Fakulteta za elektrotehniko,
računalništvo in informatiko
Inštitut za avtomatiko
Laboratorij za obdelavo signalov in daljinska vodenja

Navodila za vaje pri predmetu Internetne tehnologije
VAJA 1

Dušan Gleich

Maribor, februar 2008

Vsebina

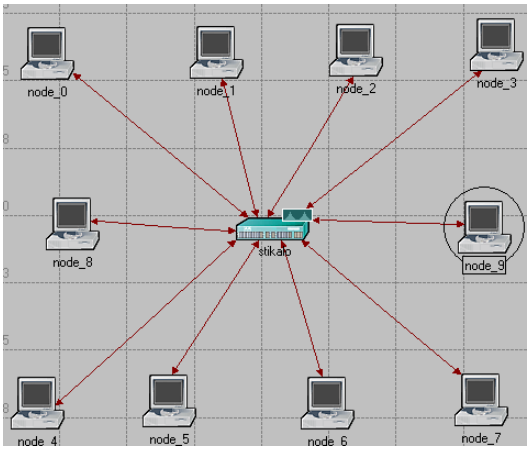
Vaja 1

Osnovni pojmi TCP/IP in protokoli

Delovna skupina

Pri teh vajah bomo uporabili operacijski sistem Windows XP Professional in osredotočili se bomo na del operacijskega sistema, ki ima opraviti z omrežjem. Omrežje je skupina med seboj povezanih naprav, ki si med seboj izmenjujejo informacije in upravljajo s podatki in mehanizmi varnosti. Omrežje je pomembno za izmenjavo podatkov in informacij. Pri teh vajah se omejimo na osebne računalnike (PC), ki so povezani med seboj. Če želimo več (več kot 2) računalnikov povezati med seboj potrebujemo usmerjevalnik ali stikalo. Poleg strojene opreme potrebujemo še programsko opremo, ki omogoči komunikacijo med računalniki s pomočjo protokolov, ki je v osnovi nabor pravil, ki jih komunikacijska naprava uporablja, da lahko komunicira.

Delovne skupine so tipične konfiguracije, ki jih najdemo v domačih omrežjih ali manjših pisarniških omrežjih. Takšno omrežje predstavlja nabor računalnikov (manj kot 20), ki si med seboj izmenjujejo podatke. Takšno omrežje nima strežnika, ki načeloma upravlja z administracijskim programom, ki nadzoruje dostop dostop do omrežja, vsak uporabnik lahko dostopa do svojih podatkov in upravlja z njimi, varnost je lokalnega značaja in delovna skupina se ponavadi nahaja na enem mestu.



Slika 1

Domena je namenjena za upravljanje računalnikov. Kadar se število računalnikov v delovni skupini poveča, se poveča tudi potreba po upravljanju s podatki, varnostjo in nastavitvami. Kadar se pojavi potreba po centralizirani organizaciji računalnikov uporabljamo domeno, ki se načeloma izvaja na strežniku, vendar to področje presega naš cilj vaj.

TCP/IP protokol

TCP/IP je nabor protokolov (več kot 100), ki zagotavljajo napravam dostop do omrežja, ki ga danes uporabljamo. Vse funkcije interneta nam omogoča TCP/IP protokol, od http, ki ga uporabljamo za brskanje po straneh, do IMAP, ki ga uporabljamo za dostopanje do e-pošte. Operacijski sistem Windows XP uporablja del TCP/IP protokola za upravljanje delovnih skupin in domen.
Za razumevanje TCP/IP protokola se moramo seznaniti z OSI (Open System Interconnection) modelom, ki ga je organizacija ISO (Organizacija za standardizacijo) predlagala leta 1978 in je zasnovan na t.i. nivojih, plasteh ali ang. Layer in definira kako naj delujejo strojne naprave in programska oprema, ki omogoča komunikacijo. OSI model tudi določa kako naj naprave med seboj komunicirajo.

OSI model določa sedem plasti, kjer vsaka plast določa del komunikacijskega procesa. OSI model določa fizično komunikacijo, ker se komunikacija izvede po fizičnem mediju od izvora do cilja.

