Poglavlje 1

Razumevanje i konfigurisanje protokola IP

Poput svakog komunikacionog sistema, računarske mreže se oslanjaju na skup standarda koji omogućavaju slanje, primanje i interpretiranje poruka. Za internet, mreže pod Windowsom i praktično sve ostale računarske mreže, taj temeljni skup standarda je grupa protokola zajednički nazvana Protokol za upravljanje prenosom/Internet protokol (Transmission Control Protocol/Internet Protocol, TCP/IP), u čijoj je osnovi protokol IP.

U ovom poglavlju ćete naučiti osnove protokola IP i kako da Windows Server 2008 konfigurišete za povezivanje sa IP mrežama.

Ciljevi ispita u ovom poglavlju su:

- konfigurisanje IPv4 i IPv6 adresiranja.

Lekcije u ovom poglavlju su:

Pre nego što počnete

Da biste uspešno savladali lekcije u ovom poglavlju, morate imati:

- dve virtuelne mašine ili fizička računara, nazvana Dcsrv1 i Boston, koji su povezani u istu izolovanu mrežu i na kojima je instaliran Windows Server 2008. Na tim računarima ne treba dodavati nijednu serversku ulogu;
- osnovno znanje administriranja Windowsa.

U praksi

J. C. Mackin

Komanda *Ipconfig* je najosnovnija alatka u priboru za rešavanje problema administratora mreže. Ako pomažete korisniku koji ne može da se poveže sa internetom, izvršavanje komande ipconfig u komandnom odzivniku će verovatno biti prvo što ćete uraditi kako biste otkrili da li je računaru dodeljena važeća adresa. Rezultat izvršavanja te komande se nije menjao od Windowsa NT i ako ste radili ili radite kao specijalista za podršku umrežavanju, nikada niste ni pomislili da ćete videti bilo šta neobično nakon unošenja te osnovne komande.

Međutim, Windows Vista i Windows Server 2008 sada pored tradicionalnih informacija o IPv4 daju i informacije o IPv6 u rezultatu izvršavanja komande Ipconfig. To vam možda ne deluje kao veliki problem, ali IPv6 može da bude prilično zastrašujući ako niste ovladali tom verzijom protokola IP, a poslednje što želite je da se nađete u situaciji u kojoj korisnik vidi izraz straha na vašem licu dok pokušavate da otkrijete uzrok problema na njegovom ili njenom računaru.

Možda ćete čak doći u iskušenje da isključite IPv6 kako biste izbegli izlaganje javnosti vašeg neznanja i - ironično - da biste ga sprečili da „usporava mrežu" (što IPv6 nikada ne radi). Istina je da IPv6 danas nije preko potreban, ali uprkos nastojanjima da negiramo njegovo postojanje, nema sumnje da će se u narednim godinama koristiti sve više i više. Jednostavno ga nećemo moći izbeći, jer ne postoji drugo rešenje za problem iscrpljivanja IPv4 adresa, a taj problem neće nestati sam od sebe. IPv6 ne ulazi u vaš svet umrežavanja pod Windowsom zato što vam je potreban, već zato što će vam uskoro zatrebati i stoga bi trebalo da počnete da se navikavate na njega. Dobra vest je da ne morate znati još mnogo toga novog pre nego što ponovo sa potpunim samopouzdanjem pročitate i protumačite rezultate izvršavanja komande Ipconfig. Da biste naučili više o IPv6 i novom rezultatu koji daje komanda Ipconfig, pročitajte lekciju, 3 „Razumevanje adresiranja IP verzije 6 (IPv6)".

Lekcija 1: Razumevanje i konfigurisanje mrežnih veza

Mrežne veze u Windowsu su softverski interfejsi koji koriste TCP/IP i pridružene servise za komunikaciju preko mreže. Ova lekcija će vam pomoći da shvatite koncepte i karakteristike protokola TCP/IP, kako da konfigurišete mrežne veze pod Windows Serverom 2008 i kako da pomoću osnovnih TCP/IP pomoćnih programa pronađete uzroke problema kod mrežnih veza.

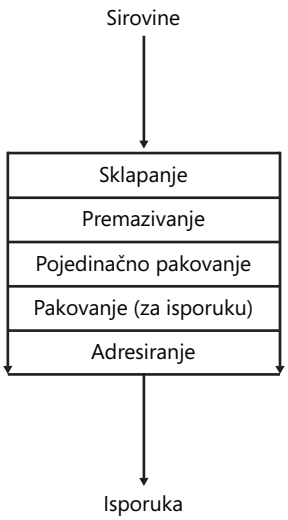
Po završetku ove lekcije, moći ćete da:

- znate šta predstavljaju četiri sloja u paketu protokola TCP/IP;
- pregledate i konfigurišeti IP konfiguraciju lokalne mreže;
- shvatite koncept neusmerenog mrežnog emitovanja;
- pronalazite uzroke problema u mreži pomoću TCP/IP pomoćnih programa.

Procenjeno vreme za lekciju: 100 minuta

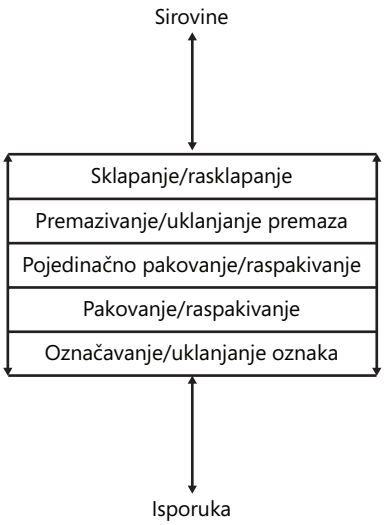
Šta su slojevi mreže?

Slojevi mreže su konceptualni koraci u mrežnoj komunikaciji koje obavljaju *protokoli* (*protocols*), programi zasnovani na standardima. Kao analogni primer iz prakse, uzećemo liniju za montažu. Ako se u nekoj fabrici, primera radi, koristi linija za montažu na kojoj se proizvod sklapa, premazuje, pakuje pojedinačno i grupno i obeležava, tih pet sekvencijalnih funkcija možete smatrati vertikalno naslaganim slojevima u proizvodnom procesu, kao što je prikazano na slici 1-1. Sledeći tu analogiju, protokoli linije za montažu su određene mašine ili procedure koje se koriste za obavljanje funkcija svakog sloja. Iako je svaki protokol projektovan da prihvati određeni ulaz i generiše određeni izlaz, možete zameniti bilo koji protokol u sistemu sve dok on ostaje kompatibilan sa susednim mašinama na liniji za montažu.



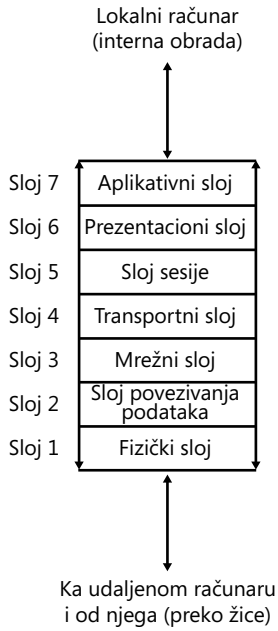
Slika 1-1 Slojevit prikaz proizvodnje na liniji za montažu

Na određen način, mrežna komunikacija zaista podseća na proizvodnju upakovanih proizvoda na liniji za montažu pošto računari međusobno komuniciraju generisanjem i slanjem učaurenih (umotanih) (encapsulated – wrapped) pakovanja koji se nazivaju *paketi* (*packets*). Za razliku od proizvodnje na liniji za montažu, međutim, komunikacija između računara je dvosmerna. To znači da slojevi umrežavanja, razmatrani objedinjeno, opisuju način za stvaranje *i raspakivanje* (*deconstruct*) paketa. Svaki sloj i svaki određeni protokol moraju biti sposobni da svoje funkcije obavljaju u oba smera. U primeru sa linijom za montažu takav dvosmerni model može se prikazati kao na slici 1-2.



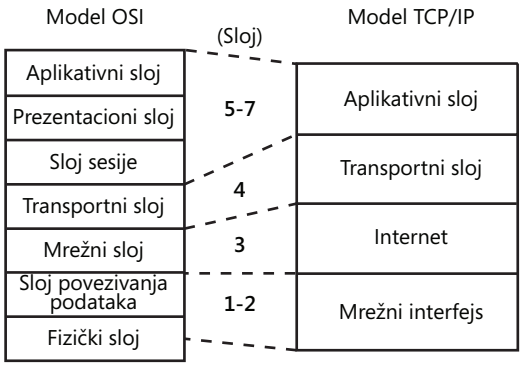
Slika 1-2 Slojevi dvosmerne linije za „montažu-demontažu"

U računarskom umrežavanju, model sa slojevima tradicionalno korišćen za opisivanje komunikacije je sedmoslojni model Open Systems Interconnect (OSI), prikazan na slici 1-3. Možete videti da je svaki od tih sedam slojeva izvorno projektovan da obavi jedan korak u komunikaciji, kao što je predstavljanje ili prenošenje informacija.



Slika 1-3 Model OSI mrežne komunikacije

Iako protokoli koji su originalno činili model OSI nikada nisu bili prihvaćeni u praksi, imena, a posebno brojevi slojeva tog modela, opstali su do današnjih dana. Rezultat: iako je protokol TCP/IP zasnovan na sopstvenom modelu, a ne na modelu OSI, četiri TPC/IP sloja umrežavanja se često definišu u pogledu njihovog odnosa sa modelom OSI (slika 1-4).

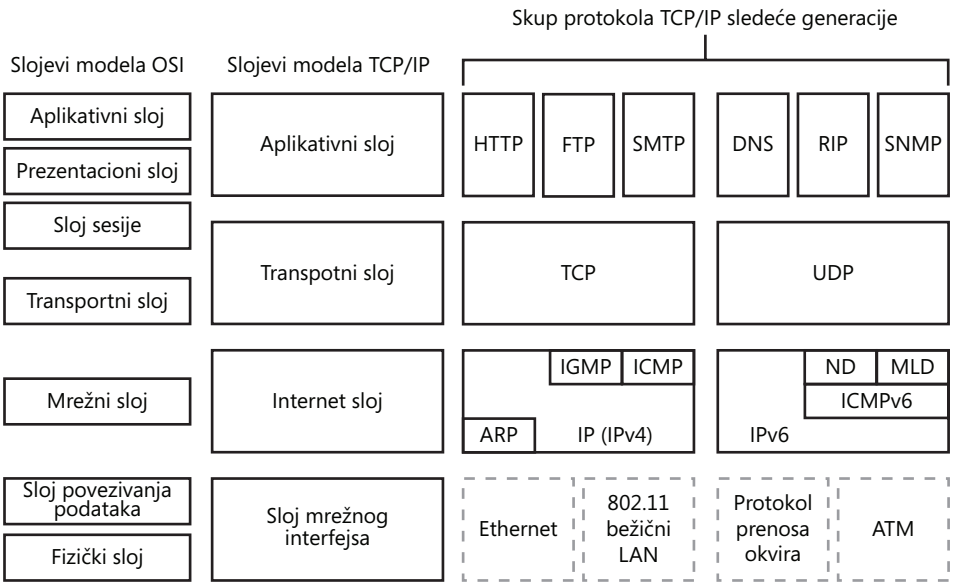


Slika 1-4 TCP/IP slojevi umrežavanja su mapirani sa modelom OSI

Istraživanje slojeva modela TCP/IP umrežavanja

Koncept modela umrežavanja sa slojevima omogućava da se pojedinačni protokoli u bilo kom sloju mogu zameniti sve dok protokoli upotrebljeni kao zamene mogu bez problema da rade sa protokolima iz susednih slojeva. Takva promena se nedavno i dogodila u modelu TCP/IP u mrežama pod Windowsom. Windows Server 2008 i Windows Vista imaju novu implementaciju skupa protokola poznatog kao skup TCP/IP sledeće generacije (Next Generation TCP/IP stack). U skup su dodati novi protokoli, ali se i ta nadograđena verzija TCP/IP zasniva na istom četvoroslojnom modelu.

