

UTP Kablovi

Kabl je medijum kroz koji se prenose informacije između mrežnih uređaja i računara. Postoji nekoliko tipova kablova koji se upotrebljavaju u mrežama. U nekim slučajevima u mreži će se koristiti samo jedan tip kabla, dok će se u drugim mrežama upotrebljavati više različitih tipova. Izbor kabla je vezan za topologiju mreže, protokol i veličinu mreže. Razumevanje karakteristika različitih tipova kablova i toga kako oni utiču na druge aspekte umrežavanja je veoma bitno za projektovanje kvalitetne mreže.



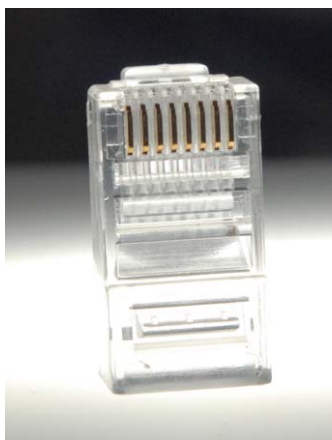
Slika 1. Neoklopljen UTP kabl



Slika 2. Kabl sa RJ45 konektorom

Neoklopljen kabl sa upletenim paricama / engl. Unshielded Twisted Pair (UTP) cable

Kablovi sa upletenim paricama postoje u četiri izvedbe: oklopljeni i neoklopljeni. Neoklopljeni (UTP) kabl je najpopularniji i obično najbolje rešenje za školske mreže. Iskustvo govori da je, ukoliko to sredstva dozvoljavaju dobro upotrebiti oklopljeni kabl za vertikalno kabliranje (STP kabl, kod koga je svaka parica obavijena metalnom folijom radi zaštite od spoljašnjih elektromagnetnih zračenja). Veze između spratova prolaze kroz svakakve građevinske konstrukcije, pa je zgodno obezbediti se. Kvalitet UTP kabla može varirati u zavisnosti od prečnika parice i kvaliteta i debljine njene izolacije. UTP kabl koji obično srećemo primenjen u računarskim mrežama je sastavljen od četiri para žica (parica) unutar gumenog omotača. Svaki par žica je upleten kako bi se smanjilo preslušavanje. Što je korak upredanja parice manji (više upletena), veća mu je otpornost na interferencije, a i cenu mu raste.



Slika 3. RJ45 Konektor

Konektor za UTP kabl

Standardni konektor za UTP kabl nosi oznaku RJ-45. On je nalik konektoru RJ-11 koji ste videli na svojim telefonima, sa tom razlikom što prima osam umesto četiri provodnika. Montiranje konektora na kabl je posao koji zahteva adekvatan alat, strpljenje i iznad svega kvalitetan kabl (ne pomišljajte da štedite na kablju). Povezivanje računara vam može uništiti žice ukoliko je kabl kineske proizvodnje i veoma niske cene. Plastificirane žice koje bi trebalo da izgledaju kao izolovani provodnici se stalno razmiču i praktično ih je nemoguće ubaciti u konektor. Čak i onome ko ima pet godina iskustva u montiranju konektora na kablove je potrebno oko 5 minuta za oba kraja kabla. Sa nekvalitetnim kablom to vreme raste i na 15 minuta, a o škartu i da ne govorimo. Namontirani delovi se ne mogu ponovo koristiti, već ih je potrebno odseći.

Da bi ste montirali konektor na kabl potreban vam je i alat. Potrebna su vam još jedna, dodatna modularna klešta kojima je moguće menjati umetke. Nabavite umetak za RJ-45 i tek tada krenite u pravljenje kablova, bez njih NE MOŽETE. Celi postupak je objašnjen u filmu koji imate u dodatku. Kao što se u filmu vidi, bitan je i raspored žica. Od početka je bitno držati se standarda. Ako budete pravili kablove, treba i da se snalazite među njima. Kada pogledate kabl treba da znate da li je prav (strait) ili ukršten (cross over). Tu dolazimo i do najčešćeg pitanja i najčešće greške. Da li se mogu dva računara povezati kablom bez upotrebe switcha? Mogu, ali kabl nije isti. Za direktno povezivanje dva računara se koristi tzv. Cross-Over kabl.



Slika 4. Obična klešta za RJ45



Slika 5. Modularna klešta sa umetkom za RJ45

Na slici sa leve strane su data profesionalna klešta za krimpovanje i mrežni tester koji se upotrebljava za proveru ispravnosti veza.

Šeme za oba kabla su vam date u prilogu.

Jedna od stvari na koju je potrebno obratiti pažnju kada pravite kabl za povezivanje dva računara, direktno, za ostvarivanje Gigabitne veze, kabl se malo razlikuje jer se koristi svih osam žica. Raspored žica ovog kabla je takođe dat u prilogu.



Slika 6. Tester za kablove

Oklopljeni kabl sa upletenim paricama /engl. Shielded Twisted Pair (STP) cable

STP kabl se sastoji od parica, od kojih je svaka obmotana metalnom folijom (tzv. ekran) da bi se sprečili spoljašnji elektromagnetni uticaji (efekat preslušavanja nastao elektromagnetnom indukcijom od signala iz susedne parice, spoljašnji elektromagnetni uticaji i dr.). Nedostatak UTP kabla je što je osetljiv na ove uticaje, dok STP kabl to nije. Kada je potrebno razvući kabl kroz neku energanu ili roentgen odeljenje bolnice, ili kada se kablovi računarske mreže vode kroz iste kanalice sa drugim telekomunikacionim i energetskim kablovima koristi se STP kabl. On je malo krući i teže je montirati konektore na njega, a i RJ-45 konektori su za ovu namenu oklopljeni i malo drugačije izgledaju, čak je i raspored izolovanih provodnika drugačiji.

Aktivna mrežna oprema

Nakon uvoda u pasivnu mrežnu opremu, na red dolazi opis uređaja koji će upravljati saobraćajem na mreži. To su takozvane aktivne komponente. Neke su sofisticiranije od drugih, ali imaju istu namenu, da podatke koje šaljete transportuju do odredišta, kao i da podatke koje vi potražujete dopreme do vas. Povezivanjem aktivne mrežne opreme kablovima još uvek nije napravljena računarska mreža, jer ona podrazumeva i konfigurisanje mrežne opreme.

Ako izuzmemo iz jednačine sam tip prenosnog medijuma, aktivni uređaji su manje više isti. Razlikuju se po broju portova, modula, tipu mreže za koji su projektovani, ali je filozofija koja stoji iza njih ista.

Još jedna stvar koju je što pre potrebno razjasniti je terminološke prirode. U mrežama postoji pojam PORTa koji se javlja u dva različita konteksta. Prvi predstavlja fizički konektor koji postoji na mrežnom uređaju ili računaru u koji ubadate recimo mrežni kabl, dok je drugi kontekst logički i malo kompleksniji.

Naime, zamislite da od mesta A do mesta B imamo položen telefonski kabl kojim se povezuju centrale u gradovima. Vrlo je verovatno da će unutar tih kablova biti veliki broj manjih

kablova , tzv. parica . Kada bi smo koristili celi kabl za telefoniranje između dva grada, građani bi morali da čekaju da njihov prethodnik obavi razgovor, kako bi dobili vezu. Ovako, ukoliko parice obeležimo brojevima od 0 do 65534 imaćemo 65535 građana koji će istovremeno komunicirati. Na isti način svaka internet aplikacija ima port na kome funkcioniše. Web stranice koriste HTTP protokol koji radi na portu 80. Kada pozovete, recimo www.microsoft.com, Microsoftov server sa vašim računarom otvori komunikaciju na portu 80, dok ostali servisi , kao recimo MSN messenger funkcionišu nesmetano i obavljaju svoju komunikaciju na nekom drugom portu. Tako imamo više istovremenih komunikacija kroz istu liniju.

HUB

Hab (engl. Hub) spada u kategoriju zastarelih (engl. Legacy) uređaja koji ima vrlo jednostavnu ulogu a to je da, kao obično čvorište, sve što stigne od podataka na jedan od njegovih konektora (portova) prosledi svima (samo pojačano i očišćeno od šumova, tj. regenerisano) Ovi uređaji nisu više u upotrebi, osim u laboratorijskim uslovima gde ova njihova osobina dolazi do izražaja kada treba nadgledati saobraćaj na mreži.