Aplikacijski nivo ima opravka z določanjem stanja komunikacije med dvema aplikacijama. Njen cilj je določiti, če so podatki na voljo za vzpostavitev komunikacije med dvema ali več gostitelji (ang. host) in za odkrivanje računalnikov, ki so sposobni komunicirati. Obstaja mnogo protokolov, ki delujejo na tem nivoju, kot so na primer, Telnet, File Transfer Protocol (FTP), hypertext transfer protokol (HTTP). Http protokol definira kako se prenese informacija iz spletnega strežnika s pomočjo spletnega brskalnika. Naloga spletnega brskalnika je, da podatke prikaže. FTP protokol je bil izdelan za prenos in upravljanje datotek med računalniki povezani z omrežjem. POP (post office protocol) je ponavadi protokol, ki se uporablja za prenos e-pošte, ki je podprt z IMAP (Internet Message Access Protocol), ki je bolj učinkovit in varen kakor POP. Telnet je program, ki je bil izdelan za komunikacijo med računalniki. Je program, ki omogoča uporabnikom povezavo na strežnike.

Prezentacijski nivo je uporabljen kot prevajalnik za servise, ki se izvajajo v aplikacijskem nivoju. Ponavadi pretvarja podatke v standardizirane formate, da se lahko uporabijo v nižjih nivojih. Na tem nivoju delujejo protokoli za prenos in delitev datotek.
Nivo seje zagotavlja vzpostavitev povezave med dvema računalnikoma v treh korakih. V prvem koraku se vzpostavijo pravila za logično povezavo, v drugem koraku se določi kdo oddaja podatke in kako se bodo naslovili. Komunikacija lahko poteka, enosmerno, izmenično ali dvosmerno (simplex, half-duplex ali full duplex). Na tem nivoju delujejo protokoli Remote Procedure Call (RPC), ki se uporablja v client/server aplikacijah in NFS (Network File System), ki omogoča dostop do podatkov preko omrežja (mapiranje diskov in map)
Transportni nivo se v glavnem uporablja za razbijanje ali sestavljanje podatkov (segmentiranje) procesov in aplikacij, ki delujejo v nivojih 5-7. Na tem nivoju se večina podatkov razbije na manjše komponente ali segmente za prenos. Nivo 4 omogoča vzpostavitev logične povezave. Fizični prenos se dogaja na nivojih 1-3. Transportni nivo tudi omogoča prenos podatkov, ang. Flow control, kar pomeni da se podatki lahko pošljejo na sprejemniku sprejemajo tako hitro, kot se oddajajo, če pa ne prispejo na svoj cilj se ponovno pošljejo. Na tem nivoju se vzpostavi TCP in UDP protokol. Vrata ali ang.

port so logične nastavitve v TCP in UDP protokolih. Do TCP in UDP protokola še pridemo.
Omrežni nivo skrbi, da pridejo podatki na najboljši način iz enega mesta na drugega. Prav tako logično povezujejo naslove omrežij (kot npr IP naslove) s fizičnimi naslovi. Segmenti, ki se naredijo v transportnem protokolu se prenesejo na protokol in servise v omrežnem nivoju. Segmenti, ki imajo ustrezno informacijo o mrežnem naslovu imenujemo pakete. V omrežnem nivoju delujejo usmerjevalniki (routers), ki zbirajo informacije, kot so poti omrežij, kamor se usmerjevalnik poveže. Usmerjevalnik zgradi usmerjevalno tabelo omrežja in poskrbi za prenos podatkov. Protokoli na omrežnem nivoju so IP, ARP (Address Resolution Protocol), Reverse Address Resolution Protocol (RARP), Internet Control Message Protocol (ICMP).
Podatkovno-povezovalna plast, poskrbi da se podatki fizično prenesejo preko omrežja s pomočjo fizičnih naslovov, ki jih lahko definira uporabnik ali pa DHCP (Dynamic Host Configuration Protocol. Vsaka mrežna kartica pa ima svoj baslov MAC ali Media Access Control (MAC). TCP/IP protokol doda podatkovno povezovalni plasti informacijo o fizičnem naslovu k paketom iz mrežne plasti. Ko se ta podatek kodira v paket dobimo okvir.
Podatkovno povezovalna plast se deli v dva dela in sicer v Logical Link Control (LLC) in Media Access Control (MAC). LLC skrbi za povezavo med zgornjimi plastmi s časovnim upravljanjem prenosa in zagotavljanjem pretoka podatkov. MAC je odgovoren za ustvarjanje novih okvirjev, ki so sestavljeni iz binarnih signalov (0 in 1) in dodajanjem zaščitne kode CRC.
Fizični nivo ima nalogo upravljanje signalov in prenos preko vmesnikov in vodnikov omrežja.