Na slici 1-5 prikazani su protokoli koji u novim mrežama pod Windowsom rade u četiri sloja modela TCP/IP.



Slika 1-5 Skup TCP/IP protokola sledeće generacije

NAPOMENA Brojevi TCP/IP slojeva

Iako ćete negde videti da su slojevima modela TCP/IP pridruženi njihovi sopstveni brojevi, nezavisni od modela OSI, u ovoj knjizi koristićemo terminologiju označavanja slojeva brojevima koja je mnogo aktuelnija.

Sloj 2

Sloj 2 (Layer 2), koji se naziva i *sloj mrežnog interfejsa* (*Network Interface Layer) ili sloj povezivanja podataka* (*Data Link Layer)*, predstavlja korak u procesu komunikacije koji opisuje specifičan skup standarda za mrežne kartice, hardverske adrese (kao što su MAC adrese) pridružene tim karticama, tipove kabliranja, čvorišta, komutatore, pridružene fizičke standarde i pridružene protokole za razmenjivanje poruka. Funkcija ovog sloja je

da poruke sa jednog uređaja isporuči drugom, a njegovi protokoli omogućavaju komunikaciju između računara koji su razdvojeni samo čvorištima, komutatorima i kablovima. Među standardima definisanim u sloju mrežnog interfejsa su, pored ostalih, Ethernet i Token Ring.

Sloj 3

Sloj 3 (Layer 3), koji se naziva i *sloj* mreže (*Network Layer*) *ili internet sloj* (*Internet Layer*), korak je u komunikacionom procesu tokom koga se softverska adresa izvora i odredišta dodaju paketu i tokom koga se paket usmerava ka odredištu u udaljenoj mreži izvan „dometa" fizičkog signala. Glavni protokol koji funkcioniše u sloju 3 je IP, a uređaj koji radi u ovom sloju je *usmerivač* (*router*). Usmerivači zaustavljaju fizičko rasprostiranje poruka (neusmereno emitovanje) (broadcasts) u mreži, čitaju softversku adresu paketa dodeljenu u sloju 3 i zatim prosleđuju poruku duž odgovarajuće putanje do odredišta.

Glavne promene u Microsoftovoj novoj implementaciji modela TCP/IP obavljene su upravo u sloju 3. Do sada je jedini protokol u ovom sloju bio IPv4. Međutim, u skupu protokola TCP/IP sledeće generacije, sloj 3 zajednički zauzimaju protokoli IPV4 i IPv6.

- **IPv4** IPv4, ili jednostavno IP, je protokol odgovoran za adresiranje i usmeravanje paketa između matičnih računara koji su međusobno udaljeni i desetak mrežnih segmenata. IPv4 se oslanja na 32-bitne adrese i zbog tog relativno malog adresnog prostora, adrese se velikom brzinom iscrpljuju u IPv4 mrežama.
- **IPv6** IPv6 koristi 128-bitne adrese umesto 32-bitnih u protokolu IPv4 i zbog toga je moguće definisati mnogo više adresa. Pošto je malo IPv6 kompatibilnih internet usmerivača, IPv6 se danas koristi na internetu uz pomoć protokola za tunelovanje. Međutim, Ipv6 je izvorno podržan u lokalnim računarskim mrežama pod Windows Vistom i Windows Serverom 2008.

Protokoli Ipv4 i IPv6 su podrazumevano uključeni. Kao rezultat te dvojne IP arhitekture, računari mogu da koriste IPv6 za komunikaciju ako ga podržavaju klijent, server i mrežna infrastruktura, ali i za komunikaciju sa računarima ili mrežnim servisima koji podržavaju samo IPv4.

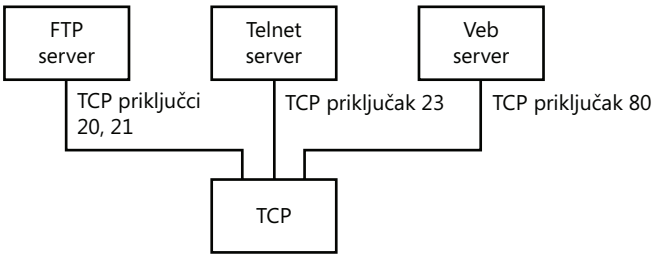
Sloj 4

Sloj 4 ili *transportni sloj* modela TCP/IP predstavlja korak u komunikacionom procesu tokom kojeg se određuju uslovi slanja i primanja podataka. Sloj 4 služi i za označavanje podataka namenjenih opštoj aplikaciji, kao što je e-pošta ili veb.

TCP i UDP su dva protokola transportnog sloja u skupu TCP/IP.

- **TCP** TCP prima podatke od aplikativnog sloja i obrađuje ih kao nizove bajtova. Ti se bajtovi grupišu u segmente koje TCP zatim označava brojevima i priprema za isporuku mrežnom matičnom računaru. TCP potvrđuje prijem podataka i uređuje da podaci budu ponovo poslati ukoliko potvrda nije primljena.

  Kada TCP primi niz podataka od matičnog računara, on ih šalje aplikaciji određenoj brojem TCP priključka . TCP priključci omogućavaju različitim aplikacijama i programima da na jednom matičnom računaru koriste TCP servise (slika 1-6). Svaki program koji koristi TCP priključak osluškuje poruke koje pristižu na njemu pridruženom broju priključka. Podatke poslate određenom TCP priključku na taj način prima aplikacija koja osluškuje taj priključak.



Slika 1-6 TCP priključci

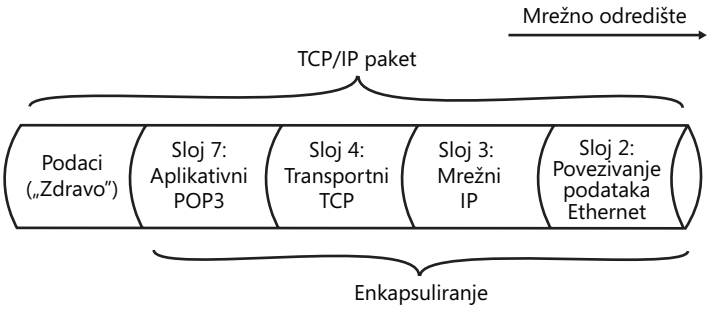
- **UDP** Mnogi mrežni servisi (kao što je DNS) umesto na TCP kao transportni protokol oslanjaju se na UDP. UDP omogućava brz transport datagrama eliminisanjem funkcija pouzdanosti protokola TCP, kao što su garantovana isporuka i verifikacija niza. Za razliku od protokola TCP, UDP je servis *bez direktnog povezivanja* (*connectionless*), koji obezbeđuje samo isporuku „po najvećem trudu" mrežnim matičnim računarima. Izvorni matični računar, kome je neophodna pouzdana komunikacija, mora da koristi ili TCP ili program koji obezbeđuje sopstvene servise raspoređivanja u nizove i potvrđivanja prijema.

Sloj 7

Sloj 7 ili *aplikativni sloj* (Application Layer) modela TCP/IP korak je u komunikacionom procesu tokom kojeg se podaci krajnjeg korisnika obrađuju, pakuju i šalju do priključaka transportnog sloja i od njih. Protokoli aplikativnog sloja često opisuju za korisnike prikladnu metodu predstavljanja, imenovanja, slanja ili primanja podataka preko protokola TCP/IP. Najpoznatiji primeri protokola aplikativnog sloja skupa TCP/IP su HTTP, Telnet, FTP, Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), DNS, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) i Network News Transfer Protocol (NNTP).

TCP/IP enkapsuliranje

Enkapsuliranjem podataka svakim od četiri prethodno opisana sloja, TCP/IP stvara paket pojednostavljeno prikazan na slici 1-7. Na njoj se vidi poruka e-pošte „Zdravo" enkapsulirana zaglavljima POP3 e-pošte (sloj 7), TCP (sloj 4), IP (sloj 3) i Ethernet (sloj 2).



Slika 1-7 Primer TCP/IP paketa

NAPOMENA Broj protokola u svakom paketu je promenljiv

Paket prikazan na slici 1-7 je pojednostavljen pošto se podaci enkapsulirani sa tačno četiri protokola ne nalaze u svakom paketu. Mnogi paketi, primera radi, treba da obezbede komunikaciju sa jednog kraja na drugi samo za donje slojeve, kao što je TCP, i samim tim sadrže manji broj protokola. Ostali paketi mogu da imaju više od četiri protokola ako na određenom sloju obuhvataju više od jednog protokola. Na primer, ICMP, IP i ARP mogu se u sloju 3 koristiti u okviru jednog paketa.

Brza provera

1. U kom sloju umrežavanja se nalazi Ethernet?
2. Šta usmerivači podrazumevano čine sa neusmerenim emitovanjem poruka u mreži?

Odgovori

1. U sloju 2.
2. Usmerivači podrazumevano blokiraju neusmereno emitovanje.

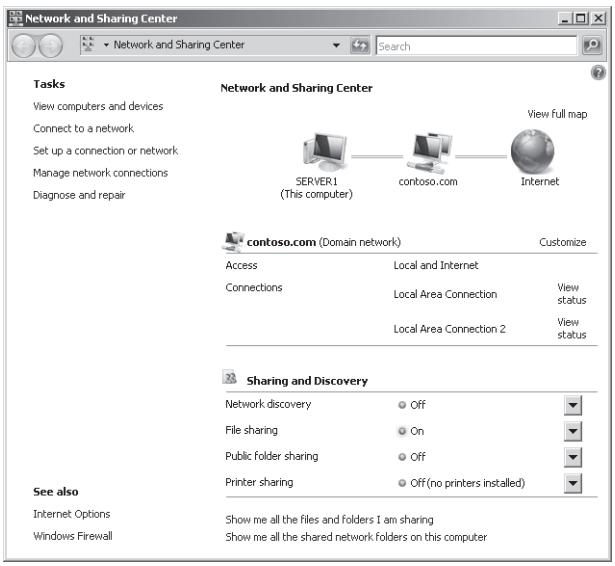
Konfigurisanje svojstava umrežavanja za klijenta pod Windows Vistom ili Windows Serverom 2008

Windows Server 2008 ima dve glavne oblasti u kojima se konfigurišu svojstva umrežavanja klijenta. To su Network and Sharing Center i Network Connections. U narednom odeljku opisaćemo te oblasti u okviru interfejsa Windows Servera 2008 i parametre koje u njima možete konfigurisati.

Network and Sharing Center

Network and Sharing Center je glavna alatka za konfigurisanje svojstava umrežavanja u Windows Serveru 2008. Da biste otvorili Network and Sharing Center, otvorite meni Start, desnim tasterom miša pritisnite Network i izaberite Properties. Alternativno, u delu Notification desnim tasterom miša pritisnite ikonicu mreže i zatim iz menija sa prečicama izaberite Network and Sharing Center. Treći način da otvorite Network and Sharing Center je iz kontrolnog panela izborom Control Panel\Network and Internet\Network and Sharing Center.

Network and Sharing Center prikazan je na slici 1-8.



Slika 1-8 Network and Sharing Center

Network and Sharing Center možete upotrebiti da biste obavili funkcije kao što su podešavanje mrežne lokacije, pregledanje mape mreže, konfigurisanje parametra Network Discovery,

konfigurisanje deljenja datoteka i štampača i pregledanje statusa mrežnih veza. Ta različita svojstva opisana su u sledećoj listi.

