



System i

Mrežni rad

Usluge daljinskog pristupa: PPP veze

*Verzija 6 Izdanje 1*







System i

Mrežni rad

Usluge daljinskog pristupa: PPP veze

*Verzija 6 Izdanje 1*

**Napomena**

Prije upotrebe ovih informacija i proizvoda koji one podržavaju, pročitajte informacije u “Napomene”, na stranici 65.

Ovo izdanje se primjenjuje na verziju 6, izdanje 1, modifikaciju 0 od IBM i5/OS (broj proizvoda 5761–SS1) i na sva sljedeća izdanja i modifikacije, dok se drukčije ne označi u novim izdanjima. Ova verzija ne radi na svim računalima sa smanjenim skupom instrukcija (RISC), niti ne radi na CISC modelima.

© **Autorsko pravo International Business Machines Corp. 1998, 2008. Sva prava pridržana.**

# Sadržaj

## Usluge daljinskog pristupa: PPP veze . . . 1

PDF datoteka za Usluge daljinskog pristupa . . . . .	1
PPP koncepti. . . . .	1
Što je PPP . . . . .	1
Profili veza . . . . .	2
Podrška politike grupe . . . . .	3
Scenarij: Udaljeni pristup korištenjem PPP veza . . . . .	4
Primjer: PPP i DHCP na jedinstvenom System i . . . . .	4
Primjer: DHCP i PPP profili na različitim System i modelima. . . . .	6
Scenarij: Zaštita L2TP dobrovoljnog tunela pomoću IPsec-a . . . . .	9
Scenarij: Povezivanje vašeg sistema sa PPPoE koncentratorom pristupa . . . . .	10
Scenarij: Spajanje udaljenih klijenata biranja na sistem . . . . .	12
Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema . . . . .	15
Scenarij: spajanje vaše korporativne i udaljene mreže modemom . . . . .	18
Scenarij: Provjera autentičnosti veza biranja pomoću RADIUS NAS-a . . . . .	21
Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja . . . . .	23
Scenarij: Dijeljenje modema između logičkih particija korištenjem L2TP-a . . . . .	26
Detalji scenarija: Dijeljenje modema između logičkih particija korištenjem L2TP-a . . . . .	27
Scenarij 1: Konfiguracija L2TP terminirajućeg profila za sva sučelja na particiji koja ima modeme u vlasništvu . . . . .	28
Korak 2: Konfiguracija L2TP izvorišnog profila na 10.1.1.74 . . . . .	29
Korak 3: Konfiguracija L2TP udaljenog profila biranja za 192.168.1.2. . . . .	30
Korak 4: Testiranje veze . . . . .	30
Planiranje PPP-a . . . . .	31
Softverski i hardverski zahtjevi . . . . .	31
Alternativne veze . . . . .	32
Analogne telefonske linije . . . . .	32
Digitalna usluga i Digitalne Podatkovne Usluge . . . . .	33
Birani-56 . . . . .	33
Integrirana mreža digitalnih usluga . . . . .	34
T1/E1 i djelomične T1 veze . . . . .	34
Frame relay . . . . .	35
Podrška za L2TP (tuneliranje) za PPP veze . . . . .	35
Dobrovoljni tunel . . . . .	36
Model obaveznog tunela - dolazeći poziv . . . . .	36
Model obaveznog tunela - udaljeni poziv . . . . .	37
L2TP multi-hop povezivanje. . . . .	37
PPPoE (DSL) podrška za PPP veze. . . . .	37
Oprema za povezivanje . . . . .	37
Modemi . . . . .	38
CSU/DSU . . . . .	38

ISDN terminalski adaptori . . . . .	38
Prijedlozi ISDN terminalskog adaptora . . . . .	39
Ograničenja ISDN terminalskog adaptora . . . . .	39
Rukovanje IP adresama . . . . .	40
Filtriranje IP paketa . . . . .	40
Strate3gija upravljanja IP adresom . . . . .	41
Sistemska provjera ovlaštenja . . . . .	42
Protokol Provjere autentičnosti izazova rukovanjem s MD5 . . . . .	43
Proširivi Protokol provjere autentičnosti . . . . .	43
Protokol provjere autentičnosti lozinkom . . . . .	43
Pregled Korisničke usluge udaljene provjere autentičnosti biranja . . . . .	44
Validacijska lista . . . . .	44
Razmatranja o pojasnoj širini za multilink. . . . .	45
Konfiguracija PPP-a . . . . .	45
Stvaranje profila veze. . . . .	45
Tip protokola: PPP ili Serijski linijski protokol Interneta (SLIP) . . . . .	46
Izbori načina . . . . .	47
Birana linija . . . . .	47
Iznajmljena linija . . . . .	47
L2TP (virtualna linija) . . . . .	48
PPPoE linija . . . . .	48
Konfiguracija veze . . . . .	49
Pojedinačna linija . . . . .	49
Skup linija . . . . .	49
Podrška profila višestrukih veza. . . . .	51
Konfiguriranje vašeg modema za PPP . . . . .	53
Konfiguracija novog modema . . . . .	53
Postavljanje naredbenih nizova modema . . . . .	54
Primjer: Konfiguriranje ISDN terminalskog adaptora . . . . .	54
Pridruživanje modema opisu linije . . . . .	55
Konfiguracija udaljenog PC-a . . . . .	55
Konfiguracija Internet pristupa kroz AT&T Globalnu Mrežu . . . . .	55
Čarobnjaci povezivanja . . . . .	56
Konfiguracija grupne politike pristupa . . . . .	57
Primjena pravila filtriranja IP paketa na PPP vezu . . . . .	58
Omogućavanje RADIUS i DHCP usluga za profile veze . . . . .	59
Upravljanje PPP-om . . . . .	59
Postavljanje svojstava za PPP profile veze. . . . .	59
Nadgledanje PPP aktivnosti . . . . .	59
Rješavanje problema vezanih uz PPP . . . . .	61
Informacije vezane uz Usluge daljinskog pristupa . . . . .	63

## Dodatak. Napomene . . . . . 65

Informacije o sučelju programiranja . . . . .	66
Zaštitni znaci . . . . .	66
Termini i uvjeti. . . . .	67



---

## Usluge daljinskog pristupa: PPP veze

Point-to-Point protokol (PPP) je Internetski standard za prijenos podataka preko serijskih linija

PPP je najšire korišteni protokol veze između pružatelja Internetskih usluga (ISP-ova). PPP omogućuje pojedinačnim računalima pristup mrežama. Te mreže nadalje pružaju pristup Internetu. System i proizvod uključuje podršku za TCP/IP PPP kao dio svoje WAN (mreža širokog područja) povezanosti.

Možete izmjenjivati podatke između lokacija korištenjem PPP-a kako bi povezali udaljeno računalo na vašu System i platformu. Kroz PPP udaljeni sistemi koji su spojeni na vaš sistem mogu pristupiti resursima ili drugim strojevima koje pripadaju istoj mreži kao i vaš sistem. Možete također konfigurirati vaš system poslužitelj za povezivanje na Internet pomoću PPP-a. System i Navigator čarobnjak povezivanja biranjem može vas voditi kroz proces povezivanja sistema na Internet ili internu mrežu.

---

## PDF datoteka za Usluge daljinskog pristupa

Možete pogledati i ispisati PDF datoteku s ovim informacijama.


Za pregled ili spuštanje PDF verzije ovog dokumenta izaberite Usluge daljinskog pristupa: PPP veze (oko 940 KB).

### Spremanje PDF datoteka

Da spremite PDF na vašu radnu stanicu za gledanje ili ispis:

1. Desno kliknite PDF vezu u svom pretražitelju.
2. Kliknite na opciju koja sprema PDF lokalno.
3. Izaberite direktorij u koji želite spremiti PDF datoteku.
4. Kliknite **Save**.

### Spuštanje Adobe Readera

Trebate instaliran Adobe Reader na vašem sistemu za pogled ili ispis ovih PDF-ova. Možete dohvatiti besplatnu kopiju sa Adobe Web stranice ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

#### Srodne reference

“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63 IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

---

## PPP koncepti

Možete koristiti PPP za spajanje System i platforme na udaljene mreže, klijentska osobna računala, druge System i platforme, ili na pružatelja Internetskih usluga (ISP). Za potpuno korištenje mogućnosti ovog protokola trebate razumjeti i sposobnosti i5/OS podrške za ovaj protokol.

#### Srodne reference


“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63 IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

## Što je PPP

Point-to-Point Protokol (PPP) je TCP/IP protokol koji se koristi za spajanje dva računalna sistema. Računala koriste PPP za komunikaciju kroz telefonsku mrežu ili Internet.

PPP veza postoji kad su dva sistema fizički povezana preko telefonske linije. Možete koristiti PPP za spajanje jednog sistema na drugi. Na primjer, neka uspostavljena PPP veza između područnog i središnjeg ureda omogućuje bilo kojem uredu da prenosi podatke onom drugom uredu preko mreže.

PPP omogućuje međuoperabilnost između softvera za udaljeni pristup od različitih proizvođača. On također omogućuje višestrukim mrežnim komunikacijskim protokolima da koriste istu fizičku komunikacijsku liniju.

Sljedeći standardi Zahtjeva za Komentarom (RFC) opisuju PPP protokol. Možete naći više informacija o RFC-ovima na RFC Editor Web stranici .

- RFC-1661 Point-to-Point Protokol
- RFC-1662 PPP na HDLC-sličnom uokvirivanju
- RFC-1994 PPP CHAP

## Profili veza

Point-to-Point profili veze definiraju skup parametara i resursa za određene veze Point-to-Point (PPP) protokola. Možete pokrenuti profile koji koriste ove postavke parametara da biraju van (izvorište) ili da slušaju (primaju) PPP veze.

Možete koristiti sljedeća dva tipa profila za definiciju skupa karakteristika za PPP vezu ili skup veza:

- *Izvorišni profili veze* su point-to-point veze koje započinju u lokalnim sistemima i bivaju primljene od udaljenog sistema. Izlazne veze možete konfigurirati pomoću ovog objekta.
- *Primateljski profili veze* su point-to-point veze koje započinju na udaljenom sistemu i bivaju primljene od lokalnog sistema. Ulazne veze možete konfigurirati pomoću ovog objekta.

Profil veze specificira kako radi PPP veza. Informacije u profilu veze odgovaraju na ova pitanja:

- Koji tip protokola veze koristite? (PPP ili Serijski linijski protokol Interneta (SLIP))
- Da li vaš sistem kontaktira drugo računalo biranjem van (izvorište)? Da li vaš sistem čeka na primanje poziva sa drugog sistema (primatelj)?
- Koje komunikacijske linije koristi veza?
- Kako vaš sistem treba odrediti koju IP adresu koristiti?
- Kako vaš sistem provjerava autentičnost drugog sistema? Gdje bi vaš sistem trebao pohraniti informacije o provjeri autentičnosti?

Profil veze je logički prikaz sljedećih detalja povezivanja:

- Linija i tip profila
- Postavke višestrukih veza
- Udaljeni telefonski brojevi i opcije biranja
- Provjera ovlaštenja
- TCP/IP postavke: IP adrese i usmjeravanje te IP filtriranje
- Upravljanje poslom i prilagodba veze
- Poslužitelji imena domene

Sistem pohranjuje konfiguracijske informacije u profil veze. Ove informacije pružaju nužni kontekst kako bi sistem mogao uspostaviti PPP vezu sa drugim sistemom. Profil veze sadrži sljedeće podatke:

- **Tip protokola.** Možete izabrati između PPP i SLIP. IBM preporučuje korištenje PPP-a kad god je to moguće.
- **Izbor načina.** Izbor načina specificira tip veze i način rada za profil veze.

**Tip veze.** Ovo navodi tip linije na koji se veza naslanja i da li se radi o biranju (izvorište) ili odgovoru (primatelj). Možete izabrati između ovih tipova veza:

- Birana linija



- Iznajmljena (namjenska) linija
  - Protokol Tuneliranja Razine Dva (L2TP) (virtualna linija)
  - Point-to-point protokol preko Ethernet-a (PPPoE) (virtualna linija)
- PPPoE je podržan samo za izvorišne profile veze.
- **Način rada.** Dostupni način rada ovisi o tipu veza.

Tablica 1. Dostupni načini rada za izvorišne profile veze

Tip veza	Dostupni operacijski načini
Birana linija	<ul style="list-style-type: none"> <li>• Biranje</li> <li>• Biranje-na-zahtjev (samo biranje)</li> <li>• Biranje-na-zahtjev (odgovor omogućenog namjenskog ravnopravnog)</li> <li>• Biranje na zahtjev (omogućen udaljeni ravnopravan)</li> </ul>
Iznajmljena linija	Inicijator
L2TP	<ul style="list-style-type: none"> <li>• Inicijator</li> <li>• Inicijator višestrukog skoka</li> <li>• Daljinsko biranje</li> </ul>
PPP preko Ethernet-a	Inicijator

Tablica 2. Dostupni načini rada za primateljske profile veze

Tip veza	Dostupni operacijski načini
Birana linija	Odgovor
Iznajmljena linija	Terminator
L2TP	Terminator (Poslužitelj mreže)

- **Konfiguracija veze.** Ovo specificira tip linijske usluge koju ova veza koristi. Ovi izbori zavise o tipu izbora načina koji ste izabrali. Za biranu i iznajmljenu liniju možete izabrati nešto od ovog:
  - Pojedinačna linija
  - Skup linija
 Za sve tipove veze (iznajmljene, L2TP, PPPoE) izbor linije servisa je samo jedna linija.

#### Srodne reference

“Softverski i hardverski zahtjevi” na stranici 31

Okolina Point-to-Point Protokola (PPP) zahtjeva posjedovanje barem dva računala koja podržavaju PPP. Jedno od ovih računala, System i platforma, može biti davalac ili primatelj.

## Podrška politike grupe

Sad podrškom za grupnu politiku, mrežni administratori mogu definirati grupne politike zasnovane na korisnicima i upravljati resursima. Pojedini korisnicima može se pridružiti pristup politikama upravljanja kad se prijave na Point-to-Point protokolom (PPP) ili sesiju Protokola Tuneliranja Razine Dva (L2TP).

Korisnici se mogu identificirati po pripadanju pojedinoj klasi korisnika. Svaka klasa ima svoju jedinstvenu politiku koja definira ograničenja nad resursima (kao npr. broj dozvoljenih veza multilink snopa), attribute (kao IP prosljeđivanje) i identifikaciju postavki pravila filtra IP paketa koja se primjenjuju. Na primjer, sa podrškom grupne politike mrežni administratori mogu definirati grupu Rad\_Kod\_Kuće koja dozvoljava puni pristup mreži ili Prodavač\_Radnik grupa koja je ograničena samo na određeni skup usluga.

#### Srodne reference

“Scenarij: Povezivanje vašeg sistema sa PPPoE koncentраторom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke

Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23 Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

---

## Scenarij: Udaljeni pristup korištenjem PPP veza

Ovi scenariji opisuju kako radi Point-to-Point protokol i kako implementirati PPP okolinu u mreži. Scenariji također predstavljaju osnovne PPP koncepte koji mogu koristiti kako početnicima tako i iskusni korisnicima pri zadacima planiranja i konfiguracije.

### Srodne reference

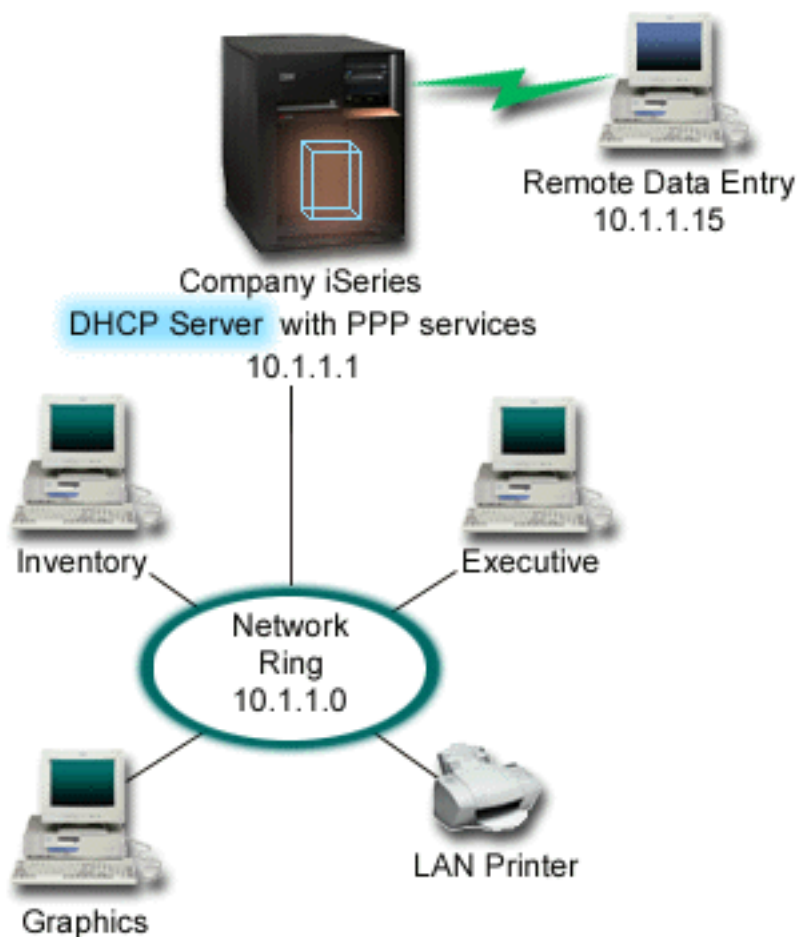
“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

## Primjer: PPP i DHCP na jedinstvenom System i

Ovaj primjer pokazuje kako postaviti System i model kao poslužitelj Protokola Konfiguracije Dinamičkog Hosta (DHCP) za LAN i udaljene klijente biranja.

Udaljeni klijenti, kao što su klijenti biranja, često zahtijevaju pristup mreži poduzeća. Klijenti biranja mogu dobiti pristup na System i model sa Point-to-Point protokolom (PPP). Za pristup mreži klijent biranja treba IP informacije kao i bilo koji drugi klijent koji se direktno spaja preko mreže. System i DHCP poslužitelj može distribuirati informacije o IP adresama PPP klijentu biranja kao i bilo kojem drugom direktno spojenom klijentu. Sljedeća slika prikazuje udaljenog klijenta koji mora birati unutar mreže poduzeća kako bi izvršio nekakav posao.



Slika 1. PPP i DHCP na jedinstvenom System i modelu

Kako bi udaljeni zaposlenik mogao uspješno biti dio mreže poduzeća, System i model mora koristiti kombinaciju Usluga Udaljenog Pristupa i DHCP. Funkcija Usluga Udaljenog Pristupa pruža mogućnost biranja za System i model. Ako se ispravno postavi, nakon što klijent uspostavi vezu kroz biranje PPP poslužitelj javlja DHCP poslužitelju da distribuiraju TCP/IP informacije udaljenom klijentu.

U ovom primjeru, jedna politika DHCP podmreže pokriva mrežne klijente na stranici i klijente s biranjem.

Ako želite da PPP profil čeka DHCP za IP distribuciju, morate to napraviti u PPP profilu. U TCP/IP postavkama profila primateljeve veze postavite metodu pridruživanja udaljene IP adrese sa Fiksne na DHCP. Kako bi klijenti biranja mogli komunicirati sa drugim mrežnim klijentom kao npr. LAN pisačem, morate također dozvoliti IP prosljeđivanje u TCP/IP postavkama profila i postavkama TCP/IP konfiguracije (stog). Ako IP prosljeđivanje postavite samo u PPP profilu, System i model neće propuštati IP pakete. Morate postaviti IP prosljeđivanje i u profilu i u stogu.

Također, lokalno sučelje IP adrese u PPP profilu mora biti IP adresa koja upada unutar definicije podmreže u DHCP poslužitelju. U ovom primjeru, IP adresa lokalnog sučelja PPP profila mora biti 10.1.1.1. Ova adresa također mora biti isključena iz DHCP poslužiteljskog spremišta adresa kako ne bi bila pridružena DHCP klijentu.

## Planiranje DHCP postava za stranicu i PPP klijente

Tablica 3. Globalne konfiguracijske opcije (odnosi se na sve klijente koje uslužuje DHCP poslužitelj)

Objekt		Vrijednost
Konfiguracijske opcije	Opcija 1: Maska pod mreže	255.255.255.0
	Opcija 6: Poslužitelj imenske domene	10.1.1.1
	Opcija 15: Ime domene	mycompany.com
Da li sistem vrši DNS ažuriranja?		Ne
Da li sistem podržava BOOTP klijente?		Ne

Tablica 4. Pod mreža za stranicu i klijente s biranjem

Objekt		Vrijednost
Ime pod mreže		MainNetwork
Adresa za upravljanje		10.1.1.3 - 10.1.1.150
Vrijeme najma		24 sata (default)
Konfiguracijske opcije	Naslijeđene opcije	Opcije iz Globalne konfiguracije
Adrese pod mreže nije dodijelio poslužitelj		10.1.1.1 (Adresa lokalnog sučelja specificirana u TCP/IP postavkama svojstava Profila Primateljeve Veze u System i Navigator)

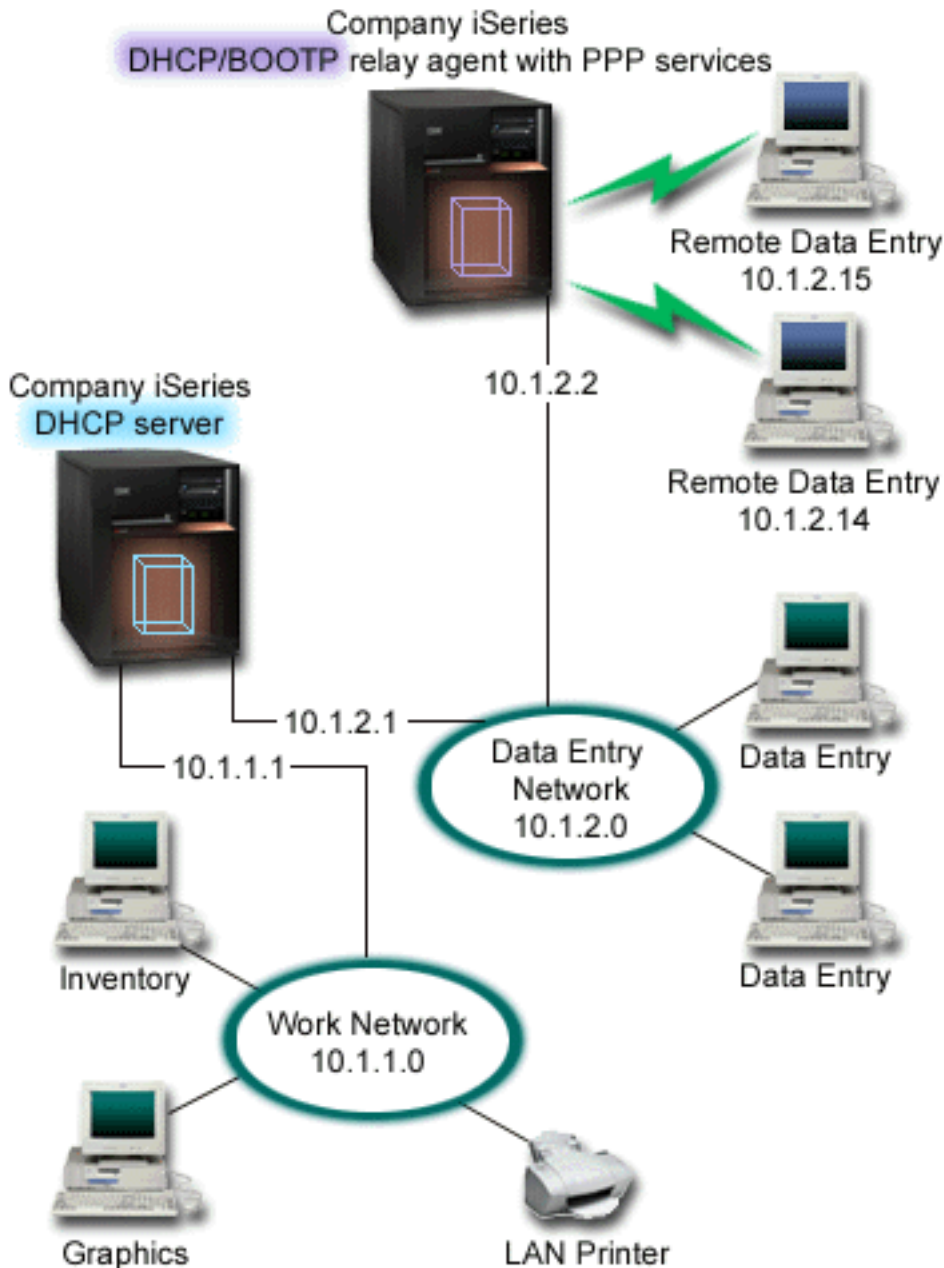
### Drugi postav

- Postavite metodu Udaljene IP adrese na DHCP u PPP profilu povezivanja primatelja.
  1. Omogućite DHCP WAN vezu sa DHCP poslužiteljem ili primopredajnu vezu korištenjem stavke izbornika **Usluge** za Usluge Udaljenog Pristupa u System i Navigator.
  2. Izaberite korištenje DHCP-a za metodu pridruživanja IP adrese pod Svojstvima TCP/IP Postavki profila Primateljeve Veze System i Navigator.
- Dozvolite pristup udaljenim sistemima prema drugim mrežama (IP prosljeđivanje) pod Svojstvima TCP/IP Postavki u Profilu Primateljeve Veze u System i Navigator.
- Omogućite prosljeđivanje IP datagrama pod Postavkama Svojstava TCP/IP konfiguracije u System i Navigator.

### Primjer: DHCP i PPP profili na različitim System i modelima

Ovaj primjer objašnjava kako postaviti dva System i modela kao mrežne poslužitelje Protokola Konfiguracije Dinamičkog Hosta (DHCP) i BOOT/DHCP posrednike primopredaje za dva LAN-a i udaljene klijente biranja.

Primjer PPP-a i DHCP-a na jedinstvenom System i modelu prikazuje kako koristiti PPP i DHCP na jedinstvenom sistemu kako bi se dozvolio pristup mreži klijentima biranja. Ako se brinete o fizičkom izgledu mreže ili o sigurnosti bilo bi bolje odvojiti PPP i DHCP poslužitelje ili imati namjenski PPP poslužitelj bez DHCP usluga. Sljedeća slika prikazuje mrežu koja ima klijente biranja sa PPP i DHCP politikama na različitim poslužiteljima.



Slika 2. DHCP i PPP profili na različitim System i modelima

Klijenti udaljenog unosa podataka biraju na System i PPP poslužitelj. PPP profil na tom poslužitelju mora imati DHCP-ovu metodu udaljene IP adrese poput one korištene u primjeru PPP i DHCP-a na jedinstvenom System i modelu. Svojstva PPP profila i TCP/IP stoga na PPP poslužitelju moraju imati IP prosljeđivanje. Nadalje, pošto ovaj poslužitelj djeluje kao DHCP posrednik primopredaje, BOOTP/DHCP posrednik primopredaje mora biti uključen. Ovo omogućuje System i poslužitelju Udaljenog Pristupa prosljeđivanje DHCPDISCOVER paketa na DHCP poslužitelj. DHCP poslužitelj potom odgovara i distribuira TCP/IP informacije na klijente biranja kroz PPP poslužitelj.

DHCP poslužitelj je odgovoran za distribuiranje IP adresa za 10.1.1.0 i 10.1.2.0 mreže. U mreži unosa podataka DHCP poslužitelj daje IP adrese u rasponu od 10.1.2.10 do 10.1.2.40 klijentima biranja te direktno priključenim klijentima. Klijenti unosa podataka također trebaju adresu usmjeritelja (opcija 3) 10.1.2.1 za komunikaciju sa poslovnom mrežom i System i DHCP poslužitelj također mora imati omogućeno IP prosljeđivanje.

Također, IP adresa lokalnog sučelja u PPP profilu mora biti IP adresa koja upada u definiciju pod mreže DHCP poslužitelja. U ovom primjeru, adresa Lokalnog sučelja PPP profila mora biti 10.1.2.2. Ova adresa mora biti isključena iz spremišta adresa DHCP poslužitelja tako da nije pridružena DHCP klijentu. IP adresa lokalnog sučelja mora biti adresa na koju DHCP poslužitelj može slati pakete odgovora.

