

IBM

@server

iSeries

Servicii de acces la distanță:
Conexiuni PPP

IBM Confidential





@server

iSeries

Servicii de acces la distanță:
Conexiuni PPP

IBM Confidential

Cuprins

Componentă 1. Servicii de acces la distanță: Conexiuni PPP.	1
Capitol 1. Ce este nou în V5R2	3
Capitol 2. Tipărește acest subiect	5
Capitol 3. Scenarii PPP	7
Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE	8
Scenariu: Conectarea clienților dial-in la distanță la serverul dvs. iSeries	9
Scenariu: Conectarea LAN-ului de birou la Internet cu un modem	11
Scenariu: Conectarea rețelei companiei și rețelele la distanță cu un modem.	13
Scenariu: Autentificarea conexiunilor dial up cu RADIUS NAS	16
Scenariu: Gestionarea accesului utilizatorilor la distanță la resurse folosind Politici de grup și filtrare IP	17
Capitol 4. Concepte PPP	21
Ce este PPP?	21
Profile de conexiuni.	21
Suport politici de grup	23
Capitol 5. Plan PPP	25
Cerințe software și hardware	25
Alternative conexiune	26
Linii telefonice analogice	26
Servicii digitale și DDS.	27
Switched-56	27
ISDN	28
T1/E1 și T1 fracțional	28
Frame Relay	29
Suport L2TP (tunel) pentru conexiuni PPP	29
Tunel voluntar.	29
Model tunel obligatoriu - apel primit	30
Model tunel obligatoriu - apel la distanță	30
Conexiune multi-hop L2TP	30
Suport PPPoE (DSL) pentru conexiuni PPP	30
Echipament conexiune	30
Modemuri	31
CSU/DSU	31
Adaptoare terminale ISDN	31
Recomandări adaptor terminal ISDN	31
Restricții adaptor terminal ISDN	32
Tratare adresă IP	33
Filtrare pachet IP.	35
Autentificare sistem.	35
CHAP-MD5.	36
EAP	36
PAP	36
Privire de ansamblu RADIUS	36
Listă de validare	37
Considerații lărgime de bandă - Multilink	37
Capitol 6. Configurare PPP	39
Crearea unui profil de conexiune	39
Tip protocol: PPP sau SLIP	40

Selecții mod	40
Linie comutată	40
Linie închiriată.	41
L2TP (linie virtuală)	41
L2TP (Layer 2 Tunneling Protocol)	42
Linie PPPoE	42
Configurare legătură	43
Linie singulară.	43
Grup de linii	43
Suport profil de conexiuni multiple	44
Grupuri de adrese IP la distanță	45
ISDN	46
Configurați-vă modem-ul pentru PPP	46
Configurați un nou modem	46
Setare șiruri comenzi modem	47
Exemplu: Configurați un adaptor terminal ISDN.	47
Asociați un modem cu o descriere de linie	48
Configurați un PC la distanță	48
Configurați accesul la Internet prin AT&T Global Network	49
Vrăjitori de conectare	50
Configurarea unei politici de acces de grup	50
Aplicarea regulilor de filtrare pachet IP unei conexiuni PPP	52
Activare servicii RADIUS și DHCP pentru profiluri conexiune	52
Capitol 7. Gestionări PPP	53
Setați proprietățile pentru profiluri conexiune PPP	53
Monitorizare activitate PPP	53
Capitol 8. Depanare PPP	57
Capitol 9. Alte informații despre PPP	59

Componentă 1. Servicii de acces la distanță: Conexiuni PPP

Protocol Punct-la-punct (PPP - Point-to-Point) este un standard Internet pentru transmiterea datelor pe linii seriale. Este cel mai utilizat protocol de conectare folosit de către ISP-uri (Furnizori de Internet). PPP permite calculatoarelor individuale să acceseze rețele care oferă acces la Internet. Serverul iSeries include suport PPP TCP/IP ca parte a conectivității sale WAN (rețele de largă răspândire geografică).

Puteți schimba date între locații folosind PPP pentru conectarea unui calculator de la distanță la serverul iSeries. Prin PPP, sistemele la distanță care sunt conectate la serverul iSeries pot accesa resurse sau alte mașini care aparțin aceleiași rețele ca și serverul dvs. Puteți configura serverul iSeries și pentru conectarea la Internet folosind PPP. Vrajitorul iSeries Navigator de conexiune dial-up vă poate ghida în procesul de conectare a serverului iSeries la Internet sau la o rețea internă.

- Ce este nou în V5R2? descrie actualizările ale Serviciilor de acces la distanță pentru această ediție.
- Tipărește acest subiect permite descărcarea sau tipărirea versiunii PDF a acestor informații.

Înțelegere Servicii de acces la distanță: Conexiuni PPP

Aceste subiecte vă introduc rapid în serviciile de acces la distanță care sunt pe serverul dvs. iSeries 400. Subiectele de mai jos vă pot ajuta la planificarea unui mediu PPP pentru rețeaua dvs.

- **Scenarii PPP** sunt exemple ale diferitelor implementări ale conexiunilor PPP. Fiecare exemplu oferă instrucțiuni și specifică valori exemplu pentru configurarea conexiunii PPP.
- **Conceptele PPP** vă oferă informații asupra conceptelor PPP și cerințelor serverului iSeries 400 pentru conexiuni PPP.
- **Plan PPP** oferă informații despre concepte PPP și cerințele serverului iSeries 400 pentru conexiuni PPP.

Folosire Servicii de acces la distanță: Conexiuni PPP

Aceste subiecte vă pot ajuta la configurarea și administrarea conexiunilor PPP pe serverul iSeries 400.

- **Configurare PPP** subliniază pașii de bază pentru configurarea unei conexiuni PPP.
- **Gestionare PPP** oferă informații pe care le puteți folosi ca ghid pentru gestionarea conexiunilor PPP.
- **Depanare PPP** descrie erorile de bază de conexiune PPP și vă îndrumă spre informații de depanare relevante.

Puteți găsi și alte informații despre PPP aici. Această pagină conține legături către informații înrudite folositoare despre serverul iSeries.

Capitol 1. Ce este nou în V5R2


Pentru V5R2, iSeries Navigator poate activa conexiuni PPP peste Ethernet (PPPoE) care provin de la serverul iSeries. Acest suport oferă un nou tip de linie virtuală PPPoE, care este legat de o linie Ethernet fizică, pentru stabilirea unei conexiuni folosind un adaptor Ethernet atașat la un modem DSL. Odată ce conexiunea dintre iSeries și ISP a pornit, utilizatori individuali de pe LAN pot accesa ISP prin conexiunea iSeries PPPoE. Puteți accesa această nouă funcție din dialogul profil conexiune generator sau din Vrajitorul conexiune universală.


Pentru informații suplimentare, vedeți **Conectați-vă serverul iSeries la un generator de acces PPPoE**

Mai multe adăugări la iSeries Navigator fac mai ușoare configurarea și gestionarea conexiunilor PPP, incluzând:

- Dialogul de configurare DHCP-WAN va contacta automat serverul DHCP și interfața client pentru a determina adresa IP pentru interfața client DHCP-WAN. Pentru a accesa acest dialog:
 - Expandați **Rețea > Servicii de acces la distanță**
 - Faceți clic dreapta pe **Servicii de acces la distanță**
 - Selectați **Servicii**
 - Selectați fișa **DHCP-WAN**
- Un dialog de stare conexiuni îmbunătățit afișează acum detalii de conexiune pentru L2TP, L2TP multihop, multilink și PPP prin conexiuni Ethernet, făcându-vă mai ușoară gestionarea conexiunilor PPP.
- Abilitatea de a crea profiluri conexiune Generator și Receptor și Politici de acces de grup a fost adăugată la Task Pad.
- Vrajitorul conexiune dial nouă și Vrajitorul conexiune universală au fost redenumite și sunt numite acum Noi conexiuni Internet sau ISP Dial și Conexiune universală IBM nouă.
- Profilurile conexiune generator pot acum "împrumuta" o linie și un modem PPP alocate unui profil de conexiune receptor care așteaptă un apel de intrare. Conexiunea generatoare va "întoarce" linia și modemul PPP profilului de conexiune receptor când conexiunea s-a încheiat. Pentru a activa această nouă funcție, selectați opțiunea **Activare partajare resurse dinamice** din fișa Modem a dialogului configurare linie PPP. Puteți configura linii PPP din fișa Conexiune a profilelelor conexiune Receptor și Generator.
- Proprietățile grupului de linii nu mai pot fi modificate cât timp sunt folosite, ceea ce previne potențiale probleme de grup de linii.
- Suportul pentru modurile de operare inițiator-la-cerere și apel-la-distanță-la-cerere a fost abandonat din profilurile conexiune Generator folosind conexiuni L2TP.

Capitol 2. Tipărește acest subiect

Puteți vizualiza sau încărca o versiune PDF a acestui document pentru vizualizare sau tipărire. Aveți nevoie de Adobe® Acrobat® Reader pentru a vizualiza fișiere PDF. Puteți descărca o copie de la Adobe .

Pentru a vizualiza sau descărca versiunea PDF, selectați Servicii de acces la distanță: conexiuni PPP 
(277 KB sau aproape 58 pagini).

Pentru a salva un fișier PDF pe stația de lucru pentru vizualizare sau tipărire:

1. Deschideți PDF-ul (apăsați cu mouse-ul legătura de mai sus).
2. În meniul browser-ului, selectați **File**.
3. Selectați **Save As**.
4. Navigați în directorul în care doriți să salvați fișierul PDF.
5. Apăsați **Save**.

Capitol 3. Scenarii PPP

Următoarele scenarii vă ajută să înțelegeți cum funcționează PPP și cum puteți implementa un mediu PPP în rețeaua dvs. Aceste scenarii introduc concepte PPP fundamentale de care începătorii și utilizatorii expermențați pot beneficia înainte de a trece la taskurile de planificare și configurare.

Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE

Multe ISP-uri oferă acces de mare viteză la Internet prin DSL folosind PPPoE. Serverul iSeries se poate conecta la acești furnizori de servicii pentru a oferi conexiuni cu lărgimi de bandă ridicate care păstrează avantajele PPP.

Scenariu: Conectarea clienților dial-in la distanță la serverul iSeries

Utilizatorii la distanță, cum sunt cei ce utilizează telecomutarea sau clienții mobili, necesită adesea accesul la rețeaua unei companii. Acești clienți conectați prin linie telefonică pot obține accesul la un server iSeries cu PPP.

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

Administratorii configurează de obicei rețele de birou care permit accesul angajaților la Internet. Aceștia pot folosi un modem pentru conectarea serverului iSeries la un ISP (Internet Service Provider - Furnizor de Internet). Clienții PC atașați la LAN pot comunica cu Internetul folosind ca poartă (gateway) serverul iSeries.

Scenariu: Conectarea rețelei companiei și rețelele la distanță cu un modem

Un modem permite ca două locații la distanță (cum ar fi birourile centrale și o filială) să schimbe date între ele. PPP poate conecta cele două rețele locale prin stabilirea unei conexiuni între un server iSeries din biroul central și un alt server iSeries din biroul filialei.

Scenariu: Autentificarea conexiunilor dial up cu RADIUS NAS

Un server de acces la rețea (NAS) ce rulează pe un server iSeries poate ruta cereri de autentificare de la clienți dial-in la alt server RADIUS. Dacă este autentificat, RADIUS poate de asemenea controla adresele IP și porturile utilizatorului.

Scenariu: Gestionarea accesului utilizatorilor la distanță la resurse folosind Politici de grup și filtrarea IP.

Politicile de acces în grup identifică grupuri de utilizatori distincte pentru o conexiune și vă permit să aplicați niște atribute de conexiune comune și setări de securitate întregului grup. În combinație cu filtrarea IP, aceasta vă permite să lăsați sau restricționați accesul la adrese IP anume din rețeaua dvs.

Scenariu: PPP și DHCP pe un singur server iSeries

Utilizatorii la distanță sau clienții conectați prin linie telefonică pot obține accesul la un server iSeries din rețeaua unei companii cu PPP. Clientul WAN DHCP din același iSeries permite utilizatorilor la distanță să obțină adrese IP alocate dinamic folosind aceleași servicii ca utilizatorii atașați LAN.

Scenariu: profil DHCP și PPP pe servere iSeries diferite

Aspectele de securitate sau dispunerea fizică a rețelei determină majoritatea companiilor să separe serviciile din rețea și să le distribuie unor servere diferite. Acest scenariu tratează complexitatea adăugată prin folosirea separată a unui server PPP și a unui server DHCP. Ca și scenariul anterior, această configurare permite utilizatorilor la distanță să se conecteze pe linie telefonică și să obțină acces la rețeaua companiei.

Scenariu: PPP și VPN: tunel voluntar L2TP protejat de VPN

Un sediu de filială se poate conecta la birourile corporative prin L2TP (Layer 2 Tunnel Protocol). Un tunel voluntar L2TP stabilește o legătură PPP virtuală. Prin urmare, L2TP extinde rețeaua birurilor corporative, astfel încât sediul de filială apare ca parte a subrețelei comune. VPN protejează traficul de date prin tunelul L2TP.

Scenariu: Conectarea serverului iSeries la un concentrator de acces PPPoE

Situație: Afacerile dvs. cer o conexiune Internet mai rapidă, deci sunteți interesat de un serviciu DSL cu un ISP local. După o investigație inițială, aflați că ISP-ul dvs. folosește PPPoE pentru a conecta clienții săi. Ați vrea să folosiți această conexiune PPPoE pentru a oferi lărgime ridicată de bandă a conexiunilor Internet prin serverul dvs. iSeries.



Figura 1. Conectarea serverului dvs. iSeries la un ISP cu PPPoE

Soluție: Puteți suporta o conexiune PPPoE către ISP-ul dvs. prin serverul dvs. iSeries. Serverul iSeries folosește un nou tip de linie virtuală PPPoE care este legată de o linie Ethernet fizică configurată să folosească un adaptor Ethernet de tip 2838. Această linie virtuală suportă protocoale de sesiune PPP printr-un LAN Ethernet conectat la un modem DSL care oferă gateway-ul spre ISP-ul la distanță. Aceasta permite utilizatorilor conectați prin LAN să aibă acces la Internet de mare viteză folosind conexiunea PPPoE a serverelor iSeries. Odată ce conexiunea dintre iSeries și ISP a început, utilizatori individuali de pe LAN pot accesa ISP prin PPPoE, folosind adresa IP alocată serverului iSeries. Pentru a oferi securitate adițională, reguli de filtrare pot fi aplicate liniei virtuale PPPoE pentru a restricționa un anumit trafic Internet de intrare.

Exemplu de configurare:

1. Configurați dispozitivul de conexiune pentru folosire cu ISP-ul dvs.
2. Configurați un Profil conexiune Generator pe serverul iSeries.
 - Asigurați-vă că ați introdus următoarele informații:
 - **Tip protocol:** PPP

- **Tip conexiune:** PPP peste Ethernet
 - **Mod operare:** Inițiator
 - **Configurație legătură:** linie singulară
3. În pagina **General** a Proprietăți profil punct-la-punct nou, introduceți un nume și o descriere pentru profilul generatorului. Acest nume se va referi la profilul conexiunii și la linia PPPoE virtuală.
 4. Selectați pagina **Conexiune**. Alegeți **Nume linie virtuală PPPoE**, care corespunde numelui pentru acest profil de conexiune. După ce selectați linia, iSeries Navigator va afișa dialogul proprietăți linie.
 - a. Pe pagina **General**, introduceți o descriere relevantă pentru linia virtuală PPPoE.
 - b. Selectați pagina **Legătură**. Din numele liniei fizice alegeți listă, alegeți linia Ethernet pe care o va folosi această conexiune și apăsați pe **Deschide**. Alternativ, dacă aveți nevoie să definiți o nouă linie Ethernet, introduceți numele liniei și apăsați pe **Nou**. iSeries Navigator va afișa dialogul proprietăți linie Ethernet. **Notă:** PPPoE cere adaptor Ethernet tip 2838.
 - 1) Pe pagina **General**, introduceți o descriere relevantă pentru linia Ethernet și verificați dacă definiția liniei folosește resursele hardware dorite.
 - 2) Selectați pagina **Legătură**. Introduceți proprietățile pentru linia Ethernet fizică. Consultați documentația plăcii dvs. Ethernet și ajutorul online pentru informații suplimentare.
 - 3) Selectați pagina **Altele**. Specificați nivelul de acces și autorizație pe care îl pot avea alți utilizatori pentru această linie.
 - 4) Selectați **OK** pentru a vă întoarce la pagina proprietăți linie virtuală PPPoE.
 - c. Selectați **Limite** pentru a defini proprietăți pentru autentificarea LCP sau apăsați **OK** pentru a vă întoarce la pagina **Conexiune** profil punct-la-punct nouă.
 5. Dacă ISP-ul dvs. cere ca serverul iSeries să se autentifice sau dacă vreți ca iSeries să autentifice serverul la distanță, selectați pagina **Autentificare**. Pentru informații suplimentare, consultați Autentificare sistem.
 6. Selectați pagina **Setări TCP/IP** și specificați parametrii Tratare adresă IP pentru acest profil conexiune. Pentru a permite utilizatorilor legați în LAN să se conecteze la ISP folosind adresele IP alocate de serverul iSeries, selectați **Ascundere adrese (Mascare totală)**.
 7. Selectați pagina **DNS**, introduceți adresa IP a serverului DNS furnizat de ISP.
 8. Dacă vreți să specificați subsistemul care va rula jobul conexiune, selectați pagina **Altele**.
 9. Apăsați **OK** pentru încheierea profilului.

Pentru informații despre restricționarea accesului utilizatorilor la adrese IP sau resurse iSeries externe, consultați Filtrare IP și Politici de acces de grup.

Scenariu: Conectarea clienților dial-in la distanță la serverul dvs. iSeries

Situație: Ca administrator al rețelei companiei, trebuie să întrețineți atât serverul iSeries, cât și clienții rețelei. În loc de a vă deplasa pentru depanarea și corectarea problemelor, ați dori să aveți posibilitatea de a lucra de la o locație la distanță, cum ar fi de acasă. Deoarece compania nu are rețeaua conectată la Internet, ați putea să vă conectați la serverul iSeries folosind o conexiune PPP. În plus, singurul modem pe care îl aveți în acest moment este 7852-400 ECS și ați dori să utilizați acest modem pentru conexiunea dvs.

