pentru a asculta (recepta) conexiuni PPP.

Puteţi utiliza următoarele două tipuri de profiluri pentru a defini un set de caracteristici pentru o conexiune PPP sau un set de conexiuni:

- *Profilurile de conexiune originatoare* sunt conexiunile punct-la-punct iniţiate de pe sistemul local şi sunt primite de un sistem la distanţă. Puteţi configura conexiunile care trebuie iniţiate folosind acest obiect.
- *Profilurile de conexiune receptoare* sunt conexiuni punct-la-punct iniţiate de pe un sistem la distanţă şi sunt primite de sistemul local. Puteţi configura conexiunile care trebuie receptate folosind acest obiect.

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

- Ce tip de protocol de conexiune utilizaţi? (PPP sau SLIP (Serial Line Internet Protocol))
- Sistemul dumneavoastră contactează celălalt caluclator printr-un apel de ieşire (originator)? Sistemul dumneavoastră aşteaptă să primească un apel de la celălalt sistem (receptor)?
- Ce linie de comunicaţii utilizează conexiunea?
- Cum ar trebui sistemul dumneavoastră să determine ce adresă IP să utilizeze?
- Cum ar trebui sistemul dumneavoastră să autentifice alt sistem? Unde ar trebui sistemul dumneavoastră să memoreze 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

Sistemul memorează aceste informaţii de configurare într-un profil de conexiune. Aceste informaţii furnizează contextul necesar pentru ca sistemul dumneavoastră 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 sugerează să utilizaţi PPP oricând e posibil.
- **Selectare mod**. Selectarea modului specifică tipul conexiunii şi modul de operare pentru acest profil de conexiune.

  Tip conexiune. Aceasta specifică tipul de linie pe care sunt conexiunile dumneavoastră şi dacă sunt de apel (originator) sau de răspuns (receptor). Puteţi selecta dintre aceste tipuri de conexiune:
  - Linie comutată
  - Linie închiriată (dedicată)
  - Protocol de tunelare nivelul doi (L2TP) (linie virtuală)
  - Protocolul punct-la-punct prin Ethernet (PPPoE) (linie virtuală)

  PPPoE este suportat numai pentru profiluri de conexiune originatoare.
- **Mod de funcţionare**. Modul de funcţionare disponibil depinde de tipul conexiunii.

Tabela 1. Modurile de funcţionare disponibile pentru profilurile de conexiune originatoare

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

Tabela 2. Modurile de funcţionare disponibile pentru profilurile de conexiune receptoare

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 de servicii de linie este doar de linie singulară.

  Referinţe înrudite

  “Cerinţe de software şi hardware” la pagina 31
  Pentru un mediu PPP este necesar să aveţi două sau mai multe calculatoare care suportă PPP. Unul dintre aceste calculatoare, platforma System i, poate fi originatorul sau receptorul.

Suportul pentru politică de grup

Cu suportul pentru politică de grup, administratorii de reţea pot defini politici pentru grupuri de utilizatori pentru a gestiona resursele. Utilizatorilor individuali le pot fi alocate politici de control al accesului atunci când se loghează în sesiunea PPP sau L2TP.

Utilizatorii pot fi identificaţi ca aparţinând unei anumite clase de utilizatori. Fiecare clasă are politica sa unică, definind limitele resurselor (precum numărul de legături permise într-un bundle de legături multiple), atribute (precum înaintarea IP) şi identificarea setului de reguli penntru filtru de pachete IP care să se aplice. De exemplu, cu suportul de politică de grup administratorii de reţea pot defini un grup Lucru_de_acasă care permite acces complet la reţea sau un grup Lucrători_vânzare care este restricţionat la un set de servicii.

Referinţe înrudite

"Scenariu: Conectarea sistemului la un concentrator de acces PPPoE" la pagina 10
Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

"Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP" la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

Scenarii: Accesul de la distanţă folosind conexiuni PPP

În aceste scenarii puteţi vedea cum funcţionează PPP şi cum se implementează un mediu PPP într-o reţea. De asemenea, scenariile prezintă concepte PPP fundamentale, care pot fi utile atât începătorilor, cât şi utilizatorilor experimentaţi pentru taskurile de configurare şi planificare.

Referinţe înrudite

"Informaţii înrudite pentru Serviciile de acces la distanţă" la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Exemplu: PPP şi DHCP pe un singur System i

Acest exemplu explică modul în care se setează un model System i ca server DHCP pentru un LAN şi un client dial-in la distanţă.

Clienţii la distanţă, cum sunt clienţii prin apel telefonic, au nevoie adesea de acces la reţeaua unei companii. Clienţii dial-in pot obţine acces la modelul System i cu Protocolul punct-la-punct (PPP). Pentru a accesa reţeaua, clientul dial-in are nevoie de informaţii IP, ca orice client ataşat direct în reţea. Un server DHCP System i poate distribui informaţii de adresă IP unui client dial-in PPP la fel ca oricărui alt client ataşat direct. Următoarea ilustraţie prezintă un client la distanţă care trebuie să apeleze telefonic reţeaua companiei pentru a lucra ceva.

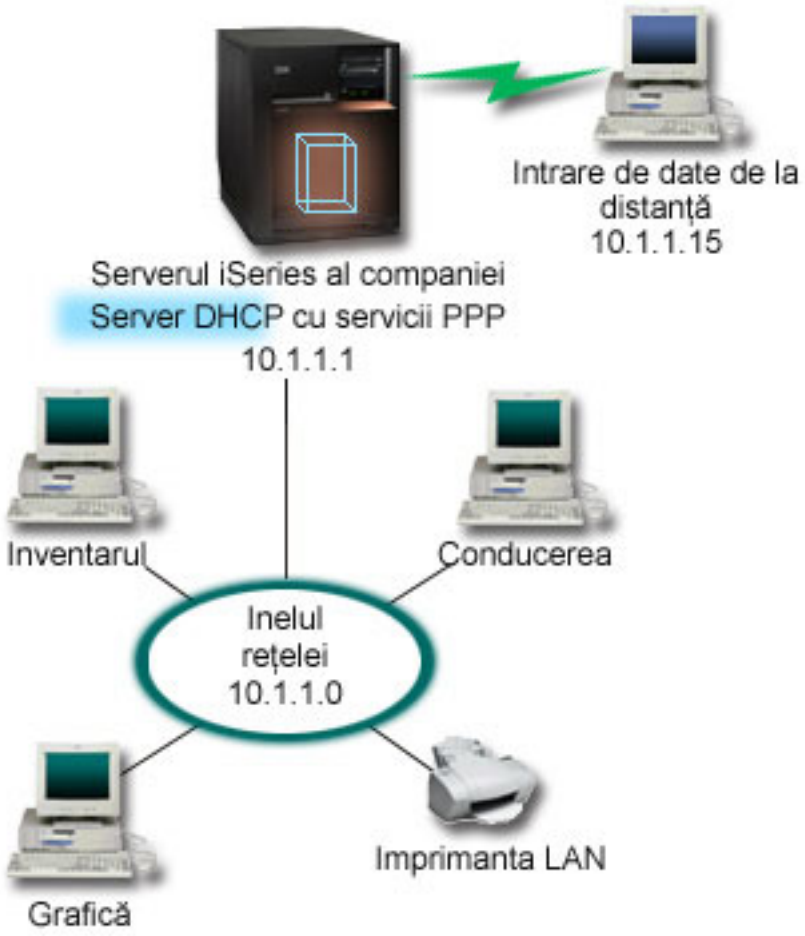


Figura 1. PPP şi DHCP pe un singur model System i

Pentru ca angajatul la distanţă să devină cu succes parte a reţelei companiei, modelul System i trebuie să utilizeze o combinaţie de Servicii de acces la distanţă şi DHCP. Funcţia Servicii acces la distanţă creează capabilitatea dial-in pentru modelul System i. Dacă este setat corespunzător, după ce clientul stabileşte conexiunea dial-in, serverul PPP anunţă serverul DHCP să distribuie informaţii TCP/IP clientului la distanţă.

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 receptoare, setaţi metoda de alocare a adresei IP la distanţă de la Fixat la DHCP. Pentru a permite clienţilor dial-in să comunice cu alţi clienţi ai reţelei, cum ar fi imprimanta din LAN, trebuie să permiteţi şi înaintarea IP în setările TCP/IP ale profilului şi proprietăţile de configurare TPC/IP (stivă). Dacă setaţi înaintarea IP doar în profilul PPP, modelul System i nu va transmite pachetele IP. Trebui să setaţi înaintarea IP atât în profil, cât şi în stivă.

De asemenea, adresa IP de interfaţă locală din profilul PPP trebuie să fie o adresă IP care se încadrează în definiţia de subreţea din serverul DHCP. În acest exemplu, adresa IP de interfaţă locală profil PPP trebuie să fie 10.1.1.1. Această adresă trebuie, de asemenea, exclusă din poolul de adrese la serverului DHCP, astfel 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 de nume domeniu	10.1.1.1
	Opţiunea 15: Nume domeniu	mycompany.com
Sistemul realizează actualizări DNS?		Nu
Sistemul 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 (Adresă interfaţă locală specificată în setările TCP/IP ale proprietăţilor Profil conexiune receptoare din System i Navigator)

Alte setări

- Setaţi metoda adresei IP de la distanţă la DHCP în profilul de conexiune receptor PPP.
  1. Activaţi conexiunea de client WAN DHCP cu un server DHCP sau retransmiteţi conexiunea utilizând elementul de meniu **Servicii** pentru Servicii de acces la distanţă din System i Navigator.
  2. Selectaţi să se utilizeze DHCP pentru metoda de alocare a adresei IP în cadrul Proprietăţilor de setări TCP/IP ale profilului de conexiune receptoare în System i Navigator.
- Permiteţi sistemului la distanţă să acceseze alte reţele (înaintare IP) în cadrul Proprietăţilor de setări TCP/IP ale profilului de conexiune receptoare în System i Navigator.
- Activaţi înaintarea datagramelor IP în cadrul Proprietăţilor de setări ale configuraţiei TCP/IP în System i Navigator.

Scenariu: Profil DHCP şi PPP pe modele diferite System i

Acest exemplu explică modul în care se setează două modele System i ca server DHCP al reţelei şi agentul de retransmitere BOOTP/DHCP pentru două LAN-uri şi clienţi dial-in la distanţă.

Exemplul despre PPP şi DHCP pe un singur model System i arată cum se utilizează PPP şi DHCP într-un singur sistem pentru a permite clienţilor de apel de intrare accesul la o reţea. Dacă sunteţi preocupat de dispunerea fizică a reţelei dumneavoastră sau de securitate, ar fi mai bine să aveţi serverele PPP şi DHCP separate sau să aveţi un server PPP dedicat fără servicii DHCP. Următoarea figură prezintă o reţea care are clienţi dial-in cu politicile PPP şi DHCP pe servere diferite.

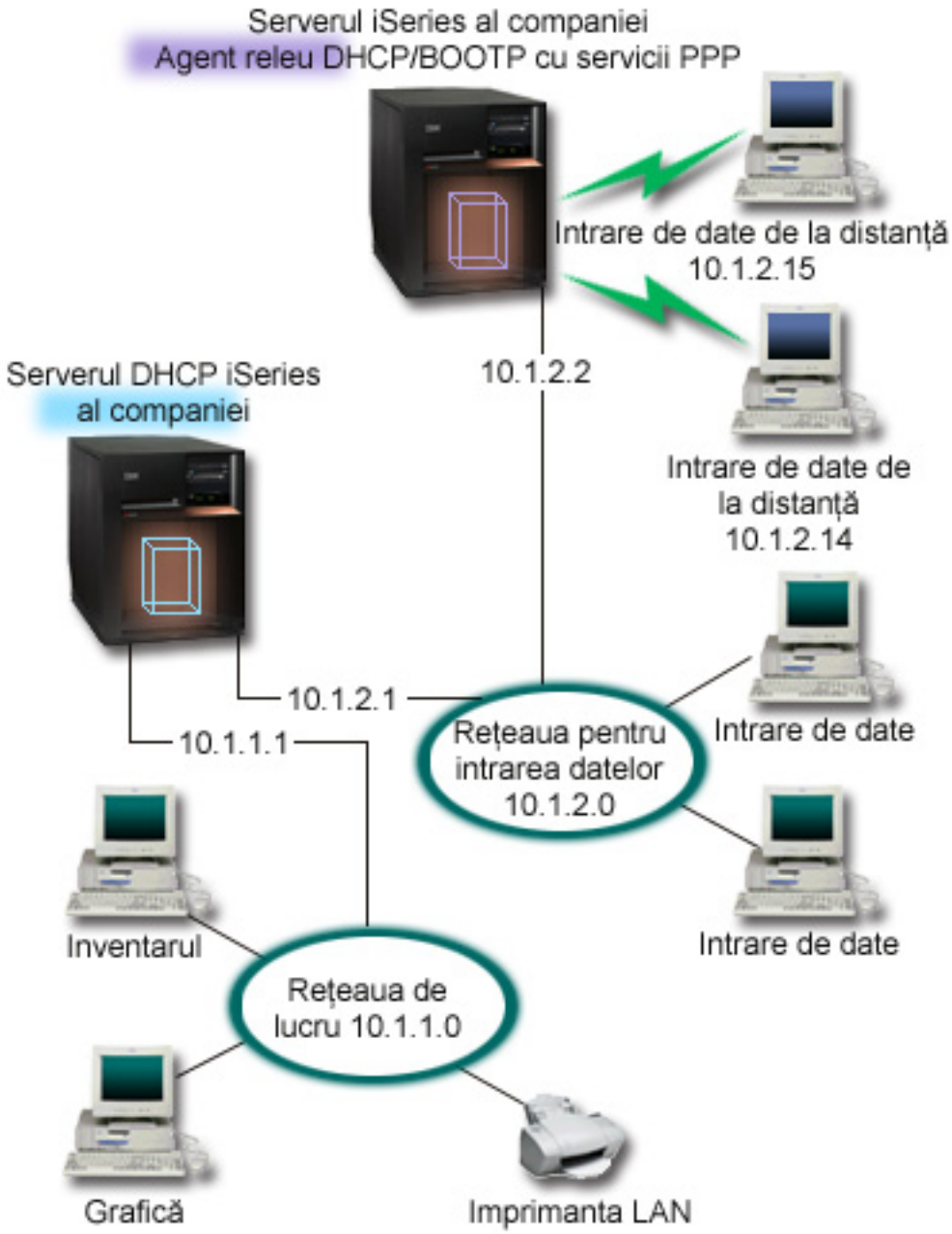


Figura 2. Profilul DHCP şi PPP pe modele diferite System i

Clienţii de introducere date la distanţă apelează telefonic serverul PPP System i. Profilul PPP de pe acel server trebuie să aibă o metodă de adresă IP la distanţă DHCP, precum cea utilizată în exemplul de PPP şi DHCP pe un singur model System i. Profilul PPP şi proprietăţile de stivă TCP/IP de pe serverul PPP trebuie să aibă înaintare IP. Mai mult, deoarece acest server acţionează ca agent de retransmitere DHCP, agentul de retransmitere BOOTP/DHCP trebuie să fie pornit. Aceasta permite serverului de acces la distanţă System i să transmită pachete DHCPDISCOVER la serverul DHCP. Serverul DHCP răspunde apoi şi distribuie informaţii TCP/IP la clienţii de apel de intrare prin serverul PPP.

Serverul DHCP este responsabil pentru distribuirea adreselor IP la amândouă reţelele, 10.1.1.0 şi 10.1.2.0. În reţeaua de introducere date, serverul DHCP dă adrese IP de la 10.1.2.10 la 10.1.2.40 fie clienţilor de apel de intrare sau celor direct ataşaţi reţelei. De asemenea, clienţii de introducere date au nevoie de o adresă de ruter (opţiunea 3) 10.1.2.1 pentru a comunica cu reţeaua de lucru şi serverul DHCP System i trebuie să aibă şi înaintarea IP activată.

De asemenea, adresa IP de interfaţă locală din profilul PPP trebuie să fie o adresă IP care se încadrează în definiţia de subreţea sin serverul DHCP. În acest exemplu, adresa de interfaţă locală profil PPP trebuie să fie 10.1.2.2. Această adresă trebuie, de asemenea, exclusă din poolul de adrese al serverului DHCP, astfel încât să nu fie alocată unui client DHCP. Adresa IP de interfaţă locală trebuie să fie o adresă la care serverul DHCP să poată trimite pachete 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 de nume de domeniu	10.1.1.1
	Opţiunea 15: Nume de domeniu	mycompany.com
Sistemul realizează actualizări DNS?		Nu
Sistemul 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
Adresele de subreţea nu sunt alocate de server		10.1.2.1 (Ruter) 10.1.2.15 (Adr. IP interfaţă locală client DataEntry la distanţă) 10.1.2.14 (Adr. IP interfaţă locală client DataEntry la distanţă)

Alte setări pe o platformă System i pe 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 de client WAN DHCP cu un server DHCP sau retransmiteţi conexiunea utilizând elementul de meniu Servicii pentru Servicii de acces la distanţă din System i Navigator

2. Selectaţi să se utilizeze DHCP pentru metoda de alocare a adresei IP în cadrul Proprietăţilor de setări TCP/IP ale profilului de conexiune receptoare în System i Navigator

- Permiteţi sistemului la distanţă să acceseze alte reţele (înaintare IP) în cadrul Proprietăţilor de setări TCP/IP ale profilului de conexiune receptoare în System i Navigator (pentru a permite clienţilor la distanţă să comunice cu reţeaua de introducere de date)
- Activaţi înaintarea datagramelor IP în cadrul Proprietăţilor de setări ale configuraţiei TCP/IP în System i Navigator (pentru a permite clienţilor 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. Biroul filialei are o adresă IP alocată dinamic, în timp ce biroul companiei are o adresă IP statică, rutabilă global.