## Planiranje DHCP postava za DHCP s DHCP posrednikom primopredaje

Tablica 5. Globalne konfiguracijske opcije (odnosi se na sve klijente koje uslužuje DHCP poslužitelj)

Objekt	Vrijednost	
Konfiguracijske opcije	Opcija 1: Maska pod mreže	255.255.255.0
	Opcija 6: Poslužitelj imenske domene	10.1.1.1
	Opcija 15: Ime domene	mycompany.com
Da li sistem vrši DNS ažuriranja?	Ne	
Da li sistem podržava BOOTP klijente?	Ne	

Tablica 6. Pod mreža Radne mreže

Objekt	Vrijednost
Ime pod mreže	WorkNetwork
Adresa za upravljanje	10.1.1.3 - 10.1.1.150
Vrijeme najma	24 sata (default)
Konfiguracijske opcije	Nasliedene opcije Opcije iz Globalne konfiguracije
Adrese pod mreže nije dodijelio poslužitelj	ništa

Tablica 7. Pod mreža mreže podatkovnog unosa

Objekt	Vrijednost	
Ime pod mreže	DataEntry	
Adresa za upravljanje	10.1.2.10 - 10.1.2.40	
Vrijeme najma	24 sata (default)	
Konfiguracijske opcije	Opcija 3: Usmeritelj	10.1.2.1
	Nasliedene opcije	Opcije iz Globalne konfiguracije
Adrese pod mreže nije dodijelio poslužitelj	10.1.2.1 (usmjerivač) 10.1.2.15 (IP adresa lokalnog sučelja Klijenta Udaljenog Unosa Podataka) 10.1.2.14 (IP adresa lokalnog sučelja Klijenta Udaljenog Unosa Podataka)	

## Druge postavke na System i platformi koja izvodi PPP

- Postavljanje BOOTP/DHCP posrednika primopredaje TCP/IP poslužitelja

Objekt	Vrijednost
Adresa sučelja	10.1.2.2
Primopredajni paketi za IP adresu poslužitelja	10.1.2.1

- Postavite metodu Udaljene IP adrese na DHCP u PPP profilu povezivanja primatelja
  1. Omogućite DHCP WAN vezu sa DHCP poslužiteljem ili primopredajnu vezu korištenjem stavke izbornika **Usluge** za Usluge Udaljenog Pristupa u System i Navigator.

2. Izaberite korištenje DHCP-a za metodu pridruživanja IP adrese pod Svojstvima TCP/IP Postavki profila Primateljve Veze System i Navigator.
- Dozvolite pristup udaljenim sistemima prema drugim mrežama (IP prosljeđivanje) pod Svojstvima TCP/IP Postavki u Profilu Primateljve Veze u System i Navigator (kako bi omogućili udaljenim klijentima komunikaciju sa mrežom za unos podataka)
  - Dozvolite pristup udaljenim sistemima prema drugim mrežama (IP prosljeđivanje) pod Svojstvima TCP/IP Postavki u Profilu Primateljve Veze u System i Navigator (kako bi omogućili udaljenim klijentima komunikaciju sa mrežom za unos podataka)

## Scenarij: Zaštita L2TP dobrovoljnog tunela pomoću IPsec-a

U ovom scenariju, naučite kako postaviti vezu između hosta područnog ureda i korporativnog ureda koji koristi L2TP koji štiti IPsec. Područni ured ima dinamički dodijeljenu IP adresu, dok korporativni ured ima statičku, globalno usmjerljivu IP adresu.

### Situacija

Pretpostavite da vaše poduzeće ima manji područni ured u drugoj županiji. U bilo kojem radnom danu ured podružnice može trebati pristup tajnim informacijama o System i modelu unutar korporativnog intraneta. Vaše poduzeće trenutno koristi skupe iznajmljene linije da omogući područnom uredu pristup na korporativnu mrežu. Iako vaše poduzeće želi nastaviti omogućavati siguran pristup vašem intranetu, vi odlučno želite smanjiti trošak koji za sobom nosi iznajmljena linija. To se može napraviti kreiranjem Sloj 2 Tunelskog protokola (L2TP) dobrovoljnog tunela koji proširuje vašu korporativnu mrežu, tako da se čini da je područni ured dio vaše korporativne podmreže. VPN štiti promet podataka preko L2TP tunela.

Pomoću L2TP dobrovoljnog tunela, udaljeni područni ured postavlja tunel direktno na L2TP mrežni poslužitelj (LNS) korporativne mreže. Funkcionalnost L2TP koncentratora pristupa (LAC) se nalazi na klijentu. Tunel je transparentan za Dobavljača Internet usluga (ISP) udaljenog klijenta, zato nije potrebno da ISP podržava L2TP. Ako želite više pročitati o L2TP konceptima, pogledajte Tunel protokol sloja 2 (L2TP).

**Važno:** Ovaj scenarij prikazuje sigurnosne gatewaye koji su direktno spojeni na Internet. Nepostojanje vatrenog zida je zbog jednostavnosti scenarija. To ne znači da upotreba vatrenog zida nije potrebna. Uzmite u obzir sigurnosne mjere svaki put kad se povezujete na Internet.

### Ciljevi

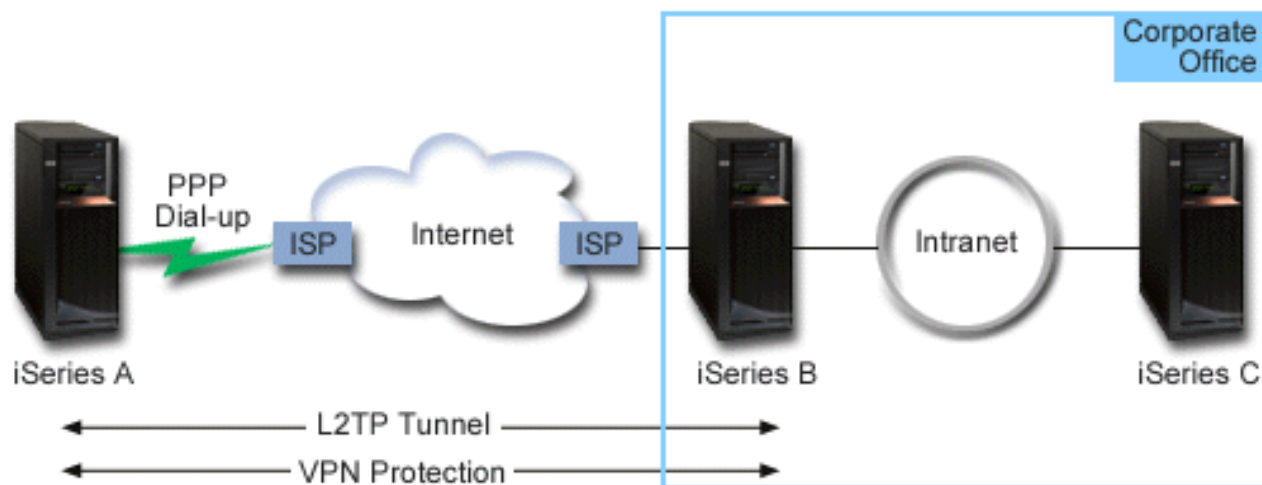
U ovom scenariju, sistem područnog ureda se spaja na korporativnu mrežu preko gateway sistema s L2TP tunelom koji štiti VPN.

Glavni ciljevi ovog scenarija su:

- Sistem područnog ureda uvijek započinje vezu s korporativnim uredom.
- Sistem područnog ureda je jedini sistem na mreži područnog ureda koji treba pristup na korporativnu mrežu. Drugim riječima, njegova uloga je uloga hosta, a ne prilaza, na mreži područnog ureda.
- Korporativni sistem je host računalo na mreži korporativnog ureda.

## Detalji

Sljedeća slika ilustrira mrežne karakteristike za ovaj scenarij:



### Sistem A

- Mora imati pristup TCP/IP aplikacijama na svim sistemima u korporativnoj mreži.
- Prima dinamički dodijeljene IP adrese od svog ISP-a.
- Mora biti konfiguriran da omogući L2TP podršku.

### Sistem B

- Mora imati pristup TCP/IP aplikacijama na Sistemu A.
- Podmreža je 10.6.0.0 s maskom 255.255.0.0. Ova podmreža za podatke predstavlja krajnju točku VPN tunela na korporativnoj strani.
- Povezuje se na Internet s IP adresom 205.13.237.6. Ovo je krajnja točka veze. Tj. Sistem B vrši upravljanje ključevima i primjenjuje IPSec na dolazne i odlazne IP datagrame. Sistem B spaja se na svoju podmrežu pomoću IP adrese 10.6.11.1.

U terminima L2TP, *Sistem A* vrši dužnost L2TP inicijatora, dok *Sistem B* vrši dužnost L2TP terminatora.

## Konfiguracijski zadaci

Pod pretpostavkom da TCP/IP konfiguracija već postoji i radi, morate dovršiti sljedeće zadatke:

## Scenarij: Povezivanje vašeg sistema sa PPPoE konzentratom pristupa

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

### Situacija

Vaš posao zahtjeva bržu vezu sa Internetom tako da vas zanima usluga Digitalne Pretplatničke Linije (DSL) od vašeg lokalnog Pružatelja Internetskih Usluga (ISP). Nakon početnog istraživanja, otkrili ste da vaš ISP koristi PPPoE za povezivanje svojih klijenata. Trebate koristiti ovu PPPoE vezu kako bi omogućili veze visoke brzine prema Internetu



kroz vaš sistem.



Slika 3. Spajanje vašeg sistema na ISP sa PPPoE

## Rješenje

Možete podržavati PPPoE vezu sa ISP-om kroz vaš sistem. Sistem koristi novi PPPoE tip virtualne linije koji je povezan sa fizičkom Ethernet linijom konfiguriranom za korištenje Ethernet adaptora tipa 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A ili 576A. Ova virtualna linija podržava PPP protokole sesije preko Ethernet Lokalne mreže (LAN) koja je spojena na DSL modem koji pruža prilaz udaljenom ISP-u. Ovaj prilaz dozvoljava korisnicima LAN-a pristup visoke brzine Internetu korištenjem PPPoE veze. Nakon što je započela veza između sistema i ISP-a, pojedini korisnici mogu pristupiti ISP-u preko PPPoE korištenjem IP adrese dodijeljene sistemu. Da se pruži dodatna sigurnost, mogu se primijeniti pravila filtriranja na PPPoE virtualnu liniju radi ograničavanja određenog ulaznog Internet prometa.

## Primjer konfiguracije

Za postavljanje PPP konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. Konfigurirajte uređaj za korištenje odnosno za povezivanje s vašim ISP-om.
2. Konfigurirajte izvorni profil veze na vašem sistemu.  
Svakako upišite sljedeće informacije:
  - **Tip protokola:** PPP
  - **Tip povezivanja:** PPP preko Ethernet
  - **Način rada:** Inicijator
  - **Konfiguracija veze:** Jedna linija
3. Na stranici Općenito Svojstava novog Point-to-Point profila, unesite ime i opis profila davatelja. Ovo ime se odnosi na profil povezivanja i virtualnu PPPoE liniju.
4. Kliknite **Povezivanje** da biste otvorili stranicu Povezivanje. Izaberite **Ime PPPoE virtualne linije** koje odgovara imenu ovog profila povezivanja. Nakon što izaberete liniju, System i Navigator prikazuje dijalog kućicu **svojstva linije**.

- a. Na stranici Općenito, unesite smisleni opis za PPPoE virtualnu liniju.
- b. Kliknite **Veza** da biste otvorili stranicu Veza. S popisa Ime fizičke linije izaberite Ethernet liniju koja će koristiti ovo povezivanje i kliknite **Otvori**. Alternativno, ako trebate definirati novu Ethernet liniju, upišite ime linije i kliknite **Novo**. System i Navigator prikazuje dijalog kućicu **Svojstva Ethernet linije**.

**Bilješka:** PPPoE zahtjeva Ethernet adaptor tipa 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A ili 576A.

- 1) Na stranici Općenito unesite smisleni opis Ethernet linije i provjerite da li definicija linije koristi potrebne hardverske resurse.
  - 2) Kliknite **Veza** da biste otvorili stranicu Veza. Unesite svojstva za fizičku Ethernet liniju. Pogledajte dokumentaciju Ethernet adaptera i online pomoć za više informacija.
  - 3) Kliknite **Ostalo** da biste otvorili stranicu Ostalo. Specificirajte razinu pristupa i ovlaštenja kojeg korisnici mogu imati za ovu liniju.
  - 4) Kliknite **OK** za povratak na stranicu Svojstva PPPoE virtualne linije.
  - c. Kliknite **Granice** da biste definirali svojstva LCP provjere autentičnosti ili kliknite **OK** da biste se vratili na stranicu Novi profil Point-to-Point povezivanja.
  - d. Kada se vratite na stranicu Povezivanje, specificirajte adresiranje PPPoE poslužitelja na temelju informacija od ISP-a.
5. Ako vaš ISP zahtijeva provjeru autentičnosti sistema ili želite da sistem provjeri autentičnost udaljenog sistema, kliknite **Provjera autentičnosti** kako bi otvorili stranicu Provjera autentičnosti i unijeli potrebne informacije.
  6. Kliknite **TCP/IP postavke** da biste otvorili stranicu TCP/IP i specificirali parametre rukovanja IP adresom za ovaj profil povezivanja. Postavku koju treba koristiti treba dostaviti vaš ISP. Kako bi dozvolili korisnicima LAN-a spajanje na ISP korištenjem IP adrese dodijeljene sistemu, izaberite **Sakrij adrese (Potpuno Maskiranje)**.
  7. Kliknite **DNS** da biste otvorili DNS stranicu i unesite IP adresu DNS poslužitelja kojeg je osigurao ISP.
  8. Kliknite **OK** da dovršite profil.

#### **Srodni koncepti**

“Podrška politike grupe” na stranici 3

Sad podrškom za grupnu politiku, mrežni administratori mogu definirati grupne politike zasnovane na korisnicima i upravljati resursima. Pojedini korisnicima može se pridružiti pristup politikama upravljanja kad se prijave na Point-to-Point protokolom (PPP) ili sesiju Protokola Tuneliranja Razine Dva (L2TP).

#### **Srodni zadaci**

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

#### **Srodne reference**

“Konfiguracija veze” na stranici 49

Konfiguracija veze definira tip servisne linije koju profil veze Protokola Point-to-Point (PPP) koristi za uspostavljanje veze<sup>4</sup>.

“Sistemska provjera ovlaštenja” na stranici 42

PPP veze sa System i platformom podržavaju nekoliko opcija provjere autentičnosti, kako udaljenih klijenata koji biraju u sistem, tako i veze prema ISP-u ili drugom sistemu prema kojima sistem bira.

“Rukovanje IP adresama” na stranici 40

Point-to-Point Protokol (PPP) veze omogućuju nekoliko različitih skupova opcija za upravljanje IP adresama ovisno o tipu profila veze.

“Filtriranje IP paketa” na stranici 40

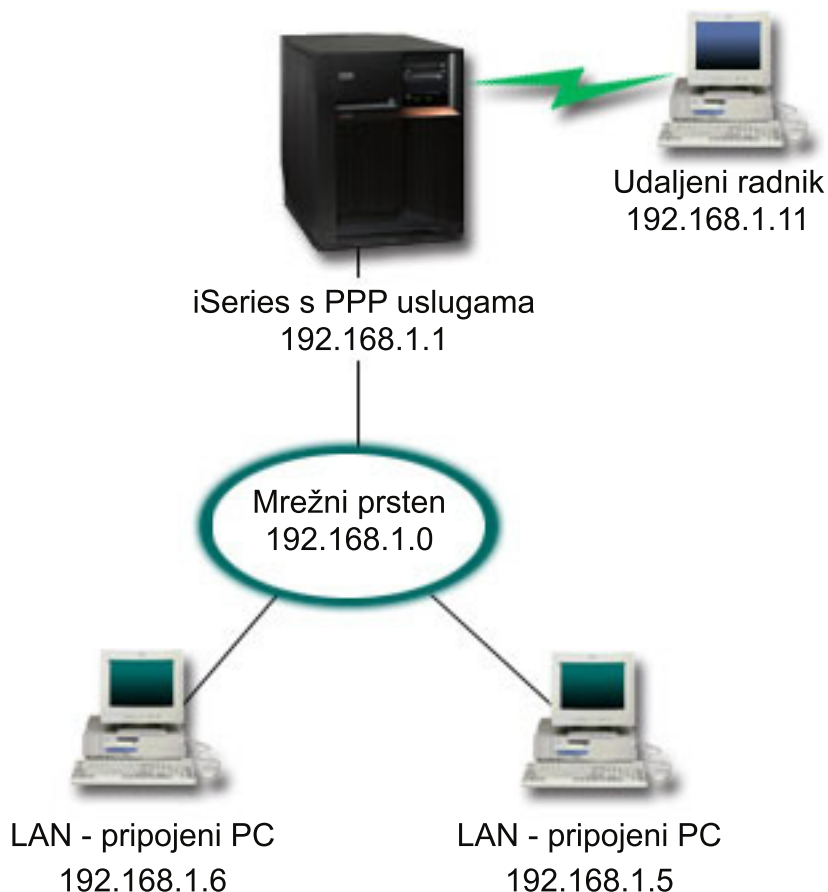
Filtriranje IP paketa ograničava usluge pojedinim korisnicima koji se prijavljuju na mrežu.

## **Scenarij: Spajanje udaljenih klijenata biranja na sistem**

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

## Situacija

Kao administrator korporativne mreže morate održavati i sistemske i mrežne klijente. Umjesto dolaska na posao za rješavanje i popravljavanje problema, potrebna vam je mogućnost rada s udaljene lokacije, kao što je vaš dom. Zbog toga što vaša tvrtka nema mrežnu vezu prema Internetu morate birati u sistem korištenjem PPP veze. Dodatno, jedini modem kojeg trenutno imate je vaš 7852-400 modem elektroničke korisničke podrške i trebate baš njega koristiti za ovu vezu.



Slika 4. Spajanje udaljenih klijenata na vaš sistem

## Rješenje

Možete koristiti PPP za spajanje vašeg kućnog računala na vaš sistem korištenjem modema. Pošto koristite modem elektroničke korisničke podrške za ovaj tip PPP veze morate biti sigurni da je vaš modem konfiguriran i za sinkroni i asinkroni način rada. Slika prikazuje sistem sa PPP uslugama koji je spojen na LAN sa dva računala. Udaljeni radnik potom bira u sistem. Sistem sam provjerava svoju autentičnost i postaje dio radne mreže 192.168.1.0). U tom slučaju, najlakše je dodijeliti statičku IP adresu klijentu koji naziva.

Udaljeni radnik koristi Protokol provjere autentičnosti izazovom rukovanja (CHAP-MD5) kako bi se provjerila autentičnost sa sistemom. Sistem ne može koristiti MS CHAP tako da morate biti sigurni da vaš PPP klijent koristi CHAP-MD5.

Ako želite da vaši udaljeni radnici imaju pristup mreži poduzeća kao što je to gore navedeno, IP prosljeđivanje mora biti postavljeno u TCP/IP stogu kao i vaš PPP profil primatelja, a IP usmjerenje mora biti ispravno konfigurirano. Ako želite ograničiti ili zaštititi akcije koje vaši udaljeni klijenti mogu raditi na vašoj mreži, morate upotrijebiti pravila filtriranja za rukovanje s njihovim IP paketima.

Prethodna slika ima samo jednog udaljenog klijenta biranja pošto model elektroničke korisničke podrške može rukovati samo jednom vezom odjednom.

## Primjer konfiguracije

Za postavljanje PPP konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. Konfigurirajte Dial-up Networking i kreirajte biranu vezu na udaljenom PC-u.
2. Konfigurirajte primateljski profil veze na vašem sistemu.  
Svakako upišite sljedeće informacije:
  - **Tip protokola:** PPP
  - **Tip povezivanja:** Komutirana linija
  - **Način rada:** Odgovor
  - **Konfiguracija veze:** Ovo može biti jedna linija ili spremište linija, ovisno o okolini.
3. Na stranici Općenito odjeljka Svojstva novog point-to-point profila unesite ime i opis profila primatelja.
4. Kliknite **Povezivanje** da biste otvorili stranicu Povezivanje. Izaberite odgovarajuće **Ime linije** ili kreirajte novu liniju tako da upišete novo ime i kliknete **Novo**.
  - a. Na stranici Općenito osvjetlite postojeći hardverski resurs gdje je pripojen 7852-400 adaptor i postavite Uokvirenje na **Asinkrono**.
  - b. Kliknite **Modem** da biste otvorili stranicu Modem. S popisa za izbor Imena, izaberite modem **IBM 7852-400**.
  - c. Kliknite **OK** da se vratite na stranicu Svojstva novog point-to-point profila.
5. Kliknite **Provjera autentičnosti** da biste otvorili stranicu Provjera autentičnosti.
  - a. Označite **Zatraži ovaj iSeries poslužitelj provjeru identiteta udaljenog sistema**.
  - b. Izaberite **Provjerite ovlaštenje lokalno pomoću validacijske liste** i dodajte novog udaljenog korisnika na validacijsku listu.
  - c. Izaberite **Dozvoli šifriranu lozinku (CHAP-MD5)**.
6. Kliknite **TCP/IP postavke** da biste otvorili TCP/IP stranicu.
  - a. Izaberite za lokalnu IP adresu 192.168.1.1.
  - b. Za udaljenu IP adresu izaberite **Stalna IP adresa** s početnom IP adresom 192.168.1.11.
  - c. Izaberite **Dozvoli pristup udaljenog sistema drugim mrežama**.
7. Kliknite **OK** da dovršite profil.

### Srodni koncepti

“Planiranje PPP-a” na stranici 31

Planiranje Point-to-Point protokola (PPP) uključuje stvaranje i administriranje PPP veza.

### Srodni zadaci

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

### Srodne reference

“Protokol Provjere autentičnosti izazova rukovanjem s MD5” na stranici 43

Protokol Provjere autentičnosti izazova rukovanjem (CHAP-MD5) koristi algoritam (MD-5) za izračunavanje vrijednosti koja je poznata samo sistemu za koji se obavlja provjera autentičnosti i udaljenom uređaju.

“Konfiguracija veze” na stranici 49

Konfiguracija veze definira tip servisne linije koju profil veze Protokola Point-to-Point (PPP) koristi za uspostavljanje veze<sup>4</sup>.

“Skup linija” na stranici 49

Za postavljanje PPP veze na korištenje linije iz spremišta linija izaberite ovu uslugu linija. Kad PPP veza započne sistem izabire neiskorištenu liniju iz spremišta linija. Za profile biranja na zahtjev sistem ne izabire linije dok ne uoči TCP/IP promet za udaljeni sistem.

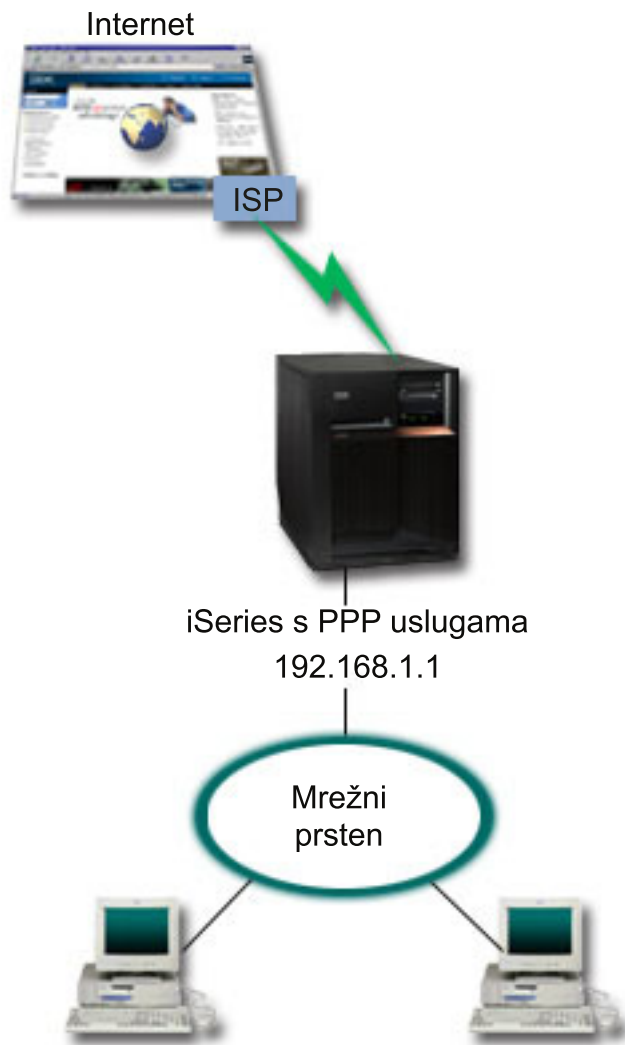
## **Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema**

Administratori u tipičnom slučaju postavljaju uredske mreže kako bi omogućili zaposlenicima izlaz na Internet.

Administratori mogu koristiti modem za spajanje sistema na Pružatelja Internetskih Usluga (ISP). PC klijenti spojeni na LAN mogu komunicirati sa Internetom koristeći i5/OS operativni sistem kao prilaz.

### **Situacija**

Korporativna aplikacija koju vaša kompanija koristi zahtjeva pristup korisnika na Internet. Pošto aplikacija ne zahtjeva prijenos velikih količina podataka morate biti u mogućnosti koristiti modem za spajanje sistema i LAN klijenata na Internet. Sljedeća slika prikazuje primjer ove situacije.



Slika 5. Spajanje vašeg uredskog LAN-a na Internet pomoću modema

## Rješenje

Možete koristiti vaš integrirani (ili bilo koji drugi kompatibilni) modem kako bi spojili vaš sistem na vaš ISP. Morate stvoriti izvorni profil Point-to-Point (PPP) protokola na sistemu kako bi uspostavili PPP vezu na ISP.

Nakon što napravite vezu između sistema i ISP-a, vaši PC-ji na LAN-u mogu komunicirati sa Internetom koristeći sistem kao prilaz. U izvornom profilu morate biti sigurni da je uključena opcija Sakrivanje adresa kako bi LAN klijenti mogli imati privatne IP adrese za komunikaciju sa Internetom.

Sad kad su vaš sistem i mreža priključeni na Internet morate biti upoznati sa sigurnosnim rizicima. Radite zajedno sa ISP-om kako bi razumjeli njihove sigurnosne politike i poduzmite dodatne akcije za zaštitu sistema i mreže.

Ovisno u korištenju Interneta, pojasna širina može postati velika briga.

## Primjer konfiguracije

Za postavku konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. Konfigurirajte izvorišni profil veze na vašem sistemu.  
Svakako izaberite sljedeće informacije:
  - **Tip protokola:** PPP
  - **Tip povezivanja:** Komutirana linija
  - **Način rada:** Biranje
  - **Konfiguracija veze:** Ovo može biti jedna linija ili spremište linija, ovisno o okolini.
2. Na stranici Općenito Svojstava novog Point-to-Point profila, unesite ime i opis profila davatelja.
3. Kliknite **Povezivanje** da biste otvorili stranicu Povezivanje. Izaberite odgovarajuće Ime linije ili kreirajte novu liniju tako da upišete novo ime i kliknete **Novo**.
  - a. Na stranici Općenito svojstava nove linije, osvjetlite postojeći hardverski resurs. Ako izaberete interni modemski resurs, tada će postavke za tip modema i tip uokvirenja biti izabrane automatski.
  - b. Kliknite **OK** da se vratite na stranicu Svojstva novog point-to-point profila.
4. Kliknite **Dodaj** i upišite telefonski broj za dobivanje ISP poslužitelja. Svakako uključite bilo koji traženi prefiks.
5. Kliknite **Provjera autentičnosti** da biste otvorili stranicu Provjera autentičnosti, izaberite **Dozvoli udaljenom sistemu provjeru identifikacije ovog iSeries poslužitelja**. Izaberite protokol za provjeru ovlaštenja i upišite bilo koje traženo ime korisnika i lozinku.
6. Kliknite **TCP/IP postavke** da biste otvorili TCP/IP stranicu.
  - a. Izaberite **Dodijeljeno od udaljenog sistema** i za lokalne i za udaljene IP adrese.
  - b. Izaberite **Dodaj udaljeni sistem kao default smjer**.
  - c. Označite **Sakrij adrese** tako da se vaše interne IP adrese ne usmjeruju na Internet.
7. Kliknite **DNS** za otvaranje stranice Poslužitelja Domenskih Imena (DNS), unesite IP adresu DNS poslužitelja koju ste dobili od ISP-a.
8. Kliknite **OK** da dovršite profil.

Za korištenje profila veze za spajanje na Internet, desni klik na profil veze iz System i Navigator i izaberite **Pokreni**. Veza je uspješna kad se status promijeni u **Aktivna**. Osvježite da ažurirate prikaz.

**Bilješka:** Morate biti sigurni da drugi sistemi na mreži imaju ispravno definirano usmjeravanje kako bi odlazni TCP/IP promet sa tih sistema bio poslan kroz sistem na Internet.

### Srodni koncepti

“Planiranje PPP-a” na stranici 31

Planiranje Point-to-Point protokola (PPP) uključuje stvaranje i administriranje PPP veza.

### Srodni zadaci

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

### Srodne reference

“Skup linija” na stranici 49

Za postavljanje PPP veze na korištenje linije iz spremišta linija izaberite ovu uslugu linija. Kad PPP veza započne sistem izabire neiskorištenu liniju iz spremišta linija. Za profile biranja na zahtjev sistem ne izabire linije dok ne uoči TCP/IP promet za udaljeni sistem.