Delovanje TCP/IP

Če želimo dobro razumeti delovanje TCP/IP moramo podrobno razumeti OSI model. Najbolj pomembne plasti so plast 3 (mrežna plast), 4 (transportna plast) in 7 (aplikacijska plast).

Protokoli v aplikacijski plasti

Vsakemu računalniku se dodeli naslov Internet Protocol (IP), kot npr. 194.168.7.4. Ker ima vsak računalnik v medmrežju in vsak strežnik v medmrežju svoj naslov IP si ljudje težko zapomnimo ta števila. V ta namen imamo DNS (Domain name System), kjer lahko IP naslove zamenjamo z bolj prijaznimi imeni. WINS je prav tako metoda za ugotavljanje imena računalnika, ki uporablja NetBIOS (Network Basic Input/Output System) protokol.
IP naslov računalnika je lahko statičen ali dinamičen. Za statičen naslov moramo vprašati našega administratorja, za dinamičen naslov pa skrbi DHCP mehanizem, ki deluje preko procesa, ki ga imenujemo leasing. Klient zahteva IP konfiguracijo in DHCP server alocira določen IP naslov za določen čas. Problem je, ker DHCP mora zagotavljati strežnik. V našem primeru bo DHCP zagotavljal usmerjevalnik. Kadar nimamo na voljo DHCP strežnika lahko uporabimo Automatic Private IP addressing (APIPA) in se ponavadi uporablja v lokalnih omrežjih.

Protokoli v transportni plasti

Transportna plast skrbi, da se podatki prenesejo iz enega računalnika na drugega.

Transmission Control Protocol (TCP)

TCP protokol je bil ustvarjen, za zagotavljanje varnega prenosa podatkov s pomočjo zaščitnih kodiranj in popravljanjem napak. TCP je protokol, ki je povezovalno orientiran, torej najprej se vzpostavi povezava z oddaljenim računalnikom, oddaljen računalnik potrdi povezavo in sprejme podatke.
V začetnem procesu vzpostavitve komunikacije računalniki uporabljajo TCP za določitev različnih parametrov kot so velikost segmentov in koliko segmentov se lahko prenese, preden se le-ti potrdijo na sprejemni strani. Ko se vzpostavi ta povezava TCP nadzoruje prenos podatkov. Med prenosom se lahko zmanjša prenos podatkov, prekine, segmenti se izgubijo, zato je pomembna kontrola podatkov. TCP lahko zmanjša velikost segmentov tako, da jih razdrobi in prilagodi pasovni širini.

User Datagram Protocol (UDP)

UDP zagotavlja funkcije Transpotrnega nivoja. Glavna značilnost je, da ko je vzpostavljena komunikacija z oddaljenim računalnikom se sproži prenos podatkov. Protokol ne nadzoruje prenosa podatkov, ni potrjevanja paketov. UDP je v primerjavi s TCP dosti krajši protokol (brez zaglavja), zato se uporablja v internetni telefoniji, DNS, SNMP.

Protokoli v mrežni plasti

Protokoli v mrežni plasti se v glavnem nanašajo na iskanje najboljše poti skozi omrežje. Obstaja nekaj pomembnih TCP/IP protokolov.

Address Resolution Protokol

Da se lahko podatek pošlje na določen naslov IP s pomočjo podatkovno povezovalnega protokola se mora najprej izvesti pretvorba MAC naslova v IP naslov.

Internet protokol (IP)

Vsak računalnik v omrežju ima svoj naslov IP. IP procesira sprejete segmente ali sporočila iz transportnega protokola kot sta TCP ali UDP. IP procesira pakete za dostavo v podatkovno povezovalne protokole.