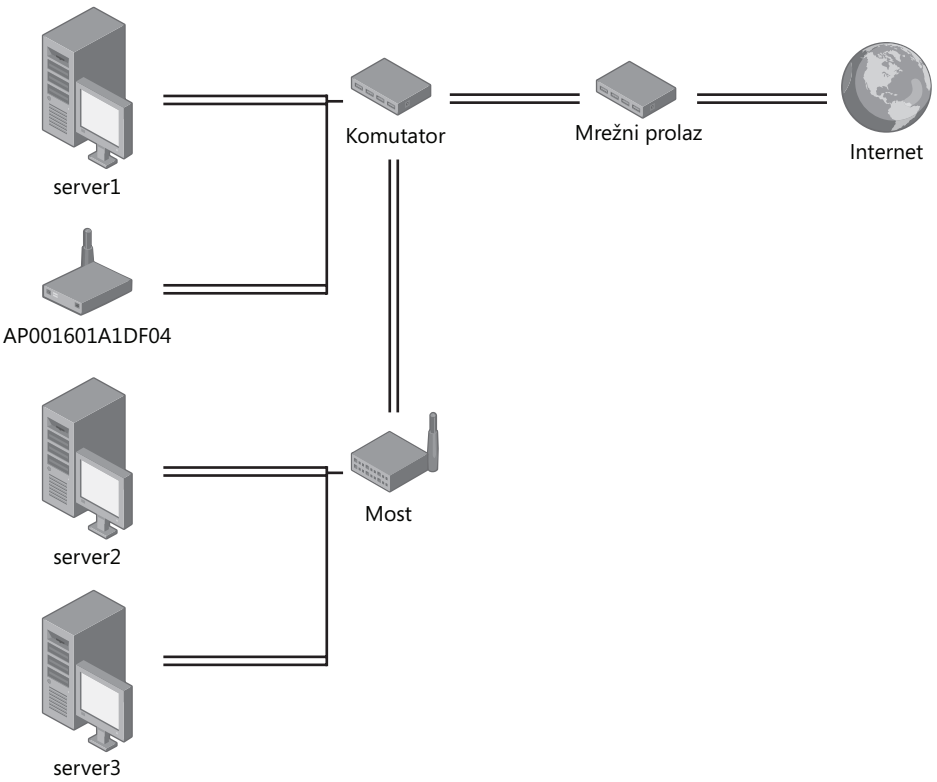
- **Network Location** Mrežna lokacija (network location) je parametar podešen za sve računare koji rade pod Windows Vistom i Windows Serverom 2008. Svim klijentima pod tim operativnim sistemima dodeljuje se jedna od tri mrežne lokacije: Public, Private i Domain. Na osnovu mrežne lokacije kojoj je dodeljena neka mašina, automatski se uključuju ili isključuju različita mrežna svojstva. Na primer, Network Map je podrazumevano uključen na nekim lokacijama, odnosno isključen na ostalim.

  Podrazumevano se svi klijenti dodeljuju lokaciji Public (javno). Za računar u javnoj mreži, Windows Firewall je uključen, a isključeni su Network Discovery, deljenje datoteka i štampača i Network Map.

  Kada računar dodelite mrežnoj lokaciji Private (privatno), Network Discovery i Network Map su uključeni. Deljenje datoteka je podrazumevano isključeno, ali za razliku od tipa lokacije Public, možete uključiti deljenje datoteka na jednom računaru dodeljenom privatnoj mreži ne menjajući podrazumevane parametre za sve računare koji su pridruženi privatnoj mreži.

  Kada se računar koji radi pod Windows Vistom pridruži domenu servisa direktorijuma Active Directory (aktivni direktorijum), on automatski konfiguriše postojeću mrežu za tip mrežne lokacije Domain. Taj tip mrežne lokacije sličan je mrežnoj lokaciji Private, sa tom razlikom što se kod mrežne lokacije Domain konfiguracija za Windows Firewall, Network Discovery i Network Map mogu odrediti parametrima grupne politike (Group Policy).

- **Network Map** Mapa mreže (Network Map) omogućava da vidite uređaje u lokalnoj računarskoj mreži i način na koji su povezani međusobno i sa internetom. Primer mape mreže prikazan je na slici 1-9.



Slika 1-9 Mapa mreže

Mapa mreže se oslanja na dve komponente:

- ❏ komponenta Link Layer Topology Discovery (LLTD) Mapper šalje mreži upite za uređaje koje treba uvrstiti u mapu;
- ❏ komponenta LLTD Responder odgovara na upite Mapper I/O.

Iako se te komponente nalaze samo u Windows Visti i Windows Serveru 2008, komponentu Responder možete instalirati i na računare pod Windowsom XP kako bi se oni pojavili u mrežnoj mapi na drugim računarima.

Ispitna napomena Ne zaboravite: da bi se računar koji radi pod Windowsom XP pojavio u mrežnoj mapi, morate na njemu instalirati komponentu LLTD Responder.

Mapa mreže u profilu Domain

Svojstvo Network Map je podrazumevano isključeno kada izaberete profil Domain. Međutim, možete ga uključiti preko grupne politike (Group Policy).

- **File Sharing** Kada je ova opcija uključena, Windows Firewall omogućava standardnim korisnicima da izaberu hoće li ili neće dozvoliti deljenje datoteka ili omotnica u svojim profilima – drugim rečima, datoteka i omotnica u delu %systemroot%\Users\%username%. Administratori mogu da dele sve datoteke i omotnice na računaru.

VAŽNO Deljenje datoteka uključuje komandu ping

Omogućavanje deljenja datoteka takođe kreira izuzetke mrežne barijere za Internet Control Message Protocol (ICMP), protokol korišćen u pomoćnim programima Ping, Pathping i Tracert. Shodno tome, ako ne dozvolite deljenje datoteka, lokalni računar podrazumevano neće odgovarati na komandu ping. Zapamtite to kako za potrebe ispita 70-642, tako i za administriranje sistema u stvarnom svetu!

- **Public Folder Sharing** Uključivanjem ove opcije automatski se deli omotnica koja se nalazi u %systemroot%\Users\Public. Dozvoljavanje deljenja javne omotnice automatski uključuje i deljenje datoteka.
- **Printer Sharing** Uključivanjem ovog svojstva dele se štampači instalirani na lokalnom računaru i omogućava njihovo korišćenje sa drugih računara u mreži. Izborom opcije Printer Sharing automatski se uključuje deljenje datoteka.
- **Password Protected Sharing** Ova opcija je dostupna samo na računarima koji nisu pridruženi domenu. Uključivanjem ove opcije dozvoljava se pristup deljenim resursima samo korisnicima koji imaju važeće naloge na lokalnom računaru.

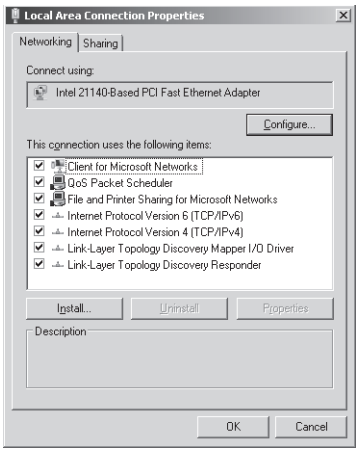
Pregledanje mrežnih veza

Windows Server 2008 automatski otkriva i konfiguriše veze pridružene mrežnim karticama instaliranim na lokalnom računaru. Te veze se zatim prikazuju u delu Network Connections, zajedno sa svim dodatnim vezama, kao što su komutirane veze, koje ste ručno dodali izborom opcije Set Up A Connection Or Network u programu Network and Sharing Center.

Mrežne veze možete otvoriti na više načina. Prvi je da u Server Manageru izaberete čvor *Server Manager* i zatim pritisnete View Network Connections. U prozoru Initial Configuration Tasks možete pritisnuti Configure Networking. U programu Network and Sharing Center možete pritisnuti Manage Network Connections. Na kraju, mrežne veze ćete otvoriti i iz komandne linije, polja Start Search ili polja Run izvršavanjem komande **ncpa.cpl** ili **control netconnections**.

Pregledanje podrazumevanih komponenata mrežnih veza Veze same po sebi ne dozvoljavaju mrežnim matičnim računarima da međusobno komuniciraju. Povezivanje preko određene veze zapravo obezbeđuju mrežni klijenti, servisi i protokoli *u granicama* te veze. Na tabulatoru General okvira za dijalog sa svojstvima veze prikazani su klijenti, servisi i protokoli „privezani” za tu vezu.

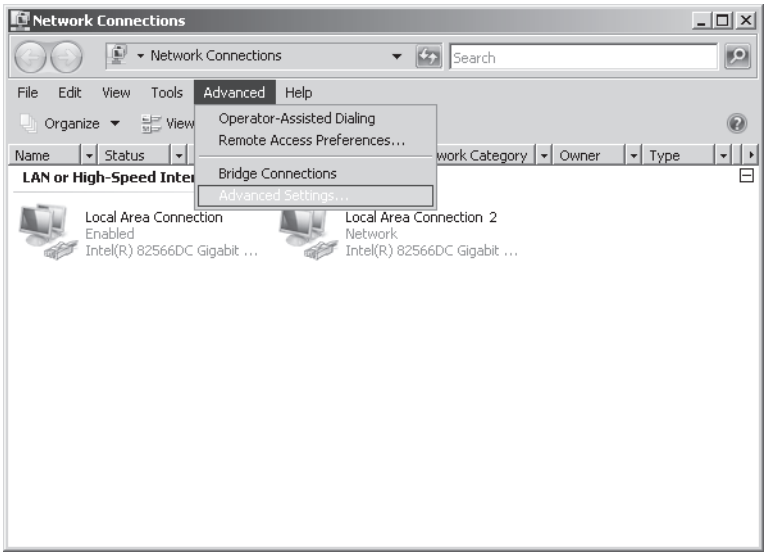
Na slici 1-10 prikazane su podrazumevane komponente instalirane u lokalnoj računarskoj mreži pod Windows Serverom 2008. Polje za potvrdu pored svake komponente ukazuje na to da je komponenta pridružena vezi.



Slika 1-10 Podrazumevane komponente veze

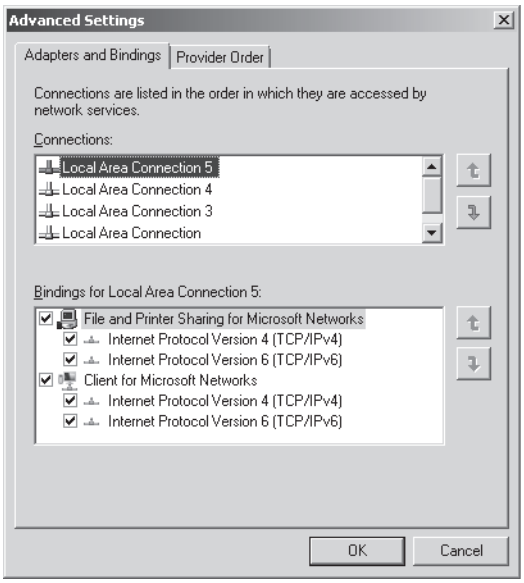
- **Mrežni klijenti** U Windowsu su *mrežni klijenti* (*network clients*) *softverske komponente, kao što je* Client For Microsoft Networks, koje omogućavaju lokalnom računaru povezivanje sa određenim mrežnim operativnim sistemom. Podrazumevano je Client For Microsoft Networks jedini mrežni klijent povezan sa svim lokalnim računarskim mrežama. Client For Microsoft Networks omogućava klijentskim računarima pod Windowsom da se povežu sa deljenim resursima na drugim računarima pod Windowsom.
- **Mrežni servisi** Mrežni servisi (network services) su softverske komponente koje obezbeđuju dodatna svojstva mrežnim vezama. File And Printer Sharing For Microsoft Networks i QoS Packet Scheduler su dva mrežna servisa podrazumevano pridružena svim lokalnim mrežnim vezama. File And Printer Sharing For Microsoft Networks omogućava lokalnom računaru deljenje omotnica za pristup sa mreže, dok QoS Packet Scheduler obezbeđuje kontrolu mrežnog saobraćaja, uključujući servise upravljanja brzinom (rate-of-flow) i davanja prvenstva (prioritization).
- **Mrežni protokoli** Računari mogu da komuniciraju preko neke veze samo korišćenjem mrežnih protokola koji su pridruženi toj vezi. Podrazumevano su za svaku mrežnu vezu instalirana i pridružena četiri mrežna protokola: IPv4, IPv6, Link-Layer Topology Discovery (LLTD) Mapper i LLTD Responder.

