3.Generatori mrežnog prometa

3.1.Općenito

Što je to generator mrežnog prometa?

Generator mrežnog prometa je sustav koji povezuje različite ili slične uređaje u jednu cjelinu. U telekomunikacijskom i podatkovnom smislu, generator povezuje uredjaje za obradu podataka i komunikacijske uredjaje, bilo na medjudržavnom planu, unutar pojedine zemlje, grada, u industrijskom postrojenju,poslovnim zgradama ili u malom uredu. Potreba za umrežavanjem posljedica je stalnog porasta razmjene podataka (pisama, poruka, memoranduma, poslovne statistike, izvještaja, baza podataka i sl.) medju zaposlenima. Izračunato je da se oko 60 % radnog vremena koristi za komunikaciju ili razmjenu podataka; u današnje vrijeme količina tako razmijenjenih informacija dosiže i do 35 otipkanih stranica po osobi dnevno.Za uštedu su vremena napravljeni razni uredjaji namijenjeni komunikaciji i razmjeni podataka (teleks, telefaks, osobna računala, pisaći, višefunkcijski terminali), a sada ih sve treba povezati u računalnu mrežu da bismo svi zajedno dijelili mogućnosti koje nam ti uredjaji pružaju.

Podjela generatora

Ovisno o udaljenostima koje prilikom umrežavanja treba premostiti, na raspolaganju su različite tehnologije generatora i vrste medija za prijenos podataka. Tako i generatore dijelimo u dvije osnovne kategorije: fiksni i varijabilni generator.

Visoko razvijena satelitska tehnologija omogućuje danas povezivanje bilo koje dvije točke na Zemlji, a postoje i instalacije na kopnu i u moru koje omogućuju medjusobno povezivanje klasičnim medijima - običnim ili optičkim kabelima. U razvijenim zemljama postoji niz telekomunikacijskih tvrtki koje pružaju usluge povezivanja raznim drugim tvrtkama i organizacijama unutar zemlje pa i preko granica.

Internet - specifična tvorevina računalne industrije - omogućuje komunikaciju i razmjenu podataka pojedincima i organizacijama iz cijelog svijeta.Danas na tržištu postoje satelitski uredjaji koji omogućuju pojedincu ili tvrtci pristup Internetu putem satelita, bez obzira na to postoji li u zemlji korisnika netko tko pruža usluge pristupa Internetu.

Generatori i računarske mreže

Na lokalnom planu zanimljive su mreže računala u uredima, u poslovnim zgradama ili industrijskim postrojenjima, odnosno na malim udaljenostima.Takve mreže spadaju u lokalne računalne mreže.Svaka od ove dvije kategorije dijeli se na podgrupe koje se razlikuju po
vrsti medija za prijenos signala, brzinama rada, mrežnim tehnologijama i protokolima koje koriste, kao i vrsti mrežnih operativnih sustava.

Svako računalo opremljeno Ethernetom, znano i pod imenom stanica,radi neovisno od svih drugih stanica u mreži: ne postoji centralni nadzornik sustava. Sve stanice priključene na Ethernet spojene su pomoću zajedničkog signalnog sustava koji nazivamo medij. Ethernet signali šalju se serijski, bit po bit, putem medija do svake priključene stanice. Da bi poslala podatke, svaka stanica najprije provjerava medij, a kad ustanovi da je medij slobodan, šalje svoje podatke u obliku Ethernet okvira ili paketa. Nakon svakog slanja paketa, sve stanice u mreži ravnopravno se natječu za mogućnost slanja sljedećeg paketa. Time se osigurava pravilna raspodjela
pristupa mediju, a nijedna stanica ne može zauzeti medij samo za sebe. Pristup mediju za slanje podataka odredjen je mehanizmom kontrole pristupa mediju (Medium Access Control – MAC) ugradjenom u svako Ethernet sučelje u svakoj stanici. Kontrola pristupa mediju temelji se na sustavu nazvanom Carrier Sense Mutiple Access with Collision Detection (CSMA/CD), odnosno višestruki pristup provjerom nositelja signala s detekcijom sukoba.

Sequential protokol

Ovaj bismo protokol mogli zorno predočiti kao večeru u zatamnjenoj sobi.Svi koji sjede oko stola moraju šutjeti odredjeno vrijeme prije nego što počnu govoriti (provjera nositelja – Carrier Sense). Kad nastupi tišina, svi imaju jednake šanse da započnu govoriti (višestruki pristup – Multiple Access). Ako dvije osobe započnu govoriti u istom trenutku, obje će detektirati tu činjenicu i prestati govoriti (detekcija sukoba – Collision Detection).U Ethernet terminologiji, svaka stanica mora čekati dok ne nestane signal
na nositelju i tek tada smije započeti emitiranje. Kada neka od stanica emitira, u mediju postoji signal koji se naziva nositelj – carrier. Sve Ethernet tehnologija – principi i standardi ostale stanice moraju čekati da nestane signal prije nego pokušaju zapo-
četi emitiranje. Ovaj se proces naziva provjerom nositelja – carrier sense.Sve su stanice jednake u pogledu mogućnosti slanja paketa u mreži. Nitko ne dobiva viši prioritet od drugih. Mogli bismo reći da vlada demokracija.Otud i značenje pojma višestrukog pristupa – multiple access. Sobzirom da signalu treba konačno vrijeme da doputuje s jednog kraja Ethernet sustava na drugi, prvi bit emitiranog paketa neće stići istovremeno do svih stanica. Zbog toga je moguća situacija da dvije stanice provjerom ustanove da je medij slobodan i započnu istovremeno emitiranje.Kada se to dogodi, Ethernet sustav ima načina da utvrdi sukob i zaustavi
slanje paketa i pripremi se za njegovo ponovno slanje. Ovakav se slučaj naziva detekcijom sukoba – collision detect.Sequential protokol napravljen je tako da omogući ravnopravno sudjelovanje u dijeljenju medija tako da svaki element sustava dobije priliku da
koristi mrežu. Nakon svakog slanja paketa, sve stanice koriste sequential protokol da bi utvrdile koja stanica će sljedeća dobiti pravo za korištenje Ethernet medija. Kao što je ranije opisano, ako više od jedne stanice započne emitiranje u istom trenutku, nastupa sukob. Sve stanice se obavještavaju o tom dogadjaju i trenutno odgadjaju emitiranje koristeći specijalno razvijeni algoritam.Dio tog algoritma je da svaka od stanica uključenih u sukob izabire vremenski interval slučajno odabranog trajanja (dakle, svaka različito) za

odgodu slanja paketa što sprečava stanice da blokiraju mrežu istovremenim pokušajima slanja. Mnogi kažu kako je šteta da je u originalnom projektu Etherneta za ovu vrstu događaja izabrana riječ sukob. Da je kojim slučajem nazvana drugač ije (npr. “događaj stohastičke arbitracije” – DSA), tada nitko ne bi brinuo zbog događaja DSA na Ethernetu. Ovako, “sukob” zvuči kao da se ne-
što loše dogodilo, upućujući mnoge na razmišljanje da su sukobi pokazatelj greške u mreži. činjenica je da je sukob sasvim normalna i očekivana pojava u mreži, a samo je dokaz da CSMA/CD protokol radi onako dobro kako je i zamišljen. [to je više računala (stanica) spojeno u mrežu i što je veći promet podataka mrežom, za očekivati je da će se pojaviti i više sukoba, kao dio normalnog rada
mreže. Izvedba sustava osigurava da se sukobi rješavaju u mikrosekundama (milijuntim dijelovima sekunde). Normalni sukobi ne uzrokuju gubitak podataka.Ponavljani sukobi za isti paket pokazuju da je mreža preopterećena. Algoritam za određivanje vremena odgode slanja paketa automatski se prilagođ ava opterećenju na mreži, a nakon 16 neuspjelih pokušaja slanja paketa, paket se odbacuje kao neposlan. Ovo se događa samo u vrlo teškim opterećenjima mreže ili ako u mreži dođe do prekida. Slanje u najboljoj namjeri Zanimljiva je činjenica da Ethernet sustav, zajedno s drugim LAN tehnologijama, radi kao sustav za isporuku podataka “u najboljoj namjeri”. Da bi se smanjila složenost sustava i troškovi izrade, nema jamstava da su isporučeni točni podaci. Iako je sam sustav projektiran uz upotrebu bitova za provjeru greške, do greške u prijenosu ipak može doći.Smetnja u obliku električnog šuma može, primjerice, negdje u kabelskom sustavu uzrokovati promjenu podataka u paketu koji putuje medijem. Ako je mreža privremeno preopterećena može doći do 16 uzastopnih doga- đanja sukoba, pri čemu se paket koji je namijenjen slanju odbacuje. Bez
obzira na upotrijebljenu tehnologiju, nijedan mrežni računalni sustav nije idealan. Viši mrežni protokoli moraju biti projektirani tako da provjeravaju pogreške pri slanju i primanju paketa. Viši mrežni protokoli provjeravaju točnost podataka uspostavljanjem
pouzdanog prijenosa podataka korištenjem brojevnih sekvenci i mehanizmima provjere u paketima koji se šalju mrežom. Srce Ethernet sustava je Ethernet paket koji se koristi za slanje podataka između računala. Paket se sastoji od skupine bitova organiziranih u nekoliko polja. U ova polja spadaju adresno polje, polje podataka promjenjive duljine (od 46 do 1500 bajtova podataka) i polje za provjeru greške u kojem se provjerava integritet bitova u paketu da bi se utvrdilo je li paket stigao netaknut.Prva dva polja u paketu sastoje se od 48-bitne adrese, nazvane izvoriš- nom i odredišnom adresom. Institute of Electrical and Electronics Engineer
(IEEE) je organizacija koja nadzire dodjelu ovih adresa tako što odre- đuje jedan njezin dio. IEEE to čini tako da dodjeljuje 24-bitnu oznaku nazvanu OUI (Organizationally Unique Identifiers) svakoj organizaciji odnosno tvrtci koja želi proizvoditi Ethernet opremu. Organizacije dalje stvaraju 48-bitnu adresu tako da dodijeljeni OUI koriste kao prva 24 bita adrese. Ova adresa poznata je kao fizička adresa, hardverska adresa ili MAC adresa Ethernet uređaja.Gore opisana adresa jedinstvena je za svaki proizvedeni Ethernet uređaj
i upisuje se u sam uređaj prilikom proizvodnje što znatno pojednostavljuje podešavanje i rad u mreži. S jedne strane, jednoznačno dodijeljene adrese poštedjet će vas administracije adresa za različite grupe korisnika koje koriste mrežu. Ako ste ikad pokušali različite radne grupe privoljeti da dobrovoljno prihvate isti skup pravila za rad,