S obzirom na veoma loše karakteristike ovih uređaja, male brzine (10Mbps) i podložnost koliziji podataka, treba ih izbaciti i zameniti sofisticiranijim svičevima.



Netgear Ethernet Hub. Sada već istorija.

SWITCH

Svič je uređaj koji ćete zasigurno njihova je uloga da regulišu saobraćaj na mreži. Možemo sve naše računare povezati na svič, a i svič na svič te tako proširiti našu mrežu. Razlika u odnosu na Hub, iako isto izgledaju, jeste da svič vodi računa o tome koji podatak kom računaru ili mrežnom uređaju prosleđuje. Svič je u stanju da razlikuje (identifikuje) uređaje koji su povezani na njega.

Ovaj uređaj funkcioniše na drugom nivou (Layer 2 uređaj, pogledati dodatak) što znači da je svestan svojih klijenata. Identifikator uređaja povezanog na svič je njegova fizička tzv. MAC (engl. Media Access Control) adresa.



Cisco Catalyst 2960 Layer 2 switch. Okosnica svake ozbiljne mreže

Ovakav način identifikacije uređaja možete poistovetiti sa automobilom. Svaki automobil ima broj šasije i registarsku tablicu. Po pravilu broj šasije se ne menja, a tablice se menjaju u zavisnosti od prebivališta. Oba ova podatka identifikuju jedan automobil. Kod svičeva nas interesuju samo unikatni brojevi, tj. brojevi šasije. Registarskim tablicama ćemo se baviti kod rutera. Kod mreža je MAC adresa broj same mrežne kartice (šasije automobila), mrežnog uređaja i data je u obliku :

00:1A:4D:7B:FA:84

MAC adresu svoje kartice možete doznati tako što ćete otići u Command prompt i izdati komandu ipconfig /all. Dobićete rezultat kao na slici:

```

Command Prompt

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . .           : NVIDIA nForce Networking Controller
    Physical Address. . . . .       : 00-1A-4D-7B-FA-84
    DHCP Enabled. . . . .           : No
    Autoconfiguration Enabled . . . : Yes
    Link-local IPv6 Address . . . . : fe80::dcf5:6493:28e6:6881%8(Preferred)
    IPv4 Address. . . . .           : 192.168.10.1(Preferred)
    Subnet Mask . . . . .           : 255.255.255.0
    Default Gateway . . . . .       : 192.168.10.20
    DNS Servers . . . . .           : 160.99.12.230
                                       160.99.12.224
                                       194.247.192.33
                                       194.247.192.1
    NetBIOS over Tcpip. . . . .     : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Description . . . . .           : VMware Virtual Ethernet Adapter for VMnet
    Physical Address. . . . .       : 00-50-56-C0-00-01
    DHCP Enabled. . . . .           : No
  
```

Rezultat komande ipconfig /all u komandnom promptu

Prva tri heksadecimalna broja su identifikator proizvođača. Ako potražite određene sajtove na internetu, moguće je da unesete MAC adresu, a da vam sajt vrati da li je karticu napravio Cisco, D-Link, Asus ili neka druga kompanija. Sledeća tri broja su serijski broj kartice. Trebalo bi da je ovaj broj unikatan, međutim zbog ekstremno velike proizvodnje, kineski proizvođači su jednostavno lepili jednu istu adresu na nekoliko hiljada proizvoda, te se može naleteti i na duplikat.

Svič prikupi sve adrese uređaja koji su uključeni u njegove portove i napravi tabelu gde uparuje port i MAC adresu. Na taj način zna da recimo sa porta 5 treba prebaciti neki podatak na port 12. I eto komunikacije!

Svičeve možete naći u nekoliko varijanti. Uglavnom se razlikuju po broju portova i po stepenu upravljivosti. Neupravljivi ili "glupi" svičevi su jeftini i prave se sa do, recimo 16 portova. U njih samo uključite uređaje koje želite da umrežite i nemate nikakvog uticaja na tok podataka.

Druga kategorija, tj. upravljivi svičevi imaju različite mogućnosti, kao što je kontrola opterećanja, protoka, podešavanje bezbednosnih parametara, međusobno povezivanje (stackovanje) i prave se sa min. 16 ili 24 porta, a maksimalno 48. Potreba za dodatnim portovima se rešava vezivanjem sviča na svič. Cena ovih uređaja je daleko veća od cene prethodne kategorije i oni se koriste za kičmu (engl. backbone) mreže.



Allied Telesyn AT-9724TS Layer 3 switch. Daleko jeftinije, ali podjednako pouzdano rešenje kao Cisco u ovoj klasi.

IP Adrese

Registarska tablica naših računara na internetu je tzv. IP adresa. Bilo bi potrebno jako puno prostora da objasnimo matematiku koja stoji iza ovih brojeva, pa ću probati da uprostim stvari..

IP adrese se dele na javne i privatne. Svaki računar na internetu, koji je javno dostupan, kao recimo `www.microsoft.com` ima svoju javnu i unikatnu IP adresu. Ta adresa se uparuje sa simboličkim imenom, jednostavnijim za pamćenje, pa je tako

`www.microsoft.com = 207.46.192.254`

Ovo možete i sami videti tako što odete u command prompt (Start->Run->kucate **Cmd** i pritisnete enter) windowsa i otkucate

`nslookup www.microsoft.com`

dobićete `207.46.192.254`

Ukoliko uradite suprotno

`nslookup 207.46.192.254`

dobićete `www.microsoft.com`. (na slici se dobija `wwwth2test1.microsoft.com` što je samo jedan od alijasa `www.microsoft.com`)

Kao da smo u telefonskom imeniku potražili Peru Perića i dobili njegov broj telefona. A onda, što je još lepše , pronašli vlasnika telefona na osnovu broja. Ovaj telefonski imenik interneta se zove DNS (domain name system). Sistem veoma kompleksno uvezanih servera sa jednostavnim namenom. Da nađe onoga ili ono što tražite. Zbog unikatnosti adresa, ovo je moguće. Zbog toga se ove adrese nazivaju JAVNIM.

Sve javne adrese se kupuju, te tako ne možete staviti bilo koju i postati vidljivi na internetu. Kada platite, provajder će vam dodeliti jednu ili više adresa iz opsega koji on poseduje.

Iz skupa svih adresa izdvojena su tri podskupa i proglašeni su za privatne. Računari sa ovim adresama se ne registruju na internetu pa ih možete koristiti za svoje školske mreže. Sada isto pravilo koje je važno za adrese na internetu biva aplicirano na našu mrežu. **Svaki računar u našoj mreži mora da ima unikatnu adresu iz opsega privatnih adrese.** Ti opsezi su sledeći:

Opsezi privatnih adresa	Početak opsega	Kraj opsega	Ukupno adresa
Opseg klase A	10.0.0.0	10.255.255.255	16 777 216
Opseg klase B	172.16.0.0	172.31.255.255	1 048 576
Opseg klase C	192.168.0.0	192.168.255.255	65 536

Klasa adresa se bira na osnovu broja računara za kojim nam trebaju adrese. Vidimo da u klasi A imamo na raspolaganju 16 777 216 adresa, što je , složićete se previše, te zaključujemo da ćemo u našim uslovima najčešće koristiti C klasu. Kod dodeljivanja adresa **OBAVEZNO**

preskočite adrese koje se završavaju na 0 i 255 (192.168.0.0 i 192.168.0.255). To su tzv, **adresa mreže i broadcast adresa**, koje su rezervisane.

Do sada smo utvrdili IP adresu naših računara i Subnet masku. Ako samo ova dva broja unesemo u naše računare, oni će početi međusobno da komuniciraju. Formirali smo tzv. LAN (lokalnu mrežu ili Local Area Network). Da bi naši računari dobili izlaz na internet, potrebno je da utvrdimo ko je naš RUTER, te tako dolazimo i do poslednjeg uređaja koji ćemo obrađivati, rutera.