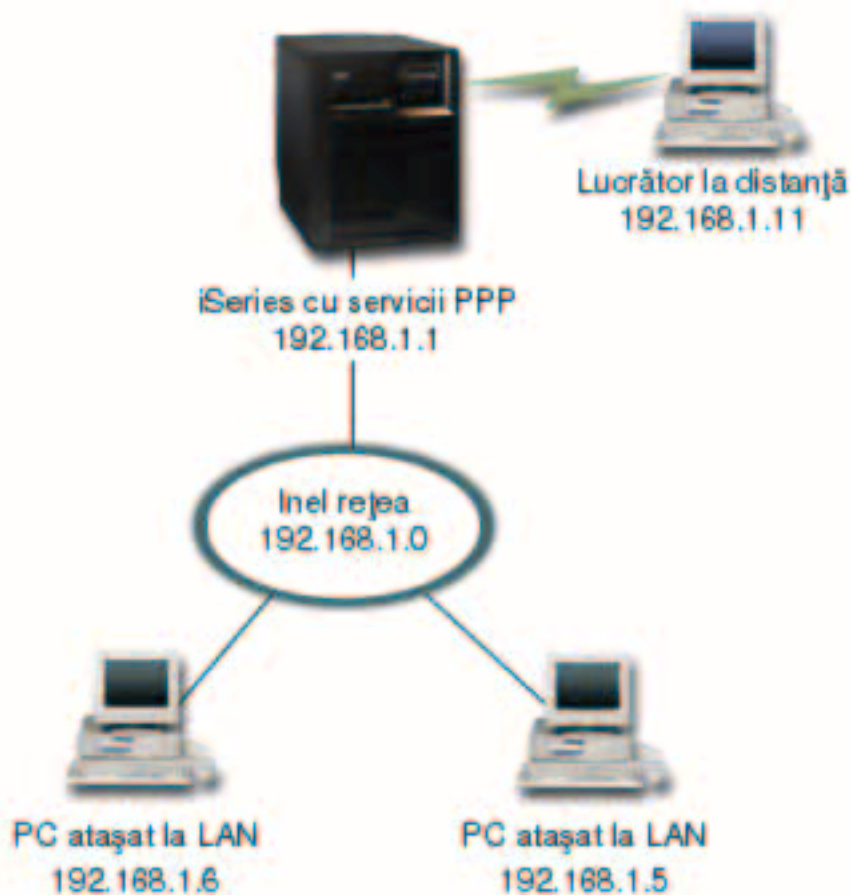


Figura 2. Conectarea clienților la distanță la serverul iSeries

Soluție: Puteți folosi PPP pentru conectarea PC-ului de acasă la serverul iSeries folosind propriul modem. Deoarece folosiți modemul ECS pentru acest tip de conexiune PPP, trebuie să vă asigurați că modemul este configurat atât pentru modul sincron cât și pentru cel asincron. Desenul de mai sus descrie un server iSeries cu servicii PPP care este conectat la un LAN cu două PC-uri. Cel care lucrează la distanță se conectează la serverul iSeries, se autentifică și apoi devine parte a rețelei de lucru (192.168.1.0). În acest caz, este mai simplu să atribuiți o adresă IP statică clientului care se conectează pe linia telefonică.

Cel care lucrează la distanță folosește CHAP-MD5 pentru a se autentifica cu serverul iSeries. iSeries nu poate folosi MS_CHAP, deci trebuie ca clientul PPP să aibă configurată utilizarea CHAP-MD5.

Dacă vreți ca clienții dvs. la distanță să aibă acces la rețeaua companiei așa cum este descris mai sus, trebuie să fie activată "IP forwarding" în stiva TCP/IP și de asemenea în profilul receptor PPP și rutarea IP trebuie configurată corect. Dacă doriți să limitați sau să securizați acțiunile pe care clientul la distanță le poate face în rețea, puteți folosi reguli de filtrare pentru a trata pachetele IP ale acestora.

Desenul de mai sus are un singur client conectat, deoarece modemul ECS nu poate lucra decât cu o singură conexiune la un moment dat. Dacă cerințele dvs. necesită ca mai mulți clienți să fie conectați pe linie telefonică simultan, atunci consultați secțiune planificare pentru considerații hardware și software.

Exemplu de configurare:

1. Configurați Dial-up Networking și creați o conexiune prin linie telefonică pe PC-ul la distanță.
2. Configurați un Profil conexiune receptor pe serverul iSeries.

Asigurați-vă că ați introdus următoarele informații:

- **Tip protocol:** PPP
 - **Tip conexiune:** Linie comutată
 - **Mod operare:** Răspuns
 - **Configurație legătură:** Aceasta ar putea fi linie singură sau un grup de linii, în funcție de mediul dvs.
3. În pagina **General** a Proprietăți profil punct-la-punct nou, introduceți un nume și o descriere pentru profilul receptorului.
 4. Selectați pagina **Conexiune**. Alegeți **Nume linie** corespunzător sau creați unul nou prin tastarea unui nume și apoi apăsați **Nou**.
 - a. În pagina **General**, evidențiați o resursă hardware existentă și setați Framing pe **Asincron**.
 - b. Selectați pagina **Modem**. Din lista de selecție nume, alegeți modemul **IBM 2772**.
 - c. Apăsați **OK** pentru revenire la pagina Proprietăți profil punct-la-punct nou.
 5. Selectați pagina **Autentificare**.
 - a. Selectați **Se cere ca acest server iSeries să verifice identitatea sistemului la distanță**.
 - b. Selectați **Autentificare locală folosind o listă de validare** și adăugați un nou utilizator la distanță în lista de validare.
 - c. Selectați **Acceptare parolă criptată (CHAP-MD5)**.
 6. Selectați pagina **Configurări TCP/IP**.
 - a. Selectați adresa IP locală 192.168.1.1.
 - b. Pentru adresa la distanță, selectați **Adresă IP fixată** cu adresa de pornire 192.168.1.11.
 - c. Selectați **Acceptă ca sistemele la distanță să acceseze alte rețele**.
 7. Apăsați **OK** pentru încheierea profilului.

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

Situație: Aplicația pe care o utilizează compania dvs. cere acum ca utilizatorii să acceseze Internetul. Deoarece aplicația nu cere un schimb mare de date, ați vrea să puteți folosi un modem pentru a conecta serverul iSeries și clienții legați în LAN la Internet. Urmează un exemplu care ilustrează această situație.

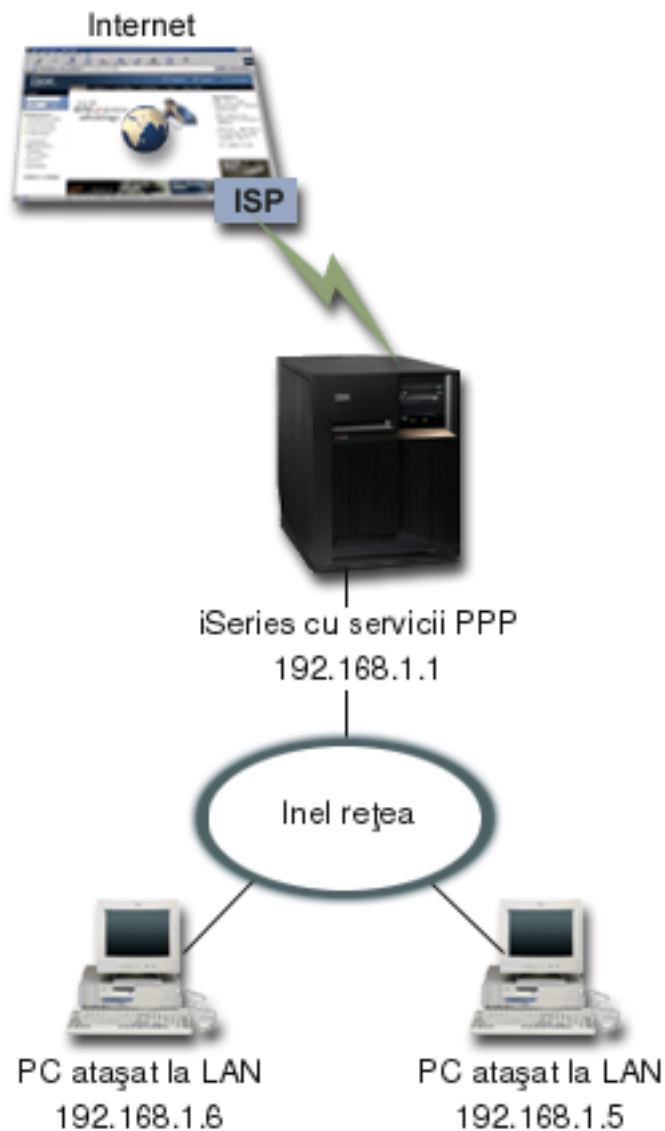


Figura 3. Conectarea LAN de birou la Internet printr-un modem

Soluție: Puteți folosi modemul ECS (sau un altul compatibil) pentru conectarea iSeries la ISP (Furnizorul de Internet). Trebuie să creați un profil generator PPP pe server pentru a stabili conexiunea PPP la ISP.

După realizarea conexiunii între iSeries și ISP, PC-urile atașate la LAN pot comunica cu Internetul folosind iSeries ca gateway. În profilul generator veți dori să vă asigurați că este activată opțiunea Ascundere adrese, astfel încât clienții LAN, care au adrese IP rezervate, să poată comunica cu Internetul.

Acum când iSeries și rețeaua sunt atașate la Internet, trebuie să înțelegeți riscurile de securitate. Consultați ISP pentru a înțelege politicile lor de securitate și luați și alte măsuri pentru a vă proteja serverul și rețeaua.

Dacă folosiți modemul dvs. ECS pentru acest tip de conexiune PPP, configurați-vă modemul pentru comunicație asincronă. În funcție de modul de utilizare a Internetului, lărgimea de bandă ar putea deveni o problemă. Pentru a afla mai multe despre cum să creșteți lărgimea de bandă a conexiunii dvs., consultați secțiunea planificare.

Exemplu de configurare:

1. Configurați un Profil conexiune generator pe serverul iSeries.
Asigurați-vă că ați selectat următoarele informații:
 - **Tip protocol:** PPP
 - **Tip conexiune:** Linie comutată
 - **Mod operare:** Conectare pe linie telefonică
 - **Configurație legătură:** Aceasta ar putea fi linie singulară sau grup de linii, în funcție de mediul dvs.
2. În pagina **General** a Proprietăți profil punct-la-punct nou, introduceți un nume și o descriere pentru profilul generatorului.
3. Selectați pagina **Conexiune**. Alegeți Nume linie corespunzător sau creați unul nou prin tastarea unui nume și apoi apăsați **Nou**.
 - a. În pagina **General** a proprietăților pentru noua linie, evidențiați o resursă hardware existentă și setați Framing în **Asincron**.
 - b. Selectați pagina **Modem**. Din lista de selecție nume, alegeți modemul pe care îl folosiți.
 - c. Apăsați **OK** pentru revenire la pagina Proprietăți profil punct-la-punct nou.
4. Apăsați **Adăugare** și tastați numărul de telefon pentru a vă conecta pe linie telefonică la serverul ISP. Asigurați-vă că ați inclus prefixele necesare.
5. Selectați pagina **Autentificare**, selectați **Permite sistemului la distanță să verifice indentitatea acestui server iSeries**. Selectați protocolul de autentificare și introduceți informațiile despre nume sau parolă necesare.
6. Selectați pagina Configurări TCP/IP.
 - a. Selectați **Atribuit de sistemul la distanță** pentru adresele IP locale și la distanță.
 - b. Selectați **Adăugare sistem la distanță ca rută implicită**.
 - c. Activați **Ascundere adrese** pentru ca adresele IP interne să nu fie rulate pe Internet.
7. Selectați pagina **DNS**, introduceți adresa IP a serverului DNS furnizat de ISP.
8. Apăsați **OK** pentru încheierea profilului.

Pentru a folosi profilul de conexiune pentru conectarea la Internet, efectuați clic-dreapta pe profilul de conexiune din Navigator operații și selectați **Start**. Conexiunea este realizată cu succes când starea se schimbă în **Activ**. Reîmprospătați pentru a actualiza afișajul.

Notă: Trebuie să vă asigurați și că celelalte sisteme din rețea au rutarea corectă definită astfel încât traficul TCP/IP către Internet de la aceste sisteme va fi trimis serverului iSeries.

Scenariu: Conectarea rețelei companiei și rețelele la distanță cu un modem.

Situație: Să presupunem că aveți Intranetul companiei și rețeaua unei filiale în două locații diferite. În fiecare zi, filiala trebuie să se conecteze la sediul central pentru schimb de informații baze de date pentru aplicațiile lor de introducere de date. Cantitatea de date schimbată nu justifică achiziționarea unei conexiuni fizice de rețea, astfel încât vă decideți să folosiți modemuri pentru conectarea celor două rețele.

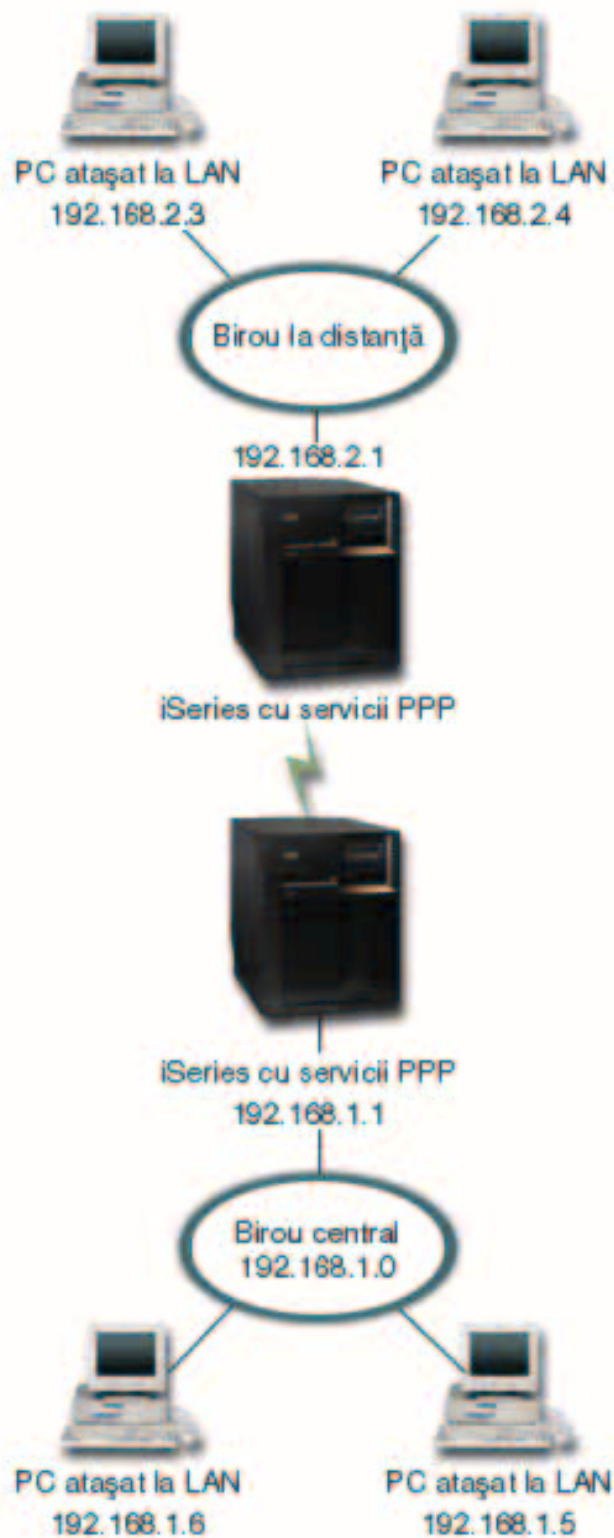


Figura 4. Conectarea Intranetului companiei și a rețelelor la distanță printr-un modem

Soluție: PPP poate conecta cele două LAN-uri prin stabilirea unei conexiuni între fiecare server iSeries ca în desenul de mai sus. În acest caz, presupuneți că biroul la distanță inițiază conexiunea cu biroul central. Veți configura un profil generator pe iSeries de la distanță și un profil receptor pe serverul din sediul central.

Dacă calculatoarele biroului la distanță au nevoie să acceseze LAN-ul companiei (192.168.1.0), atunci profilul receptor din biroul central trebuie să aibă activată "IP forwarding" și rutarea adreselor IP pentru calculatoare (192.168.2, 192.168.3, 192.168.1.6 și 192.168.1.5 în acest exemplu). De asemenea, trebuie activată "IP forwarding" TCP/IP. Această configurație activează comunicații TCP/IP de bază între LAN-uri. Va trebui să luați în considerare factori de securitate și DNS pentru a hotărî numele gazdă între rețelele locale.

Exemplu de configurare:

1. Configurați un Profil conexiune generator pe serverul iSeries al sediului la distanță.
Asigurați-vă că ați selectat următoarele informații:
 - **Tip protocol:** PPP
 - **Tip conexiune:** Linie comutată
 - **Mod operare:** Conectare pe linie telefonică
 - **Configurație legătură:** Aceasta ar putea fi linie singură sau grup de linii, în funcție de mediul dvs.
2. În pagina **General** a Proprietăți profil punct-la-punct nou, introduceți un nume și o descriere pentru profilul generatorului.
3. Selectați pagina **Conexiune**. Alegeți Nume linie corespunzător sau creați unul nou prin tastarea unui nume și apoi apăsând **Nou**.
 - a. În pagina **General** a proprietăților pentru noua linie, evidențiați o resursă hardware existentă și setați Framing în **Asincron**.
 - b. Selectați pagina **Modem**. Din lista de selecție Nume, alegeți modemul pe care îl folosiți.
 - c. Apăsați **OK** pentru revenire la pagina Proprietăți profil punct-la-punct nou.
4. Apăsați **Adăugare** și tastați numărul de telefon pentru a vă conecta pe linie telefonică la serverul iSeries al sediului central. Asigurați-vă că ați inclus prefixele necesare.
5. Selectați pagina **Autentificare** și selectați **Permite sistemului la distanță să verifice identitatea acestui server iSeries**. Selectați **Necesită parolă criptată (CHAP-MD5)** și introduceți informațiile despre nume sau parolă necesare.
6. Selectați pagina **Configurări TCP/IP**.
 - a. Pentru adrese IP locale, selectați adresa IP a interfeței LAN a sediului la distanță (192.168.2.1) din caseta de selecție **Utilizare adresă IP fixată**.
 - b. Pentru adresa IP la distanță, selectați **Atribuit de sistemul la distanță**.
 - c. În secțiunea de rutare, selectați **Adăugare sistem la distanță ca rută implicită**.
 - d. Apăsați **OK** pentru încheierea profilului inițiator.
7. Configurați un **Profil conexiune receptor** pe serverul iSeries al sediului central.
Asigurați-vă că ați selectat următoarele informații:
 - **Tip protocol:** PPP
 - **Tip conexiune:** Linie comutată
 - **Mod operare:** Răspuns
 - **Configurație legătură:** Aceasta ar putea fi linie singură sau grup de linii, în funcție de mediul dvs.
8. În pagina **General** a Proprietăți profil punct-la-punct nou, introduceți un nume și o descriere pentru profilul receptorului.
9. Selectați pagina **Conexiune**. Alegeți Nume linie corespunzător sau creați unul nou prin tastarea unui nume și apoi apăsând **Nou**.
 - a. În pagina **General**, evidențiați o resursă hardware existentă și setați Framing în **Asincron**.
 - b. Selectați pagina **Modem**. Din lista de selecție Nume, alegeți modemul pe care îl folosiți.
 - c. Apăsați **OK** pentru revenire la pagina Proprietăți profil punct-la-punct nou.
10. Selectați pagina **Autentificare**.
 - a. Bifați **Se cere ca acest server iSeries să verifice identitatea sistemului la distanță**.
 - b. Adăugați un nou utilizator la distanță în lista de validare.