Pregledanje naprednih parametara veze Da biste videli napredne parametre veze, otvorite prozor Network Connections i iz menija Advanced izaberite Advanced Settings (slika 1-11).



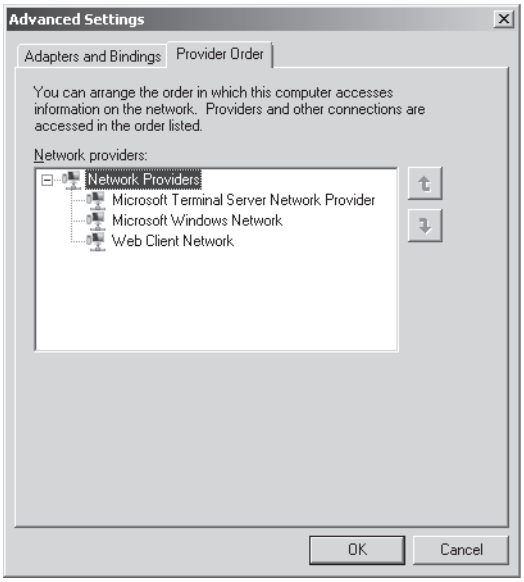
Slika 1-11 Otvaranje okvira za dijalog Advanced Settings iz prozora Network Connections

Okvir za dijalog Advanced Settings (slika 1-12) prikazuje redosled (prioritet) svake veze. Podešavanjem redosleda veza možete konfigurisati računar da pokuša ostvarivanje mrežne komunikacije preko različitih dostupnih veza, i to redosledom koji vi definišete. Takođe možete podešavati redosled povezivanja (binding order) servisa koji se koriste za svaku vezu.



Slika 1-12 Okvir za dijalog Advanced Settings

Tabulator Provider Order Na tabulatoru Provider Order okvira za dijalog Advanced Settings (slika 1-13) prikazuje se redosled kojim će veza pokušati da komunicira sa drugim računarima korišćenjem različitih mrežnih posrednika, kao što su Microsoft Windows Network ili Microsoft Terminal Services. Imajte na umu da se redosled mrežnih posrednika, naveden u ovom okviru za dijalog, primenjuje na sve mrežne veze.



Slika 1-13 Tabulator Provider Order

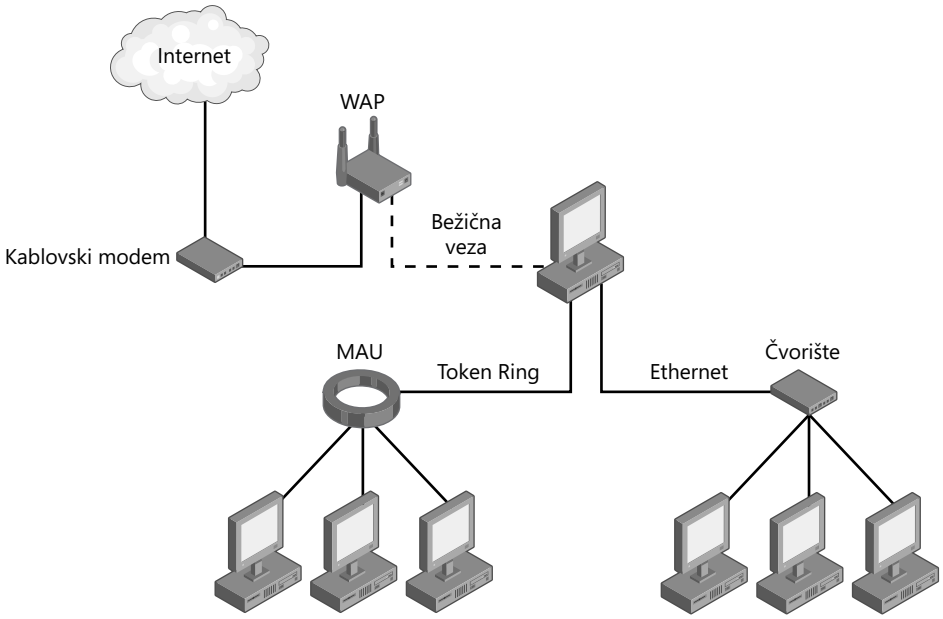
Premošćavanje mrežnih veza

U nekim slučajevima ćete hteti da kombinujete više mrežnih veza na određenom računaru da bi Windows te veze tretirao kao da su u istoj mreži (u jednom domenu neusmerenog emitovanja). Na primer, možda ćete hteti da delite jednu bežičnu pristupnu tačku (wireless access point, WAP) sa više različitih topologija veze, kao što je prikazano na slici 1-14.

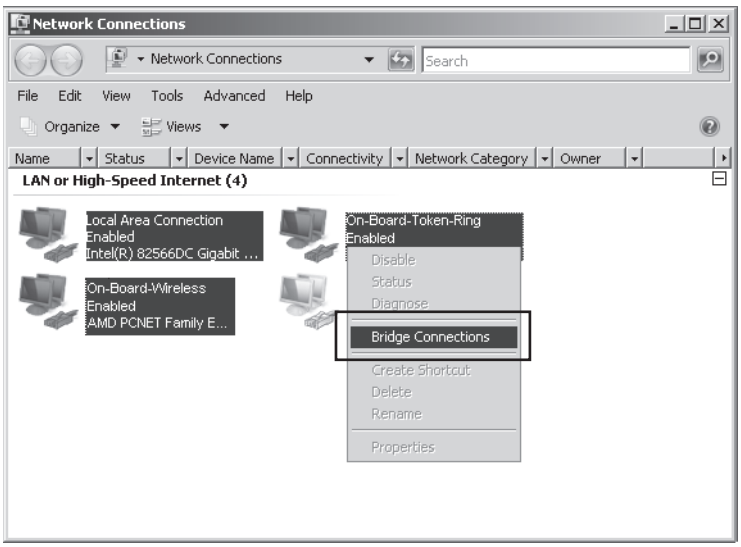
U tom primeru, veza sa internetom je pridružena jednoj bežičnoj pristupnoj tački (WAP). WAP zatim komunicira sa karticom za bežično umrežavanje u serveru. Pored toga, server ima Ethernet vezu i Token Ring vezu priključenu drugim mrežama.

Kada na toj vezi uključite *mrežno premošćavanje*, sve tačke koje ulaze u server (bežična veza, Token Ring i Ethernet) pojavljuju se u istoj mreži. Posledično, sve mogu da dele bežičnu vezu i izađu na internet.

Da biste premostili mreže, pritisnite taster Ctrl dok na serveru birate više mrežnih veza. Zatim pritisnite desnim tasterom miša i izaberite Bridge Networks (slika 1-15).



Slika 1-14 Primer mreže koja može da iskoristi prednosti mrežnog premošćavanja



Slika 1-15 Biranje više mreža uz njihovo premošćavanje pritiskom na desni taster miša

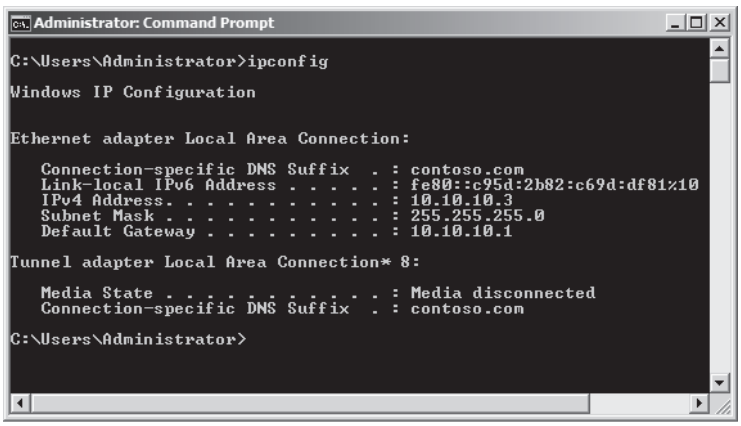
Kada konfigurišete mrežno premošćavanje, vi zapravo dozvoljavate saobraćaju sa bežične, Ethernet i Token Ring kartice mrežnog interfejsa da dele isti mrežni prostor. Stoga, jedna bežična kartica mrežnog interfejsa može da bude izlazni mrežni prolaz do različitih mreža.

Pregledanje adresne konfiguracije

IP konfiguracija veze sastoji se najmanje od jedne IPv4 adrese i maske podmreže, ili jedne IPv6 adrese i prefiksa podmreže. Pored tih minimalnih parametara, IP konfiguracija može da sadrži i informacije kao što su podrazumevani mrežni prolaz, adrese DNS servera, sufiks DNS imena i adrese WINS servera.

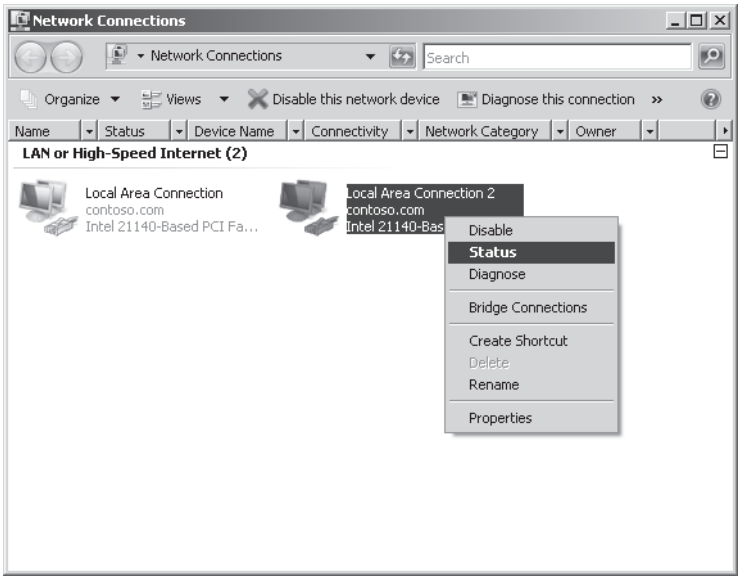
Da biste za datu vezu videli konfiguraciju IP adrese, možete upotrebiti komandu *Ipconfig* ili okvir za dijalog Network Connection Details.

Da biste upotrebili *Ipconfig*, unesite u komandnom odzivniku **ipconfig**. Dobićete rezultat sličan onome prikazanom na slici 1-16.



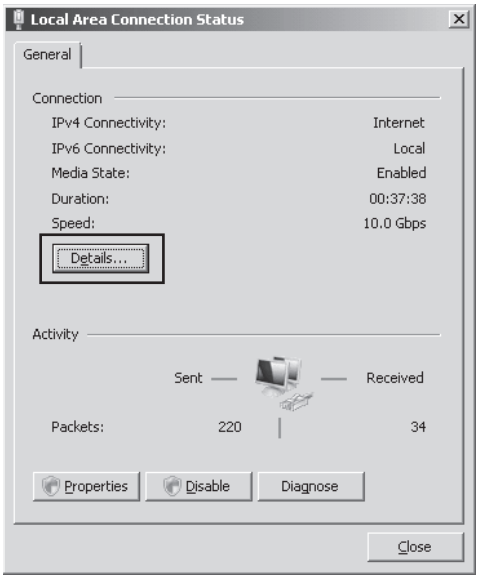
Slika 1-16 Pregledanje IP adrese

Okvir za dijalog Network Connection Details otvoraćete ako desnim tasterom miša pritisnete vezu u prozoru Network Connections i zatim iz menija sa prečicama izaberete Status (slika 1-17).