ROUTER

Ruter predstavlja i tehnički najsavršenije rešenje na mreži. On povezuje uređaje u različitim zgradama, gradovima i kontinentima. Postoje varijante i varijante rutera sa jednom jedinom namenom, a to je da upravljaju saobraćajem preko različitih mreža povezanih različitim prenosnim medijumima. Ruter možete upotrebiti da spojite dva predstavništva firme u dva grada preko telefonske iznajmljene linije, bežične veze ili bilo koje druge.



Cisco 1841 modularni ruter.

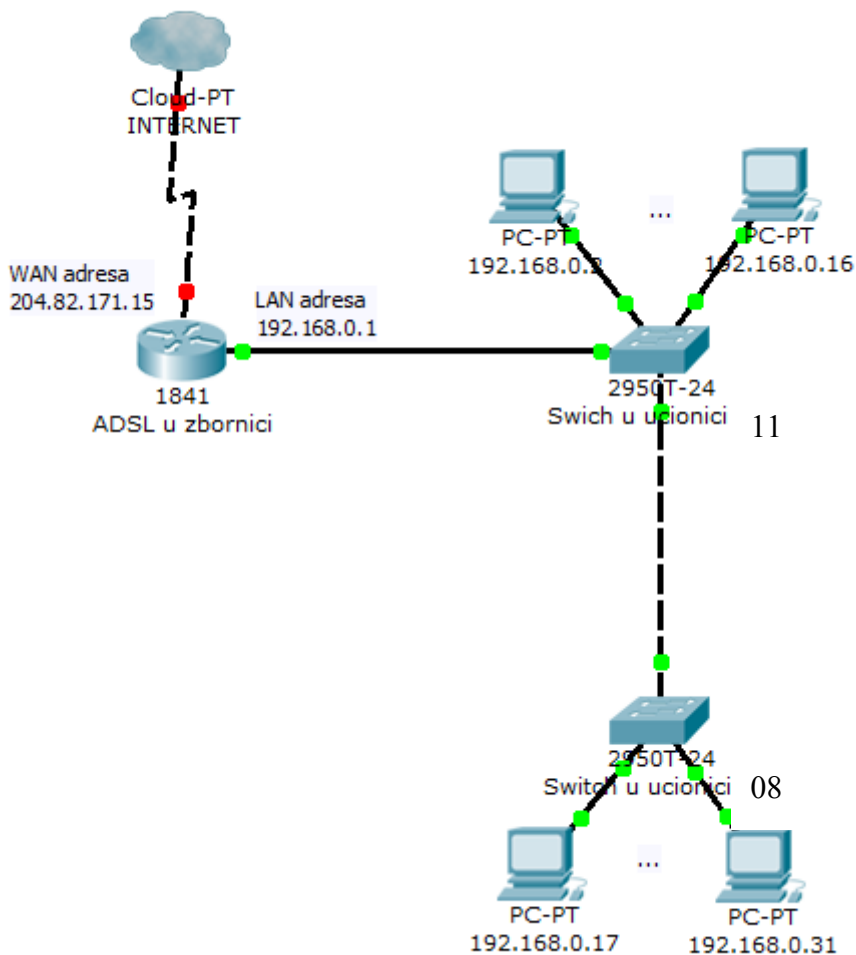
Kao što je ranije napomenuto ruter je uređaj koji reguliše saobraćaj na osnovu IP adrese klijenta, za razliku od svičeva koji su to činili na osnovu MAC adrese. Ako bi pokušali da uprostimo objašnjenje ove razlike, svič bi bio ekvivalent gradskog MUP-a koji je zadužen za regulisanje saobraćaja u svom gradu, dok bi ruter bio ekvivalent Republičkog MUP-a zaduženog da koordinira rad policije u svim gradovima.

MAC adresa ne može da se prostire van svoje mreže (učionice, škole). Svičevi mogu da se izbore sa saobraćajem dok ne naiđu na ruter koji spaja dve različite mreže. U dodatku imate primer naše škole. Unutar škole sve funkcioniše uz pomoć svičeva. Čim probamo da izađemo na internet, počinju da važe nova pravila.

Kao što možete videti na slikama, postoje različite verzije rutera. Ovi jeftiniji imaju jednu zajedničku karakteristiku, a to je da imaju odvojen tzv. WAN port (engl. Wide Area Network port, tj. port za vezu sa većom mrežom) koji je ili jedini zastupljen na uređaju, ili odvojen od druge grupe portova (kao na slici) koje nazivamo LAN portovima koji vode ka našim računarima i svičevima u školskoj mreži. WAN port može biti ADSL, običan Ethernet (mrežni) ili kablovski. LAN portovi su obični Ethernet svič portovi, kao na bilo kom drugom sviču. Poenta je u tome da ruter prevodi pakete sa LAN portova na WAN, označava ih i pušta kroz mrežu. Naš privatni poštar. Isto važi i za pakete koji pristižu iz spoljnog sveta. Oni dolaze na WAN port, tu bivaju dekodirani i prosleđeni jednom od naših 30 računara, na

osnovu "etikete", tj. adrese, koju nose. Uvek ćemo na WAN port dovesti internet vezu od našeg provajdera, a našu internu mrežu ukopčati u bilo koji od LAN portova.

Evo i šeme veze dva sviča i jednog rutera za našu školu.



U našoj mreži ruter je tačka preko koje mreža izlazi na internet. Ta tačka se naziva gejtvaj (engl. Gateway). Kod podešavanja parametara mreže bitno je definisati gejtvaj. Iz perspektive naše mreže, naš gejtvaj je 192.168.0.1. Prevođenje na javnu adresu radi sam ruter. Ako stavite da vam je gejtvaj 204.82.171.15, mreža sigurno neće raditi.



Linksys WRT54GL. Najbolji ruter SOHO klase (Small Office - Home Office). Pored klasičnog rutiranja ima i bežičnu vezu, firewall, kvalitet usluga (QoS). Jednom reči sve što i profesionalni ruteri samo za manje mreže

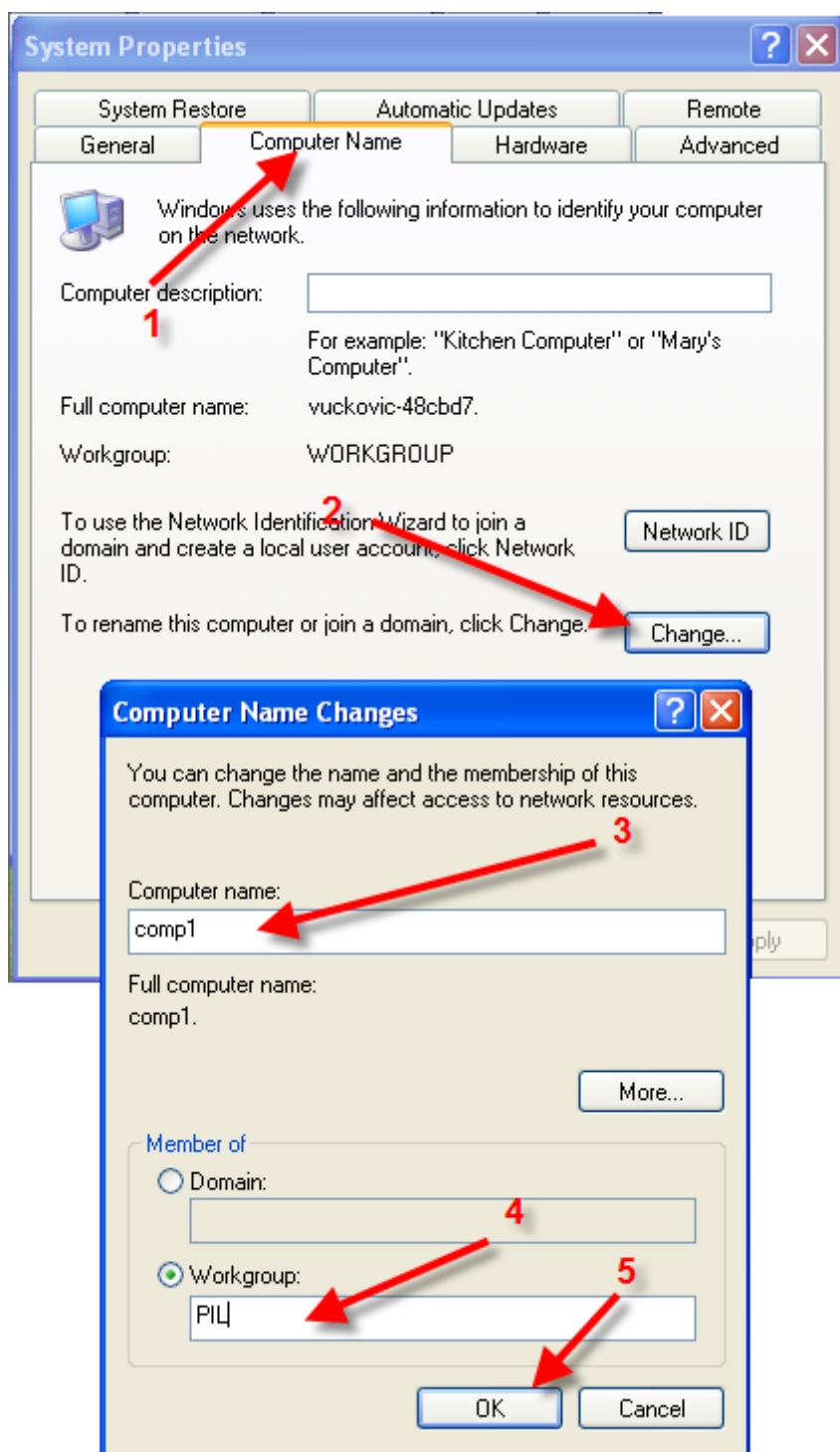
Na zadnjoj strani rutera jasno se vidi WAN port odvojen od četiri LAN porta.