- c. Verificați autentificarea CHAP-MD5.
11. Selectați pagina **Configurări TCP/IP**.
- Pentru adresele IP locale, selectați adresa IP a interfeței sediului central (192.168.1.1) din caseta de selecție.
 - Pentru adresa IP la distanță, selectați **Pe baza ID utilizator al sistemului la distanță**. Va apare dialogul Adrese IP definite de nume utilizator. Apăsați **Adăugare**. Completați câmpurile nume utilizator, adresă IP și mască subrețea pentru Apelant. În acest scenariu, ar putea fi indicate următoarele:
 - Nume utilizator apelant: Locație_la_distanță
 - Adresă IP: 192.168.2.1
 - Mască subrețea: 255.255.255.0

Apăsați **OK** și apoi apăsați din nou **OK** pentru a reveni la pagina Configurări TCP/IP.
 - Selectați **IP forwarding** pentru a permite altor sisteme din rețea să folosească aceste servere iSeries ca gateway.
12. Apăsați **OK** pentru încheierea profilului receptor.

Scenariu: Autentificarea conexiunilor dial up cu RADIUS NAS

Situație: Rețeaua companiei dvs. are utilizatori la distanță ce se conectează la două servere iSeries dintr-o rețea dial-up distribuită. Ați vrea un mod de a centraliza autentificarea, serviciile și contabilitatea, permițând unui server să manipuleze cereri de validare ID și parolă utilizator și să determine care adrese IP sunt ale lor.

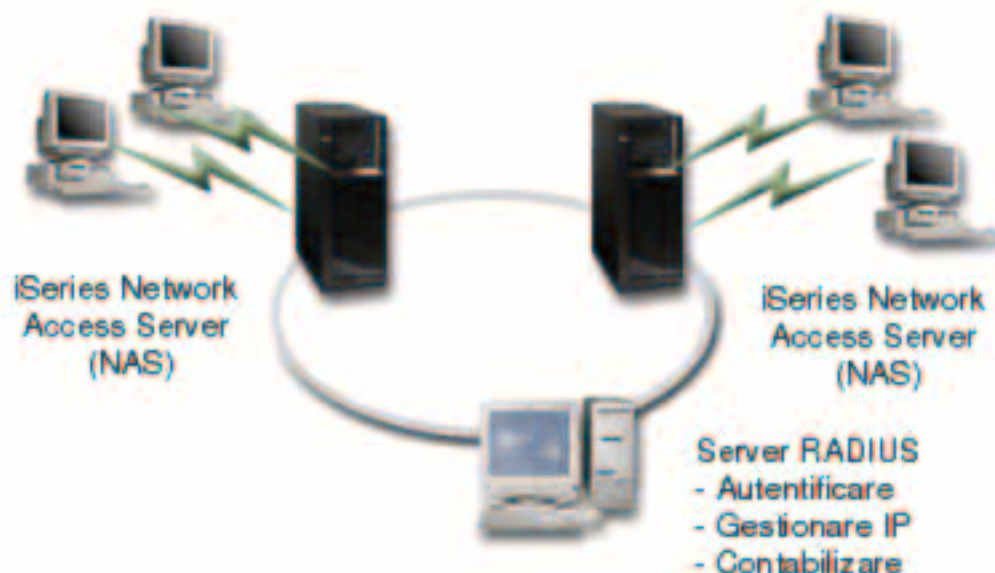


Figura 5. Autentificarea conexiunilor dial up cu un server RADIUS

Soluție: Când utilizatorii încearcă să se conecteze, Serverul de acces la rețea (NAS) ce rulează pe serverele iSeries expediază informațiile de autentificare la un server RADIUS din rețea. Serverul RADIUS, care menține toate informațiile de autentificare pentru rețeaua dvs., procesează cererile de autentificare și răspunsurile. Dacă utilizatorul este validat, serverul RADIUS poate fi de asemenea configurat să asocieze adresa IP a perechii și poate activa contabilizarea pentru a urmări activitatea și funcționarea utilizatorilor. Pentru a suporta RADIUS, trebuie să definiți serverul RADIUS NAS pe iSeries.

Exemplu de configurare:

1. În iSeries Navigator, expandați **Rețea** , dați clic–dreapta pe **Servicii de acces la distanță** și selectați **Servicii**.
2. În fișa **RADIUS** , selectați **Activează conexiunea Server acces rețea RADIUS** și **Activează RADIUS pentru autentificare**. În funcție de soluția RADIUS, puteți de asemenea alege ca RADIUS să trateze contabilizarea conexiunilor și configurarea adreselor TCP/IP.
3. Apăsați pe butonul **Setări RADIUS NAS**.
4. Pe pagina **General** , introduceți o descriere pentru acest server.
5. Pe pagina(le) Server autentificare (și opțional Server contabilizare), apăsați pe **Adăugare** și introduceți următoarele informații:
 - a. În caseta **Adresă IP locală** , introduceți adresa IP pentru interfața iSeries folosită pentru conectare la serverul RADIUS.
 - b. În **Caseta adresă IP server**, introduceți adresa IP pentru serverul RADIUS.
 - c. În caseta **Parolă** , introduceți parola folosită pentru a identifica serverul iSeries pentru serverul RADIUS.
 - d. În caseta **Port**, introduceți portul de pe iSeries folosit pentru a comunica cu serverul RADIUS. Introduceți portul 1812 pentru serverul de autentificare sau 1813 pentru serverul de contabilizare.
6. Apăsați **OK**.
7. În iSeries Navigator, expandați **Rețea > Servicii de acces la distanță**.
8. Selectați profilul conexiune care va folosi serverul RADIUS pentru autentificare. Serviciile RADIUS sunt aplicabile doar pentru profile conexiune Receptor.
9. Pe pagina Autentificare, selectați **Se cere ca acest server iSeries să verifice identitatea sistemului la distanță**.
10. Selectați **Autentificare la distanță folosind server RADIUS**.
11. Selectați protocolul de autentificare. (EAP, PAP sau CHAP-MD5) Acest protocol trebuie folosit și de serverul RADIUS. Consultați Autentificare sistem pentru informații suplimentare.
12. Selectați **Folosire RADIUS pentru editarea și contabilizarea conexiunii** .
13. Apăsați pe **OK** pentru a salva schimbările profilului conexiune.

Trebuie de asemenea să setați serverul RADIUS, incluzând suport pentru protocolul de autentificare, parole și informații de contabilizare. Consultați vânzătorul dvs. RADIUS pentru mai multe informații.

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

Scenariu: Gestionarea accesului utilizatorilor la distanță la resurse folosind Politici de grup și filtrare IP

Situație: Rețeaua dvs. are mai multe grupuri de utilizatori distribuiți și fiecare din ei are nevoie de acces la resurse diferite din LAN-ul companiei. Un grup de utilizatori are nevoie de acces la baza de date și încă alte câteva aplicații, în timp ce un partener de afaceri are nevoie de acces dial-up la servicii HTTP, FTP și Telnet, dar din motive de securitate nu trebuie să îi fie permis accesul la alte servicii TCP/IP sau trafic. Definirea detaliată a atributelor conexiunii și a permisiunilor pentru fiecare utilizator ar mări eforturile dvs. și furnizarea restricțiilor de rețea pentru toți utilizatorii acestui profil conexiune nu ar oferi destul control. Ați prefera un mod de a defini setările și permisiunile conexiunii pentru mai multe grupuri distincte de utilizatori care apelează acest server frecvent.



Figura 6. Aplicați setările de conexiune la conexiunile dial-up pe baza setărilor politicii de grup.

Soluție: Trebuie să aplicați restricții de filtrare IP unice asupra a două grupuri diferite de utilizatori. Pentru a realiza aceasta, veți crea politici de acces de grup și reguli de filtrare IP. Politicile de acces de grup fac referință la regulile de filtrare IP, deci trebuie să creați mai întâi regulile de filtrare. În acest exemplu, trebuie să creați un filtru PPP pentru a include reguli de filtrare IP pentru Politica de acces de grup "Partener de afaceri". Aceste reguli de filtrare vor permite serviciile HTTP, FTP și Telnet, dar vor restricționa accesul la alte servicii și trafic TCP/IP prin serverul iSeries. Acest scenariu arată numai regulile filtru necesare pentru grupul vânzări; totuși puteți de asemenea să setați filtre similare pentru grupul "Intrare date".

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

Exemplu de configurare:

1. Creați identificatorul filtru PPP și filtrele reguli pachet IP care specifică permisiunile și restricțiile pentru această politică de acces de grup. Pentru informații suplimentare despre filtrarea IP, vedeți Reguli pachet IP (Filtrare și NAT) .
 - a. În iSeries Navigator, expandați **Rețea > Servicii de acces la distanță**.
 - b. Apăsați pe **Profiluri conexiune receptor**, clic-dreapta pe profilul conexiune pentru această conexiune și selectați **Proprietăți**.
 - c. Selectați fișa **Setări TCP/IP** și apăsați pe **Avansat**.
 - d. Selectați **Folosește reguli pachet IP pentru această conexiune** și apăsați **Editare fișier reguli**. Aceasta va porni Editorul de reguli pachet IP și va deschide fișierul de reguli pachet pentru filtre PPP.
 - e. Deschideți meniul **Inserare** și selectați **Filtre** pentru a adăuga seturi de filtre. Folosiți fișa **General** pentru a defini seturile de filtre și fișa **Servicii** pentru a defini serviciul pe care îl permiteți, ca HTTP. Următorul set filtru, "services_rules", va permite serviciile HTTP, FTP și Telnet. Regulile filtru includ o declarație de negare implicită, restricționând orice serviciu TCP/IP sau trafic IP care nu sunt permise în mod specific.

Notă: Adresele IP din următorul exemplu sunt rutabile global și 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
```

```
FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR = %
* DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * 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 = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT %
= * FRAGMENTS = NONE JRN = OFF
```

```
FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR %
= 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT %
= 23 FRAGMENTS = NONE JRN = OFF
```

- f. Deschideți meniul **Inserare** și selectați **Interfață filtru**. Folosiți interfața filtru pentru a crea un identificator filtru PPP și includeți seturile filtru pe care le-ați definit.

- 1) În fișa **General**, introduceți

```
permitted_services
```

pentru identificatorul filtru PPP.

- 2) În fișa **Seturi filtru**, alegeți setul filtru **services_rules** și apăsați pe **Adăugare**.

- 3) Apăsați pe **OK**. Următoarea linie va fi adăugată la fișierul de reguli:

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

```
FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

- g. Salvați schimbările și ieșiți. Dacă trebuie să anulați aceste schimbări mai târziu, folosiți interfața pe bază de caractere pentru a introduce comanda:

```
RMVTCPTBL
```

Aceasta va înlătura toate regulile filtru și NAT de pe server.

- h. În dialogul **Setări TCP/IP avansate**, lăsați goală căsuța **Identificator filtru PPP** și apăsați pe **OK** pentru a ieși. Ulterior ar trebui să aplicați identificatorul filtru pe care tocmai l-ați creat unei Politici de acces de grup, nu acestui profil conexiune.

2. Definiți o nouă Politică de acces de grup pentru acest grup utilizatori. Pentru o descriere detaliată a opțiunilor pentru Politici de acces de grup, vedeți Configurare politică de acces de grup.

- a. În iSeries Navigator, expandați **Rețea > Servicii de acces la distanță > Profiluri conexiune receptor**.
 - b. Clic dreapta pe icoana Politică de acces de grup și selectați Politică de acces de grup nouă. iSeries Navigator va afișa dialogul definiție Politică de acces de grup nouă.
 - c. Pe pagina General, introduceți un nume și o descriere pentru Politica de acces de grup.
 - d. Pe pagina **Setări TCP/IP** :
 - Selectați **Folosește reguli pachet IP pentru această conexiune** și selectați identificatorul filtru **PPP permitted_services**.
 - e. Selectați **OK** pentru a salva Politica de acces de grup
3. Aplicați Politica de acces de grup utilizatorilor asociați acestui grup.
 - a. Deschideți Profil conexiune receptor care controlează aceste conexiuni dial-up.
 - b. Pe pagina **Autentificare** a Profilului conexiune receptor, selectați lista de validare care conține informația de autentificare a utilizatorilor și apăsați pe **Deschide**.
 - c. Selectați un utilizator din grupul Vânzări asupra căruia vreți să aplicați Politica de acces de grup și apăsați pe **Deschide**.
 - d. apăsați pe **Aplică o politică de grup utilizatorului** și selectați Politica de acces de grup definită la pasul 2.
 - e. Repetați pentru fiecare utilizator Vânzări.

Pentru informații suplimentare despre autentificarea utilizatorilor printr-o conexiune PPP, vedeți Autentificare sistem.

Capitol 4. Concepte PPP

Puteți folosi PPP pentru a conecta un server iSeries la rețele de la distanță, PC-uri ale clienților, alt iSeries sau un ISP. Pentru a utiliza pe deplin acest protocol, ar trebui să înțelegeți capacitățile și suportul iSeries pentru acest protocol. Consultați următoarele subiecte pentru informații suplimentare.

Ce este PPP?

Protocolul punct-la-punct (PPP) este un protocol TCP/IP folosit să conecteze un calculator la altul. Vedeți acest subiect pentru o definiție mai detaliată.

Profile de conexiuni

Profilurile conexiune punct-la-punct definesc un set de parametri și resurse pentru conexiuni PPP specifice. Puteți porni profile care folosesc aceste setări de parametri pentru a apela (iniția) sau pentru a aștepta (recepționa) conexiuni PPP.

Politici de acces de grup

Aceste politici definesc un set de atribute de conexiune și securitate pentru un grup de utilizatori. Vedeți acest subiect pentru informații despre definirea acestora pe sistemul dvs.

Ce este PPP?

Calculatoarele folosesc **PPP** sau **Protocolul Punct-la-punct**, pentru a comunica pe Internet prin linii telefonice. O conexiune PPP există atunci când două sisteme sunt conectate fizic printr-o linie telefonică. Puteți folosi PPP pentru a conecta un sistem la altul. De exemplu, o conexiune PPP stabilită între un sediu central și un sediu filială permite ambelor sedii să transfere date celuilalt prin rețea.

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

PPP permite interoperabilitatea între software-ul de acces la distanță al diferiților fabricanți. De asemenea, permite și ca protocoale multiple de comunicație în rețea să folosească aceeași linie fizică de comunicație.

Următoarele standarde RFC (Request For Comment) descriu protocolul PPP. Puteți găsi mai multe informații despre RFC la <http://www.rfc-editor.org>.

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

Profile de conexiuni

V5R2 folosește două tipuri de profile pentru a vă permite să definiți un set de caracteristici pentru o conexiune PPP sau set de conexiuni.

- **Profile conexiune inițiator** sunt conexiuni punct-la-punct care provin de la serverul iSeries local și care sunt receptate de un sistem la distanță. Puteți configura conexiunile care trebuie inițiate folosind acest obiect.
- **Profile conexiune receptor** sunt conexiuni punct-la-punct care provin de la un sistem la distanță și care sunt receptate de serverul iSeries local. Puteți configura conexiunile care trebuie receptate folosind acest obiect.

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

- Ce tip de protocol de conexiune veți folosi? (PPP sau SLIP)
- Serverul iSeries contactează celălalt calculator prin apel telefonic în afară (generator)? Serverul iSeries așteaptă primirea unui apel de la celălalt sistem (receptor)?

- Ce linie de comunicație va folosi conexiunea?
- Cum ar trebui serverul iSeries să determine adresa IP pe care o va folosi?
- Cum ar trebui serverul iSeries să autentifice un alt sistem? Unde ar trebui ca serverul iSeries să memoreze informațiile de autentificare?

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

- Tip linie și profil
- Configurări multilink
- Numere de telefon la distanță și opțiuni de apelare.
- Autentificare
- Setări TCP/IP: adrese și rutare IP și filtrare IP.
- Control funcționare și personalizare conexiune
- Servere nume domeniu

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

- **Tip protocol.** Puteți opta între PPP și SLIP. IBM recomandă utilizarea PPP de fiecare dată când este posibil.
- **Selectare mod.** Tipul de conexiune și modul de operare pentru acest profil de conexiune.

Tip conexiune specifică tipul de linie pe care se bazează conexiunile și dacă acestea sunt **dial (apel)** sau **answer (răspuns)** (generator sau, respectiv, receptor). Puteți selecta dintre aceste tipuri de conexiune:

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

PPPoE este suportat numai pentru profiluri conexiune Generator.

- **Mod de funcționare.** Modul de funcționare disponibil depinde de tipul conexiunii. Consultați următorul tabel:

Consultați următorul tabel pentru profiluri conexiune Generator:

Tabela 1. Moduri de funcționare disponibile pentru profiluri conexiune Receptor.

Tip conexiune	Moduri de funcționare disponibile
Linie comutată	<ul style="list-style-type: none"> – Apel – Apel-la-cerere (doar apel) – Apel-la-cerere (pereche dedicată cu răspuns activat). – Apel la cerere (pereche activată la distanță)
Linie închiriată	Inițiator
L2TP	<ul style="list-style-type: none"> – Inițiator – Inițiator multi-hop – Apel la distanță
PPP peste Ethernet	Inițiator

Consultați următorul tabel pentru profiluri conexiune receptor:

Tabela 2. Moduri de funcționare disponibile pentru profiluri conexiune Generator.

Tip conexiune	Moduri de funcționare disponibile
Linie comutată	Răspuns
Linie închiriată	Terminator
L2TP	Terminator (server rețea)

- **Configurare legătură.** Aceasta specifică tipul de serviciu linie folosit de conexiune. Aceste opțiuni depind de tipul selecției de mod ales. Pentru o linie comutată și o linie închiriată puteți alege din următoarele:
 - Linie comutată
 - Grup de linii
 - Linie ISDN integrată

Pentru toate celelalte tipuri de conexiune (închiriată, L2TP, PPPoE) selecția service linie este doar Linie singulară.

Suport politici de grup

Suportul pentru Politici de grup permite administratorilor de rețea să definească politici de grup la nivel de utilizator pentru ajutor în administrarea resurselor și permite ca politicile de control al accesului să fie atribuite utilizatorilor individuali în momentul deschiderii de sesiuni PPP sau L2TP în rețea. Conceptul se referă la faptul că utilizatorii pot fi identificați ca aparținând unei anumite clase de utilizatori, iar fiecare clasă are propria politică unică. Fiecare Politică de acces de grup unică permite definirea limitelor resurselor ca numărul de legături permis într-un buchet multilegături, attribute ca "IP forwarding" și identificarea cărui set de reguli Filtru pachet IP să fie aplicate. Cu suportul pentru Politici de grup, administratorii de rețea pot defini de exemplu un grup `Lucru_acasă` care permite acestei clase de utilizatori accesul complet la rețea, în timp ce un grup `Lucrător_vânzări` ar putea fi restricționat la un set limitat de servicii.

De exemplu, vedeți Scenariu: Gestionarea accesului utilizatorilor la resurse folosind Politici de acces de grup și filtrare adrese IP.

Capitol 5. Plan PPP

Crearea și administrarea conexiunilor PPP cere cunoașterea suportului PPP și alternativelor conexiune din serverele iSeries și de asemenea a multor din planurile de rețea și securitate pe care le folosește afacerea dvs. Următoarele subiecte vă pot ajuta să vă familiarizați cu opțiunile și cerințele disponibile pentru conexiunile PPP iSeries.

Cerințe software și hardware

iSeries Navigator V4R4 sau mai sus suportă conexiuni PPP. Vedeți acest subiect pentru o listă cu alte cerințe.

Alternative conexiune

iSeries suportă conexiuni PPP peste o varietate media, de la liniile telefonice analogice sau digitale, la conexiuni T1 dedicate sau fracționale. Vedeți acest subiect pentru o descriere a opțiunilor de conexiune suportate.