Internet Control Message Protocol (ICMP)

Zagotavlja diagnostiko in poročanje o napakah v IP omrežjih

Naslavljanje Internet Protokola

IP naslov lahko razdelimo na 5 razredov (A, B, C, D in E). Razredi A, B in C določajo internet ponudniki, kot je prikazano spodaj

A	1.0.0.0	do	126.0.0.0
B	128.0.0.0	do	191.255.0.0
C	192.0.0.0	do	233.255.255.0

Razred D je rezerviran za pošiljanje na več naslovov, prejemnikov (multicasting) in razred E je rezerviran za raziskovalne namene. Vsako polje je naslovljeno z 8. Biti. Poleg IP naslova še moramo definirati masko podomrežja (subnet mask) in prehod (gateway).

Maska podomrežja (Subnet Mask)

TCP/IP omrežja so razdeljena v različna podomrežja. Vsak klient glede na svoj IP pripada določenemu podomrežju. Maska podomrežja pomaga računalniku, da ve kateri del IP naslova se nanaša na identifikacijsko število omrežja in kateri del se nanaša na kliente. Maska omrežja je 32 bitno število, ki se kombinira z IP naslovom. Rezultat definira identifikacijsko številko omrežja. Npr. če IP naslov 192.168.0.50 uporablja masko omrežja 255.255.0.0, v tem primeru število 192.168 identificira omrežje in 0.50 predstavlja klienta. V tem primeru se IP naslovi nahajajo v območju 0.1 in 255.254.

IP razred	
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0.0

Uporaba prehoda

Poleg IP naslova in maske omrežja še moramo poznati privzet prehod (ang. gateway). Včasih se zgodi, da klienti pripadajo določenemu podomrežju in morajo komunicirati s klienti, ki se nahajajo v drugem podomrežju. Klienti morajo poznati računalnik ali usmerjevalnik na katerega bodo poslali promet, ki zapusti lokalno podomrežje in potuje do naslednjega omrežja. Ta računalnik je znan pod imenom privzet prehod in je zelo pomemben za odhoden in dohoden promet.

Javni in privatni IP naslovni

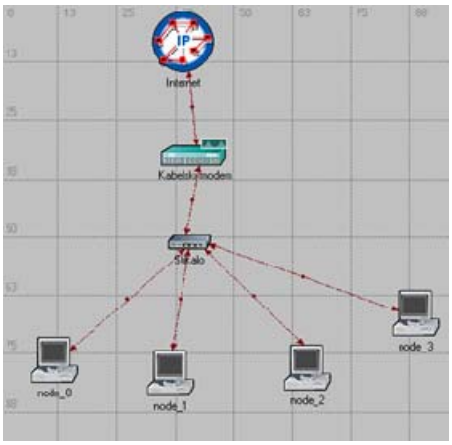
Definiramo lahko privatna omrežja, ki se povezujejo z usmerjevalnikom, ki ima javno dostopen IP naslov. Na ta način je tudi rešeno, da nima vsaka naprava javni IP, saj bi se na ta način št. IP naslovov drastično zmanjšalo Privatni IP naslovi se nahajajo med

10.0.0.0	do	10.255.255.255
172.16.0.0	do	172.31.255.255
192.168.0.0	do	192.168.255.255

Če želimo, da postani privaten IP naslov viden moramo uporabiti network address translation (NAT).

Zvezdišča (ang. hub)

Zvezdišča omogočajo komunikacijo med računalniki v omrežju. Vsak računalniku je priključen na zvezdišče z ethernetnim kablom in informacije, ki jih en računalnik pošlje drugemu, grejo skozi zvezdišče. Zvezdišče ne more prepoznati vira ali cilja prejetih informacij, zato jih pošlje vsem priključenim računalnikom, tudi tistemu, ki jih je poslal. Zvezdišče lahko pošilja ali sprejema informacije, vendar ne more početi obojega hkrati. Ravno zaradi tega so zvezdišča počasnejša od stikal. Izmed vseh teh naprav so zvezdišča najmanj zapletena in najcenejša.