shvatit ćete kakva je to prednost. Kako se koji Ethernet paket šalje po mediju, sve Ethernet stanice gledaju u prvo 48-bitno polje paketa koje sadrži odredišnu ili ciljnu adresu paketa. Stanice uspoređuju ovu adresu s vlastitom adresom. Stanica s istom adresom koja je sadržana u odredišnoj adresi paketa pročitat će cijeli paket i isporučiti ga mrežnom softveru koji radi na tom računalu. Sve ostale stanice prestat će čitati paket kad otkriju da se njihova adresa razlikuje od odredišne adrese paketa.
Grupne i zajedničke adrese

Grupna adresa (multicast) dozvoljava da grupa stanica primi isti paket.Mrežni softver može postaviti Ethernet stanicu da očekuje posebnu vrstu grupne adrese. Na taj način moguće je podesiti grupu stanica kao posebnu grupu i dodijeliti joj zajedničku grupnu adresu. Jedan paket poslan na takvu grupnu adresu primit će sve stanice u toj grupi. Specijalni slučaj grupne adrese je broadcast adresa, koja je 48-bitna adresa sastavljena od jedinica. Sve Ethernet stanice koje prime paket s ovakvom adresom pročitat će cijeli paket i isporučiti ga mrežnom softveru u računalu.
Viši mrežni protokoli i Ethernet adresa

Računala priključena na Ethernet mogu slati podatke za aplikacije jednodrugome koristeći više softverske protokole kao što je TCP/IP protokol koji se koristi u Internetu. Paketi viših protokola šalju se u podatkovnom polju Ethernet paketa. Sustav viših protokola i Ethernet sustav dva su neovisna entiteta koji kooperiraju prilikom razmjene podataka između računala. Viši protokoli imaju svoj sustav adresiranja kao što je 32-bitna adresa koriš tena u trenutnoj inačici IP protokola. IP temeljeni mrežni softver više razine u nekom računalu brine samo o svojoj IP adresi i može čitati 48-bitnu Ethernet adresu svojeg mrežnog sučelja, te pritom ne zna koje su
Ethernet adrese drugih mrežnih stanica.Da bi sve to moglo raditi, mora postojati način da se otkrije Ethernet adresa druge -temeljene stanice u mreži. Za nekoliko viših mrežnih protokola, uključujući i TCP/IP, ovo se obavlja koristeći drugi viši protokol koji se zove Adress Resolution Protocol – protokol za određivanje adresa.

Princip rada ARP protokola

Rad ARP protokola je jednostavan. Pretpostavimo da IP-temeljena stanica (stanica “A”) s IP adresom 192.0.2.1. želi poslati podatke putem Ethernet sustava drugoj IP-temeljenoj stanici (stanica “B”) s IP adresom 192.0.2.2. Stanica “A” šalje paket s broadcast adresom koji sadrži ARP upit. ARP upit u osnovi pita: “Hoće li mi, molim, stanica u ovom Ethernet sustavu koja ima IP adresu 192.0.2.2., poslati adresu svog Ethernet sučelja?”Budući da se ARP upiti šalju u broadcast paketu, sve stanice u tom Ethernet sustavu primit će taj paket i proslijediti ga višem protokolu. Samo stanica “B”, s IP adresom 192.0.2.2 će odgovoriti, šaljući stanici koja je uputila zahtjev paket sa svojom Ethernet adresom. Sada stanica “A” ima Ethernet adresu stanice “B” i komunikacija na višem protokolu može početi.

Sequential generators

Sequential generator razvili su se kako bi se ostvarila maksimalna performansa u generisanju mrežnog prometa i namenjen je za mreže brzog protoka.Standardni korisnički modeli nisu bili dovoljni za protok paketa u poredjenju sa sequential generatorima.

Glavni razlog za ovo je što standardni modeli i alati gube dosta na vremenu pri presecanju paketa i njihovom putu prema kompletnom mrežnom staništu.Još jedna prednost sekvencijalnih generator je to što šalju podatke dosta preciznije i tačnije i to zato što generišu podatke u sekvencama,tačnije deo po deo i na taj način šalju delove celog paketa.

Ova vrste generatora ima dve vrste osnovnih modula – modul za slanje, koji šalje pakete što je brže moguće direktno na hardverski drajver i zaobilazi mrežno stajalište. Može da razvije dosta veliku brzinu pri slanju i služi za testiranje performansi hardvera i softvera, performance prijema paketa, rutera,svičera itd.

Modul za prijem paketa,to je modul koji se može nakačiti na glavni protocol ili se direktno povezati na hardverski drajv od koga prima podatke.Ova generator ima mogućnost da prebrojava pakete I meri njihovo dolazno vreme.Merenje vrši precizno I može se koristiti zajedno sa modulom za slanje kako razna testiranja performansi.

Predstavljanje

Generator mrežnog prometa najčešće se koristi za okarakterisanje performansi komunikacionih protokola u mreži.Sekvencijalni generatori može da prima i da šalje pakete koji se emitiraju putem mreže.Često se koristi za uniks operativne sisteme i služi za povezivanje izmedju source-a i čvora u mreži.Različiti protokoli, ili različite verzije istog protokola mogu biti testirane kako bi se utvrdile različitosti i sličnosti medju njima. Ovaj generator u sebi ima posebno kreiran programski jezik koji mu pomaže da obavlja svoj zadatak, ali i dozvoljava pristup drugim operativnim modovima, protokolima, specifičnom jeziku i performansama.On omogućava protok nekoliko različitih paketa, različite veličine i različitih vremenskih intervala.

Raspon multiprotoka može da se kontroliše uz pomoć posebne funkcije.Kvalitet i tip parametara se podešava uz pomoć polja DiffServ i tako se kontroliše slanje I prijem. Sekvencijalni generator se fokusira na praćenje paketa i snimanje podataka o njihovom protoku,brzini itd.Da bi se ovo obezbedilo, potrebno je da izvor prijema i izvor predaje budu aktivni kako bi se testiranje izvršilo.Protok prijema uzima podatke iz dokumenta I na taj način se vrši testiranje.
Kada se koristi servis komunikacionog transporta, potrebno je da se predajniku uputi zahtev od strane prijemnika.U generatoru se nakon toga kreira datagram sa podacima o vremenu slanja.Na taj način moguće je pratiti i otkriti uzroke blokada merino prometa ili prilikom učitavanja mreže.

U zavisnosti od toga da si radi o servisima koji se oslanjaju na konekciju ili ne, potrebno je jedan ili više mrežnih portova.Za protokole dijagrama, mnogostruki izvori protoka mogu slati svoje podatke jednom portu (odnos više prema jednom). Generator skuplja podatke sa svih izvora protoka i beleži ih u svoj log fajl.Uz pomoć polja DiffServ može se podesiti takozvani **setsockopt** fi tako se označiti broj bitova koji ostaju nepromenjeni.U budućnosti ova opcija može da bude nadogradjena u zavisnosti od operativnog sistema

Kada se koristi neki poseban protocol, mora postojati mapiranje jedan na jedan, izmedju prijemnika i predajnika za svaku konekciju.Svako pozivanje generatora omogućuje da se ostvari i održi aktivna konekcija.U sekvencama, ako su dve konekcije potrebne, mora postojati otvorena dva porta.