Echipament conexiune

Serverele iSeries folosesc modem-uri, adaptoare terminale ISDN, adaptoare Token Ring, adaptoare Ethernet sau dispozitive CSU/DSU pentru a trata conexiuni PPP. Vedeți acest subiect pentru informații despre hardware suportat.

Tratare adresă IP

Conexiunile PPP au mai multe opțiuni pentru alocarea adreselor IP și filtrarea pachetelor IP în timpul conexiunilor. Vedeți acest subiect pentru descrieri ale acestor opțiuni.

Autentificare sistem

iSeries poate autentifica conexiuni dial-up folosind ori o listă de validare și schimbul de parole, ori un server RADIUS. De asemenea oferă informații de autentificare sistemelor la care se conectează. Vedeți acest subiect pentru o descriere a opțiunilor de autentificare.

Considerații lărgime de bandă

iSeries suportă protocolul multilegătură pentru conexiuni PPP. Aceasta vă permite să folosiți mai multe linii telefonice analogice pentru o singură conexiune pentru a crește lățimea de bandă. Vedeți acest subiect pentru o privire generală asupra acestui suport.

Cerințe software și hardware

Un mediu PPP necesită două sau mai multe calculatoare care suportă PPP. Unul din aceste calculatoare, serverul iSeries, poate fi fie generatorul, fie receptorul. Serverul iSeries trebuie să îndeplinească următoarele cerințe preliminare pentru a putea fi accesat de sistemele la distanță.

- **Navigator operații** Versiunea 4 Ediția 4 (V4E4) sau ulterior cu suport TCP/IP
- Unul din cele două profile de conexiune:
 - Un Profil conexiune generator pentru tratarea conexiunilor PPP care trebuie expediate
 - Un Profil conexiune receptor pentru tratarea conexiunilor PPP care trebuie primite
- O consolă stație de lucru PC ce are instalat **iSeries Access pentru Windows (95/98/NT/Millennium/2000/XP)** cu iSeries Navigator.
- Un adaptor instalat

Puteți alege unul din următoarele adaptoare:

 - 2699*: Two-line WAN IOA
 - 2720*: PCI WAN/Twinaxial IOA
 - 2721*: PCI Two-line WAN IOA
 - 2745*: PCI Two-line WAN IOA (înlocuiește IOA 2721)
 - 2742*: two line IOA (înlocuiește IOA 2745)
 - 2750: PCI ISDN V.90 Basic Rate Interface U IOA (interfață 2-wire)
 - 2751: PCI ISDN V.90 Basic Rate Interface U IOA (interfață 4-wire)
 - 2761: Eight-port analog modem IOA

- 2771: Two-port WAN IOA, cu un modem integrat V.90 la portul 1 și o interfață standard de comunicații la portul 2. Pentru a folosi portul 2 al adaptorului 2771, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător.
- 2772: Two port V.90 integrated modem WAN IOA
- 2838: Adaptor Ethernet pentru conexiuni PPPoE.
- 2793*: Two-port WAN IOA, cu un modem integrat V.92 la portul 1 și o interfață standard de comunicații la portul 2. Pentru a folosi portul 2 al adaptorului 2793, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător. Acesta înlocuiește IOA model 2771.
- 2805 Four port WAN IOA, cu un modem analog V.92 integrat. Acesta înlocuiește modelele 2761 și 2772.

* Aceste adaptoare cer un modem V.90 extern (sau mai sus) sau adaptor terminal ISDN și un cablu RS232 sau compatibil.

- Unul din următoarele, în funcție de tipul de conexiune și linie:
 - modem intern sau extern sau CSU (channel service unit)/DSU (data service unit)
 - adaptor terminal ISDN (integrated services digital network)
- Dacă doriți să vă conectați la Internet, trebuie să aveți și un cont pentru conectarea pe linie telefonică cu un ISP (Furnizor de Internet). ISP ar trebui să vă ofere numerele de telefon și informațiile necesare pentru conectarea la Internet.

Alternative conexiune

PPP poate transmite datagrame prin legături punct-la-punct seriale. PPP permite interconectarea de echipamente ale mai multor fabricanți și protocoale multiple prin standardizarea comunicațiilor punct-la-punct. Nivelul legătură de date al PPP folosește framing stil HDLC pentru încapsularea datagramelor în legăturile de telecomunicație punct-la-punct sincrone și asincrone.

În timp ce PPP suportă o mare varietate de tipuri de legături, SLIP suportă doar tipuri de legături sincrone. SLIP este folosit în general numai pentru legături analogice. Companiile locale de telefoane oferă servicii de telecomunicații tradiționale într-o scală crescătoare a capacităților și costurilor. Aceste servicii folosesc facilitățile existente de voce ale companiei de telefoane între client și sediul central.

Legăturile PPP stabilesc o conexiune fizică între o gazdă locală și una la distanță. Legăturile cu conectare oferă lărgime de bandă dedicată. Aceste conțin și o varietate de protocoale și rate de date. Cu legăturile PPP, puteți opta între următoarele alternative de conectare:

- Linii telefonice analogice
- Servicii digitale și DDS
- Switched-56
- ISDN
- T1/E1 și T1 fracțional
- Frame Relay
- Suport L2TP (tunel) pentru conexiuni PPP
- Suport PPPoE (DSL) pentru conexiuni PPP

Linii telefonice analogice

Conexiunea analogică, care folosește modemuri pentru transportarea datelor prin linii închiriate sau comutate, stă la baza PPP. Liniile închiriate sunt conexiuni permanente între două locații specificate, în timp ce liniile comutate sunt linii telefonice de voce obișnuite. Cele mai rapide modemuri actuale operează la o rată necomprimată de 56Kbps. Totuși, din cauza raportului semnal-zgomot din circuitele telefonice cu voce necondiționată, această rată nu poate fi atinsă de obicei.

Pretențiile fabricanților de modemi cu rate bps (bit-per-secundă) mai mari se bazează de obicei pe algoritmul de compresie a datelor (CCITT V.42bis) utilizat de aceste modemi. Deși V.42bis are potențialul de a duce la o reducere de patru ori a volumului datelor, compresia depinde de date și rareori atinge chiar și 50%. Datele deja comprimate sau criptate pot chiar să crească când este aplicat V.42bis. X2 sau 56Flex extind rata bps la 56k pentru liniile telefonice analogice. Aceasta este o tehnologie hibridă care necesită ca un capăt al legăturii PPP să fie digital în timp ce celălalt trebuie să fie analog. În plus, rata de 56Kbps este valabilă doar când transferați date de la capătul digital al legăturii la cel analogic. Această tehnologie este potrivită pentru conexiuni cu ISP dacă capătul digital al legăturii și hardware-ul se află la locația lor. În mod obișnuit, vă puteți conecta la un modem analog V.24 printr-o interfață serială RS232 cu un protocol asincron la rate de până la 115.2Kbps.

Standardul V.90 a rezolvat problema compatibilității K56flex/x2. Standardul V.90 este rezultatul unui compromis între taberele x2 și K56flex din industria modemurilor. Prin vizualizarea rețelei telefonice comutate publice ca rețea digitală, tehnologia V.90 poate accelera datele de pe Internet la un calculator la viteze de până la 56Kbps. Tehnologia V.90 diferă de alte standarde deoarece aceasta criptează datele digitale în loc de a le modula așa cum fac modemurile analogice. Transferul datelor este o metodă asimetrică, astfel că transmisiile ascendente (de obicei apăsarea tastelor și comenzi mouse de la un calculator la locația centrală, care necesită o lărgime de bandă mai mică) continuă la ratele convenționale de până la 33.6Kbps. Datele de la un modem sunt transferate ca o transmisie analogică care oglindește standardul V.34. Numai transferul de date descendent profită de ratele mari ale V.90.

Standardul V.92 îmbunătățește V.90 permițând rate upstream de până la 48Kbps. În plus, timpii de conectare pot fi reduși multă parte datorită îmbunătățirilor aduse la procesul hand-shaking și modem-urile care suportă o caracteristică "hold" pot rămâne acum conectate în timp ce linia telefonică acceptă apeluri sau folosește apel în așteptare.

Servicii digitale și DDS

Serviciu digital

Prin serviciul digital, datele sunt transmise de la calculatorul emitentului la sediul central al companiei telefonice, la furnizorul de la distanță, la sediul central și apoi la calculatorul receptorului în format digital. Semnalul digital oferă o lărgime de bandă mult mai mare și o siguranță sporită față 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 și atenuarea semnalului.

DDS

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

Vă puteți conecta la DDS folosind o casetă specială numită CSU/DSU (Channel Service Unit/Data Service Unit), care înlocuiește modemul din scenariul analogic. DDS are limitări fizice care se referă în principal la distanța dintre CSU/DSU și sediul central al companiei telefonice. DDS funcționează cel mai bine când distanța este mai mică de 30,000 picioare. Companiile telefonice pot face adaptări pentru distanțe mai mari prin derivații ale semnalului, dar acest serviciu este mai scump. DDS este cel mai potrivit pentru conectarea a două locații care sunt deservite de același sediu central. Pentru conexiuni între distanțe mari care se întind între mai multe sedii centrale, cheltuielile datorate distanței vor face DDS inaplicabil. În aceste cazuri, Switched-56 poate fi o soluție mai bună. În mod obișnuit, vă puteți conecta la un DDS CSU/DSU prin interfața serială V.35, RS449 sau X:21 cu un protocol sincron la rate de până la 56Kbps.

Switched-56

Când nu aveți nevoie de o conexiune permanentă, puteți economisi bani folosind serviciul digital comutat, care este numit de obicei Switch-56 (SW56). O legătură SW56 este similară setării DDS prin faptul că DTE se conectează la serviciul digital prin intermediul CSU/DSU. Totuși, un CSU/DSU SW56 include un dispozitiv

de la care se introduce numărul de telefon al gazdei la distanță. SW56 vă permite să realizați conexiuni digitale prin apel telefonic la oricare utilizator SW56 de oriunde din țară sau din lume. Un apel SW56 este transportat în rețeaua digitală la distanță ca și un apel vocal digitalizat. SW56 folosește aceleași numere de telefon ca și sistemul telefonic local, iar taxele de utilizare sunt aceleași ca și pentru apeluri vocale. SW56 este doar în rețelele nord americane și este limitat la canale singulare care pot transporta doar date. SW56 este o alternativă pentru locurile unde ISDN nu este disponibil. În mod obișnuit, vă puteți conecta la un SW56 CSU/DSU prin interfața serială V.35 sau RS449 cu un protocol sincron la rate de până la 56Kbps. Cu o unitate de apelare/răspuns V.25bis, controlul datelor și al apelului se face printr-o singură interfață serială.

ISDN

Ca și Switched-56, ISDN oferă conectivitate comutată și între capete digitale. Totuși, spre deosebire de alte servicii, ISDN poate transporta atât voce cât și date prin aceeași conexiune. Există mai multe tipuri de servicii ISDN, dintre care BRI (Basic Rate Interface) este cel mai folosit. BRI este format din două canale B de 64Kbps pentru transportul datelor client și un canal D pentru transportul datelor de semnalizare. Cele două canale B pot fi legate pentru a obține o rată combinată de 128Kbps. În unele zone, compania telefonică poate limita fiecare canal B fie la 56Kbps, fie la 112Kbps în combinație. Există și o restricție fizică, aceea că localizarea clientului trebuie să fie la cel mult 18,000 picioare de comutatorul sediului central. Această distanță poate fi extinsă prin repetoare. Vă puteți conecta la ISDN cu un dispozitiv numit adaptor terminal. Cele mai multe adaptoare terminale au o unitate integrată de sfârșit de rețea (NT1) care permite conexiunea directă la o mufă de telefon. În mod obișnuit, adaptoarele terminale se conectează la calculatorul dvs. printr-o legătură asincronă RS232 și folosesc setul de comenzi AT pentru configurare și control, asemănător cu modemurile analogice convenționale. 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 varietății protocoalelor de adaptare a ratei care erau în V.110 și V.120 ca și schemele de legare pentru cele două canale B.

Industria a convers spre protocol PPP sincron cu PPP Multilink pentru legarea a două canale B. Unii fabricanți de adaptoare terminale integrează capacitatea V.34 (modem analogic) în adaptoarele lor terminale. Aceasta permite clienților cu o singură linie ISDN să folosească atât apeluri ISDN cât și analogice convenționale profitând de capacitățile de simultaneitate voce/date ale serviciilor ISDN. Noua tehnologie permite adaptorului terminal și operarea ca parte server digital pentru clienți 56K(X2/56Flex).

În mod obișnuit, ați dori să vă conectați la un adaptor terminal ISDN printr-o interfață serială RS232 folosind un protocol asincron la rate de până la 230.4Kbps. Totuși, rata în baud maximă a serverului iSeries pentru asincron prin RS232 este de 115.2Kbps. Din păcate, aceasta restricționează rata maximă de transfer de octeți la 11.5k octeți/sec, în timp ce adaptorul terminal cu multi-linking este capabil de 14/16k octeți necomprimați. Unele adaptoare terminale suportă sincron în RS232 la 128Kbps, dar rata maximă în baud a serverului iSeries pentru sincron prin RS232 este de 64Kbps.

Serverul iSeries este capabil de rulare asincronă în V.35 la rate de până la 230.4Kbps, dar fabricanții de adaptoare terminale nu oferă în general o astfel de configurare. Convertoarele de interfață care convertesc RS232 în interfața V.35 ar putea fi o soluție rezonabilă a problemei, dar această abordare nu a fost evaluată pentru serverul iSeries. O altă posibilitate este de a utiliza adaptoarele terminale cu protocolul sincron interfață V.35 la rata de 128Kbps. Deși această clasă de adaptoare terminale există, se pare că nu sunt multe oferte de PPP multilink sincron.

T1/E1 și T1 fracțional

T1/E1

O conexiune T1 unește 24 de canale multiplexate cu diviziunea timpului (TDM) de 64Kbps (DS0) într-un circuit de cupru cu 4 fire. Aceasta creează o lărgime totală de bandă de 1.544Mbps. Un circuit E1 în Europa și alte părți ale lumii unește 32 de canale de 64Kbps într-un total de 2.048Mbps. TDM permite ca mai mulți utilizatori să partajeze un mediu de transmisie digital prin folosirea porțiunilor de timp prealocat. Multe PBX digitale profită de serviciul T1 pentru a importa multiple circuite de apel printr-o singură linie T1 în loc de a

avea 24 de perechi de fire rutate între PBX și compania telefonică. Este important de remarcat faptul că T1 poate fi partajat între voce și date. Un serviciu telefonic poate interveni asupra unui subset din cele 24 de canale ale unei legături T1, de exemplu, lăsând canalele rămase pentru conectarea la Internet. Un dispozitiv multiplexor T1 este necesar pentru administrarea celor 24 de canale atunci când un trunchi T1 este partajat de servicii multiple. Pentru o singură conexiune numai pentru date, circuitul poate fi rulat fără a se face TDM asupra semnalului. În consecință, se poate folosi un dispozitiv CSU/DSU mai simplu. În mod obișnuit, vă puteți conecta la un multiplexor sau CSU/DSU T1/E1 prin interfața serială V.35 sau RS cu protocol sincron la rate care sunt multiplu de 64Kbps până la 1.544Mbps sau 2.048Mbps. Multiplexorul sau CSU/DSU oferă temporizarea în rețea.

T1 fracțional

Cu FT1 (Fractional T1), un client poate închiria orice submultiplu de 64Kbps al unei linii T1. FT1 este util atunci când costul T1 dedicat ar fi prohibitiv pentru lărgimea de bandă efectivă pe care o folosește clientul. Cu FT1, plățiți doar pentru ceea ce aveți 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 distanță al unui circuit FT1 este la un comutator de conectare încrucișată cu acces digital (Digital Access Cross-Connect Switch) care este întreținut de compania telefonică. Sistemele care partajează același comutator digital pot comuta canalele DS0. Această schemă este utilizată de ISP care folosesc un singur trunchi T1 de la locația lor la comutatorul digital al companiei telefonice. În aceste cazuri, clienți multipli pot fi serviți cu serviciul FT1. În mod obișnuit, vă puteți conecta la un multiplexor sau CSU/DSU T1/E1 prin interfața serială V.35 sau RS 449 cu protocol sincron la un multiplu de 64Kbps. Cu FT1, aveți pre-alocat un subset al celor 24 de canale. Multiplexorul T1 trebuie să fie configurat să folosească doar porțiunile de timp care sunt atribuite serviciului dvs.

Frame Relay

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

Rețelele cu Frame Relay din U.S. suportă rate de transfer al datelor cu viteze T-1 (1.544 Mbps) și T-3 (45 Mbps). Vă puteți gândi la Frame Relay ca fiind o modalitate de utilizare a liniilor T-1 și T-3 existente deținute de un furnizor de servicii. Majoritatea companiilor telefonice oferă acum servicii Frame Relay pentru clienții care doresc conexiuni la viteze de între 56 Kbps și T-1. (În Europa, vitezele Frame Relay variază între 64 Kbps și 2 Mbps. În S.U.A., Frame Relay este foarte utilizat deoarece este relativ ieftin. Totuși, acesta este înlocuit în unele zone de tehnologii mai rapide, cum este ATM.

Suport L2TP (tunel) pentru conexiuni PPP

L2TP (Layer 2 Tunneling Protocol) este un protocol tunel care extinde PPP pentru a suporta un tunel la nivel de legătură între un client L2TP care face o cerere (L2TP Access Concentrator sau LAC) și un punct final server destinație L2TP (L2TP Network Server sau LNS). Folosind tunele L2TP, este posibilă separarea locației la care se încheie protocolul de conectare pe linie telefonică de locul de unde este furnizat accesul în rețea, de aceea L2TP este numit și PPP virtual. Protocolul L2TP este referit ca standard Request For Comment RFC2661. Informații suplimentare despre RFC se pot găsi la <http://www.rfc-editor.org>. Un tunel L2TP se poate extinde pe o întreagă sesiune PPP sau doar pe un singur segment al unei sesiuni cu două segmente. Aceasta se poate reprezenta prin patru modele de tunelare diferite:

- Tunel voluntar
- Tunel obligatoriu - apel primit
- Tunel obligatoriu - apel la distanță
- Conexiune L2TP multi-hop.

Tunel voluntar

În modelul tunel voluntar, un tunel este creat de utilizator, de obicei prin folosirea unui client activat L2TP. Prin urmare, utilizatorul va trimite pachete L2TP la ISP (Internet Service Provider), care le va trimite la LNS.

Pentru tunelul voluntar, ISP nu trebuie să suporte L2TP, iar inițiatorul tunelului L2TP se află efectiv pe același sistem ca și clientul la distanță. În acest model, tunelul se extinde peste întreaga sesiune PPP de la clientul L2TP la LNS.

Model tunel obligatoriu - apel primit

În modelul tunel obligatoriu - apel primit, un tunel este creat fără acțiuni ale utilizatorului și fără ca acesta să aibă opțiuni. Prin urmare, utilizatorul va trimite pachete PPP la ISP (LAC), care le va încapsula în L2TP și le va transmite la LNS. În cazurile cu tunel obligatoriu, ISP trebuie să fie capabil de L2TP. În acest model, tunelul se întinde doar pe segmentul sesiunii PPP dintre ISP și LNS.