“Konfiguracija veze” na stranici 49

Konfiguracija veze definira tip servisne linije koju profil veze Protokola Point-to-Point (PPP) koristi za uspostavljanje veze<sup>4</sup>.

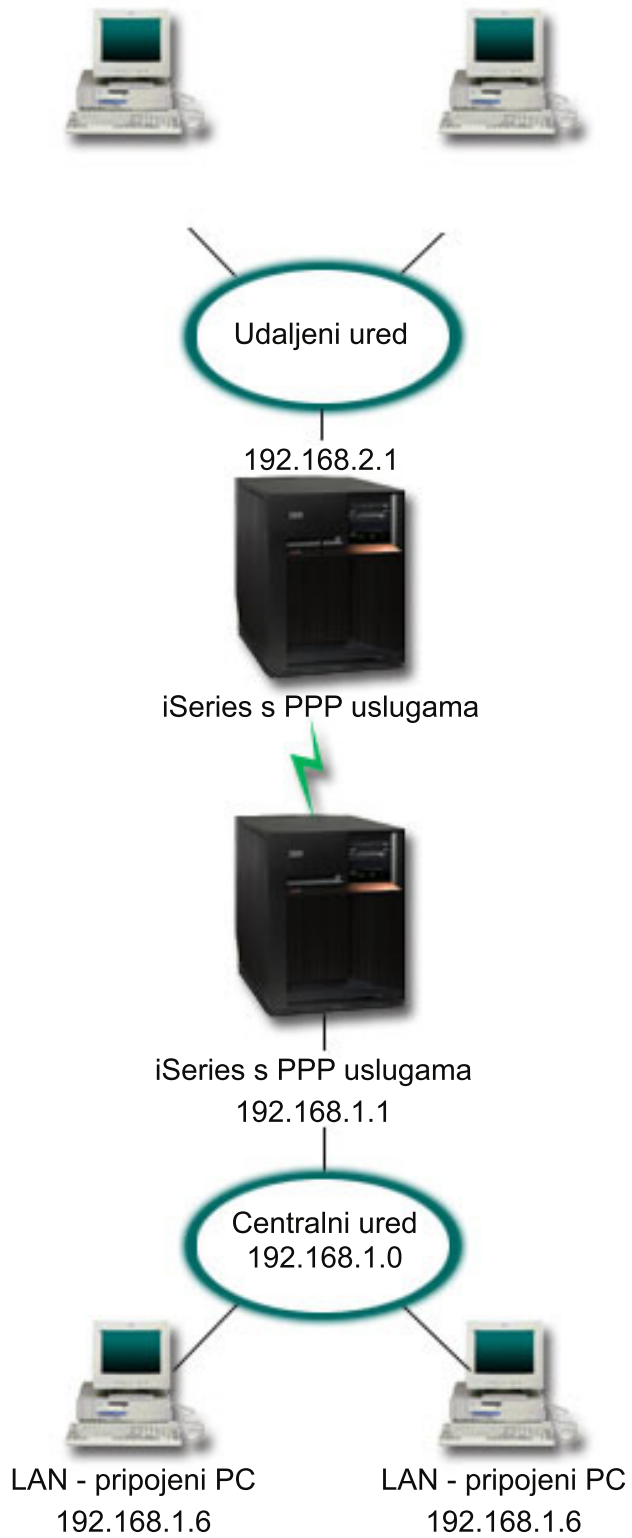
## **Scenarij: spajanje vaše korporativne i udaljene mreže modemom**

Modem omogućuje izmjenu podataka između dvije udaljene lokacije (kao npr. centralni ured i podružnica). Point-to-Point Protokol (PPP) može spojiti dva LAN-a postavljanjem veze između sistema u centralnom uredu i drugom u podružnici.

### **Situacija**

Pretpostavimo da imate područne i korporativne mreže na različitim lokacijama. Svaki dan se područni ured treba povezati sa centralnim uredom radi izmjene informacija baze podataka za njihove aplikacije za unos podataka. Količina tako izmijenjenih podataka ne opravdava kupovinu fizičke mrežne veze, tako da ste odlučili koristiti modeme za spajanje dviju mreža prema potrebi.





Slika 6. Spajanje vaše korporativne i udaljene mreže modemom

## Rješenje

PPP može spojiti dva LAN-a postavljanjem veze između sistema kao što je prikazano na slici. U tom slučaju, pretpostavite da udaljeni ured započinje vezu sa središnjim uredom. Možete konfigurirati izvorišni profil na udaljenom sistemu i primateljski profil na sistemu centralnog ureda.

Ako udaljena uredska računala trebaju pristupiti na korporativni LAN (192.168.1.0), primateljski profil centralnog ureda će trebati imati uključeno IP prosljeđivanje te mora biti omogućeno usmjeravanje IP adresa za računala (u ovom primjeru 192.168.2, 192.168.3, 192.168.1.6 i 192.168.1.5). Također, mora biti aktivirano IP prosljeđivanje za TCP/IP stog. Ta konfiguracija omogućuje osnovnu TCP/IP komunikaciju između LAN-ova. Trebate razmotriti sigurnosne faktore i DNS da riješite imena hostova između LAN-ova.

## Primjer konfiguracije

Za postavku konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. Konfigurirajte izvorišni profil veze na udaljenom uredskom sistemu.  
Svakako izaberite sljedeće informacije:
  - **Tip protokola:** PPP
  - **Tip povezivanja:** Komutirana linija
  - **Način rada:** Biranje
  - **Konfiguracija veze:** Ovo može biti jedna linija ili spremište linija, ovisno o okolini.
2. Na stranici Općenito Svojstava novog Point-to-Point profila, unesite ime i opis profila davatelja.
3. Kliknite **Povezivanje** da biste otvorili stranicu Povezivanje. Izaberite odgovarajuće Ime linije ili kreirajte novu liniju tako da upišete novo ime i kliknete **Novo**.
  - a. Na stranici Općenito svojstava nove linije, osvjetlite hardverski resurs i postavite Uokvirenje na **Asinkrono**.
  - b. Kliknite **Modem** da biste otvorili stranicu Modem. S popisa za izbor Imena, izaberite modem koji koristite.
  - c. Kliknite **OK** da se vratite na stranicu Svojstva novog point-to-point profila.
4. Kliknite **Dodaj** i upišite telefonski broj za dobivanje centralnog uredskog sistema. Pazite da uključite potrebne predbrojeve.
5. Kliknite **Provjera autentičnosti** da biste otvorili stranicu Provjera autentičnosti i izaberite **Dozvoli udaljenom sistemu provjeru identifikacije ovog iSeries poslužitelja**. Izaberite **Zahijeva šifriranu lozinku (CHAP-MD5)** i unesite potrebno korisničko ime i lozinku.
6. Kliknite **TCP/IP postavke** da biste otvorili stranicu TCP/IP postavke.
  - a. Za lokalnu IP adresu, izaberite IP adresu LAN sučelja udaljenog ureda (192.168.2.1) iz kućice za izbor **Koristi fiksnu IP adresu**.
  - b. Za udaljenu IP adresu, izaberite **Dodijeljeno od udaljenog sistema**.
  - c. U dijelu za usmjeravanje, izaberite **Dodaj udaljeni sistem kao default smjer**.
  - d. Kliknite **OK** da završite profil davatelja.
7. Konfigurirajte primateljski profil veze na vašem centralnom uredskom sistemu.  
Svakako izaberite sljedeće informacije:
  - **Tip protokola:** PPP
  - **Tip povezivanja:** Komutirana linija
  - **Način rada:** Odgovor
  - **Konfiguracija veze:** Ovo može biti jedna linija ili spremište linija, ovisno o okolini.
8. Na stranici Općenito odjeljka Svojstva novog point-to-point profila unesite ime i opis profila primatelja.
9. Kliknite **Povezivanje** da biste otvorili stranicu Povezivanje. Izaberite odgovarajuće Ime linije ili kreirajte novu liniju tako da upišete novo ime i kliknete **Novo**.
  - a. Na stranici Općenito osvjetlite postojeći hardverski resurs i postavite Uokvirenje na **Asinkrono**.
  - b. Kliknite **Modem** da biste otvorili stranicu Modem. S popisa za izbor Imena, izaberite modem koji koristite.

- c. Kliknite **OK** da se vratite na stranicu Svojstva novog point-to-point profila.
10. Kliknite **Provjera autentičnosti** da biste otvorili stranicu Provjera autentičnosti.
  - a. Označite **Zatraži ovaj iSeries poslužitelj provjeru identiteta udaljenog sistema**.
  - b. Dodajte novog udaljenog korisnika na validacijsku listu.
  - c. Označite CHAP-MD5 provjeru ovlaštenja.
11. Kliknite **TCP/IP postavke** da biste otvorili stranicu TCP/IP postavke.
  - a. Za lokalnu IP adresu, izaberite IP adresu sučelja centralnog ureda (192.168.1.1) iz kućice **Izaberi**.
  - b. Za udaljenu IP adresu, izaberite **Bazirano na ID-u korisnika udaljenog sistema**. Pojavit će se dijalog **IP adrese definirane korisničkim imenom**. Kliknite **Dodaj**. Popunite polja Ime korisnika pozivatelja, IP adresa i Maska pod mreže. U našem scenariju bit će prikladno sljedeće:
    - Ime korisnika pozivatelja: Remote\_site
    - IP adresa: 192.168.2.1
    - Maska pod mreže: 255.255.255.0

Kliknite **OK** i kliknite **OK** opet da se vratite na stranicu TCP/IP postavke.

  - c. Izaberite **IP prosljeđivanje** kako bi omogućili drugim sistemima na mreži korištenje ovog sistema kao prilaz.
12. Kliknite **OK** da završite profil primatelja.

#### **Srodni zadaci**

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

#### **Srodne reference**

“Konfiguracija veze” na stranici 49

Konfiguracija veze definira tip servisne linije koju profil veze Protokola Point-to-Point (PPP) koristi za uspostavljanje veze4.

“Skup linija” na stranici 49

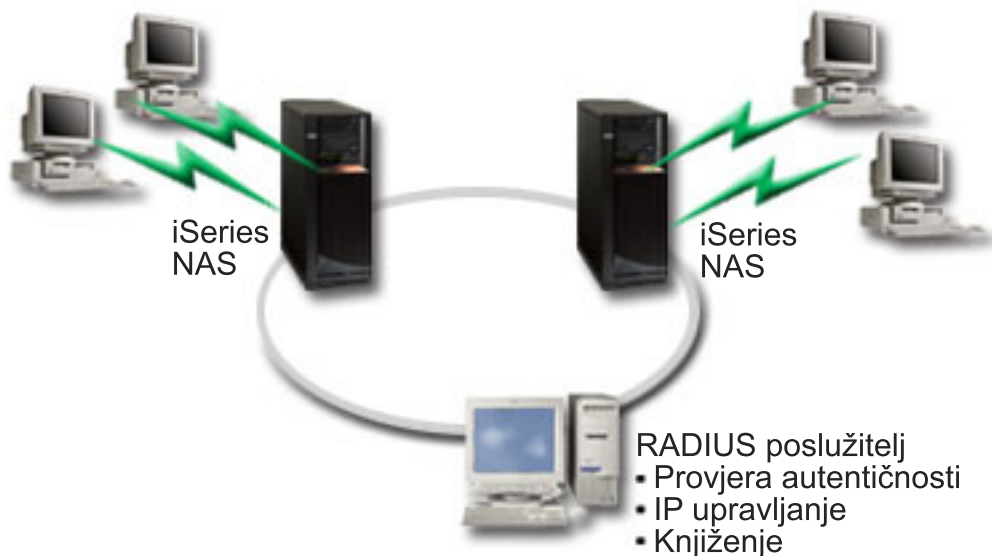
Za postavljanje PPP veze na korištenje linije iz spremišta linija izaberite ovu uslugu linija. Kad PPP veza započne sistem izabire neiskorištenu liniju iz spremišta linija. Za profile biranja na zahtjev sistem ne izabire linije dok ne uoči TCP/IP promet za udaljeni sistem.

## **Scenarij: Provjera autentičnosti veza biranja pomoću RADIUS NAS-a**

Poslužitelj Pristupa Mreži (NAS) koji se izvodi na sistemu može usmjeravati zahtjeve za provjerom autentičnosti od klijenata biranja do zasebnog Poslužitelja usluge provjere autentičnosti udaljenog korisnika biranja (RADIUS). Ako mu je provjerena autentičnost, RADIUS također kontrolira IP adrese koje se pridružuju korisnicima.

### **Situacija**

Vaša korporativna mreža ima udaljene korisnike koji biraju u sistem iz distribuirane mreže biranja. Morate centralizirati provjeru autentičnosti, uslugu i knjiženje kako bi jedan sistem mogao rukovati zahtjevima za provjerom valjanosti korisničkih identifikatora i lozinki za određivanje IP adresa koje im se pridružuju.



Slika 7. Provjera autentičnosti veza biranja pomoću RADIUS poslužitelja

## Rješenje

Kad se korisnici pokušaju spojiti, NAS koji se izvodi na sistemima prosljeđuje informacije o provjeri autentičnosti na RADIUS poslužitelj u mreži. RADIUS poslužitelj, koji održava sve informacije o provjeri autentičnosti za vašu mrežu, obrađuje zahtjeve za provjerom autentičnosti i odgovore. Ako je korisniku provjerena valjanost, RADIUS poslužitelj može biti konfiguriran tako da dodijeli ravnopravne IP adrese i može aktivirati knjiženje za praćenje korisnikove aktivnosti i upotrebe. Morate definirati RADIUS NAS poslužitelj na sistemu kako bi podržali RADIUS.

## Primjer konfiguracije

Za postavku konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. U System i Navigator, proširite **Mreža**, desni klik na **Usluge Udaljenog Pristupa** i izaberite **Usluge**.
2. Na kartici **RADIUS** izaberite **Omogući vezu RADIUS Poslužitelj Mrežnog Pristupa** i **Omogući RADIUS za provjeru autentičnosti**. Ovisno o vašem RADIUS rješenju možete izabrati da RADIUS upravlja knjiženjem veze i konfiguracijom TCP/IP adresa.
3. Kliknite tipku **RADIUS NAS postavke**.
4. Na stranici Općenito, unesite opis ovog poslužitelja.
5. Na stranicama Provjere autentičnosti poslužitelja (i opcijski Poslužitelj knjiženja) kliknite **Dodaj** i unesite sljedeće informacije:
  - a. U kućici **Lokalna IP adresa** unesite IP adresu sučelja koje se koristi za spajanje na RADIUS poslužitelj.
  - b. U kućicu **IP adresa poslužitelja** unesite IP adresu RADIUS poslužitelja.
  - c. U kućicu **Lozinka** unesite lozinku koja se koristi za identifikaciju sistema na RADIUS poslužitelju.
  - d. U kućicu **Port** unesite port koji sistem koristi za komunikaciju sa RADIUS poslužiteljem. Defaulti su port 1812 za poslužitelj za provjeru autentičnosti ili 1813 za poslužitelj za obračun.
6. Kliknite **OK**.
7. U System i Navigator, proširite **Mreža** → **Usluge Udaljenog Pristupa**.
8. Izaberite Profil veze koji će koristiti RADIUS poslužitelj za provjeru autentičnosti. RADIUS usluge primjenjive su samo za primateljske profile veze.
9. Na stranici Provjera autentičnosti izaberite **Zatraži provjeru identiteta ovog iSeries poslužitelja od udaljenog sistema**.

10. Izaberite **Provjeri autentičnost udaljeno pomoću RADIUS poslužitelja**.
11. Izaberite protokol provjere autentičnosti. (PAP ili CHAP-MD5) Ovaj protokol mora također koristiti RADIUS poslužitelj.
12. Izaberite **Koristi RADIUS za uređivanje veze i knjiženje**.
13. Kliknite **OK** da spremite promjenu profila veze.

Morate postaviti RADIUS poslužitelj, uključujući podršku za protokol provjere autentičnosti, korisničke podatke, lozinke i informacije knjiženja. Kontaktirajte RADIUS prodavača za više informacija.

Kad korisnici biraju korištenjem ovaj profil veze sistem prosljeđuje informacije o provjeri autentičnosti na određeni RADIUS poslužitelj. Ako je korisniku ispravno provjerena valjanost, dozvoljava se veza i koriste se ograničenja veze navedena u korisničkim informacijama o RADIUS poslužitelju.

#### **Srodni zadaci**

“Omogućavanje RADIUS i DHCP usluga za profile veze” na stranici 59

Ovo su koraci za omogućavanje usluga RADIUS-a ili Protokola Konfiguracije Dinamičkog Hosta (DHCP) za PPP primateljske profile veze.

#### **Srodne reference**

“Sistemska provjera ovlaštenja” na stranici 42

PPP veze sa System i platformom podržavaju nekoliko opcija provjere autentičnosti, kako udaljenih klijenata koji biraju u sistem, tako i veze prema ISP-u ili drugom sistemu prema kojima sistem bira.

“Pregled Korisničke usluge udaljene provjere autentičnosti biranja” na stranici 44

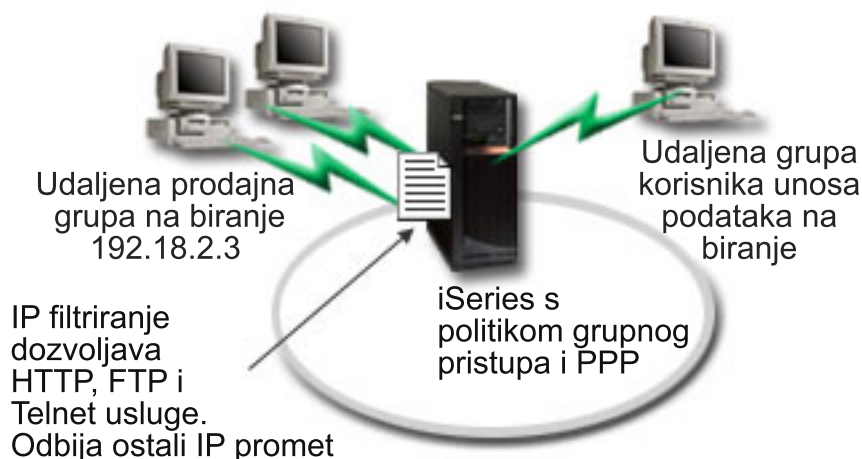
*Korisnička Usluga udaljene provjere autentičnosti biranja (RADIUS)* je Internetski standardni protokol koji pruža centraliziranu provjeru autentičnosti, knjiženje i usluge IP upravljanja za udaljene korisnike u distribuiranoj mreži biranja.

## **Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja**

Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

### **Situacija**

Vaša mreža ima nekoliko grupa distribuiranih korisnika od kojih svi trebaju pristup različitim resursima korporativnog LAN-a. Grupa korisnika za unos podataka treba pristup bazi podataka i nekim drugim aplikacijama. Grupa ljudi iz drugih tvrtki treba pristup biranjem na usluge HTTP-a, FTP-a i Telnet-a ali iz sigurnosnih razloga ova grupa ne bi trebala imati pristup drugim TCP/IP uslugama ili prometu. Definiranje detaljnih atributa veze i dozvola za svakog pojedinog korisnika stvara nepotrební trošak, a pružanje mrežnih ograničenja za sve korisnike u profilu veze ne dopušta dovoljnu razinu kontrole. Vi trebate način definiranja postavki veze i dozvola za nekoliko točno određenih grupa korisnika koji rutinski biraju unutar sistema.



Slika 8. Primjena postavki veze na veze biranja zasnovane na postavkama grupnih politika

## Rješenje

Morate primijeniti jedinstvena ograničenja filtriranja IP-a na dvije različite grupe korisnika. Kako bi ovo izveli stvarate grupne politike pristupa i pravila IP filtriranja. Grupne politike pristupa odnose se na IP pravila filtriranja tako da prvo morate stvoriti pravila filtriranja. U ovom primjeru trebate stvoriti PPP filter za uključivanje pravila IP filtriranja za Grupnu Politiku Pristupa IBM Grupe Poslovnih Partnera. Oca pravila filtriranja dopuštaju HTTP, FTP i Telnet usluge ali ograničavaju pristup drugom TCP/IP prometu i uslugama u sistemu. Ovaj scenarij prikazuje samo pravila filtriranja koja su potrebna grupi prodaje; slična pravila možete postaviti za grupu Unosa Podataka.

Konačno, trebate kreirati politike grupnog pristupa (jednu po grupi) da definirate svoju grupu. Grupna politika pristupa omogućuje vam definiranje zajedničkih atributa veze za grupu korisnika. Dodavanjem grupne politike pristupa listi provjere valjanosti za sistem možete primijeniti ove postavke veze tokom procesa autentikacije. Ova grupna politika pristupa specificira nekoliko postavki za korisničku sesiju uključujući i mogućnost primjene pravila IP filtriranja koja ograničuju IP adrese i TCP/IP usluge koje su dostupne korisniku tokom sesije.

## Primjer konfiguracije

Za postavljanje konfiguracije primjera iz System i Navigator, pratite sljedeće korake:

1. Stvorite identifikator filtra Point-to-Point (PPP) protokola i filtre pravila IP paketa koji navode dozvole i ograničenja za ovu grupnu politiku pristupa.
  - a. U System i Navigator, proširite **Mreža** → **Usluge Udaljenog Pristupa**.
  - b. Kliknite **Profili veze primatelja** i izaberite Politike grupnog pristupa.
  - c. Desno kliknite predefiniranu grupu ispisanu u desnom oknu i izaberite **Svojstva**.

**Bilješka:** Ako želite stvoriti novu grupnu politiku pristupa desni klik na **Grupne Politike Pristupa** i izaberite **Novo Grupno Politike Pristupa**. Ispunite karticu **Općenito**. Potom izaberite karticu **TCP/IP Postavke** i izvršite korak e ispod.

- d. Izaberite karticu **TCP/IP Postavke** i kliknite **Napredno**.
- e. Izaberite **Koristi IP pravila paketa za ovu vezu** i kliknite **Uređivanje datoteke pravila**. To će pokrenuti editor IP pravila paketa i otvoriti datoteke pravila paketa PPP filtera.
- f. Otvorite izbornik **Umetanje** i izaberite **Filteri** da dodate skupove filtera. Koristite karticu **Općenito** za definiciju skupova filtera i karticu **Usluge** za definiranje usluga koje su dozvoljene kao npr. HTTP. Sljedeći skup filtera, "services\_rules," će dopustiti HTTP, FTP i Telnet usluge. Pravila filtera uključuju defaultno izraz odbijanja, ograničenje bilo kojih TCP/IP usluga ili IP prometa koji nije posebno dozvoljen.

**Bilješka:** IP adrese u sljedećem primjeru su globalno usmjerene i mogu se koristiti samo kao primjeri.

###Sljedeća 2 filtera će dopustiti HTTP (Web pretražitelj) promet u & van sistema.

```
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
```

###Sljedeća 4 filtera će dopustiti FTP promet u & van sistema.

```
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
```

###Sljedeća 2 filtera će dopustiti telnet promet u & van sistema.

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

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

- g. Otvorite izbornik **Umetanje** i izaberite **Sučelje filtera**. Koristite sučelje filtera da kreirate PPP identifikator filtera i uključite postavke filtera koje ste definirali.

- 1) Na kartici **Općenito** unesite **permitted\_services** za identifikator PPP filtra.
- 2) Na kartici **Skupovi filtera** izaberite skup filtera **services\_rules** i kliknite **Dodaj**.
- 3) Kliknite OK. Sljedeće linije će se dodati datoteci pravila:

```
###Sljedeći izraz povezuje (pridružuje) 'services_rules' postavke filtera s  
ID-om PPP filtera "permitted_services." Taj ID PPP filtera  
se onda može odnositi na fizičko sučelje pridruženo PPP profilu veze  
ili Politici grupnog pristupa.
```

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

- h. Spremite svoje promjene i izađite. Ako trebate kasnije poništiti ove promjene koristite sučelje zasnovano na znakovima i unesite naredbu **RMVTCPTBL \*ALL**. Ova naredba uklanja sva pravila filtera i NAT na sistemu
  - i. U dijalog kućici **Napredne TCP/IP postavke** ostavite kućicu **PPP identifikator filtra** praznom i kliknite **OK** za izlaz. Kasnije bi trebali primjeniti identifikator filtra kojeg ste upravo napravili na grupnu politiku pristupa, a ne na ovaj profil veze.
2. Definirajte novu grupnu politiku pristupa za ovu korisničku grupu.
- a. U System i Navigator, proširite **Mreža** → **Usluge Udaljenog Pristupa** → **Profili Veze Primatelja**.
  - b. Desno kliknite **Politike pristupa grupe** i izaberite **Nova grupna politika pristupa**. System i Navigator prikazuje dijalog **Definicija nove grupne politike pristupa**.
  - c. Na stranici Općenito unesite ime i opis grupne politike pristupa.
  - d. Na stranici TCP/IP postavke:

- Izaberite **Koristi IP pravila paketa za ovu vezu** i izaberite identifikator PPP filtera **permitted\_services**.
  - e. Izaberite **OK** za spremanje grupne politike pristupa.
3. Primjenite grupnu politiku pristupa na korisnike pridružene ovoj grupi.
    - a. Otvorite profil primateljske veze koja upravlja ovim telefonskim vezama.
    - b. Na stranici Provjera autentičnosti na profilu primateljske veze, izaberite listu provjere valjanosti koja sadrži informacije za provjeru autentičnosti korisnika i kliknite **Otvori**.
    - c. Izaberite korisnika iz grupe Prodaja kojoj želite primijeniti grupnu politiku pristupa i kliknite **Otvori**.
    - d. Kliknite **Primjeni Grupnu politiku na korisnika** i izaberite grupnu politiku pristupa iz koraka 2.
    - e. Ponovite za svakog korisnika Prodaje.

#### Srodni koncepti

“Konfiguracija grupne politike pristupa” na stranici 57

Folder **Politike grupnog pristupa** pod Profili povezivanja primatelja osigurava opcije za konfiguriranje parametara point-to-point povezivanja koji se odnose na grupu udaljenih korisnika. Primjenjuje se samo na one point-to-point veze koje potječu od udaljenog sistema i primljene su od lokalnog sistema.

“Podrška politike grupe” na stranici 3

Sad podrškom za grupnu politiku, mrežni administratori mogu definirati grupne politike zasnovane na korisnicima i upravljati resursima. Pojedini korisnicima može se pridružiti pristup politikama upravljanja kad se prijave na Point-to-Point protokolom (PPP) ili sesiju Protokola Tuneliranja Razine Dva (L2TP).

#### Srodni zadaci

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

“Primjena pravila filtriranja IP paketa na PPP vezu” na stranici 58

Možete koristiti pravila filtriranja paketa kako bi ograničili pristup korisnicima ili grupama na neke IP adrese mreže.

#### Srodne reference

“Validacijska lista” na stranici 44

Validacijska lista se koristi za pohranjivanje informacija korisničkog ID-a i lozinke udaljenih korisnika.

“Sistemska provjera ovlaštenja” na stranici 42

PPP veze sa System i platformom podržavaju nekoliko opcija provjere autentičnosti, kako udaljenih klijenata koji biraju u sistem, tako i veze prema ISP-u ili drugom sistemu prema kojima sistem bira.

#### Srodne informacije

IP filtriranje i prijevod mrežne adrese

## Scenarij: Dijeljenje modema između logičkih particija korištenjem L2TP-a

Imate virtualni Ethernet postavljen kroz četiri logičke particije. Želite da izabrane logičke particije dijele modem kako bi pristupale vanjskom LAN-u.

### Situacija

Vi ste sistemski administrator tvrtke srednje veličine. Vrijeme je za ažuriranje računalne opreme ali želite više od toga; želite uskladiti hardver. Započinjete proces konsolidacije rada tri stara sistema na jedan novi sistem. Stvarate tri logičke particije na sistemu. Novi sistem dolazi sa 2793 internim modemom. Ovo je jedini ulazno/izlazni procesor (IOP) koji podržava Point-to-Point protokol (PPP). Imate također stari 7852-400 modem elektroničke korisničke podrške.