Situaţie

Să presupunem că compania dumneavoastră are un mic birou de filială în alt stat. Pe parcursul oricărei zile de lucru, filiala ar putea necesita acces la informaţii confidenţiale despre un model System i din cadrul reţelei dumneavoastră interne de corporaţie. Compania dumneavoastră foloseşte în prezent o linie închiriată scumpă pentru a furniza accesul biroului filială la reţeaua companiei. Deşi compania dumneavoastră doreşte să asigure în continuare un acces sigur la intranet, în ultimă în cele din urmă doriţi să reduceţi costul pe care îl implică linia închiriată. Aceasta se poate realiza prin crearea unui tunel voluntar Layer 2 Tunnel Protocol (L2TP) pentru a vă extinde reţeaua companiei, astfel ca biroul filialei să apară ca o parte a subreţelei companiei. VPN protejează traficul de date prin tunelul L2TP.

Cu un tunel voluntar L2TP, biroul filialei de la distanţă stabileşte un tunel direct la serverul de reţea L2TP (LNS) al reţelei companiei. Funcţionalitatea concentratorului de acces L2TP (LAC) se află la client. Tunelul este transparent pentru furnizorul de servicii Internet (ISP) al clientului de la distanţă, astfel că ISP-ul nu trebuie 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 are intenţia de a simplifica scenariul. Nu vrea să sugereze faptul că folosirea unui firewall nu este necesară. Trebuie să luaţi în considerare riscurile de securitate implicate de fiecare dată când vă conectaţi la Internet.

Obiective

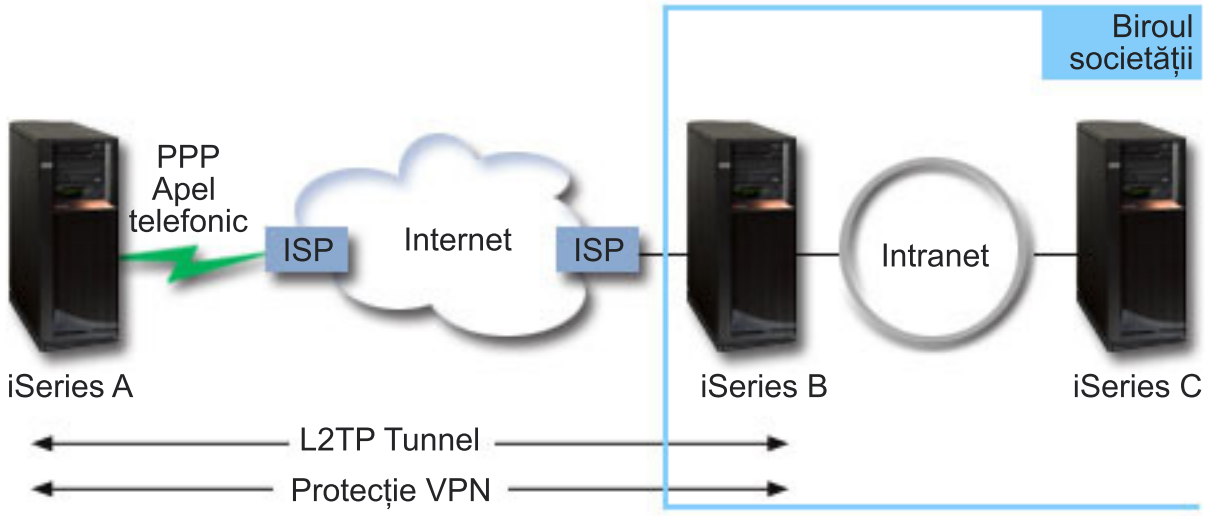
În acest scenariu, un sistem al filialei se conectează la reţeaua companiei printr-un sistem gateway cu un tunel L2TP protejat de VPN.

Obiectivele principale ale acestui scenariu sunt:

- Biroul de filială iniţiază întotdeauna conexiunea la biroul companiei.
- Sistemul biroului de filială este singurul sistem din reţeaua biroului de filială care are nevoie de acces la reţeaua companiei. Cu alte cuvinte, rolul său este acela al unei gazde, nu al unui gateway, în reţeaua biroului de filială.
- Sistemul companiei este un calculator gazdă din reţeaua biroului companiei.

Detalii

Următoarea ilustraţi prezintă caracteristicile reţelei pentru acest scenariu:



Sistem A

- Trebuie să aibă acces la aplicaţiile TCP/IP pe toate sistemele din reţeaua companiei.
- Primeşte adrese IP alocate dinamic de la ISP-ul său.
- Trebuie să fie configurat să furnizeze suport L2TP.

Sistem B

- Trebuie să aibă acces la aplicaţiile TCP/IP pe Sistemul A.
- Subreţeaua este 10.6.0.0 cu masca 255.255.0.0. Această subreţea reprezintă punctul final de 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, Sistemul B realizează gestiune chei şi aplică IPSec datagramelor IP de intrare şi de ieşire. Sistemul B se conectează la subreţeaua sa cu adresa IP 10.6.11.1.

În termeni L2TP, *Sistemul A* acţionează ca iniţiator L2TP, în timp ce *Sistemul B* acţionează ca terminator L2TP.

Taskurile de configurare

Presupunând că deja există şi funcţionează configurarea TCP/IP, trebuie să executaţi următoarele operaţii:

Scenariu: Conectarea sistemului la un concentrator de acces PPPoE

Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

Situaţie

Activitatea dumneavoastră necesită o conexiune Internet mai rapidă, deci sunteţi interesat de un serviciu DSL de la un ISP local. După o investigaţie iniţială, aflaţi că ISP-ul dumneavoastră foloseşte PPPoE pentru a-şi conecta clienţii. Trebuie să utilizaţi această conexiune PPPoE pentru a furniza conexiuni Internet cu lăţime de bandă mare prin sistemul dumneavoastră.

Figura 3. Conectarea sistemului la un ISP cu PPPoE

Soluţie

Puteţi suporta o conexiune PPPoE la ISP-ul dumneavoastră prin sistemul dumneavoastră. Sistemul utilizează un nou tip de linie virtuală PPPoE care este legat la o linie fizică Ethernet configurată să utilizeze un adaptor Ethernet de tipul 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A sau 576A. Această linie virtuală suportă protocoale de sesiune PPP printr-o reţea locală (LAN) Ethernet, care este conectată la un modem DSL care furnizează poarta (gateway) către ISP-ul la distanţă. Acest gateway permite utilizatorilor conectaţi la LAN să aibă acces Internet de viteză înaltă utilizând conexiunea PPPoE. După ce a pornit conexiunea dintre sistem şi ISP, utilizatorii individuali din LAN pot accesa ISP-ul prin PPPoE, utilizând adresa IP alocată sistemului. 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

Pentru a seta un exemplu de configuraţie PPP din System i Navigator, urmaţi aceşti paşi:

1. Configuraţi dispozitivul de conexiune pentru a fi folosit cu ISP-ul dumneavoastră.
2. Configuraţi un profil de conexiune originatoare pe sistemul dumneavoastră.

   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, System i Navigator afişează dialogul **proprietăţi linie**.

   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**. System i Navigator afişează dialogul **proprietăţi linie Ethernet**.

   Notă: PPPoE necesită un adaptor Ethernet de tipul 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A sau 576A.

   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 necesită ca sistemul să se autentifice singur sau dacă doriţi ca sistemul să autentifice sistemul la distanţă, apăsaţi pe **Autentificare** pentru a deschide pagina Autentificare şi pentru a introduce informaţiile cerute.
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 LAN-ului să se conecteze la ISP utilizând adresele IP alocate sistemului, selectaţi **Ascundere adrese (Travestire completă)**.
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.

Concepte înrudite

“Suportul pentru politică de grup” la pagina 4
Cu suportul pentru politică de grup, administratorii de reţea pot defini politici pentru grupuri de utilizatori pentru a gestiona resursele. Utilizatorilor individuali le pot fi alocate politici de control al accesului atunci când se loghează în sesiunea PPP sau L2TP.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

Referinţe înrudite

“Configurarea legăturii” la pagina 49
Configurarea legăturii defineşte tipul de service linie pe care profilul conexiunii dumneavoastră Protocol punct-la-punct (PPP) îl utilizează pentru a stabili o conexiune.

“Autentificarea sistemului” la pagina 43
Conexiunile PPP cu o platformă System i suportă mai multe opţiuni pentru autentificare, atât a clienţilor la distanţă care apelează sistemul, cât şi a conexiunilor la un ISP sau la alt sistem pe care îl apelează sistemul.

“Tratarea adreselor IP” la pagina 40
Conexiunile PPP permit mai multe seturi diferite de opţiuni pentru gestionarea adreselor IP, în funcţie de tipul profilului de conexiune.

“Filtrarea pachetelor IP” la pagina 41
Filtrarea pachetelor IP limitează serviciile pentru utilizatorii individuali atunci când se înregistrează pe o reţea.

Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră

Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

Situaţie

Ca administrator al reţelei companiei dumneavoastră, trebuie să întreţineţi atât sistemul, 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 dumneavoastră nu are o conexiune de reţea legată la Internet, vă puteţi apela sistemul utilizând o conexiune PPP. În plus, singurul modem pe care îl aveţi în prezent este modemul de suport electronic pentru client 7852-400 şi trebuie să utilizaţi acest modem pentru conexiunea dumneavoastră.

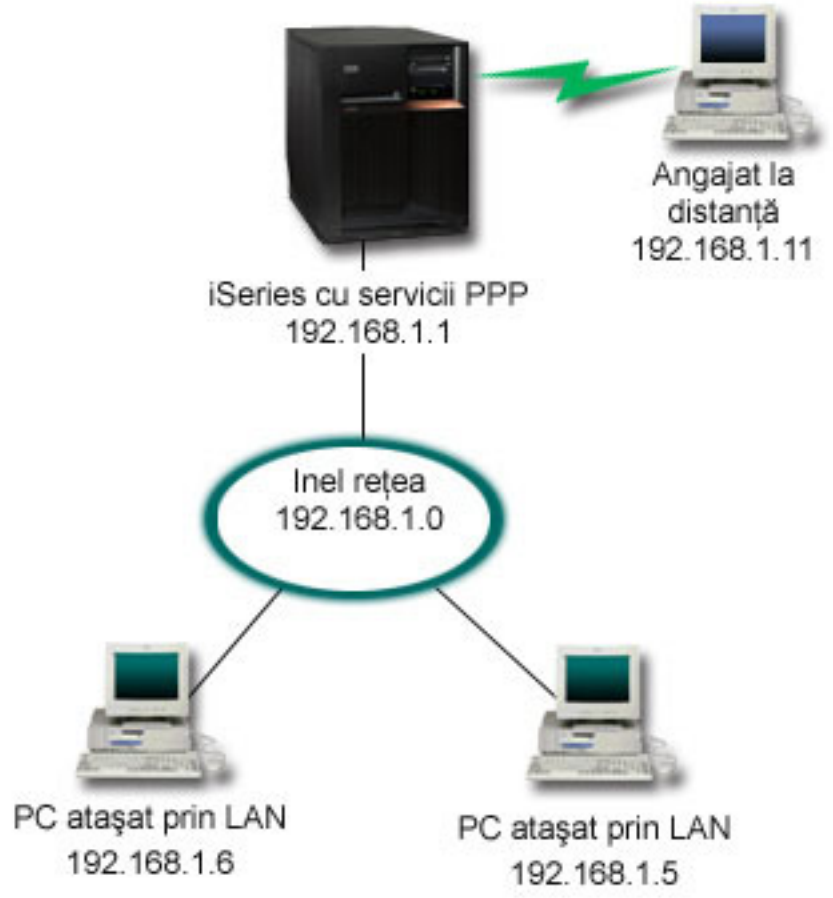


Figura 4. Conectarea clienţilor de la distanţă la sistemul dumneavoastră

Soluţie

Puteţi utiliza PPP pentru a vă conecta PC-ul de bază la sistemul dumneavoastră, utilizându-vă modemul. Deoarece vă utilizaţi modemul de suport electronic client pentru acest tip de conexiune PPP, trebuie să vă asiguraţi că modemul dumneavoastră este configurat atât pentru mod sincron, cât şi asincron. Figura afişează un sistem cu servicii PPP care este conectat la un LAN cu două PC-uri. Lucrătorul de la distanţă apelează apoi sistemul. Sistemul se autentifică şi 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.

Lucrătorul de la distanţă utilizează Protocolul de autentificare dialog de confirmare (CHAP-MD5) pentru a se autentifica cu sistemul. Sistemul nu poate utiliza MS_CHAP, astfel încât trebuie să vă asiguraţi că clientul dumneavoastră PPP utilizează 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.

Figura anterioară are un singur client de apel telefonic de la distanţă, deoarece modemul de suport electronic client poate manipula doar o singură conexiune deodată.

Configuraţie exemplu

Pentru a seta un exemplu de configuraţie PPP din System i Navigator, urmaţi aceşti paşi:

1. Configuraţi Dial-up Networking şi creaţi o conexiune prin linie telefonică pe PC-ul la distanţă.
2. Configuraţi un profil de conexiune receptoare pe sistemul dumneavoastră.

   Aveţi grijă să introduceţi următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Răspuns
   - **Configurare legătură**: Aceasta 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

“Planificarea PPP” la pagina 31
Planificarea Protocolului punct-la-punct (PPP) include crearea şi administrarea conexiunilor PPP.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

Referinţe înrudite

“CHAP (Challenge Handshake Authentication Protocol) cu MD5” la pagina 43
CHAP-MD5 utilizează un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul de autentificare şi de dispozitivul la distanţă.

“Configurarea legăturii” la pagina 49
Configurarea legăturii defineşte tipul de service linie pe care profilul conexiunii dumneavoastră Protocol punct-la-punct (PPP) îl utilizează pentru a stabili o conexiune.

“Pool de linii” la pagina 50
Pentru a seta conexiunea PPP să utilizeze o linie dintr-un pool de linii, selectaţi acest serviciu de linie. Când porneşte conexiunea PPP, sistemul selectează o linie neutilizată din poolul de linii. Pentru profiluri de apel la cerere, sistemul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

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

Administratorii, de obicei, setează reţelele de birou pentru ca angajaţii să poată accesa Internetul. Administratorii pot utiliza un modem pentru a conecta sistemul la un furnizor de servicii Internet (ISP). Clienţii PC-urilor ataşate LAN-ului pot să comunice cu Internetul utilizând sistemul de operare i5/OS ca poartă (gateway).

Situaţie

Aplicaţia corporativă pe care o utilizează compania dumneavoastră necesită ca utilizatorii dumneavoastră să acceseze Internetul. Deoarece aplicaţia nu necesită schimbul de cantităţi mari de date, trebuie să puteţi utiliza un modem pentru a conecta atât sistemul dumneavoastră cât şi clienţii PC-urilor ataşate LAN-ului la Internet. Figura următoare prezintă un exemplu al acestei situaţii.