Model tunel obligatoriu - apel la distanță

În modelul cu tunel obligatoriu - apel la distanță, poarta principală (LNS) inițiază un tunel la un ISP (LAC) și instruește ISP să apeleze clientul care răspunde PPP. Acest model este pentru cazurile în care Clientul care răspunde PPP de la distanță are un număr de telefon permanent cu un ISP. Acest model ar trebui folosit atunci când o companie cu o prezență stabilă pe Internet trebuie să realizeze o conexiune cu un sediu la distanță care necesită o legătură prin linie telefonică. În acest model, tunelul se întinde doar pe segmentul sesiunii PPP dintre LNS și ISP.

Conexiune multi-hop L2TP

O conexiune multi-hop L2TP este un mod de redirecționare a traficului L2TP din partea LAC și LNS client. O conexiune multi-hop este stabilă folosind o poartă multi-hop L2TP (un sistem care leagă profilele L2TP Terminator și Inițiator). Pentru stabilirea unei conexiuni multi-hop, poarta multi-hop L2TP se va comporta ca un LNS pentru un set de LAC cât și ca un LAC pentru un anumit LNS în același moment. Un tunel este stabilit de la un LAC client la o poartă multi-hop L2TP și apoi se stabilește un alt tunel între poarta multi-hop L2TP și un LNS destinație. Traficul L2TP de la LAC client va fi apoi redirecționat de poarta multi-hop L2TP către LNS destinație, iar traficul de la LNS destinație va fi redirecționat la LAC client.

Suport PPPoE (DSL) pentru conexiuni PPP

DSL se referă la o clasă tehnologică folosită pentru a obține mai multă lărgime de bandă pe cablurile telefonice din cupru existente ce se află între un client și un furnizor ISP. Permite servicii vocale și de transmitere a datelor cu viteză mare simultan printr-o singură pereche de fire telefonice din cupru. Vitezele modem-urilor au crescut treptat folosind diferite compresii și alte tehnologii, dar la maximum de azi (56 kbit/s) ele se apropie de limita teoretică pentru această tehnologie. Tehnologia DSL permite viteze mult mai mari de la un capăt la altul al perechii răsucite de linii de la Biroul central acasă, la școală sau afaceri. Viteze de până la 2 Megabiți pe secundă sunt realizabile în unele zone - de 30 de ori mai rapide sau mai mult față de cele mai rapide modem-uri actuale. PPPoE vine de la Protocol punct la punct peste Ethernet (Point to Point Protocol over Ethernet). PPP este de obicei folosit peste comunicații seriale cum sunt conexiunile modem dial-up. Mulți furnizori de servicii Internet DSL folosesc acum PPP peste Ethernet datorită trăsăturilor sale de logare și securitate adăugate. Ce este un modem DSL? Un "modem" DSL este un dispozitiv care este plasat la oricare capăt al liniei telefonice din cupru pentru a permite unui calculator (sau LAN) să fie conectate la Internet printr-o conexiune DSL. Spre deosebire de o conexiune dial up, de obicei nu necesită o linie telefonică dedicată (un splitter permite liniei să fie împărțită simultan). DSL este considerat următoarea generație în tehnologia modem. Deși modem-urile DSL se aseamănă modem-urilor analogice convenționale ele oferă transfer mult mai ridicat.

Echipament conexiune

Acestea sunt cele trei tipuri de echipamente de comunicație pe care le puteți folosi în mediul PPP.

- Modemuri
- CSU/DSU
- Adaptoare terminale ISDN
- Adaptoare tip 2838 Ethernet (pentru conexiuni PPPoE).
-

Modemuri

Pentru conexiuni PPP pot fi folosite atât modemuri interne, cât și externe. Setul de comenzi folosit de un modem este de obicei descris în documentația modemului. Comenzile sunt folosite pentru resetarea și inițializarea modemului și pentru a indica modemului să formeze numărul de telefon al sistemului la distanță. Fiecare model de modem trebuie definit înainte ca acesta să poată fi utilizat cu un profil de conexiune PPP deoarece modelele de modem diferite au șiruri de comenzi de inițializare diferite. Dacă este un modem intern, atunci șirurile modemului sunt deja definite pentru utilizare.

Serverul iSeries are multe modele de modemuri predefinite, iar noile modele pot fi definite în Navigator operații. O definiție existentă poate fi folosită ca bază pentru noul tip care va fi definit. Dacă nu sunteți sigur de comenzile folosite de modemul dvs sau dacă nu aveți acces la documentația modemului, începeți cu definiția modem generic Hayes. Definițiile predefinite livrate nu pot fi modificate. Totuși, pot fi adăugate comenzi suplimentare șirului de apelare sau de comenzi de inițializare.

Puteți folosi modemul ECS (electronic customer support) furnizat cu serverul iSeries pentru a stabili conexiuni PPP. Pe sistemele mai vechi, modemul ECS era un modem extern IBM 7852-400. Pe sistemele mai noi, modemurile interne 2771 sau 2772 ar putea fi folosite ca modem ECS.

CSU/DSU

Un CSU (Channel Service Unit) este un dispozitiv care conectează un terminal la o linie digitală. Un DSU (Data Service Unit) este un dispozitiv care realizează funcții de protecție și diagnostic pentru o linie de telecomunicații. În mod obișnuit, cele două dispozitive formează o singură unitate, CSU/DSU.

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

Adaptoare terminale ISDN

ISDN oferă o conexiune digitală care permite comunicarea folosind orice combinație de voce, date și video, printre alte aplicații multimedia.

Verificați dacă adaptorul terminal poate fi folosit pentru serverul iSeries:

- Recomandări adaptor terminal ISDN listează cel mai bun adaptor terminal care poate fi folosit.
- Restricții adaptor terminal ISDN oferă informații și scurte evaluări ale diferitelor adaptoare terminale ISDN care au fost testate cu serverul iSeries.

Urmați acești pași pentru configurarea adaptorului terminal:

1. În iSeries Navigator, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
2. Efectuați clic-dreapta pe **Modemuri** și selectați **Modem nou**.
3. În caseta de dialog Proprietăți modem nou, introduceți valorile corecte în toate casetele câmp ale fișei General. Asigurați-vă că ați specificat adaptor terminal ISDN ca dispozitiv de comunicare.
4. Selectați fișa **Parametri ISDN**.
5. Adăugați sau modificați proprietățile ISDN din fișa **Parametri ISDN** pentru a corespunde proprietăților necesare pentru adaptorul terminal.

Reluați exemplul Configurarea unui adaptor terminal ISDN pentru exemple de proceduri care folosesc Navigator operații.

Recomandări adaptor terminal ISDN

Adaptorul terminal ISDN extern recomandat sau modem-ul ISDN este **3Com/U.S. Robotics Courier I ISDN V.Everything**. El suportă conexiuni modem analogic V.34, V.90 (X2), V.92 și Multilink PPP peste ISDN în ambele moduri generator și răspuns de pe serverul iSeries. De asemenea, suportă în mod automat CHAP

(Challenge Handshake Authentication Protocol) pentru conexiunea PPP ISDN. Următoarele adaptoare terminale ISDN sunt de asemenea disponibile: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA și ADtran ISU 2x64 Dual Port.

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

Dacă folosiți un modem Courier I anterior 1999, verificați dacă modemul Courier I este conectat la serverul iSeries printr-un cablu V.35 pentru a obține performanțe maxime de la conexiunea ISDN. O RS-232 cu cablu de modem V.35 este furnizată împreună cu modemul Courier I; totuși, versiunile mai vechi ale acestui cablu au un tip greșit de conector V.35. Contactați 3Com/US Robotics Customer Support pentru înlocuire.

Notă: Potrivit 3Com/US Robotics, versiunea V.35 a acestui adaptor terminal nu mai există, deși unele ar mai putea fi găsite la furnizori terță parte. Versiunea RS-232 încă mai este recomandată cu unele performanțe reduse pe serverul iSeries, deoarece conexiunile RS-232 sunt limitate la 115.2 Kb.

Puteți obține un V.35 pentru adaptorul RS-232 și de la Black Box Corporation. Numărul de parte componentă este FA-058.

Asigurați-vă că ați setat viteza liniei V.35 pe serverul iSeries la 230.4 Kbps.

Restricții adaptor terminal ISDN

Au fost evaluate următoarele adaptoare terminale. Acestea sunt recomandate numai pentru generarea conexiunilor la distanță ISDN de la serverul iSeries.

3Com Impact IQ ISDN:

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

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuși, ar putea suporta conexiuni prin modem analogic V.34 folosind conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.
- Adaptorul terminal nu se poate conecta la serverul iSeries cu viteze mai mari de 115200 bps.
- Adaptorul terminal nu suportă automat CHAP (Challenge Handshake Authentication Protocol). Totuși, setarea S84=0 permite efectuarea autentificării server iSeries CHAP.
- Serverul iSeries nu poate determina momentul de încheiere a conexiunii atunci când monitorizează semnalul Data Set Ready de la adaptorul terminal. Aceasta poate duce la o eventuală expunere de securitate a sistemului.

Motorola BitSurfr Pro ISDN:

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

- Adaptorul terminal nu suportă conexiuni prin modem analogic V.34. Totuși, ar putea suporta conexiuni prin modem analogic V.34 folosind conexiunea externă RJ-11.
- Adaptorul terminal nu suportă conexiuni V.90 în acest moment.
- Adaptorul terminal nu se poate conecta la serverul iSeries cu viteze mai mari de 115200 bps.
- Adaptorul terminal nu suportă automat autentificarea CHAP. Totuși, setarea @M2=C permite efectuarea autentificării server iSeries CHAP.

- Adaptorul terminal nu permite în mod automat răspunsul la apeluri single-link și Multilink PPP. Adaptorul terminal generator la distanță trebuie să fie setat pe același protocol (single-link sau Multilink) ca și adaptorul terminal ce răspunde.
- Mecanismul hardware de control al fluxului pentru serverul iSeries nu funcționează bine cu acest adaptor terminal. Aceasta duce la performanțe degradate când serverul iSeries trimite date pe o conexiune Multilink PPP.

Tratare adresă IP

Conexiunile PPP permit mai multe seturi diferite de opțiuni pentru gestiunea adreselor IP în funcție de tipul de profil conexiune care permite gestiunea adresei IP astfel încât conexiunea PPP să funcționeze fără probleme cu arhitectura rețelei existente. Pentru informații despre definirea unei scheme de adresă IP pentru rețeaua dvs., consultați următoarele subiecte:

- DHCP
DHCP poate gestiona centralizat alocările adreselor IP pentru rețeaua dvs. Învățați cum să setați și să gestionați serviciile DHCP pentru rețeaua dvs.
- DNS
DNS vă poate ajuta să gestionați numele de gazdă și adresele IP asociate. Învățați cum să setați și să gestionați servicii DNS pentru rețeaua dvs.
- BOOTP
BOOTP este folosit pentru a asocia stații de lucru client cu serverul dvs. iSeries și pentru a le aloca adrese IP. Învățați cum să setați și să gestionați servicii BOOTP pentru rețeaua dvs.
- Filtrare pachet IP
Restricționați accesul utilizatorilor și grupurilor la adrese IP prin crearea unui fișier de reguli filtru IP. Învățați despre suportul filtru IP și cum să implementați această opțiune în rețeaua dvs.

Ar trebui să fiți familiar cu strategia gestiunii adresei IP din rețeaua dvs. înainte configurării unui profil conexiune PPP. Această strategie va avea impact asupra multor decizii pe parcursul procesului de configurare inclusiv strategia dvs. de autentificare, considerații de securitate și setări TCP/IP.

Profile conexiune generator:

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

Dacă definiți adrese IP fixate pentru adresa IP locală sau la distanță, va trebui să vă fiți sigur că sistemul la distanță are definită acceptarea adreselor pe care le definiți. O aplicație tipică este definirea adresei locale ca adresă IP fixată și cea la distanță să fie atribuită de către sistemul la distanță. Sistemul pe care îl conectați poate fi definit în același mod astfel ca la realizarea conexiunii cele două sisteme să schimbe între ele adresele ca modalitate de învățare a adresei sistemului la distanță. Acest fapt ar putea fi util atunci când un sediu apelează un altul pentru conectivitate temporară.

Un alt aspect este dacă doriți să activați Mascarea adreselor IP. De exemplu, dacă serverul iSeries se conectează la Internet via un ISP, atunci aceasta ar putea permite unei rețele atașate din spatele serverului iSeries să acceseze și ea Internetul. În principiu, serverul iSeries va 'ascunde' adresele IP ale sistemelor din rețeaua din spatele adresei IP locale atribuite de ISP, făcând astfel ca traficul IP să pară ca provenind de la serverul iSeries. Există și aspecte legate de rutare pentru ambele sisteme din LAN (pentru a asigura faptul că traficul lor pe Internet este trimis serverului iSeries) cât și pentru serverul iSeries unde va trebui să activați caseta 'adăugare sistem la distanță ca rută implicită'.

Profile conexiune receptor

Profilurile conexiune receptor au mult mai multe considerații și opțiuni despre adresa IP decât are profilul conexiune generator. Cum vă configurați adresele IP depinde de planul de gestiune al adresei IP pentru rețeaua dvs., performanța specifică și cerințele funcționale pentru această conexiune și planul de securitate.

Adrese IP locale

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

Adrese IP la distanță

Sunt multe opțiuni pentru alocarea adreselor IP la distanță clienților PPP. Următoarele opțiuni pot fi specificate în pagina **TCP/IP** a profilului conexiune receptor.

Notă: Dacă vreți ca sistemul la distanță să fie considerat parte din LAN, ar trebui să configurați rutarea adresei IP, să specificați o adresă IP din intervalul adresei pentru sistemele din LAN, și să verificați activarea "IP forwarding" pentru acest profil conexiune și pentru sistemul iSeries.

Tabela 3. Opțiuni alocare adresă IP pentru conexiuni profil receptor

Opțiune	Descriere
Adresă IP fixă	Definiți singura adresă IP care va fi atribuită utilizatorilor la distanță în momentul conectării pe linie telefonică. Aceasta este o adresă IP doar pentru gazdă (masca subrețea este 255.255.255.255) și este numai pentru profiluri receptor conexiune singulară.
Grup de adrese	Definiți adresa IP de început și apoi un domeniu al numărului de adrese IP suplimentare care se vor defini. Fiecare utilizator care se conectează va primi astfel o adresă unică din domeniul definit. Aceasta este o adresă IP doar pentru gazdă (masca subrețea este 255.255.255.255) și este numai pentru profiluri receptor conexiune multiplă.
RADIUS	Adresa IP la distanță și masca sa de subrețea vor fi determinate de serverul Radius. Aceasta este valabil doar dacă sunt definite următoarele: <ul style="list-style-type: none"> • Suportul Radius pentru autentificare și adresare a fost activat din configurarea serviciilor Server de acces la distanță. • Este activată autentificarea pentru profilul de conexiune receptor și este definită autentificarea la distanță de către Radius.
DHCP	Adresa IP la distanță este determinată de serverul DHCP direct sau indirect prin retransmisie DHCP. Aceasta este valabilă doar dacă suportul DHCP a fost activat din configurația serviciilor Server de acces la distanță. Aceasta este o adresă IP numai pentru gazdă (masca subrețea este 255.255.255.255).
Pe baza ID-ului utilizator al sistemului la distanță.	Adresa IP la distanță este determinată de ID-ul utilizator definit pentru sistemul la distanță atunci când este autentificat. Aceasta permite administratorului să atribuie diferite adrese IP la distanță (și măștile subrețea asociate) utilizatorului care se conectează pe linie telefonică. Aceasta permite de asemenea rutelor adiționale să fie definite pentru fiecare din aceste ID-uri utilizator ca să puteți "croi" mediul pentru utilizatorul la distanță cunoscut. Autentificarea trebuie să fie activată pentru ca această funcție să fie corectă.

Tabela 3. Opțiuni alocare adresă IP pentru conexiuni profil receptor (continuat)

Opțiune	Descriere
Definiți adrese IP suplimentare bazate pe ID-ul utilizator al sistemului la distanță.	Această opțiune permite definirea adreselor pe baza ID utilizator al sistemului la distanță. Această opțiune este selectată automat (și trebuie folosită) dacă alocarea adresei IP la distanță este definită ca fiind Pe baza ID-ului utilizator al sistemului la distanță . Această opțiune este acceptată și pentru metodele de atribuire a adresei Adresă IP fixată și Grup de adrese. Când un utilizator la distanță se conectează la serverul iSeries, se va face o căutare pentru a determina dacă o adresă IP la distanță este definită special pentru acest utilizator. Dacă da, acea adresă, mască și set de rute posibile vor fi folosite pentru conexiune. Dacă utilizatorul nu este definit atunci adresa va avea valoarea implicită definită Adresă IP fixă sau următoarea adresă IP din grupul de adrese IP.
Permite sistemului la distanță să-și definească propria adresă IP	Această opțiune permite ca un utilizator la distanță să își definească propria adresă dacă negociază aceasta. Dacă nu negociază pentru folosirea propriei adrese atunci adresa IP la distanță va fi determinată de metoda de alocare a adresei IP definită la distanță. Această opțiune este inițial dezactivată și aveți grijă înainte de activarea ei.
Rutare adresă IP	Clientul dial-up și iSeries trebuie să aibă rutarea adresei IP configurată corect dacă clientul are nevoie de acces la orice adrese IP de pe LAN-ul de care aparține iSeries.

Filtrare pachet IP

Filtrare pachet IP este mecanismul care poate limita serviciile pentru un utilizator individual când este logat la o rețea. Filtrare pachet poate "Permite" sau "Nega" accesul pe baza adreselor IP și/sau porturilor destinație. Politici diferite sunt aplicate prin definirea de seturi multiple de Reguli de filtrare pachet, fiecare având propriul Identificator filtru PPP unic. Regulile filtru pachet pot fi alocate pentru un profil conexiune receptor particular sau pot fi alocate folosind o politică de grup care ar aplica regulile filtru pentru acea categorie de utilizator. Regulile filtru pachet nu sunt definite în PPP, dar sunt definite sub Reguli pachet IP în iSeries Navigator. Vedeti subiectul din Centrul de informare Reguli pachet IP pentru mai multe informații.

Pentru conexiuni L2TP, trebuie folosit VPN cu filtrare IP SEc pentru a proteja traficul rețelei. Vedeti subiectul din Centru informații VPN pentru informații suplimentare.

Autentificare sistem

Conexiunile PPP cu un server iSeries suportă mai multe opțiuni pentru autentificarea clienților la distanță pentru iSeries și a conexiunilor la un ISP sau alt server pe care îl apelează iSeries. iSeries suportă mai multe metode pentru menținerea informațiilor de autentificare, începând de la simple liste de validare pe iSeries care conțin liste de utilizatori autorizați și parolele asociate, până la suport pentru serverele RADIUS care mențin informații de autentificare detaliate pentru utilizatorii rețelei dvs. iSeries suportă de asemenea mai multe opțiuni pentru criptarea ID-ului utilizator și parolei, începând de la un simplu schimb de parole până la suport macerare cu CHAP-MD5. Vă puteți specifica preferințele pentru autentificarea sistemului, inclusiv un ID utilizator și parolă pentru a valida iSeries la închiderea conexiunii, în fișa **Autentificare** a profilului conexiune din iSeries Navigator.