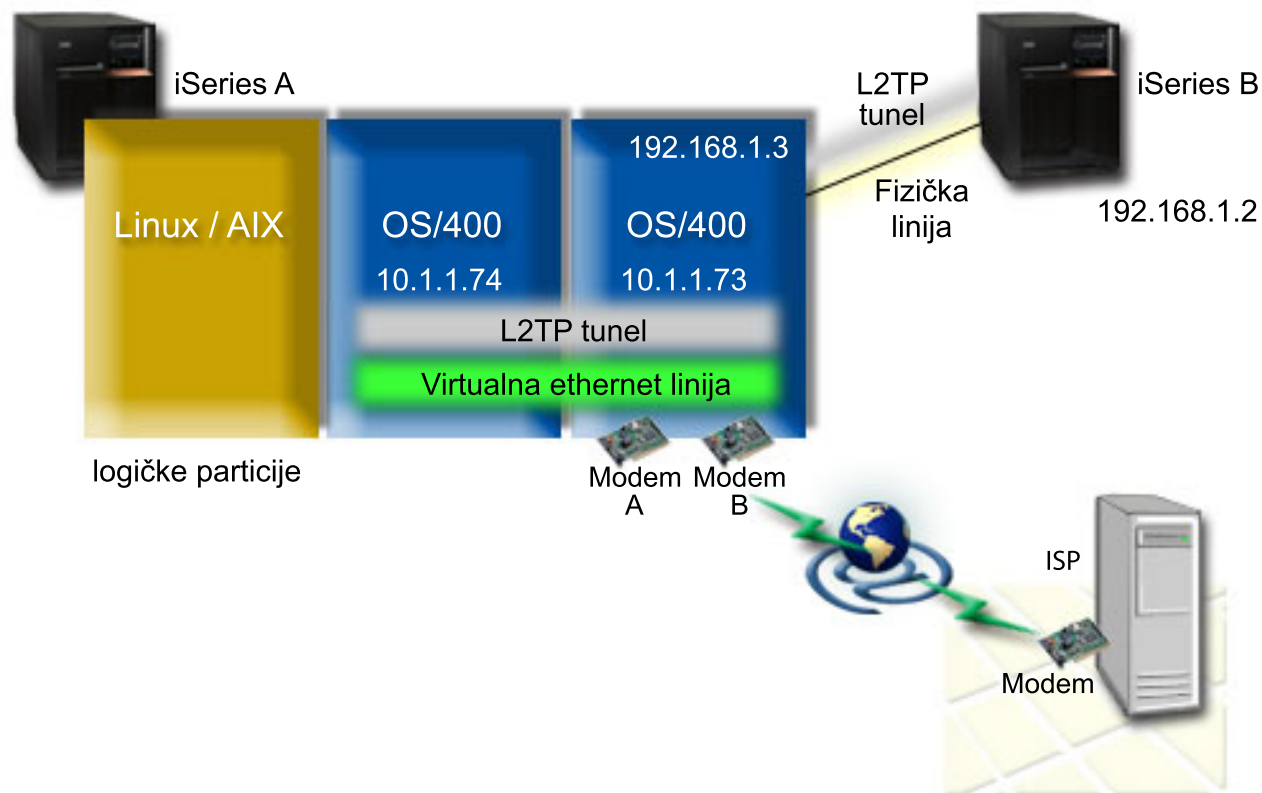
### Rješenje

Višestruki sistemi i particije mogu dijeliti iste modeme za telefonska povezivanja, čime se eliminira potreba za tim da svaki sistem ili particija moraju imati vlastiti modem. Ovo je moguće ako koristite L2TP tunele i konfigurirate L2TP profile da prihvaćaju izlazne pozive. U vašoj mreži, tuneli će raditi preko virtualne Ethernet mreže i fizičke mreže. Fizička linija je spojena na drugi sistem koji dijeli modeme u vašoj mreži.



## Detalji

Sljedeća slika ilustrira karakteristike mreže za ovaj scenarij:



Slika 9. Višestruki sistemi koji dijele isti modem za birana povezivanja

## Preduvjeti i pretpostavke

Sistem A mora zadovoljiti sljedeće zahtjeve postavljanja:

- i5/OS Verzija 5 Izdanje 3 ili novije, instalirano na particiju koja je u vlasništvu modema sa ASYNC mogućnosti
- Hardver koji dopušta particioniranje.
- System i Access za Windows i System i Navigator (Konfiguracijska i Uslužna komponenta System i Navigator), Verzija 5 Izdanje 3, ili novije,
- Imate stvorene barem dvije logičke particije (LPAR) na sistemu. Particija u vlasništvu modema mora imati instaliran i5/OS V5R3, ili novije. Druge particije mogu imati instaliran OS/400 V5R2, i5/OS V5R3, Linux, ili AIX. U ovom scenariju, particije koriste ili i5/OS ili Linux operativni sistem.
- Imate kreiran virtualni Ethernet za komunikaciju među particijama.

Sistem B mora imati instaliran licencirani program i ključne komponente System i Navigator: System i Access za Windows and System i Navigator (Konfiguracijska i Uslužna Komponenta System i Navigator) V5R2, ili novijeg.

### Srodne informacije

Logičke particije

## Detalji scenarija: Dijeljenje modema između logičkih particija korištenjem L2TP-a

Nakon što izvršite sve preduvjete, spremni ste za početak konfiguracije Profila Protokola Tuneliranja Razine Dva (L2TP).

## Scenarij 1: Konfiguracija L2TP terminirajućeg profila za sva sučelja na particiji koja ima modeme u vlasništvu:

Sa stvaranje terminirajućeg profila za sva sučelja, pratite sljedeće korake:

1. U System i Navigator, proširite **vaš sistem** → **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Profili veze primatelja** i izaberite **Novi profil**.
3. Izaberite sljedeće opcije na stranici Postav i kliknite **OK**:
  - **Tip protokola:** PPP
  - **Tip veze:** L2TP (virtualna linija)
  - **Način rada:** Terminator (mrežni poslužitelj)
  - **Tip linijske usluge:** Jednostruka linija
4. Na kartici **Novi profil - Općenito** dovršite sljedeća polja:
  - **Ime:** toExternal
  - **Opis:** Veza primatelja za biranje van
  - Izaberite **Pokreni profil s TCP-om**.
5. Na kartici **Novi profil - Povezivanje** dovršite sljedeća polja.
  - **IP adresa krajnje točke lokalnog tunela:** ANY
  - **Ime virtualne linije:** toExternal. Ova linija nema pridruženih fizičkih sučelja. Virtualna linija opisuje različite karakteristike ovog PPP profila. Nakon što se otvori prozor Svojstva L2TP Linije kliknite karticu **Provjera autentičnosti** i unesite ime hosta vašeg sistema. Kliknite **OK** za povratak na karticu **Veza** na prozoru Svojstva Novog PPP Profila.
6. Kliknite **Dozvoli uspostavljanje izlaznog poziva**. Pojavit će se dijalog **Svojstva biranja izlaznog poziva**.
7. Na stranici Svojstva biranja izlaznog poziva izaberite tip usluge linije.
  - **Tip linijske usluge:** Spremište linija
  - **Ime:** dialOut
  - Kliknite **Novo**. Pojavljuje se dijalog **Svojstva novog spremišta linija**.
8. U prozoru svojstava novog spremišta linija izaberite linije i modeme za koje ćete dozvoliti izlazne pozive i kliknite **Dodaj**. Ako trebate definirati te linije, izaberite **Nova linija**. Sučelja na particiji koja je vlasnik ovih modema će pokušati upotrijebiti bilo koju otvorenu liniju iz tog spremišta. Otvara se novi prozor Svojstva Linije.
9. Na kartici **Svojstva nove linije - Općenito** unesite informacije u sljedeća polja:
  - **Ime:** line1
  - **Opis:** prva linija i prvi modem za spremište linija (2793 interni modem)
  - **Hardverski resurs:** cmn03 (komunikacijski port)
10. Prihvatite defaulte na svim drugim karticama i kliknite **OK** da se vratite na prozor Svojstva novog spremišta linija.
11. U prozoru Svojstva novog spremišta linija izaberite linije i modeme za koje ćete dozvoliti izlazne pozive i kliknite **Dodaj**. Provjerite da li je 2793 modem izabran za spremište.
12. Izaberite ponovo **Nove Linija** kako bi dodali 7852–400 modem elektroničke korisničke podrške. Otvara se novi prozor Svojstva Linije.
13. Na kartici **Svojstva nove linije - Općenito** unesite informacije u sljedeća polja:
  - **Ime:** line2
  - **Opis:** druga linija i drugi modem za spremište linija (7852-400 vanjski modem elektroničke korisničke podrške)
  - **Hardverski resurs:** cmn04 (V.24 port)
  - **Uokvirenje:** Asinkrono
14. Na kartici **Svojstva nove linije - Modem** izaberite vanjski modem (7852–400) i kliknite **OK** da biste se vratili u prozor Svojstva novog spremišta linija.

15. Izaberite bilo koje druge dostupne linije koje želite dodati u spremište linija i kliknite **Dodavanje**. U ovom primjeru provjerite jesu li dodana dva nova modema unutar polja **Izabrane linije za spremište** i kliknite **OK** da biste se vratili u prozor Svojstva biranja izlaznog poziva.
16. U prozoru Svojstva biranja izlaznog poziva unesite **Defaultni pozivni brojevi** i kliknite **OK** da biste se vratili u prozor Svojstva novog PPP profila.

**Bilješka:** Ovi brojevi mogu biti nešto poput Pružatelja Internetskih Usluga (ISP) tj. nešto što će biti često zvano od strane drugih sistema koji koriste ovaj modem. Ako drugi sistemi specificiraju telefonski broj \*PRIMARY ili \*BACKUP, stvarni brojevi koji se biraju bit će oni koji su ovdje specificirani. Ako drugi sistemi navedu konkretni telefonski broj onda će se taj broj i koristiti.

17. Na kartici **TCP/IP postavke**, izaberite sljedeće vrijednosti:

- **Lokalna IP adresa:** Nema
- **Udaljena IP adresa:** Nema

**Bilješka:** Ako želite koristiti profil za završavanje L2TP sesija morate izabrati lokalnu IP adresu koja predstavlja sistem. Za udaljenu IP adresu možete izabrati spremište adresa koje je u istoj podmreži kao i vaš sistem. Sve L2TP sesije dohvaćaju njihove IP adrese iz ovog spremišta.

18. Na kartici **Provjera autentičnosti**, prihvatite sve default vrijednosti.

Sada ste završili sa konfiguracijom vašeg L2TP terminirajućeg profila na particiji sa modemima. Idući korak je konfiguracija L2TP udaljenog biranja, izvorišni profil za 10.1.1.74

#### **Srodne reference**

“Podrška profila višestrukih veza” na stranici 51

Point-to-point profili veze koji podržavaju višestruke veze omogućuju vam posjedovanje jednog profila veze koji rukuje sa više digitalnih, analognih ili L2TP poziva.

#### **Korak 2: Konfiguracija L2TP izvorišnog profila na 10.1.1.74:**

Ovi koraci vode vas kroz stvaranje izvorišnog profila Protokola Tuneliranja Razine Dva (L2TP):

1. U System i Navigator, proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Profili veze davatelja** i izaberite **Novi profil**.
3. Izaberite sljedeće opcije na stranici Postav i kliknite **OK**:
  - **Tip protokola:** PPP
  - **Tip veze:** L2TP (virtualna linija)
  - **Način rada:** Udaljeno biranje
  - **Tip linijske usluge:** Jednostruka linija
4. Na kartici **Općenito** ispunite sljedeća polja:
  - **Ime:** toModem
  - **Opis:** veza davatelja koja ide u particiju koja je vlasnik modema
5. Na kartici **Općenito** ispunite sljedeća polja:

**Ime virtualne linije:** toModem. Ova linija nema pridruženo fizičko sučelje. Virtualna linija opisuje različite karakteristike ovog PPP profila. Otvara se prozor Svojstva L2TP linije.
6. Na kartici **Općenito** unesite opis za virtualnu liniju.
7. Na kartici **Provjera autentičnosti** unesite ime lokalnog hosta particije i kliknite **OK** da biste se vratili na stranicu Povezivanje.
8. U polju **Udaljeni telefonski brojevi** dodajte \*PRIMARY i \*BACKUP. Ovo dozvoljava da profili koriste iste telefonske brojeve kao i profil terminatora na particiji koji posjeduje modeme.
9. U polju **Ime hosta krajnje točke udaljenog tunela ili IP adresa** unesite IP adresu krajnje točke udaljenog tunela (10.1.1.73).

10. Na kartici **Provjera autentičnosti**, izaberite **Dozvoli da udaljeni sistem provjeri identitet ovog iSeries poslužitelja**.
11. U odjeljku Protokol provjere autentičnosti izaberite **Zahtijeva šifriranu lozinku (CHAP-MD5)**. Po defaultu je također izabrano **Dozvoli protokol proširive provjere autentičnosti**.

**Bilješka:** Protokol bi trebao odgovarati kojem god protokolu kojeg koristi sistem u kojeg birate.

12. Unesite ime korisnika i lozinku.

**Bilješka:** Korisničko ime i lozinka moraju odgovarati kojem god korisničkom imenu i lozinki koji se nalaze na sistemu u kojem birate.

13. Otidite na karticu **TCP/IP postavke** i provjerite obavezna polja:

- **Lokalna IP adresa:** Dodjeljuje ju udaljeni sistem
- **Udaljena IP adresa:** Dodjeljuje ju udaljeni sistem
- **Usmjeravanje:** Nije potrebno dodatno usmjeravanje

14. Kliknite **OK** da spremite PPP profil.

### **Korak 3: Konfiguracija L2TP udaljenog profila biranja za 192.168.1.2:**

Možete konfigurirati profil udaljenog biranja Protokola Tuneliranja Razine Dva (L2TP) za 192.168.1.2 ponavljanjem Koraka 2 i izmjenom krajnje točke udaljenog tunela na 192.168.1.3 (fizičko sučelje na koje se Sistem B spaja)

**Bilješka:** To su izmišljene IP adrese koje se koriste samo u svrhu primjera.

### **Korak 4: Testiranje veze:**

Nakon što završite sa konfiguracijom oba sistema, trebate testirati povezanost kako bi bili sigurni da sistemi dijele modem za dohvaćanje vanjskih mreža.

1. Budite sigurni da je završni profil Protokola Tuneliranja Razine Dva (L2TP) aktivan.
  - a. U System i Navigator, proširite **10.1.1.73** → **Mreža** → **Usluge Udaljenog Pristupa** → **Profili Veze Primatelja**.
  - b. U desnom prozoru pronađite potrebni profil (toExternal) i provjerite da li je u polju **Status** Aktivno. Ako nije, desno kliknite profil i izaberite **Pokreni**.
2. Pokrenite Profil udaljenog biranja na 10.1.1.74.
  - a. U System i Navigator, proširite **10.1.1.74** → **Mreža** → **Usluge Udaljenog Pristupa** → **Profil Veze Davalaca**.
  - b. U desnom prozoru pronađite potrebni profil (toModem) i provjerite da li je u polju **Status** Aktivno. Ako nije, desno kliknite profil i izaberite **Pokreni**.
3. Pokrenite profil udaljenog biranja na Sistemu B.
  - a. U System i Navigator, proširite **192.168.1.2** → **Mreža** → **Usluge Udaljenog Pristupa** → **Profili Veze Davalaca**.
  - b. U desnom prozoru pronađite stvoreni profil i provjerite da li je u polju **Status** Aktivno. Ako nije, desno kliknite profil i izaberite **Pokreni**.
4. Ako je moguće, pingajte pružatelja Internetskih usluga ili drugo odredište koje ste birali kako bi provjerili da li su oba profila aktivna. Trebate pokušati pingati i iz 10.1.1.74 i iz 192.168.1.2.
5. Kao alternativa možete također provjeriti status veze.
  - a. U System i Navigator, proširite **sistem** → **Mreža** → **Usluge Udaljenog Pristupa** → **Profili Veze Davalaca**.
  - b. U desnom oknu desno kliknite profil kojeg ste kreirali i izaberite **Povezivanja**. U prozoru Status veze možete vidjeti koji profili su aktivni, neaktivni, u povezivanju i još više.

---

## Planiranje PPP-a

Planiranje Point-to-Point protokola (PPP) uključuje stvaranje i administriranje PPP veza.

### Srodne reference

“Scenarij: Spajanje udaljenih klijenata biranja na sistem” na stranici 12

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

“Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema” na stranici 15

Administratori u tipičnom slučaju postavljaju uredske mreže kako bi omogućili zaposlenicima izlaz na Internet. Administratori mogu koristiti modem za spajanje sistema na Pružatelja Internetskih Usluga (ISP). PC klijenti spojeni na LAN mogu komunicirati sa Internetom koristeći i5/OS operativni sistem kao prilaz.

“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

## Softverski i hardverski zahtjevi

Okolina Point-to-Point Protokola (PPP) zahtjeva posjedovanje barem dva računala koja podržavaju PPP. Jedno od ovih računala, System i platforma, može biti davalac ili primatelj.

Sistem mora podržavati sljedeće preduvjete kako bi mu mogli pristupiti udaljeni sistemi.

- System i Navigator sa TCP/IP podrškom.
- Jedan od dva profila povezivanja:
  - Davalac profila veze za rukovanje izlaznim PPP vezama.
  - Primateljski profil veze za rukovanje dolaznim PPP vezama.
- PC konzola radne stanice instalirana sa System i Access za Windows 95 ili kasnijim sa System i Navigator.
- Instalirani adaptor.

Možete izabrati jedan od sljedećih adaptora:

- 2699\*: Dvolinijski WAN ulaz/izlaz adaptor (IOA).
  - 2720\*: PCI WAN/dvoosni IOA.
  - 2721\*: PCI Dvolinijski WAN IOA.
  - 2745\*: PCI Dvolinijski WAN IOA (zamjenjuje IOA 2721).
  - 2742\*: Dvolinijski IOA (zamjenjuje IOA 2745).
  - 2771: Dvoportni WAN IOA, s V.90 integriranim modemom na portu 1 i standardnim komunikacijskim sučeljem na portu 2. Za korištenje porta 2 adaptora 2771, potreban je vanjski modem ili ISDN terminalni adaptor s odgovarajućim kabelom.
  - 2772: Dvoulazni V.90 integrirani modem WAN IOA.
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: Ethernet adaptor za PPPoE veze.
  - 2793/576C: Dvoulazni WAN IOA, sa V.92 integriranim modemom na ulazu 1 i standardnim komunikacijskim sučeljem na ulazu 2. Za korištenje ulaza 2 potrebni su vanjski modem ili ISDN terminalski adaptor sa odgovarajućim kablom.
  - 2805 četveroportni WAN IOA, s integriranim V.92 analognim modemom. To zamjenjuje modele 2761 i 2772.
- \* Ovi adaptori zahtijevaju vanjski V.90 modem (ili više), ili terminalski adaptor Digitalne Mreže Integriranih Usluga (ISDN) i RS-232 (EIA 232) ili kompatibilni kabel.
- Jedno od sljedećeg, zavisno o tipu vaše veze i o liniji:
    - vanjski ili interni modem ili jedinicu usluge kanala (CSU)/jedinicu usluge podataka (DSU).
    - Terminalski adaptor digitalne mreže integriranih usluga (ISDN).
  - Trebate se dogovoriti s Dobavljačem Internet usluga (ISP) oko računa za biranje, ako se namjeravate spajati na Internet. ISP bi vam trebao dati potrebne telefonske brojeve i informacije o Internet povezivanju.

## Srodne reference

“Profili veza” na stranici 2

Point-to-Point profili veze definiraju skup parametara i resursa za određene veze Point-to-Point (PPP) protokola. Možete pokrenuti profile koji koriste ove postavke parametara da biraju van (izvorište) ili da slušaju (primaju) PPP veze.

“Modemi” na stranici 38

I vanjski i interni modem mogu se koristiti za veze Point-to-point (PPP) protokola.

“CSU/DSU” na stranici 38

Jedinica usluge kanala (CSU) je uređaj koji spaja terminal na digitalnu liniju. Jedinica usluge podataka (DSU) je uređaj koji vrši zaštitne i dijagnostičke funkcije telekomunikacijske linije. Tipično, dva uređaja su pakirana kao jednostruka jedinica, CSU/DSU.

“ISDN terminalski adaptori” na stranici 38

Digitalna Mreža Integriranih Usluga (ISDN) pruža vam digitalnu vezu koja omogućuje komunikaciju korištenjem bilo koje kombinacije glasa, podataka, video-signala i sl. unutar raznih multimedijalnih aplikacija.

## Alternativne veze

Point-to-Point Protokol (PPP) može prenositi datagrama preko serijskih point-to-point veza.

PPP omogućuje međupovezivanje višestruke opreme prodavača i višestrukih protokola standardiziranjem point-to-point komunikacije. Sloj PPP podatkovne veze koristi uokvirenje u obliku Kontrole podatkovne veze visoke razine (HDLC) za sažimanje datograma preko asinkronih i sinkronih point-to-point telekomunikacijskih veza.

PPP podržava širok raspon tipova veza ali Internetski Protokol Serijske Linije (SLIP) podržava samo asinkrone tipove veze. SLIP je općenito korišten samo za analogne veze. Mjesna telefonska poduzeća nude tradicionalne telekomunikacijske usluge u uzlaznoj skali sposobnosti i cijene. Ove usluge koriste postojeće mogućnosti glasovne mreže telefonske tvrtke između korisnika i centralnog ureda.

PPP veze postavljaju fizičku vezu između lokalnog i udaljenog hosta. Spojene veze omogućuju namjensku pojasnu širinu. One također dolaze i u širokoj raznolikosti brzina podataka i protokola. S PPP vezama, možete izabrati između sljedećih mogućnosti veza:

### Analogne telefonske linije

Analogna veza, koja koristi modeme za prijenos podataka preko iznajmljenih ili biranih linija, nalazi se na dnu point-to-point ljestvice.

Iznajmljene linije su stalne veze između dvije specificirane lokacije, dok su komutirane linije obične glasovne telefonske linije. Najbrži modemi danas rade na nekomprimiranim brzinama od 56 kbps. Kada je dan omjer signal-šum na bezuvjetnom telefonskom krugu telefonske razine, ipak, ovaj je omjer često nevažan.

Proizvođač modema tvrdi da je viša brzina bita po sekundi (bps) obično bazirana na algoritmu komprimiranja podataka (CCITT V.42bis) kojeg koriste njihovi modemi. Iako V.42bis ima potencijal postizanja do četverostrukog smanjenja, komprimiranje ovisi o podacima i rijetko dostiže i 50%. Podaci koji su već komprimirani ili šifrirani mogu to čak i povećati sa primjenjenim V.42bis. X2 ili 56Flex povećava brzinu na 56 kbps za analogne telefonske linije. To je hibridna tehnologija koja zahtijeva da jedan kraj PPP veze bude digitalan, dok je suprotni kraj analogan. Dodatno, 56 kbps se primjenjuje samo kad premještate podatke sa digitalnog na analogni kraj veze. Ova tehnologija je pogodna za veze na ISP-ove s digitalnim krajem veze i hardverom na njihovoj lokaciji. U tipičnom slučaju možete spojiti V.24 analogni modem preko RS-232 serijskog sučelja sa asinkronim protokolom na brzinu do 115.2 kbps.

V.90 standard je kraj pitanja K56flex/x2 kompatibilnosti. V.90 standard je rezultat kompromisa između x2 i K56flex borbi u industriji modema. Gledanjem javne izmjenjive telefonske mreže kao digitalne, V.90 tehnologija može ubrzate podatke sa Interneta na računalo na brzine do 56 kbps. V.90 tehnologija se razlikuje od drugih standarda zato što digitalno šifrira podatke umjesto da ih modulira poput analognih modema. Prijenos podataka je asimetrična metoda tako da ulazni prijenos (većinom tipkanje i naredbe mišem od računala do centralne lokacije što zahtjeva manje pojasne širine) nastavlja teći na konvencionalnim brzinama od 33.6 kbps. Podaci poslani s modema su poslani kao analogni prijenos koji odražava V.34 Standard. Samo smjer od mreže prema terminalu koristi visoke V.90 brzine.

V.92 standard se poboljšava na V.90 dozvoljavanjem ulaznih brzina do 48 kbps. Dodatno, vremena čekanja mogu se smanjiti zbog poboljšanja na procesu rukovanja i modemi koji podržavaju sposobnost zadržavanja sad mogu ostati spojeni dok telefonska linija prihvaća dolazne pozive ili koristi pozive na čekanju.

## Digitalna usluga i Digitalne Podatkovne Usluge

Možete koristiti digitalnu uslugu i Digitalne Podatkovne Usluge (DDS) pomoću Point-to-Point protokola (PPP).

### Digitalna usluga

S digitalnim uslugama, podaci putuju cijelim putem od računala pošiljatelja do centralnog ureda telefonskog poduzeća, do dobavljača velikih udaljenosti, do centralnog ureda i tada do računala primatelja u digitalnom obliku. Digitalno signaliziranje pruža veću pojasnu širinu i veću pouzdanost od analognog signaliziranja. Digitalni sistem signalizacije eliminira mnogo problema s kojima se analogni modemi susreću, kao šum, promjenjiva kvaliteta linije i prigušivanje signala.

### Digitalne podatkovne usluge

Digitalne podatkovne usluge (DDS) su osnova digitalnih usluga. DDS veze su iznajmljene, trajne veze koje podržavaju brzine do 56 kbps. Ova usluga se također obično naziva DS0.

Možete se spojiti na DDS korištenjem specijalne kutije zvane *servisna jedinica kanala/servisna jedinica podataka (CSU/DSU)*, koja nadomješta modem u analognom scenariju. DDS ima fizička ograničenja koja su prvenstveno vezana uz udaljenosti između CSU/DSU i centralnog ureda telefonske tvrtke. DDS radi najbolje kada je udaljenost manja od 9000 m (30 000 ft). Telefonske tvrtke se mogu prilagoditi većim udaljenostima korištenjem proširitelja signala ali ova usluga ima veću cijenu. DDS je najbolji za povezivanje dvije lokacije koje uslužuje isti centralni ured. Za veze velikih udaljenosti koje prelaze više centralnih ureda troškovi brzo rasti sa razdaljinom i DDS više ne mora biti toliko praktičan. U ovim slučajevima Switched-56 bi moglo biti bolje rješenje. U tipičnom slučaju možete se spojiti na DDS CSU/DSU preko V.35, RS449, ili X.21 serijskog sučelja sa sinkronim protokolom na brzinama do 56 kbps.

#### Srodne reference

“CSU/DSU” na stranici 38

Jedinica usluge kanala (CSU) je uređaj koji spaja terminal na digitalnu liniju. Jedinica usluge podataka (DSU) je uređaj koji vrši zaštitne i dijagnostičke funkcije telekomunikacijske linije. Tipično, dva uređaja su pakirana kao jednostruka jedinica, CSU/DSU.

“Birani-56”

Kada vam nije potrebna stalna veza, možete uštedjeti novac korištenjem komutirane digitalne usluge koja se općenito naziva *Switch-56 (SW56)*.

### Birani-56

Kada vam nije potrebna stalna veza, možete uštedjeti novac korištenjem komutirane digitalne usluge koja se općenito naziva *Switch-56 (SW56)*.

SW56 veza je slična postavki Digitalnih Podatkovnih Usluga (DDS) u smislu da se oprema podatkovnog terminala (DTE) spaja na digitalnu usluge preko jedinice usluge kanala/jedinice usluge podataka (CSU/DSU). SW56 CSU/DSU, međutim uključuje brojčanik s kojeg možete unijeti telefonski broj udaljenog hosta. Možete koristiti SW56 za stvaranje digitalnih veza na bilo kojeg drugog SW56 pretplatnika bilo gdje u regiji ili preko internacionalnih granica.

SW56 poziv se prenosi preko digitalne mreže velike udaljenosti kao i digitalizirani govorni poziv. SW56 koristi iste telefonske brojeve kao i lokalni telefonski sistem, a upotreba se naplaćuje isto kao i kod poslovnih glasovnih poziva.

SW56 postoji samo u mrežama Sjeverne Amerike i ograničen je na jednostruke kanale koji mogu samo prenositi podatke. SW56 je alternativa za lokacije gdje je ISDN nedostupan.

U tipičnom slučaju možete se spojiti na SW56 CSU/DSU preko V.35 ili RS449 serijskog sučelja sa sinkronim protokolom na brzinama do 56 kbps. S V.25bis poziv/odgovor jedinicom, podaci i kontrola poziva teku preko jednostrukog serijskog sučelja.

### **Srodne reference**

“Digitalna usluga i Digitalne Podatkovne Usluge” na stranici 33

Možete koristiti digitalnu uslugu i Digitalne Podatkovne Usluge (DDS) pomoću Point-to-Point protokola (PPP).

“Integrirana mreža digitalnih usluga”

Digitalna mreža integriranih usluga (ISDN) pruža izmjenjivu digitalnu povezanost s kraja na kraj. ISDN može prenositi i glas i podatke preko iste veze.

## **Integrirana mreža digitalnih usluga**

Digitalna mreža integriranih usluga (ISDN) pruža izmjenjivu digitalnu povezanost s kraja na kraj. ISDN može prenositi i glas i podatke preko iste veze.