Korisničko uputstvo

Ovaj deo opisuje kako koristiti sekvencijalni generator. Kao prvo, treba napomenuti da se ključne reči upisuju boldovanim fontom, cifre i brojevi se upisuju italikom, dok se parametri označavaju i selektuju velikim zagradama.

Parametri koji se unose u generator imaju dvostruku zaštitu i ne može doći do greške.Preciznost cifara će biti očuvana iako je moguće da dodje do nestabilnosti sistema.

Hijerarhija distribucije softvera

Hijerarhija distribucije softvera se sastoji od nekoliko direktorija visokog nivoa, koja je u tesnoj vezi sa uniks konvecijama.Postoje tri vrste sekvencijalnih generator,tačnije softvera za njihovu upotrebu,a to su: kao prvo,sam generator, drugi je filter za čitanje i očitavanje log fajlova i skripta koja generiše informacije koju koriste grafički alati.

Direktoriji za njihov sadržaj su:

- **./bin**
- **./docs**
- **./examples**
- **./src**

Konfiguracija generatora

Sekvencijalni generator je realiziran sa izvornim kodom kako bi se poboljšanja dodavala kasnije i kako bi se podržali novi protokoli ili statistička distribucija koja će biti potrebna za nova istraživanja.Distribucija je smeštena u **./bin** direktorij.

Kako bi se sekvencijalni generator rekonfigurisao, potrebno je ući u direktorij **./src** I pokrenuti komandu **make**. U sistemu će takodje biti potrebni program kako bi se rekonfigurisali kodovi potrebni za funkcionisanje ovog generator.Ovaj softver može da radi u SunOS, Solaris, FreeBSD, i Linux operativnim sistemima, mada se pretpostavlja da može funkcionisati i u unixu.

Specifikacija fajlova

Sadrži komande koje se upisuju u sledećoj formi:

< start-time >
< association-spec >
< tg-action-list >

start-time – označava se vreme za koje se pretpostavlja da je vreme početka testiranja .Akcije koje se zadaju uz pomoć druge dve komande će se izvršiti nakon označavanja vremena početka.Pre nego što se testiranje može izvršiti, moraju se definirati protokoli koji se žele testirati i raspon u kome se odvija protok informacija. Pored protoka, proverava se i testira ispravnost i tačnost parametra. Linije forme koja uključuje komandu *filename"* cuzrokuje to da imenovani fajl bude pročitan i izvršen.Obavezni su i znaci navoda. Maksimalna dužina inkluzije koja se kompilira u program može se predefinirati ukoliko se zada komanda **MAX_INCLUDE_LEVEL**. Specifikacioni fajl, stoga, sadrži kompletan set komandi kao što su *start-time*, *association-spec, -action-list.*

Statistička distribucija

Statistička distribucija odnosi se sa vremenom dolaska paketa i dužinom slučajnih varijabli paketa.Vreme dolaska je specificirano ključnom reči **arrival**, dok se dužina paketa označava komandom **length**. Trenutno, četiri tipa distribucije je podržano – ostali načini distribucije su planirani i biće dodavani kada budu usavršeni.Četiri komande koji su trenutno u upotrebi:

constant *vrednost*
uniform maksimum *ili* **uniform** *minimum i maksimum*
exponential vrednost *ili* **exponential** *značenje*
markov2 *broj distribucija broj*

constant distribucija uvek vraća broj na odredjeni parameter,i ukoliko se to želi, može se podesiti za stalno.U**niform** distribucija zahteva broj koji specificira maksimalnu vrednost intvervala koji se otvara, od kojih se jedan izvlači i biva testiran.Ako je leva strana takodje specificirana, slučajan broj biva biran od otvorenog intervala [*min*, *max*). **Exponential** distribucija je klasična distribucija sa specifičnim značenjem.Moguće je zabraniti vrednosti koji su već uzeti iz intervala [*min*, *max*);

Odredjivanjem gornje granice za eksponencijalnu distribuciju otvara se mogućnost da samo paketi odredjene veličine budu transportovani.Beskonačna veličina paketa može se generirati i greška će biti prikazana.Mark2 ključna reč je reč koja specificira dva stanja distribucije: prvi broj pokazuje vreme početnog stanja,drugi broj pokazuje vreme krajnjeg stanja.Svako stanje je povezano sa sopstvenom distribucijom.Ove distribucije mogu biti na oba mesta pojedinačno, kako god korisnik odluči.

Primeri

Sledeći primer prikazuje specifičan ulaz za mrežni izvor.

na 0:15
ip adresa 128.18.4.97.2345
u 5 start
u 6 odredište exp 0.1 dužina exp 576
321423 vreme 10

Na 0:15 je komanda koja zadaje generatoru zadatak da čeka petneast sekundi pre nego što počne sa bilo kakvom aktivnošću protokola. Pošto se reč server ne

upotrebljava u liniji specifikacije, sledećom komandom će se označiti adresa i port servera.
Start komanda pokazuje da se pet sekundi nakon intervala od petnaest sekundi aktiviranja pokreće zahtev za konekciju ka repetitoru.Sekundu kasnije protok će biti izvršen sa medjurazmakom od 0.1 sekundom.Veličina segmenta se distribuira u sekvencama od 576 bajta. Poslednja linija komande postavlja zadatak da se izvrši testiranje u trajanju od deset sekundi na slučajno odabranoj liniji protoka.

na 0:15 128.18.4.97.2345 server
do 1.1 čekaj

U ovoj komandi se pominje reč server i generator ulazi u stanje čekanja, 1,1 sekundu nakon početka sinhronizacije.

Kreiranje LOG fajla

TSekvencijalni generator ima mogućnost da beleži i snima podatke o svim značajnim dogadjajima nakon izvršene analize. Sa izuzetkom opisivanja zaglavlja, ovaj fajl se kreira u binarnom zapisu sa fiskiranim i varijabilnim kodom dužine, kako bi se uštedelo na prostoru. Takvi pojmovi se čuvaju u sekvencama bajtova, sedam bitova po bajtu u malom formatu. Vrednost broja nije pod uticajem sledećeg samo ako je njegova vrednost 0x00. Ovo dozvoljava komandi 0x00 da se obeleži i markira broj koji se odnosi na tu stavku.

U suštini, sekvencijalni generator u sebi sadrži program kako bi se enkriptirani podaci iz programskog dela konvertirali u tekstualni fajl koji se može čitati.Unutar ovog programa postoji filter kako bi se ti podaci na pravi način generisali, i odvojili prema posebnim direktorijima.
Opcija **-a** prikazuje mogućnost kopiranja podataka iz svih fajlova prisutnih na programskom displeju.

Zaglavlje datagrama

Zaglavlje datagrama sadrži u sebi ASCII kod i vrši prikaz općih informacija o testiranju i rezultatima testiranja.Ovo zaglavlje sadrži u sebi sledeće:
• Verziju fajla
• Verziju generatora
• Podatke o korisnicima
• Konfiguraciju mašine
• Ime specifikacijskog fajla
• Početak testiranja
• Ime protokola koji se testira
• Indikator adrese.

Fixed length generator

Ovaj generator je specifican po tome sto ima fiksnu duzinu protokola.Predstavnik ovog generator je DHCP server.

Zahvaljujuci popularnosti Interneta i svojoj sposobnosti da se prilagodi i vecim mrezama, TCP/IP je postao protokol koji se najcesce koristi za rad u mrezi. Posto svaki racunar unutar mreze koja koristi protokol TCP/IP mora da ima jedinstvenu IP adresu, njihovo konfigurisanje moze da oduzme mnogo vremena. Postoje samo dva nacina da umrezenom racunaru koji se sluzi protokolom TCP/IP dodelite IP adrese: rucno i dinamicki.

Ako odlucite da IP adrese konfigurisite rucno, onda izvesno preuzimate veliki zadatak. Pri rucnom konfigurisanju vrlo cesto se desavaju greske. Povrh toga, trebace vam mnogo vremena da licno obidete svaki racunar u mrezi i na njemu konfigurisete sve parametre protokola. Dinamicko konfigurisanje IP adresa je, bez daljeg, pogodniji postupak. Potrebno je da ispravno konfigurisete samo jedan racunar - DHCP server.