Slika 2

Stikala (ang. switch)

Stikala delujejo na enak način kot zvezdišča, le da prepoznajo cilj prejetih informacij; tako te informacije pošljejo samo računalnikom, katerim so namenjene. Stikala lahko hkrati pošiljajo in sprejemajo informacije, zato je pošiljanje hitrejše kot v zvezdiščih. Če so v vašem domačem omrežju štirje računalniki ali več ali če želite omrežje uporabljati za dejavnosti, ki zahtevajo prenos velike količine informacij med računalniki (npr. igranje omrežnih iger ali skupna raba glasbe), namesto zvezdišča raje uporabljajte stikalo. Stikala so malo dražja od zvezdišč.

Usmerjevalniki (ang. router)

Usmerjevalniki omogočajo komunikacijo med računalniki in lahko prenašajo informacije med dvema omrežjema — npr. med domačim omrežjem in internetom. Prav po tej zmožnosti usmerjanja omrežnega prometa je usmerjevalnik dobil svoje ime. Usmerjevalniki so žični (z ethernetnimi kabli) ali brezžični. Če želite samo medsebojno povezati računalnike, lahko uporabljate tudi zvezdišča in stikala; če pa želite vsem računalnikom omogočiti dostop do interneta z uporabo enega modema, uporabite usmerjevalnik ali modem z vgrajenim usmerjevalnikom. Usmerjevalniki ponavadi omogočajo tudi vgrajeno varnost, kot je požarni zid. Usmerjevalniki so dražji od zvezdišč in stikal

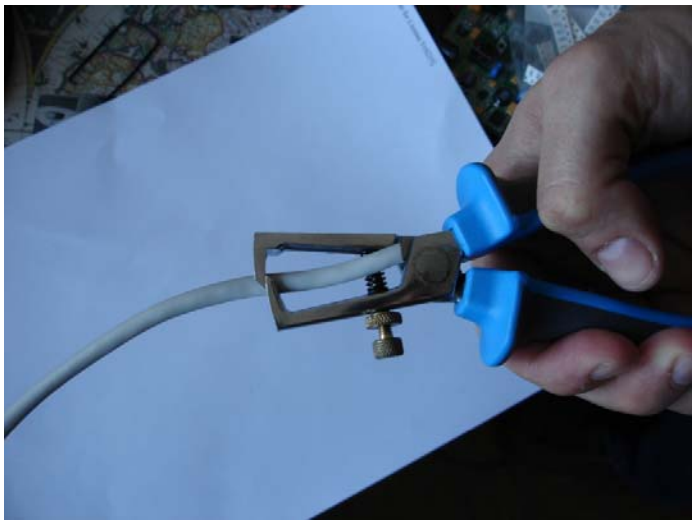
Vstopne točke

Vstopne točke (imenovane tudi *bazne postaje*) omogočajo brezžični dostop do žičnega ethernetnega omrežja. Ko vstopno točko priključite na zvezdišče, stikalo ali žični usmerjevalnik, začne pošiljati brezžične signale. Tako je računalnikom in napravam omogočeno, da vzpostavijo brezžično povezavo z žičnim omrežjem. Vstopne točke so po funkciji zelo podobne stolpom za mobilne telefone: lahko se premikate z enega mesta na drugo in imate vedno brezžičen dostop do omrežja. Ko vzpostavite brezžično povezavo z internetom prek javnega brezžičnega omrežja na letališču, v kavarni ali v hotelu, ponavadi vzpostavljate povezavo prek vstopne točke. Če želite računalnike brezžično povezati in že imate usmerjevalnik, ki omogoča brezžično možnost, ne potrebujete vstopne točke. Vstopne točke nimajo vgrajene tehnologije za skupno rabo internetnih povezav. Če želite imeti v skupni rabi internetno povezavo, morate vstopnjo točko priključiti v usmerjevalnik ali v modem z vgrajenim usmerjevalnikom.