Podešavanje IP adrese

Nakon što povežete mrežu, napravite kablove, podesite ruter i završite sve poslove koji uključuju trčanje unaokolo po školi, na red dolazi podešavanje parametara mreže. Postoji jednostavan način da se to uradi. Manje više svaki ruter ima opciju takozvanog DHCP servera, programa koji ima u sebi koji dodeljuje automatski parametre svim klijentima u mreži. Vaše je da ubodete kabl i uključite kompjuter. I radiće. Bez sumnje. Jedini problem je što će se adrese menjati u određenim vremenskim intervalima. Takva je koncepcija DHCP servera, da ukoliko mu eksplicitno nije rečeno vrši zanavljanje adresa svakih , recimo 8 sati. Da bi ovu stavku promenili, biće potrebno da se detaljnije upoznamo sa DHCPom.

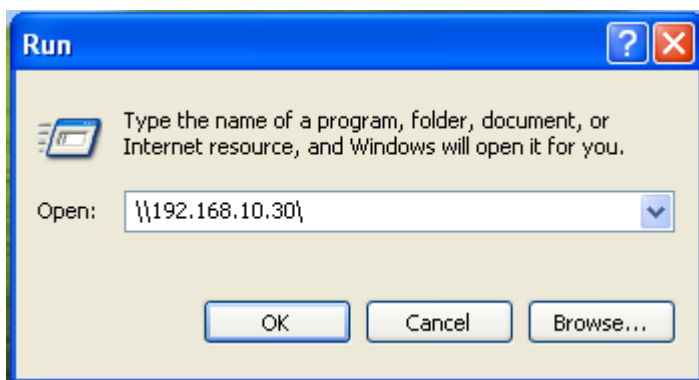
Nakon što je podešena IP adresa, potrebno je i podesiti radnu grupu kojoj računar pripada. To će nam omogućiti da upotrebom programa My Network Places vidimo susedne računare koji pripadaju istoj radnoj grupi.

Kliknite desnim tasterom na My Computer i izaberite Properties. U dijalogu koji se otvorio potrebno je odabrati jezičak **Computer Name**. Tu vidimo trenutno stanje, tj. koje je ime računara i radna grupa. Kliknite na **Change**. U novootvorenom dijalogu unesite ime i radnu grupu kojoj želite da računar pripada. Kod unosa radne grupe VODITE RAČUNA O VELIKIM I MALIM SLOVIMA. Radne grupe PIL, Pil i pil nisu iste. Proces je prikazan na slici :



Nakon promene imena, računar će se restartovati. Ukoliko ste sve obavili kako treba, nakon restartovanja aktiviranjem programa My Network Places, prikazaće Vam se ostali računari u učionici.

Upotreba My Network Places je u neku ruku ograničavajuća jer nećete uvek promptno dobiti spisak svih računara. Ovo zavisi od mnogo faktora, a najčešće od topologije mreže. Da bi ste direktno prozvali neki računar u mreži možete koristiti jedan trik. On se sastoji u tome da kliknete na START , pa RUN i unesete IP adresu računara kome želite pristupiti.



Na ovaj način možete uvek i odmah pristupiti bilo kom računaru na vašoj mreži , a i bilo kom računaru sa javnom IP adresom, koji administrativno dozvoljava pristup.

Protokol koji je zadužen za ovakav pristup resursima na mreži se naziva **NetBIOS**. On radi na TCP i UDP portovima 135 do 139, pa ukoliko branite svoju mrežu firewall -om, a želite od spolja da pristupate deljenim resursima, morate da otvorite ove portove

Deljenje dokumenata

Deljenje fajlova, ukoliko se pogrešno implementira može da bude ozbiljna bezbednosna rupa u mreži. Politika deljenja treba da bude što restriktivnija. Inicijalno podešavanje Windowsa je takvo da podržava tzv. Jednostavno Deljenje Dokumentata ili **Simple File Sharing**. U uputstvu koje je dato dole, prvo se isključuje ova opcija jer je potrebno imati potpunu kontrolu nad tim ko pristupa podacima i na koji način, za razliku od jednostavnog deljenja gde svi pristupaju svemu.

Opcija deljenja dokumenata je projektovana tako, da kod računara koji imaju NTFS fajl sistem, postoje dve linije odbrane dokumenata. Prva podrazumeva dodeljivanja prava pristupa dokumentima kroz mrežu. To su **Sharing** dozvole. Druga linija je sam pristup hard disku, odn. NTFS particiji.

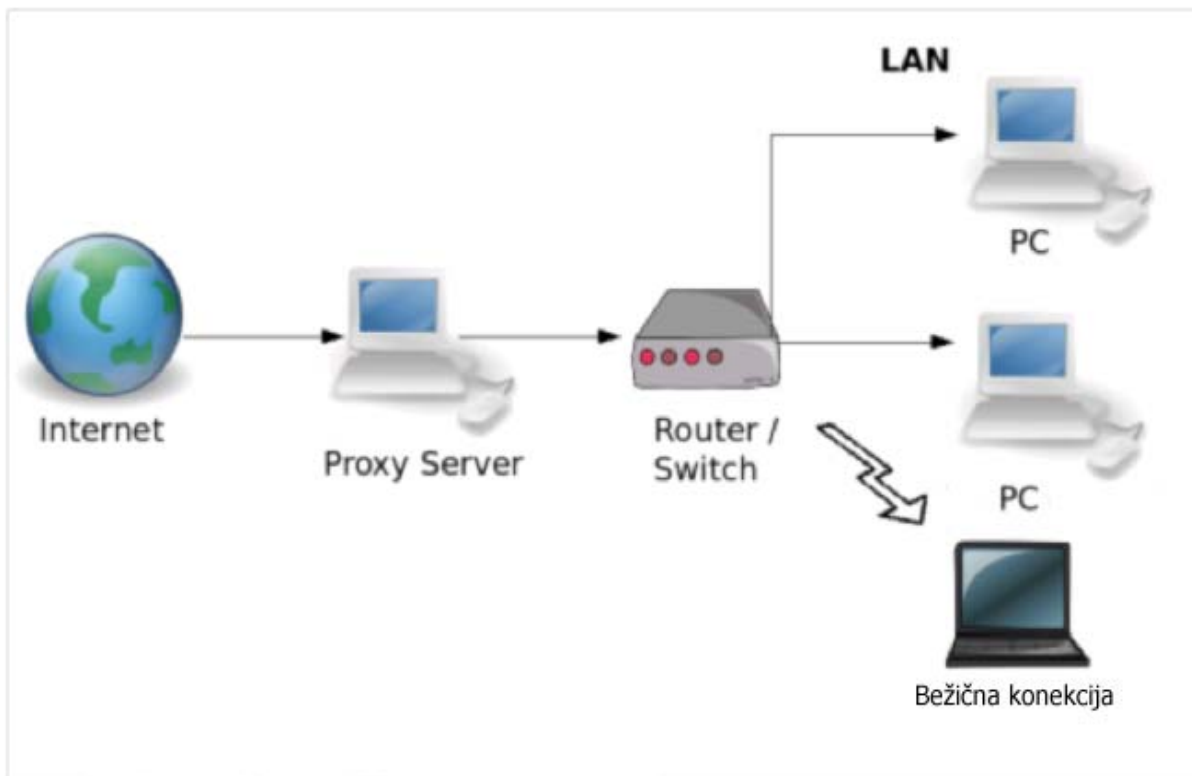
Podešavanje deljenja foldera objasnićemo na primeru novokreiranog foldera "MojDeljeniFolder" na C disku. Napravite ovaj folder i pratite uputstvo dato u instrukcionom filmu.