Usluge DHCP servera na vasem Windowsu 2000 Server predstavlja, u stvari, samo podskup usluge BootP. BootP je usluga koja omogucuje da se u mrezi nalaze racunari koji nemaju cvrsti disk. Posto klijentski racunari nemaju cvrste diskove, mora se obezbediti alternativno sredstvo za podizanje takvih racunara. To alternativno sredstvo je mrezna kartica sa BIOS cipom koji sadrzi program BootP. Pomocu posebnog softvera mreznu karticu mozete tako da konfigurilete da se pri podizanju racunara ona ukljuci na mrezu, pronade BootP server, sa njega preuzme operativni sistem i prosledi ga u operativnu memoriju klijenta,sto u krajnjoj liniji znaci da se racunar podize preko mreznekartice.
Deo procesa BootP je i konfigurisanje protokola. Kada se klijent inicijalizuje, on BootP serveru Salje zahtev za dobijanje podataka potrebnih za konfigurisanje IP adrese. Ovo je samo deo procesa BootP koji Windows 2000 podrzava.
Kada se klijenti Microsoftove mreze (konfigurisani da koriste DHCP) inicijalizuju, oni, kroz prikljucak 67, sirom mreze salju protokol za razmenu korisnickih datagrama (engl. User Datagram Protocol, UDP). Samo ce BootP serveri, odnosno DHCP serveri, prihvatiti UDP zahteve prikljucka 67 (BootP servera). Zahtev DHCP klijenta za dobijanje usluga DHCP servera naziva se DHCP objava (engl. DHCP discovery). Kada DHCP server primi paket sa objavom, on klijentu odgovara DHCP ponudom (engl. DHCP client offer). Ponuda sadrzi IP adresu koju DHCP server nudi klijentu. Kada klijent primi DHCP ponudu, on serveru odgovara DHCP zahtevom (engl. DHCP client request). Ovim paketom se zahteva IP adresa koju je ponudio DHCP server. U poslednjoj fazi ovog procesa, DHCP server klijentu salje DHCP potvrdu (engL DHCP acknowledgment). DHCP potvrda, ili DHCP ACK, sadrzi sve parametre koji su klijentu potrebni za

konfigurisanje protokola TCP/IP Tek u ovoj fazi klijent stvarno inicijalizuje protokol i prijavijuje se na mrezu.

Autorizovanje

DHCP u Windowsu 2000 veoma lici na ono sto je ugradeno u Windows NT 4, uz nekoliko razlika. Razlike se ogledaju u tome kako pokrecete uslugu i kako pravite opseg IP adresa. Na primer, Windows 2000 ce automatski instalirati uslugu DHCP ukoliko kao protokol za instaliranje izaberete protokol TCP/IP. Medutim, usluga DHCP nece biti dostupna sve dok za nju ne ovlastite server, tj. dok ga ne proglasite serverom DHCP usluge.

Da biste server ovlastili za pruzanje DHCP-usluge, uradite sledece:

1. Prijavite se serveru u svojstvu administratora.
2. Izaberite Start/Programs/Administrative Tools/DHCP. Windows 2000 ce otvoriti administrativnu DHCP konzolu.
3. Desnim tasterom misa pritisnite server koji zelite da ovlastite za pruzanje DHCP usluga i iz prirucnog menija izaberite Ail Tasks -> Authorize.

Formiranje opsega IP adresa
Pre nego sto pomocu DHCP usluga pocnete da dodeljujete IP adrese klijentima, morate instalirati ove usluge i oformiti opseg adresa. Opseg (engl. scope) nije nista drugo do raspon adresa koje se mogu dodeljivati klijentima.
Da biste oformili opseg IP adresa, uradite sledece:

1. U administrativnoj DHCP konzoli pritisnite desnim tasterom misa server za koji zelite da oformite opseg adresa. Windows 2000 ce prikazati prirucni meni.
2. Iz prirucnog menija odaberite stavku New, a zatim stavku Scope. Windows 2000 de pokrenuti carobnjaka Create Scope. Pritisnite dugme Next.
3. U prozoru Scope Names od vas se trazi da unesete ime i opis opsega. Ime obavezno morate uneti, a opis - ako zelite. Pritisnite dugme Next.
4. Carobnjak ce prikazati prozor Address Range. Unesite pocetnu i krajnju IP adresu za raspon adresa koji zelite da formirate. Moracete da zadate i podmasku za mrezu. Mozete da je zadate preko broja bitova koje zelite da maskirate (na primer, 24), ili uobicajenom decimalnom notacijom, npr. 255.255.255.0. Pritisnite dugme Next.
5. Carobnjak ce prikazati prozor Exclusion Range. Mozete da zadate interval izuzetih adresa ukoliko unutar raspona IP adresa zelite da neke adrese budu stalne. O ovome samo vi odlucujete. Pritisnite dugme Next.
6. Carobnjak ce otvoriti prozor Lease Duration. Upisite vremenski interval vazenja IP adresa svojih DHCP klijenata, po cijem isteku klijenti treba da obnove najam. (Klijenti ce, u stvari, obnavljati najam u trenutku kada istekne polovina iznajmljenog vremena.) Bice vam ponudeno da predete na prozor Most Common Options. Odgovorite odrecno (No), a zatim pritisnite dugme Next. (Opcije koje se odnose na opseg obradicemo u

narednom odeljku.)
7. Pritisnite dugme Finish.

Posto ste obrazovali opseg adresa, treba da konfigurigete DHCP opcije koje cete proslediti svojim DHCP klijentima. Medu opcijama se nalaze IP adrese DNS servera, standardni mrezni prolaz i adresa WINS servera.
Iako na administrativnoj DHCP konzoli postoji 61 opcija koju mozete da podesite, nisu sve namenjene DHCP klijentima. Medu opcije koje cete najcesce koristiti spadaju:

-003 Router: Ovu opciju iskoristite da biste konfigurisali standardni mrezni prolaz za svoje DHCP klijente. Standardni mrezni prolaz je, u stvari, standardna skretnica koju ce klijenti koristiti onda kada do odredista nije poznat nijedan drugi put.
-006 DNS Servers: Ova opcija utice na to koje ce DNS servere klijenti koristiti za upite koji se odnose na prevodenje imena. Treba da imate na umu da za ovu uslugu mozete da zadate vise DNS servera, pa ipak de samo prvi server na listi odgovarati na upite. Tek ako on nije dostupan, upiti se prosleduju sledecem DNS serveru na listi.
-015 DNS Domain Name: Ovom opcijom zadajete ime domena koje ce vasi klijenti koristiti. Iako ce klijenti Windowsa 2000 vec imati ime domena, ova opcija se cesto koristi u heterogenom okruzenju u kome imate racunare koji rade pod Windowsom 9x, ali i one koji koriste Windows NT.
-044 WINS/NBNS Servers: Ovo je opcija za konfigurisanje servera za Windowsove usluge obrade imena na Internetu, odnosno servera NetBIOS imena. Klijentima Windowsa 2000 ova opcija ne treba, ali je morate koristiti svaki put kada imate racunar koji radi pod Windowsom 9x ili Windowsom NT. Opcija je zgodna i kada u organizaciji imate vise podmreza. Ovom opcijom mozete da kontrolisete kojim ce serverima za obradu imena vasi klijenti upucivati upite za prepoznavanje NetBIOS imena.
-046 WINS/NBT Node Type: Opciju 044 morate koristiti u sprezi sa opcijom 046. Ova opcija odreduje vrstu cvora u kome je racunar vaseg klijenta. Jos jednom naglasavamo da je ovo opcija samo za racunare pod Windowsom 9x i Windowsom NT, jer je klijenti Windowsa 2000 nece koristiti. Postoje cetiri vrste NetBIOS dvorova:
-B-node je cvor za neusmereno emitovanje podataka. Ova vrsta cvora ce zahtev za prevodenje imena uputiti sirom mreze.
-P-node je cvor za transmisiju podataka od jednog do drugog racunara. Ova vrsta klijenta ce za prevodenje imena koristiti samo NetBIOS server. Ovi klijenti nece slati upite svim racunarima u mrezi.
-M-node je cvor sa mesovitim nacinom rada. Klijent ce upit za prevodenje imena uputiti sirom mreze, pa ako ne dobije odgovor, onda ce stupiti u vezu sa serverom NetBIOS imena.
-H-node ce uraditi obrnuto. Najpre ce stupiti u vezu sa serverom NetBIOS imena, pa ako ostane bez odgovora, poslace upit za prevodenje imena svim racunarima u mrezi.

-047 NetBIOS Scope ID: Ova opcija vam dozvoljava da svoje NetBIOS klijente svrstate u opsege adresa (grupe). Samo de klijenti unutar istog opsega adresa moci medusobno da komuniciraju. Na primer, neka se Server.APPS i Server.MGMT nalaze u dva opsega adresa. Ova dva racunara nece mocli da vide jedan drugog na mrezi.

Kada zelite da konfigurisete opcije koje se odnose na opseg adresa, uradite sledece:
1. Prijavite se na server u svojstvu administratora.
2. Izaberite komandu Start/Programs / Administrative Tools / DHCP. Windows 2000 ce otvoriti administrativnu DHCP konzolu.
3. Razgranajte svoj DHCP server. Desnim tasterom misa pritisnite objekat Scope Options. Iz prirucnog menija odaberite stavku Configure Options. Windows 2000 ce otvoriti okvir za dijalog Configure DHCP Options: Scope Properties.
4. Potvrdite opcije koje zelite da primenite na svoje klijente i zadajte pojedinacne parametre u donjem delu ovog okvira.
5. Pritisnite dugme OK.