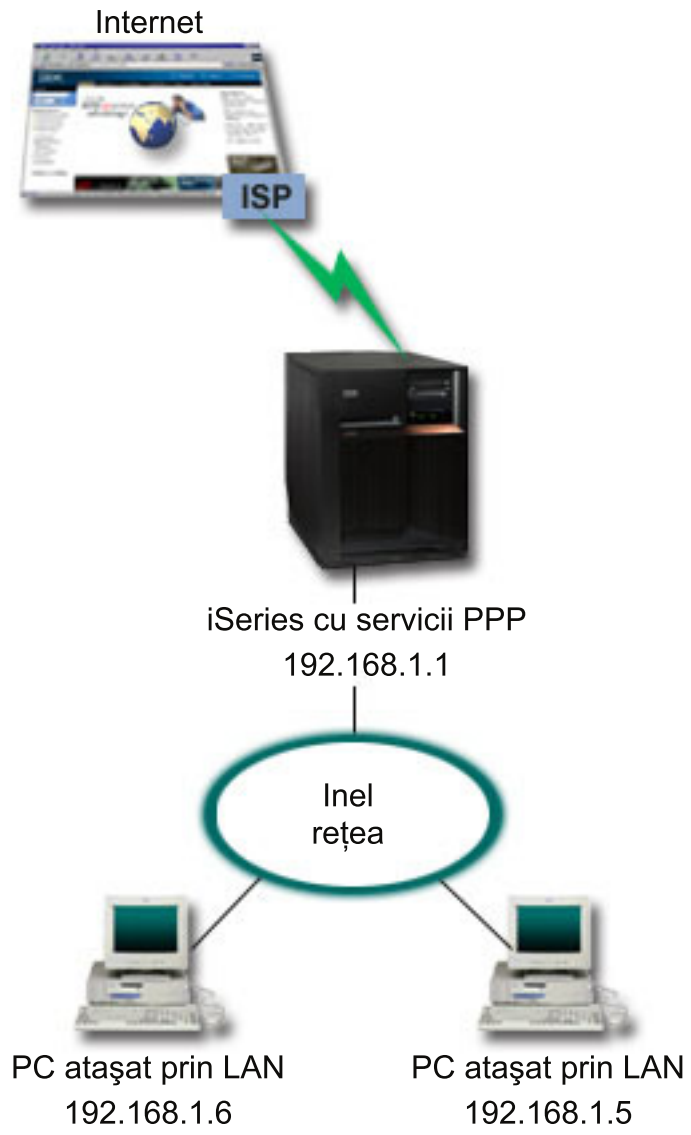


Figura 5. Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem

Soluţie

Vă puteţi utiliza modemul integrat (sau altul compatibil) pentru a vă conecta sistemul la ISP-ul dumneavoastră. Trebuie să creaţi un profil originator Protocol punct-la-punct (PPP) pe sistem pentru a stabili o conexiune PPP la ISP.

După ce faceţi conexiunea dintre sistem şi ISP, PC-urile ataşate la LAN-ul dumneavoastră pot să comunice cu Internetul utilizând sistemul ca poartă (gateway). În profilul originator, trebuie să vă asiguraţi că opţiunea Ascundere adrese este activată, astfel încât clienţii LAN-ului care au adrese IP private să poată să comunice cu Internetul.

Acum, după ce reţeaua şi sistemul sunt legate la Internet, trebuie să înţelegeţi riscurile de securitate cu care vă confruntaţi. Consultaţi furnizorul de servicii Internet pentru a-i înţelege politicile de securitate şi pentru a lua măsurile necesare pentru protejarea reţelei şi sistemului dumneavoastră.

În funcţie de modul de utilizare a Internetului, lărgimea de bandă ar putea deveni o problemă.

Configuraţie exemplu

Pentru a seta un exemplu de configuraţie din System i Navigator, urmaţi aceşti paşi:

1. Configuraţi un profil de conexiune originatoare pe sistemul dumneavoastră.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Apel telefonic
   - **Configurare 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. Apăsaţi pe **DNS** pentru a deschide pagina Sistem nume domeniu (DNS), introduceţi adresa IP a serverului DNS care este furnizată de ISP.
8. Faceţi clic pe **OK** pentru încheierea profilului.

Pentru a utiliza profilul de conexiune pentru a vă conecta la Internet, faceţi clic dreapta pe profilul conexiunii din System i Navigator şi selectaţi **Pornire**. Conexiunea este realizată cu succes când starea se schimbă în **Activ**. Reîmprospătaţi pentru a actualiza ecranul.

Notă: Trebuie să vă asiguraţi şi că celelalte sisteme din reţeaua dumneavoastră au definită rutarea corespunzătoare, astfel încât traficul TCP/IP Internet e la aceste sisteme să fie trimis prin sistem.

Concepte înrudite

"Planificarea PPP" la pagina 31
Planificarea Protocolului punct-la-punct (PPP) include crearea şi administrarea conexiunilor PPP.

Operaţii înrudite

"Crearea unui profil de conexiune" la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

Referinţe înrudite

"Pool de linii" la pagina 50
Pentru a seta conexiunea PPP să utilizeze o linie dintr-un pool de linii, selectaţi acest serviciu de linie. Când porneşte conexiunea PPP, sistemul selectează o linie neutilizată din poolul de linii. Pentru profiluri de apel la cerere, sistemul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

"Configurarea legăturii" la pagina 49
Configurarea legăturii defineşte tipul de service linie pe care profilul conexiunii dumneavoastră Protocol punct-la-punct (PPP) îl utilizează pentru a stabili o conexiune.

Scenariu: Conectarea reţelei dumneavoastră corporative şi la distanţă cu un modem

Un modem permite ca două locaţii la distanţă (precum un birou central şi o filială) să interschimbe date. Protocolul punct-la-punct (PPP) poate conecta împreună două LAN-uri, stabilind o conexiune între un sistem din biroul central şi un altul din filială.

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 reţelelor dumneavoastră corporative şi la distanţă cu un modem

Soluţie

PPP poate conecta împreună două LAN-uri, stabilind o conexiune între sisteme aşa cum se indică în figură. În acest caz, presupuneţi că biroul la distanţă iniţiază conexiunea cu biroul central. Configuraţi un profil originator pe sistemul la distanţă şi un profil receptor pe sistemul biroului central.

Dacă PC-urile biroului la distanţă necesită acces la LAN-ul corporativ (192.168.1.0), profilul receptor al biroului central va necesita ca înaintarea IP să fie pornită şi rutarea adreselor IP să fie activată pentru PC-uri (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

Pentru a seta un exemplu de configuraţie din System i Navigator, urmaţi aceşti paşi:

1. Configuraţi un profil de conexiune originatoare pe sistemul biroului la distanţă.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Apel telefonic
   - **Configurare 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. Apăsaţi pe **Adăugare** şi tastaţi numărul de telefon pentru a ajunge la sistemul biroului central. Asiguraţi-vă că includeţi toate 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 **Cerere parolă criptată (CHAP-MD5)** şi introduceţi informaţiile de parolă şi nume utilizator 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 de conexiune receptoare pe sistemul biroului central.

   Asiguraţi-vă că aţi selectat următoarele informaţii:

   - **Tip protocol**: PPP
   - **Tip conexiune**: Linie comutată
   - **Mod operare**: Răspuns
   - **Configurare 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 adresa IP locală, selectaţi adresa IP a interfeţei biroului central (192.168.1.1) din caseta **selectare**.
    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 permite altor sisteme din reţea să utilizeze acest sistem ca poartă (gateway).
12. Faceţi clic pe **OK** pentru încheierea profilului receptor.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

Referinţe înrudite

“Configurarea legăturii” la pagina 49
Configurarea legăturii defineşte tipul de service linie pe care profilul conexiunii dumneavoastră Protocol punct-la-punct (PPP) îl utilizează pentru a stabili o conexiune.

“Pool de linii” la pagina 50
Pentru a seta conexiunea PPP să utilizeze o linie dintr-un pool de linii, selectaţi acest serviciu de linie. Când porneşte conexiunea PPP, sistemul selectează o linie neutilizată din poolul de linii. Pentru profiluri de apel la cerere, sistemul nu selectează linia până când nu detectează trafic TCP/IP pentru sistemul la distanţă.

Scenariu: Autentificarea conexiunilor dial-up cu RADIUS NAS

Un Server de acces reţea (NAS) rulând pe sistem poate ruta cereri de autentificare de la clienţi de apel de intrare la un alt server Remote Authentication Dial In User Service (RADIUS). Dacă este autentificat, RADIUS poate controla şi adresele IP alocate utilizatorului.

Situaţie

Reţeaua dumneavoastră corporativă are utilizatori la distanţă care fac apeluri telefonice în două sisteme de la o reţea dial-up distribuită. Trebuie să centralizaţi autentificarea, serviciile şi contabilizarea, permiţând unui sistem să manipuleze cereri pentru validarea parolelor şi ID-urilor de utilizator şi pentru determinarea adresei IP care le este alocată.

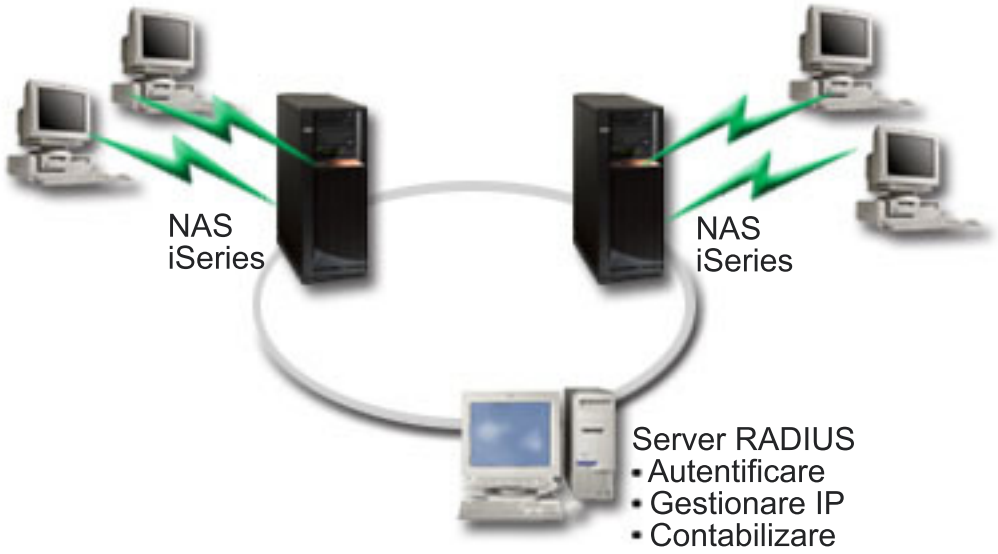


Figura 7. Autentificarea conexiunilor dial-up cu un server RADIUS

Soluţie

Când utilizatorii încearcă să se conecteze, NAS-ul care rulează pe sisteme înaintează informaţiile de autentificare la un server RADIUS de pe 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 a suporta RADIUS, trebuie să definiţi serverul RADIUS NAS pe sistem.

Configuraţie exemplu

Pentru a seta un exemplu de configuraţie din System i Navigator, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi **Reţea**, faceţi clic dreapta pe **Servicii de acces la distanţă** şi selectaţi **Servicii**.
2. În fişa **RADIUS**, selectaţi **Activare conexiune Server acces reţea RADIUS** şi **Activare RADIUS pentru autentificare**. În funcţie de soluţia dumneavoastră RADIUS, puteţi alege şi ca RADIUS să manipuleze 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 care este utilizată pentru conectare la serverul RADIUS.
   b. În caseta **Adresă IP server**, introduceţi adresa IP pentru serverul RADIUS.
   c. În caseta **Parolă**, introduceţi parola care este utilizată pentru a identifica sistemul la serverul RADIUS.
   d. În caseta **Port**, introduceţi portul de pe sistem care este utilizat pentru comunicarea 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 System i Navigator, expandaţi **Reţea → Servicii acces la distanţă**.
8. Selectaţi profilul conexiune care va folosi serverul RADIUS pentru autentificare. Serviciile RADIUS se aplică doar pentru profiluri de conexiune receptoare.

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.

Atunci când utilizatori fac un apel de intrare utilizând acest profil de conexiune, sistemul înaintează informaţiile de autentificare la serverul RADIUS specificat. Dacă utilizatorul este validat, conexiunea este permisă şi utilizează orice restricţie de conexiune specificată în informaţiile utilizatorului despre serverul RADIUS.

Operaţii înrudite

"Activarea serviciilor RADIUS şi DHCP pentru profiluri de conexiune" la pagina 60
Iată paşii pentru activarea serviciilor RADIUS sau DHCP pentru profiluri de conexiune receptoare PPP.

Referinţe înrudite

"Autentificarea sistemului" la pagina 43
Conexiunile PPP cu o platformă System i suportă mai multe opţiuni pentru autentificare, atât a clienţilor la distanţă care apelează sistemul, cât şi a conexiunilor la un ISP sau la alt sistem pe care îl apelează sistemul.

"Privire generală asupra RADIUS" la pagina 44
Remote Authentication Dial In User Service (RADIUS) este un protocol standard de Internet care furnizează autentificare centralizată, contabilizare şi servicii de gestiune a IP-urilor pentru utilizatorii de acces la distanţă într-o reţea dial-up distribuită.

Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP

Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

Situaţie

Reţeaua dumneavoastră are mai multe grupuri de utilizatori distribuiţi şi fiecare are nevoie de acces la alte resurse din LAN-ul dumneavoastră corporativ. Un grup de utilizatori de introducere date necesită acces la baza de date şi la mai multe alte aplicaţii. Unele persoane din alte companii au nevoie de acces dial-up la servicii HTTP, FTP şi, dar din motive de securitate, acestui grup nu trebuie să i se permită accesul la alt trafic sau la alte servicii TCP/IP. Definirea permisiunilor şi atributelor de conexiune detaliate pentru fiecare utilizator vă dublează eforturile, iar furnizarea de restricţii de reţea pentru toţi utilizatorii acestui profil de conexiune nu asigură suficient control. Doriţi o modalitate de a defini permisiuni şi setări de conexiune pentru mai multe grupuri diferite de utilizatori care apelează sistemul în mod curent.

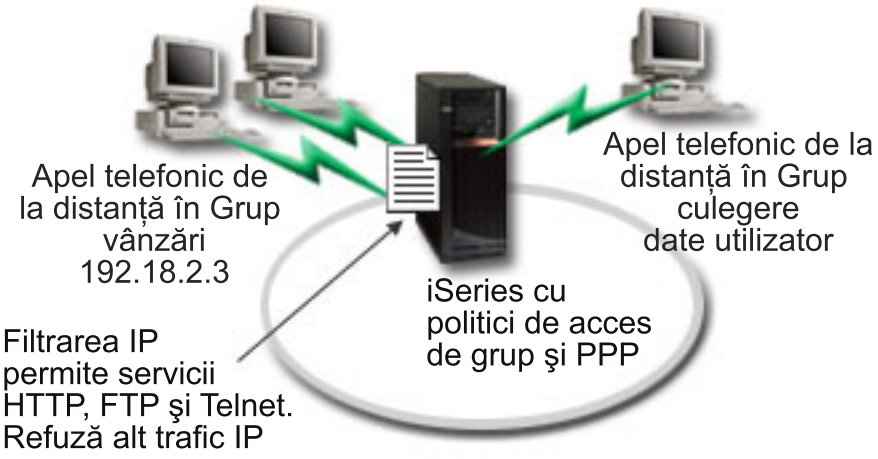


Figura 8. Aplicarea setărilor conexiunii pentru conexiuni dial-up pe baza setărilor de politici de grup

Soluţie

Trebuie să aplicaţi restricţii de filtrare IP unice asupra a două grupuri diferite de utilizatori. Pentru a realiza aceasta, creaţi politici de acces de grup şi reguli de filtrare IP. Politicile de acces de grup fac referire la reguli de filtru IP, astfel încât trebuie să vă creaţi mai întâi regulile de filtrare. În acest exemplu, trebuie să creaţi un filtru PPP pentru a include regulile de filtrare IP pentru Politica de acces de grup partener de afaceri IBM. Aceste reguli de filtrare permit HTTP, FTP şi servicii Telnet, dar restricţionează accesul la toate celelalte servicii şi trafic TCP/IP prin sistem. Acest scenariu arată doar regulile de filtrare necesare pentru grupul de vânzări, puteţi seta filtre similare pentru grupul Introducere date.

În final, trebuie să creaţi politicile de acces de grup (câte una pentru fiecare grup) pentru a defini grupul dumneavoastră. O politică de acces de grup vă permite să definiţi atribute de conexiune comune unui grup de utilizatori. Adăugând o politică de acces de grup la o listă de validare de pe sistem, puteţi aplica aceste setări de conexiune în timpul procesului de autentificare. Politica de acces de grup specifică mai multe setări pentru sesiunea utilizatorului, inclusiv abilitatea de a aplica reguli de filtrare IP care restricţionează adresele IP şi serviciile TCP/IP disponibile unui utilizator în timpul sesiunii.

Configuraţie exemplu

Pentru a seta un exemplu de configuraţie din System i Navigator, urmaţi aceşti paşi:

1. Creaţi identificatorul filtru Protocol punct-la-punct (PPP) şi filtrele de reguli pachet IP care specifică permisiunile şi restricţiile pentru această politică de acces de grup.
   a. În System i Navigator, 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 **Politici acces grup** şi selectaţi **Politică acces grup nouă**. Completaţi 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 **Folosire 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. Utilizaţi fişa **General** pentru a defini seturile filtru şi fişa **Servicii** pentru a defini serviciile pe care le permiteţi, precum 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**, selectaţi 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 modificăei mai târziu, utilizaţi interfaţa pe bază de caractere pentru a introduce comanda RMVTCPTBL *ALL. Această comandă înlătură toate regulile filtru şi NAT de pe sistem.

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

2. Definiţi o nouă politică de acces de grup pentru acest grup de utilizatori.
   a. În System i Navigator, expandaţi **Reţea → Servicii de acces la distanţă → Profiluri de conexiune receptoare**.

b. Faceţi clic dreapta pe pictograma **Politică acces grup** şi selectaţi **Politică acces grup nouă**. System i Navigator afişează dialogul **Definiţie Politică acces grup nouă**.
c. În pagina General, introduceţi un nume şi o descriere pentru politica de acces de grup.
d. Pe pagina Setări TCP/IP:
   - Selectaţi **Folosire reguli pachet IP pentru această conexiune** şi selectaţi identificatorul de filtru PPP **permitted_services**.
e. Selectaţi **OK** pentru a salva politica de acces de grup.