Postoje različiti tipovi ISDN usluga, sa Sučeljem osnovne brzine (BRI) kao najčešćim. BRI se sastoji od dva 64 kbps B kanala za prijenos podataka o korisnicima i D kanal za prijenos signalizacijskih podataka. Dva B kanala mogu se spojiti kako bi zajedno davali prijenos od 128 kbps. U nekim područjima telefonska tvrtka može ograničiti svaki B kanal na ili 56 kbps ili 112 kbps kombinirano. Postoji također i fizičko ograničenje u kojem lokacija korisnika mora biti unutar 5400 m (18 000 ft) od komutacije središnjeg ureda. Ova udaljenost se može proširiti s ponavljačima. Možete se povezati ISDN-om s uređajem koji se naziva terminalni adaptor. Većina terminal adaptora imaju integriranu jedinicu završetka mreže (NT1) koja dozvoljava direktno povezivanje u telefonsku utičnicu. Tipično, terminalni adaptori povezuju se s računalom preko asinkrone RS-232 veze i koriste AT skup naredbi za postavljanje i kontrolu, uglavnom kao uobičajeni analogni modemi. Svaka vrsta ima vlastita proširenja AT naredbe za postavljanje parametara koji su jedinstveni za ISDN. U prošlosti, postojalo je mnogo problema međuoperabilnosti između različitih vrsta ISDN terminal adaptora. Ti problemi su uglavnom nastali zbog raznolikih protokola za prilagodbu brzine koji su postojali u V.110 i V.120 kao i u shemama povezivanja za dva B kanala.

Industrija je sada konvergirala na sinkroni PPP protokol sa PPP multilinkom za povezivanje dva B kanala. Neke proizvodnje terminal adaptora integriraju V.34 (analogni modem) sposobnost u njihove terminal adaptore. Ova sposobnost omogućuje korisnicima sa jednom ISDN linijom rukovanje ili ISDN ili uobičajenim analognim pozivima iskorištavanjem simultanih govor/podaci sposobnosti ISDN usluga. S ovom tehnologijom, terminalski adaptor može raditi kao digitalna sistemska strana za V.92 klijente.

U tipičnom slučaju trebate spojiti ISDN terminalski adaptor preko RS-232 serijskog sučelja korištenjem asinkronog protokola na brzinama do 230.4 kbps. Međutim, maksimalna sistemska brzina prijenosa za asinkroni protokol preko RS-232 je 115.2 kbps. Nažalost, ovo ograničava maksimalnu brzinu prijenosa bajtova na 11.5 kbps dok je terminalski adaptor sa multilinkom u mogućnosti prijenosa 14 ili 16 KB nekomprimirano. Neki terminalski adaptori podržavaju sinkroni protokol preko RS-232 na 128 kbps ali sistemska maksimalna brzina prijenosa za sinkroni protokol preko RS-232 iznosi 64 kbps.

Sistem je u mogućnosti izvoditi asinkroni protokol preko V.35 na brzinama do 230.4 kbps ali proizvođači terminalskih adaptora obično ne nude takvu konfiguraciju. Konvertori sučelja koji pretvaraju RS-232 sučelje u V.35 sučelje mogu predstavljati prihvatljivo rješenje problema ali ovaj pristup nije još procijenjen za sistem. Druga mogućnost je korištenje terminalskih adaptora sa V.35 sučeljem i sinkronim protokolom na brzini 128 kbps. Iako ova klasa terminalskih adaptora postoji ona najčešće ne nudi sinkroni multilink PPP.

### **Srodne reference**

“Birani-56” na stranici 33

Kada vam nije potrebna stalna veza, možete uštedjeti novac korištenjem komutirane digitalne usluge koja se općenito naziva *Switch-56 (SW56)*.

“ISDN terminalski adaptori” na stranici 38

Digitalna Mreža Integriranih Usluga (ISDN) pruža vam digitalnu vezu koja omogućuje komunikaciju korištenjem bilo koje kombinacije glasa, podataka, video-signala i sl. unutar raznih multimedijalnih aplikacija.

## **T1/E1 i djelomične T1 veze**

T1/E1 i djelomični T1 su dvije vrste važećih alternativa povezivanja.



## T1/E1

T1 veza grupira zajedno 24 64-kbps (DS0) vremenski podijeljene multipleks (TDM) kanale preko četverožičnog bakrenog kruga. Ovo stvara ukupnu pojasnu širinu od 1.544 mbps. E1 krug u Europi i drugim dijelovima svijeta grupira zajedno 32 64-kbps kanala za ukupno 2.048 mbps. TDM dozvoljava da više korisnika dijeli prijenosni medij korištenjem unaprijed određenih vremenskih proreza. Puno PBX-ova koriste T1 uslugu kako bi izveli višestruke pozive preko jedne T1 linije umjesto potrebe za 24 parice između PBX-a i telefonske tvrtke.

Važno je napomenuti da T1 može biti dijeljen između glasa i podataka. Telefonska usluga može doći preko podskupa od 24 kanala T1 veze ostavljajući preostale kanale za npr. vezu na Internet. T1 uređaj multipleksora je potreban za upravljanje 24 DS0 kanala kada je T1 sabirница podijeljena između više usluga. Za jednostruku samo-podaci vezu, krug može biti izveden ne kanalizirano (TDM se ne izvodi na signalu). Kao rezultat toga jednostavniji uređaj servisne jedinice kanala/podataka (CSU/DCU) se može koristiti. U tipičnom slučaju možete se spojiti na T1/E1 CSU/DSU ili multipleksor preko V.35 ili RS 449 serijskog sučelja na brzinama koje su višekratnici od 64 kbps do 1.544 mbps ili 2.048 mbps. CSU/DSU ili multipleksor omogućavaju takt u mreži.

## Djelomičan T1

Sa Djelomičnim T1 (FT1), korisnik može unajmiti bilo koji 64-kbps dio T1 linije. FT1 je koristan kad god trošak namjenskog T1 nije podesan za stvarnu pojasnu širinu koju korisnik koristi. S FT1 plaćate samo za ono što trebate. Dodatno, FT1 ima sljedeće svojstvo koje je nedostupno s potpunim T1 krugom: Multipleksiranje DS0 kanala u centralnom uredu telefonskog poduzeća. Udaljeni kraj FT1 kruga je na Cross-Connect preklopniku digitalnog pristupa koji održava telefonsko poduzeće. Sistemi koji dijele isti digitalni preklopnik mogu se prebacivati između DS0 kanala. Ova shema je popularna kod Pružatelja Internetskih Usluga (ISP) koji koriste jedinstvenu T1 sabirnicu iz njihove lokacije do digitalnog preklopnika u telefonskoj tvrtki. U tim slučajevima, više klijenata može biti posluženo FT1 uslugom. U tipičnom slučaju možete spojiti T1/E1 CSU/DSU ili multipleksor preko V.35 ili RS 449 serijskog sučelja na višekratnik od 64 kbps. Sa FT1 imate prealocirani podskup od 24 kanala. T1 multipleksor mora biti konfiguriran da ispuni samo vremenske proreze koji su pridruženi vašoj usluzi.

## Frame relay

Frame relay je protokol za usmjeravanje okvira kroz mrežu na temelju polja IP adrese (identifikator povezivanja podatkovne veze) u okviru i za upravljanje smjerom ili virtualnim povezivanjem.

Frame-relay mreže u U.S. podržavaju brzine prijenosa podataka od T1 (1.544 mbps) i T3 (45 mbps). Frame relay možete shvatiti kao način iskorištavanja postojećih T1 i T3 linija koje su u vlasništvu dobavljača usluge. Većina telefonskih tvrtki danas pružaju uslugu Frame Relay za korisnike koji žele veze na 56 kbps do T1 brzina. (U Europi, Frame Relay brzine variraju od 64 kbps do 2 mbps. U U.S.A., Frame Relay je iznimno popularan zbog niske cijene. Međutim, u nekim područjima je zamijenjen bržom tehnologijom, kao što je asinkroni način prijenosa (ATM).

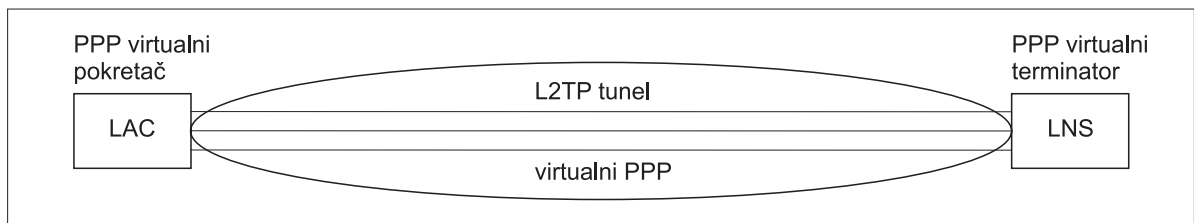
## Podrška za L2TP (tuneliranje) za PPP veze

Protokol Tuneliranja Razine Dva (L2TP) je tunelirajući protokol koji predstavlja proširenje Protokola Point-to-Point (PPP) kako bi podržao tunel na razini veze između L2TP klijenta koji šalje zahtjev (L2TP Koncentrator Pristupa ili LAC) i ciljne L2TP poslužiteljske krajnje točke (L2TP Mrežni Poslužitelj ili LNS).

## Protokol Tuneliranja Razine Dva

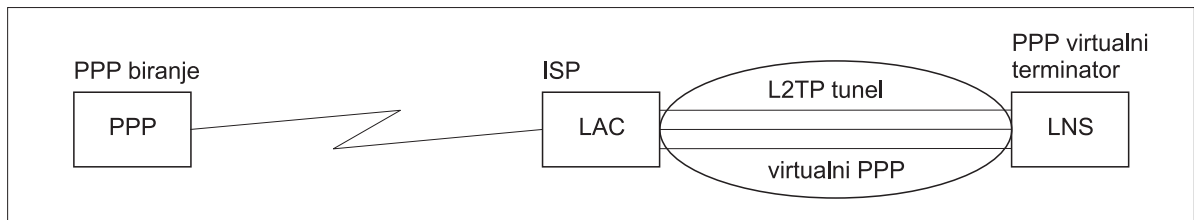
Korištenjem tunela Protokola Tuneliranja Razine Dva (L2TP) moguće je odvojiti lokaciju na kojoj protokol biranja završava i mjesto gdje se pruža pristup mreži. Zato se L2TP naziva i *Virtualni PPP*.

Ove slike ilustriraju tri različite implementacije tuneliranja L2TP-a.



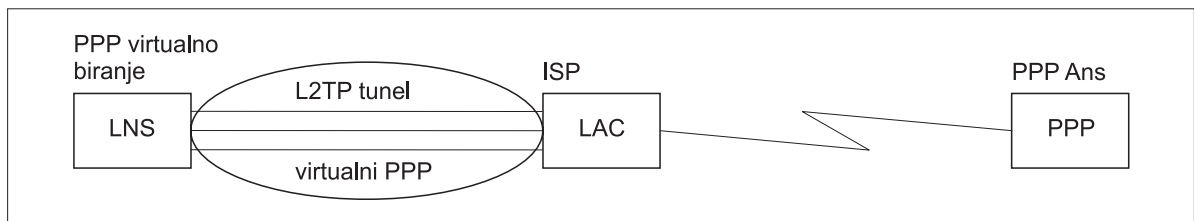
RBAEE563-0

Slika 10. PPP virtualni inicijator ili PPP virtualni terminator



RBAEE561-0

Slika 11. PPP inicijator biranja ili PPP virtualni terminator



RBAEE562-0

Slika 12. PPP virtualno biranje ili PPP virtualni odgovor

L2TP protokol dokumentiran je kao RFC standard RFC-2661. L2TP tunel se može prostirati kroz cijelu PPP sesiju ili samo kroz jedan dvodijelne sesije. Ovo se može predstaviti kao četiri različita tunelirajuća modela.

### Srodne informacije

Scenarij: Zaštita L2TP dobrovoljnog tunela s IPSec

 RFC editor

### Dobrovoljni tunel:

U modelu proizvoljnog tunela, korisnik stvara tunel, najčešće korištenjem klijenta sa omogućenim Protokolom Tuneliranja Razine Dva (L2TP).

Kao rezultat toga, korisnik šalje L2TP pakete pružatelju Internetskih usluga (ISP) koji ih onda prosljeđuje na mrežni poslužitelj L2TP-a (LNS). Kod proizvoljnog tuneliranja ISP ne treba podržavati L2TP i inicijator L2TP tunela je na istom sistemu kao i udaljeni klijent. U ovom modelu, tunel se širi kroz cijelu sesiju Point-to-Point protokola od L2TP klijenta prema LNS-u.

### Model obaveznog tunela - dolazeći poziv:

U modelu obaveznog tunela - dolazni poziv, tunel se kreira bez ikakve akcije od korisnika i bez izbora za korisnika.

Kao rezultat toga, korisnik šalje pakete Point-to-Point protokola Pružatelju Internetskih usluga (ISP) (Protokol Tuneliranja Razine Dva (L2TP) konzentator pristupa (LAC)). ISP sažima pakete u L2TP i šalje ih u tunel L2TP mrežnom poslužitelju (LNS). U slučajevima obaveznog tunela ISP mora biti omogućen za L2TP. U ovom modelu tunel se prostire kroz dio PPP sesije između LNS-a i ISP-a.

### **Model obaveznog tunela - udaljeni poziv:**

U modelu obaveznog tunela-udaljenom biranju kućni gateway (L2TP mrežni poslužitelj - LNS) inicira tunel prema Pružatelju Internetskih Usluga (ISP) (LAC) i upućuje ISP na postavljanje lokalnog poziva prema klijentu odgovora Protokola Point-to-Point (PPP).

Ovaj model je namijenjen za slučajeve gdje udaljeni klijent PPP odgovora ima trajno uspostavljeni telefonski broj s ISP-om. Ovaj model se treba koristiti kada poduzeće s uspostavljenom prisutnošću na Internetu treba uspostaviti vezu do udaljenog ureda koji zahtijeva vezu biranja. U ovom modelu tunel se prostire kroz dio PPP sesije između LNS-a i ISP-a.

### **L2TP multi-hop povezivanje:**

Multi-hop veza Protokola Tuneliranja Razine Dva (L2TP) je način preusmjerenja L2TP prometa za klijentske L2TP konzentatore pristupa (LAC) i L2TP mrežne poslužitelje (LNS).

Multi-hop veza se uspostavlja korištenjem L2TP multi-hop prilaza (sistem koji povezuje profil L2TP Terminatora i L2TP Inicijatora). Da biste uspostavili multi-hop povezivanje, L2TP multi-hop prilaz ponaša se kao LNS za skup LAC-ova istovremeno kad se ponaša i kao LAC za dani LNS. Tunel je uspostavljen od klijentskog LAC-a do L2TP multi-hop prilaza, a zatim je drugi tunel uspostavljen između L2TP multi-hop prilaza i ciljnog LNS-a. L2TP promet od klijentskog LAC-a je zatim preusmjeren L2TP multi-hop prilazom do ciljnog LNS-a, a promet od ciljnog LNS-a je preusmjeren do klijentskog LAC-a.

### **PPPoE (DSL) podrška za PPP veze**

*Digitalna Pretplatnička Linija (DSL)* odnosi se na klasu tehnologije korištenu za postizanje veće pojasne širine kroz postojeće bakrene telefonske kablove koji su provedeni između korisnikove lokacije i Pružatelja Internetskih Usluga (ISP)

DSL dopušta istovremene usluge glasa i prijenosa podataka velike brzine preko jedne parice bakrene telefonske žice. Brzine modema su se polako povećavale korištenjem raznih metoda kompresije i drugih tehnika ali na današnjim najvećim brzinama (56 Kbps) dosegnut je limit ove tehnologije. DSL tehnologija omogućuje puno veće brzine kroz linije dvostruke parice iz centralnog ureda do kuće, škole ili poslovnih lokacija. U nekim područjima mogu se dostići brzine do 2 Mbps. PPP se obično koristi preko serijskih komunikacija kao što su modemske veze s biranjem. Mnogi DSL Dobavljači Internetskih Usluga sada koriste PPP preko Etherneta (PPPoE) zbog njegovih dodanih svojstava prijave na sustav i sigurnosti.

*DSL modem* je uređaj koji se stavlja na obje strane bakrene telefonske linije kako bi se računalo (ili LAN) moglo spojiti na Internet kroz DSL vezu. Za razliku od telefonske veze, obično nije potrebna namjenska telefonska linija (POTS razdjeljivač omogućuje istovremeno dijeljenje linija). Iako DSL modemi izgledaju poput klasičnih analognih modema oni pružaju puno veću propusnost.

### **Oprema za povezivanje**

Sistem koristi modeme, terminalske adaptore Digitalne Mreže Integriranih Usluga, token-ring adaptore, Ethernet adaptore ili jedinice usluge kanala/jedinice usluge podataka (CSU/DSU) uređaje za rukovanje vezama Protokola Point-to-Point (PPP).

Postoje četiri vrste komunikacijske opreme koje možete koristiti za vašu PPP okolinu:

- Modemi
- CSU/DSU
- ISDN terminalski adaptori

- Ethernet adaptori (za PPPoE povezivanja)

## Modemi

I vanjski i interni modem mogu se koristiti za veze Point-to-point (PPP) protokola.

Skup naredbi korišten u modemu je normalno opisan u dokumentaciji modema. Naredbe se koriste za resetiranje i inicijaliziranje modema i za izdavanje naredbe modemu za biranje telefonskog broja udaljenog sistema. Svaki model modema se mora definirati prije nego što se može koristiti s PPP profilom veze, jer različiti modeli modema imaju različiti inicijalizacijski naredbeni niz. Ako se radi o internom modemu, modemska nizovi su već preddefinirani za korištenje.

Sistem ima puno preddefiniranih modela modema, a novi modeli mogu se definirati kroz System i Navigator. Postojeća definicija se može koristiti kao osnova za definiranje novog tipa. Ako niste sigurni koje naredbe koristi vaš modem ili ako nemate pristup dokumentaciji modema, počnite s Generic Hayes definicijom modema. Preddefinirane definicije ne mogu se mijenjati. Ipak, dodatne naredbe se mogu dodati postojećoj inicijalizacijskoj naredbi ili nizu biranja.

Možete koristiti elektroničku korisničku podršku koja je uključena sa sistemom kako bi postavili PPP veze. Na starijim sistemima modem elektroničke korisničke podrške je bio IBM 7852-400 vanjski modem. Ovaj modem zamijenjen je sa modelom MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. Na novijim sistemima 2771, 2793, ili neki drugi podržani interni modemi mogu se koristiti kao modemi elektroničke korisničke podrške.

### Srodne reference

“Softverski i hardverski zahtjevi” na stranici 31

Okolina Point-to-Point Protokola (PPP) zahtjeva posjedovanje barem dva računala koja podržavaju PPP. Jedno od ovih računala, System i platforma, može biti davalac ili primatelj.

## CSU/DSU

Jedinica usluge kanala (CSU) je uređaj koji spaja terminal na digitalnu liniju. Jedinica usluge podataka (DSU) je uređaj koji vrši zaštitne i dijagnostičke funkcije telekomunikacijske linije. Tipično, dva uređaja su pakirana kao jednostruka jedinica, CSU/DSU.

Možete zamisliti CSU/DSU kao skupi modem visoke snage. Takav uređaj je potreban za oba kraja T-1 ili T-3 veze; jedinice na oba kraja moraju biti od istog proizvođača.

### Srodne reference

“Softverski i hardverski zahtjevi” na stranici 31

Okolina Point-to-Point Protokola (PPP) zahtjeva posjedovanje barem dva računala koja podržavaju PPP. Jedno od ovih računala, System i platforma, može biti davalac ili primatelj.

“Digitalna usluga i Digitalne Podatkovne Usluge” na stranici 33

Možete koristiti digitalnu uslugu i Digitalne Podatkovne Usluge (DDS) pomoću Point-to-Point protokola (PPP).

## ISDN terminalski adaptori

Digitalna Mreža Integriranih Usluga (ISDN) pruža vam digitalnu vezu koja omogućuje komunikaciju korištenjem bilo koje kombinacije glasa, podataka, video-signalu i sl. unutar raznih multimedijalnih aplikacija.

Trebate provjeriti da li je vaš terminalski adaptor podesan za korištenje na sistemu.

Slijedite ove korake da bi konfigurirali vaš terminal adaptor:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Modemi** i izaberite **Novi Modem**.
3. Iz dijalog kućice **Svojstva Novog Modema** unesite ispravne vrijednosti za sva **polja** na kartici **Općenito**. Osigurajte da ste specifikirali ISDN terminal adaptor kao komunikacijski uređaj.
4. Izaberite karticu **ISDN parametri**.
5. Dodajte ili promijenite ISDN svojstva na kartici **ISDN parametri** da bi uparili svojstva koje su potrebna vašem terminal adaptoru.

### Srodni zadaci

“Primjer: Konfiguriranje ISDN terminalskog adaptora” na stranici 54

Ovaj primjer demonstrira kako konfigurirani terminalski adaptor Digitalne Mreže Integriranih Usluga (ISDN).

### Srodne reference

“Softverski i hardverski zahtjevi” na stranici 31

Okolina Point-to-Point Protokola (PPP) zahtjeva posjedovanje barem dva računala koja podržavaju PPP. Jedno od ovih računala, System i platforma, može biti davalac ili primatelj.

“Integrirana mreža digitalnih usluga” na stranici 34

Digitalna mreža integriranih usluga (ISDN) pruža izmjenjivu digitalnu povezanost s kraja na kraj. ISDN može prenositi i glas i podatke preko iste veze.

### Prijedlozi ISDN terminalskog adaptora:

Postoji nekoliko različitih adaptora terminala koje možete koristiti.

Predloženi vanjski terminalski adaptor Integrirane Mreže Digitalnih Usluga (ISDN), ili ISDN modem, je **3Com/U.S. Robotics Courier I ISDN V.Everything**. On podržava V.34 analogne modemske veze, V.90 (X2), V.92 i multilink PPP preko ISDN u načinu rada originator i odgovor. Također automatski podržava Protokol provjere autentičnosti rukovanja (CHAP) preko ISDN PPP veze. Dostupni su i sljedeći ISDN terminalni adaptori: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA i ADtran ISU 2x64 Dual Port.

- **Veze koje potiču iz sistema.** Na CHAP izazove koji dolaze sa strane koja prima, odgovara Courier I terminalski adaptor, dok sa sistemom dogovara provjeru autentičnosti Protokola provjere autentičnosti lozinkom (PAP). PAP odgovori se ne pojavljuju na ISDN vezi.
- **Veze na koje sistem odgovara.** Courier I zahtijeva CHAP provjeru autentičnosti pozivajuće strane ako konfiguracija odgovora uzrokuje time da sistem otvara provjeru autentičnosti sa CHAP izazovom. Ako sistem otvara provjeru autentičnosti s PAP-om, Courier I terminalski adaptor provjerava autentičnost pomoću PAP-a.

Ako koristite Courier I modem proizveden prije 1999, provjerite da li je taj modem spojen sa vašim sistemom pomoću V.35 kabla kako bi dobili najbolje performanse vaše ISDN veze. RS-232 do V.35 modemska kabela je isporučena sa Courier I modemom; međutim, starije verzije tog kabela imaju krivi spol V.35 konektora. Kontaktirajte 3Com/US Robotics korisničku podršku radi zamjene.

**Bilješka:** Prema 3Com/US Robotics, V.35 verziju terminalskog adaptora više nije moguće dobiti od dobavljača treće stranke iako neke V.35 verzije još uvijek mogu biti dostupne od njih. RS-232 se još uvijek ponešto preporuča iako uz smanjene performanse sistema pošto su RS-232 veze ograničene na 115.2 KB.

Osigurajte se da je V.35 brzina linije sistema postavljena na 230.4 kbps.

### Ograničenja ISDN terminalskog adaptora:

U ovom poglavlju procijenjeni su terminalni adaptori. Oni se preporučuju samo kao izvorište udaljenih veza Digitalne Mreže Integriranih Usluga (ISDN) iz sistema.

### 3Com Impact IQ ISDN:

Ovaj terminalni adaptor preporuča se za System i platformu iz sljedećih razloga:

- Terminalni adaptor ne podržava V.34 analogne modemske veze. Međutim, on može podržavati veze V.34 analognog modema korištenjem vanjske RJ-11 veze.
- Terminalni adaptor trenutno ne podržava V.90 veze.
- Terminalni adaptor možda nije povezan na sistem brzinama većim od 115 200 bps.
- Terminalni adaptor ne podržava automatski Protokol provjere autentičnosti rukovanja (CHAP). Ako postavite S84 na 0, vrši se CHAP provjera autentičnosti.

- Sistem ne može odrediti kad veza završava kod nadgledanja signala Podatkovni Skup Spreman iz terminalskog adaptora. Ovo može uzrokovati potencijalno sigurnosno izlaganje sistema.

### **Motorola BitSurfr Pro ISDN:**

Ovaj terminalski adaptor se ne preporuča za System i platformu iz sljedećih razloga:

- Terminal adaptor ne podržava V.34 analogne modemske veze. Međutim, on može podržavati veze V.34 analognog modema korištenjem vanjske RJ-11 veze.
- Terminalski adaptor trenutno ne podržava V.90 veze.
- Terminalski adaptor možda nije povezan na sistem brzinama većim od 115 200 bps.
- Terminalski adaptor automatski ne podržava Protokol provjere autentičnosti rukovanja (CHAP). Međutim, postavljanje @M2=C dozvoljava izvođenje CHAP autorizacije.
- Terminalski adaptor ne dozvoljava automatski odgovor na pozive jednostruke i višestruke veze. Udaljeni terminalski adaptor koji je izvor poziva mora biti postavljen na isti protokol (jednostruka ili višestruka veza) kao terminalski adaptor koji odgovara na poziv.
- Mehanizam kontrole toka hardvera ne radi dobro sa ovim terminalskim adaptorom. Ovo rezultira smanjenjem performansi kad sistem šalje podatke na multilink PPP vezu.

## **Rukovanje IP adresama**

Point-to-Point Protokol (PPP) veze omogućuju nekoliko različitih skupova opcija za upravljanje IP adresama ovisno o tipu profila veze.

- DHCP može središnje upravljati dodjeljivanjem IP adrese za vašu mrežu. Saznajte kako postaviti i upravljati DHCP uslugama za vašu mrežu. Pogledajte Protokol Konfiguracije Dinamičkog Hosta
- DNS vam može pomoći u upravljanju imenima hosta pridruženim IP adresama. Saznajte kako postaviti i upravljati DNS uslugama za vašu mrežu. Pogledajte Sistem Domenskih Imena
- BOOTP se koristi za pridruživanje klijentskih radnih stanica sistemu i pridruživanje IP adresa istim. Saznajte kako postaviti i upravljati BOOTP uslugama za vašu mrežu. Pogledajte Bootstrap protokol

### **Srodne reference**

“Scenarij: Povezivanje vašeg sistema sa PPPoE koncentratorom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

## **Filtriranje IP paketa**

Filtriranje IP paketa ograničava usluge pojedinim korisnicima koji se prijavljuju na mrežu.

Filtriranje paketa može dozvoliti ili onemogućiti pristup na temelju određinih IP adresa, portova ili oboje. Različite politike se mogu nametati definiranjem višestrukih skupova pravila filtriranja paketa gdje svaki ima svoj vlastiti identifikator PPP filtra. Pravila filtriranja paketa mogu se dodijeliti pojedinom primateljskom profilu veze ili se dodijeliti korištenjem Grupne Politike koja primjenjuje pravila filtriranja određenoj kategoriji korisnika. Pravila filtra paketa sama po sebi nisu definirana u PPP-u ali su definirana pod Pravilima IP Paketa u System i Navigator.

Za L2TP veze, VPN s IPsec filtriranjem se treba koristiti radi zaštite mrežnog prometa.

### **Srodne reference**

“Scenarij: Povezivanje vašeg sistema sa PPPoE koncentratorom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

### **Srodne informacije**

IP filtriranje i prijevod mrežne adrese

Virtualno privatno umrežavanje (VPN)

## Strategija upravljanja IP adresom

Prije konfiguriranja PPP profila veze morate se upoznati sa strategijom upravljanja IP adresama vaše mreže. Ova strategija utječe na puno odluka u konfiguracijskom procesu uključujući strategije provjere autentičnosti, sigurnosna razmatranja i TCP/IP postavke.

### Izvorišni profili veze

Uobičajeno, lokalne i udaljene IP adrese definirane na neki profil davatelja biti će definirane kao *Dodijeljeno od udaljenog sistema*. Ovo administratorima omogućuje kontrolu IP adresa koje će biti korištene za vezu sa udaljenih sistema. Većina svih veza na Dobavljača Internet servisa (ISP) biti će definirane na ovaj način, iako mnogi ISP-ovi mogu, uz dodatnu naknadu, ponuditi i fiksne IP adrese.

Ako definirate fiksne IP adrese za lokalnu ili udaljenu IP adresu morate biti sigurni da je udaljeni sistem definiran tako da prihvaća IP adrese koje ste definirali. Jedna tipična aplikacija je da definirate lokalnu IP adresu kao stalnu IP adresu i udaljenu koju će dodijeliti udaljeni sistem. Sistem koji povezujete se može definirati na isti način, tako da će prilikom povezivanja dva sistema međusobno razmijeniti IP adrese kao način za učenje IP adresa udaljenog sistema. Ovo može biti korisno za ured koji naziva drugi ured radi privremene povezanosti.