Slozenije DHCP opcije

Razmotrili smo standardne DHCP opcije, ali postoji i odeljak unutar DHCP opcija koji se odnosi na opseg adresa specificno namenjenih klijentima u mrezi Windowsa 2000. U okviru za dijalog Configure DHCP Options: Scope Properties mozete da pritisnete jezicak kartice Advanced a onda da izaberete opcije za pojedine vrste klijenata. Opcije koje se konfigurisu za klijente u mrezi Windowsa 2000 obuhvataju:
-001 Microsoft Disable NetBIOS Option: Ovom opcijom mozete klijentima u mrezi Windowsa 2000 da omogucite ili onemogucite koriscenje NetBIOS-a. Ako u okruzenju imate samo Windows 2000, ukljucite ovu opciju, jer NetBIOS opterecuje resurse. Ukoliko se nalazite u mesovitom okruzenju, sa racunarima koji rade pod Windowsom 9x ili Windowsom NT, verovatno cete ovu opciju iskljuciti (i omoguciti koriscenje NetBIOS-a),kako bi klijenti mogli medusobno da se vide
-002 Microsoft Release DHCP Lease On Shutdown Option: Ovom opcijom mozete uspesnije da uticete na trajanje najma IP adrese, omogucujuci klijentima da svaki put kada zaustave radunar oslobode svoje IP adrese.
-003 Microsoft Default Router Metric Base: Ovom opcijom odredujete u koliko skokova ova skretnica moze da isporuci paket podataka.
Kada zelite da podesite slozenije DHCP opcije koje se odnose na opseg adresa, uradite sledede:

1. U administrativnoj DHCP konzoli desnim tasterom misa pritisnite objekat Scope i iz prirucnog menija izaberite stavku Configure Options
2. Windows 2000 ce otvoriti okvir za dijalog Configure DHCP Options: Scope Properties. Pritisnite jezicak kartice Advanced. Otvorite padajucu listu Vendor Class i izaberite stavku Microsoft Windows 2000 Options.
3. Otvorice se prozor sa opcijama Windowsa 2000 koje se odnose na opseg adresa. Odaberite opcije koje zelite da podesite i pritisnite dugme OK.

HTTP/IP generatori

Ovi generatori su usko vezani za korišćenje interneta, tačnije postavlje web sajtova, praćenje protoka informacija na web sajtove.Koristi se za IIS,IP protokole, HTTP protokole itd.
IIS je skup servisa sa različitim konfiguracionim parametrima, ali postoji nekoliko zajedničkih postavki za sve IIS servise. Da biste ih videli, selektujte naziv svog servera na vrhu stabla konzole u iis.msc, kliknite desnim tasterom i izaberite opciju (prikazano na slici 17.5). Odavde možete da osposobite Direct Metabase Edits dok je IIS pokrenut, možete da koristite UTF-8 kodiranje u log fajlovima kao podršku za internacionalne i ne-ASCII karaktere, ili možete da konfigurišete MIME tipove.
1570 Windows Server 2003
Konfigurisanje globalnih svojstava servera za IIS
Treća globalna opcija za IIS servise tiče se postavljanja MIME (Multipurpose Internet Mail Extensions) mapiranja koje IIS Web servis šalje u pretraživače na klijentskim mašinama koje postavljaju zahtev za fajlom. Web serveri koriste MIME mapiranja prilikom slanja informacija o tipu fajla do pretraživača ili aplikacija za mail. Pretraživač ili aplikacija za mail mora da zna da li su informacije koje prima tekstualnog tipa, da li je reč o grafici, audio fajlu, izvršnom kodu ili ugra|enom fajlu koji za prikazivanje svog sadržaja zahteva drugu aplikaciju, kao što je Excel za čitanje tabelarnih podataka.
Ovde naznačene postavke za MIME tipove koriste se na svim sajtovima na sistemu. Mapiranja mogu da se podese i na nivou svih sajtova (All Web Sites level) ili za individualne sajtove. Me|utim, ako promenite MIME tip u glavnim svojstvima nakon modifikovanja istog MIME tipa na nižem nivou, konfiguracija u glavnim svojstvima prepisuje postavke na nivou sajta ili direktorijuma. Da biste izbegli zabune, na globalnom
nivou možete da zadržite podrazumevana MIME mapiranja, a modifikujete ih samo za individualne sajtove po potrebi. Ionako su podrazumevana mapiranja prikladna u većini situacija. Jedini izuzetak je situacija u kojoj želite da uklonite odre|ena mapiranja na globalnom nivou, kako biste sprečili korišćenje odre|enih tipova na nivou sistema. IIS opslužuje samo fajlove za koje je definisan MIME tip, osim ako niste kreirali džoker zapis
za mapiranje nedefinisanih tipova fajlova.
Ako bi trebalo da dodate, uklonite ili promenite MIME mapiranja na sistemu, kliknite dugme Mime Types na stranici sa globalnim svojstvima servera, kako bi se otvorio okvir za dijalog sa slike 17.6. Odavde možete da prikazujete, dodajete, uklanjate ili menjate mapiranja za ekstenzije fajlova za sve web sajtove i direktorijume.
TCP/IP servisi na serveru (IIS, NNTP, Telnet, SMTP, POP3 i FTP)

Konfigurisanje MIME tipova za sve IIS servise i sajtove

Konfigurisanje web servisa

Kada su globalne postavke servera ispravno konfigurisane, vreme je da pre|emo na objavljivanje sadržaja. U narednim sekcijama diskutujem o postavljanju Web i FTP sajtova na Vašem sistemu i o konfiguracionim postavkama za svakog od njih. Radi dalje diskusije, u ostatku ovog poglavlja, pretpostavljam da u svakom slučaju konfigurišete nove sajtove ili virtuelne servere.

Glavna svojstva web sajtova

Da biste postavili podrazumevane postavke i parametre svih web sajtova na sistemu, selektujte IIS server u konzoli iis.msc, proširite listu čvorova, selektujte Web Sites, a zatim iz menija Action izaberite opciju Properties. Trebalo bi da vidite stranicu sa svojstvima organizovanu u više kartica, poput one na slici 17.7. Svojstva koja su jedinstvena za individualne sajtove, kao što su identifikacione informacije web sajta prikazane na slici 17.7, nisu dostupne (zasenčene su) sa glavne stranice sa svojstvima. Kartica Service, prikazana na slici 17.8, nije dostupna sa stranica sa svojstvima individualnih web sajtova. Na ovoj kartici postoje dve nove karakteristike web servera. Podrazumeva se da se web servis pokreće u modu izolovanja radnog procesa, koji predstavlja novi model procesa za IIS 6. U modu izolovanja radnog procesa, aplikacijama je moguće dodeliti individualne radne procese, tako da se postiže bolja zaštita i pozudanost u pore|enju sa modelom u IIS 5. Me|utim, možete da izaberete da se web servis pokreće u IIS 5 izolacionom modu, ukoliko imate aplikacije koje se oslanjaju na IIS 5 model procesa i ispoljavaju probleme zbog kompatibilnosti. Biranje ove opcije zahteva restartovanje IIS-a.
Kartica Service na stranici sa svojstvima za čvor Web Sites
Mogućnost kompresovanja odziva na HTTP zahteve nije sasvim nova, ali je kod IIS 5 bila implementirana kroz ISAPI filter. Kod IIS 6, kompresija se implementira kao karakteristika servisa i može biti osposobljena zasebno za statičke fajlove ili dinamički kreirani TCP/IP servisi na serveru (IIS, NNTP, Telnet, SMTP, POP3 i FTP) sadržaj (aplikacioni fajlovi). Ako je kompresija osposobljena za statički sadržaj, kompresovani fajlovi se smeštaju u privremeni direktorijum, sa podrazumevanom lokacijom u \Windows\IIS Temporary CompressedFiles. Kompresovani aplikacioni fajlovi ne smeštaju se u privremeni direktorijum; kompresuju se u vreme kreiranja. Pomoću opcije HTTP Compression na kartici Service možete da naznačite različite privremene direktorijume i možete da ograničite veličinu direktorijuma.
U opštem slučaju, kada konfigurišete postavke koje se primenjuju za sve web sajtove, koristite druge kartice na glavnoj stranici sa svojstvima servera. Individualni sajtovi nasle|uju ove glavne konfiguracione postavke, mada postavke definisane na nivou sajta mogu da prevladaju postavke sa višeg nivoa. Na primer, ako ste za sve sajtove na serveru postavili ograničenje za maksimalnu propusnost od 64KB u sekundi, a zatim ste za individualni web sajt postavili da je maksimalna propusnost 16KB u sekundi, individualni web sajt ima propusni opseg u skladu sa sopstvenim postavkama, a globalna postavka se primenjuje na sve ostale sajtove (uskoro ću reći nešto više o ovom regulisanju propusnog opsega). Slično, anonimni pristup se osposobljava na globalnom nivou, a specifično onesposobljava za Administration sajt.