S obzirom da ova podešavanja zahtevaju više koraka, dato je video uputstvo. Za pregled Vam je potreban Adobe ShockWave Player. Njega možete preuzeti [ovde](#).

Šta je proxy server ?

U računarskim mrežama termin PROXY server se upotrebljava za označavanje servera (računarskog sistema ili aplikativnog programa) koji servisira zahteve svojih korisnika tako što prosleđuje zahteve drugim serverima. U engleskom jeziku termin proxy označava „posrednika“ . Klijent se povezuje na proxy server i zahteva neki servis, kao što je recimo dokument, konekcija, web stranica ili neki drugi resurs koji je na raspolaganju na nekom drugom računaru . Proxy omogućava upotrebu servisa tako što se povezuje na odgovarajući server i zahteva uslugu u ime klijenta. Ponekad proxy modifikuje zahtev klijenta ili sam odgovor servera, a ponekad može i da opsluži zahtev klijenta, a da uopšte ne kontaktira server.

Ovaj proces se naziva keširanjem i biće kasnije objašnjen. U prethodnim lekcijama nije posebno naglašeno da je gateway u suštini vrsta proxy servera koja prosleđuje zahteve klijenata serveru, ali nepromenjene. Ovakav proxy se obično naziva tunneling proxy. Proxy se može postaviti na više tačaka u mreži između korisnika i servera. Najčešća mu je pozicija pak, sam obod mreže.



Dodatak

Testiranje mreže

Nakon što ste obavili sve prethodno opisane radnje za povezivanje na internet, potrebno je i testirati mrežu. U tu svrhu ćemo koristiti alate koji se već nalaze u windowsu. Potrebno je da otvorimo command prompt. To se može postići, kao što je ranije opisano, klikom, na START, RUN, unosom naredbe CMD i pritiskom na ENTER.

Prvo je potrebno proveriti da li je naš računar dobro podešen komandom `IPCONFIG /ALL`. Rezultat ove komande dat je na slici:

```

C:\Windows\system32\cmd.exe

Ethernet adapter 192.168.10.1:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : NVIDIA nForce Networking Controller
    Physical Address. . . . . : 00-1A-4D-7B-FA-84
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::dcf5:6493:28e6:6881%3(Preferred)
    IPv4 Address. . . . . : 192.168.10.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.20
    DNS Servers . . . . . : 160.99.12.230
                           160.99.12.224
                           194.247.192.33
                           194.247.192.1

    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
    Physical Address. . . . . : 00-50-56-C0-00-01
    DHCP Enabled. . . . . : No

```

Ukoliko su svi parametri podešeni onako kako smo želeli, prelazi se na proveru konekcije ka susedima. Pošto je adresa ovog računara 192.168.10.1, proveravamo konekciju ka gejtvjeju koji je u ovom slučaju 192.168.10.20. Proveru vršimo upotrebom naredbe **PING <adresa gejtvjeja>** . Ova naredba šalje određeni broj paketa ka odredištu, u našem slučaju gejtvjeju i očekuje odgovor o njihovom prijemu.

```

C:\Windows\system32\cmd.exe

C:\Users\vuckovic>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:
Reply from 192.168.10.20: bytes=32 time=2ms TTL=64
Reply from 192.168.10.20: bytes=32 time=8ms TTL=64
Reply from 192.168.10.20: bytes=32 time=35ms TTL=64
Reply from 192.168.10.20: bytes=32 time=9ms TTL=64

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 35ms, Average = 13ms

C:\Users\vuckovic>

```

Na osnovu statistike koja je dobijena ovom komandom vidimo da su poslata četiri paketa ka odredištu, a i primljena su četiri pa je test 100% uspešan. Put paketa ka odredištu i nazad trajao je u proseku 13ms, što je malo više , ali u redu s obzirom da je reč o WiFi vezi na razdaljini od 3 kilometra.

Ukoliko odredište iz nekog razloga nije dostupno, odgovor na PING komandu će biti :

```

C:\Windows\system32\cmd.exe

C:\Users\vuckovic>ping 192.168.10.30

Pinging 192.168.10.30 with 32 bytes of data:
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.10.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\vuckovic>

```

Poslednja komanda koja će biti obrađena, a može pomoći u dijagnostifikovanju kvarova na mreži je TRACERT, što je skraćenica od TRACE ROUTE (napomena: na Linuxu i Unix-u je ova komanda TRACEROUTE). Ako banalizujemo stvari, ova naredba će predstavljati našeg Ivicu i našu Maricu. Krenuće ka odredištu koje smo naveli i bacati kamenčiće uz put, tako da kada mi budemo pratili rutu kojom su prošli, tamo gde "prestaju kamenčići" tu je i kvar na mreži. Kada komanda naiđe na ruter na putu preko koga ne može da pređe počinju da se pojavljuju zvezdice. Tada znamo tačno mesto gde treba proveravati ima li problema.

Za primer ćemo uraditi trace web sajta Niškog medicinskog fakulteta. Ukućaćemo komadu TRACERT www.medfak.ni.ac.yu. Rezultat je dat na slici :

```

C:\Windows\system32\cmd.exe

C:\Users\vuckovic>tracert www.medfak.ni.ac.yu

Tracing route to wwserver.medfak.ni.ac.yu [160.99.41.2]
over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms    192.168.10.20
  2   20 ms   19 ms   16 ms   160.99.35.11
  3   17 ms   16 ms   18 ms   elfakban.elfak.ni.ac.yu [160.99.11.252]
  4   18 ms    3 ms    5 ms   wwserver.medfak.ni.ac.yu [160.99.41.2]

Trace complete.

C:\Users\vuckovic>