Druga stvar koju treba uzeti u obzir je ta da li želite omogućiti maskiranje IP adrese. Na primjer, ako se sistem spaja na Internet kroz ISP ovo može omogućiti pripojenoj mreži iza sistema da pristupi Internetu. U osnovi, sistem sakriva IP adrese sistema mreže iza lokalne IP adrese pridružene ISP-u tako da sav IP promet izgleda kao da dolazi sa tog sistema. Postoje dodatna razmatranja glede usmjeravanja kako za sisteme na LAN-u (kako bi bili sigurni da je njihov Internetski promet poslan na sistem) tako i za sistem gdje trebate omogućiti kućicu **dodaj udaljeni sistem kao defaultni smjer**.

### Primateljski profili veze

Primateljski profili veze imaju više razmatranja IP adresa i opcija nego što imaju Izvorišni Profili Veze. Kako ćete konfigurirati IP adrese ovisi o planu upravljanja IP adresama za vašu mrežu, vašim specifičnim potrebama za performansama i funkcionalnosti ove veze i planu sigurnosti.

### Lokalne IP adrese

Za jedan primateljski profil možete definirati jedinstvenu IP adresu ili koristiti postojeću lokalnu IP adresu vašeg sistema za identificiranje kraja PPP veze. Za profile primatelja definirane za istovremenu podršku višestrukim vezama morate koristiti postojeću lokalnu IP adresu. Ako ne postoje lokalne IP adrese možete stvoriti virtualnu IP adresu za ovu svrhu.

### Udaljene IP adrese

Postoji mnogo opcija za dodjeljivanje udaljenih IP adresa PPP klijentima. Sljedeće opcije se mogu specificirati na TCP/IP stranici profila povezivanja primatelja.

**Bilješka:** Ako želite da se udaljeni sistem smatra dijelom LAN-a trebate konfigurirati usmjeravanje IP adresa, navesti IP adresu unutar raspona IP adresa za sisteme pripojene LAN-u i provjeriti da je IP prosljeđivanje omogućeno i za ovu vezu i za sistem.

Tablica 8. Opcije dodjele IP adresa za profil veze primatelja

Opcija	Opis
Fiksna IP adresa	Definirati ćete pojedinačnu IP adresu koja se treba dati udaljenim korisnicima kad nazovu. To je IP adresa samo za hosta (Maska podmreže je 255.255.255.255) i samo za jednostruke profile veze primatelja.

Tablica 8. Opcije dodjele IP adresa za profil veze primatelja (nastavak)

Opcija	Opis
Spremište adresa	Definirati ćete početnu IP adresu i tada raspon onoliko dodatnih IP adresa koliko treba definirati. Svaki korisnik koji se povezuje dobit će jedinstvenu IP adresu unutar definiranog raspona. To je IP adresa samo za hosta (Maska pod mreže je 255.255.255.255) i samo za višestruke profile veza primatelja.
RADIUS	Udaljenu IP adresu i njenu masku pod mreže će odrediti Radius poslužitelj. To vrijedi samo ako je definirano sljedeće: <ul style="list-style-type: none"> <li>• Radius podrška za provjeru ovlaštenja i IP adresiranje je omogućena iz konfiguracije usluga Poslužitelja udaljenog pristupa.</li> <li>• Provjera ovlaštenja je omogućena za profil primatelja veze i definirana je tako da se provjera ovlaštenja radi udaljeno s Radius-om.</li> </ul>
DHCP	Udaljena IP adresa je određena putem DHCP poslužitelja izravno ili neizravno preko DHCP primopredajnika. To vrijedi samo ako je DHCP podrška bila omogućena iz konfiguracije usluga Udaljenog poslužitelja pristupa. To je samo-host IP adresa (Maska pod mreže je 255.255.255.255).
Bazirano na korisničkom ID-u udaljenog sistema	Udaljena IP adresa je određena korisničkim ID-om definiranim za udaljeni sistem prilikom provjere autentičnosti. To omogućuje administratoru da dodijeli različite udaljene IP adrese (i njima pridružene maske pod mreže) korisniku koji poziva. Ovo također omogućuje definiranje dodatnih smjerova za ove korisničke ID-ove tako da možete prilagoditi okolinu poznatom udaljenom korisniku. Provjera ovlaštenja mora biti omogućena da bi ova funkcija radila ispravno.
Definiranje dodatnih IP adresa baziranih na ID-u korisnika udaljenog sistema	Ova opcija dozvoljava definiranje IP adresa na temelju korisničkog ID-a udaljenog sistema. Ova opcija je automatski izabrana (i mora se koristiti) ako je metoda dodjele udaljene IP adrese definirana kao <b>Na temelju korisničkog ID-a udaljenog sistema</b> . Ova opcija je također dozvoljena za načine dodjele IP adrese ili Stalne IP adrese i Spremišta adresa. Kad se udaljeni korisnik spoji na sistem izvesti će se pretraga za određivanje IP adrese koja je definirana posebno za tog korisnika. Ako jest, tada će se ta IP adresa, maska i skup mogućih smjerova koristiti za povezivanje. Ako korisnik nije definiran IP adresa će preuzeti defaultnu vrijednost Fiksne IP adrese ili sljedeće adrese iz IP Spremišta Adresa.
Dopuštanje udaljenom sistemu da definira vlastitu IP adresu	Ova opcija omogućuje udaljenim korisnicima da definiraju svoju vlastitu IP adresu ako se tako dogovore. Ako ne dođe do pregovora za korištenje njihove vlastite IP adrese, udaljena IP adresa će se odrediti prema udaljenoj metodi pridruživanja IP adrese. Ova opcija je inicijalno onemogućena i potrebno ju je pažljivo razmotriti prije omogućavanja.
Usmjeravanje IP adrese	Klijent biranja i sistem moraju imati ispravno konfigurirano usmjeravanje IP adresa ako klijent treba pristup bilo kojim IP adresama LAN-a kojem sistem pripada.

## Sistemska provjera ovlaštenja

PPP veze sa System i platformom podržavaju nekoliko opcija provjere autentičnosti, kako udaljenih klijenata koji biraju u sistem, tako i veze prema ISP-u ili drugom sistemu prema kojima sistem bira.

Sistem podržava nekoliko metoda za održavanje informacija za provjeru autentičnosti. Ove metode uključuju jednostavne popise provjere valjanosti na sistemu koji sadrži popise autoriziranih korisnika i njihove lozinke za podršku poslužitelja Korisničke usluge udaljene provjere autentičnosti biranja (RADIUS). RADIUS poslužitelji održavaju detaljne informacije o mrežnim korisnicima. Sistem također podržava nekoliko opcija za šifriranje korisničkog ID-a i informacije o lozinki u rasponu od jednostavne razmjene lozinke do podrške za Protokol provjere autentičnosti rukovanjem (CHAP-MD5). Možete navesti svoje preference za sistemska provjeru autentičnosti, uključujući korisnički i ID i lozinku za provjeru valjanosti sistema kod biranja prema van na kartici **Provjera autentičnosti** u profilu veze u System i Navigator.

### Srodne reference

“Scenarij: Povezivanje vašeg sistema sa PPPoE konzentratorom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke



Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

“Scenarij: Provjera autentičnosti veza biranja pomoću RADIUS NAS-a” na stranici 21

Poslužitelj Pristupa Mreži (NAS) koji se izvodi na sistemu može usmjeravati zahtjeve za provjerom autentičnosti od klijenata biranja do zasebnog Poslužitelja usluge provjere autentičnosti udaljenog korisnika biranja (RADIUS). Ako mu je provjerena autentičnost, RADIUS također kontrolira IP adrese koje se pridružuju korisnicima.

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23  
Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

## Protokol Provjere autentičnosti izazova rukovanjem s MD5

Protokol Provjere autentičnosti izazova rukovanjem (CHAP-MD5) koristi algoritam (MD-5) za izračunavanje vrijednosti koja je poznata samo sistemu za koji se obavlja provjera autentičnosti i udaljenom uređaju.

Sa CHAP, korisnički ID i lozinka su uvijek šifrirani, tako da je to sigurniji protokol od Protokola za provjeru autentičnosti lozinke (PAP). Ovaj protokol je djelotvoran protiv pokušaja pristupa reprodukcijom i metodom pokušaja i pogrešaka. CHAP provjera identiteta se može odigrati više nego jednom tokom veze.

Sistem koji provjerava identitet šalje poziv udaljenom uređaju koji se pokušava spojiti na mrežu. Udaljeni uređaj odgovara s vrijednošću koja se izračuna običnim algoritmom (MD-5) koji koriste oba uređaja. Sistem koji provjerava uspoređuje odgovor s vlastitim izračunom. Provjera identiteta se potvrđuje ako se vrijednosti slažu; u protivnom veza se prekida.

### Srodne reference

“Scenarij: Spajanje udaljenih klijenata biranja na sistem” na stranici 12

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

“Protokol provjere autentičnosti lozinkom”

Protokol provjere autentičnosti lozinkom (PAP) koristi dvostrano rukovanje kako bi omogućio ravnopravnim sistemima jednostavnu metodu dokazivanja svog identiteta.

## Proširivi Protokol provjere autentičnosti

Proširivi Protokol provjere autentičnosti (EAP) omogućuje interakciju modela provjere autentičnosti treće stranke i PPP implementacije.

EAP proširuje PPP, pružajući standardne mehanizme podrške za sheme provjere identiteta, kao što su token (smart) kartice, Kerberos, Public Key i S/Key. EAP odgovara na zahtjev povećanja provjere autentičnosti sa sigurnosnim uređajima drugih proizvođača. EAP štiti sigurne virtualne privatne mreže (VPN) od hakera koji koriste napade rječnikom i pogađanjem lozinke. EAP poboljšava Protokol provjere autentičnosti (PAP) i Protokol provjere autentičnosti rukovanja (CHAP).

S EAP-om, podaci o provjeri identiteta nisu uključeni u podatke, nego su uključeni s podacima. Ovo omogućuje udaljenim sistemima pregovaranje o nužnoj provjeri autentičnosti prije primanja ili prosljeđivanja informacija.

Sistem ne podržava EAP direktno. Međutim, možete koristiti udaljenu provjeru autentičnosti pomoću poslužitelja Usluge provjere autentičnosti Udaljenog Korisnika Biranja (RADIUS), koji može podržavati neke dodatne sheme provjere autentičnosti koje su prethodno opisane.

## Protokol provjere autentičnosti lozinkom

Protokol provjere autentičnosti lozinkom (PAP) koristi dvostrano rukovanje kako bi omogućio ravnopravnim sistemima jednostavnu metodu dokazivanja svog identiteta.

Rukovanje se provodi dok se uspostavlja veza. Kada se uspostavi veza, udaljeni uređaj šalje korisnički ID i lozinku sistemu za provjeru autentičnosti. Ovisno o ispravnosti tog para šifri, sistem koji provjerava identitet ili nastavlja ili prekida vezu.

PAP provjera zahtijeva da ime korisnika i lozinka budu poslani udaljenom sistemu u obliku čistog teksta. S PAP-om korisnički ID i lozinka se nikad ne šifriraju što ih čini osjetljivim na hakerski napad i praćenje. Iz ovog razloga trebali biste koristiti Protokol provjere autentičnosti izazovom rukovanja (CHAP) kad god je moguće.

#### **Srodne reference**

“Protokol Provjere autentičnosti izazova rukovanjem s MD5” na stranici 43

Protokol Provjere autentičnosti izazova rukovanjem (CHAP-MD5) koristi algoritam (MD-5) za izračunavanje vrijednosti koja je poznata samo sistemu za koji se obavlja provjera autentičnosti i udaljenom uređaju.

## **Pregled Korisničke usluge udaljene provjere autentičnosti biranja**

*Korisnička Usluga udaljene provjere autentičnosti biranja (RADIUS)* je Internetski standardni protokol koji pruža centraliziranu provjeru autentičnosti, knjiženje i usluge IP upravljanja za udaljene korisnike u distribuiranoj mreži biranja.

Model RADIUS klijent-poslužitelja ima Poslužitelj mrežnog pristupa (NAS) koji radi kao klijent na RADIUS poslužitelju. Sistem u ulozi NAS-a šalje korisničke informacije i informacije o vezi namjenskom RADIUS poslužitelju koristeći standardni RADIUS protokol definiran u RFC 2865.

RADIUS poslužitelji reagiraju na primljene korisničke zahtjeve za vezom provjerom autentičnosti korisnika i vraćanjem kompletnih konfiguracijskih informacija potrebnih NAS-u kako bi NAS (sistem) mogao isporučiti autorizirane usluge korisniku biranja provjerene autentičnosti.

Ako se RADIUS poslužitelj ne može pozvati, sistem može usmjeriti autentikacijske zahtjeve na drugi poslužitelj. Ovo omogućuje globalnim poduzećima pružanje korisnicima usluge biranja za jedinstvenim korisničkim ID-om za prijavu pristupa na razini korporacije neovisno o korištenoj točki pristupa.

Kad se zahtjev za autorizacijom primi od strane RADIUS poslužitelja provjerava se njegova valjanost; potom RADIUS poslužitelj dešifrira podatkovni paket kako bi pristupio informacijama o korisničkom imenu i lozinki. Informacija se prosljeđuje odgovarajućem sigurnosnom sistemu koji je podržan. Ovo mogu biti datoteke UNIX lozinke, Kerberos, komercijalni sigurnosni sistem ili čak prilagođeno razvijeni sigurnosni sistem. RADIUS poslužitelj šalje natrag sistemu sve usluge za koje je korisnik provjerene autentičnosti autoriziran za korištenje kao što je IP adresa. Zahtjevima RADIUS knjiženja rukuje se na sličan način. Podaci o obračunu za udaljene korisnike se mogu poslati na predodređeni RADIUS obračunski poslužitelj. Standardni RADIUS protokol knjiženja definiran je u RFC 2866. RADIUS obračunski poslužitelj odgovara na primljene zahtjeve za obračun tako da zapisuje podatke iz zahtjeva za RADIUS obračun.

#### **Srodne reference**

“Scenarij: Provjera autentičnosti veza biranja pomoću RADIUS NAS-a” na stranici 21

Poslužitelj Pristupa Mreži (NAS) koji se izvodi na sistemu može usmjeravati zahtjeve za provjerom autentičnosti od klijenata biranja do zasebnog Poslužitelja usluge provjere autentičnosti udaljenog korisnika biranja (RADIUS). Ako mu je provjerena autentičnost, RADIUS također kontrolira IP adrese koje se pridružuju korisnicima.

## **Validacijska lista**

Validacijska lista se koristi za pohranjivanje informacija korisničkog ID-a i lozinke udaljenih korisnika.

Možete koristiti postojeće validacijske liste ili kreirati vlastite na stranici provjere valjanosti Profila veze korisnika. Unosi validacijske liste također zahtijevaju identifikaciju tipa protokola za provjeru autentičnosti za pridruživanje s korisničkim ID-om i lozinkom. Ovo može biti **šifrirano - CHAP-MD5/EAP** ili **nešifrirano - PAP**.

Pogledajte online pomoć za više informacija.

#### **Srodne reference**

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23  
Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih

atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

## Razmatranja o pojasnoj širini za multilink

Često je potrebno osigurati dodatnu pojasnu širinu za izvršavanje određenih zadataka, ali to nije uvijek slučaj.

Nabavka specijaliziranog hardvera i skupih komunikacijskih linija ne mora biti uistinu potrebna. Protokol PPP Multilink (MP) grupira više PPP veza kako bi oformile jedinstvenu virtualnu vezu ili snop. Agregacija višestrukih linija povećava ukupnu učinkovitu pojasnu širinu između dva sistema korištenjem standardnih modema i telefonskih linija. Možete uključiti do šest veza u MP snop. Kako bi postavili multilink vezu oba kraja PPP veze moraju podržavati multilink protokol. Multilink protokol dokumentiran je kao RFC standard RFC-1990.

### Pojasna širina na zahtjev

Sposobnost dinamičkog dodavanja i uklanjanja fizičkih veza dozvoljava sistemu da bude konfiguriran da dobavi pojasnu širinu samo kada je potrebna. Ovaj pristup često se naziva kao Pojasna Širina na Zahtjev i omogućuje vam plaćanje za dodatnu pojasnu širinu samo kad ju zaista i koristite. Kako bi koristili prednosti Pojasne Širine na Zahtjev barem jedna strana mora biti u mogućnosti nadgledanja uporabe potpune pojasne širine koja trenutno postoji u MP snopu. Veze se mogu dodavati u i uklanjati iz snopa kad vrijednost uporabe pojasne širine premašuje vrijednosti definirane od strane konfiguracije. Protokol Dodjeljivanja Pojasne Širine omogućuje stranama komunikacije pregovaranje o dodavanju i uklanjanju veza iz MP snopa. RFC-2125 dokumentira i PPP Protokol Dodjeljivanja Pojasne Širine (BAP) i Protokol Kontrole Dodjeljivanja Pojasne Širine (BACP).

#### Srodne informacije



RFC editor

---

## Konfiguracija PPP-a

Prije no što možete koristiti PPP za postavljanje point-to-point veze morate konfigurirati vašu PPP okolinu.

#### Srodne reference

“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

## Stvaranje profila veze

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

Profil veze je logički prikaz sljedećih detalja povezivanja:

- Linija i tip profila
- Postavke višestrukih veza
- Udaljeni telefonski brojevi i opcije biranja
- Provjera ovlaštenja
- TCP/IP postavke: IP adrese i usmjeravanje
- Upravljanje poslom i prilagodba veze
- Poslužitelji imena domene

**Usluge daljinskog pristupa**, pod direktorijem Mreža, sadrži sljedeće objekte:

- Izvorišni profili veze
- Primateljski profili veze
- **Modemi**

Slijedite ove korake da bi konfigurirali profil veze:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Izaberite jednu od sljedećih opcija:
  - Desni klik na **Izvorišni Profili Veze** za postavljanje sistema koji inicira vezu.
  - Desni klik na **Primateljski Profili Veze** za postavljanje sistema koji dozvoljava ulazne zahtjeve od udaljenih sistema i korisnika.
3. Izaberite **Novi profil**.
4. Na stranici Postav profila povezivanja point-to-point izaberite tip protokola.
5. Specificirajte izbore načina.
6. Izaberite konfiguraciju veze.
7. Kliknite **OK**.

Pojavljuje se nova stranica Svojstava profila point-to-point. Možete postaviti ostale vrijednosti koje su specifične za vašu mrežu. Pogledajte online pomoć za više informacija.

#### **Srodni zadaci**

“Pridruživanje modema opisu linije” na stranici 55

Ova tema demonstrira korake za pridruživanje modema opisu linije.

#### **Srodne reference**

“Scenarij: Povezivanje vašeg sistema sa PPPoE koncentratorom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke Linije (DSL) korištenjem Point-to-Point protokola preko Etherneta (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

“Scenarij: Spajanje udaljenih klijenata biranja na sistem” na stranici 12

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

“Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema” na stranici 15

Administratori u tipičnom slučaju postavljaju uredske mreže kako bi omogućili zaposlenicima izlaz na Internet. Administratori mogu koristiti modem za spajanje sistema na Pružatelja Internetskih Usluga (ISP). PC klijenti spojeni na LAN mogu komunicirati sa Internetom koristeći i5/OS operativni sistem kao prilaz.

“Scenarij: spajanje vaše korporativne i udaljene mreže modemom” na stranici 18

Modem omogućuje izmjenu podataka između dvije udaljene lokacije (kao npr. centralni ured i podružnica). Point-to-Point Protokol (PPP) može spojiti dva LAN-a postavljanjem veze između sistema u centralnom uredu i drugom u podružnici.

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23

Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

## **Tip protokola: PPP ili Serijski linijski protokol Interneta (SLIP)**

PPP zamjenjuje Internetski Protokol Serijske Linije (SLIP) kao izabrani protokol za point-to-point veze.

PPP omogućuje interoperabilnost između softvera udaljenog pristupa različitih proizvođača. PPP također omogućuje mrežnim komunikacijskim protokolima korištenje istih fizičkih linija za komunikaciju.

SLIP Zahtjev za Komentarom (RFC) nikad nije postao Internetski standard zbog sljedećih nedostataka:

- SLIP nema standardni način za definiranje IP adresiranja između dva hosta. To znači da se ne može koristiti nenumerirana mreža.
- SLIP nema podršku za otkrivanje grešaka ili sažimanje grešaka. Otkrivanje grešaka ili sažimanje grešaka je implementirano u PPP-u.
- SLIP nema podršku za provjeru ovlaštenja sistema, dok PPP ima dvosmjernu provjeru ovlaštenja.

SLIP se još uvijek koristi i podržan je od strane i5/OS operativnog sistema. Međutim, IBM predlaže da koristite PPP prilikom postavljanja point-to-point povezanosti. SLIP ne pruža podršku za multilink veze. U usporedbi sa SLIP-om, PPP ima bolju provjeru ovlaštenja. PPP se bolje izvodi zbog svojih mogućnosti sažimanja.

**Bilješka:** SLIP profili veza koji su definirani s ASYNC tipovima linija nisu više podržani u ovom izdanju. Ako imate te profile veza, morate ih premjestiti ili na SLIP profil ili PPP profil koji koristi PPP tip linije.

## Izbori načina

Odabir načina za profile veze Protokola Point-to-Point (PPP) uključuju odabire tipa veze i načina rada. Vaši odabiri načina navode kako sistem koristi novu PPP vezu.

Slijedite ove korake da bi odredili vaše izbore načina:

1. Izaberite jedan od sljedećih tipova veza:
  - Birana linija
  - Iznajmljena linija
  - Protokol Tuneliranja Razine Dva (L2TP) (virtualna linija)
  - Point-to-point protokol preko Etherneta (PPPoE) linija
2. Izaberite način rada koji je prikladan za novu PPP vezu.
3. Zapišite tip veze i način rada koji ste izabrali. Trebate ove informacije kada počinjete konfigurirati vaše PPP veze.

### Birana linija:

Kad koristite modem (interni ili vanjski) ili vanjski terminalski adaptor Digitalne Mreže Integriranih Usluga (ISDN) za spajanje preko telefonske linije, izaberite vezu komutirane linije.

Tip veze komutirane linije ima sljedeće načine rada:

### Odgovor

Izaberite ovaj način rada kako bi omogućili udaljenom sistemu biranje u sistem.

### Biranje

Izaberite ovaj način rada kako bi omogućili sistemu biranje van na udaljeni sistem.

### Biranje na zahtjev (samo biranje)

Izaberite ovaj način rada kako bi omogućili sistemu da automatski bira van na udaljeni sistem kad je TCP/IP promet za udaljeni sistem primijećen na sistemu. Veza završava kada je prijenos podataka potpuno i u određenom vremenskom periodu nema prometa.

### Biranje na zahtjev (omogućen namjenski ravnopravan za odgovor)

Izaberite ovaj način rada kako bi omogućili sistemu odgovaranje na pozive iz namjenskog udaljenog sistema. Ovaj način omogućuje sistemu automatsko zvanje udaljenog sistema kad je TCP/IP promet za udaljeni sistem primijećen na sistemu. Ako oba sistema koriste i5/OS operativni sistem i ovaj način rada, TCP/IP promet teče između dva sistema na zahtjev i bez potrebe za stalnog fizičkom vezom. Ovaj način rada treba namjenski resurs. Udaljeni ravnopravan mora birati način rada da bi ispravno funkcionirao.

### Biranje na zahtjev (omogućen udaljeni ravnopravan)

Izaberite ovaj način rada da omogućite udaljenom sistemu da bude biran ili da mu se odgovori. Za rukovanje dolaznim pozivima morate se referencirati na postojeći profil iz PPP profila veze koji navodi ovaj način rada. To omogućuje da jedan profil odgovora rukuje svim dolaznim pozivima od jednog ili više udaljenih ravnopravnih i odvojeni profil biranja na zahtjev za svaki odlazni poziv. Ovaj način rada ne treba namjenski resurs za rukovanje dolaznim pozivima od udaljenih ravnopravnih.

### Iznajmljena linija:

Ako imate namjensku liniju između lokalnog i udaljenog sistema izaberite vezu iznajmljene linije. Ako imate iznajmljenu liniju onda ne trebate modem ili terminalski adaptor Digitalne Mreže Integriranih Usluga za spajanje dva sistema.

Unajmljenom linijom između dva sistema smatra se stalna ili namjenska linija. Ona je uvijek otvorena. Jedan kraj iznajmljene linije je konfiguriran kao pokretač, a drugi kraj je konfiguriran kao terminator.

Tip veze iznajmljene linije ima sljedeće načine rada:

#### **Terminator**

Izaberite ovaj način rada kako bi omogućili udaljenom sistemu pristup kroz namjensku liniju. Ovaj način rada se odnosi na profil odgovora iznajmljene linije.

#### **Inicijator**

Izaberite ovaj način rada kako bi omogućili sistemu pristup udaljenom sistemu kroz namjensku liniju. Ovaj način rada se odnosi na profil biranja iznajmljene linije.

#### **L2TP (virtualna linija):**

Ako želite uspostaviti vezu između sistema koji koriste Protokol Tuneliranja Razine Dva (L2TP) izaberite L2TP vezu.

Nakon što je uspostavljen L2TP tunel, napravila se virtualna Point-to-Point (PPP) veza između vašeg sistema i udaljenog sistema. Korištenjem L2TP tunelske komunikacije zajedno s IP zaštitom (IP-SEC), možete slati, usmjeravati i primati zaštićene podatke preko Interneta.

Tip veze L2TP (virtualna linija) ima sljedeće načine rada:

#### **Terminator**

Izaberite ovaj način rada kako bi omogućili da se udaljeni sistem spoji na sistem preko L2TP tunela.

#### **Inicijator**

Izaberite ovaj način rada kako bi omogućili da se sistem spoji na udaljeni sistem preko L2TP tunela.

#### **Daljinsko biranje**

Izaberite ovaj način rada kako bi omogućili da se sistem spoji na drugi sistem ili Pružatelja Internetskih Usluga (ISP) preko L2TP tunela i da uputite ISP-a na biranje udaljenom PPP klijentu.

#### **Inicijator višestrukog skoka**

Izaberite ovaj način rada kako bi omogućili sistemu uspostavljanje multi-hop veze.

**Bilješka:** L2TP terminirajući profil kojem je pridružen ovaj multi-hop inicijator mora imati označenu kućicu **Dozvoli multi-hop vezu** te stavku u PPP listi provjere valjanosti koja povezuje PPP korisničko ime sa profilom multi-hop inicijatora.

#### **PPPoE linija:**

Veze Point-to-Point protokola preko Ethernet-a (PPPoE) koriste virtualnu liniju za slanje PPP podataka (kroz Ethernet adaptor) na model Linije Digitalnog Pretplatnika (DSL) kojeg osigurava Dobavljač Internetskih Usluga (ISP). Modem je također spojen na LAN zasnovan na Ethernet-u.

Ovo omogućuje pristup visoke brzine Internetu za korisnike LAN-a kroz PPP sesije na i5/OS operativnom sistemu. Nakon što je započela veza između sistema i ISP-a, pojedinačni korisnici mogu započinjati jedinstvene sesije sa ISP-om kroz PPPoE.

PPPoE vezama se koriste samo profili veze davalaca. Veze podrazumijevaju Inicijatorski način rada i koriste samo jednu liniju.

## Konfiguracija veze

Konfiguracija veze definira tip servisne linije koju profil veze Protokola Point-to-Point (PPP) koristi za uspostavljanje veze<sup>4</sup>.

Tipovi linijske usluge ovise o tipu veze koji specificirate.

### Srodne reference

“Scenarij: Povezivanje vašeg sistema sa PPPoE koncentраторom pristupa” na stranici 10

Mnogi Pružatelji Internetskih Usluga (ISP-ovi) nude pristup visoke brzine Internetu preko Digitalne Pretplatničke Linije (DSL) korištenjem Point-to-Point protokola preko Ethernet (PPPoE). Možete spojiti vaš sistem sa ovim ISP-ovima kako bi omogućili veze velike pojasne širine koje i dalje zadržavaju prednosti Point-to-Point protokola (PPP).

“Scenarij: Spajanje udaljenih klijenata biranja na sistem” na stranici 12

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

“Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema” na stranici 15

Administratori u tipičnom slučaju postavljaju uredske mreže kako bi omogućili zaposlenicima izlaz na Internet. Administratori mogu koristiti modem za spajanje sistema na Pružatelja Internetskih Usluga (ISP). PC klijenti spojeni na LAN mogu komunicirati sa Internetom koristeći i5/OS operativni sistem kao prilaz.

“Scenarij: spajanje vaše korporativne i udaljene mreže modemom” na stranici 18

Modem omogućuje izmjenu podataka između dvije udaljene lokacije (kao npr. centralni ured i podružnica). Point-to-Point Protokol (PPP) može spojiti dva LAN-a postavljanjem veze između sistema u centralnom uredu i drugom u podružnici.