Sa takvom konfiguracijom, anonimni korisnici automatski imaju dozvolu pristupa za sve novokreirane sajtove, a individualni sajtovi mogu da se konfigurišu tako da zahtevaju drugačiju potvrdu autentičnosti.
Ostale postavke na stranici sa svojstvima čvora Web Sites objašnjavamo kasnije, u sekciji "Modifikovanje svojstava web sajta". Ako već posedujete sajtove koji su pokrenuti i konfigurisani, i promenite glavna svojstva za sve web sajtove, IIS Vam daje opciju da primenite te promene na postojeće individualne Web ili FTP sajtove na sistemu. Na primer, na slici 17.9 naznačio sam da bi sadržaj web sajta trebalo da istekne odmah za sve web sajtove na mom serveru. IIS mi ukazuje na to da je ta postavka u konfliktu sa postavkama za dva web sajta na sistemu.

HTTP port web sajta

Druga informacija potrebna Web Site Creation Wizardu jeste port koji će biti korišćen za novi web sajt. Port 80 je standardni port koji se inicijalno dodeljuje HTTP protokolu.Ako nameravate da hostujete javni web sajt, dostupan svima, koristite port 80.Pretraživači će pokušati da se povežu sa web sajtovima preko ovog porta kada korisnik unese URL. Me|utim, ako imate neke specifične potrebe ili želite da osigurate web sajt,možete da izaberete neki drugi port, izme|u 1 i 65535. Da bi se povezali na web server sa nestandardnim portom, korisnici moraju da znaju broj porta i da ga dodaju na na kraj URL stringa, kao u sledećem primeru:

http://www.redhilltown.com:9000/.

Ovo preusmerava korisnikov pretraživač koji pokušava da otvori HTTP sesiju na port 9000 umesto na podrazumevani port 80. Na primer, mom web sajtu možete da pristupite i sa http://www.minasi.com/ i sa http://www.minasi.com:80/, oba URL stringa su validna.

Zapisi naziva hosta

Jedinstvene IP adrese su ranije predstavljale način da se više web sajtova hostuje iz istog fizičkog okvira. Me|utim, kako IP adrese sve više postaju stvar komoditeta, ima smisla pridruživati više web sajtova istoj IP adresi i broju porta uz korišćenje nečega što se naziva nazivima hosta (host header names). Naziv hosta predstavlja način da uključite naslov hosta (npr. www.microsoft.com) u HTTP zaglavlje koje se prenosi do HTTP servera. Moderni pretraživači (nakon 1997.) ne kažu web sajtovima: "Molim Vas, dajte mi Vaše web stranice", već kažu: "Molim Vas, dajte mi Vaše web stranice - i inače, mislim da kontaktiram www.bigfirm.biz". Ovo je bitno zbog toga što jedan web sajt može da ima nekoliko naziva; na primer, ako unesete www.minasi.com, www.learnwindows.biz, ili www.windowsnetworking.info, u svakom slučaju dobijate moj web sajt. U ovom slučaju nije bitno koji URL koristite za dobijanje mog sajta. Ali, imajte na umu i da isti web server pokreće i sasvim drugi sajt, www.softwareconspiracy.com. Ako su IP adrese i brojevi porta isti za dva web sajta, kako IIS zna koji sajt želite da kontaktirate? On osluškuje zapis sa nazivom hosta kog šalje Vaš web pretraživač zajedno sa svojim HTTP zahtevom.

Kada klijentov pretraživač počne da otvara web sajt, on (podrazumeva se) traži IP adresu sa nazivom hosta iz URL-a i otvara TCP konekciju na portu 80. Kada se konekcija uspostavi, prenosi svoj zahtev za stranicom do servera i u zahtev uključuje naziv hosta. IIS traži taj naziv hosta, poredi ga sa nazivima u listi servera, a zatim reaguje u skladu sa tim vraćajući tačne stranice odgovarajućeg sajta. Ovo je brz i lak način za hostovanje više TCP/IP servisi na serveru (IIS, NNTP, Telnet, SMTP, POP3 i FTP) 1577 sajtova na jednom serveru, ali da bi sve ispravno funkcionisalo, klijenti moraju da koriste barem Microsoft Internet Explorer 3 ili Netscape Navigator 2. Svi koji koriste starije pretraživače bivaju preusmereni na podrazumevani web sajt.

Konflikti SSL-a i naziva hosta

Pomoću SSL-a web serveri i pretraživači mogu da održavaju bezbedne komunikacije. Ako ste ikada kupovali bilo šta preko Interneta, verovatno ste koristili SSL. Ne bi trebalo mešati SSL i nazive hosta. Ako planirate da koristite SSL, možete da postavite samo jedan naziv hosta za sajt, jer je naziv domena šifrovan u sertifikatu. Ako morate da hostujete nekoliko SSL sajtova iz istog okvira, koristite različite IP adrese. Definisanje pristupa za anonimne korisnike i putanje do fajlova na sajtu Sada ćete definisati lokaciju za fajlove ovog web sajta i da li ćete dopustiti pristup sajtu i za anonimne korisnike. Putanja je prilično jednostavna: unesete lokalnu putanju koju bi IIS trebalo da koristi za fajlove kada se neko povezuje na taj sajt. Ili, ako nameravate da hostujete svoj sadržaj na nekoj drugoj mašini u okviru organizacije, možete da unesete UNC putanju u formi \\nazivservera\nazivdirektorijuma. Ako izaberete opciju sa UNC putanjom, čarobnjak traži da unesete odgovarajuće kombinaciju korisničkog imena i lozinke potrebnu za uzimanje sadržaja sa ciljnog sistema. Ako želite da web sajt bude javno dostupan, neka opcija Allow Anonymous Access to This Web Site ostane potvr|ena. Ovim dopuštate povezivanje svih korisnika na web sajt bez ikakve provere autentičnosti. Me|utim, ako želite da sajt bude privatan, zaštićeni sajt, izbrišite potvrdu iz polja za pristup anonimnih korisnika. Specifične sigurnosne postavke koje možete da primetite prona|ite u sekciji "Modifikovanje svojstava web sajta", nešto kasnije u ovom poglavlju. Kliknite Next za prelazak na finalni ekran čarobnjaka.

Postavljanje dozvola za pristup web sajtu

Poslednji korak Web Site Creation Wizarda definiše dozvole za pristup ovom sajtu. Ovde definisane dozvole primenjuju se od početka sajta i automatski se prenose na sve poddirektorijume ispod sajta. Naravno, ove postavke uvek možete naknadno da izmenite, ili možete da postavite korisnički prilago|ene postavke za bilo koji poddirektorijum sajta. Sledi kratko objašnjenje svake dozvole pristupa:

Read (čitanje) Korisnicima omogućava čitanje fajlova sa web servera. U većini instanci, ova opcija će biti postavljena za početak (root) novog sajta. Primarni razlog za isključivanje ove opcije jesu situacije u kojima direktorijumi sadrže CGI (Common Gateway Interface) ili ISAPI (Internet Server Application Program Interface) aplikacije,

koje se obično smeštaju na nivou poddirektorijuma.
Run Scripts (Izvršavanje skriptova - kao za ASP) Ako bi trebalo da dopustite izvršavanje Active Server Pages (ASP) skriptova, uključite ovu opciju.
Execute (Izvršavanje - kao u primeru ISAPI ili CGI aplikacija) Ako bi trebalo da dopustite izvršavanje ISAPI ili CGI aplikacija, uključite ovu opciju. Kada je ova opcija uključena, implicitno uključuje i opciju Run Scripts.
Write (Upis) Ako se iz klijentovog pretraživača postavljaju novi fajlovi na web server, ili ako je potrebno upisati neke informacije u postojeći fajl (možda zbog registracije ili nečeg sličnog), mora biti uključena dozvola za upis. Ja više volim da postavljam ovu dozvolu na nivou poddirektorijuma, umesto za glavni direktorijum web sajta.
Browse (Pretraživanje) Ako korisnik ne šalje zahtev za specifičnim fajlom na web serveru (na primer, default.html) i ako na sistemu nije definisan podrazumevani dokument, IIS vraća HTML reprezentaciju fajlova i poddirektorijuma u rootu sajta. Osim u specijalnim okolnostima, ova opcija bi trebalo da bude isključena.
Kada postavite osnovnu zaštitu sajta, kliknite Next za kraj rada čarobnjaka, i nakon toga se kreira novi web sajt. Ako bi trebalo da objavite HTML sadržaj, možete da počnete sa postavljanjem potrebnih fajlova u direktorijum koji je definisan za TCP/IP servisi na serveru (IIS, NNTP, Telnet, SMTP, POP3 i FTP) 1579 potrebe novog sajta. Podrazumeva se da svi novi web sajtovi (osim ako niste promenili glavna svojstva za ovu opciju) traže fajl pod nazivom default.htm, default.asp, index.htm ili Default.aspx (tim redosledom), kako bi ga upotrebili kao podrazumevanu polaznu stranicu, i zato proverite da li je fajl koji želite da predstavite korisnicima po povezivanju na sajt ispravno imenovan. Pomoću klijentskih radnih stanicama, iz pretraživača testirajte sajt kako biste bili sigurni da ispravno funkcioniše.
Ne zaboravite NTFS dozvole! Kada anonimni web korisnik pokuša da pristupi sadržaju HTML fajla, JPEG ili sličnog fajla, NTFS tu osobu identifikuje kao korisnika sa imenom IUSR_nazivkompjutera. Ako ste zabranili pristup za takvog korisnika, onda ljudi sa Interneta neće moći da pristupaju Vašem web sajtu - IIS otvara okvir u kom bi trebalo uneti korisničko ime i lozinku.
Savet
Takodje, skript iisWeb.vbs koji se izvršava iz komandne linije možete da koristite za kreiranje
ili brisanje web sajtova, i stopiranje, startovanje ili pauziranje individualnih sajtova. Na primer,
da biste kreirali sajt pod nazivom Web Pizza, sa polaznim direktorijumom u F:\PizzaSite i
nazivom hosta www.Webpizza.com, koristili biste sledeću sintaksu: iisWeb /create F:\PizzaSite "Web Pizza" /d www.Webpizza.com. Ako ne želite da IIS odmah pokrene novi
sajt, na kraju linije navedite i opciju /dontstart.
Postavljanje