Izdelovanje Ethernet vodnika

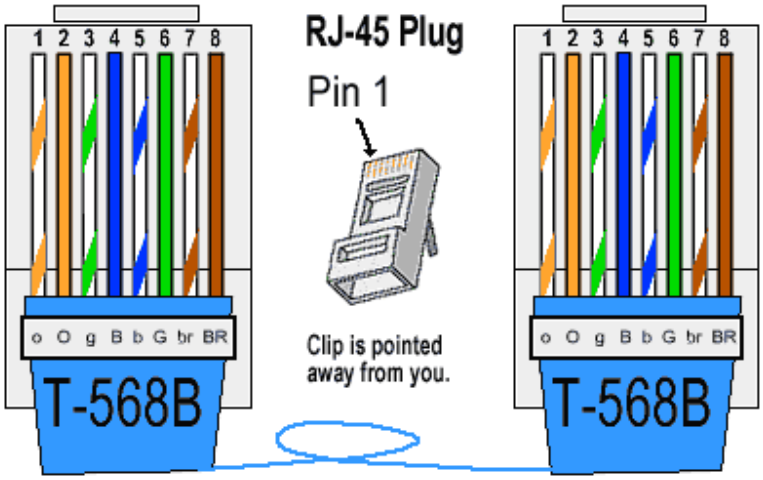
Za praktičen uvod v predmet internetne tehnologije je potrebno izdelati vodnik, ki ga bomo uporabljali za povezavo med mrežno kartico osebnega računalnika in usmerjevalnikom oz. stikalom. Izdelali bomo vodnik po standardu T-568B s priključkom RJ-45. Postopek izdelave kabla je prikazan na spodnjih slikah.