Pentru mai multe informații despre menținerea validării și a informațiilor de autentificare, consultați :

- RADIUS (Remote Authentication Dial In User Service)
- Listă de validare

Pentru informații suplimentare despre protocoalele de autentificare a parolei, consultați :

- Protocol autentificare dialog de confirmare provocare (Challenge Handshake Authentication Protocol - CHAP-MD5)
- PAP (Password Authentication Protocol)
- EAP (Extensible Authentication Protocol)

CHAP-MD5

Challenge Handshake Authentication Protocol (CHAP-MD5) folosește un algoritm (MD-5) pentru a calcula o valoare care este cunoscută doar de sistemul care autentifică și de dispozitivul la distanță. Cu CHAP, ID-ul utilizator și parola sunt întotdeauna criptate, așa că el este un protocol mai sigur decât PAP. Acest protocol este eficient împotriva playback-ului și încercărilor de acces prin încercare-și-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 distanță care încearcă să se conecteze la rețea. Sistemul la distanță 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.

EAP

EAP (Extensible Authentication Protocol) permite modulelor de autentificare terțe să interacționeze cu implementarea PPP. EAP extinde PPP prin furnizarea unui mecanism suport standard pentru scheme de autentificare cum sunt cartelele cu jeton, Kerberos, Public Key și S/Key. EAP răspunde cererii în creștere de mărire a autentificării RAS cu terțe dispozitive de securitate. EAP protejează VPN-urile securizate de hackeri care folosesc atacuri prin dicționar și ghicirea parolei. EAP îmbunătățește PAP și CHAP.

Cu EAP, informațiile de autentificare nu sunt incluse în informații, ci mai degrabă cu informațiile. Aceasta permite serverelor la distanță să negocieze autentificarea necesară înainte de a recepta sau transmite orice informație.

Serverul iSeries suportă în acest moment numai o versiune a EAP care este în principiu echivalentă cu CHAP-MD5. Puteți totuși folosi autentificarea la distanță folosind un server RADIUS care poate suporta unele din schemele suplimentare de autentificare descrise mai sus.

PAP

PAP (Password Authentication Protocol) folosește un dialog de confirmare pentru a oferi sistemului pereche o metodă simplă de stabilire a propriei identități. Dialogul (handshake) are loc la stabilirea legăturii. După ce legătura s-a stabilit, dispozitivul la distanță trimite un ID utilizator și parola sistemului care face autentificarea. În funcție de corectitudinea perechii, sistemul de autentificare continuă sau încheie conexiunea.

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

Privire de ansamblu RADIUS

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

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

Serverele RADIUS acționează asupra cererilor de conectare utilizator recepționate prin autentificarea utilizatorului și apoi returnează toate informațiile de configurare necesare, către NAS, astfel încât NAS (serverul iSeries) poate furniza serviciile autentificate utilizatorului autentificat care se conectează prin linie telefonică.

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

Când serverul RADIUS primește o cerere de autentificare, cererea este validată, apoi serverul RADIUS decriptează pachetul de date pentru a accesa informațiile despre nume și parolă utilizator. Informațiile sunt transmise sistemului de securitate corespunzător care este acceptat. Acestea ar putea fi fișiere parolă UNIX, Kerberos, un sistem de securitate comercial sau chiar și un sistem de securitate proiectat personal. Serverul RADIUS trimite înapoi la serverul iSeries orice servicii este autorizat să folosească utilizatorul, ca o adresă IP. Cererile de contabilizare RADIUS sunt tratate într-o manieră similară. Informațiile de contorizare ale utilizatorului la distanță pot fi trimise unui server de contorizare RADIUS desemnat. Protocolul standard de contorizare RADIUS este definit în RFC 2866. Serverul de contorizare RADIUS acționează asupra cererilor de contorizare prin înregistrarea informațiilor din cererea de contorizare RADIUS. Pentru o configurație RADIUS exemplu, consultați scenariul Autentificare utilizatori dial up cu un server RADIUS.

Listă de validare

O listă de validare este folosită pentru a păstra informațiile ID utilizator și parolă despre utilizatorii la distanță. Puteți folosi liste de validare existente sau puteți să creați propriile liste din pagina de autentificare Profil de conexiune receptor. Intrările listă de validare vă cer de asemenea să identificați un tip protocol de autentificare pentru a fi asociat cu ID-ul utilizator și parola. Acesta poate fi **criptat - CHAP-MD5/EAP** sau **necriptat - PAP**.

Consultați ajutorul interactiv pentru informații suplimentare.

Considerații lărgime de bandă - Multilink

Adesea, este necesară o lărgime de bandă suplimentară pentru efectuarea anumitor task-uri, dar aceasta nu este necesară tot timpul. În aceste cazuri, achiziționarea de hardware specializat și de linii de comunicație costisitoare nu este justificată. Protocolul PPP Multilink (MP) grupează mai multe legături PPP împreună pentru a forma o singură legătură virtuală sau "bucet". Agregarea mai multor legături crește lărgimea de bandă efectivă totală dintre două sisteme prin folosirea modem-urilor și liniilor telefonice standard. Puteți include până la șase legături într-un buchet MP. Pentru a stabili o conexiune Multilink, ambele capete ale legăturii PPP trebuie să suporte protocolul Multilink. Protocolul Multilink este referit ca standard RFC (Request For Comment) RFC1990. Informații suplimentare despre RFC se găsesc la <http://www.rfc-editor.org>.

Lărgime de bandă la cerere:

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

Capitol 6. Configurare PPP

Înainte de a putea folosi PPP pentru configurarea unei conexiuni punct-la-punct, trebuie să configurați mai întâi mediul PPP. Aceste secțiuni oferă informații de configurare pentru medii PPP:

- Crearea unui profil de conexiune
- Configurarea modem-ului
- Configurarea unui PC la distanță
- Configurarea accesului la Internet prin AT&T Global Network
- Vrajitori de conectare
- Configurare unei politici de acces de grup
- Aplicarea de reguli de filtrare pachet IP pentru o conexiune PPP
- Activarea serviciilor RADIUS și DHCP pentru profile conexiune receptor PPP

Crearea unui profil de conexiune

Primul pas în configurarea unei conexiuni PPP între sisteme este de a crea un profil de conexiune pe serverul iSeries. Profilul de conexiune este reprezentarea logică a următoarelor detalii ale conexiunii:

- Tip linie și profil
- Configurări multilink
- Numere telefonice la distanță și opțiuni de apelare
- Autentificare
- Configurări TCP/IP: rutare și adrese IP
- Control funcționare și personalizare conexiune
- Servere de nume domeniu

Servicii de acces la distanță, din directorul Rețea, conține următoarele obiecte:

- **Profile conexiune generator** sunt conexiuni punct-la-punct care trebuie expediate și care provin de la serverul iSeries (sistem local). Acestea sunt conexiunile PPP pe care le primește un sistem la distanță.
- **Profile conexiune receptor** sunt conexiuni punct-la-punct care trebuie primite și care provin de la un sistem la distanță. Acestea sunt conexiuni PPP pe care le primește serverul iSeries (sistem local).
- **Modemuri**

Urmați acești pași pentru a crea un profil de conexiune:

1. În iSeries Navigator, selectați sistemul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
2. Selectați una din următoarele opțiuni:
 - Clic dreapta pe **Profiluri conexiune generator** pentru a seta serverul iSeries ca server care inițiază conexiuni.
 - Efectuați clic-dreapta pe **Profile conexiune receptor** pentru a configura serverul iSeries ca server care acceptă conexiunile primite de la sisteme și utilizatori la distanță.
3. Selectați **Profil nou**.
4. Din pagina **Configurare profil nou conexiune punct-la-punct**, selectați tip protocol.
5. Specificați selecții mod.
6. Selectați configurare legătură.
7. Apăsăți **OK**.
Apare pagina **Proprietăți profil nou punct-la-punct**. Puteți seta restul de valori care sunt specifice rețelei. Consultați ajutorul interactiv pentru informații specifice.

Tip protocol: PPP sau SLIP

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

PPP este o conexiune la Internet standard. PPP permite interoperabilitatea între software-ul de acces la distanță al diferiților fabricanți. De asemenea, PPP permite și ca protocoale multiple de comunicație în rețea să folosească aceeași linie fizică de comunicație.

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

- SLIP nu are un mod standard de definire a adresării IP între cele două gazde. Aceasta înseamnă că nu poate fi folosită o rețea nenumărată.
- 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 bidirecțională.

SLIP încă este folosit și încă este suportat pe serverul iSeries. Totuși, IBM recomandă utilizarea PPP la setarea conectivității punct-la-punct. SLIP nu oferă suport pentru conexiuni Multilink. În comparație cu SLIP, PPP are o autentificare mai bună. PPP funcționează mai bine datorită facilităților de comprimare.

Notă: Profilele de conexiune SLIP care sunt definite cu tipuri de linie ASYNC nu mai sunt suportate în această ediție. Dacă aveți aceste profile de conexiune, trebuie să le migrați fie la un profil SLIP, fie la unul PPP care folosesc un tip de linie PPP.

Selecții mod

Selecțiile de mod pentru un profil de conexiune PPP includ selecții pentru **tip conexiune** și **mod de operare**. Selecțiile de mod specifică modul în care serverul folosește noua conexiune PPP.

Urmați acești pași pentru a specifica selecțiile de mod:

1. Selectați unul din următoarele tipuri de conexiune:
 - Linie comutată
 - Linie închiriată
 - L2TP (linie virtuală)
 - Linie PPPoE
2. Selectați modul de operare potrivit pentru noua conexiune PPP.
3. Înregistrați tipul de conexiune și modul de operare selectate. Aveți nevoie de aceste informații atunci când începeți configurarea conexiunilor PPP.

Linie comutată

Selectați acest tip de conexiune dacă folosiți unul din următoarele pentru conectarea printr-o linie telefonică:

- Modem (intern sau extern)
- Adaptor intern ISDN Basic Rate Interface
- Adaptor terminal extern ISDN

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

- **Răspuns**
Alegeți acest mod de operare pentru a permite unui sistem la distanță să se conecteze pe linie telefonică la serverul iSeries.
- **Apel telefonic**
Alegeți acest mod de operare pentru a permite serverului iSeries să se conecteze pe linie telefonică la un sistem la distanță.
- **Apel telefonic la cerere (numai apel)**

Alegeți acest mod de operare pentru a permite serverului iSeries să se conecteze automat pe linie telefonică la un sistem la distanță atunci când în sistem este detectat traficul TCP/IP . Conexiunea se încheie când transmisia datelor este terminată și nu mai există trafic TCP/IP pe o anumită perioadă de timp.

- **Apel telefonic la cerere (pereche dedicată capabilă de răspuns)**

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

- **Apel telefonic la cerere (pereche la distanță activată)**

Alegeți acest mod de operare pentru a permite unui sistem la distanță să fie apelat sau să i se răspundă. Pentru tratarea apelurilor primite, trebuie să referiți un profil de răspuns existent dintr-un profil de conexiune PPP care specifică acest mod de operare. Acesta permite unui profil de răspuns să trateze toate apelurile primite de la unul sau mai mulți parteneri la distanță și 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 distanță.

Linie închiriată

Selectați acest tip de conexiune dacă aveți o linie dedicată între serverul iSeries local și sistemul la distanță. Dacă aveți o linie închiriată, nu aveți nevoie de un modem sau un adaptor terminal ISDN pentru conectarea celor două sisteme.

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

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

- **Terminator**

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

- **Inițiator**

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

L2TP (linie virtuală)

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

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

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

- **Terminator**

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

- **Inițiator**

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

- **Apel telefonic la distanță**

Alegeți acest mod de operare pentru a permite serverului iSeries să se conecteze la un ISP printr-un tunel L2TP și apelați la ISP pentru a apela un client PPP la distanță.

- **Inițiator multi-hop**

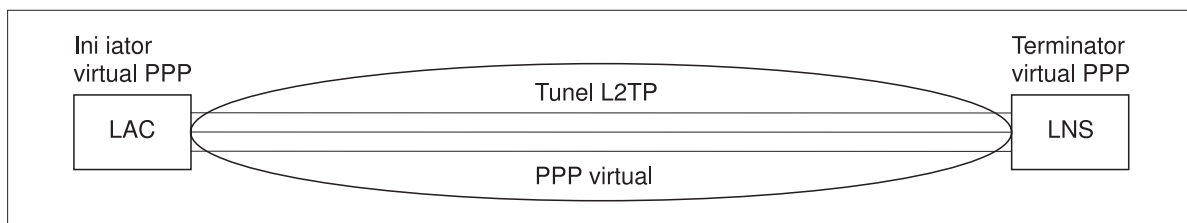
Alegeți acest mod de operare pentru a permite serverului iSeries să stabilească o conexiune multi-hop.

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

L2TP (Layer 2 Tunneling Protocol): L2TP extinde PPP pentru a suporta un tunel la nivelul de legătură între un client L2TP care face cererea și punctul final server L2TP destinație. Folosind tunele L2TP, este posibilă separarea locației la care se încheie protocolul de conectare pe linie telefonică de locul de unde este furnizat accesul în rețea.

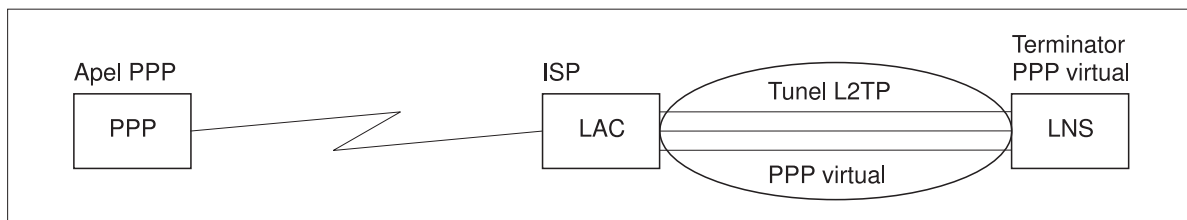
Un ISP (Furnizor de Internet) folosește modul de linie virtuală pentru operarea în VPN (Virtual Private Networks - rețele private virtuale). Vedeți Configurare conexiune L2TP protejată de VPN pentru o mai bună înțelegere a modului în care VPN lucrează cu L2TP.

Aceste exemple ilustrează trei diferite implementări ale L2TP:



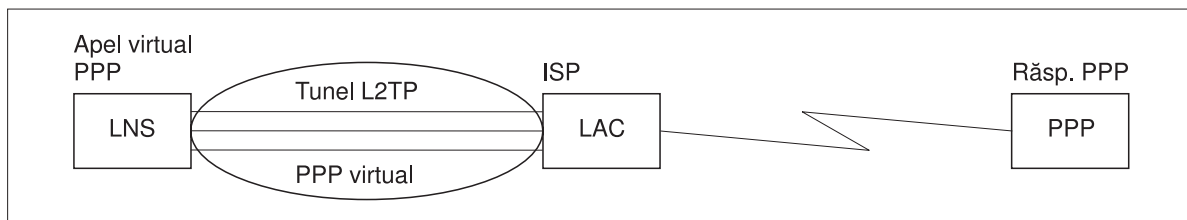
RBAEE563-0

Figura 7. Inițiator virtual PPP sau Terminator virtual PPP



RBAEE561-0

Figura 8. Inițiator prin apel telefonic PPP sau Terminator virtual PPP



RBAEE562-0

Figura 9. Apel telefonic virtual PPP sau Răspuns virtual PPP

Linie PPPoE

Conexiunile PPPoE folosesc o linie virtuală pentru a trimite date PPP printr-un adaptor Ethernet de tip 2838 către un modem DSL oferit de ISP-ul dvs. care este de asemenea conectat la LAN-ul bazat pe Ethernet.

Aceasta permite acces de mare viteză la Internet pentru utilizatorii LAN via sesiuni PPP prin serverul iSeries. Odată ce conexiunea dintre iSeries și ISP a început, utilizatorii individuali de pe LAN pot porni sesiuni unice cu ISP prin PPPoE.

Conexiunile PPPoE sunt folosite doar de profilurile conexiune generator și implică un mod de funcționare Inițiator și folosesc doar o linie singulară.

Configurare legătură

Configurare legătură definește tipul de serviciu linie folosit de profilul de conexiune PPP pentru stabilirea unei conexiuni. Tipurile de servicii linie depind de tipul de conexiune specificat.

- Linie singulară
- Grup de linii
- Linie ISDN integrată

Linie singulară

Selectați acest serviciu linie pentru a defini o linie PPP care este asociată cu un modem analogic. Această opțiune este de asemenea folosită pentru liniile închiriate unde nu este necesar un modem. Profilul de conexiune PPP folosește întotdeauna aceeași resursă port de comunicații a serverului iSeries.

O linie singulară analogică, dacă se dorește, ar putea fi configurată ca "împărțită" de un profil răspuns și unul apel. Partajarea dinamică a resurselor este o nouă funcție proiectată pentru a mări capacitatea de funcționare a resurselor. Până la V5R2, resursele modem erau comise imediat ce era pornit profilul care le folosea. Aceasta limita utilizatorul la o resursă pe sesiune, chiar dacă resursa se afla în stare pasivă de așteptare. Acum se aplică noi reguli de partajare atunci când a fost accesată o resursă anume. Sunt două cazuri: Primul, un profil apel a fost pornit înaintea unui profil răspuns. Al doilea, un profil răspuns a fost pornit înaintea unui profil apel. Se face presupunerea că partajarea resurselor este activată. În primul caz, profilul apel care a fost pornit se va conecta cu succes. Profilul răspuns care a fost pornit al doilea va aștepta ca linia să devină disponibilă. Odată ce conexiunea apel s-a sfârșit profilul răspuns va revendica linia și va porni. În al doilea caz, profilul răspuns care a fost pornit va aștepta conexiunile de intrare. Dacă nu a fost realizată o conexiune de intrare, profilul apel care a fost pornit al doilea va "împrumuta" linia de la profilul răspuns care va "închiria" linia. Conexiunea de ieșire va fi apoi stabilită. Odată ce conexiunea s-a sfârșit, profilul apel va returna linia profilului răspuns care va fi din nou gata să accepte conexiuni de intrare. Pentru a activa funcția de partajare, apăsați pe fișa modem pentru o descriere a liniei comutator și selectați 'Activează partajarea dinamică a resurselor'.

Serviciul linie singulară este de asemenea folosit pentru tipurile de conexiune L2TP (linie virtuală) și PPPoE (linie virtuală). Pentru tipurile de conexiuni L2TP (linie virtuală), nu există resurse port de comunicații 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 și cum ar fi o linie PPP care suportă conexiuni la distanță. Linia virtuală PPPoE este legată de o linie fizică Ethernet și este folosită pentru a suporta transferul de date protocol PPP peste conexiunea LAN Ethernet către un modem DSL.

Grup de linii

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

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

Un grup 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 folosiți grupul de linii pentru a trata simultan mai multe apeluri analogice primite, trebuie să indicați numărul maxim de conexiuni recepționate. Puteți seta aceasta în fișa Conexiuni a dialogului **Proprietăți profil nou punct-la-punct** atunci când configurați profilul de conexiune. Folosiți setarea Multilink pentru a folosi grupuri de linii pentru conexiuni singulare cu lățime de bandă crescută.