FTP/TCP generatori

FTP generatori služe, kao što im samo ime kaže, za praćenje protoka vezano za FTP sajtove,testiranje ovih sajtova, i razne druge mogućnosti.Iako se danas veliki deo

transfera fajlova na Internetu odvija preko HTTP-a, FTP i dalje predstavlja značajan protokol za podršku ako pokrećete javni web sajt, iz prostog razloga što ovaj protokol podržavaju skoro svi klijenti. Softver FTP klijenta razvijen je za skoro sve moguće kompjuterske platforme - uključujući mainframe i midrange sisteme. Klijenti koji ne mogu da primaju fajlove preko HTTP-a najverovatnije to mogu da izvedu preko FTP-a. Ali, FTP nije deo podrazumevane instalacije za IIS 6. Morate ga specijalno dodati pomoću Windows Components Wizarda. Više informacija o tome možete da pročitate u prethodnoj sekciji, kada smo opisivali instalaciju IIS-a. FTP servis koji se nalazi u okviru IIS-a 6 sada uključuje jednu veliku novu karakteristiku: mod izolacije korisnika (user isolation mode) ograničava korisnika samo na pristup njegovom matičnom direktorijumu. To je bilo dizajnirano za Internet Service Providers koji su klijentima dopuštali da postavljaju fajlove i web sadržaj na server. Me|utim, ponekad je korisno dopustiti, primera radi, korisnicima Macintosh ili Unix klijenara da pristupe svojim matičnim direktorijumima na fajl serveru preko FTP-a. U narednim primerima najpre postavljamo FTP sajt bez moda za izolaciju korisnika, a zatim postavljamo mod izolacije korisnika. Kao što će uskoro biti rečeno, FTP podržava virtuelne direktorijume,ali ne i nazive hosta, tako da se nekoliko FTP sajtova na istom serveru može konfigurisati jedino na različitim IP adresama ili različitim TCP/IP portovima.

Postavljanje glavnih svojstava za FTP sajtove

Kao i za web (HTTP) servise, IIS obezbe|uje niz stranica sa glavnim svojstvima pomoću kojih administratori mogu da naznače podrazumevane postavke za sve FTP sajtove. Da biste postavili glavna svojstva za sve FTP sajtove, kliknite desnim tasterom na direktorijum FTP Sites u panelu dometa u okviru iis.msc. Uz jedan izuzetak (kartica Service nije dostupna na nivou FTP sajta), stranice sa glavnim svojstvima su identične onima za individualne web sajtove. Informacije koje se primenjuju samo u kontektsu individualnih sajtova (kao što su postavke za identifikaciju ili za polazni direktorijum) zasenčene su i nedostupne iz stranica sa glavnim svojstvima. Postavke koje su definisane u glavnim svojstvima FTP sajtova nasle|uju se za sve nove I postojeće sajtove, osim ako za to svojstvo već nije bila definisana neka druga vrednost.Na primer, ako na nivou direktorijuma FTP Sites zabranite anonimni pristup, svi novokreirani sajtovi neće inicijalno dopuštati anonimni pristup. Me|utim, ako ste eksplicitno dopustili anonimni pristup za javni FTP sajt, ta vrednost ima veći prioritet od postavke na višem nivou. Kasnije, ako odlučite da resetujete glavna svojstva tako da se dopusti anonimni pristup, IIS će pitati da li želite da resetujete svojstvo Allow Anonymous za bilo koji individualni sajt koji trenutno ne dopušta anonimni pristup.Postoji jedna stranica sa glavnim svojstvima koja nije dostupna na nivou individualnih sajtova. Kartica Service, prikazana na slici 17.39, dopušta osposobljavanje postavke za regulisanje propusnog opsega za sve FTP sajtove. Nije moguće postaviti specifične paramtere za redukovanje opsega na individualnim FTP sajtovima, kao što je bilo moguće kod individualnih web sajtova. Više informacija o redukovanju količine propusnog opsega možete da pročitate u ranijoj sekciji, "Glavna svojstva web sajtova".

Kreiranje novog FTP sajta

Da bi se postavili FTP servisi u okviru Internet Information Servicesa, morate unapred da pripremite sledeće informacije:

l Sa koje IP adrese želite da FTP server osluškuje zahteve (ili bi trebalo da se odaziva na sve raspoložive IP adrese).
l Koji bi broj TCP/IP porta ovaj FTP server trebalo da osluškuje na prethodno naznačenoj IP adresi(ama). Obično je to port 21.
l Da li je za FTP sajt dopušten pristup radi čitanja, upisa ili oboje.
l U kom se direktorijumu smeštaju FTP fajlovi.

Kreiranje novog FTP sajta počinje uz pomoć čarobnjaka - u ovom slučaju, FTP Site Creation Wizard. Da bi se čarobnjak startovao, selektujte direktorijum FTP Sites na IIS serveru u panelu dometa u okviru alatke Internet Information Services. Selektujte komandu New/FTP Site iz padajućeg menija Action i čarobnjak će Vas provesti kroz neophodni konfiguracioni proces.
U prvom koraku, prikazanom na slici 17.40, traži se da unesete prepoznatljivi naziv pomoću kog ćete referencirati FTP sajt.

Da bi korisnici mogli da kontaktiraju FTP server, morate da dodelite IP adresu i broj TCP porta za servis radi osluškivanja dolazećih konekcija. FTP ne podržava nazive hosta. ^arobnjak podrazumeva da bi FTP server trebalo da osluškuje TCP port 21 za sve raspoložive IP adrese na sistemu. Ako je serveru dodeljeno više IP adresa (na primer, za interni i spoljašnji interfejs), možete da selektujete odre|ene adrese iz padajuće liste IP Address. Ili, ako će FTP sajt biti dostupan sa Interneta, ali ne želite da koristite podrazumevani port 21, možete da pridružite bilo koji broj porta izme|u 1 i 65535.

Savet

Promena broja porta za FTP sajt često je dobra ideja ukoliko se sajt koristi za objavljivanje ili primanje fajlova od izabranih klijenata, dobavljača, itd. Jedan moj klijent je donedavno koristio otvoreni FTP server (koristio je podrazumevani TCP port 21) i razni hakeri su njegov server koristili kao skladište za piratski softver. Ako su podrazumevane postavke zadovoljavajuće, kliknite Next za prelazak na sledeći korak FTP Site Creation Wizarda.

Ova verzija FTP-a može da preusmerava korisnike na njihove matične direktorijume i da im ograniči pristup samo na taj direktorijum. U prvom primeru nećemo uključivati izolovanje korisnika (to je i podrazumevana postavka). Kasnije ću diskutovati o karakteristikama moda za izolaciju korisnika i kako se mod konfiguriše. Kliknite Next za prelazak na sledeći korak.

Kada se FTP klijenti inicijalno povežu na server, biće usmereni na polazni direktorijum na sistemu i neće moći da pre|u bilo gde iznad tog polaznog direktorijuma. Za njih je taj polazni direktorijum u stvari "root" direktorijum. Taj direktorijum može da se nalazi na IIS serveru ili može da bude deljeni direktorijum bilo gde na istoj mreži. Iz root

direktorijuma možete da kreirate poddirektorijume po kojima će biti organizovani fajlovi za preuzimanje ili fajlovi koje bi korisnici sami trebalo da postave na server. Unesite odgovarajući naziv direktorijuma ili UNC putanju do njega i kliknite Next. Ako unesete UNC putanju, u sledećem koraku se zahteva da unesete korisničko ime i lozinku za IIS koji će se koristiti prilikom pristupa tom deljenom direktorijumu. U suprotnom, ako ste uneli lokalnu putanju, sledeći korak je finalni, kao što je prikazano na slici 17.44.Kada ste definisali kako se sajt može kontaktirati i koji direktorijum bi trebalo da koristi, poslednja stvar koju IIS mora da zna jeste da li bi trebalo da dopusti pristup sajtu radi čitanja, radi upisa ili oboje. Ponu|ene opcije su jasne same po sebi: ako FTP server koristite samo da biste korisnicima ili klijentima obezbedili fajlove za preuzimanje, onda je pristup samo radi čitanja zadovoljavajući izbor; ako bi korisnici trebalo da postavljaju svoje fajlove na server, onda selektujte pristup radi upisa; ukoliko je potrebno, možete da selektujete obe opcije. Kliknite Next za kompletiranje konfigurisanja sajta, i FTP Site Creation Wizard će kreirati sajt i odmah ga startovati. Ako čarobnjak prijavi neki problem, verovatno ste kreirali sajt sa IP adresom ili brojem porta koji se već koristi za neki drugi sajt. Sajt se i pored toga kreira, samo ne može da se startuje sve dok ne rešite problem i dok ručno ne pokrenete sajt pomoću menija Action ili kontekstnog menija za taj sajt.