3. Aplicaţi politica de acces de grup utilizatorilor asociaţi cu acest grup.
   a. Deschideţi profilul de conexiune receptoare care controlează aceste conexiuni dial-up.
   b. În pagina Autentificare a profilului de conexiune receptoare, selectaţi lista de validare care conţine informaţiile de autentificare ale utilizatorilor şi apăsaţi pe **Deschidere**.
   c. Selectaţi un utilizator din grupul Vânzări căruia doriţi să-i aplicaţi politica de acces de grup şi apăsaţi pe **Deschidere**.
   d. Apăsaţi pe **Aplicare politică grup utilizatorului** şi selectaţi politica de acces de grup definită în pasul 2.
   e. Repetaţi pentru fiecare utilizator Vânzări.

Concepte înrudite

“Configurarea unei politici de acces de grup” la pagina 58
Folderul **Politici de acces de 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.

“Suportul pentru politică de grup” la pagina 4
Cu suportul pentru politică de grup, administratorii de reţea pot defini politici pentru grupuri de utilizatori pentru a gestiona resursele. Utilizatorilor individuali le pot fi alocate politici de control al accesului atunci când se loghează în sesiunea PPP sau L2TP.

Operaţii înrudite

“Crearea unui profil de conexiune” la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

“Aplicarea regulilor de filtrare a pachetelor IP la o conexiune PPP” la pagina 59
Puteţi utiliza un fişier de reguli pachet pentru a restricţiona accesul unui utilizator sau al unui grup la adresele IP de pe reţeaua dumneavoastră.

Referinţe înrudite

“Lista de validare” la pagina 45
O listă de validare este folosită pentru a păstra informaţiile ID utilizator şi parolă despre utilizatorii la distanţă.

“Autentificarea sistemului” la pagina 43
Conexiunile PPP cu o platformă System i suportă mai multe opţiuni pentru autentificare, atât a clienţilor la distanţă care apelează sistemul, cât şi a conexiunilor la un ISP sau la alt sistem pe care îl apelează sistemul.

Informaţii înrudite

Filtrarea IP şi translatarea adreselor de reţea

Scenariu: Partajarea unui modem între partiţii logice utilizând L2TP

Aveţi Ethernet virtual setat pe patru partiţii logice. Doriţi ca partiţiile logice selectate să partajeze un modem pentru a accesa un LAN extern.

Situaţie

Sunteţi administratorul de sistem la o companie mijlocie. E momentul să vă actualizaţi echipamentul calculatorului, dar vreţi să faceţi mai mult de atât; vreţi să vă fluidizaţi hardware-ul. Începeţi procesul consolidând lucrul a trei sisteme vechi pe un sistem nou. Creaţi trei partiţii logice pe sistem. Sistemul nou vine cu un modem intern 2793. Acesta este

singurul procesor intrare/ieşire (IOP) pe care îl aveţi care suportă Protocolul punct-la-punct (PPP). Aveţi şi un modem vechi de suport electronic client 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 dacă utilizaţi tunele L2TP şi configuraţi 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 este conectată la alt sistem care împarte modemurile în reţeaua dumneavoastră.

Detalii

Următoarea figură ilustrează caracteristicile reţelei pentru acest scenariu:

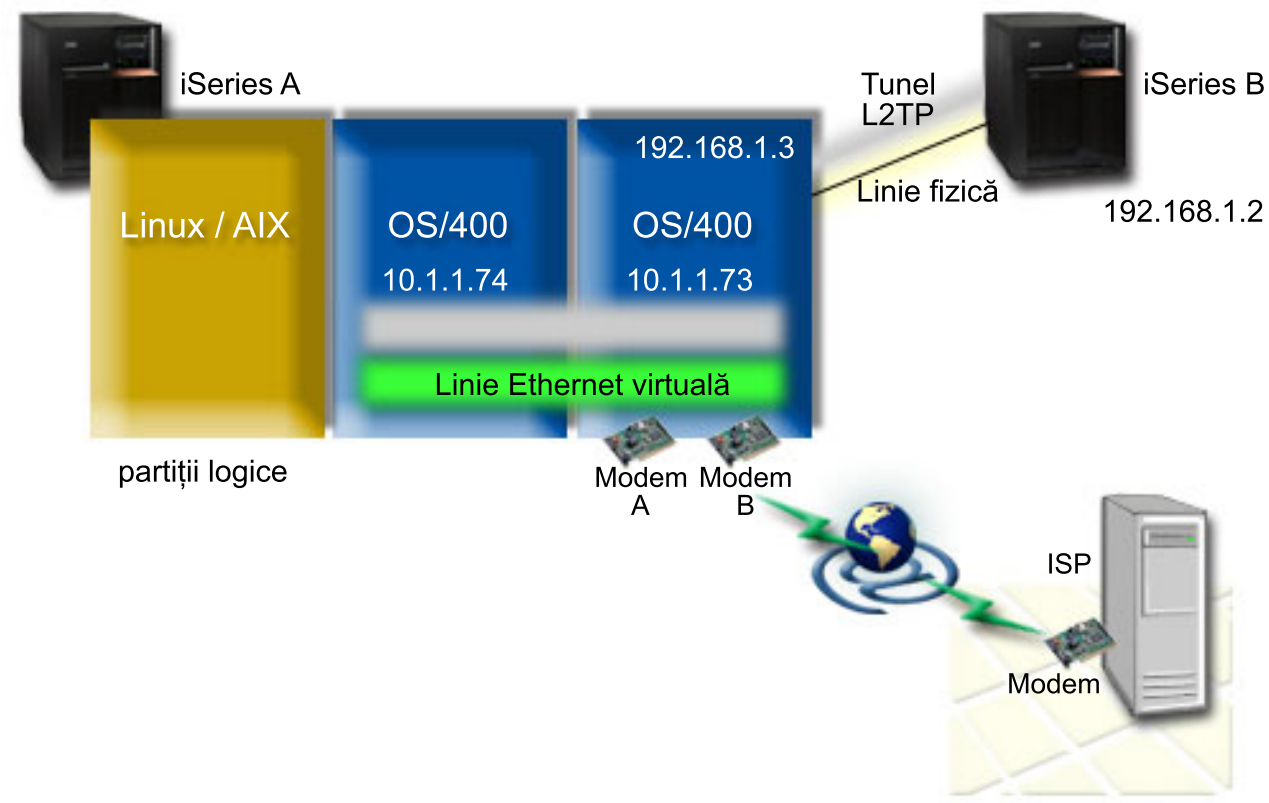


Figura 9. Mai multe sisteme care partajează acelaşi modem pentru conexiunile apel telefonic

Cerinţe preliminare şi presupuneri

Sistemul A trebuie să îndeplinească următoarele cerinţe de setare:

- i5/OS Versiunea 5 Ediţia 3 sau ulterioară, instalată pe partiţia care deţine modemurile capabile ASYNC
- Hardware care să vă permită partiţionarea.
- System i Access pentru Windows şi System i Navigator (componenta Configuraţie şi service a System i Navigator), Versiunea 5 Ediţia 3 sau ulterioară
- Aţi creat cel puţin două partiţii logice (LPAR) pe sistem. Partiţia care deţine modemul trebuie să aibă instalat i5/OS V5R3 sau ulterioară. Celelalte partiţii pot avea instalat OS/400 V5R2, i5/OS V5R3, Linux sau AIX. În acest scenariu, partiţiile fie utilizează sistemul de operare i5/OS sau Linux.

- Aveţi creat Ethernet virtual pentru a comunica între partiţii.

Sistemul B trebuie să aibă instalate programul cu licenţă şi componentele relevante ale System i Navigator: System i Access pentru Windows şi System i Navigator (componenta Configuraţie şi service a System i Navigator) V5R2 sau ulterioară.

Informaţii înrudite

Partiţiile logice

Detalii scenariu: Partajare unui modem între partiţii logice utilizând L2TP

După ce finalizaţi cerinţele preliminare, sunteţi gata să începeţi configurarea profilurilor Protocol de tunelare nivelul doi (L2TP).

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

Pentru a crea un profil terminator pentru orice interfaţă, urmaţi aceşti paşi:

1. În System i Navigator, expandaţi ***sistemul dumneavoastră*** → **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 nicio interfaţă fizică asociată. Linia virtuală descrie caracteristici diverse ale acestui profil PPP. După ce se deschide fereastra Proprietăţi linie L2TP, apăsaţi pe fişa **Autentificare** şi introduceţi numele gazdă al sistemului dumneavoastră. Apăsaţi pe **OK** pentru a vă întoarce la fişa **Conexiune** din fereastra Proprietăţi profil PPP 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. Se deschide fereastra 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 de suport electronic client 7852–400. Se deschide fereastra 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 poolul de linii (modem extern suport electronic client 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 ar putea fi ceva de genul Furnizorului dumneavoastră de servicii Internet (ISP) care va fi apelat frecvent de celelalte sisteme care utilizează 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 celellte sisteme specifică un număr de telefon real, se va folosi numărul de telefon.
17. În fişa **Setări TCP/IP**, selectaţi următoarele valori:
    - **Adresă IP locală**: Fără
    - **Adresă IP de la distanţă**: Fără

    Notă: Dacă doriţi să utilizaţi profilul pentru a termina sesiuni L2TP, trebuie să alegeţi adresa IP locală care reprezintă sistemul. Pentru adresa IP la distanţă, puteţi selecta un pool de adrese care este în aceeaşi subreţea cu sistemul dumneavoastră. Toate sesiunile L2TP îşi obţin adresele IP de la acest pool.
18. În fişa **Autentificare**, acceptaţi toate valorile implicite.

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

Referinţe înrudite

"Suport pentru profil conexiuni multiple" la pagina 52
Profilurile de conexiune punct-la-punct care suportă conexiuni multiple vă permit să aveţi un profil de conexiune care manipulează mai multe apeluri digitale, analoage sau L2TP.

Pasul 2: Configurarea unui profil originator L2TP pe 10.1.1.74:

Aceşti paşi vă ghidează să creaţi un profil originator Protocol de tunelare nivelul doi (L2TP):

1. În System i Navigator, 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 ar trebui să se potrivească oricărui protocol pe care îl utilizează sistemul la care apelaţi.
12. Introduceţi numele utilizatorului şi parola.

    Notă: Parola şi numele de utilizator trebuie să se potrivească indiferent care sunt parola şi numele de utilizator valide pe sistemul la care 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 la distanţă L2TP pentru 192.168.1.2:

Puteţi configura un profil de apel la distanţă Protocol de tunelare nivelul doi (L2TP) pentru 192.168.1.2, repetând Pasul 2 şi modificând punctul final al tunelului la distanţă la 192.168.1.3 (interfaţa fizică la care se conectează Sistemul B).

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

Pasul 4: Testarea conexiunii:

După ce terminaţi de configurat ambele sisteme, ar trebui să testaţi conectivitatea pentru a vă asigura că sistemele împart modemul pentru a ajunge la reţele externe.

1. Asiguraţi-vă că profilul terminator Protocol de tunelare nivelul doi (L2TP) este activ.
   a. În System i Navigator, expandaţi **10.1.1.73 → Reţea → Servicii acces la distanţă → Profiluri de conexiune receptoare**.
   b. În panoul din dreapta, găsiţi profilul cerut (toExternal) şi verificaţi să fie Active câmpul **Stare**. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.
2. Porniţi profilul de apel de la distanţă pe 10.1.1.74.
   a. În System i Navigator, expandaţi **10.1.1.74 → Reţea → Servicii acces la distanţă → Profiluri de conexiune originatoare**.
   b. În panoul din dreapta, găsiţi profilul cerut (toModem) şi verificaţi să fie Active câmpul **Stare**. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.
3. Porniţi profilul de apel la distanţă pe Sistemul B.
   a. În System i Navigator, expandaţi **192.168.1.2 → Reţea → Servicii acces la distanţă → Profiluri de conexiune originatoare**.

b. În panoul din dreapta, găsiţi profilul pe care l-aţi creat şi verificaţi câmpul **Stare** să fie Active. Dacă nu este, faceţi clic-dreapta şi selectaţi **Pornire**.

4. Dacă e posibil, efectuaţi ping către Furnizorul de servicii Internet (ISP) sau altă destinaţie pe care aţi apelat-o să verificaţi că ambele profiluri sunt active. Veţi încerca ping de la ambele 10.1.1.74 şi 192.168.1.2.
5. Ca alternativă, puteţi verifica şi starea conexiunii.
   a. În System i Navigator, expandaţi **sistemul → Reţea → Servicii acces la distanţă → Profiluri de conexiune originatoare**.
   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.

Planificarea PPP

Planificarea Protocolului punct-la-punct (PPP) include crearea şi administrarea conexiunilor PPP.

Referinţe înrudite

"Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră" la pagina 13
Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

"Scenariu: Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem" la pagina 15
Administratorii, de obicei, setează reţelele de birou pentru ca angajaţii să poată accesa Internetul. Administratorii pot utiliza un modem pentru a conecta sistemul la un furnizor de servicii Internet (ISP). Clienţii PC-urilor ataşate LAN-ului pot să comunice cu Internetul utilizând sistemul de operare i5/OS ca poartă (gateway).

"Informaţii înrudite pentru Serviciile de acces la distanţă" la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Cerinţe de software şi hardware

Pentru un mediu PPP este necesar să aveţi două sau mai multe calculatoare care suportă PPP. Unul dintre aceste calculatoare, platforma System i, poate fi originatorul sau receptorul.

Sistemul trebuie să îndeplinească următoarele cerinţe preliminare, astfel încât sistemele la distanţă să-l poată accesa.

- System i Navigator cu suport TCP/IP.
- Unul din cele două profiluri de conexiune:
  - Un profil de conexiune originatoare pentru a manipula conexiunile PPP de ieşire.
  - Un profil de conexiune receptoare pentru a manipula conexiunile PPP de intrare.
- O consolă de staţie de lucru PC instalată cu System i Access pentru Windows 95 sau ulterior cu System i Navigator.
- Un adaptor instalat.

  Puteţi alege unul din următoarele adaptoare:
  - 2699*: Adaptor intrare/ieşire (IOA) WAN cu două linii.
  - 2720*: PCI WAN/Twinaxial IOA.
  - 2721*: PCI WAN IOA cu două linii.
  - 2745*: PCI WAN IOA cu două linii (înlocuieşte IOA 2721).
  - 2742*: IOA cu 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: Modem integrat V.90 cu două porturi WAN IOA.
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: Adaptor Ethernet pentru conexiuni PPPoE.

– 2793/576C: WAN IOA cu două porturi, cu un modem integrat V.92 pe portul 1 şi o interfaţă de comunicaţii standard pe portul 2. Pentru a utiliza portul 2, este nevoie de un modem extern sau adaptor terminal ISDN cu cablul corespunzător.
– 2805: IOA cu patru porturi WAN, cu un modem analog V.92 integrat. Acesta înlocuieşte modelele 2761 şi 2772.

* Aceste adaptoare necesită un modem extern V.90 (sau mai sus), sau adaptor terminal Reţea digitală servicii integrate (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 unitate de servicii canal (CSU)/unitate de servicii date (DSU).
  – adaptor terminal reţea digitală servicii integrate (ISDN).
- 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

"Profilurile de conexiune" la pagina 2
Profilurile de conexiune punct-la-punct definesc un set de parametri şi resurse pentru conexiuni Protocol punct-la-punct (PPP) specifice. Puteţi porni profiluri care utilizează aceste setări de parametri pentru apeluri telefonice de ieşire (iniţiatoare) sau pentru a asculta (recepta) conexiuni PPP.

"Modemuri" la pagina 38
Pot fi utilizate atât modemuri interne cât şi externe pentru conexiuni Protocol punct-la-punct (PPP).

"CSU/DSU" la pagina 38
O unitate de service canal (CSU) este un dispozitiv care conectează un terminal la o linie digitală. O unitate de service date (DSU) este un dispozitiv care realizează funcţii de diagnoză şi protecţie pentru o linie de telecomunicaţii. În mod obişnuit, cele două dispozitive formează o singură unitate, CSU/DSU.

"Adaptoare terminale ISDN" la pagina 39
Reţeaua digitală de servicii integrate (ISDN) vă furnizează o conexiune digitală care vă permite să comunicaţi utilizând orice combinaţie de voce, date şi video, printre alte aplicaţii multimedia.

Alternative de conexiune

Protocolul punct-la-punct (PPP) poate transmite datagrame peste legături seriale punct-la-punct.

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.