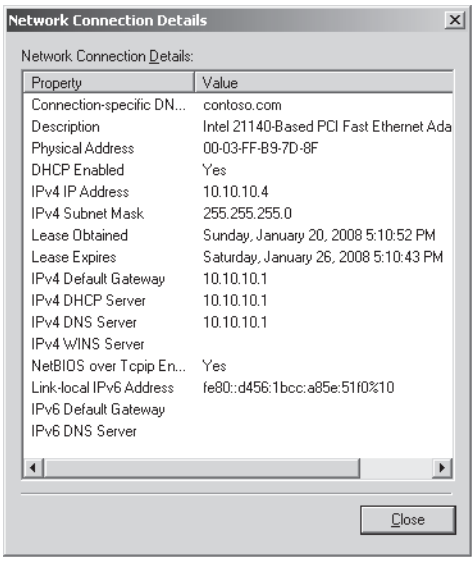
Slika 1-17 Otvaranje okvira za dijalog Local Area Connection Status

Nakon toga, u okviru za dijalog Local Area Connection Status pritisnite dugme Details (slika 1-18).



Slika 1-18 Okvir za dijalog Local Area Connection Status

Tako ćete otvoriti okvir za dijalog Network Connection Details, prikazan na slici 1-19.



Slika 1-19 Okvir za dijalog Network Connection Details

Ručno dodeljivanje IP konfiguracije

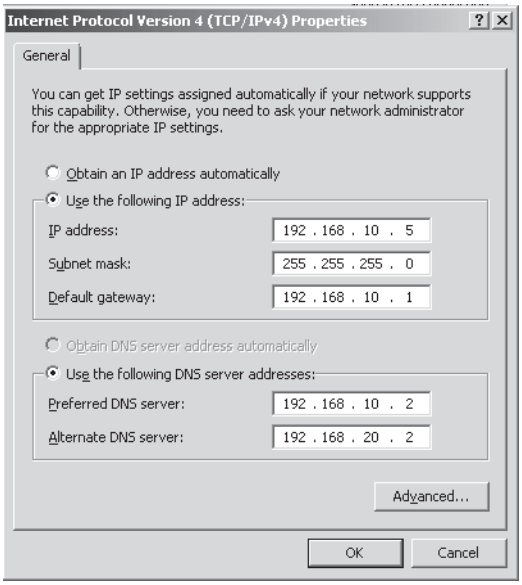
Mrežnoj vezi se IP konfiguracija može dodeliti ručno ili automatski. U narednom odeljku objasnićemo vam kako da IPv4 i IPv6 konfiguraciju dodelite ručno.

Ručno dodeljivanje IPv4 konfiguracije

Ručno konfigurisana adresa je poznata kao statička adresa pošto jedna takva adresa ostaje stalna čak i nakon ponovnog pokretanja računara. Statičke adrese su odgovarajuće za kritične infrastrukturne servere kao što su kontroleri domena, DNS serveri, DHCP serveri, WINS serveri i usmerivači.

Statičku adresu i druge parametre IPv4 konfiguracije možete dodeliti ručno mrežnoj vezi korišćenjem okvira za dijalog Internet Protocol Version 4 (TCP/IP) Properties. Da biste pristupili tom okviru za dijalog, otvorite svojstva mrežne veze kojoj želite da dodelite IPv4 konfiguraciju. U okviru za dijalog sa svojstvima veze, dva puta pritisnite u listi komponenata odrednicu Internet Protocol Version 4 (TCP/IPv4).

Okvir za dijalog Internet Protocol Version 4 (TCP/IPv4) Properties prikazan je na slici 1-20.

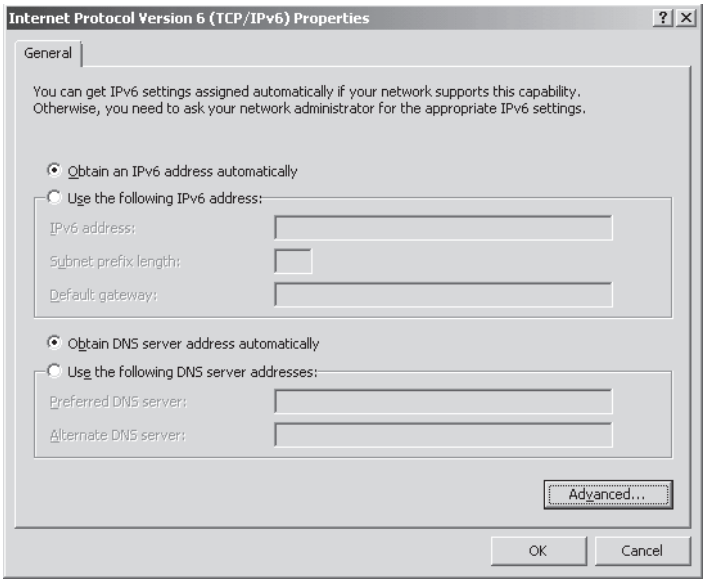


Slika 1-20 Ručno dodeljivanje IPv4 konfiguracije za mrežnu vezu

Mrežne veze su podrazumevano konfigurisane da IP adresu i adresu DNS servera dobijaju automatski. Da biste, zbog toga, konfigurisali statičku IP adresu, morate upotrebiti opciju Use The Following IP Address i zatim navesti IP adresu, masku podmreže i (opcionalno) podrazumevani mrežni prolaz. Da biste vezi dodelili statičku adresu DNS servera, izaberite opciju Use The Following DNS Server Addresses i zatim navedite adresu prioritetnog i (opcionalno) alternativnog DNS servera.

Ručno dodeljivanje IPv6 konfiguracije U većini slučajeva ne morate ručno da konfigurišete IPv6 adresu pošto se statičke IPv6 adrese, po pravilu, dodeljuju samo usmerivačima, a ne i matičnim računarima. Tipično se IPv6 konfiguracija dodeljuje matičnom računaru autokonfigurisanjem.

Ipak, IPv6 adresu možete dodeliti ručno korišćenjem okvira za dijalog Internet Protocol Version 6 (TCP/IPv6) Properties. Da biste ga otvorili, dva puta pritisnite Internet Protocol Version 6 (TCP/IPv6) u okviru za dijalog sa svojstvima veze. Okvir za dijalog Internet Protocol Version 6 (TCP/IPv6) prikazan je na slici 1-21.



Slika 1-21 Okvir za dijalog Internet Protocol Version 6 (TCP/IPv6)

Kao i kod IPv4, mrežne veze su konfigurisane da IPv6 adresu i adresu DNS servera dobijaju automatski. Da biste konfigurisali statičku IPv6 adresu, izaberite opciju Use The Following IPv6 Address i navedite IPv6 adresu, dužinu prefiksa podmreže (tipično 64) i (opcionalno) podrazumevani mrežni prolaz. Imajte na umu da, ako konfigurišete statičku IPv6 adresu, morate navesti i statičku IPv6 adresu DNS servera.

Ručno konfigurisanje IPv4 i IPv6 parametara iz komandnog odzivnika Za dodeljivanje IP konfiguracije iz komandnog odzivnika možete upotrebiti pomoćni program Netsh.

Da biste vezi iz komandnog odzivnika dodelili statičku IPv4 adresu i masku podmreže, unesite sledeću komandu, u kojoj je *Connection_Name* ime veze (recimo, Local Area Connection), *Address* IPv4 adresa, a *Subnet_Mask* maska podmreže.

```
netsh interface ip set address "Connection_Name" static Address Subnet_Mask
```

Na primer, da biste za Local Area Connection podesili IPv4 adresu 192.168.33.5 sa maskom podmreže 255.255.255.0, treba da unesete sledeću komandu:

```
netsh interface ip set address "local area connection" static 192.168.33.5
255.255.255.0
```

Ako pored IPv4 konfiguracije želite da definišete i podrazumevani mrežni prolaz, tu informaciju možete dodati na kraj komande. Na primer, da biste konfigurisali istu IPv4 adresu za lokalnu mrežu sa podrazumevanim mrežnim prolazom čija je adresa 192.168.33.1, unesite sledeće:

```
netsh interface ip set address "local area connection" static 192.168.33.5
255.255.255.0 192.168.33.1
```

NAPOMENA Alternativna sintaksa komande Netsh

Postoji mnogo prihvatljivih varijacija sintakse komande Netsh. Primera radi, umesto netsh interface ip, možete uneti netsh interface ipv4. Više informacija ćete saznati u sistemu pomoći, do koga dolazite unošenjem komande Netsh Help (ili Netsh ?) u komandnom odzivniku.

Da biste vezi dodelili statičku IPv6 adresu iz komandnog odzivnika, unesite sledeću komandu, u kojoj je *Connection_Name* ime veze (recimo, Local Area Connection) a *Address* IPv6 adresa.

```
netsh interface ipv6 set address "Connection_Name" Address
```

Na primer, da biste adresu 2001:db8:290c:1291::1 dodelili vezi Local Area Connection (ostavljajući neizmenjen podrazumevani prefiks podmreže dužine 64), unesite sledeće:

```
netsh interface ipv6 set address "Local Area Connection" 2001:db8:290c:1291::1
```

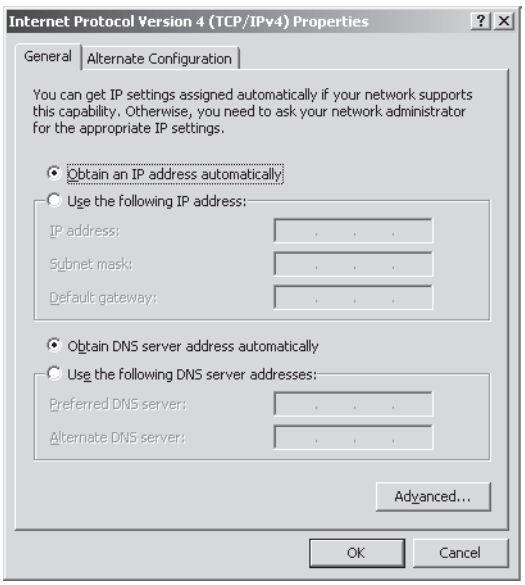
Pomoćni program Netsh ima mnoge druge opcije za konfigurisanje IPv4 i IPv6. O tim opcijama i sintaksi komande saznaćete više u sistemu pomoći, do koga dolazite unošenjem komande Netsh Help (ili Netsh ?) u komandnom odzivniku.

Konfigurisanje IPv4 veze za automatsko dobijanje adrese

Sve veze su podrazumevano konfigurisane, tako da IPv4 adresu dobijaju automatski. Kada je tako konfigurisan, računar sa tim tipom veze poznat je kao DHCP klijent.

Kao rezultat takvog podešavanja, sve mrežne veze će dobiti IPv4 adresu od DHCP servera, pod uslovom da je dostupan. Ukoliko nijedan DHCP server nije dostupan, veza će automatski sama sebi dodeliti alternativnu konfiguraciju koju ste za nju definisali. U slučaju da niste definisali alternativnu konfiguraciju, veza će automatski sama sebi dodeliti automatsku adresu APIPA (Automatic Private IP Addressing) za IPv4.

Da biste vezu konfigurisali tako da IPv4 adresu dobija automatski, izaberite odgovarajuću opciju u okviru za dijalog Internet Protocol Version 4 (TCP/IPv4) Properties, kao što je prikazano na slici 1-22.