### Pojedinačna linija:

Za definiranje linije Protokola Point-to-Point (PPP) koja je pridružena analognom modemom izaberite ovaj servis linije. Ova se opcija koristi i za stalne unajmljene linije na kojima modem nije potreban. Profil PPP veze koristi isti i5/OS resurs komunikacijskog porta.

Analogna jednostruka linija, ako je to potrebno, se može konfigurirati kao dijeljena između profila odgovora i profila biranja. Dinamičko dijeljenje resursa je nova funkcija razvijena radi povećanja upotrebljivosti resursa. Do V5R2 resursi modema bili su predani čim se pokrenuo profil koji ih je koristio. To je ograničavalo korisnika na jedan resurs po sesiji, čak i ako je resurs bio u pasivnom stanju čekanja. Sada se primjenjuju nova pravila dijeljenja kada se pristupi određenom resursu. Postoje dva slučaja: prvo, profil biranja pokrenut je prije profila odgovora; drugo, profil odgovora pokrenut je prije profila biranja. Pretpostavka je da je dijeljenje resursa omogućeno. U prvom slučaju, pokrenuti profil pozivača će uspješno uspostaviti vezu. Profil odgovora koji je pokrenut kasnije će pričekati da linija postane dostupna. Kada se završi telefonska veza, profil odgovora zatražit će liniju i pokrenut će se. U drugom slučaju, pokrenuti profil odgovora će pričekati ulazno povezivanje. Osim ako nije napravljena dolazna veza, profil biranja koji je drugi pokrenut, “posudit” će liniju od profila odgovora koji će “iznajmiti” liniju. Tada će biti uspostavljena izlazna veza. Kada se završi povezivanje, profil biranja vratit će liniju profilu odgovora koji će opet biti spreman za prihvatanje dolaznih veza. Kako bi omogućili funkciju dijeljenja kliknite karticu **modem** za opis izmjenjive linije i izaberite **Omogućiti Dinamičko Dijeljenje Resursa**.

Usluga jednostruke linije se također koristi za L2TP (virtualna linija) i PPPoE (virtualna linija) tipove povezivanja. Za L2TP (virtualna linija) tipove veza, ne postoji hardverski resurs komunikacijskog porta korišten s jednostrukom linijom. Umjesto toga, jednostruka linija korištena s L2TP vezom je *virtualna* jer ne postoji fizički PPP hardver koji je potreban za postavljanje tunela. Jednostruka linija korištena s PPPoE vezom je također virtualna jer pruža mehanizam za tretiranje fizičke Ethernet linije kao da postoji PPP linija koja podržava udaljene veze. PPPoE virtualna linija je vezana na fizičku Ethernet liniju i koristi se za podršku prijenosa podataka PPP protokola preko Ethernet LAN veze na DSL modem.

### Skup linija:

Za postavljanje PPP veze na korištenje linije iz spremišta linija izaberite ovu uslugu linija. Kad PPP veza započne sistem izabire neiskorištenu liniju iz spremišta linija. Za profile biranja na zahtjev sistem ne izabire linije dok ne uoči TCP/IP promet za udaljeni sistem.

Umjesto definiranja pojedinog opisa linije za profil veze, možete koristiti linijski skup. U linijskom skupu se može odrediti jedan ili više opisa linija.

Skup linija omogućuje da profil pojedinačne veze rukuje ili s više dolaznih analognih poziva ili pojedinačnim odlaznim analognim pozivom. Linija se vraća u skup linija kada se PPP veza završi.

Ako koristite skup linija za simultano rukovanje s više analognih poziva, trebate označiti maksimalan broj dolaznih veza. Možete ovo postaviti na kartici **Veze** na dijalog kućici **Svojstva Novog Point-to-Point Profila** kad konfigurirate vaš profil veze. Koristite postav višestruke veze za korištenje spremišta linija za jednostruke veze s povećanom pojasnom širinom.

### **Prednosti u korištenju spremišta linija:**

- Ne predajete linijski resurs PPP vezi dok ne započne.

Za PPP veze koje koriste određenu liniju, veza se prekida ako linija nije dostupna, osim ako je omogućeno dijeljenje resursa. Za veze koje koriste spremište linije, barem jedna linija u spremištu linije mora biti dostupna kada se pokrene profil.

Uz to, ako su resursi konfigurirani kao dijeljeni (omogućujući dinamičko dijeljenje resursa), dostupnost dodatnih resursa dosegnuta je osobito za izlazna povezivanja.

- Profile biranja na zahtjev možete koristiti s linijskim skupovima u cilju boljeg iskorištenja resursa.

Sistem odabire liniju iz spremišta linija samo kad se koristi veza biranja na zahtjev. Druge veze mogu koristiti istu liniju u različitim vremenima.

- Možete započeti više PPP veza s manje resursa za održavanje.

Na primjer, ako vaša okolina treba jedinstvene tipove veza, ali trebate samo dvije linije u dano vrijeme, možete koristiti skup linija da bi okolina radila. Možete kreirati četiri profila veza biranja-na-zahtjev tako da se svaki odnosi na skup linija koji sadrži dva opisa linija. Svaku liniju će koristiti sva četiri profila povezivanja, uz dozvolu korištenja dva povezivanja u bilo koje vrijeme. Kad koristite linijski skup, ne trebate imati četiri odvojene linije.

Također, ako je vaše okruženje kombinacija između PPP klijenta i PPP poslužitelja, linije se mogu dijeliti (omogućavanjem dinamičkog dijeljenja resursa), bez obzira da li se one koriste kao 'jednostruke linije' ili su smještene u 'spremište linija'. Profil koji je prvi pokrenut neće predati resurse osim ako je veza aktivna. Na primjer, ako je pokrenut PPP poslužitelj i osluškuje dolazne veze, on će 'iznajmiti' liniju koju koristi PPP Klijentu koji je pokrenuo i 'posudio' podijeljenu liniju od PPP Poslužitelja.

### **Konfiguriranje spremišta linija**

Spremišta linija se definiraju u profilu veze. Za osnovnu konfiguraciju spremišta linija slijedite ove korake:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža → Usluge Udaljenog Pristupa**.
2. Kreirajte profil veze da ili bira ili prima pozive. Izaberite jednu od sljedećih opcija:
  - Desni klik na **Izvorišni Profili Veze** za postavljanje sistema koji inicira vezu prema udaljenom sistemu.
  - Desni klik na **Primateljski Profili Veze** za postavljanje sistema koji dozvoljava ulazne zahtjeve od udaljenih sistema i korisnika.
3. Izaberite **Novi profil**.
4. Za profil davatelja (biranje van) izaberite: PPP, Birana linija i Način rada (tipično biranje). Za konfiguraciju veze izaberite **Spremište linija**. Kliknite **OK** i System i Navigator otvara prozor svojstava za ovaj profil veze.

**Bilješka:** Možete također izabrati spremište linija kad stvarate primateljske profile veze. Opcija spremišta linija može ali ne mora biti na popisu ovisno o sljedećim vrijednostima polja: tip protokola, tip veze i način rada.

5. Na stranici Općenito imenujte profil i unesite opis.



6. Na stranici Povezivanja unesite ime za spremište linija i kliknite **Novo**. To će otvoriti dijalog **Svojstva novog spremišta linija** koji će prikazati sve dostupne linije i modeme za ovaj sistem.
7. Izaberite linije koje želite koristiti i dodajte ih u spremište. Možete također i kliknuti na **Nova linija** da definirate novu liniju.
8. Kliknite **OK** da spremite ovo spremište linija i da se vratite na svojstva Novog Point-to-Point profila.
9. Dovršite potrebne informacije o drugim stranicama (na primjer, TCP/IP postavke i provjera autentičnosti).
10. Profil veze spušta se na popisu dostupnih linija (unutar spremišta) sve dok se ne pojavi dostupan resurs koji koristi tu liniju za vezu. Koristite System i Navigator pomoć za daljnje informacije.

#### **Srodne reference**

“Scenarij: Spajanje udaljenih klijenata biranja na sistem” na stranici 12

Udaljeni klijenti kao što su mobilni klijenti, često trebaju pristup na korporativnu mrežu. Ovi klijenti biranja mogu dobiti pristup sistemu pomoću Point-to-Point protokola (PPP).

“Scenarij: Spajanje uredskog LAN-a na Internet pomoću modema” na stranici 15

Administratori u tipičnom slučaju postavljaju uredske mreže kako bi omogućili zaposlenicima izlaz na Internet. Administratori mogu koristiti modem za spajanje sistema na Pružatelja Internetskih Usluga (ISP). PC klijenti spojeni na LAN mogu komunicirati sa Internetom koristeći i5/OS operativni sistem kao prilaz.

“Scenarij: spajanje vaše korporativne i udaljene mreže modemom” na stranici 18

Modem omogućuje izmjenu podataka između dvije udaljene lokacije (kao npr. centralni ured i podružnica).

Point-to-Point Protokol (PPP) može spojiti dva LAN-a postavljanjem veze između sistema u centralnom uredu i drugom u podružnici.

#### **Podrška profila višestrukih veza:**

Point-to-point profili veze koji podržavaju višestruke veze omogućuju vam posjedovanje jednog profila veze koji rukuje sa više digitalnih, analognih ili L2TP poziva.

Ovo je korisno kad želite da se više korisnika spaja na vaš sistem ali ne želite specificirati posebne point-to-point profile veze za rukovanje svakom pojedinom PPP linijom. Ova sposobnost je posebno korisna za 2805 4-portni integrirani modem gdje se četiri linije mogu koristiti sa jednog adaptoru.

Kod analognih linija s podrškom za viševezni profil, sve linije u navedenom linijskom skupu se koriste za maksimalan broj veza. U osnovi posebna nit profila veze se započinje za svaku liniju definiranu u spremištu linija. Sve niti profila veze čekaju dolazne pozive na svojim linijama.

#### **Lokalne IP adrese za profile višestrukih veza**

Možete koristiti lokalnu IP adresu sa profilima višestrukih veza ali to mora biti postojeća IP adresa već definirana na sistemu. Možete koristiti padajuću listu lokalnih IP adresa za odabir postojeće IP adrese. Udaljeni korisnici mogu pristupiti resursima koji su na lokalnoj mreži ako izaberete lokalnu IP adresu kao lokalnu adresu vašeg PPP profila. Isto tako morate definirati IP adrese koje su u skupu udaljenih IP adresa tako da budu u istoj mreži kao i lokalna IP adresa.

Ako nemate lokalnu IP adresu ili ne želite da udaljeni korisnici pristupaju LAN-u, morate definirati virtualnu IP adresu za vaš sistem. Virtualna IP adresa se zove i sučelje bez kruga. Vaši PPP profili mogu koristiti ovu IP adresu kao svoju lokalnu IP adresu. Pošto ova IP adresa nije povezana sa fizičkom mrežom, ona ne prosljeđuje automatski promet prema drugim mrežama koje su priključene na vaš sistem.

Ako kreirate virtualnu IP adresu, slijedite ove korake:

1. U System i Navigator, proširite vaš sistem i pristupite **Mreža → TCP/IP konfiguracija → IPV4 → Sučelja**.
2. Desno kliknite **Sučelja** i izaberite **Novo sučelje → Virtualni IP**.
3. Slijedite upute čarobnjaka sučelja i kreirajte svoje virtualno IP sučelje. Vaši profili point-to-point veze mogu koristiti virtualne IP adrese jednom kad se one stvore. Možete koristiti padajući popis iz polja **Lokalna IP adresa** na stranici TCP/IP postavke kako bi koristili IP adresu sa vašim profilom.

**Bilješka:** Virtualna IP adresa mora biti aktivna prije pokretanja profila višestruke veze; inače profil neće započeti. Da biste aktivirali IP adresu, nakon kreiranja sučelja izaberite opciju za pokretanje IP adrese prilikom korištenja čarobnjaka za sučelje.

## Udaljene IP adrese za profile višestrukih veza

Možete koristiti i spremište udaljenih IP adresa s profilima višestrukih veza. Tipičan jednevezni point-to-point profil vam omogućuje da odredite samo jednu udaljenu IP adresu, koja se predaje sistemu koji poziva kad se veza uspostavi. Budući da se višestruki pozivatelji mogu sada povezivati istovremeno, koristi se spremište udaljenih IP adresa za definiranje početne IP adrese i raspona dodatnih IP adresa koja se daju pozivajućem sistemu.

## Ograničenja spremišta linija

Ova ograničenja važe kad se linijski skup koristi kod višestrukih veza:

- Pojedina veza može istovremeno postojati samo u jednom skupu linija. Ako uklonite neku liniju iz skupa, ona se može koristiti u nekom drugom skupu linija.
- Kod pokretanja profila višestrukih veza koji koristi skup linija, sve linije u skupu linija se koriste do maksimalnog broja veza u profilu. Ako ne postoje linije, sve nove veze će se prekinuti. Također, ako ne postoje linije u skladištu linija i pokreće se drugi profil, on će se prekinuti.
- Kad pokrenete profil pojedine veze koji ima linijski skup, sistem koristi samo jednu liniju iz skupa linija. Ako pokrenete višestruki profil veze koji koristi isto skladište linije, sve preostale linije u skladištu linija se mogu koristiti.

### Srodni zadaci

“Scenarij 1: Konfiguracija L2TP terminirajućeg profila za sva sučelja na particiji koja ima modeme u vlasništvu” na stranici 28

Sa stvaranje terminirajućeg profila za sva sučelja, pratite sljedeće korake:

### Udaljena spremišta IP adresa:

Sistem može koristiti spremište udaljenih IP adresa za bilo koje odgovaranje ili zaustavljanje profila point-to-point povezivanja koje se koristi s višestrukim dolaznim povezivanjima.

Ovo uključuje Protokol Tuneliranja Razine Dva (L2TP) i spremišta linija sa maksimalnim brojem veza većim od jedan. Ova funkcija omogućuje sistemu pridruživanje jedinstvene IP adrese svakoj dolaznoj vezi.

Prvi sistem koji se spaja prima IP adresu definiranu u polju početne IP adrese. Ako se već koristi ta IP adresa, daje se sljedeća IP adresa unutar raspona. Na primjer, pretpostavimo da je Početna IP adresa 10.1.1.1, a Broj IP adresa je definiran kao 5. IP adrese unutar spremišta udaljenih adresa bit će 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 i 10.1.1.5. Podmreža maske definirana za adrese skladišta udaljenih IP adresa će uvijek biti 255.255.255.255.

Ova ograničenja važe kad se koriste skupovi udaljenih IP adresa:

- Profil s više od jednom vezom može određivati isti skup adresa. Međutim, kada se iskoriste sve IP adrese u spremištu, svako daljnje povezivanje bit će odbijeno dok se ne završi neko drugo povezivanje, a IP adresa postane dostupna.
- Da biste dodijelili specifične IP adrese nekim udaljenim sistemima, a drugim dolaznim sistemima dozvolili korištenje IP adrese iz spremišta, napravite sljedeće korake:
  1. Aktivirajte provjeru identiteta udaljenih sistema iz oznake **Provjera autentičnosti**, tako da se može saznati korisničko ime udaljenog sistema.
  2. Definirajte skup udaljenih IP adresa za sve dolazne zahtjeve za uspostavu veze koji ne trebaju neku određenu IP adresu.
  3. Definirajte udaljene IP adrese za specifične korisnike označavanjem **Definiraj dodatne IP adrese na osnovi ID-a korisnika udaljenog sistema** i kliknite **IP adrese definirane po Imenu korisnika**.

Kad je udaljeni korisnik spojen na sistem, sistem određuje da li je za korisnika definirana posebna IP adresa. U tom slučaju se IP adresa daje udaljenom sistemu; inače se vraća IP adresa od udaljenog spremišta IP adresa.

## Konfiguriranje vašeg modema za PPP

Modem vam pruža mogućnost analognog povezivanja (iznajmljene i komutirane linije). Za vaše analogne point-to-point (PPP) konekcije možete koristiti eksterni modem, interni modem ili terminalni adaptor digitalne mreže integriranih usluga (ISDN).

### Srodne reference

“Rješavanje problema vezanih uz PPP” na stranici 61

Ako dođe do problema vezanih uz veze Protokola Point-to-Point (PPP) možete se koristiti kontrolnom listom za prikupljanje informacija o grešci. Ova kontrolna lista pomoći će vam u identifikaciji simptoma greške i rješavanju PPP problema veze.

## Konfiguracija novog modema

Možete konfigurirati novi modem korištenjem postojećeg opisa modema ili zasnovati opis modema na prethodnom opisu.

Da biste konfigurirali novi modem, pratite ove korake.

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Modemi** i izaberite **Novi Modem**.
3. Na kartici **Općenito** unesite ispravne vrijednosti u sve kućice **polja**.
4. Opcijski: kliknite karticu **Dodatni parametri** da biste dodali potrebne inicijalizacijske naredbe vašeg modema.
5. Kliknite **OK** da sačuvate vaše unose i zatvorite stranicu Svojstva novog modema.

## Korištenje postojećeg opisa modema

Da biste odredili možete li koristiti postojeći opis modema, pratite ove korake:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Izaberite **Modemi**.
3. Pregledajte listu modema i nađite ime proizvođača, model i izvedbu vašeg modema.

**Bilješka:** Ako je vaš modem uključen u default popis, ne trebate poduzimati daljnje korake.

4. Desno kliknite opis modema koji približno odgovara vašem modemu i izaberite **Svojstva** da pregledate naredbene nizove.
5. Posavjetujte se s dokumentacijom modema da odredite specifične naredbene nizove za vaš modem.  
Koristite svojstva default modema ako se naredbeni nizovi podudaraju sa zahtjevima vašeg modema. U suprotnom morate kreirati opis modema i dodati ga na modemsku listu.

## Stvaranje opisa modema prema prethodnom opisu

Da biste kreirali opis modema na temelju prethodnog opisa, pratite ove korake:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Izaberite **Modemi**.
3. Na modemskoj listi desno kliknite **Generic Hayes** i izaberite **Novi modem na temelju**.
4. U dijalogu **Novi modem** promijenite naredbene nizove tako da odgovaraju onima koje treba vaš modem.

### Srodne reference

“Rješavanje problema vezanih uz PPP” na stranici 61

Ako dođe do problema vezanih uz veze Protokola Point-to-Point (PPP) možete se koristiti kontrolnom listom za prikupljanje informacija o grešci. Ova kontrolna lista pomoći će vam u identifikaciji simptoma greške i rješavanju PPP problema veze.

## Postavljanje naredbenih nizova modema

Možete naći ekvivalentni naredbeni niz u priručniku za korisnika za vaš modem. Koristite predložene postavke proizvođača u opisu modema.

Tablica 9. Modemi definirani na sistemu i naredbeni nizovi

Svojstvo modema	Ispravan niz naredbi za većinu modema
Modem vraćen na tvorničke postavke	AT&F ili AT&Z
<b>Inicijalizacija modema:</b>	
Display Verbal Results Codes	Q0 i V1
Normalni CD i DTR načini	&C1 i &D2
Echo mode off	E0
Data Set Ready (DSR) za praćenje Carrier Detect	&S1
Omogući hardversku kontrolu protoka (RTS/CTS)	
Omogući ispravljanje grešaka i neobavezno sažimanje (V.42/V.42 bis)	
Osigurajte se da je DTE-DCE brzina linije omogućena za izvođenje na fiksnih 115.2 kbps (ili maksimum dozvoljen od strane modema).	
(Neobavezno) Omogući vrijeme neaktivnosti ako modem podržava tu funkciju	
<b>Način odgovora modema:</b>	
Odgovor nakon $n$ zvonjenja	S0= $n$ gdje je $n = 1$ ili $2$
Odspajanje ako se veza ne uspostavi nakon $m$ sekundi	S7= $m$
Tip biranja modema	ATDT za tonsko biranje ili ATDP za pulsno biranje

## Primjer: Konfiguriranje ISDN terminalskog adaptora

Ovaj primjer demonstrira kako konfigurirani terminalski adaptor Digitalne Mreže Integriranih Usluga (ISDN).

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Modemi** i izaberite **Novi Modem**.
3. Na kartici **Općenito** unesite ispravne vrijednosti u sve kućice **polja**.
4. Opcijsko: Kliknite karticu **ISDN parametri** kako bi dodali sve nužne inicijalizacijske naredbe za vaš modem.  
Za ISDN terminalske adaptore, naredbe i parametri u ovoj listi se šalju na terminalski adaptor samo u sljedećim uvjetima:

- Kad su naredbe ili parametri u listi ili promijenjeni ili dodani
- Kao rezultat određenih akcija oporavka od greške koje sistem izvodi

Prema tome, ove naredbe bi trebale uključivati i biti ograničene na sljedeće postavke:

- Postavljanje ISDN tipa prekidača i verzije koju vam daje lokalna telefonska tvrtka.
  - Postavljanje brojeva direktorija i identifikatora profila usluga (SPID) koje daje lokalna telefonska tvrtka.
  - Postavljanje Identifikatora Stavki Terminala (TEI) koje vam može dati lokalna telefonska tvrtka.
  - Postavljanje protokola kanala B (asinkroni-na-sinkroni PPP).
  - Druge postavke modema koje imaju varijabilne duljine parametara koji zahtijevaju vraćanje na početak reda kako bi označili duljinu parametra.
  - Spremanje i aktiviranje novih postavki tako da se oni mogu vratiti kad se resetiraju ili kad se sistem isključi.
  - Naredba provjere aktivnog stanja sučelja  $U$  (ATD $x$ ), koja sistemu omogućuje određivanje kad je uspješno izvedena sinkronizacija sa ISDN sklopom centralnog ureda.  $X$  može biti bilo koja znamenka dozvoljena za telefonski broj, uključujući # i \*.
5. Kliknite **Dodaj** da dodate dodatne naredbe modema. One mogu biti sa ili bez pridruženog parametra i kratkog opisa popisa naredbi. Sve naredbe koje navedete bez pridruženog parametra mogu dobiti pridruženi parametar kad se modem dodijeli opisu linije.

6. Kliknite **OK** da sačuvate vaše unose i zatvorite stranicu Svojstva novog modema.

#### **Srodne reference**

“ISDN terminalski adaptori” na stranici 38

Digitalna Mreža Integriranih Usluga (ISDN) pruža vam digitalnu vezu koja omogućuje komunikaciju korištenjem bilo koje kombinacije glasa, podataka, video-signalala i sl. unutar raznih multimedijalnih aplikacija.

### **Pridruživanje modema opisu linije**

Ova tema demonstrira korake za pridruživanje modema opisu linije.

1. U System i Navigator, izaberite vaš sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa** → **Izvorišni Profili Veze ili Primateljski Profili Veze**.
2. Izaberite jednu od sljedećih opcija:
  - DA biste radili s postojećim profilom povezivanja, desno kliknite profil povezivanja i izaberite **Svojstva**.
  - Da biste radili s novim profilom povezivanja, kreirajte novi .
3. Na stranici Svojstva novog point-to-point profila, izaberite karticu **Veza** i kliknite **Nova**.
  - Unesite ime za konfiguraciju linka.
  - Kliknite **Novo** da biste otvorili prozor Svojstva nove linije.
4. U prozoru Svojstva nove linije kliknite karticu **Modem** i s popisa izaberite modem. Izabrani će modem biti pridružen tom opisu linije. Za interne modeme bi odgovarajuća definicija modema već trebala biti izabrana. Za više informacija pogledajte online pomoć.

Možete konfigurirati izvorišne profile veze kako bi posuđivali PPP liniji i modem pridružen primateljskom profilu veze koji čeka dolazni poziv. Izvorišna veza će vratiti PPP liniju i modem primateljskom profilu veze čim veza završi. Za omogućavanje ove funkcije izaberite opciju **Omogućiti dinamičko dijeljenje resursa** na kartici **Modem** prozora konfiguracije PPP linije. Možete konfigurirati PPP linije iz kartice **Veza** na Izvorišnom i Primateljskom profilu veze.

#### **Srodni zadaci**

“Stvaranje profila veze” na stranici 45

Prvi korak konfiguracije PPP veze između sistema je stvaranje profila veze na sistemu.

### **Konfiguracija udaljenog PC-a**

Za spajanje na System i platformu sa osobnog računala (PC) koje radi na nekom od Windows 32-bitnih operativnih sistema morate provjeriti da je modem instaliran i ispravno konfiguriran te da ste instalirali TCP/IP i Dial-up Networking na osobno računalo.

Pogledajte vašu Microsoft Windows dokumentaciju za informacije o konfiguraciji Dial-up Networking-a za PC. Svakako specificirajte ili unesite sljedeće informacije:

- Tip telefonske veze mora biti **PPP**.
- Ako koristite šifrirane lozinke budite sigurni da koristite CHAP-MD5 (MS-CHAP nije podržan od strane i5/OS operativnih sistema). Neke verzije Windowsa ne podržavaju MD-5 CHAP izravno, ali se mogu konfigurirati uz dodatnu pomoć Microsofta.
- Ako koristite nešifrirane (ili neosigurane) lozinke, automatski se koristi Protokol za provjeru autentičnosti lozinke (PAP). Drugi nesigurni tipovi protokola nisu podržani od strane sistema.
- U tipičnom slučaju IP adresiranje je definirano od strane udaljenog sistema ili i5/OS operativnog sistema. Ako namjeravate koristiti alternativne metode IP adresiranja (kao npr. definiranje vlastitih IP adresa) morate biti sigurno da je sistem konfiguriran za korištenje vaše metode adresiranja.
- Dodajte DNS IP adresu ako je prikladna vašoj okolini.

### **Konfiguracija Internet pristupa kroz AT&T Globalnu Mrežu**

Ako želite komunicirati sa AT&T Globalnom Mrežom morate konfigurirati posebne profile.

Da biste pristupili ovoj usluzi, možete koristiti čarobnjaka telefonske veze AT&T globalne mreže koji će vam pomoći konfigurirati profil PPP povezivanja komutiranog biranja za biranje AT&T globalne mreže. Čarobnjak će vas provesti kroz osam ekrana, a trebat će vam oko deset minuta da obavite posao. Možete opozvati čarobnjaka u bilo kojem trenutku i nikakvi postojeći podaci neće biti spremljeni.

Sljedeći tipovi aplikacija mogu koristiti vezu AT&T Globalne Mreže:

- **Izmjena Pošte:** Omogućuje vam periodično dohvaćanje pošte sa jedinstvenog računa AT&T Globalne Mreže i slanje istog na vaš sistem za distribuciju vašim korisnicima Lotus Pošte ili korisnicima Jednostavnog Protokola Za Slanje Pošte (SMTP).
- **Dial-up Networking:** koristite druge dial-up networking aplikacije s AT&T globalnom mrežom, kao što je standardni Internet pristup.

Profile povezivanja AT&T globalne mreže održavate kao i druge PPP profile povezivanja.

Trebate jedan od sljedećih adaptora za korištenje čarobnjaka za vezu AT&T Globalne Mreže:

- 2699: Dvolinijski WAN IOA
- 2720: PCI WAN/Dvopolni IOA
- 2721: PCI Dvolinijski WAN IOA
- 2745: PCI Dvolinijski WAN IOA (zamjenjuje IOA 2721)
- 2771: Dvoportni WAN IOA, s V.90 integriranim modemom na portu 1 i standardnim komunikacijskim sučeljem na portu 2. Za korištenje porta 2 adaptora 2771, potreban je vanjski modem ili ISDN terminal adaptor s odgovarajućim kablom.
- 2772: Dvoportni V.90 integrirani modem WAN IOA
- 2793/576C: Dvoportni WAN IOA, sa V.92 integriranim modemom na portu 1 i standardnim komunikacijskim sučeljem na portu 2. Ovo zamjenjuje model 2771.
- 2805: Četvero-portni WAN IOA, sa integriranim V.92 modemom. To zamjenjuje modele 2761 i 2772.

Prije pokretanja čarobnjaka za povezivanje biranjem AT&T globalne mreže, morate skupiti ove informacije o vašem okruženju:

- Informacije računa AT&T globalne mreže (broj računa, korisnički ID i lozinka) za aplikaciju razmjene pošte ili dial-up networking aplikaciju.
- IP adrese poslužitelja pošte i poslužitelja imena domene za aplikaciju razmjene pošte.
- Ime modema koji se koristi za pojedine veze.

Da biste pokrenuli čarobnjaka za povezivanje biranjem AT&T globalne mreže pratite ove korake:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**.
2. Desno kliknite **Profili povezivanja davatelja** i izaberite **Novo povezivanje biranjem AT&T globalne mreže**.
3. Kada se pokrene čarobnjak za povezivanje biranjem AT&T globalne mreže, kliknite **Pomoć** za informacije o dovršavanju panela.

## Čarobnjaci povezivanja

Možete koristiti čarobnjake za povezivanje koji će vas voditi kroz konfiguraciju profila povezivanja.