```

Na slici se vidi da je do odredišta bilo potrebno preći preko tri rutera. Prvi je lokalni gejtvej 192.168.10.20, drugi je gejtvej fakulteta 160.99.35.11, treći je gejtvej Univerziteta 160.99.11.252 i poslednji je samo odredište. Ukoliko pak, ne stignemo na cilj, odziv će biti ovakav:

```
C:\Windows\system32\cmd.exe - tracert 160.99.12.239

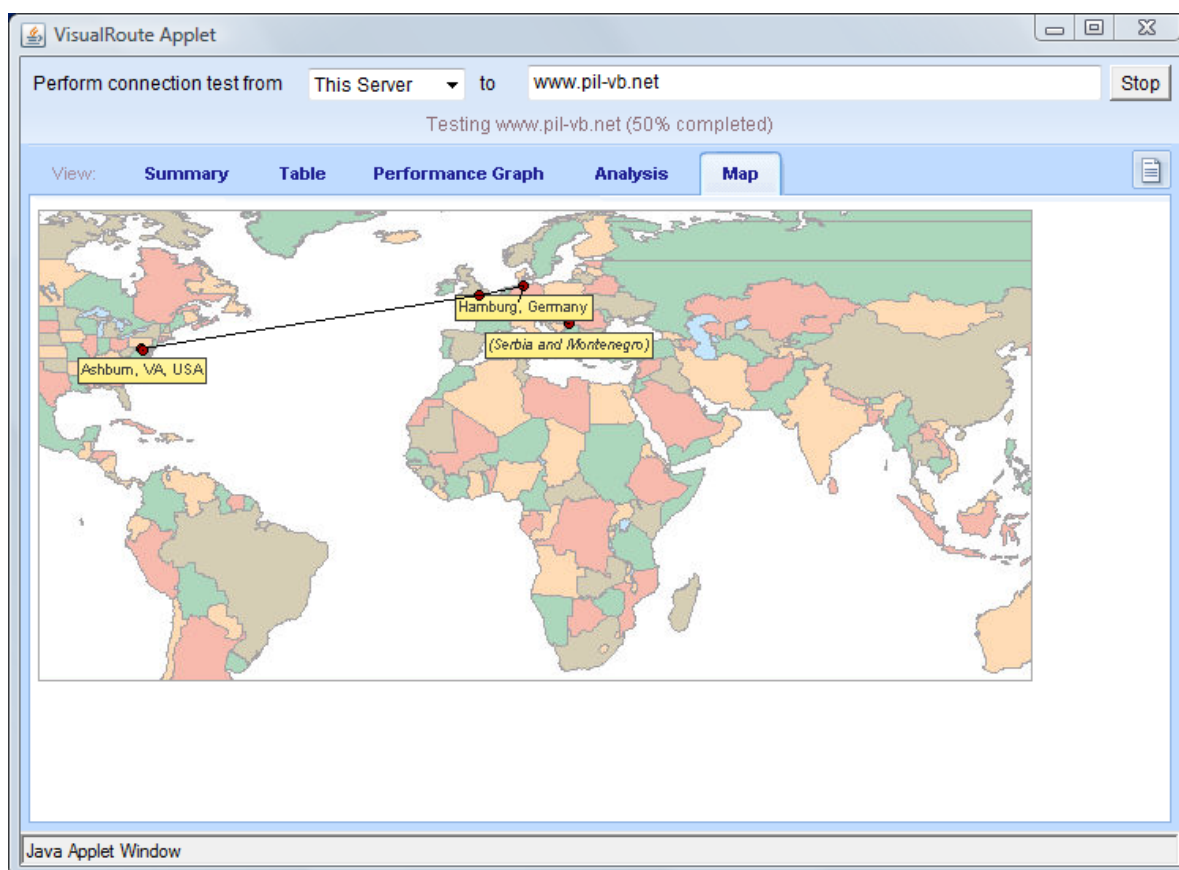
C:\Users\vuckovic>tracert 160.99.12.239

Tracing route to nebojsa.elfak.ni.ac.yu [160.99.12.239]
over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms   192.168.10.20
  1  16 ms   19 ms   19 ms   160.99.35.11
  2  *        *        *       Request timed out.
  3  *        *        *       Request timed out.
  4  *        *        *
  5  *        *        *
```

Na ovoj slici uočavamo da računar NEBOJŠA sa adresom 160.99.12.239 nije dostupan. Prošli smo lokalni gejtvej. Prošli smo gejtvej fakulteta i nakon toga više nema odziva. Na osnovu toga, najjednostavniji mogući zaključak bi bio da problem nije unutar naše zgrade, što je nekada dovoljno da Vam uštedi sate i sate rešavanja problema koji i nemate.

Na internetu postoji puno vizuelnih TRACE alata, kao recimo Visual Trace Route (<http://visualroute.visualware.com/>) koji će vam dati prikaz na karti preko kojih se sve rutera prelazi kako bi se došlo do odredišta. Možete trejsovati od sebe ka drugima i sa američkog servera ka drugima. Rezultat je više nego očigledan:



Ovaj set alata je nezamenljiv u dijagnostifikovanju kvarova na mreži. Što pre naučite da ih uspešno koristite, brže ćete početi da otklanjate kvarove na mreži koji se svakodnevno javljaju.

PRAVA PRISTUPA FOLDERIMA - NAPREDNA PODEŠAVANJA

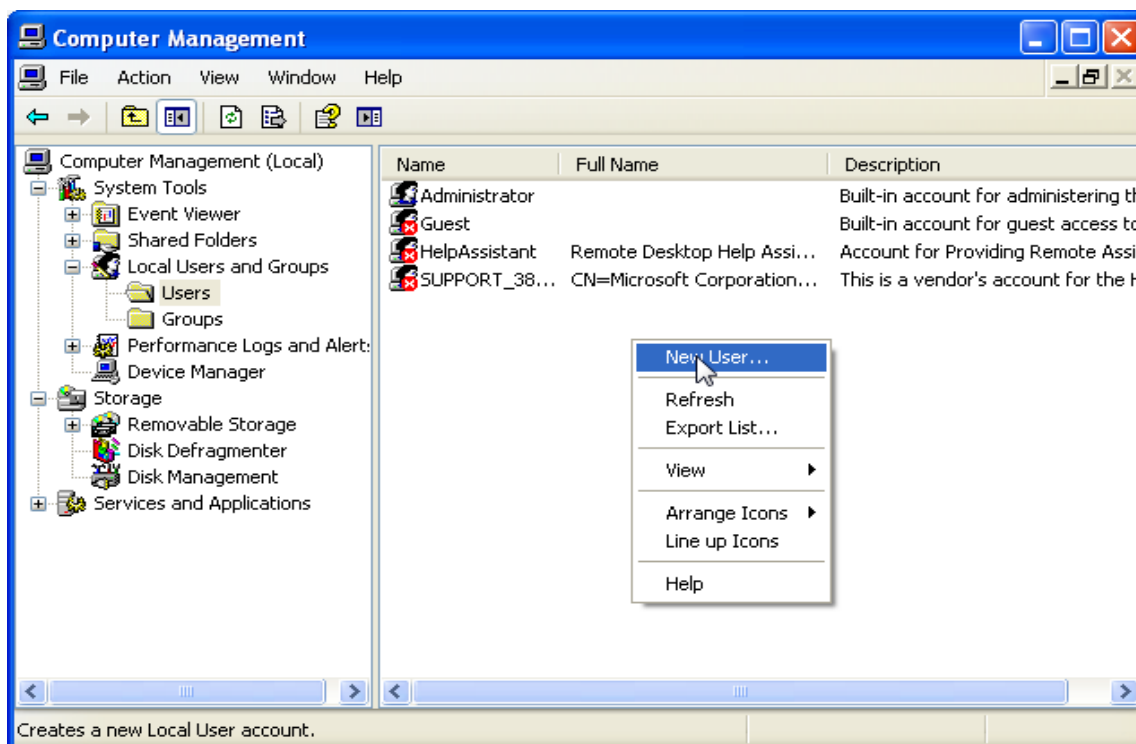
Podimo od scenarija da folderu MojDeljeniFolder želimo da ograničimo pristup. Želimo da se kad god neko pristupa tom folderu otvori dijalog koji će tražiti da unesemo korisničko ime i lozinku.

Redosled operacija je sledeći. Prvo je potrebno kreirati korisnika koji će imati pravo pristupa. Drugo, moramo postaviti lozinku za njega. Treća operacija se poklapa sa operacijom datom u odeljku "Deljenje dokumenata" i uključuje podešavanje prava pristupa folderu MojDeljeniFolder, pri čemu dozvoljavamo samo kreiranom korisniku da prođe.

Novi korisnički nalog kreiramo upotrebom Administrativnih alata kojima prilazimo na sledeći način:

START->Control Panel-> Kliknemo na "Switch to Classic View" sa leve strane prozora, ako postoji->Administrative Tools->Computer Management.

Došli smo u konzolu gde možemo podešavati parametre računara.



U levom delu prozora izaberemo **Local Users and Groups**. Nakon toga kliknemo desnim tasterom u desni deo prozora i izaberemo opciju **New User**.