Avantaje la utilizarea grupurilor de linii:

- Nu se repartizează o resursă linie unei conexiuni PPP până când aceasta nu pornește.
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 grup de linii, trebuie să fie disponibilă cel puțin o linie din grup atunci când pornește profilul.
În plus, dacă resursele erau configurate ca partajate (activare partajarea dinamică a resurselor), este obținută o disponibilitate suplimentară a resurselor mai ales pentru conexiunile de ieșire.
- Se pot folosi profile apel-la-cerere cu grupuri de linii pentru a folosi resursele mai eficient.
Serverul iSeries selectează o linie din grupul de linii doar atunci când folosește o conexiune prin apel-la-cerere. Alte conexiuni pot folosi aceeași linie în alte momente.
- Puteți porni mai multe conexiuni PPP cu mai puține resurse pentru suport.
De exemplu, dacă mediul necesită patru tipuri unice de conexiuni dar la un anumit moment aveți nevoie doar de două linii, puteți folosi un grup de linii pentru ca acest mediu să funcționeze. Puteți crea patru profile de conexiuni apel-la-cerere și să faceți astfel încât fiecare profil să refere un grup de linii care conține două descrieri de linie. Fiecare din linii ar fi pentru uzul tuturor celor patru profiluri conexiune, permițând astfel ca două conexiuni să fie active în orice moment. Prin folosirea unui grup de linii, nu aveți nevoie să aveți patru linii separate.
De asemenea, dacă mediul dvs. este o combinație între Client PPP și Server PPP, liniile pot fi partajate (activare partajarea dinamică a resurselor) dacă sunt folosite ca "linii singulare" sau plasate într-un "grup de linii". Profilul care a pornit primul nu va implica resursa decât dacă conexiunea este activă. De exemplu, dacă serverul PPP este pornit și așteaptă conexiunile de intrare, el va "închiria" o linie pe care o folosește pentru clientul PPP care a pornit și "împrumutat" linia partajată de la serverul PPP.

Support profil de conexiuni multiple

Profilele de conexiune punct-la-punct care suportă mai multe conexiuni vă permit să aveți un profil de conexiune care manevrează mai multe apeluri de tip digital, analog sau L2TP. Acest fapt este folositor atunci când doriți ca mai mulți utilizatori să se conecteze la serverul iSeries, dar nu doriți să specificați un profil de conexiune punct-la-punct separat pentru lucrul cu fiecare linie. Această caracteristică este folositoare în mod special pentru modem-ul 2805 4-port integrated unde patru linii sunt pentru uzul unui adaptor sau pentru adaptoarele 2750 și 2751, care suportă opt conexiuni ISDN B-channel separate.

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

Adresa IP locală pentru profilele de conexiuni multiple:

Puteți folosi adresa IP locală cu profile de conexiune multiple, dar aceasta trebuie să fie o adresă IP existentă care este definită pe serverul iSeries. Puteți folosi lista derulantă Adresă IP locală pentru a selecta o adresă existentă. Utilizatorii la distanță pot accesa resursele din rețeaua locală dacă alegeți adresa IP locală a serverului iSeries ca adresa IP locală pentru profilul PPP. De asemenea, trebuie să definiți adresele IP care sunt în grupul de adrese IP la distanță pentru a fi în aceeași rețea ca și adresa IP locală.

Dacă nu aveți o adresă IP locală a serverului iSeries sau nu doriți ca utilizatorii la distanță să acceseze LAN-ul, trebuie să definiți o adresă IP virtuală pentru serverul iSeries. O adresă IP virtuală este de asemenea cunoscută ca o interfață fără circuit. Profilele punct-la-punct pot folosi această adresă IP ca adresă IP locală. Deoarece această adresă nu este legată la o rețea fizică, ea va transfera automat traficul către alte rețele care sunt atașate serverului iSeries.

Pentru a crea o Adresă IP virtuală, urmați acești pași:

1. În iSeries Navigator expandați serverul dvs. și accesați **Rețea → Configurație TCP/IP > IPv4 > Interfețe**.
2. Clic dreapta pe **Interfețe** și selectați **Interfață nouă → IP virtual**.
3. Uurmați instrucțiunile Vrăjitorului interfață pentru a crea interfața IP virtuală. Profilele de conexiune punct-la-punct pot folosi adresa IP virtuală, după ce aceasta a fost creată. Puteți folosi lista derulantă din câmpul Adresă IP locală, din pagina Configurări TCP/IP, pentru a folosi adresa cu profilul dvs.

Notă: Adresa IP virtuală trebuie să fie activă înainte de pornirea profilului de conexiuni multiple; altfel, profilul nu va porni. Pentru a activa adresa după crearea interfeței, selectați opțiunea de pornire adresă atunci când folosiți Vrăjitorul interfață.

Grupuri de adrese IP la distanță pentru profile de conexiuni multiple:

Puteți folosi grupuri de adrese IP la distanță cu profile de conexiuni multiple. Un profil tipic punct-la-punct cu o singură conexiune vă va permite să specificați doar o adresă IP la distanță, care este atribuită sistemului apelant, la efectuarea conexiunii. Din moment ce acum mai mulți apelanți pot să se conecteze simultan, un grup de adrese IP la distanță este folosit pentru a defini o adresă IP de pornire precum și intervalul de adrese IP suplimentare care sunt atribuite sistemelor apelante.

Restricții grup de linii:

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

- O linie nu se poate afla decât într-un singur grup de linii la un moment dat. Dacă înlăturați o linie dintr-un grup de linii, ea poate fi folosită într-un alt grup.
- La pornirea unui profil de conexiuni multiple care folosește un grup 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 eșua. De asemenea, dacă nu sunt linii în grupul de linii și alt profil pornește, el se va termina.
- Dacă porniți un profil conexiune unică ce folosește un grup de linii, doar o linie din grupul de linii va fi folosită de către sistem. Dacă porniți un profil conexiune multiplă care folosește același grup de linii, pot fi folosite orice linii rămase în grup.

Grupuri de adrese IP la distanță: Sistemul poate folosi grupurile de adrese IP la distanță pentru orice profil de conexiune punct-la-punct de răspuns sau terminator care este folosit cu conexiunile de intrare multiple. Acestea includ L2TP, ISDN nativ și grupuri de linii cu numărul maxim de conexiuni mai mare ca unu. Această funcție permite sistemului să atribuie o adresă IP la distanță unică pentru fiecare conexiune de intrare.

Primul sistem ce se va conecta va primi adresa IP definită în câmpul Adresă IP de start. Dacă acea adresă este folosită deja, este acordată următoarea adresă IP din interiorul intervalului de adrese. De exemplu, presupuneți că adresa IP de început este 10.1.1.1 și numărul de adrese este definit ca 5. Adresele din grupul de adrese IP la distanță vor fi 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 și 10.1.1.5. Masca subrețea definită pentru adresele grupului de adrese IP la distanță va fi întotdeauna 255.255.255.255.

Aceste restricții se aplică atunci când se folosesc grupuri de adrese IP la distanță:

- Mai multe profile conexiune pot specifica același grup de adrese. Dar, în momentul în care toate adresele grupului sunt folosite, orice cerere ulterioară este refuzată, până când o altă conexiune se oprește și eliberează o adresă.
- Pentru a aloca adrese specifice unor sisteme la distanță, permițând în același timp altor sisteme care apelează să folosească o adresă din grup, urmați următorii pași:
 1. Se activează autentificarea sistemului la distanță din fișa **Autentificare**, astfel încât să poată fi învățat numele de utilizator al sistemului la distanță.
 2. Se definește un grup de adrese IP la distanță pentru toate cererile de conectare sosite ce nu necesită o adresă IP specifică.
 3. Se definesc adresele IP la distanță pentru utilizatori specifici prin activarea **Definire adrese IP suplimentare pe baza ID-ului utilizatorului sistemului la distanță** și apoi prin apăsarea **Adrese IP definite după Nume utilizator**.

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

ISDN

Selectați acest serviciu linie pentru a defini o linie PPP care este asociată cu o conexiune de rețea ISDN.

Avantaje la utilizarea ISDN:

- ISDN oferă comunicații de calitate la viteze mai mari.
- ISDN tinde să ofere conectivitate universală prin folosirea unei singure interfețe și a unei rețele digitale de mare viteză pentru transportarea tuturor tipurilor de date.
- ISDN are de asemenea capacitatea de conectare rapidă pentru conexiunile comutate. Conexiunile cu modem analogic pot lua până la 30 de secunde sau mai mult pentru a se stabili, în timp ce o conexiune ISDN ia doar câteva secunde.

Configurați-vă modem-ul pentru PPP

Pentru conexiunile dvs. analogice PPP puteți folosi un modem extern, intern sau un adaptor terminal ISDN. Un modem vă oferă capacitățile conexiunilor analogice (linii închiriate și comutate). Descrierile de modem pentru cele mai folosite modeme au fost definite pentru serverul iSeries.

Puteți efectua aceste taskuri de configurare modem:

- Configurați un nou modem
- Asociați un modem cu o descriere de linie
- Setare șir comenzi modem

Configurați un nou modem

1. În iSeries Navigator, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
2. Efectuați clic-dreapta pe **Modemuri** și selectați **Modem nou**.
3. În fișa General, introduceți valorile corecte în toate casetele câmp.
4. **Opțional:** Selectați fișa Parametri suplimentari pentru a adăuga alte comenzi de inițializare necesare pentru modem.
5. Apăsați **OK** pentru a salva ceea ce ați introdus și închideți pagina Proprietăți modem nou.

Pentru a determina dacă puteți folosi o descriere modem existentă, urmați acești pași:

1. În iSeries Navigator, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
2. Selectați **Modemuri**.
3. Revedeți lista de modeme și aflați numele fabricantului, modelul și data fabricației.

Notă: Dacă modemul dvs. se află în lista implicită, nu trebuie să mai faceți nimic.

- Efectuați clic-dreapta pe descrierea modem care se potrivește cu modemul dvs. și selectați **Proprietăți** pentru a vedea șirurile de comandă.
- Consultați documentația modemului pentru a determina șirurile specifice de comandă pentru modemul dvs.
Folosiți proprietățile implicite ale modemului dacă șirurile de comandă corespund cerințelor modemului. Altfel, trebuie să creați o descriere modem pentru modemul dvs. și să o adăugați în lista de modemi.

Pentru a crea o descriere modem, urmați acești pași:

- În Navigator operații, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
- Selectați **Modemi**.
- Din lista de modemi, efectuați clic-dreapta pe **\$generic Hayes** și selectați **Modem nou pe baza**.
- Din dialogul **Modem nou**, modificați șirurile de comandă pentru a corespunde informațiilor cerute de modem.

Setare șiruri comenzi modem

Tabelul de mai jos indică un set minim de șiruri de comandă folosite de modemurile definite pentru serverul iSeries. Puteți găsi șirul de comandă echivalent în manualul pentru utilizator al modemului dvs. Folosiți setările recomandate de fabricant din descrierea modem.

Proprietate modem	Șir de comandă corect pentru majoritatea modemurilor
Reset modem la valorile implicite de fabrică	AT&F sau AT&Z
Inițializare modem:	
Afișare coduri verbale rezultat	Q0 și V1
Moduri DTR și CD normal	&C1 și &D2
Mod echo dezactivat	E0
DSR (Data Set Ready) urmează după Carrier Detect	&S1
Activare control hardware flux (RTS/CTS)	
Activare corecție erori și, opțional, compresie (V.42/V.42 bis)	
Asigurare că viteza liniei DTE-DCE este activată pentru a rula la fix 115.2 Kbps (sau maximul permis de modem)	
(Opțional) Activare timp de inactivitate dacă modemul suportă această funcție	
Mod de răspuns modem:	
Răspuns după n apeluri	S0= n unde $n = 1$ sau 2
Deconectare dacă nu există conectare (carrier) după m secunde	S7= m
Tip modem Apel telefonic	ATDT pentru apel tone sau ATDP pentru apel pulse

Exemplu: Configurați un adaptor terminal ISDN

- În Navigator operații, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță**.
- Efectuați clic-dreapta pe **Modemi** și selectați **Modem nou**.
- În fișa General, introduceți valorile corecte în toate casetele cu câmpuri.
- Opțional:** Selectați fișa Parametri ISDN pentru a adăuga alte comenzi de inițializare necesare pentru modem.

Pentru adaptoare terminale ISDN, comenzile și parametri din această listă sunt transmiși adaptorului terminal doar în următoarele condiții:

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

În consecință, aceste comenzi ar trebui să includă și să fie limitate la următoarele:

- Setarea tipului de comutare ISDN și versiune furnizate de compania telefonică locală
 - Setarea numerelor directoarelor și SPID-uri (service profile identifiers - identificatori profil serviciu) furnizate de compania telefonică locală
 - Setarea TEI (Terminal Entry IDs - identificatori intrare terminal) care ar putea fi furnizați de compania telefonică locală
 - Setarea protocolului canal B (PPP asincron-la-sincron)
 - Alte setări modem care au parametri de lungime variabilă ce necesită un început de linie pentru a indica lungimea parametrului
 - Salvarea și activarea noilor setări pentru a fi restaurate după resetarea lor sau după întreruperea alimentării sistemului.
 - Comanda de probă a stării interfeței *U* (ATD*x*), care permite serverului iSeries să determine când este activată sincronizarea cu comutatorul sediului central ISDN. *x* poate fi oricare din cifrele permise pentru un număr de telefon, incluzând # și *.
5. Apăsați **Adăugare** pentru comenzi modem suplimentare. Acestea pot fi cu sau fără un parametru asociat și o scurtă descriere în lista de comenzi. Comenzilor specificate fără un parametru asociat li se poate atribui un parametru atunci când modemului i se asociază o descriere linie.
 6. Apăsați **OK** pentru a salva ceea ce ați introdus și închideți pagina Proprietăți modem nou.

Asociați un modem cu o descriere de linie

1. În iSeries Navigator, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță** → **Profiluri conexiune generator** sau **Profiluri conexiune receptor**.
2. Selectați una din următoarele opțiuni:
 - Pentru gestionarea unui profil de conexiune existent, efectuați clic-dreapta pe un profil de conexiune și selectați **Proprietăți**.
 - Pentru gestionarea unui profil de conexiune nou, creați unul nou.
3. Din pagina Proprietăți profil nou punct-la-punct, selectați fișa **Conexiune** și selectați **Nou**.
 - Introduceți numele pentru configurarea liniei.
 - Selectați **Nou** pentru a deschide caseta de dialog Proprietăți linie nouă.
4. Din caseta de dialog Proprietăți linie nouă, selectați fișa **Modem** și selectați modemul din listă. Modemul selectat va fi asociat cu această descriere de linie. Pentru modem-uri interne definiția modem corectă ar trebui să fie deja selectată. Pentru mai multe informații, consultați ajutorul interactiv.

Pentru V5R2, puteți configura ca profilurile conexiune generator să "împrumute" o linie și un modem PPP alocate unui profil conexiune receptor care așteaptă un apel de intrare. Conexiunea generatoare va "returna" linia și modemul PPP profilului conexiune receptor când conexiunea s-a încheiat. Pentru a activa această nouă funcție, selectați opțiunea **Activare partajare dinamică de resurse** din fișa Modem a dialogului de configurare linie PPP. Puteți configura linii PPP din fișa Conexiune a profilelelor conexiune Receptor și Generator.

Configurați un PC la distanță

Pentru conectarea la un server iSeries de la un PC care rulează orice sistem de operare Windows pe 32 de biți, verificați dacă modemul este instalat și configurat corespunzător și asigurați-vă că ați instalat TCP/IP și Dial-Up Networking pe calculatorul personal.

Consultați documentația Microsoft Windows pentru informații despre configurarea Dial-up Networking pe PC. Asigurați-vă că ați specificat sau introdus următoarele informații:

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

Configurați accesul la Internet prin AT&T Global Network

IBM oferă acces la Internet prin AT&T Global Network. Pentru a accesa acest serviciu, puteți folosi vrăjitorul AT&T Global Network Dial Connection 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 și necesită cam zece minute pentru terminare. Puteți anula vrăjitorul în orice moment și nu sunt salvate nici un fel de date.

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

- **Mail Exchange:** Permite extragerea periodică a poștei de la un singur cont AT&T Global Network și transmiterea ei la serverul iSeries pentru distribuire către utilizatorii Lotus Mail sau cei ai SMTP (Simple Mail Transfer Protocol).
- **Dial-up Networking:** Folosiți alte aplicații de rețea cu conectare prin apel telefonic cu AT&T Global Network, cum este accesul standard Internet.

Întrețineți profilele de conexiune AT&T Global Network ca orice alte profile de conexiune PPP.

Aveți nevoie de unul din aceste adaptoare pentru a folosi vrăjitorul AT&T Global Network Dial Connection:

- 2699: Two-line WAN IOA
- 2720: PCI WAN/Twinaxial IOA
- 2721: PCI Two-line WAN IOA
- 2745: PCI Two-line WAN IOA (înlocuiește IOA 2721)
- 2761: Eight-port analog modem IOA
- 2771: Two-port WAN IOA, cu un modem integrat V.90 la portul 1 și o interfață standard de comunicații la portul 2. Pentru a folosi portul 2 al adaptorului 2771, este necesar un modem extern sau adaptor terminal ISDN cu cablul corespunzător.
- 2772: Two port V.90 integrated modem WAN IOA
- 2793: Two-port WAN IOA, cu un modem integrat V.92 la portul 1 și o interfață standard de comunicații la portul 2. Acesta înlocuiește modelul 2771.
- 2805 Four port WAN IOA, cu un modem integrat V.92 integrat. Acesta înlocuiește modelele 2761 și 2772.

Înainte de a porni vrăjitorul AT&T Global Network Dial Connection, trebuie să aveți aceste informații despre mediu:

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

Pentru a porni vrăjitorul AT&T Global Network Dial Connection, urmați acești pași:

1. În iSeries Navigator expandați serverul dvs. și accesați **Rețea** → **Servicii de acces la distanță**.
2. Efectuați clic-dreapta pe **Profile de conexiune generator** și selectați **Nou AT&T Global Network Dial Connection**.
3. La pornirea vrăjitorului AT&T Global Network Dial Connection, selectați **Ajutor** pentru informații despre completarea unui panou.

Vrăjitori de conectare

Vrăjitor conexiune nouă prin apel telefonic

Acest vrăjitor vă ghidează prin pașii de configurare a unui profil de conexiune prin apel telefonic pentru accesarea ISP (Furnizor de Internet) sau a Intranetului. Ar putea fi nevoie de informații de la administratorul rețelei dvs. sau de la furnizorul dvs. de Internet (ISP) pentru a termina vrăjitorul. Pentru mai multe informații despre completarea vrăjitorului, consultați ajutorul interactiv.

Vrăjitor de conexiune universal

Selectarea acestui vrăjitor vă ghidează prin pașii de configurare a unui profil care poate fi folosit de software-ul Electronic Customer Support pentru conectarea la IBM. Suportul service electronic oferă monitorizarea mediului dvs. unic pentru sistemul server iSeries pentru a vă furniza recomandări de corecții personalizate pentru sistemul și situația particulară. Pentru mai multe informații despre completarea vrăjitorului, consultați ajutorul interactiv.

Configurarea unei politici de acces de grup

Folderul **Politici de acces grup** din **Profile de conexiune receptor** oferă opțiuni pentru configurarea parametrilor conexiunilor punct-la-punct care se referă la un grup de utilizatori la distanță. Aceasta e valabil numai pentru acele conexiuni punct-la-punct inițiate de un sistem la distanță și care sunt recepționate de sistemul local.