PPP suportă un interval larg de tipuri de legături, dar SLIP (Serial Line Internet Protocol) suportă doar tipuri de linie asincrone. 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 utilizează facilităţile de reţea vocală existente ale companiei telefonice între beneficiar şi biroul 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 modem-uri de astăzi 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 ar putea chiar să crească atunci când se aplică V.42bis. X2 sau 56Flex extinde rata de bps la 56 kbps pentru linii telefonice analoage. 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, cei 56kbps se aplică numai când mutaţi date de la capătul digital la cel analog al legăturii. Această tehnologie este potrivită pentru conexiuni cu ISP dacă capătul digital al legăturii şi hardware-ul se află la locaţia lor. În mod tipic, vă puteţi conecta la un modem analog V.24 peste 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. Vizualizând reţeaua telefonică publică comutată ca o reţea digitală, tehnologia V.90 poate accelera datele de la Internet la 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 de date este o metodă asimetrică, astfel încât transmisiile ″upstream″ (în principal comenzi de mouse şi de tastare de la un calculator la situl central, care necesită mai puţină lăţime de bandă) continuă să curgă 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 ratele V.90 de viteză înaltă.

Standardul V.92 îmbunătăţeşte V.90, permiţând rate ″upstream″ de până la 48 kbps. În plus, duratele conexiunii pot fi reduse datorită îmbunătăţirilor din procesul de stabilire a legăturii şi modem-urile care suportă o caracteristică de reţinere pot rămâne acum conectate în timp ce linia telefonică acceptă un apel de intrare sau utilizează apel în aşteptare.

Serviciul digital şi DDS

Puteţi utiliza serviciul digital şi DDS (Digital Data Services) cu PPP (Point-to-Point Protocol).

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 conexiune permanente, închiriate, care rulează la rate fixe de până la 56 kbps. Acest serviciu mai este numit în mod frecvent DS0.

Puteţi conecta DDS-ul utilizând o casetă specială numită *unitate service canal/unitate service date (CSU/DSU)*, care înlocuieşte modemul într-un scenariu analog. DDS are limitări fizice care sunt înrudite în principal cu distanţa dintre CSU/DSU şi biroul central al companiei de servicii telefonice. DDS funcţionează cel mai bine când distanţa este mai mică de 9000 m (30000 picioare). Companiile telefonice pot acomoda distanţe mai lungi cu extendere de semnal, dar acest serviciu vine la un preţ mai mare. DDS este cel mai potrivit pentru conectarea a două locaţii care sunt servite de acelaşi birou central. Pentru conexiuni la distanţă lungă care se întind pe mai multe birouri centrale, cheltuielile de deplasare care se adună pot face cu uşurinţă DDS-ul nepractic. În asemenea cazuri, Switched-56 ar putea fi o soluţie mai bună. În mod tipic, vă puteţi conecta la un DDS CSU/DSU peste V.35, RS449, sau interfaţa serială X.21 cu protocol sincron la rate de până la 56 kbps.

Referinţe înrudite

“CSU/DSU” la pagina 38
O unitate de service canal (CSU) este un dispozitiv care conectează un terminal la o linie digitală. O unitate de service date (DSU) este un dispozitiv care realizează funcţii de diagnoză şi protecţie 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 asemănătoare setării Servicii date digitale (DDS) prin aceea că echipamentul terminalului de date (DTE) se conectează la serviciile digitale prin intermediul unităţii service canal/unitate service date (CSU/DSU). Totuşi, un CSU/DSU SW56 include un dispozitiv de la care se introduce numărul de telefon al gazdei la distanţă. Puteţi utiliza SW56 pentru a face conexiuni digitale dial-up la orice alt abonat SW56 de oriunde din regiune sau dincolo de graniţele internaţionale.

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 tipic, vă puteţi conecta la un SW56 CSU/DSU prin V.35 sau interfaţa serială RS 449 cu protocol sincron la rate de până la 56 kbps. Cu o unitate de apelare/răspuns V.25bis, controlul datelor şi al apelului se face printr-o singură interfaţă serială.

Referinţe înrudite

"Serviciul digital şi DDS" la pagina 33
Puteţi utiliza serviciul digital şi DDS (Digital Data Services) cu PPP (Point-to-Point Protocol).

"ISDN (Integrated Services Digital Network)"
Reţeaua digitală de servicii integrate (ISDN) furnizează conectivitate digitală cap-la-cap comutată. ISDN poate purta atât voce cât şi date pe aceeaşi conexiune.

ISDN (Integrated Services Digital Network)

Reţeaua digitală de servicii integrate (ISDN) furnizează conectivitate digitală cap-la-cap comutată. ISDN poate purta atât voce cât şi date pe aceeaşi conexiune.

Există mai multe tipuri de servicii ISDN, dintre care BRI (Basic Rate Interface) este cel mai folosit. BRI constă în două canale B de 64 kbps pentru a purta datele beneficiarului şi un canal D pentru a purta datele de semnalizare. Cele două canale B pot fi legate împreună pentru a oferi o rată combinată de 128 kbps. În unele zone, compania telefonică ar putea limita fiecare canal B fie la 56 kbps sau 112 kbps combinat. 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.

Industria tinde în prezent spre protocol PPP sincron cu legături multiple PPP pentru legarea celor două canale B. Unii fabricanţi de adaptoare terminale integrează capacitatea V.34 (modem analogic) în adaptoarele lor terminale. Această capabilitate permite beneficiarilor de o singură linie ISDN să manipuleze fie apeluri analoage convenţionale sau ISDN, profitând de avantajul capabilităţilor de voce/date simultane ale serviciilor ISDN. Cu această tehnologie, un adaptor terminal poate opera şi ca parte de sistem digital pentru clienţii V.92.

În mod obişnuit, trebui să vă conectaţi la un adaptor terminal ISDN peste o interfaţă serială RS-232 utilizând protocolul asincron la rate de până la 230,4 kbps. Totuşi, rata baud maximă a sistemului pentru protocol asincron peste RS-232 este de 115,2 kbps. Din păcate, aceasta restricţionează rata de transfer maximă octeţi la 11,5 kbps, în timp ce adaptorul terminal cu legături multiple este capabil de 14 sau 16 KB necomprimat. Unele adaptoare terminale suportă protocol sincron peste RS-232 la 128 kbps, dar rata baud maximă a sistemului pentru protocol sincron peste RS-232 este de 64 kbps.

Sistemul este capabil să ruleze protocolul asincron peste V.35 la rate de până la 230,4 kbps, dar producătorii de adaptoare terminale în general nu oferă o asemenea configuraţie. Convertoarele de interfaţă care convertesc o interfaţă RS-232 la o interfaţă V.35 ar putea fi o soluţie rezonabilă pentru problemă, dar această abordare nu a fost evaluată pentru sistem. O altă posibilitate ar fi să utilizaţi adaptoarele terminale cu protocolul sincron al interfeţei V.35 la o rată de 128 kbps. Deşi această clasă de adaptoare terminale există, nu par să fie mulţi cei care oferă PPP de legătură multiplă sincronă.

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
Reţeaua digitală de servicii integrate (ISDN) vă furnizează o conexiune digitală care vă permite să comunicaţi utilizând orice combinaţie de voce, date şi video, printre alte aplicaţii multimedia.

Conexiuni T1/E1 şi T1 fracţional

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

T1/E1

O conexiune T1 cuprinde într-un bundle 24 de canale multiplexate divizie de timp (TDM) de 64 kbps (DS0) printr-un circuit de cupru cu 4 fire. Aceasta creează o lăţime de bandă totală de 1.544 mbps. Un circuit E1 în Europa şi alte părţi ale lumii cuprinde într-un bundle 32 de canale de 64-kbps pentru 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 schimburi de ramuri private (PBX-uri) digitale profită de serviciul T1 pentru a importa mai multe circuite de apeluri printr-o linie T1 în loc să aibă 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 veni printr-un subset al celor 24 de canale ale unei legături T1, de exemplu, lăsând canalele rămase pentru conectivitate 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, poate fi utilizat un dispozitiv mai simplu unitate service canal/unitate service date (CSU/DSU). În mod tipic, vă puteţi conecta la un CSU/DSU T1/E1 sau multiplexor printr-o interfaţă serială RS 449 sau V.35 cu protocol sincron la rate multiplu de 64 kbps până la 1.544 mbps sau 2.048 mbps. Multiplexorul sau CSU/DSU oferă temporizarea în reţea.

T1 fracţional

Cu T1 fracţional (FT1), un client poate închiria orice submultiplu de 64-kbps dintr-o linie T1. FT1 este util oricând costul unui T1 dedicat este prohibitiv pentru lăţimea de bandă reală pe care o utilizează un client. 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 populară printre furnizorii de servicii Internet (ISP) care utilizează un singur trunchi T1 de la locaţia lor către switch-ul digital al unei companii telefonice. În aceste cazuri, clienţi multipli pot fi serviţi cu serviciul FT1. În mod tipic, vă puteţi conecta la un CSU/DSU T1/E1 sau multiplexor printr-o interfaţă serială RS 449 sau V.35 cu protocol sincron la un multiplu de 64 kbps. Cu FT1, vi se prealocă 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 S.U.A suportă rate de transfer de date la 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 furnizează acum service Frame relay pentru clienţii care doresc conexiuni la viteze de la 56kbps la T1. (În Europa, vitezele Frame relay variează între 64 kbps şi 2 mbps. În S.U.A., Frame relay e destul de popular deoarece este oarecum necostisitor. Totuşi, acesta este înlocuit în unele zone de tehnologii mai rapide, cum este ATM (asynchronous transfer mode).

Suport L2TP pentru conexiuni PPP

Protocolul de tunelare nivel 2 (L2TP) este un protocol de tunelare care extinde Protocolul punct-la-punct (PPP) pentru a suporta un nivel de legătură între un client care cere L2TP (Concentrator acces L2TP sau LAC) şi un punct final server L2TP destinaţie (Server reţea L2TP sau LNS).

Protocol de tunelare nivelul doi

Utilizând tunele Protocol de tunelare nivelul doi (L2TP), este posibil să se separe locaţia la care se opreşte protocolul dial-up şi cea unde se furnizează accesul la reţea. Acest lucru face ca L2TP să mai fie numit şi *Virtual PPP*.

Aceste figuri ilustrează trei implementări diferite de tunel ale L2TP.

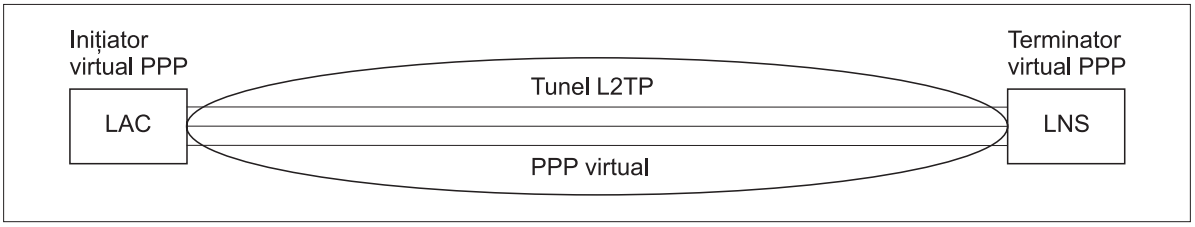


Figura 10. Iniţiator virtual PPP sau terminator virtual PPP

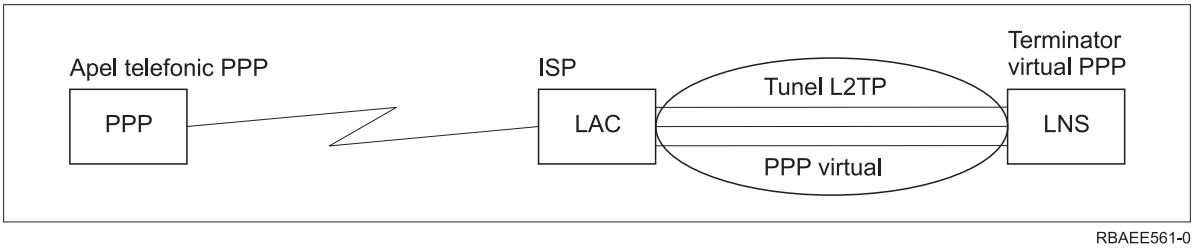


Figura 11. Iniţiator apel telefonic PPP sau terminator virtual PPP

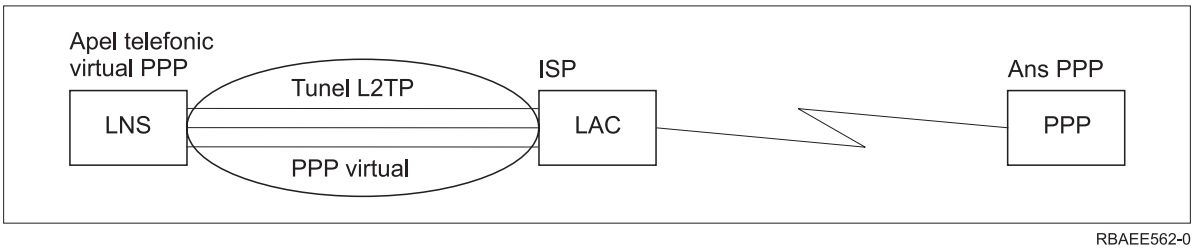


Figura 12. Apel telefonic virtual PPP sau răspuns virtual PPP

Protocolul L2TP este documentat ca standard Cerere pentru comentariu (RFC), RFC-2661. Un tunel L2TP se poate extinde peste toată sesiunea PPP sau numai peste un segment dintr-o sesiune cu două segmente. Aceasta poate fi reprezentată de patru modele diferite de tunelare.

Informaţii înrudite

Scenariu: Protejarea unui tunel voluntar L2TP cu IPSec

RFC Editor

Tunel voluntar:

În modelul tunelului voluntar, un tunel este creat de utilizator, de obicei utilizând un client cu Protocolul de tunelare nivelul doi (L2TP) activat.

Ca rezultat, utilizatorul trimite pachete L2TP la furnizorul de servicii Internet (ISP), care le înaintează la serverul de reţea L2TP (LNS). În tunelarea voluntară, nu e nevoie ca ISP-ul să suporte L2TP şi iniţiatorul tunelului L2TP este pe acelaşi sistem cu clientul la distanţă. În acest model, tunelul se extinde pe întreaga sesiune Protocol punct-la-punct (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.

Ca rezultat, utilizatorul trimite pachete Protocol punct-la-punct la Furnizorul de servicii Internet (ISP) (concentrator acces (LAC) Protocol de tunelare nivelul doi (L2TP)). ISP-ul încapsulează pachetele în L2TP şi le trimite într-un tunel la serverul de reţea L2TP (LNS). În cazurile de tunel obligatoriu, ISP-ul trebuie să fie capabil de L2TP. În acest model, tunelul se extinde numai peste segmentul de sesiune PPP dintre ISP şi LNS.

Model de tunel obligatoriu - apel la distanţă:

În modelul de tunel obligatoriu - apel la distanţă, poarta de bază (serverul de reţea L2TP (LNS)) iniţiază un tunel la un furnizor de servicii Internet (ISP) (LAC) şi instruieşte ISP-ul să amplaseze un apel local la clientul receptor al Protocolului punct-la-punct (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 Protocol de tunelare nivelul doi (L2TP) este un mod de a redirecţiona traficul în numele concentratorilor de acces L2TP client (LAC-uri) şi a serverelor de reţea L2TP (LNS-uri).

O conexiune multi-hop se stabileşte utilizând o poartă (gateway) multi-hop L2TP (un sistem care leagă Terminatorul L2TP şi profilurile iniţiatoare împreună). 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.

Suportul PPPoE (DSL) pentru conexiuni PPP

Digital Subscriber Line (DSL) se referă la o clasă de tehnologie utilizată pentru a obţine mai multă lăţime de bandă prin cablarea telefonică de cupru existentă între sediul unui beneficiar şi un furnizor de servicii Internet (ISP).

DSL permite servicii vocale şi de transmitere a datelor cu viteză mare simultan printr-o singură pereche de fire telefonice din cupru. Vitezele de modem au crescut gradat prin utilizarea diferitor tehnici de comprimare şi nu numai, dar avându-le în vedere pe cele mai rapide de astăzi (56 kbps), se apropie de limita teoretică pentru această tehnologie. Tehnologia DSL permite viteze mult mai mari prin liniile pereche torsadate, de la biroul central şi până la şcoală, acasă sau la întreprindere. În unele zone sunt realizabile viteze de până la 2 Mbps. PPP este de obicei folosit peste comunicaţii seriale cum sunt conexiunile apel telefonic prin modem. Mulţi furnizori de servicii Internet utilizează acum PPP peste Ethernet (PPPoE) datorită caracteristicilor suplimentare de securitate şi logare.

Un *modem DSL* este un dispozitiv care este amplasat la oricare din capetele liniei telefonice de cupru pentru a permite unui calculator (sau LAN) să fie conectat 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 seamănă cu modemurile analoage convenţionale, furnizează un debit mult mai mare.

Echipamentul conexiunii

Sistemul utilizează modem-uri, adaptoare terminale Reţea digitală de servicii integrate (ISDN), adaptoare Token-Ring, adaptoare Ethernet sau dispozitive unitate service canal/unitate service date (CSU/DSU) pentru a manipula conexiunile punct-la-punct (PPP).