Sada je potrebno popuniti upitnik za kreiranje novog korisnika. Na primer:

New User

Username: vuckovic

Full name: Dusan Vuckovic

Description: Administrator Sistema

Password: ●●●●●●

Confirm password: ●●●●●●

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

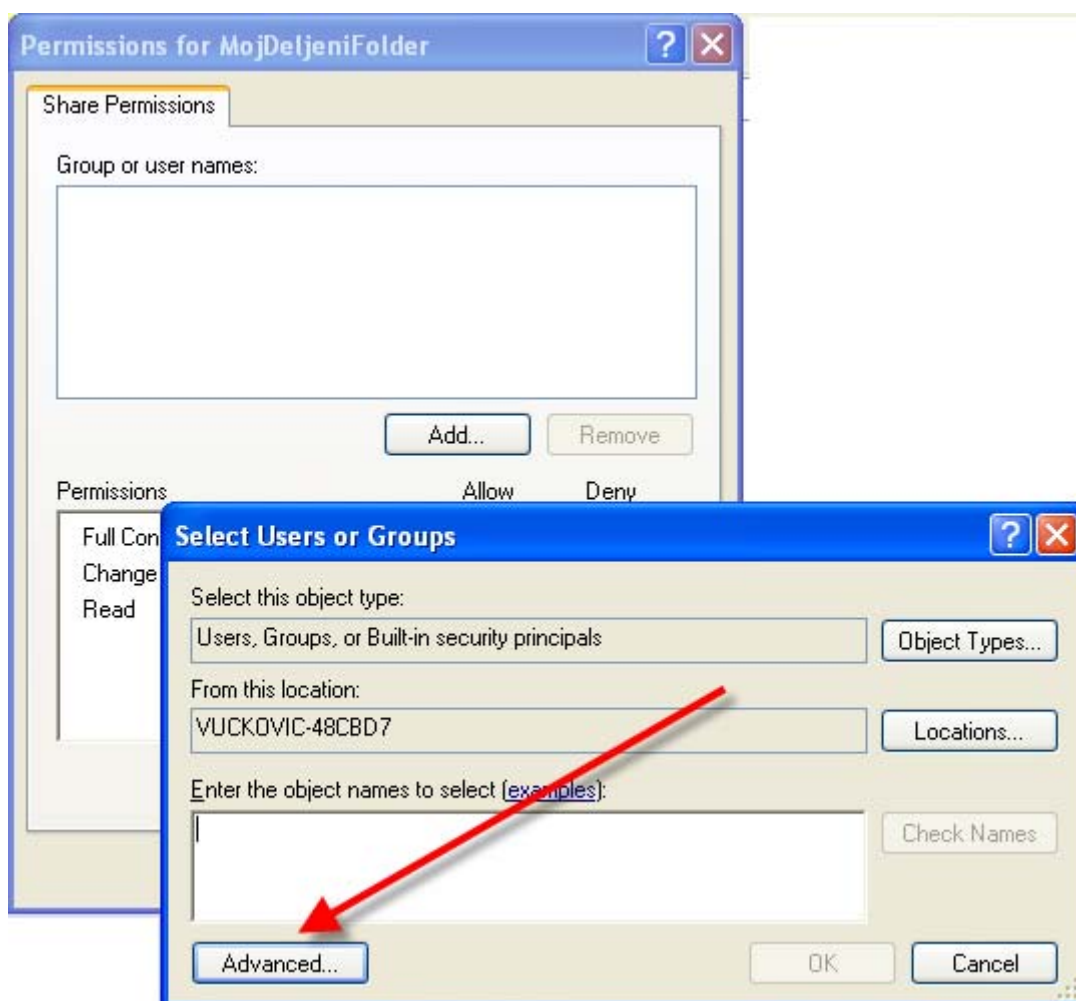
Create Close

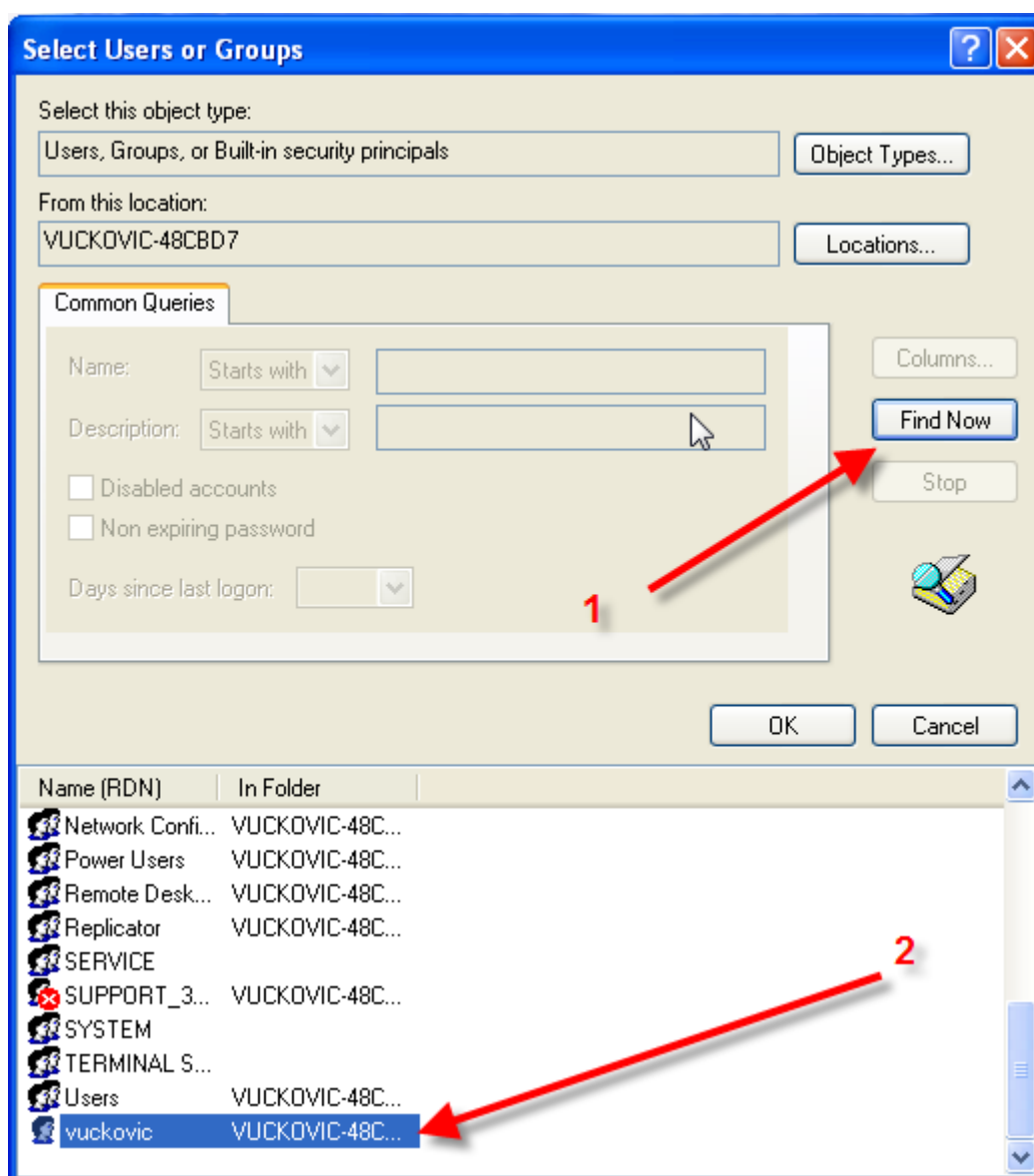
Unesite password, recimo 123456, a poželjno je neki jači. Microsoft obično koristi password "P@ssw0rd" kako bi demonstrirao koje karaktere bi sve trebalo da ima tzv. jaki password .

Poželjno je i uključiti opciju **Password never expires**, kako računar ne bi od nas tražio da menjamo lozinku prvi put kada se logujemo. Dakle, isključite **User must change password at next logon**, uključite **Password never expires** i kliknite na **Create**. Primetićete da novi korisnik pojavio u spisku korisnika.