Pentru a configura o nouă politică de acces grup:

1. În Navigator operații, selectați serverul dvs. și expandați **Rețea** → **Servicii de acces la distanță** → **Profile de conexiune receptor**.
2. Efectuați clic-dreapta pe **Politici de acces grup** și selectați **Politică nouă de acces grup**.
3. În fișa **General**, introduceți un nume și o descriere pentru noua politică de acces a grupului.
4. Apăsați pe fișa **Multilink** și setați configurația Multilink.

Configurația Multilink precizează că vreți să aveți linii fizice multiple unite într-un buchet. Numărul maxim de legături dintr-un pachet poate fi între 1 și 16. Deoarece nu știți 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 capacitățile protocolului Multilink pentru un utilizator anume.

- **Maxim de legături per pachet** specifică numărul maxim de legături (sau linii) care doriți 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.
 - Activați **Necesar protocol de alocare a lărgimii de bandă** dacă doriți să specificați faptul că o conexiune este stabilită doar dacă sistemul la distanță suportă protocolul BACP (Bandwidth Allocation Protocol). Dacă nu poate fi negociat BACP, este permisă doar o legătură singulară.
5. Selectați fișa **Configurări TCP/IP** pentru a activa una din următoarele:
 - Acceptarea ca sistemele la distanță să acceseze alte rețele (IP forwarding)
Această opțiune specifică dacă doriți "IP forwarding". Dacă o selectați, veți permiteți serverului iSeries să se comporte ca un ruter pentru această conexiune. Aceasta permite ca datagramele IP (Internet Protocol) care nu sunt destinate serverului iSeries să treacă prin acest sistem către o rețea conectată. Dacă lăsați această opțiune neselectată, IP (Internet Protocol) ignoră acele datagrame de la sistemul la distanță care nu sunt destinate nici uneia dintre adresele locale acestui server iSeries.

Ar putea exista motive de securitate pentru care nu s-ar permite "IP forwarding". Prin contrast, un ISP (Furnizor de Internet) permite în general "IP forwarding" întotdeauna. Observați că aceasta va avea efect doar dacă este activată transmiterea datagramelor IP pe întreg sistemul, altfel aceasta va fi ignorată chiar dacă este activată. Transmiterea datagramelor IP pe întreg sistemul poate fi afișată din fișa Configurări a paginii Proprietăți TCP/IP.

- Cerere compresie antet TCP/IP (VJ)

Această opțiune specifică dacă doriți ca IP (Internet Protocol) să comprime informațiile din antet după stabilirea unei conexiuni. Comprimarea duce de obicei la creșterea performanțelor, în special pentru traficul interactiv sau liniile seriale lente. Compresia antetelor folosește metoda Van Jacobson (VJ) definită în RFC 1332. Pentru PPP, compresia este negociată la stabilirea conexiunii. Dacă celălalt capăt al conexiunii nu suportă compresia VJ, serverul iSeries va stabili o conexiune care nu folosește compresia.

- Folosire reguli pachet IP pentru această conexiune

Această opțiune specifică dacă doriți să aplicați o regulă de filtrare pentru această politică de grup. Regulile de filtrare vă permit controlarea traficului IP acceptat de rețea. Puteți folosi această componentă de filtrare a pachetului IP pentru protejarea sistemului. Componenta de filtrare a pachetului IP protejează sistemul prin filtrarea pachetelor în funcție de regulile pe care le specificați. Regulile se bazează pe informațiile din antetul pachetului.

Pentru informații suplimentare despre regulile pachetului IP, consultați subiectul Filtrare pachete IP și NAT din Centru de informații.

Pentru un exemplu, consultați Gestiunea accesului utilizatorilor la resurse folosind Politici de acces de grup și filtrarea IP.

Aplicarea unei politici de grup unui utilizator cu acces la distanță:

Puteți aplica o politică de grup unui utilizator cu acces la distanță după ce ați completat Proprietăți punct-la-punct pentru un nou **Profil de conexiune receptor**.

Pentru a aplica o politică de grup unui utilizator la distanță:

1. Selectați pagina **Autentificare**.
2. Bifați **Se cere ca acest server iSeries să verifice identitatea sistemului la distanță**.
3. Selectați **Autentificare locală folosind o listă de validare**.
4. Dacă există o listă de validare, selectați-o din lista derulantă și apăsați **Deschidere**. Dacă o creați pentru prima dată, introduceți un nume pentru noua listă de validare și apăsați **Nou**.
5. Apăsați **Adăugare** pentru a adăuga un nou utilizator în lista de validare.
6. În caseta de dialog Adăugare utilizator, faceți următoarele:
 - Selectați protocolul de autentificare pentru care este definit numele utilizatorului.
 - Introduceți numele și parola de utilizator.

Notă: Din motive de securitate, este recomandat să nu folosiți aceeași parolă pentru un utilizator definit pentru CHAP (Challenge Handshake Authentication Protocol22314), EAP (Extensible Authentication Protocol) și PAP (Password Authentication Protocol).

- Activați **Aplicarea unei politici de grup utilizatorului**, selectați o politică de grup din lista derulantă și apăsați **Deschidere**.

Puteți modifica proprietățile politicii de grup sau puteți folosi setările existente. Apăsați **OK** pentru încheierea configurării și revenire la pagina Proprietăți punct-la-punct.

Aplicarea regulilor de filtrare pachet IP unei conexiuni PPP

Subiectul Reguli filtrare pachet IP și NAT din Centrul de informare discută despre modul de creare a regulilor pachet IP pe care să le puteți referi pentru un profil de conexiune PPP. Puteți folosi un fișier reguli pachet pentru a restricționa accesul unui utilizator sau unui grup la adrese IP din rețeaua dvs. Pentru un exemplu de folosire a fișierului de reguli filtru cu o conexiune PPP, vedeți Scenariu: Gestionarea accesului utilizatorilor la distanță la resurse folosind Politici de grup și filtrare IP.

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

- Nivel profil de conexiune
 1. La completarea **Proprietăți punct-la-punct** pentru un **Profil de conexiune receptor**, selectați pagina Configurări TCP/IP și apăsați **Avansat**.
 2. Activați **Folosire reguli pachet IP pentru această conexiune** și selectați un identificator de filtru PPP din lista derulantă.
 3. Apăsați **OK** pentru a aplica filtrul PPP profilului de conexiune.
- Nivel utilizator
 1. Deschideți o politică de acces grup existentă sau creați una nouă.
 2. Selectați pagina Configurări TCP/IP.
 3. Activați **Folosire reguli pachet IP pentru această conexiune** și selectați un identificator filtru PPP din lista derulantă.
 4. Apăsați **OK** pentru a aplica filtrul PPP.

Activare servicii RADIUS și DHCP pentru profiluri conexiune

Pentru a activa serviciile RADIUS și DHCP pentru profile de conexiuni receptor PPP:

1. În Navigator operații, selectați serverul dvs. și expandați **Rețea**→ **Servicii de acces la distanță**.
2. Efectuați clic-dreapta pe **Servicii de acces la distanță** și selectați **Servicii**.
3. Selectați fișa **DHCP-WAN**. Aceasta va activa automat DHCP și va detecta ce server DHCP și agenți retransmitere (dacă există) rulează pe sistem.
4. Pentru a activa serviciile RADIUS selectați fișa **RADIUS**.
 - a. Selectați **Activare conexiune server de acces rețea RADIUS**
 - b. Selectați **Activare RADIUS pentru autentificare**.
 - c. În funcție de soluția RADIUS, puteți de asemenea alege ca RADIUS să trateze contabilizarea conexiunilor și configurarea adreselor TCP/IP.
5. Apăsați pe butonul **Setări RADIUS NAS** pentru a configura conexiunea cu serverul RADIUS.
6. Apăsați pe OK pentru a vă întoarce la iSeries Navigator.

Pentru un exemplu de configurație RADIUS, consultați scenariul Autentificare utilizatori dial up cu un server RADIUS.

Capitol 7. Gestionăți PPP

Acestea sunt task-urile de administrare PPP pe care le puteți efectua pe serverul iSeries:

- Setăți proprietățile pentru profilurile conexiune.
- Monitorizați activitatea PPP

Setăți proprietățile pentru profiluri conexiune PPP

La crearea unui profil de conexiune, de obicei selectați protocolul, tipul de conexiune și modul de operare pentru noul profil de conexiune în caseta de dialog Configurare profil de conexiune punct-la-punct. După introducerea selecțiilor în această casetă de dialog, va apare pagina de proprietăți a profilului de conexiune. Selecțiile specificate în caseta de dialog Configurare profil de conexiune punct-la-punct determină conținutul și ordinea fișelor din pagina de proprietăți a profilului de conexiune. Pagina de proprietăți este diferită pentru profile de conexiune generator și cele receptor.

Puteți folosi aceste îndrumări pentru a completa fiecare pagină a casetei de dialog **Proprietăți profil punct-la-punct**. Setările pe care le selectați în fiecare pagină depind de mediu și de tipul de conexiune configurată. Ajutorul online iSeries Navigator descrie fiecare opțiune care apare în căsuța de dialog. Puteți consulta și exemplele și procedurile PPP pentru informații suplimentare.

Monitorizare activitate PPP

Această pagină explică modul de vizualizare a unui profil de conexiune și un istoric sesiune folosind Navigator operații.

Despre joburi conexiune PPP:

- Există două joburi de control PPP care sunt folosite pentru administrarea joburilor individuale ale conexiunii PPP. Aceste joburi rulează în subsistemul QSYSWRK:
 - QTPPPCTL - Jobul principal de control PPP. Acest job administrează fiecare job al conexiunii PPP.
 - QTPPPL2TP - Server L2TP. Acest job gestionează stabilirea tunelului L2TP și rulează doar dacă rulează în mod curent un profil L2TP.
- Joburile conexiune PPP rulează sub profilul utilizator QTCP și sunt folosite pentru tratarea fiecărei conexiuni PPP individual. Aceste joburi rulează implicit în subsistemul QUSRWRK, dar pot fi configurate pentru a rula în alte subsisteme. Sunt folosite două nume de joburi pentru conexiunile PPP:
 - QTPPPSSN - Acest job este folosit pentru tratarea tuturor conexiunilor PPP non-L2TP.
 - QTPPPL2SSN - Acest job este folosit pentru tratarea datelor PPP virtuale după ce joburile QTPPPL2TP au negociat cu succes un tunel L2TP.
- 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 și 99.
 - QTPPANS nn sunt joburi cu primire apel unde nn este orice număr între 1 și 99.

Gestionare profile de conexiune:

1. În iSeries Navigator expandați serverul dvs. și accesați **Rețea** → **Servicii de acces la distanță**. Selectați **Profil de conexiune inițiator** sau **Profil de conexiune receptor**.
2. În coloana Profil, efectuați clic-dreapta pe orice nume de profil de conexiune și selectați una din următoarele opțiuni:
 - **Joburi** deschide istoricul jobului pentru joburi QTPPxxx.

- **Conexiuni** deschide o casetă de dialog pentru a afișa informații despre toate conexiunile asociate cu acel profil. Informațiile pot include datele despre conexiunea curentă, despre conexiunile anterioare sau ambele. Sunt disponibile și opțiuni pentru a vizualiza ieșirea jobului sau detalii despre conexiune pentru fiecare din conexiuni.
- **Proprietăți** deschide pagina Proprietăți pentru a afișa proprietățile curente ale unei conexiuni.

Vizualizarea informațiilor despre conexiune:

1. În iSeries Navigator expandați serverul dvs. și accesați **Rețea** → **Servicii de acces la distanță**. Selectați **Profil de conexiune generator** sau **Profil de conexiune receptor**.
2. În coloana Profil, efectuați clic-dreapta pe orice nume de profil de conexiune care nu are starea Inactiv și selectați **Conexiuni** pentru a vedea informații despre conexiune.
Fiecare conexiune pentru acest profil va fi arătată (curentă sau anterioară). Câmpul de stare indică starea curentă a conexiunii. Informații suplimentare cum sunt ID utilizator pentru utilizatorul conectat, adrese IP locale și la distanță și numele jobului PPP ar putea fi afișate în funcție de starea fiecărui job PPP.
3. Pentru a vizualiza ieșirea jobului sau detalii despre o conexiune, efectuați clic-dreapta pe o conexiune și butoanele vor fi activate.
4. Pentru a vedea ieșirea jobului, selectați **Joburi**. Din istoric job, efectuați clic-dreapta pe numele jobului și selectați **Afișare ieșire**. Atunci vor putea fi afișate conținutul istoricelor sesiunii de conectare și al istoricelor job (pentru sesiuni încheiate).
5. Pentru a vedea detaliile conexiunii, selectați **Detalii**. Detaliile nu pot fi afișate decât pentru conexiunile care sunt active în acel moment. Dialogul pentru detalii vă va permite să vedeți informații suplimentare despre această conexiune.

Gestionare ieșire PPP de la serverul iSeries:

Pentru gestionarea ieșirii PPP, tastați WRKTCPTP în linia de comandă a serverului iSeries:

- Pentru gestionarea TUTUROR joburilor PPP active (incluzând joburile QTPPPCTL și QTPPPL2TP), apăsați **F14** (Gestionare joburi active).
- Pentru gestionarea tuturor ieșirilor pentru un anumit profil de conexiune, selectați **opțiunea 8** (gestionare ieșiri) pentru acel profil.
- Pentru a tipări configurările profilului PPP, selectați **opțiunea 6** (Tipărire) pentru acel profil. Folosiți comanda WRKSPLF pentru a accesa ieșirea tipărită.


Stare conexiune:

Starea profilului conexiune este afișată în câmpul **Stare** pentru fiecare profil din lista profilurilor conexiune din **Rețea > Servicii de acces la distanță** după selectarea fie a profilului generator, fie receptor. Starea unei conexiuni individuale este afișată folosind dialogul Conexiuni.

Descriere stare primară	Explicație
Așteaptă cereri de conectare	Profilul receptor gata pentru conectare
Așteaptă primire apel	Server gata pentru conectare
În curs de conectare	În procesul de conectare cu sistemul la distanță
Activ/Conexiuni active	Conexiune realizată și jobul rulează cu succes
Inactiv	În acest moment nu rulează nici un job pentru acest profil de conexiune
Încheiat	Informații disponibile
Terminatorul multihop pornește inițiatorul multihop	Multihop în desfășurare
Conexiunea multihop este activă	Multihop conectat cu succes

Decriere stare secundară	Explicație
Inițializare modem	inițializare modem la începutul conexiunii dialup
Așteptare conexiune modem	Serverul PPP în stare de ascultare
APELARE xxx-xxxx	număr apelat de clientul dialup
Apel de intrare detectat	Serverul PPP detectează un apel modem de intrare
Modem conectat	Dialog de confirmare PPP completat cu succes
Operațional	Conexiune PPP activă
Legătură terminată	Conexiune terminată de pereche
Oprit	Profil sau job terminat
Eșec autentificare	Conexiunile PPP au eșuat să se stabilească datorită autentificării eșuate
Expirare timp de așteptare pentru inactivitatea conexiunii	Conexiunile PPP au eșuat să se stabilească datorită expirării timpului de așteptare activitate
Negociere adrese IP	Conexiunile PPP s-au terminat datorită problemelor de negociere IP
Modem-ul la distanță nu a răspuns	Conexiunile PPP au eșuat să se stabilească datorită inexistenței răspunsului de la cealaltă parte
Refuzare protocol	Conexiunile PPP au eșuat datorită eșecului negocierii NCP
Eșec reîncercare	Conexiunea PPP a eșuat să se stabilească datorită numărului depășit de reîncercări
Confirmare sesiune PPPoE primită de la pereche	Negociere PPPoE completată cu succes
Apel L2TP stabilit	Mesaj tunel L2TP

Capitol 8. Depanare PPP

Informațiile curente și relevante despre corecțiile temporare de program (PTF-uri) și despre depanare sunt documentate pe pagina de casă a TCP/IP pentru serverul iSeries . Această legătură oferă ultimele informații care suplimentează și suprascriu informațiile conținute în acest subiect.


Dacă aveți probleme cu conexiunile PPP, puteți folosi această listă de verificare pentru a strânge informații despre eroare. Lista de verificare vă poate ajuta la identificarea simptomelor de eroare și la rezolvarea problemelor conexiunilor PPP.

1. Material necesar pentru suport:

- Tip gazdă la distanță, sistem de operare și nivel
- Nivel sistem de operare al serverului iSeries
- Istoric job al sesiunii în eroare și fișier de dialog al conexiunii
În V5R1, istoricele job și ieșirea dialogului conexiunii sunt salvate în OUTQ cu același nume ca și profilul.
- Scriptul de conexiune dacă este folosit de mediu
- Starea profilului de conexiune înainte și după eșuarea conexiunii

2. Material recomandat pentru suport:

- Descriere linie
- Profil de conexiune
Opțiunea 6 din WRKTCPPPTP tipărește setările profilului.
- Tip și model modem
- Șiruri de comandă modem
- Urmărire comunicații



Cartea roșie TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  acoperă extensiv următoarele probleme PPP. De asemenea, oferă și informații detaliate de rezolvare a problemelor.

Problemă	Soluție
<p>Configurare hardware modem</p> <p>Configurare greșită a comutatoarelor dip și a altor setări hardware</p>	<p>Asigurați-vă că modemul este configurat cu tipul corect de framing. Acesta poate fi fie <i>Asincron</i>, fie <i>Sincron</i>. Consultați manualul modemului pentru informații suplimentare.</p>
<p>Comenzi AT modem</p> <p>Modemul pe care încercați să îl folosiți nu este în lista predefinită de modemi a Navigator operații.</p>	<p>Creați un nou modem.</p>
<p>Utilizatori și parole PPP</p> <p>Obțineți erori de nume și parolă utilizator atunci când încercați o conexiune PPP.</p>	<ul style="list-style-type: none"> • Asigurați-vă că ID-ul și parola utilizatorului sunt introduse folosind majuscule sau litere mici, după cum este cazul. • Asigurați-vă că protocolul de autentificare folosit de parteneri este același. • Nu folosiți PAP la unul din parteneri în timp ce celălalt partener este configurat pentru CHAP.
<p>Linii PPP pentru pornirea unui profil de conexiune</p> <p>Linii PPP identificate sunt folosite de aceeași resursă hardware.</p>	<p>Nu uitați să schimbați celelalte linii care folosesc aceeași resursă hardware.</p>

Problemă	Soluție
Protocol PPP Erorile de conectare pot apare din cauza configurării greșite a protocolului PPP.	Investigarea nivelelor de jos ale protocolului PPP ar putea fi necesară în unele situații în care partenerii nu reușesc să comunice între ei din cauza unei erori de configurare. Dacă istoricul PPP sau istoricul job al jobului PPP nu dau nici o indicație despre problemă, puteți investiga problema folosind funcția de urmărire a comunicației.

Capitol 9. Alte informații despre PPP

Alte surse de informare despre PPP:

- Găsiți cele mai noi corecții temporare de program (PTF-uri) și cele mai noi informații despre configurare pentru PPP și L2TP prin legătura PPP de pe pagina de casă TCP/IP pentru serverul iSeries  . Această legătură oferă ultimele informații care suplimentează și suprascriu informațiile conținute în subiectul **Servicii de acces la distanță: Conexiuni PPP**.
- Cartea roșie ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  acoperă extensiv serviciile și aplicațiile TCP/IP.



IBM Confidential
Tipărit în S.U.A.