### Čarobnjak za novo povezivanje biranjem

Ovaj čarobnjak opisuje korake za konfiguraciju profila veze biranja za pristup vašem ISP-u ili intranetu. Trebate dobiti neke informacije od vašeg mrežnog administratora ili ISP-a za izvršavanje čarobnjaka. Za više informacija o izvršavanju čarobnjaka pogledajte online pomoć.

## IBM čarobnjak univerzalnog povezivanja

Ovaj čarobnjak opisuje korake za konfiguraciju profila kojeg može koristiti softver Elektroničke Korisničke Podrške za spajanje na IBM. Elektronička korisnička podrška pruža nadgledanje vašeg jedinstvenog i5/OS okruženja kako bi vam pružila preporuke personaliziranih popravaka za vaš sistem i situacije.

### Srodne informacije

Univerzalno povezivanje

## Konfiguracija grupne politike pristupa

Folder **Politike grupnog pristupa** pod Profilima povezivanja primatelja osigurava opcije za konfiguriranje parametara point-to-point povezivanja koji se odnose na grupu udaljenih korisnika. Primjenjuje se samo na one point-to-point veze koje potječu od udaljenog sistema i primljene su od lokalnog sistema.

Za konfiguraciju grupne politike pristupa pratite sljedeće korake:

1. U System i, proširite vaš sistem i proširite **Mreža → Usluge Udaljenog Pristupa → Profili Veze Primatelja**.
2. Desno kliknite **Politike pristupa grupe** i izaberite **Nova politika pristupa grupe**.
3. Na kartici **Općenito**, unesite ime i opis za novu politiku pristupa grupe.
4. Kliknite karticu **Višestruka veza** i postavite konfiguraciju višestruke veze.

Konfiguracija višestruke veze specificira da želite imati višestruke fizičke linije povezane u snop. Maksimalni broj linija po snopu može biti između 1 i 6. Budući da ne znate tip postavke linije dok se ne uspostavi veza, default vrijednost je uvijek 1. Politika grupe se može koristiti za proširenje ili ograničavanje sposobnosti protokola Višestruke veze za određenog korisnika.

**Maksimum veza po snopu** specificira maksimalan broj veza (ili linija) za koje želite da postanu logička linija. Maksimalni broj linija ne može biti veći od slobodnih linija kada se ova politika grupe primijeni na sesiju za PPP profil.

Označite **Zatraži protokol dodjele pojasne širine** ako želite specificirati da je povezivanje uspostavljeno samo ako udaljeni sistem podržava Protokol dodjele pojasne širine (BACP). Ako se ne može dogovoriti BACP, dozvoljena je samo jednostruka veza.

5. Kliknite karticu **TCP/IP postavke** da biste omogućili bilo koje od sljedećih postavki:

**Dozvoli udaljenom sistemu pristup drugim mrežama (IP prosljeđivanje)**. Ova opcija određuje želite li IP prosljeđivanje. Ako izaberete ovu opciju onda zapravo omogućujete sistemu da preuzme ulogu usmjeritelja za ovu vezu. Ovo omogućuje IP datagramima prolazak kroz sistem na spojenu mrežu. Ako ostavite ovu opciju praznom IP odbacuje one datagrame namijenjene udaljenim sistemima koji nisu navedeni kao odredišta za bilo koje lokalne adrese ovog sistema.

Mogu postojati sigurnosni razlozi zbog kojih ne želite dozvoliti IP prosljeđivanje. Nasuprot tome, ISP obično osigurava IP prosljeđivanje. Uočite da ovo ima učinak samo ako je omogućeno prosljeđivanje IP datograma na razini sistema; inače se ignorira čak i ako je označeno. Prosljeđivanje IP datograma kroz sistem može se prikazati na kartici **Općenito** sa stranice IPv4 svojstva.

**Zatraži komprimiranje TCP/IP zaglavlja (VJ)**. Ova opcija specificira da li želite da IP komprimira informacije zaglavlja nakon uspostave povezivanja. Komprimiranje obično povećava izvedbu, posebno za interaktivni promet ili spore serijske linije. Komprimiranje zaglavlja slijedi Van Jacobson (VJ) metodu definiranu u RFC 1332. Za PPP, komprimiranje se dogovara nakon uspostavljanja veze. Ako drugi kraj veze ne podržava VJ komprimiranje sistem uspostavlja vezu bez komprimiranja.

**Koristi pravila IP paketa za ovo povezivanje**. Ova opcija određuje želite li primijeniti pravilo filtera za ovu politiku grupe. Pravila filtriranja kontroliraju IP promet u vašoj mreži. Možete koristiti ovu komponentu filtriranja IP paketa kako bi zaštitili vaš sistem filtriranjem paketa prema pravilima koje specificirate. Pravila su osnovana na informaciji u zaglavlju paketa.

## Primjena politike grupe na udaljenog korisnika

Možete primijeniti politiku grupe na korisnika udaljenog pristupa kada dovršite svojstva point-to-point za novi profili povezivanja primatelja.

Da biste primijenili politiku grupe na korisnika udaljenog pristupa, dovršite sljedeće korake:

1. Kliknite **Provjera autentičnosti** da biste otvorili stranicu Provjera autentičnosti.
2. Kliknite **Zatraži od ovog iSeries poslužitelja provjeru identiteta udaljenog sistema**.
3. Izaberite **Provjeri valjanost lokalno upotrebom validacijske liste**.
4. Ako postoji validacijska lista, izaberite je iz liste i kliknite **Otvori**. Ako je kreirate prvi put, unesite ime za novu validacijsku listu i kliknite **Nova**.
5. Kliknite **Dodaj** za dodavanje novog korisnika na validacijsku listu.
6. U prozoru Dodaj korisnika specificirajte sljedeće informacije:
  - a. Izaberite protokol provjere ovlaštenja za koji je definirano ime korisnika.
  - b. Unesite ime korisnika i lozinku.

**Bilješka:** Iz sigurnosnih razloga preporuka je da ne koristite istu lozinku za korisnika definiranu u 22341 protokolu rukovanja provjere autentičnosti (CHAP), Protokolu proširive provjere autentičnosti (EAP) i Protokolu provjere autentičnosti lozinke (PAP).

- c. Označite **Primijeni politiku grupe na korisnika**, izaberite politiku grupe iz liste i kliknite **Otvori**.

Možete promijeniti svojstva politike grupe ili raditi s postojećim postavom.

7. Kliknite **OK** za dovršenje konfiguracije i vratite se na stranicu Point-to-Point svojstva.

#### Srodne reference

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23 Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži

#### Srodne informacije

IP filtriranje i prijevod mrežne adrese

## Primjena pravila filtriranja IP paketa na PPP vezu

Možete koristiti pravila filtriranja paketa kako bi ograničili pristup korisnicima ili grupama na neke IP adrese mreže.

Tema IP filtriranje i prevodenje mrežnih adresa u informacijskom centru spominje kako stvoriti pravila IP paketa koje možete referencirati u PPP profilu veze.

Možete vidjeti postojeća pravila filtriranja IP paketa na dva načina:

- Razina profila veze
  1. Kada dovršite **Point-to-Point svojstva za Profil veze primatelja**, izaberite stranicu TCP/IP postavke i kliknite **Napredno**.
  2. Označite **Koristi pravila IP paketa za ovo povezivanje** i izaberite identifikator PPP filtera iz liste.
  3. Kliknite **OK** za primjenu PPP filtera na profil veze.
- Razina korisnika
  1. Otvorite postojeću politiku pristupa grupe ili kreirajte novu politiku pristupa grupe
  2. Kliknite na stranicu TCP/IP postavke.
  3. Označite **Koristi pravila IP paketa za ovo povezivanje** i izaberite identifikator PPP filtera iz liste.
  4. Kliknite **OK** za primjenu PPP filtera.

#### Srodne reference

“Scenarij: Upravljanje udaljenim korisničkim pristupom korištenjem grupnih politika i IP filtriranja” na stranici 23 Politike grupnog pristupa identificiraju pojedine korisničke grupe za vezu i omogućuju vam primjenu zajedničkih atributa veze i sigurnosnih postavki za cijelu grupu. Možete koristiti grupne politike zajedno sa IP filtriranjem kako bi dozvolili i ograničili pristup pojedinim IP adresama na mreži



## Omogućavanje RADIUS i DHCP usluga za profile veze

Ovo su koraci za omogućavanje usluga RADIUS-a ili Protokola Konfiguracije Dinamičkog Hosta (DHCP) za PPP primateljske profile veze.

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža → Usluge Udaljenog Pristupa**.
2. Desno kliknite **Usluge daljinskog pristupa** i izaberite **Usluge**.
3. Kliknite **DHCP-WAN** karticu. To će automatski omogućiti DHCP i otkriti koji se DHCP poslužitelj i posrednik primopredaje (ako postoji) izvodi na sistemu.
4. Za omogućavanje RADIUS usluga, kliknite na **RADIUS** karticu.
  - a. Izaberite **Omogući povezivanje RADIUS poslužitelja mrežnog pristupa**
  - b. Izaberite **Omogući RADIUS za provjeru autentičnosti**.
  - c. Ovisno o vašem RADIUS rješenju možete izabrati da RADIUS upravlja knjiženjem veze i konfiguracijom TCP/IP adresa.
5. Kliknite na tipku **RADIUS NAS postavke** da konfigurirate vezu na RADIUS poslužitelju.
6. Kliknite **OK** za povratak na System i Navigator.

### Srodne reference

“Scenarij: Provjera autentičnosti veza biranja pomoću RADIUS NAS-a” na stranici 21

Poslužitelj Pristupa Mreži (NAS) koji se izvodi na sistemu može usmjeravati zahtjeve za provjerom autentičnosti od klijenata biranja do zasebnog Poslužitelja usluge provjere autentičnosti udaljenog korisnika biranja (RADIUS). Ako mu je provjerena autentičnost, RADIUS također kontrolira IP adrese koje se pridružuju korisnicima.

---

## Upravljanje PPP-om

Ova tema sadrži informacije o zadacima upravljanja PPP-om koje možete raditi na sistemu.

### Srodne reference

“Informacije vezane uz Usluge daljinskog pristupa” na stranici 63

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

## Postavljanje svojstava za PPP profile veze

Kada kreirate profil povezivanja, obično birate protokol, tip povezivanja i način rada za novi profil povezivanja u prozoru Postav profila Point-to-Point povezivanja.

Kada unesete izbore u ovom prozoru, pojavljuje se list svojstava profila povezivanja. Specificirani izbori u prozoru Postav profila Point-to-Point povezivanja određuju sadržaj stranice i poredak kartica lista svojstava profila povezivanja. Ova stranica svojstava je različita za profile veze davatelja i profile veze primatelja.

Možete koristiti ove naputke kad završite sa svakom stranicom prozora Nova Svojstva Point-to-Point profila. Postavke koje izaberete na svakoj stranici ovise o vašoj okolini i tipu veze koju konfigurirate. System i Navigator online pomoć opisuje svaku opciju koja se pojavljuje u prozoru. Za više informacija možete pogledati PPP primjere i procedure.

## Nadgledanje PPP aktivnosti

Možete vidjeti profil veze i dnevnik sesije korištenjem System i Navigator.

### O poslovima PPP povezivanja:

- Postoje dva PPP kontrolna posla koji se koriste za upravljanje pojedinim nitima PPP veza. Ti se poslovi izvode na QYSWRK podsistemu:
  - QTPPPCTL - Glavni posao PPP kontrole. Ovaj posao upravlja svakom niti PPP veze.
  - QTPPPL2TP - L2TP poslužitelj. Ovaj posao upravlja utemeljenjem L2TP tunela i izvodi se samo ako se trenutno izvodi L2TP profil.
- Niti PPP povezivanja u QTPPPCTL-u izvode se pod QTCP korisničkim imenom.

- Poslovi SLIP veze izvode se na QSYSWRK podsistemu pod QTCP imenom korisnika. Dva su tipa imena SLIP poslova:
  - QTPPDIAL $nn$  su dial-out poslovi gdje  $nn$  bilo koji broj od 1 do 99.
  - QTPPANS $nnn$  su poslovi biranja gdje je  $nnn$  neki broj od 1 do 999.

## Rad sa profilima veze:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**. Izaberite **Profil veze davatelja** ili **Profil veze primatelja**.
2. U stupcu Profil, desno kliknite bilo koje ime profila veze i izaberite jednu od sljedećih opcija:
  - **Veze** otvara prozor za prikaz informacija o svim povezivanjima pridruženim s profilom. Informacije mogu uključivati podatke o vezi za trenutnu vezu, prethodne veze ili oboje. Dostupne su opcije za gledanje izlaza posla, detalji povezivanja, dnevnicu poziva ili dnevnicu poruka za svako povezivanje.
  - **Svojtva** otvara stranicu Svojtava za prikaz trenutnih svojtava za povezivanje.

## Pregled informacija o vezi:

1. U System i Navigator, izaberite svoj sistem i proširite **Mreža** → **Usluge Udaljenog Pristupa**. Izaberite **Profil veze davatelja** ili **Profil veze primatelja**.
2. U stupcu Profil, desno kliknite na bilo koje ime profila veze koje nema status Interaktivno i izaberite **Veze** za gledanje trenutnih informacija.  
Prikazano je svako povezivanje ovog profila (trenutno i prethodno). Polje statusa pokazuje trenutno stanje veze. Ovisno o statusu svakog PPP posla mogu se prikazati dodatne informacije, kao što su korisnički ID povezanog korisnika, ID niti, lokalna i udaljena IP adresa i ime PPP posla.
3. Da pogledate izlaz posla, detalje za vezu, dnevnik poziva ili dnevnik poruka, desno kliknite na vezu i omogućite tipke.
4. Da pogledate QTPPPCTL, kliknite **Poslovi**. U prozoru povezivanja desno kliknite ime posla i izaberite **Izlaz pisača** ili **Dnevnik posla** da prikazete informacije o svim nitima povezivanja koje su pridružene QTPPPCTL-u.
5. Za gledanje detalja veze kliknite **Detalji**. Detalji se mogu prikazati samo za trenutno aktivne sesije. Prozor s detaljima će dozvoliti gledanje dodatnih informacija o povezivanju za ovu određenu vezu.
6. Da pogledate dnevnik poziva, kliknite **Dnevnik poziva**.
7. Da pogledate dnevnik poruka, kliknite **Dnevnik poruka**.

## Rad sa PPP izlazom iz sistema:

Za rad sa PPP izlazom utipkajte WRKTCPPTP sa sistemske komandne linije:

- Za rad sa SVIM aktivnim PPP poslovima (uključujući QTPPPCTL i QTPPPL2TP poslovima), pritisnite F14 (Rad s aktivnim poslovima).
- Da bi radili sa svim izlazima određenog profila povezivanja, izaberite **opcija 8** (rad s izlazom) za taj profil.
- Za ispis konfiguracije PPP profila, izaberite **opcija 6** (Ispis) za taj profil. Zatim koristite naredbu WRKSPLF da pristupite ispisanom izlazu.

## Status povezivanja:

Status profila povezivanja prikazan je u polju **Status** za svaki profil u listi profila povezivanja pod **Mreža** → **Usluge daljinskog pristupa** nakon izbora profila Davatelja ili Primatelja. Status za pojedinu vezu prikazan je pomoću prozora Povezivanja.

Tablica 10. Opis primarnog statusa

Opis primarnog statusa	Objašnjenje
Čekanje na zahtjeve za vezom	Profil primatelja je spreman za vezu
Čekanje na dolazeći poziv	Sistem je spreman za vezu

Tablica 10. Opis primarnog statusa (nastavak)


Opis primarnog statusa	Objašnjenje
Povezivanje	U obradi povezivanja s udaljenim sistemom
Aktivna/Aktivna povezivanja	Povezivanje je napravljeno i posao se uspješno izvodi
Neaktivna	Za ovaj profil povezivanja se trenutno ne izvode nikakvi poslovi
Završeno	Informacija dostupna
Terminator višestrukog skoka pokreće inicijator višestrukog skoka	Višestruki skok je u toku
Veza višestrukog skoka je aktivna	Multihop je uspješno povezan

Tablica 11. Opis sekundarnog statusa

Opis sekundarnog statusa	Objašnjenje
Inicijaliziranje modema	inicijaliziranje modema na početku veze biranja
Čekanje na vezu modema	PPP Poslužitelj u stanju slušanja
BIRANJE xxx-xxxx	broj kojeg je birao klijent biranja
Otkriven dolazeći poziv	PPP Poslužitelj otkriva dolazeći poziv modema
Modem je povezan	PPP rukovanje uspješno je dovršeno
Operativan	PPP veza je aktivna
Veza je završila	Ravnopravan je prekinuo vezu
Zaustavljeno	Profil ili posao je završio
Greška provjere autentičnosti	PPP veze se nisu uspjele uspostaviti zbog neuspjele provjere autentičnosti
Timeout neaktivnosti veze	PPP veze se nisu uspjele uspostaviti zbog timeouata neaktivnosti
Dogovaranje IP adresa	PPP veze su prekinute zbog problema s IP dogovaranjem
Udaljeni modem nije odgovorio	PPP veze se nisu mogle uspostaviti zbog toga jer nije bilo odgovora s druge strane
Protokol je odbijen	PPP veze se nisu mogle uspostaviti zbog neuspješnog NCP dogovaranja
Neuspješno ponovno pokušavanje	PPP veza se nije uspjela uspostaviti zbog prevelikog broja ponovnih pokušaja
Primljena potvrda PPPoE sesije iz ravnopravnog	PPPoE pregovaranje uspješno je dovršeno
Uspostavljen je L2TP poziv	L2TP usmjeravanje poruke

## Rješavanje problema vezanih uz PPP

Ako dođe do problema vezanih uz veze Protokola Point-to-Point (PPP) možete se koristiti kontrolnom listom za prikupljanje informacija o grešci. Ova kontrolna lista pomoći će vam u identifikaciji simptoma greške i rješavanju PPP problema veze.

Trenutne i bitne informacije o privremenim popravcima programa (PTF-ovima) i rješavanju problema dokumentirane su na TCP/IP za i5/OS Web stranicama . Ova Web stranica pruža najnovije informacije koje nadomještaju i zamjenjuju informacije koje se nalaze u ovom skupu tema.


### 1. Zahtijevani materijal za podršku:

- Tip udaljenog hosta, operativni sistem i razinu
- i5/OS operativna systemska razina hosta

- Sve izlazne datoteke koje su spremljene u izlazni red s istim imenom kao i profil
- Dnevnicima posla za QTPPPCTL i QTPPPL2TP (ako je L2TP profil)
- Skript veze koji se koristi u vašoj okolini
- Status profila povezivanja prije i nakon što se povezivanje prekinulo

## 2. Preporučeni materijal za podršku:

- Opis linije
- Profil povezivanja  
Opcija 6 iz WRKTCPPPTP ispisuje postavke profila.
- Tip i model modema
- Naredbeni nizovi modema
- Komunikacijski trag

ITSO Redbook V4 TCP/IP za AS/400: Više Cool Stvari Nego Ikad Prije  spominje sljedeće PPP probleme. Također pruža detaljne informacije o rješavanju problema.

Za identifikaciju problema i pronalaženje rješenja pogledajte kontrolnu listu sljedeće tablice.

Tablica 12. PPP problemi iz ITSO Redbooka

Problem	Rješenje
<p><b>Konfiguracija hardvera modema</b></p> <p>Netočna konfiguracija dip-preklopnika i drugih postavki hardvera</p>	<p>Provjerite je li modem konfiguriran za ispravan tip uokvirenja. To može biti ili <i>Asinkrono</i> ili <i>Sinkrono</i>. Pogledajte priručnik modema za više informacija.</p>
<p><b>Modem AT naredbe</b></p> <p>Modem kojeg pokušavate koristiti nije u preddefiniranom popisu modema u System i Navigator.</p>	<p>Kreirajte novi modem.</p>
<p><b>PPP korisnici i lozinke</b></p> <p>Dohvaćate greške imena korisnika i lozinke kod pokušaja PPP veze.</p>	<ul style="list-style-type: none"> <li>• Osigurajte da su ID korisnika i lozinka uneseni korištenjem istih malih/velikih slova.</li> <li>• Osigurajte da je protokol provjere ovlaštenja koji je korišten među ravnopravnima isti.</li> <li>• Ne koristite PAP na jednom ravnopravnom, dok je drugi ravnopravan konfiguriran kao CHAP.</li> </ul>
<p><b>PPP linije za pokretanje profila veze</b></p> <p>Identificirane PPP linije se koriste od istog hardverskog resursa.</p>	<p>Imajte na umu isključivanje drugih linija korištenjem istog hardverskog resursa.</p>
<p><b>PPP protokol</b></p> <p>Greške u vezi se mogu dogoditi zbog loše konfiguracije PPP protokola.</p>	<p>Proučavanje nižih razina PPP protokola može biti nužno u nekim situacijama kad ravnopravni sistemi nisu u mogućnosti komunicirati međusobno zbog konfiguracijske greške. Ako PPP dnevnik ili dnevnik PPP posla ne pokazuju znak problema, možete istražiti problem korištenjem funkcije praćenja komunikacije.</p>

### Srodni koncepti

“Konfiguriranje vašeg modema za PPP” na stranici 53

Modem vam pruža mogućnost analognog povezivanja (iznajmljene i komutirane linije). Za vaše analogne point-to-point (PPP) konekcije možete koristiti eksterni modem, interni modem ili terminalni adaptor digitalne mreže integriranih usluga (ISDN).

“Konfiguracija novog modema” na stranici 53

Možete konfigurirati novi modem korištenjem postojećeg opisa modema ili zasnovati opis modema na prethodnom opisu.

### Srodne reference

“Informacije vezane uz Usluge daljinskog pristupa”



IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

---


## Informacije vezane uz Usluge daljinskog pristupa

IBM Redbooks publikacije i Web stranice sadrže informacije koje se odnose na skup tema vezanih uz Usluge daljinskog pristupa. Možete pogledati ili ispisati bilo koju od PDF datoteka.

### IBM Redbooks

- IBM i5/OS IP Mreže: Dinamično! 
- V4 TCP/IP za AS/400: Više Cool Stvari Nego Ikad Prije 

### Web stranice

Pronađite najnovije privremene popravke programa (PTF-ove) i najnovije konfiguracije za PPP i L2TP kroz PPP vezu na TCP/IP za i5/OS Web stranicama . Ova Web stranica pruža najnovije informacije koje nadomještaju i zamjenjuju informacije koje se nalaze u ovom skupu tema.

### Srodne reference

“PDF datoteka za Usluge daljinskog pristupa” na stranici 1

Možete pogledati i ispisati PDF datoteku s ovim informacijama.



---

## Dodatak. Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM možda ne nudi proizvode, usluge ili dodatke o kojima se raspravlja u ovom dokumentu u drugim zemljama. Za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području kontaktirajte vašeg lokalnog IBM predstavnika. Bilo koje upućivanje na neki IBM proizvod, program ili uslugu, nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg proizvoda, programa ili usluge.

IBM može imati patente ili molbe za patente koje su još u toku, a koje pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta ne daje vam nikakvu licencu za korištenje tih patenata. Možete poslati upit za licence, u pismenom obliku, na:

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

Za upite o licenci u vezi s dvobajtnim (DBCS) informacijama, kontaktirajte IBM odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite upite, u pisanom obliku na adresu:

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

**Sljedeći odlomak ne odnosi se na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju u kojoj takvi propisi nisu konzistentni s lokalnim zakonima:** INTERNATIONAL BUSINESS MACHINES CORPORATION OSIGURAVA OVU PUBLIKACIJU "KAKVA JE" BEZ IKAKVIH JAMSTAVA, IZRAVNIH ILI NEIZRAVNIH, UKLJUČUJUĆI, ALI NE OGRANIČENO NA, NEIZRAVNA JAMSTVA O NEKRŠENJU, TRŽIŠNOM POTENCIJALU ILI PRIKLADNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga, se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Povremeno se rade promjene na ovim informacijama; te promjene bit će uključene u nova izdanja ove publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

IBM može koristiti ili distribuirati sve informacije koje vi dobavite, na bilo koji način za koji smatra da je prikladan i bez ikakvih obaveza prema vama.

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N

Rochester, MN 55901  
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program opisan u ovim informacijama i sav licencni materijal koji je za njega dostupan, IBM isporučuje pod uvjetima IBM Ugovora s korisnicima, IBM Internacionalnog ugovora o licenci za programe, IBM Ugovora o licenci za strojni kod ili bilo kojeg ekvivalentnog ugovora između nas.

Podaci o performansama sadržani u ovom dokumentu su utvrđeni u kontroliranom okruženju. Zbog toga se rezultati dobiveni u nekom drugom operativnom okruženju mogu značajno razlikovati. Neka mjerenja su možda napravljena na sistemima razvojne razine i zbog toga nema jamstva da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda procijenjena ekstrapoliranjem. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta bi trebali provjeriti primjenjivost podataka na njihovo specifično okruženje.

Informacije koje se odnose na ne-IBM proizvode su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih javno dostupnih izvora. IBM nije testirao te proizvode i ne može potvrditi koliko su točne tvrdnje o performansama, kompatibilnosti ili druge tvrdnje koje se odnose na ne-IBM proizvode. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Ove informacije sadrže primjere podataka i izvještaja koji se koriste u svakodnevnom poslovnim operacijama. Da bi ih se ilustriralo što je bolje moguće, primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena, a svaka sličnost s imenima i adresama stvarnih poslovnih subjekata u potpunosti je slučajna.

#### AUTORSKO PRAVO LICENCE:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku, koji ilustriraju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati te primjere programa u bilo kojem obliku, bez plaćanja IBM-u, za svrhe razvoja, upotrebe, marketinga ili distribucije aplikacijskih programa, u skladu sa sučeljem programiranja aplikacija za operativnu platformu za koju su primjeri programa napisani. Ti primjeri nisu bili temeljito testirani u svim uvjetima. IBM, zbog toga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcioniranje tih programa.

Svaka kopija ili bilo koji dio tih primjera programa ili iz njih izvedenih radova, mora uključivati sljedeću napomenu o autorskom pravu:

© (ime vašeg poduzeća) (godina). Dijelovi ovog koda su izvedeni iz IBM Corp. primjera programa. © Autorsko pravo IBM Corp. \_unesite godinu ili godine\_. Sva prava pridržana.

Ako gledate nepostojanu kopiju ovih informacija, slike i fotografije u boji se možda neće vidjeti.

---

## Informacije o sučelju programiranja

Ovi dokumenti publikacije Usluge daljinskog pristupa: PPP veze opisuju sučelja programiranja koja omogućuju korisniku da piše programe za IBM i5/OS.

---

## Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, drugim zemljama ili oboje:

AIX  
AS/400  
eServer  
i5/OS



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

Adobe, Adobe logo, PostScript i PostScript logo su registrirani zaštitni znaci ili zaštitni znaci Adobe Systems Incorporated u Sjedinjenim Državama i drugim zemljama.

Linux je registrirani zaštitni znak Linus Torvaldsa u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Ostala imena poduzeća, proizvoda ili usluga mogu biti zaštitni znaci ili oznake usluga drugih.

---

## Termini i uvjeti

Dozvole za upotrebu ovih publikacija se dodjeljuju prema sljedećim terminima i uvjetima.

**Osobna upotreba:** Možete reproducirati ove publikacije za vašu osobnu, nekomercijalnu upotrebu, uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete distribuirati, prikazivati ili raditi izvedena djela iz ovih publikacija ili bilo kojeg njihovog dijela, bez izričite suglasnosti IBM-a.

**Komercijalna upotreba:** Možete reproducirati, distribuirati i prikazivati ove publikacije samo unutar vašeg poduzeća uz uvjet da su sve napomene o vlasništvu sačuvane. Ne smijete raditi izvedena dijela iz ovih publikacija ili kopirati, distribuirati ili prikazivati te publikacije ili bilo koji njihov dio izvan vašeg poduzeća, bez izričite suglasnosti IBM-a.

Osim kako je izričito dodijeljeno u ovoj dozvoli, nisu dane nikakve dozvole, licence ili prava, niti izričita niti posredna, na publikacije ili bilo koje podatke, softver ili bilo koje drugo intelektualno vlasništvo sadržano unutar.

IBM rezervira pravo da bilo kad, po vlastitom nahođenju, povuče ovdje dodijeljene dozvole, ako je upotreba publikacija štetna za njegove interese ili je ustanovljeno od strane IBM-a da gornje upute nisu bile ispravno slijedene.

Ne smijete spustiti, eksportirati ili reeksportirati ove informacije, osim kod potpune usklađenosti sa svim primjenjivim zakonima i propisima, uključujući sve zakone i propise o izvozu Sjedinjenih Država.

IBM NE DAJE NIKAKVA JAMSTVA NA SADRŽAJ OVIH PUBLIKACIJA. PUBLIKACIJE SE DAJU "KAKVE JESU" I BEZ JAMSTAVA BILO KOJE VRSTE, IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, POSREDNA JAMSTVA PROĐE NA TRŽIŠTU, NEKRŠENJA I PRIKLADNOSTI ZA ODREĐENU SVRHU.







Tiskano u Hrvatskoj