Acestea sunt patru tipuri de echipamente de comunicaţii pe care le puteţi utiliza cu mediul dumneavoastră PPP:

- Modemuri
- CSU/DSU
- Adaptoare terminale ISDN
- Adaptoare Ethernet (pentru conexiuni PPPoE).

Modemuri

Pot fi utilizate atât modemuri interne cât şi externe pentru conexiuni Protocol punct-la-punct (PPP).

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, şirurile de modem sunt deja definite pentru a fi utilizate.

Sistemul are multe modeluri de modem predefinite, dar pot fi definite şi modele noi prin System i Navigator. 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 predefinite nu pot fi modificate. Pot fi însă adăugate comenzi suplimentare şirului de apelare sau comenzii de iniţializare.

Puteţi utiliza modemul de suport electronic client care este inclus cu sistemul pentru a stabili conexiuni PPP. Pe sisteme mai vechi, modemul de suport electronic client era un modem extern IBM 7852-400. Acest modem a fost înlocuit de MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. Pe sistemele mai noi, modemul 2771, 2793, sau oricare din celelalte modemuri interne suportate poate fi utilizat ca modem de suport electronic client.

Referinţe înrudite

“Cerinţe de software şi hardware” la pagina 31
Pentru un mediu PPP este necesar să aveţi două sau mai multe calculatoare care suportă PPP. Unul dintre aceste calculatoare, platforma System i, poate fi originatorul sau receptorul.

CSU/DSU

O unitate de service canal (CSU) este un dispozitiv care conectează un terminal la o linie digitală. O unitate de service date (DSU) este un dispozitiv care realizează funcţii de diagnoză şi protecţie 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 de software şi hardware" la pagina 31
Pentru un mediu PPP este necesar să aveţi două sau mai multe calculatoare care suportă PPP. Unul dintre aceste calculatoare, platforma System i, poate fi originatorul sau receptorul.

"Serviciul digital şi DDS" la pagina 33
Puteţi utiliza serviciul digital şi DDS (Digital Data Services) cu PPP (Point-to-Point Protocol).

Adaptoare terminale ISDN

Reţeaua digitală de servicii integrate (ISDN) vă furnizează o conexiune digitală care vă permite să comunicaţi utilizând orice combinaţie de voce, date şi video, printre alte aplicaţii multimedia.

Trebuie să verificaţi că adaptorul dumneavoastră terminal este evaluat pentru utilizare pe sistem.

Urmaţi aceşti paşi pentru configurarea adaptorului terminal:

1. În System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Faceţi clic-dreapta pe **Modemuri** şi selectaţi **Modem nou**.
3. Din caseta de dialog **Proprietăţi noi modem**, 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 55
Exemplul demonstrează cum se configurează un adaptor terminal ISDN (Integrated Services Digital Network).

Referinţe înrudite

"Cerinţe de software şi hardware" la pagina 31
Pentru un mediu PPP este necesar să aveţi două sau mai multe calculatoare care suportă PPP. Unul dintre aceste calculatoare, platforma System i, poate fi originatorul sau receptorul.

"ISDN (Integrated Services Digital Network)" la pagina 34
Reţeaua digitală de servicii integrate (ISDN) furnizează conectivitate digitală cap-la-cap comutată. ISDN poate purta atât voce cât şi date pe aceeaşi conexiune.

Sugestii pentru adaptorul terminal ISDN:

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

Adaptorul terminal extern sugerat de Reţea digitală de servicii integrate (ISDN), sau modemul ISDN, este **3Com/U.S. Robotics Courier I ISDN V.Everything**. Suportă conexiuni de modem analog V.34, V.90 (X2), V.92 şi legătură multiplă PPP peste ISDN atât în mod de originare cât şi de răspuns pe sistem. 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 iniţiate de pe sistem.** La cererile de identificare CHAP iniţiate de pe partea de recepţie se răspunde de către adaptorul terminal Courier I, în timp ce se negociază autentificarea PAP (Password Authentication Protocol) cu sistemul. Răspunsurile PAP nu apar în conexiunea ISDN.
- **Conexiuni la care răspunde sistemul.** Courier I necesită autentificare CHAP de către partea apelantă dacă configuraţia de răspuns cauzează sistemul să deschidă autentificarea cu o cerere de identificare CHAP. Dacă sistemul deschide autentificarea cu PAP, adaptorul terminal Courier I se autentifică cu PAP.

Dacă utilizaţi un modem Courier I dinainte de 1999, verificaţi ca modemul Courier I să fie conectat la sistemul dumneavoastră printr-un cablu V.35 pentru a obţine cea mai bună performanţă de la conexiunea dumneavoastră 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: Conform 3Com/US Robotics, versiunea V.35 a acestui adaptor terminal nu mai este de la furnizori de terţă parte, deşi unele versiuni V.35 ar mai putea veni încă de la furnizori de terţă parte. Versiunea RS-232 este încă sugerată la o performanţă mai scăzută pe sistem, deoarece conexiunile RS-232 sunt limitate la 115,2 KB.

Asiguraţi-vă că setaţi viteza de linie V.35 de pe sistem la 230,4 kbps.

Restricţii la adaptoarele terminale ISDN:

Au fost evaluate următoarele adaptoare terminale din acest subiect. Sunt sugerate numai pentru originarea conexiunilor la distanţă Reţea digitală de servicii integrate (ISDN) de la sistem.

3Com Impact IQ ISDN:

Acest adaptor terminal nu este sugerat pentru platforma System i din următoarele motive:

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuşi, poate suporta conexiuni de modem analog V.34, utilizând conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.
- Adaptorul terminal s-ar putea să nu fie conectat la sistem la viteze mai mari de 115 200 bps.
- Adaptorul terminal nu suportă automat CHAP (Challenge Handshake Authentication Protocol). Dacă setaţi S84 la 0, se realizează autentificare CHAP.
- Sistemul nu poate să determine terminarea conexiunii când se monitorizează semnalul Set date gata de la adaptorul terminal. Aceasta cauzează o potenţială expunere a securităţii sistemului.

Motorola BitSurfr Pro ISDN:

Acest adaptor terminal nu este sugerat pentru platforma System i din următoarele motive:

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuşi, poate suporta conexiuni de modem analog V.34, utilizând conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.
- Adaptorul terminal s-ar putea să nu fie conectat la sistem la viteze mai mari de 115 200 bps.
- Adaptorul terminal nu suportă automat autentificarea CHAP. Totuşi, setarea @M2=C permite realizarea autentificării CHAP.
- Adaptorul terminal nu permite automat răspunsul la ambele apeluri PPP, de legătură unică şi multiplă. Adaptorul terminal de originare la distanţă trebuie setat la acelaşi protocol (legătură unică sau multiplă) cu adaptorul terminal de răspuns.
- Mecanismul de control al fluxului hardware nu funcţionează bine cu acest adaptor terminal. Aceasta cauzează o performanţă scăzută atunci când sistemul trimite date pe o conexiune PPP de legătură multiplă.

Tratarea adreselor IP

Conexiunile PPP permit mai multe seturi diferite de opţiuni pentru gestionarea adreselor IP, în funcţie de tipul profilului de conexiune.

- DHCP poate gestiona centralizat alocările adreselor IP pentru reţeaua dumneavoastră. Învăţaţi cum să setaţi şi să gestionaţi serviciile DHCP pentru reţeaua dumneavoastră. Vedeţi DHCP (Dynamic Host Configuration Protocol)
- DNS vă poate ajuta să gestionaţi numele de gazdă şi adresele IP asociate. Învăţaţi cum să setaţi şi să gestionaţi servicii DNS pentru reţeaua dumneavoastră. Vedeţi DNS (Domain Name System)

- BOOTP este utilizat pentru a asocia staţiile de lucru ale clienţilor cu sistemul dumneavoastră şi pentru a le aloca adrese IP. Învăţaţi cum să setaţi şi să gestionaţi servicii BOOTP pentru reţeaua dumneavoastră. Vedeţi Bootstrap Protocol

  Referinţe înrudite

  “Scenariu: Conectarea sistemului la un concentrator de acces PPPoE” la pagina 10
  Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

Filtrarea pachetelor IP

Filtrarea pachetelor IP limitează serviciile pentru utilizatorii individuali atunci când se înregistrează pe o reţea.

Filtrarea pachetelor poate permite sau refuza accesul pe baza adreselor IP de destinaţie sau porturilor, sau pe baza ambelor. Diferite politici sunt impuse prin definirea de seturi multiple de reguli filtru pachet, având fiecare identificatorul de filtru PPP unic propriu. Regulile de filtru pachet pot fi alocate pentru un anumit profil de conexiune receptoare sau pot fi alocate utilizând o Politică de grup care va aplica regulile filtru pentru acea categorie de utilizatori. Regulile filtru pachet în sine nu sunt definite în PPP, ci sub Reguli pachet IP în System i Navigator.

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

Referinţe înrudite

“Scenariu: Conectarea sistemului la un concentrator de acces PPPoE” la pagina 10
Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

Informaţii înrudite

Filtrarea IP şi translatarea adreselor de reţea

VPN (Virtual Private Networking)

Strategia de gestionare a adreselor IP

Înainte de a configura un profil de conexiune PPP, ar trebui să fiţi familiar cu strategia de gestiune a adreselor IP ale reţelei dumneavoastră. Această strategie influenţează multe din deciziile de pe parcursul procesului de configurare, inclusiv strategiile dumneavoastră de autentificare, considerentele de securitate şi setările TCP/IP.

Profiluri de conexiune originatoare

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 deţină controlul asupra adreselor IP care vor fi utilizate 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 fixe fie pentru adresa IP locală sau la distanţă, trebuie să vă asiguraţi că sistemul la distanţă este definit pentru a accepta adresele IP pe care le-aţi definit. 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 considerent ar fi dacă doriţi să activaţi travestirea adresei IP. De exemplu, dacă sistemul se conectează la Internet printr-un ISP, acesta poate permite unei reţele ataşate în spatele sistemului să acceseze Internetul. În principiu, sistemul ascunde adresele IP ale sistemelor de pe reţea în spatele adresei IP locale alocate de ISP, făcând astfel ca întregul trafic IP să pară a fi de la sistem. De asemenea, sunt şi considerente suplimentare de rutare atât pentru sistemele din LAN (pentru a se asigura că traficul lor Internet este trimis la sistem), cât şi pentru sistemul unde trebuie să activaţi caseta **adăugare sistem la distanţă ca rută implicită**.

Profiluri de conexiune receptoare

Profilurile de conexiune receptoare au mult mai multe opţiuni şi considerente de adresă IP decât are Profilul conexiunii originatoare. 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 singur profil receptor, puteţi defini o adresă IP unică sau puteţi utiliza o adresă IP locală existentă pe sistemul dumneavoastră pentru a identifica oprirea conexiunii PPP. Pentru profiluri receptor definite pentru a suporta conexiuni multiple în acelaşi timp, trebuie să folosiţi o adresă IP locală existentă. Dacă nu este nicio adresă IP locală existentă, puteţi crea o adresă IP virtuală pentru 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 doriţi ca sistemul la distanţă să fie considerat parte din LAN, ar trebui să configuraţi rutarea adresei IP, să specificaţi o adresă IP din intervalul de adrese IP pentru sistemele ataşate LAN-ului şi să verificaţi că înaintarea IP a fost activată atât pentru acest profil de conexiune cât şi pentru sistem.

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.
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. Aceasta permite şi definirea de rute suplimentare pentru fiecare din aceste ID-uri de utilizator, astfel încât să puteţi ajusta mediul la utilizatorul de la distanţă cunoscut. Autentificarea trebuie să fie activată pentru ca această funcţie să fie corectă.

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

Opţiune	Descriere
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 sistem, se va face o căutare pentru a determina dacă o adresă IP la distanţă este definită anume pentru acest utilizator. Dacă da, acea adresă IP, mască şi set de rute posibile vor fi folosite pentru conexiune. Dacă utilizatorul nu este definit, adresa IP va deveni implicit adresa IP fixă definită sau următoarea adresă IP pool de adrese.
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 să utilizeze propria adresă IP, adresa IP la distanţă va fi determinată de metoda de alocare a adreselor IP la distanţă definite. Această opţiune este iniţial dezactivată şi aveţi grijă înainte de activarea ei.
Rutare adresă IP	Clientul dial-up şi sistemul trebuie să aibă rutarea adresei IP configurată corespunzător dacă clientul necesită acces la vreo adresă IP de pe LAN-ul căruia îi aparţine sistemul.

Autentificarea sistemului

Conexiunile PPP cu o platformă System i suportă mai multe opţiuni pentru autentificare, atât a clienţilor la distanţă care apelează sistemul, cât şi a conexiunilor la un ISP sau la alt sistem pe care îl apelează sistemul.

Sistemul suportă mai multe metode pentru menţinerea informaţiilor de autentificare. Aceste metode includ liste de validare simple de pe sistem, care conţin liste ale a utilizatorilor autorizaţi şi ale parolelor lor pentru a suporta serverele Remote Authentication Dial In User Service (RADIUS). Serverele RADIUS menţin informaţii detaliate pentru utilizatorii reţelei. De asemenea, sistemul suportă mai multe opţiuni pentru criptarea informaţiilor de parolă şi ID utilizator, variind de la un simplu schimb de parolă la suport cu Protocolul de autentificare dialog de confirmare (CHAP-MD5). Vă puteţi specifica preferinţele pentru autentificarea sistemului, inclusiv o parolă şi un ID de utilizator pentru a valida sistemul la un apel de ieşire, în fişa **Autentificare** a profilului de conexiune din System i Navigator.

Referinţe înrudite

"Scenariu: Conectarea sistemului la un concentrator de acces PPPoE" la pagina 10
Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

"Scenariu: Autentificarea conexiunilor dial-up cu RADIUS NAS" la pagina 21
Un Server de acces reţea (NAS) rulând pe sistem poate ruta cereri de autentificare de la clienţi de apel de intrare la un alt server Remote Authentication Dial In User Service (RADIUS). Dacă este autentificat, RADIUS poate controla şi adresele IP alocate utilizatorului.

"Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP" la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

CHAP (Challenge Handshake Authentication Protocol) cu MD5

CHAP-MD5 utilizează un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul de autentificare 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 de apel de intrare la distanţă la sistemul dumneavoastră" la pagina 13
Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

"PAP (Password Authentication Protocol)"
PAP utilizează un dialog de confirmare în ambele sensuri pentru a furniza sistemului peer o metodă simplă de stabilire a identităţii sale.

EAP (Extensible Authentication Protocol)

EAP permite modulelor de autentificare de terţă parte 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 sistemelor la distanţă să negocieze autentificarea necesară înainte de a primi sau transmite vreo informaţie.

Sistemul nu suportă direct EAP. Puteţi, totuşi, utiliza autentificare la distanţă cu un server Service utilizator apel de intrare autentificare la distanţă (RADIUS) care s-ar putea să suporte câteva din schemele de autentificare suplimentare descrise anterior.

PAP (Password Authentication Protocol)

PAP utilizează un dialog de confirmare în ambele sensuri pentru a furniza sistemului peer o metodă simplă de stabilire a identităţii sale.

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, parola şi ID-ul de utilizator nu sunt criptate niciodată, ceea ce face posibilă urmărirea lor şi le face vulnerabile la atacul hackerilor. Din acest motiv, ar trebui să utilizaţi Protocolul de autentificare dialog de confirmare (CHAP) oricând este posibil.

Referinţe înrudite

"CHAP (Challenge Handshake Authentication Protocol) cu MD5" la pagina 43
CHAP-MD5 utilizează un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul de autentificare şi de dispozitivul la distanţă.

Privire generală asupra RADIUS

Remote Authentication Dial In User Service (RADIUS) este un protocol standard de Internet care furnizează autentificare centralizată, contabilizare şi servicii de gestiune a IP-urilor pentru utilizatorii de acces la distanţă într-o reţea dial-up distribuită.

Modelul client-server RADIUS are un NAS (Network Access Server - Server de acces la reţea) care operează drept client al unui server RADIUS. Sistemul, acţionând ca NAS-ul, trimite informaţiile de conexiune şi utilizator la un server RADIUS desemnat utilizând protocolul standard RADIUS definit în RFC 2865.

Serverele RADIUS acţionează la cererile de conexiune utilizator autentificând utilizatorul şi apoi returnează toate informaţiile de configurare necesare la NAS, astfel încât NAS (sistemul) să poată livra servicii autorizate la utilizatorul de apel de intrare autentificat.

Dacă nu se poate ajunge la un server RADIUS, sistemul poate ruta cererile de autentificare la un server alternativ. Aceasta permite întreprinderilor globale să le ofere utilizatorilor lor un serviciu de apel de intrare cu un ID de logare utilizator unic pentru acces la nivelul corporaţiei, indiferent de punctul de acces care este utilizat.