Slika 1-22 Konfigurisanje veze za automatsko dobijanje IPv4 adrese (podrazumevano podešavanje)

Da biste konfigurisali klijenta da automatski dobija IPv4 adresu, možete upotrebiti i pomoćni program Netsh. U komandnom odzivniku unesite sledeću komandu, gde je *Connection_Name* ime mrežne veze:

```
netsh interface ip set address "Connection_Name" dhcp
```

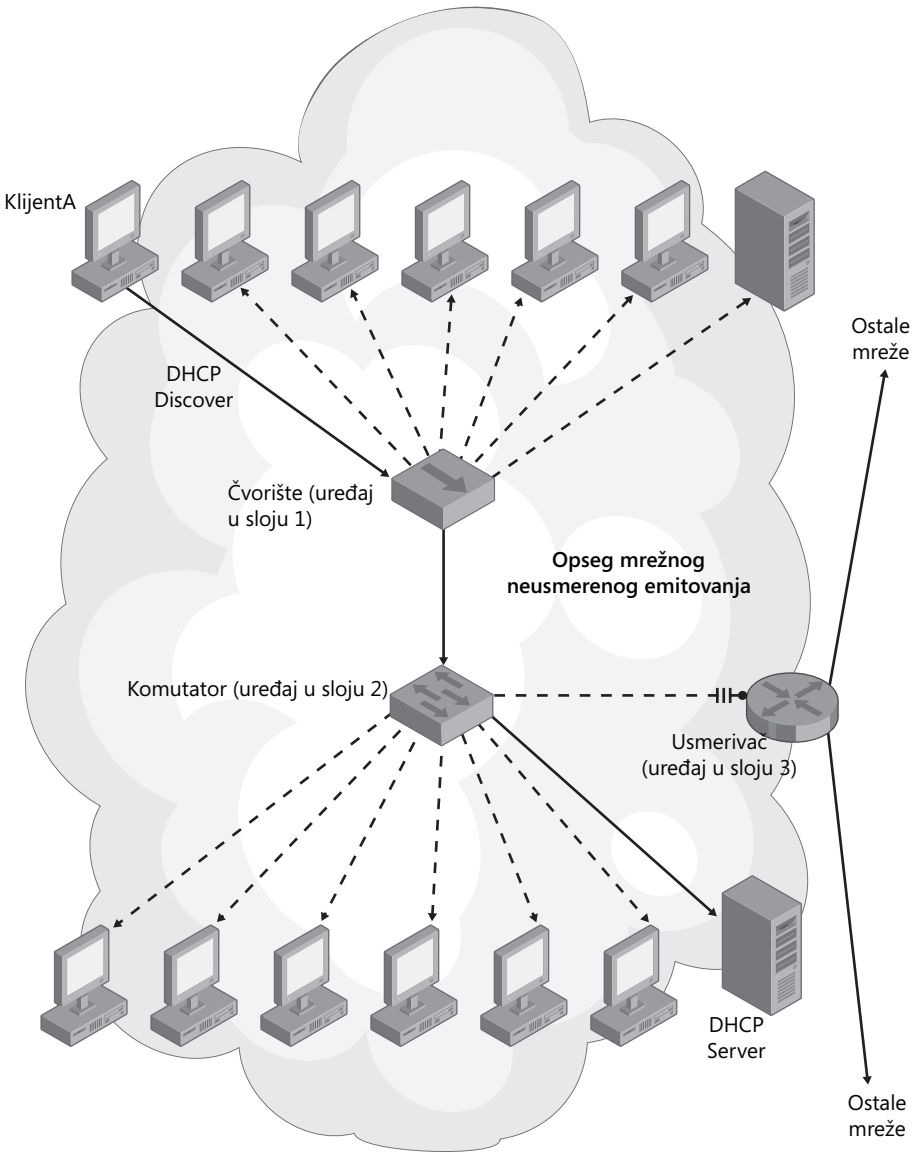
Na primer, da bi veza Local Area Connection automatski dobijala adresu, unesite sledeću komandu:

```
netsh interface ip set address "Local Area Connection" dhcp
```

Adrese koje dodeljuje DHCP Adrese koje dodeljuje DHCP uvek imaju prioritet nad metodama automatskog IPv4 konfigurisanja. Matični računar u IP mreži može da dobije IP adresu od DHCP servera kada se DHCP server (ili DHCP Relay Agent) nalazi u opsegu neusmerenog emitovanja.

Mrežno neusmereno emitovanje (network broadcast) je prenošenje poruka upućenih svim lokalnim adresama. Takvo emitovanje se prenosi kroz sve uređaje u sloju 1 i sloju 2 (kao što su kablovi, repetitori, čvorišta, mostovi i komutatori), ali ga blokiraju uređaji u sloju 3 (usmerivači). Za računare koji međusobno mogu da komuniciraju pomoću neusmerenog emitovanja kaže se da se nalaze u istom domenu neusmerenog emitovanja.

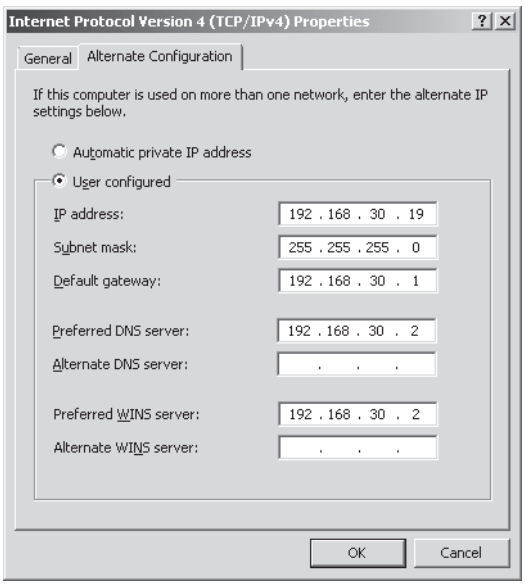
Mrežno neusmereno emitovanje predstavljeno je na slici 1-23.



Slika 1-23 KlijentA može da dobije IP adresu od DHCP servera, jer se ta dva računara nalaze u istom domenu neusmerenog emitovanja. Obratite pažnju na to da je granica neusmerenog emitovanja usmerivač u sloju 3

Definisanje alternativne konfiguracije Ukoliko u opsegu neusmerenog emitovanja klijenta nema dostupnog DHCP servera, klijent koji je konfigurisan da automatski dobija adresu podrazumevano će koristiti alternativnu konfiguraciju, pod uslovom da ste je definisali.

Alternativnu konfiguraciju možete dodeliti vezi na tabulatoru Alternate Configuration okvira za dijalog Internet Protocol Version 4 (TCP/IPv4) Properties (slika 1-24). U alternativnoj konfiguraciji možete navesti IP adresu, masku podmreže, podrazumevani mrežni prolaz, DNS server i WINS server.



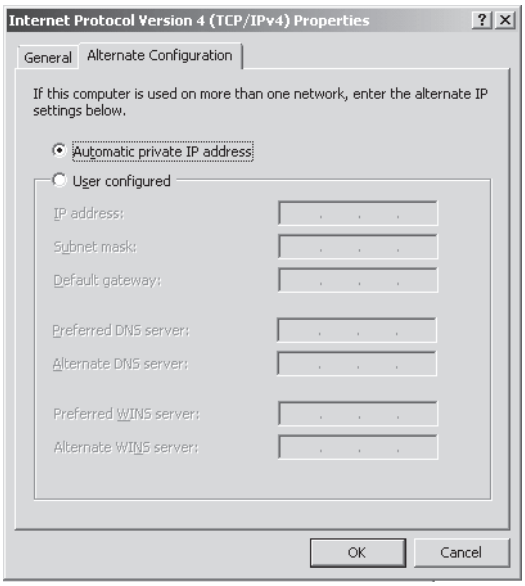
Slika 1-24 Definisanje alternativne IP konfiguracije

Pošto alternativna konfiguracija omogućava računaru da dobije specifičnu i detaljnu IP konfiguraciju kada nijedan DHCP server nije dostupan, definisanje alternativne konfiguracije je korisno za prenosive računare koji prelaze iz mreže u mrežu sa DHCP serverima i bez njih.

Ispitna napomena Za ispit 70-642 morate znati koje su prednosti definisanja alternativne konfiguracije.

Automatsko privatno IP adresiranje (APIPA) *APIPA* je funkcija automatskog adresiranja, korisna za ad hoc ili privremene mreže. Kada je računar pod Windowsom konfigurisan da automatski dobija IP adresu, a DHCP server ili alternativna konfiguracija nisu dostupni, računar koristi automatsko privatno adresiranje da bi sebi dodelio privatnu IP adresu iz opsega 169.254.0.1-169.254.255.254 i masku podmreže 255.255.0.0.

Sve mrežne veze su podrazumevano podešene na adresiranje APIPA kada nijedan DHCP server nije dostupan, što je prikazano na slici 1-25.



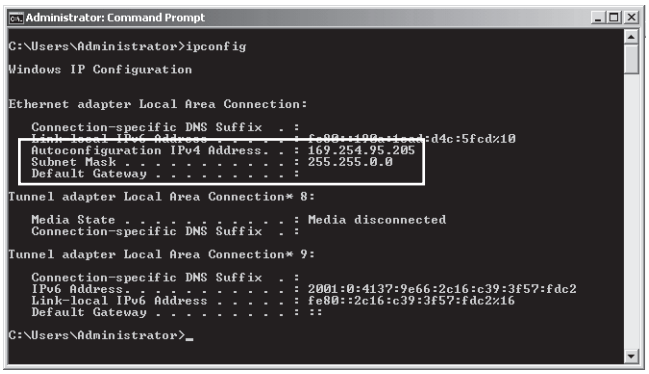
Slika 1-25 U odsustvu DHCP servera, mrežne veze su podrazumevano konfigurisane na adresu APIPA

Funkcija APIPA je veoma korisna, jer omogućava da dva računara pod Windowsom u istom domenu neusmerenog emitovanja komuniciraju međusobno bez DHCP servera ili korisničke konfiguracije. Ako u određenom trenutku DHCP server postane dostupan, adresa APIPA se zamenjuje adresom dobijenom od DHCP servera.

Ispitna napomena Kada dva klijentska računara „vide" jedan drugog, ali ne mogu da se povežu sa ostatkom mreže (ili internetom), posumnjajte na adresiranje APIPA. Ili postoji problem sa DHCP serverom u mreži ili je veza sa DHCP serverom raskinuta.

Iako adresiranje APIPA u izvesnoj meri omogućava komunikaciju u lokalnoj mreži, ograničenja koja nameće dodeljivanje takve adrese su značajna. Veze kojima su dodeljene adrese APIPA mogu da komuniciraju samo sa drugim računarima koji koriste adrese APIPA u opsegu neusmerenog emitovanja u mreži; pored toga, ti računari ne mogu da pristupe internetu. Imajte na umu i to da preko adresiranja APIPA ne možete konfigurisati računar adresom DNS servera, adresom podrazumevanog mrežnog prolaza, niti adresom WINS servera.

Konfiguracija adrese APIPA prikazana je na slici 1-26.



Slika 1-26 Adresa APIPA ukazuje na problem u mreži

Popravljanje mrežne veze komandom *Ipconfig /renew* i funkcijom Diagnose Ako je vezi dodeljena adresa APIPA, to je najčešće znak da veza nije pravilno dobila IP adresu od DHCP servera. Pošto veze sa dodeljenom adresom APIPA mogu da komuniciraju samo sa susednim računarima kojima su takođe dodeljene adrese APIPA, takvo adresiranje je obično nepoželjno. Treba očekivati da će veza kojoj je dodeljena adresa APIPA imati ograničenu mogućnost povezivanja ili je uopšte neće imati.

Ako je vezi dodeljena adresa APIPA, a u mreži nije dostupan DHCP server, možete ili instalirati DHCP server ili vezi dodeliti statičku IP konfiguraciju, odnosno alternativnu konfiguraciju.

Ukoliko je vezi dodeljena adresa APIPA u mreži u kojoj već postoji operativan DHCP server, prvo bi trebalo da pokušate sa obnavljanjem IP konfiguracije ili sa korišćenjem funkcije Diagnose. Da biste obnovili IP konfiguraciju, u komandnom odzivniku unesite **ipconfig /renew**. Funkciju Diagnose ćete upotrebiti ako u prozoru Network Connections desnim tasterom miša pritisnete vezu kojoj je dodeljena adresa APIPA i zatim iz menija sa prečicama izaberete Diagnose. Nakon toga će vam biti data mogućnost da popravite vezu.