Kada se sajt kreira, preostaje samo da se u polazni direktorijum postavi odgovarajući sadržaj. Moguće je postaviti od svega nekoliko fajlova do nekoliko hiljada fajlova. Ako imate veliki broj fajlova, verovatno ćete ih lakše kontrolisati ako ih organizujete u okviru neke logičke strukture direktorijuma. U svakom slučaju, postavite fajlove tako da ihkorisnici mogu lako pronaći. Tako|e, uobičajeno je da se za FTP sajtove sa većim brojem fajlova postavljaju index.txt i/ili readme.txt fajlovi u direktorijumima u okviru sajta, tako da korisnici razumeju kakvog je tipa sadržaj u okviru svakog direktorijuma. Na kraju krajeva, niko ne želi da do|e u situaciju da naga|a čemu služe fajlovi 8.3 ili šta stvarno znače nazivi direktorijuma.

Novi FTP sajt možete da kreirate i iz komandnog prompta pomoću skripta iisftp.vbs. Na primer, da biste kreirali novi FTP sajt pod nazivom Pizza Recipes sa polaznim direktorijumom f:\pizzarecipes koji osluškuje samo zahteve sa IP adrese 204.177.51.199, upotrebite sledeću sintaksu (sve u jednoj liniji): iisftp /create f:\pizzarecipes "Pizza Recipes" /I 204.177.51.199. Možete da izaberete neki drugi port umesto porta 21 pomoću opcije /b broj porta i dodajte opciju /dontstart kako biste sprečili startovanje sajta odmah po kreiranju. Opcije /isolation Local ili /isolation AD govore FTP servisu da kreira sajt u nekom od modova izolacije.

Modifikovanje svojstava FTP sajta

Iako FTP Site Creation Wizard odradi sjajan posao prilikom konfigurisanja funkcionalnog FTP sajta, postoje i neki dodatni parametri koje možete da podesite naknadno. Na primer, možete da kreirate logon poruku koja će se prikazivati prilikompovezivanja na sistem, ili možete da ograničite broj simultanih korisnika na sistemu. U bilo kom slučaju, da biste podesili parametre FTP sajta nakon kreiranja,

koristite stranice sa svojstvima FTP sajta. Zapamtite, ako želite da vidite postavke za sve FTP sajtove, koristite stranice sa glavnim svojstvima čvora FTP Sites.

Svojstva FTP sajta
Da biste otvorili stranice sa svojstvima za novi FTP sajt, selektujte ikonicu novog sajta u panelu dometa u okviru konzole iis.msc, a zatim izaberite opciju Properties iz menija Action.

Sa ove stranice sa svojstvima FTP sajta, možete da menjate parametre za sajt, definisane na sledeći način: Identification (Identifikacija) Ova grupa kontrola omogućava promenu "razumljivog naziva" sajta, IP adrese koju sajt osluškuje i broja TCP porta koji osluškuje. Podrazumevana vrednost za IP adresu (osim ako drugačije nije naznačeno prilikom kreiranja) je All Unassigned, tako da novi sajt osluškuje zahteve FTP korisnika sa svih IP adresa koje ne koristi neki drugi sajt na sistemu. Ako bi na istom serveru trebalo postaviti više FTP sajtova, svakom od njih dodelite drugu adresu ili podesite broj porta.Broj porta možete da promenite radi bolje zaštite sajta (na primer, ljudi neće znati da traže FTP server na portu 28,324) ili da biste mogli da hostujete više FTP sajtova na istoj IP adresi. U polje TCP Port možete da unesete bilo koju vrednosti izme|u 1 i 65535. Ipak, kada promenite broj porta, korisnici će morati da znaju koji port bi trebalo da koriste, jer softver FTP klijenta podrazumeva da se koristi port 21.

Connections (Konekcije)

U zavisnosti od kapaciteta i raspoloživog propusnog opsega na sistemu, možete da ograničite broj simultanih konekcija na serveru, kako bi se održale adekvatne performanse. Ako planirate da pokrenete veliki sajt sa velikom količinom saobraćaja, onda je opcija Unlimited najbolji izbor. Ako ste odlučili da ograničite broj simultanih konekcija, korisnici koji pokušaju da se povežu nakon što je dostignuta definisana granica, dobijaju poruku greške (koju sami možete da definišete na stranici sa glavnim svojstvima.
"Konekcija" - barem sa stanovišta IIS-a - ne mora obavezno da se odnosi na sve aktivnosti jednog korisnika. Na primer, korisnik koji se poveže na FTP sajt preko pretraživača može istovremeno da preuzima više fajlova sa sajta. U tom slučaju,svaka sesija za preuzimanje pojedinačnog fajla ne predstavlja konekciju. Zbog toga, ograničavanje servera na pet konekcija ne mora nužno da garantuje da će pet korisnika istovremeno moći da pristupi sajtu u bilo kom trenutku; jedan korisnik može da zauzme mesta za svih pet konekcija.

Ako planirate da za FTP sajt dopustite pristup radi upisa, i znate da nikada nećete imati više od par istovremenih korisnika na FTP serveru, možete da razmotrite mogućnost ograničavanja sistema na jednu ili dve konekcije. Ako neko sa Interneta otkrije kako da pristupi Vašem server i počne da ga koristi kao skladište za piratski softver ili pornografiju, verovatno će početi da reklamira njegovu lokaciju. Ovakvim graničavanjem konekcija barem svodite na minimum potencijalnu zloupotrebu sistema.
Da biste bili sigurni da korisnici neće ostati povezani sa serverom do u beskonačnost,

unesite time-out vrednosti u polje Connection Timeout, u sekundama.Podrazumevani timeout interval iznosi 900 sekundi ili 15 minuta. Ako iz nekog razloga FTP sesija ne uspeva pravovremeno da zatvori svoje konekcije, ovim ćete se osigurati od toga da fantomski otvorene konekcije ne zatrpaju server.

Enable Logging (Osposobljavanje beleženja aktivnosti)

Jedan od najboljih načina za praćenje svega što se dešava na sistemu jeste beleženje svih aktivnosti.Potvrdom opcije Enable Logging (podrazumevana vrednost je uključeno) omogućava beleženje aktivnosti na sajtu u tri formata: Microsoft IIS Log Format,
W3C Extended Log File Format ili ODBC Logging. U zavisnosti od izabrane opcije, klikom na dugme Properties dobijate specifični niz parametara koji semože podesiti za svaki tip.

Current Sessions (Tekuće sesije)

Iako tehnički ovo nije parametar koji se podešava, ponekad možete da proverite ko je trenutno povezan na FTP server imožete da isključite neke ili sve korisnike koji su povezani na sajt. Klik na dugme Current Sessions vodi Vas u okvir za dijalog FTP User Sessions.
U ovom okviru za dijalog navode se svi korisnici koji su trenutno povezani na FTP server, zajedno sa dodeljenim IP adresama i trajanjem konekcije. Korisnici koji su anonimno povezani - ulogovani sa korisničkim imenom "anonymous" (o ovome će biti više reči u sledećoj sekciji) - imaće znak pitanja pored korisničke ikonice, i biće navedeni sa e-mail adresom koju su naveli u polju za lozinku sa FTP servera. Ako posetilac koristi Internet Explorer za anonimno logovanje, e-mail adresa može da se prikaže kao IEUser@ ili IE40user@, u zavisnosti od verzije Explorera koju koristi. Ikonica će imati mali znak pitanja preko lica. Korisnici koji su se ulogovali preko stvarnih korisničkih naloga za Windows Server 2003 imaće normalnu korisničku ikonicu pored svog korisničkog imena. Ako želite da isključite bilo kog korisnika sa sistema, selektujte njegov zapis i kliknite dugme Disconnect. Za isključivanje svih korisnika sa sistema (na primer, ako se pripremate na isključivanje sistema zbog
održavanja), kliknite dugme Disconnect All.

TIM VRHUNSKIH PREVODILACA PREVODI ZA VAS SA I NA SLEDEĆE JEZIKE:
ENGLESKI, FRANCUSKI, ŠPANSKI, NEMAČKI, ITALIJANSKI