Când se primeşte o cerere de autentificare de către serverul RADIUS, cererea este validată; apoi serverul RADIUS decriptează pachetul de date pentru a accesa informaţiile de parolă şi nume utilizator. Informaţiile sunt transmise la sistemul de securitate corespunzător care este suportat. 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 la sistem toate serviciile pe care utilizatorul autentificat este autorizat să le utilizeze, 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 contabilizare 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 dial-up cu RADIUS NAS” la pagina 21
Un Server de acces reţea (NAS) rulând pe sistem poate ruta cereri de autentificare de la clienţi de apel de intrare la un alt server Remote Authentication Dial In User Service (RADIUS). Dacă este autentificat, RADIUS poate controla şi adresele IP alocate utilizatorului.

Lista 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 ar putea fi **criptat - CHAP-MD5/EAP** sau **necriptat - PAP**.

Vedeţi ajutorul online pentru informaţii suplimentare.

Referinţe înrudite

“Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP” la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

Considerente de lăţime de bandă pentru legătură multiplă

Deseori, este necesară lăţime de bandă suplimentară pentru a finaliza anumite operaţii, dar nu este necesară tot timpul.

Achiziţionarea de hardware specializat şi de linii de comunicaţii scumpe s-ar putea să nu fie justificată. Protocolul de legătură multiplă (MP) PPP grupează mai multe legături PPP pentru a forma o singură legătură virtuală sau un 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 6 legături într-un bundle MP. Pentru a stabili o conexiune de legătură multiplă, ambele capete ale legăturii PPP trebuie să suporte protocolul de legătură multiplă. Protocolul de legătură multiplă este documentat ca standard Cerere pentru comentariu (RFC) RFC-1990.

Lăţime 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 de obicei numită Lăţime de bandă la cerere şi vă permite să plătiţi pentru lăţimea de bandă suplimentară doar când chiar o utilizaţi. Pentru a realiza avantajele de Lăţime de bandă la cerere, cel puţin un peer trebuie să fie capabil să monitorizeze utilizarea lăţimii de bandă totale care se află în prezent într-un bundle MP. Pot fi adăugate sau înlăturate legături din bundle atunci când utilizarea lăţimii de

bandă depăşeşte valori definite de configuraţie. Protocolul de alocare a lăţimii de bandă permite unui peer să negocieze adăugarea şi înlăturarea legăturilor dintr-un bundle MP. RFC-2125 documentează atât Protocolul de alocare a lăţimii de bandă (BAP) PPP şi Protocolul de control al alocării lăţimii de bandă (BACP).

Informaţii înrudite

RFC Editor

Configurarea PPP

Înainte de a putea utiliza PPP pentru a seta o conexiune punct-la-punct, trebuie să vă configuraţi mediul PPP.

Referinţe înrudite

"Informaţii înrudite pentru Serviciile de acces la distanţă" la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Crearea unui profil de conexiune

Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

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:

- Profiluri de conexiune originatoare
- Profiluri de conexiune receptoare
- **Modemuri**

Urmaţi aceşti paşi pentru a crea un profil de conexiune:

1. În System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii de acces la distanţă**.
2. Selectaţi una din următoarele opţiuni:
   - Faceţi clic dreapta pe **Profiluri de conexiune originatoare** pentru a seta sistemul pentru iniţiere.
   - Faceţi clic dreapta pe **Profiluri de conexiune receptoare** pentru a seta sistemul să permită conexiuni de intrare de la utilizatori şi sisteme 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. Vedeţi ajutorul online pentru anumite informaţii.

Operaţii înrudite

"Asocierea unui modem cu o descriere de linie" la pagina 56
Subiectul demonstrează paşii pentru asocierea unui modem cu o descriere de linie.

Referinţe înrudite

"Scenariu: Conectarea sistemului la un concentrator de acces PPPoE" la pagina 10
Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

"Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră" la pagina 13
Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

"Scenariu: Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem" la pagina 15
Administratorii, de obicei, setează reţelele de birou pentru ca angajaţii să poată accesa Internetul. Administratorii pot utiliza un modem pentru a conecta sistemul la un furnizor de servicii Internet (ISP). Clienţii PC-urilor ataşate LAN-ului pot să comunice cu Internetul utilizând sistemul de operare i5/OS ca poartă (gateway).

"Scenariu: Conectarea reţelei dumneavoastră corporative şi la distanţă cu un modem" la pagina 18
Un modem permite ca două locaţii la distanţă (precum un birou central şi o filială) să interschimbe date. Protocolul punct-la-punct (PPP) poate conecta împreună două LAN-uri, stabilind o conexiune între un sistem din biroul central şi un altul din filială.

"Scenariu: Gestionarea accesului utilizatorilor de la distanţă la resurse utilizând politicile de grup şi filtrarea IP" la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

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

PPP înlocuieşte SLIP (Serial Line Internet Protocol) ca protocol ales pentru conexiuni punct-la-punct.

PPP permite interoperabilitate între software-ul de acces la distanţă al diferitor producători. De asemenea, PPP permite mai multor protocoale de comunicaţii reţea să utilizeze aceeaşi linie de comunicaţii fizică.

Cererea de comentariu (RFC) SLIP nu devine 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 încă este utilizat astăzi şi este suportat pe sistemul de operare i5/OS. Totuşi, IBM recomandă utilizarea PPP la setarea conectivităţii punct-la-punct. SLIP nu furnizează niciun suport pentru conexiuni de legătură multiplă. 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 Protocol punct-la-punct (PPP) includ selecţii pentru tipul conexiunii şi modul de operare. Selecţiile dumneavoastră de mod specifică modul în care sistemul dumneavoastră utilizează noua conexiune PPP.

Urmaţi aceşti paşi pentru a specifica selecţiile de mod:

1. Selectaţi unul din următoarele tipuri de conexiune:
   - Linie comutată
   - Linie închiriată
   - Protocol de tunelare nivelul doi (L2TP) (linie virtuală)
   - Linia Protocol punct-la-punct peste Ethernet (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:

Când utilizaţi un modem (intern sau extern) sau un adaptor terminal extern Reţea digitală de servicii integrate (ISDN) pentru a vă conecta printr-o linie telefonică, selectaţi conexiunea de linie comutată.

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 apeleze telefonic sistemul.

Apel

Alegeţi acest mod de operare pentru a permite sistemului să apeleze telefonic un sistem la distanţă.

Apel telefonic la cerere (numai apel)

Alegeţi acest mod de operare pentru a permite sistemului să apeleze telefonic automat un sistem la distanţă atunci când traficul TCP/IP pentru sistemul la distanţă este detectat pe sistem. 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 sistemului să răspundă apelurilor de la un sistem la distanţă dedicat. De asemenea, acest mod de operare permite sistemului să apeleze sistemul la distanţă atunci când se detectează trafic TCP/IP pentru sistemul la distanţă. Dacă ambele sisteme utilizează sistemul de operare i5/OS şi acest mod de operare, traficul TCP/IP curge între cele două sisteme la cerere şi 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 a manipula apeluri de intrare, trebuie să faceţi referire la un profil de răspuns existent de la un profil de conexiune Protocol punct-la-punct (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:

Dacă aveţi o linie dedicată între sistemul local şi sistemul la distanţă, selectaţi conexiunea de linie închiriată. Dacă aveţi o linie închiriată, nu aveţi nevoie de un modem sau de un adaptor terminal Reţea digitală de servicii integrate (ISDN) pentru a conecta cele 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 sistemul 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 sistemului 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):

Dacă doriţi să furnizaţi o conexiune între sistemele care utilizează Protocol de tunelare nivelul doi (L2TP), selectaţi conexiunea L2TP.

După ce s-a stabilit un tunel L2TP, se face o conexiune virtuală Protocol punct-la-punct (PPP) între sistemul dumneavoastră 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 sistemului la distanţă să se conecteze la sistem printr-un tunel L2TP.

Iniţiator

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

Apel la distanţă

Alegeţi acest mod de operare pentru a permite sistemului să se conecteze la alt sistem sau un furnizot de servicii Internet (ISP) printr-un tunel L2TP şi pentru a direcţiona ISP-ul să apeleze un client PPP la distanţă.

Iniţiator multi-hop

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

Notă: Profilul terminator L2TP cu care este asociat acest iniţiator multi-hop trebuie să aibă bifată caseta **Permitere conexiune multi-hop** şi să aibă o intrare listă validare PPP care leagă numele de utilizator PPP la profilul iniţiator multi-hop.

Linie PPPoE:

Conexiunile Protocol punct-la-punct prin Ethernet (PPPoE) utilizează o linie virtuală pentru a trimite date PPP (printr-un adaptor Ethernet) la un modem DSL care este furnizat de ISP. Modemul este conectat şi la LAN-ul bazat pe Ethernet.

Aceasta permite acces Internet de viteză înaltă pentru utilizatorii LAN-ului prin sesiuni PPP pe sistemul de operare i5/OS. După ce a pornit conexiunea dintre sistem şi ISP, utilizatorii individuali din LAN pot porni sesiuni unice cu ISP-ul prin PPPoE.

Conexiunile PPPoE sunt utilizate numai de profiluri de conexiune originatoare. conexiunile implică un mod de operare iniţiator şi utilizează o singură linie.

Configurarea legăturii

Configurarea legăturii defineşte tipul de service linie pe care profilul conexiunii dumneavoastră Protocol punct-la-punct (PPP) îl utilizează pentru a stabili o conexiune.

Tipurile de servicii linie depind de tipul de conexiune specificat.

Referinţe înrudite

“Scenariu: Conectarea sistemului la un concentrator de acces PPPoE” la pagina 10
Mulţi furnizori de servicii Internet (ISP-uri) furnizează acces Internet de viteză mare prin DSL (Digital Subscriber Line), folosind PPP peste Ethernet (PPPoE). Va puteţi conecta sistemul la aceste ISP-uri pentru a furniza conexiuni de cu lăţime de bandă mare care păstrează avantajele Protocolului punct-la-punct (PPP).

“Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră” la pagina 13
Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

“Scenariu: Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem” la pagina 15
Administratorii, de obicei, setează reţelele de birou pentru ca angajaţii să poată accesa Internetul. Administratorii pot utiliza un modem pentru a conecta sistemul la un furnizor de servicii Internet (ISP). Clienţii PC-urilor ataşate LAN-ului pot să comunice cu Internetul utilizând sistemul de operare i5/OS ca poartă (gateway).

“Scenariu: Conectarea reţelei dumneavoastră corporative şi la distanţă cu un modem” la pagina 18
Un modem permite ca două locaţii la distanţă (precum un birou central şi o filială) să interschimbe date. Protocolul punct-la-punct (PPP) poate conecta împreună două LAN-uri, stabilind o conexiune între un sistem din biroul central şi un altul din filială.

Linie singulară:

Pentru a defini o linie Protocol punct-la-punct (PPP) care este asociată cu un modem analog, selectaţi acest serviciu de linie. Această opţiune este de asemenea folosită pentru liniile închiriate unde nu este necesar un modem. Profilul de conexiune PPP utilizează mereu aceeaşi resursă de port de comunicaţii i5/OS.

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 descrierea unei linii comutate şi selectaţi **Activare partajare resursă dinamică**.

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:

Pentru a seta conexiunea PPP să utilizeze o linie dintr-un pool de linii, selectaţi acest serviciu de linie. Când porneşte conexiunea PPP, sistemul selectează o linie neutilizată din poolul de linii. Pentru profiluri de apel la cerere, sistemul 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 din fişa **Conexiuni** a dialogului **Proprietăţi profil**

punct-la-punct nou atunci când vă configuraţi profilul conexiunii. 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.

  Sistemul selectează o linie dintr-un pool de linii numai când se utilizează o conexiune de 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 de 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 System i Navigator, selectaţi-vă sistemul şi expandaţi **Lucru în 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 de conexiune originatoare** pentru a seta sistemul să iniţieze o conexiune la un sistem la distanţă.
   - Faceţi clic dreapta pe **Profiluri de conexiune receptoare** pentru a seta sistemul să permită conexiuni de intrare de la utilizatori şi sisteme 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**. Apăsaţi pe **OK** şi System i Navigator deschide o fereastră de proprietăţi pentru acest profil de conexiune.

   Notă: De asemenea, puteţi selecta un pool de linii atunci când creaţi profiluri de conexiune receptoare. Opţiunea Pool de linii ar putea să fie sau nu listată, în funcţie de următoarele valori de câmp: tip protocol, tip conexiune şi mod de 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 parcurge în jos lista de linii disponibile (din pool) până când o resursă este disponibilă şi utilizează acea linie pentru conexiune. Utilizaţi ajutorul System i Navigator pentru continuarea asistenţei.

Referinţe înrudite

"Scenariu: Conectarea clienţilor de apel de intrare la distanţă la sistemul dumneavoastră" la pagina 13
Utilizatorii de la distanţă, precum telecomutatoarele sau clienţii mobili, necesită deseori acces la reţeaua unei companii. Aceşti clienţi de apel de intrare pot obţine acces la un sistem cu Protocolul punct-la-punct (PPP).

"Scenariu: Conectarea LAN-ului dumneavoastră de birou la Internet cu un modem" la pagina 15
Administratorii, de obicei, setează reţelele de birou pentru ca angajaţii să poată accesa Internetul. Administratorii pot utiliza un modem pentru a conecta sistemul la un furnizor de servicii Internet (ISP). Clienţii PC-urilor ataşate LAN-ului pot să comunice cu Internetul utilizând sistemul de operare i5/OS ca poartă (gateway).

"Scenariu: Conectarea reţelei dumneavoastră corporative şi la distanţă cu un modem" la pagina 18
Un modem permite ca două locaţii la distanţă (precum un birou central şi o filială) să interschimbe date. Protocolul punct-la-punct (PPP) poate conecta împreună două LAN-uri, stabilind o conexiune între un sistem din biroul central şi un altul din filială.

Suport pentru profil conexiuni multiple:

Profilurile de conexiune punct-la-punct care suportă conexiuni multiple vă permit să aveţi un profil de conexiune care manipulează mai multe apeluri digitale, analoage sau L2TP.

Acest lucru este util atunci când doriţi ca mai mulţi utilizatori să se conecteze la sistemul dumneavoastră dar nu doriţi să specificaţi un profil de conexiune punct-la-punct separat pentru a manipula fiecare linie PPP. Această caracteristică este utilă mai ales pentru modemul integrat 2805 cu 4 porturi, unde pot fi utilizate patru linii de la un 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 porneşte un fir de execuţie de profil conexiune separat pentru fiecare linie care este definită în poolul de linii. Toate firele de execuţie aşteaptă apeluri de intrare pe liniile lor corespunzătoare.

Adresă IP locală pentru profiluri de conexiune multiplă

Puteţi utiliza adresa IP locală cu profiluri de conexiune multiplă, dar trebuie să fie o adresă IP existentă care este definită pe sistemul dumneavoastră. Puteţi utiliza lista derulantă de adrese IP pentru a selecta adresa IP existentă. Utilizatorii la distanţă pot accesa resursele care sunt pe reţeaua dumneavoastră locală dacă alegeţi adresa IP locală ca adresa IP locală pentru profilul dumneavoastră 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 sau nu doriţi ca utilizatorii la distanţă să acceseze LAN-ul, trebuie să definiţi o adresă IP virtuală pentru sistemul dumneavoastră. O adresă IP virtuală este cunoscută şi ca interfaţă fără hardware. Profilurile punct-la-punct pot folosi această adresă IP ca adresă IP locală. Deoarece această adresă IP nu este legată de o reţea fizică, nu înaintează automat traficul către alte reţele care sunt ataşate sistemului dumneavoastră.

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

1. În System i Navigator, expandaţi-vă sistemul 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 dumneavoastră de conexiune punct-la-punct pot utiliza adresa IP virtuală odată ce este creată. Puteţi utiliza lista derulantă din câmpul **Adresă IP locală** care este pe pagina Setări TCP/IP pentru a utiliza adresa IP cu profilul dumneavoastră.

   Notă: Adresa IP virtuală trebuie să fie activă înainte de a vă porni profilul de conexiune multiplă; 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.

Pooluri de adrese IP la distanţă pentru profiluri de conexiune multiplă

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 de pool 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.

  Operaţii înrudite

  “Pasul 1: Configurarea unui profil terminator L2TP pentru orice interfaţă de pe partiţia care deţine modemurile” la pagina 28
  Pentru a crea un profil terminator pentru orice interfaţă, urmaţi aceşti paşi:

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 Protocolul de tunelare nivelul doi (L2TP) şi pooluri de linie cu un număr maxim de conexiuni mai mare decât unu. Această funcţie permite sistemului să aloce o adresă IP la distanţă unică fiecărei conexiuni 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**.

Atunci când utilizatorul la distanţă este conectat la sistem, sistemul determină dacă o anumită adresă IP este definită pentru acest utilizator. 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

Un modem vă furnizează capabilităţi de conexiune analogică (linii închiriate şi comutate). Pentru conexiunile PPP analogice, puteţi utiliza un modem extern, intern sau un adaptor terminal ISDN (Integrated Services Digital Network).

Referinţe înrudite

"Depanarea PPP" la pagina 63
Dacă întâlniţi probleme de conexiune Protocol punct-la-punct (PPP), puteţi utiliza lista de verificare pentru a strânge informaţii despre eroare. Această listă de verificare vă poate ajuta să identificaţi simptomele erorii şi să rezolvaţi problemele de conexiune PPP.