U slučaju da ovom strategijom ne obezbedite matičnom računaru novu IP adresu, trebalo bi da proverite da li DHCP server pravilno radi. Ako DHCP server funkcioniše, istražite moguće hardverske probleme, kao što su neispravni kablovi, čvorišta i komutatori, koji možda nastaju između DHCP servera i klijenta.

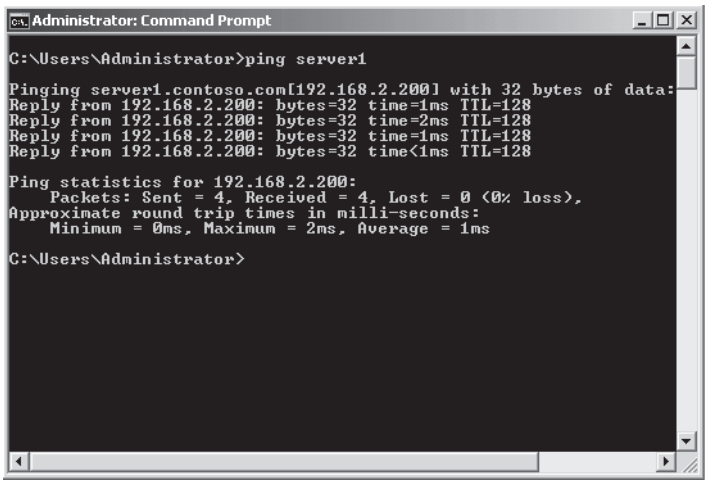
NAPOMENA Obnavljanje IPv6 konfiguracije

Da biste obnovili IPv6 konfiguraciju, u komandnom odzivniku unesite **ipconfig/renew**.

Pronalaženje uzroka problema u mreži pomoćnim programima Ping, Tracert, PathPing i Arp Ukoliko funkcijom Diagnose ili komandom *Ipconfig /renew* ne rešite problem u mreži, upotrebite pomoćne programe kao što su Ping, Tracert, PathPing i Arp, za pronalaženje uzroka problema. Ta četiri pomoćna programa opisaćemo u narednom odeljku.

- **Ping** Ping je ključna alatka za testiranje mrežnih veza. Da biste upotrebili pomoćni program Ping, u komandnom odzivniku unesite komandu **ping *remote_host*,** gde je *remote_host* ime ili IP adresa udaljenog računara, servera ili usmerivača za koji želite da proverite povezanost. Ako udaljeni računar odgovori na komandu ping, veza sa udaljenim matičnim računarom je proverena i potvrđena.

  Na slici 1-27 prikazan je uspešan pokušaj korišćenja komande ping servera sa imenom server1.



Slika 1-27 Uspešno korišćenje komande ping dokazuje da lokalni računar može da komunicira sa serverom server1

VAŽNO ICMP, mrežne barijere i Ping

Pomoćni programi Ping, Tracert i Pathping oslanjaju se na protokol za razmenjivanje poruka sloja 3, koji se zove Internet Control Message Protocol (ICMP). ICMP, međutim, u Windows Visti i Windows Serveru 2008 podrazumevano blokira Windows Firewall, kao i neki usmerivači i samostalne mrežne barijere. Posledično, da biste na pravi način otkrili uzrok problema sa povezivanjem u mreži, morate biti sigurni da ICMP ne blokira udaljeni matični računar. Da biste uključili izuzimanje od blokiranja mrežnom barijerom za ICMP u Windows Visti i Windows Serveru 2008, uključite deljenje datoteka (File Sharing) u programu Network and Sharing Center.

- **Tracert** Tracert je mrežni pomoćni program koji možete koristiti da biste pratili putanju do mrežnog odredišta i testirali status svakog usmerivača na toj putanji. Na primer,

ako se na putu od ServeraA do ServeraE nalaze UsmerivačB, UsmerivačC i UsmerivačD, Tracert možete upotrebiti da biste testirali odgovaraju li ti posrednički usmerivači (kao i odredišni ServerE) na ICMP poruke. Svrha tog testa je da se odredi lokacija bilo kojeg prekida veze između lokalnog računara i udaljenog odredišta.

Pomoćni program Tracert iz komandnog odzivnika koristite unošenjem komande **tracert *remote_host,*** gde je *remote_host* ime ili adresa odredišnog računara, servera ili usmerivača do koga želite da pratite putanju.

Rezultat izvršavanja komande Tracert je prikazan u nastavku. Obratite pažnju na prekidač -d koji je upotrebljen za ubrzavanje testa, jer on sprečava razrešavanje imena svake IP adrese na putanji.

```
C:\Users\jcmackin>tracert -d 69.147.114.210

Tracing route to 69.147.114.210 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  192.168.2.1
  2   822 ms   708 ms   659 ms  67.142.148.2
  3   708 ms   649 ms   658 ms  67.142.131.209
  4   632 ms   619 ms   629 ms  67.142.131.254
  5   726 ms   698 ms   619 ms  67.142.128.246
  6   732 ms   679 ms   709 ms  65.46.24.177
  7   713 ms   650 ms   679 ms  207.88.81.245
  8   732 ms   719 ms   719 ms  71.5.170.41
  9   957 ms   739 ms   719 ms  71.5.170.34
 10   734 ms   736 ms   677 ms  64.212.107.85
 11   723 ms   690 ms   862 ms  64.208.110.166
 12   824 ms   849 ms   739 ms  216.115.101.137
 13   781 ms   799 ms   869 ms  216.115.101.152
 14   822 ms   719 ms   678 ms  216.115.108.72
 15   759 ms   709 ms   799 ms  216.115.108.61
 16   724 ms   819 ms  1479 ms  68.142.238.65
 17   775 ms   859 ms   739 ms  69.147.114.210

Trace complete.
```

- **PathPing** PathPing je sličan programu Tracert, sa tom razlikom što je PathPing namenjen pronalaženju veza koje uzrokuju *povremene* gubitke podataka. PathPing šalje pakete do svakog usmerivača na putu do konačnog odredišta u određenom vremenskom periodu i zatim izračunava procenat paketa koji su se vratili iz svakog skoka (hop). Pošto PathPing pokazuje broj paketa izgubljenih na svakom datom usmerivaču ili vezi, ovaj pomoćni program možete iskoristiti da biste otkrili koji usmerivači ili veze izazivaju probleme u mreži.

  Pomoćni program PathPing ćete iz komandnog odzivnika pokrenuti ako unesete **PathPing *remote_host,*** gde je *remote_host* ime ili adresa odredišnog računara, servera ili usmerivača na čijoj putanji želite da testirate povremeni gubitak podataka.

  Ovo je primer rezultata koji daje PathPing:

```
D:\>pathping -n testpc1
Tracing route to testpc1 [7.54.1.196]
over a maximum of 30 hops:
0 172.16.87.35
1 172.16.87.218
2 192.168.52.1
3 192.168.80.1
4 7.54.247.14
5 7.54.1.196
Computing statistics for 25 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 172.16.87.35
0/ 100 = 0% |
1 41ms 0/ 100 = 0% 0/ 100 = 0% 172.16.87.218
13/ 100 = 13% |
2 22ms 16/ 100 = 16% 3/ 100 = 3% 192.168.52.1
0/ 100 = 0% |
3 24ms 13/ 100 = 13% 0/ 100 = 0% 192.168.80.1
0/ 100 = 0% |
4 21ms 14/ 100 = 14% 1/ 100 = 1% 7.54.247.14
0/ 100 = 0% |
5 24ms 13/ 100 = 13% 0/ 100 = 0% 7.54.1.196
Trace complete.
```

Obratite pažnju na to da se u rezultatu prvo navodi pet skokova na putanji do navedenog odredišta, a zatim i procenat izgubljenih podataka u svakom skoku. U našem slučaju, PathPing pokazuje da se 13 procenata podataka izgubi između lokalnog računara (172.16.87.35) i prvog skoka (172.16.87.218).

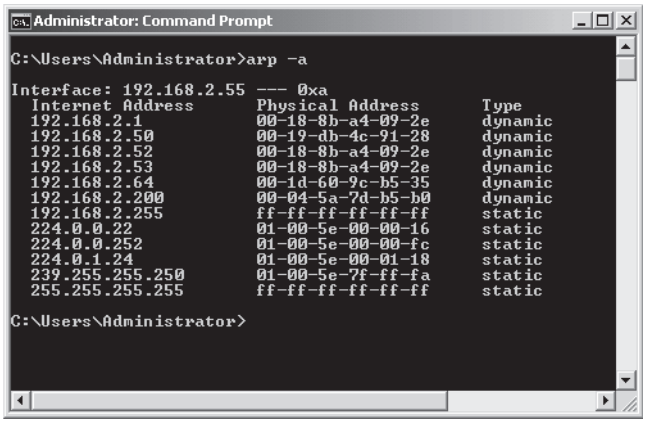
- **Arp** Arp je ime i pomoćnog programa i protokola. Protokol za razrešavanje adresa (Address Resolution Protocol, ARP) se koristi za prevođenje IPv4 (softverske) adrese računara ili usmerivača u opsegu neusmerenog emitovanja u MAC (hardversku) adresu neke određene mrežne kartice u mreži. Drugim rečima, protokol ARP omogućava računarima da fizički komuniciraju sa susednim računarom ili usmerivačem predstavljenim IPv4 adresom. Pomoćni program Arp obavlja srodnu funkciju. Možete ga upotrebiti za prikazivanje i upravljanje ARP keš memorijom računara, u kojoj se čuvaju mapiranja IPv4 adresa-MAC adresa drugih računara u lokalnoj mreži.

  Pošto veza sa računarom u opsegu neusmerenog emitovanja zavisi od preciznog mapiranja IPv4 adresa-MAC adresa tog računara u lokalnoj keš memoriji, pomoćni program Arp vam može pomoći da rešite probleme u mreži kada je uzrok neprecizno mapiranje. Na primer, prikazivanjem sadržaja keš memorije komandom ***arp -a***, mogli biste da otkrijete problem – recimo, sa dve susedne virtuelne mašine koje su same sebi dodelile

istu virtuelnu MAC adresu. (Što je prilično uobičajeno.) Komandu ***arp -d*** možete upotrebiti i za brisanje odrednice iz ARP keš memorije računara ili virtuelne mašine, čija je MAC adresa upravo promenjena i za koju znate da je nevažeća.

U retkim slučajevima pomoćni program Arp možete iskoristiti za otkrivanje pokušaja hakera da „zarazi" vašu ARP keš memoriju povezivanjem nekih ili svih lokalnih IPV4 adresa, najčešće IPv4 adrese lokalnog usmerivača, sa MAC adresom samog hakera. To je dobro poznata tehnika koja omogućava hakeru da tajno usmeri vaše mrežne veze preko njegovog računara.

Primer „zaražene" ARP keš memorije prikazan je na slici 1-28. Obratite pažnju na to da su IPv4 adrese 192.168.2.1, 192.168.2.52 i 192.168.2.53 sve povezane sa istom MAC adresom. Da je hakerov računar predstavljen kao 192.168.2.52, ova ARP keš memorija bi omogućila presretanje svih veza sa adresama 192.168.2.1 i 192.168.253. Ako adresa 192.168.2.1 predstavlja IPv4 adresu lokalnog usmerivača, sva internet komunikacija bila bi presretnuta.



Slika 1-28 „Zaražena" ARP keš memorija

NAPOMENA Da li je duplirana MAC adresa navedena u ARP keš memoriji uvek znak problema?