Snamemo izolacijo



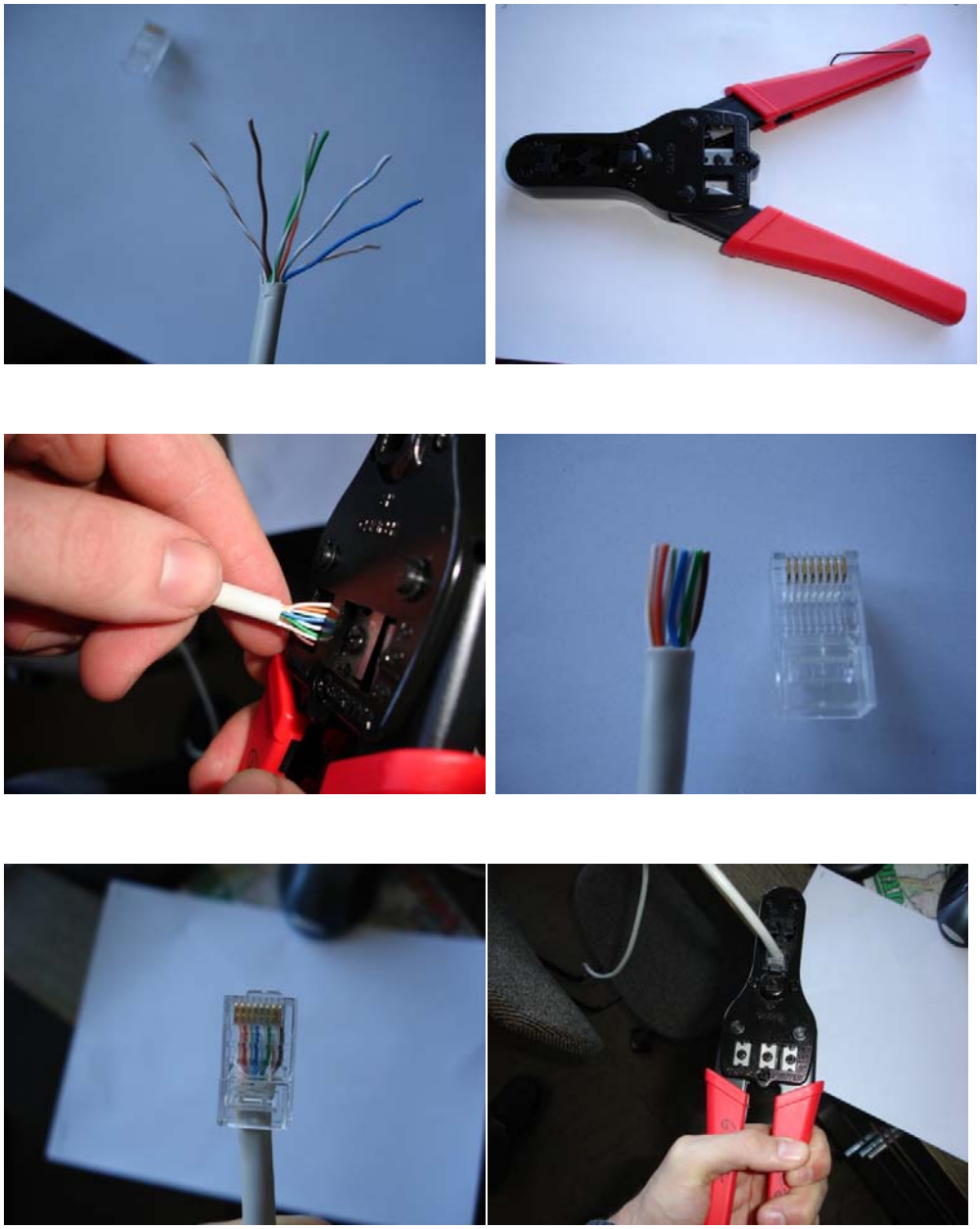
Slika 3

Razporedimo vodnike tako, kot prikazuje spodnja slika



Slika 4

Pri tem moramo paziti, da posamezne vodnike razvrstimo kar se da ob izolaciji vodnika, jih vstavimo v konektor RJ-45 in jih stisnemo s pomočjo klešč.



Slika 5

Nastavitev usmerjevalnika

Usmerjevalnik je tipa WRT54GL, proizvajalca Linksys in ga prikazuje spodnja slika.

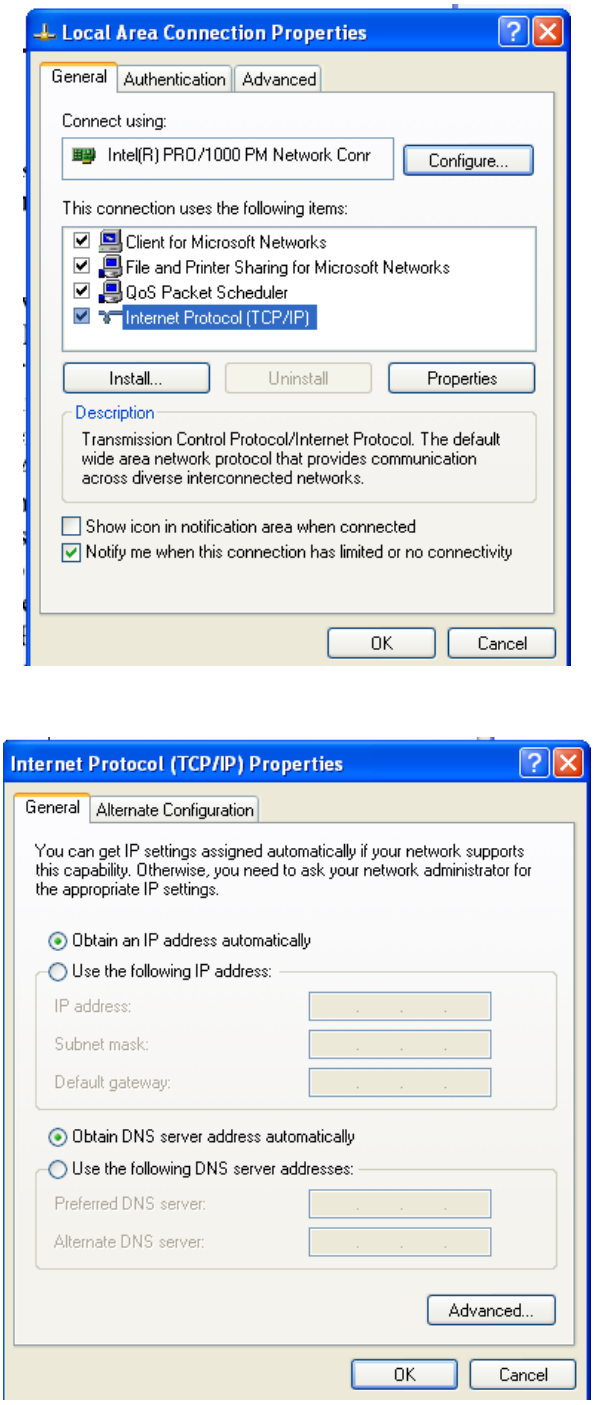
Slika 6

Usmerjevalnik ima 4 izhode. Podrobnejša navodila lahko najdete na http://www.linksys.com