Configurarea unui modem nou

Puteţi configura un modem nou utilizând o descriere de modem existentă sau puteţi baza descrierea modemului pe o descriere de modem anterioară.

Pentru a configura un modem nou, urmaţi aceşti paşi:

1. În System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii 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 System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii 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 pe baza unei descrieri de modem anterioare

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

1. În System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii 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

"Depanarea PPP" la pagina 63
Dacă întâlniţi probleme de conexiune Protocol punct-la-punct (PPP), puteţi utiliza lista de verificare pentru a strânge informaţii despre eroare. Această listă de verificare vă poate ajuta să identificaţi simptomele erorii şi să rezolvaţi problemele de conexiune PPP.

Setarea şirurilor de comenzi pentru modem

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

Tabela 9. Modemuri definite pe sistem şi şiruri 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:	
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)	
Asiguraţi-vă că viteza de linie DTE-DCE este activată să ruleze la cei 115,2 kbps fixaţi (sau la 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 (purtătoare) după *m* secunde	S7=*m*
Tip modem Apel telefonic	ATDT pentru apel ton sau ATDP pentru apel puls

Exemplu: Configurarea unui adaptor terminal ISDN

Exemplul demonstrează cum se configurează un adaptor terminal ISDN (Integrated Services Digital Network).

1. În System i Navigator, selectaţi-vă sistemul 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: Apăsaţi pe fişa **Parametri ISDN** pentru a adăuga vreo comandă de iniţializare necesară pentru modemul dumneavoastră.

   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 recuperare la eroare pe care le realizează sitemul

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

   - Setarea versiunii şi tipului de switch ISDN care este furnizat de compania de telefonie locală.
   - Setarea numerelor din cartea de telefon şi a identificatorilor de profil service (SPID-uri) care sunt furnizate de compania telefonică locală.
   - Setarea ID-urilor de intrare terminal (TEI-uri) care ar putea fi furnizate de compania telefonică locală.
   - Setarea protocolului de canal B (PPP asincron-la-sincron).
   - Alte setări de modem care au parametri de lungime variabilă care 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 stare activă interfaţă *U* (ATD*x*), care permite sistemului să determine când se realizează suncronizarea cu switch-ul de birou 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. Oricărei comenzi pe care o specificaţi fără un parametru asociat îi poate fi alocat un parametru atunci când modemul este asociat cu o descriere de 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
Reţeaua digitală de servicii integrate (ISDN) vă furnizează o conexiune digitală care vă permite să comunicaţi utilizând orice combinaţie de voce, date şi video, printre alte aplicaţii multimedia.

Asocierea unui modem cu o descriere de linie

Subiectul demonstrează paşii pentru asocierea unui modem cu o descriere de linie.

1. În System i Navigator, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii de acces la distanţă → Profiluri de conexiune originatoare sau Profiluri de conexiune receptoare**.
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 de modem corespunzătoare ar trebui să fie deja selectată. Pentru informaţii suplimentare, vedeţi ajutorul online.

Puteţi configura profiluri de conexiune originatoare pentru a împrumuta o linie PPP şi un modem alocat unui profil de conexiune receptoare care aşteaptă un apel de intrare. Conexiunea originatoare va returna linia PPP şi modemul la profilul de conexiune receptoare atunci când se termină conexiunea. Pentru a activa această nouă funcţie, selectaţi opţiunea **Activare partajare resursă dinamică** din fişa **Modem** a ferestrei de configurare a liniei PPP. Puteţi configura linii PPP din fişa **Conexiune** a Profilurilor de conexiune originatoare şi receptoare.

Operaţii înrudite

"Crearea unui profil de conexiune" la pagina 46
Primul pas în configurarea unei conexiuni PPP dintre sisteme este să se creeze un profil de conexiune pe sistem.

Configurarea unui PC la distanţă

Pentru a vă conecta la o platformă System i de la un calculator personal (PC) care rulează orice sistem de operare pe 32 de biţi Windows, ar trebui să verificaţi că modemul dumneavoastră este instalat şi configurat corespunzător şi să vă asiguraţi că aţi instalat TCP/IP şi Dial-Up Networking pe PC.

Vedeţi documentaţia Microsoft Windows pentru informaţii despre configurarea Dial-up Networking pe PC. Asiguraţi-vă că aţi specificat sau introdus următoarele informaţii:

- Tipul de conexiune dial-up ar trebui să fie **PPP**.
- Dacă utilizaţi parole criptate, asiguraţi-vă că utilizaţi CHAP-MD5 (MS-CHAP nu este suportat de sistemul de operare i5/OS). 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. Niciun alt tip de protocol nesecurizat nu este suportat de sistem.

- În mod tipic, adresarea IP este definită de sistemul la distanţă sau de sistemul de operare i5/OS. Dacă intenţionaţi să utilizaţi metode de adresare IP alternative (precum definirea propriilor adrese IP), asiguraţi-vă că sistemul este, de asemenea, configurat pentru a vă accepta metoda de adresare.
- Adăugaţi adrese IP DNS dacă acestea sunt potrivite mediului dumneavoastră.

Configurarea accesului la Internet prin AT&T Global Network

Dacă doriţi să comunicaţi cu AT&T Global Network, trebuie să configuraţi profiluri 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 oricând şi nu se vor salva deloc datele existente.

Următoarele tipuri de aplicaţii pot utiliza conexiunea AT&T Global Network:

- **Schimb poştă**: Vă permite să extrageţi din când în când de la un singur cont AT&T Global Network şi să o trimiteţi la sistemul dumneavoastră pentru distribuire la utilizatorii dumneavoastră de Lotus Mail sau la utilizatorii dumneavoastră de Simple Mail Transfer Protocol (SMTP).
- **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 utiliza vrăjitorul Conexiune apel 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
- 2793/576C: WAN IOA cu două porturi, cu modem V.92 integrat pe portul 1 şi o interfaţă de comunicaţii standard pe portul 2. Acesta înlocuieşte modelul 2771.
- 2805: WAN IOA cu patru porturi, cu modem integrat V.92. 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 System i Navigator, expandaţi-vă sistemul 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.

Vrăjitorul Conexiune nouă prin apel telefonic

Acest vrăjitor descrie paşii pentru configurarea unui profil de conexiune dial-up pentru a vă accesa ISP-ul sau reţeaua internă. Trebuie să obţineţi câteva informaţii de la administratorul dumneavoastră de reţea sau ISP pentru a finaliza vrăjitorul. Pentru informaţii suplimentare despre finalizarea acestui vrăjitor, vedeţi ajutorul online.

Vrăjitorul Conexiune universală IBM

Acest vrăjitor descrie paşii pentru configurarea unui profil care poate fi utilizat de software-ul Suport electronic client pentru a se conecta la IBM. Suportul de service electronic furnizează monitorizarea mediului dumneavoastră unic i5/OS pentru a vă livra recomandări şi corecţii personalizate pentru situaţia şi sistemul dumneavoastră.

Informaţii înrudite

Conexiunea universală

Configurarea unei politici de acces de grup

Folderul **Politici de acces de 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 de grup, urmaţi aceşti paşi:

1. În System i, selectaţi-vă sistemul şi expandaţi **Reţea → Servicii de acces la distanţă → Profiluri de conexiune receptoare**.
2. Faceţi clic-dreapta pe **Politici de acces de grup** şi selectaţi **Politică nouă de acces de 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, activaţi în principal sistemul pentru a acţiona ca ruter pentru această conexiune. Aceasta permite datagrame IP nedestinate acestui sistem pentru a trece prin acest sistem la o reţea conectată. Dacă lăsaţi această opţiune goală, IP-ul ignoră acele datagrame de la sistemul la distanţă care nu sunt destinate pentru nicio adresă locală la acest sistem.

   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. Luaţi la cunoştinţă că aceasta are efect numai dacă este activată înaintarea de datagrame IP în tot sistemul; altfel, este ignorată chiar dacă este bifată. 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 comprimare VJ, sistemul stabileşte o conexiune care nu utilizează comprimare.

   Folosire reguli pachet IP pentru această conexiune. Această opţiune specifică dacă doriţi să aplicaţi o regulă de filtrare pentru această politică de grup. Regulile filtru controlează traficul IP din reţeaua dumneavoastră. Puteţi

utiliza această componentă de filtrare a pachetului IP pentru a vă proteja sistemul prin filtrarea pachetelor conform regulilor 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 de la distanţă la resurse utilizând politicile de grup şi filtrarea IP” la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

Informaţii înrudite

Filtrarea IP şi translatarea adreselor de reţea

Aplicarea regulilor de filtrare a pachetelor IP la o conexiune PPP

Puteţi utiliza un fişier de reguli pachet pentru a restricţiona accesul unui utilizator sau al unui grup la adresele IP de pe reţeaua dumneavoastră.

Subiectul Filtrare IP şi traducere adresă reţea din Centrul de informare discută modul în care se creează reguli de pachet IP la care puteţi face referire pentru un profil de conexiune PPP.

Puteţi vedea regulile 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 de 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 de la distanţă la resurse utilizând politicile de grup şi filtrarea IP" la pagina 23
Politicile de acces de grup identifică grupuri de utilizator diferite pentru o conexiune şi vă permit să aplicaţi setări de securitate şi atribute de conexiune comune pentru întregul grup. De asemenea, puteţi utiliza politicile de grup împreună cu filtrarea IP pentru a permite şi restricţiona accesul la anumite adrese IP din reţeaua dumneavoastră.

Activarea serviciilor RADIUS şi DHCP pentru profiluri de conexiune

Iată paşii pentru activarea serviciilor RADIUS sau DHCP pentru profiluri de conexiune receptoare PPP.

1. În System i Navigator, selectaţi-vă sistemul 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. Dacă se poate aplica soluţiei dumneavoastră RADIUS, puteţi activa şi contabilizarea RADIUS şi configurarea de adresă TCP/IP.
5. Faceţi clic pe butonul **Setări RADIUS NAS** pentru a configura conexiunea cu serverul RADIUS.
6. Apăsaţi pe **OK** pentru a vă întoarce la System i Navigator.

Referinţe înrudite

"Scenariu: Autentificarea conexiunilor dial-up cu RADIUS NAS" la pagina 21
Un Server de acces reţea (NAS) rulând pe sistem poate ruta cereri de autentificare de la clienţi de apel de intrare la un alt server Remote Authentication Dial In User Service (RADIUS). Dacă este autentificat, RADIUS poate controla şi adresele IP alocate utilizatorului.

Gestionarea PPP

Acest subiect conţine informaţii despre operaţiile de gestiune PPP pe care le puteţi realiza pe sistem.

Referinţe înrudite

"Informaţii înrudite pentru Serviciile de acces la distanţă" la pagina 64
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Setarea proprietăţilor pentru profiluri de 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 utiliza aceste indicaţii atunci când completaţi fiecare pagină a ferestrei Proprietăţi profil punct-la-punct nou. Setările pe care le selectaţi în fiecare pagină depind de mediu şi de tipul de conexiune configurată. Ajutorul online System i Navigator descrie fiecare opţiune care este afişată în fereastră. Pentru informaţii suplimentare, vă puteţi adresa şi procedurilor şi exemplelor PPP.

Monitorizarea activităţii PPP

Puteţi vizualiza un profil de conexiune şi un istoric de sesiune, utilizând System i Navigator.

Despre joburile conexiunii PPP:

- Sunt două joburi de control PPP care sunt utilizate pentru a gestiona firele de execuţie ale conexiunii individuale PPP. Aceste joburi rulează în subsistemul QSYSWRK:
  - QTPPPCTL - Jobul principal de control PPP. Acest job gestionează fiecare fir de execuţie 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*nnn* sunt joburi de apel de intrare, unde *nnn* este orice număr între 1 şi 999.

Lucrul cu profiluri de conexiune:

1. În System i Navigator, expandaţi-vă sistemul 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 conexiunii:

1. În System i Navigator, expandaţi-vă sistemul 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**.

Lucrul cu ieşire PPP de la sistem:

Pentru a lucra cu ieşiri PPP, introduceţi WRKTCPPTP din linia de comandă a sistemului:

- 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	Sistemul este gata pentru o conexiune
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
Confirmare sesiune PPPoE primită de la peer	Negociere PPPoE terminată cu succes
Apel L2TP stabilit	Mesaj tunel L2TP

Depanarea PPP

Dacă întâlniţi probleme de conexiune Protocol punct-la-punct (PPP), puteţi utiliza lista de verificare pentru a strânge informaţii despre eroare. Această listă de verificare vă poate ajuta să identificaţi simptomele erorii şi să rezolvaţi problemele de conexiune PPP.

Informaţiile relevante şi actuale despre corecţiile temporare de program (PTF-uri) şi depanare sunt documentate pe situl web TCP/IP pentru i5/OS . Acest sit web furnizează cele mai recente informaţii care suplimentează şi înlocuiesc informaţiile conţinute în acest subiect.

1. Material necesar pentru suport:
   - Tip gazdă la distanţă, sistem de operare şi nivel
   - i5/OS nivel sistem de operare gazdă
   - 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)
   - Scriptul de conexiune care este utilizat în 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

Publicaţia ITSO Redbook V4 TCP/IP for AS/400: More Cool Things Than Ever acoperă următoarele probleme PPP. De asemenea, oferă şi informaţii detaliate de rezolvare a problemelor.

Pentru a identifica problemele şi a găsi soluţiile, vedeţi lista de verificare din tabela următoare.

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 utilizaţi nu este în lista predefinită de modemuri din System i Navigator.	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.
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.

Tabela 12. Probleme PPP din ITSO Redbook (continuare)

Problemă	Soluţie
Protocol PPP Erorile de conectare pot apare din cauza configurării greşite a protocolului PPP.	Investigarea nivelurilor mai joase ale protocolului PPP ar putea fi necesară în unele situaţii în care peer-ii nu pot comunica unul cu altul 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
Un modem vă furnizează capabilităţi de conexiune analogică (linii închiriate şi comutate). Pentru conexiunile PPP analogice, puteţi utiliza un modem extern, intern sau un adaptor terminal ISDN (Integrated Services Digital Network).

"Configurarea unui modem nou" la pagina 54
Puteţi configura un modem nou utilizând o descriere de modem existentă sau puteţi baza descrierea modemului pe o descriere de modem anterioară.

Referinţe înrudite

"Informaţii înrudite pentru Serviciile de acces la distanţă"
Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

Informaţii înrudite pentru Serviciile de acces la distanţă

Publicaţiile IBM Redbooks şi siturile Web conţin informaţii care au legătură cu colecţia de subiecte Serviciile de acces la distanţă. Puteţi vizualiza sau tipări oricare dintre fişierele PDF.

IBM Redbooks

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

Situri web

Găsiţi cele mai recente corecţii temporare de program (PTF-uri) şi cele mai recente informaţii de configurare pentru PPP şi L2TP prin legătura PPP de pe situl Web TCP/IP for i5/OS. Acest sit web furnizează cele mai recente informaţii, care completează sau înlocuiesc informaţiile conţinute în această colecţie de subiecte.

Referinţe înrudite

"Fişierul PDF pentru Serviciile de acces la distanţă" la pagina 1
Puteţi vizualiza şi tipări un fişier PDF cu aceste informaţii.

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 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. Oferirea acestui document nu vă conferă nici o licenţă cu privire la 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 (pe doi octeţi), contactaţi departamentul IBM de proprietate intelectuală 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 NICIUN FEL DE GARANŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUSIV, DAR NU NUMAI, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot conţine greşeli tehnice sau erori de tipar. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) descris în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri 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 pentru dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să obţină 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, trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

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

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat la care se referă acest document şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM în conformitate cu termenii din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau din alt acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi 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, unele măsurători pot fi estimări obţinute prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat produsele respective şi nu poate confirma acurateţea performanţei, compatibilitatea sau orice alte pretenţii legate de produsele non-IBM. Întrebări legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără ca IBM să pretindă vreo plată, când o faceţi în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare a aplicaţiilor pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunţit în toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

Fiecare copie sau porţiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (an). Unele porţiuni din acest cod sunt derivate din programele exemplu oferite de IBM Corp. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vizualizaţi aceste informaţii în format electronic, este posibil să nu apară fotografiile şi ilustraţiile color.

Informaţii despre interfaţa de programare

Această publicaţie, Serviciile de acces la distanţă: Conexiunile PPP, conţine informaţii despre interfeţele de programare menite să permită beneficiarului scrierea de programe pentru obţinerea serviciilor IBM i5/OS.

Mărci comerciale

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

AIX
AS/400
eServer

i5/OS
IBM
IBM (logo)
iSeries
Lotus
OS/400
Redbooks
System i

Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt mărci comerciale înregistrate sau mărci comerciale deţinute de Adobe Systems Incorporated în Statele Unite şi/sau alte ţări.

Linux este o marcă comercială înregistrată deţinută de 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 logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Alte nume de companii, de produse sau de 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 obiecte 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 al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţină în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII 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 NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.