Sem ako ste dve ili više IPv4 adrese dodelili jednoj mrežnoj kartici negde u lokalnoj mreži (što se retko čini, ali je moguće), svaka IPv4 adresa u ARP keš memoriji trebalo bi da bude pridružena jedinstvenoj fizičkoj adresi.

NAPOMENA IPv6 sprečava „zarazu" ARP keš memorije

Da bi razrešio mapiranje IP-MAC adresa, IPv6 koristi protokol Neighbor Discovery (ND) umesto protokola ARP, koji koristi IPv4. Zato je korisna osobina neke isključivo IPv6 mreže, što sprečava mogućnost da dođe do „zaraze" ARP keš memorije.

VEŽBA Konfigurisanje TCP/IP adresa

U ovom delu ćete konfigurisati statičku IP adresu za lokalnu vezu na računaru Dcsrv1, alternativnu adresu za lokalnu vezu na računaru Boston i, na kraju, statičku adresu na računaru Boston, koristeći komandnu liniju. Do sada su tim vezama bile pridružene adrese APIPA. Nakon konfigurisanja adresa, omogućićete deljenje datoteka na oba računara i testirati veze komandom Ping.

Podrazumeva se da ste obavili podešavanje računarske laboratorije na način opisan u uvodu ove knjige. Na računaru Dcsrv1, Local Area Connection mora biti povezana sa privatnom laboratorijskom mrežom, dok veza *Local Area Connection 2 mora biti isključena*. Na računaru Boston, Local Area Connection mora biti povezana sa istom privatnom laboratorijskom mrežom.

Ni na jednom računaru ne treba da bude instalirana nijedna serverska uloga.

▶ Vežba 1 Verifikovanje trenutne IP adrese

U ovoj vežbi proverićete trenutnu IP konfiguraciju na računaru Dcsrv1.

1. Prijavite se na računar Dcsrv1 kao administrator.
2. Otvorite komandni odzivnik. Pritisnite Start i zatim izaberite Command Prompt.
3. U komandnom odzivniku unesite **ipconfig i zatim pritisnite taster Enter. Ta komanda se koristi za prikazivanje konfiguracije IP adrese.**

   Rezultat prikazuje vaše mrežne veze. Ispod odrednice „Ethernet adapter Local Area Connection" i posle odrednice Autoconfiguration IPv4 Address, videćete adresu 169.254.y.z, gde y i z ukazuju na identifikator matičnog računara trenutno pridružen toj vezi. Maska podmreže je podrazumevano 255.255.0.0. Pošto podrazumevana instalacija Windows Servera 2008 određuje da se IP adresa matičnog računara dodeljuje automatski , u odsustvu DHCP servera matični računar koristi adresu APIPA (pod pretpostavkom da nije definisana alternativna konfiguracija). Obratite pažnju takođe i na to da je istoj vezi dodeljena veza-lokalna IPv6 adresa koja počinje sa fe80::. Ta adresa je IPv6 ekvivalent jedne adrese APIPA.

   Na kraju, videćete i lokalne veze tunel adaptera. One su povezane sa Ipv6 i biće detaljnije opisane u lekciji 3 „Razumevanje adresiranja IP verzije 6 (IPv6)".

▶ Vežba 2 Ručno konfigurisanje adrese

U ovoj vežbi ćete na računaru Dcsrv1 dodeliti statičku IP adresu vezi Local Area Connection. Statička IP adresa je neophodna za računare koji će kasnije postati domaćini mrežnim infrastrukturnim servisima kao što su DNS i DHCP.

1. Dok ste još uvek prijavljeni na računaru Dcsrv1 kao administrator, unesite **ncpa.cpl** u komandnom odzivniku.
2. U prozoru Network Connections desnim tasterom miša pritisnite Local Area Connection i zatim izaberite Properties. Ta veza je uspostavljena sa privatnom laboratorijskom mrežom.

3. U okviru za dijalog Local Area Connections Properties, u delu This Connection Uses The Following Items, dva puta pritisnite Internet Protocol Version 4 (TCP/IPv4).
4. Na tabulatoru General okvira za dijalog Internet Protocol Version 4 (TCP/IPv4) Properties, izaberite Use The Following IP Address.
5. U polje IP Address unesite **192.168.0.1.**
6. Izaberite polje Subnet Mask da biste u njega postavili kursor. U polju Subnet Mask pojavljuje se adresa 255.255.255.0. Pritisnite OK.
7. U okviru za dijalog Local Area Connection Properties pritisnite OK.
8. U komandnom odzivniku unesite **ipconfig**.

   Videćete novu statičku IPv4 adresu pridruženu vezi Local Area Connection.

▶ Vežba 3 Definisanje alternativne konfiguracije

U ovoj vežbi ćete izmeniti IP konfiguraciju računara Boston da bi u odsustvu DHCP servera u privatnoj laboratorijskoj mreži Boston dodelio adresu 192.168.0.200 vezi Local Area Coonection.

1. Prijavite se na računar Boston kao administrator.
2. U Server Manageru, pritisnite View Network Connections.
3. U prozoru Network Connections, otvorite svojstva veze Local Area Connection.
4. U okviru za dijalog Local Area Connection Properties, otvorite svojstva protokola Internet Protocol Version 4 (TCP/IPv4).

   Na tabulatoru General okvira za dijalog Internet Protocol (TCP/IP) Properties obratite pažnju na to da su izabrane opcije Obtain An IP Address Automatically i Obtain DNS Server Address Automatically.
5. Pritisnite tabulator Alternate Configuration.

   Izabrana je opcija Automatic Private IP Address. Pošto nije dostupan nijedan DHCP server i taj je parametar podrazumevano uključen, računar Boston je vezi Local Area Connection automatski dodelio adresu APIPA.
6. Izaberite User Configured.
7. U polje IP Address unesite **192.168.0.200**.
8. Pritisnite polje Subnet Mask da biste u njega postavili kursor. U polju Subnet Mask pojavljuje se podrazumevana maska podmreže 255.255.255.0. Tu vrednost ostavite kao podrazumevanu masku podmreže.

   Upravo ste za računar Boston definisali alternativnu konfiguraciju IP adrese 192.168.0.200/24. Tu konfiguraciju možete koristiti dok u mreži ne konfigurišete DHCP server.
9. Pritisnite OK.

10. U okviru za dijalog Local Area Connection Properties, pritisnite OK.
11. Otvorite komandni odzivnik i unesite **ipconfig /all**.

    U rezultatu komande Ipconfig videćete novu alternativnu adresu dodeljenu računaru Boston. Obratite pažnju na to da je i parametar Autoconfiguration Enabled postavljen na Yes.

▶ Vežba 4 Konfigurisanje statičke IPv4 adrese iz komandnog odzivnika

U ovoj vežbi ćete komandni odzivnik koristiti za konfigurisanje statičke IPv4 adrese 192.168.0.2 i maske podmreže 255.255.255.0 za računar Boston.

1. Dok ste na računaru Boston prijavljeni kao administrator, otvorite administratorski komandni odzivnik (elevated command prompt). (Taj korak nije neophodan ako ste prijavljeni nalogom Administrator. Administratorski komandni odzivnik ćete otvoriti ako pritisnete dugme Start, desnim tasterom miša pritisnete Command Prompt i zatim izaberete Run As Administrator.)
2. U komandnom odzivniku unesite sledeću komandu:

   ```
   netsh interface ip set address "local area connection" static 192.168.0.2
   255.255.255.0
   ```

3. U komandnom odzivniku unesite **ipconfig**.

   Rezultat izvršavanja komande Ipconfig otkriva novu IPv4 adresu.

▶ Vežba 5 Omogućavanje deljenja datoteka

U Windows Serveru 2008 morate omogućiti deljenje datoteka pre nego što lokalni računar počne da odgovara na komandu ping. Zato ovaj korak morate obaviti u programu Network and Sharing Center na oba računara - Dcsrv1 i Boston.

1. Dok ste na računaru Dcsrv1 prijavljeni kao administrator, otvorite Network and Sharing Center. Desnim tasterom miša pritisnite ikonicu mreže u delu Notification Area i izaberite Network and Sharing Center. (Notification Area je deo na desnoj strani palete poslova.)
2. U prozoru Network and Sharing Center, u delu Sharing And Discovery, pritisnite dugme označeno sa Off pored odrednice File Sharing.
3. Izaberite opciju za uključivanje deljenja datoteka i zatim pritisnite Apply.

   Pojaviće se okvir za dijalog sa pitanjem da li želite da uključite deljenje datoteka za sve javne mreže.
4. Pritisnite Yes, Turn On File Sharing For All Public Networks.

   Imajte na umu da je ova opcija preporučljiva samo za mreže u kojima se obavlja testiranje.
5. Ponovite korake 1 do 4 na računaru Boston.

▶ Vežba 6 Verifikovanje veze

U ovoj vežbi ćete verifikovati da dva računara mogu da komuniciraju preko privatne laboratorijske mreže.

1. Dok ste na računaru Boston prijavljeni kao administrator, otvorite komandni odzivnik.
2. U komandnom odzivniku unesite ping **192.168.0.1**.

   Rezultat potvrđuje da računari Dcsrv1 i Boston komuniciraju preko protokola IP.
3. Odjavite se sa oba računara.

Pregled lekcije

- Transmission Control Protocol/Internet Protocol (TCP/IP) definiše četvoroslojnu arhitekturu u kojoj su sloj mrežnog interfejsa (Network Interface) ili sloj povezivanja podataka (Data Link), internet ili mrežni (Network) sloj, transportni (Transport) sloj i aplikativni (Application) sloj. Zbog pozicije koju zauzimaju u modelu umrežavanja OSI, ti slojevi su poznati i kao sloj 2, sloj 3, sloj 4 i sloj 7, redom.
- Network and Sharing Center je glavna alatka za konfigurisanje mreže u Windows Serveru 2008. Možete je upotrebiti za obavljanje funkcija, kao što su podešavanje mrežne lokacije, pregledanje mape mreže, konfigurisanje parametra Network Discovery, konfigurisanje deljenja datoteka i štampača i pregledanje statusa mrežnih veza.
- Korišćenjem svojstava mrežne veze, računar možete konfigurisati statičkom adresom ili automatski konfigurisanom adresom. Automatski konfigurisane adrese dobijaju se od DHCP servera, pod uslovom da je dostupan u mreži.
- Kada je veza konfigurisana tako da adresu dobija automatski, a nijedan DHCP server nije dostupan, veza će podrazumevamo sama sebi dodeliti adresu u obliku 169.254.x.y. Možete definisati i alternativnu konfiguraciju koju će veza sebi dodeliti u odsustvu DHCP servera.
- Određeni osnovni TCP/IP pomoćni programi se koriste za testiranje i pronalaženje uzroka problema sa vezama u mreži. Među njima su Ipconfig, Ping, Tracert, PathPing i Arp.

Obnavljanje lekcije

Pitanja koja slede imaju za cilj da još jednom posebno istaknu najvažnije informacije iz ove lekcije. Možete ih naći i na pratećem CD-u ako vam više odgovara da ih pregledate u elektronskoj formi.

NAPOMENA Odgovori

Odgovori na ova pitanja i objašnjenja zašto su neki ponuđeni odgovori tačni ili pogrešni nalaze se u odeljku „Odgovori" na kraju knjige.

---

1. Korisnica u vašoj organizaciji se žali da ne može da se poveže ni sa jednim mrežnim resursom. Na njenom računaru izvršavate komandu *Ipconfig* i zaključujete da je vezi Local Area Connection dodeljena adresa 169.254.232.21.

   Koju bi od navedenih komandi trebalo prvo da izvršite?

   A. Ipconfig /renew

   B. ping 169.254.232.21

   C. tracert 169.254.232.21

   D. Arp -a

2. Koji od navedenih tipova adresa najviše odgovara DNS serveru?

   A. Adresa koju dodeljuje DHCP

   B. Adresa APIPA

   C. Alternativno konfigurisana adresa

   D. Ručno konfigurisana adresa