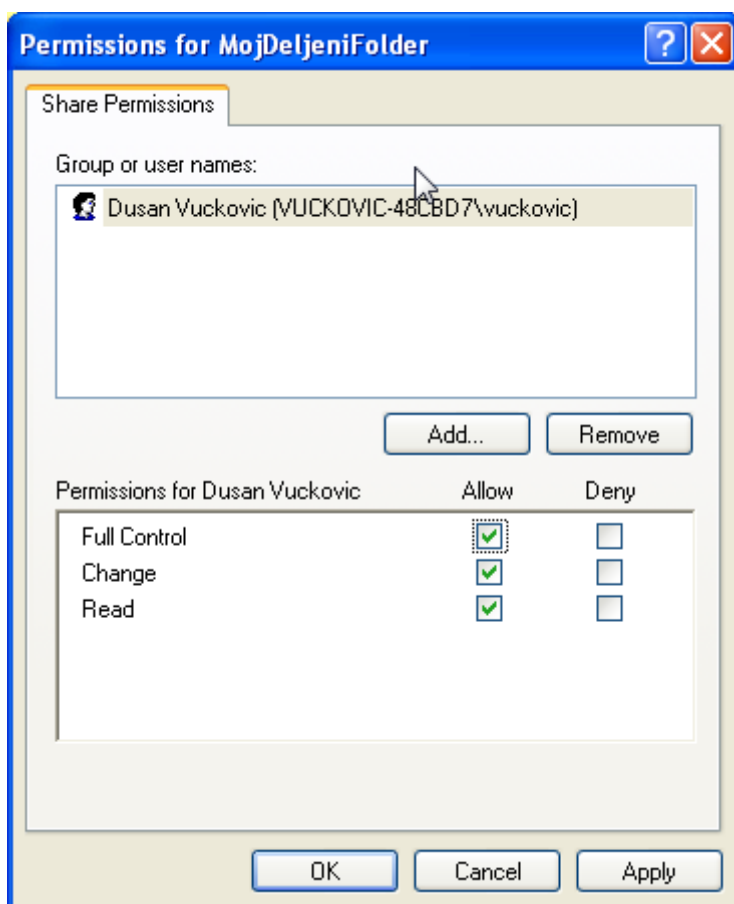
Sledeći korak uključuje podešavanje parametara deljenja foldera MojDeljeniFolder. Pronadite taj folder, kliknite desnim tasterom na njega i odaberite opciju **Sharing and Security** (podrazumeva se da ste isključili Simple File Sharing, kao što je u drugom odeljku lekcije objašnjeno).

Ukoliko već to nije urađeno, uključite opciju **Share this folder** i kliknite na dugme **Permissions**. Sada treba da podesimo da samo korisnik *vuckovic* ima pristup deljenom folderu. Obrišite sve korisnike iz spiska klikom na ime i upotrebom dugmeta **remove**, pa nakon toga dodajte novog korisnika klikom na dugme **Add**. Za razliku od prošloga puta kada smo direktno unosili korisnika kome želimo da odobrimo pristup, sada ćemo naučiti kako ga možemo pronaći u spisku svih korisnika. Kliknite na dugme **Advanced**, pa u novootvorenom prozoru na **Find Now**. Spisak će se pojaviti u donjem delu dijaloga. Pronađite korisnika kog ste kreirali, u našem slučaju *vuckovic* i kliknite na njega. Izbor potvrdite sa **OK** i još jednim **OK** da zatvorite Add dijalog.



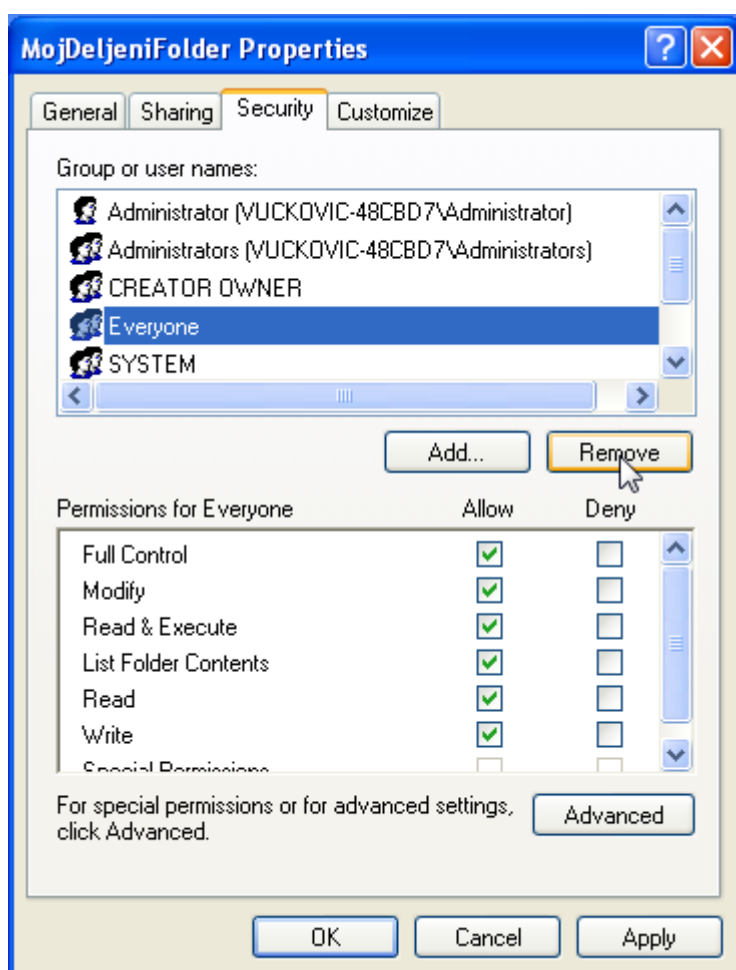


Nakon što ste potvrdili dodavanje korisnika, kliknite na ček boks **Full Control**, kako bi mu dali pravo da rukuje fajlovima;

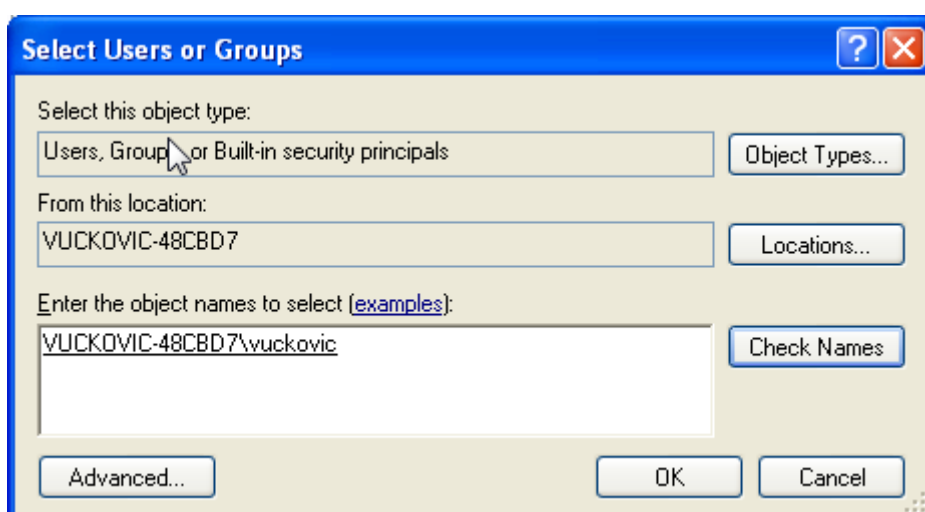


Zatvorite dijalog klikom na OK.

Istu ovu operaciju je potrebno ponoviti i za **Security** jezičak, kao što je opisano u drugom delu lekcije. Jedina razlika je u tome što nećemo brisati sve korisnike, već samo *Everyone*, ukoliko je na spisku. Pa tako, prvo brišemo *Everyone* sa spiska



,pa nakon toga, kliknemo na **Add** i gore navedenom procedurom dodamo korisnika *vuckovic* na spisak, na potpuno isti način ili ukucavanjem imena *vuckovic* i klikom na dugme **Check Names**, koje će proveriti imamo li tog korisnika u spisku i dodati ga ako je tako. Rezultat je isti .



Potvrdite vaš izbor sa OK dok se svi dijalozi na zatvore.

Obavljeni posao možete proveriti tako što ćete na drugom računaru u mreži kliknuti na START, pa RUN i ukucati

\\<adresa racunara na kome je deljeni folder>\MojDeljeniFolder,

kao recimo \\192.168.10.1\MojDeljeniFolder. Kad stisnete ENTER, ukoliko je mreža dobro podešena, pojaviće vam se dijalog koji će zahtevati da unesete korisničko ime i lozinku. Nakon što unesete *vuckovic/123456* pojaviće vam se sadržaj foldera. Time smo okončali podešavanje deljenja foldera.