Pred pričetkom vaje resetirajte usmerjevalnik s pritiskom na reset tipko in priklopite usmerjevalnik na 1. vhod(port) z izdelanim kablom, v Internet vhod pa priključite vodnik, ki zagotavlja internetno povezavo.

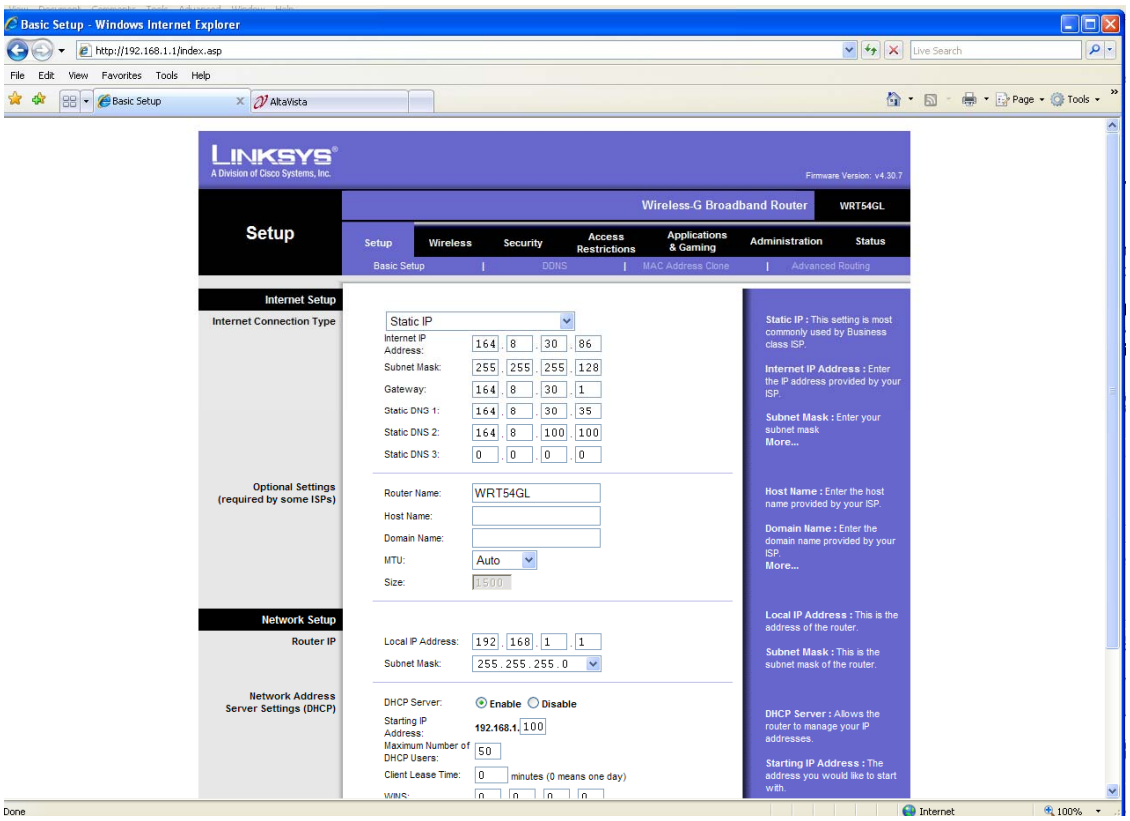
Slika 7

Na računalniku nastavite samodejno pridobitev IP naslova.
Start->Control Panel in kliknite Network (Omrežje). Z desnim miškinim gumbom kliknite na Local Area Connection



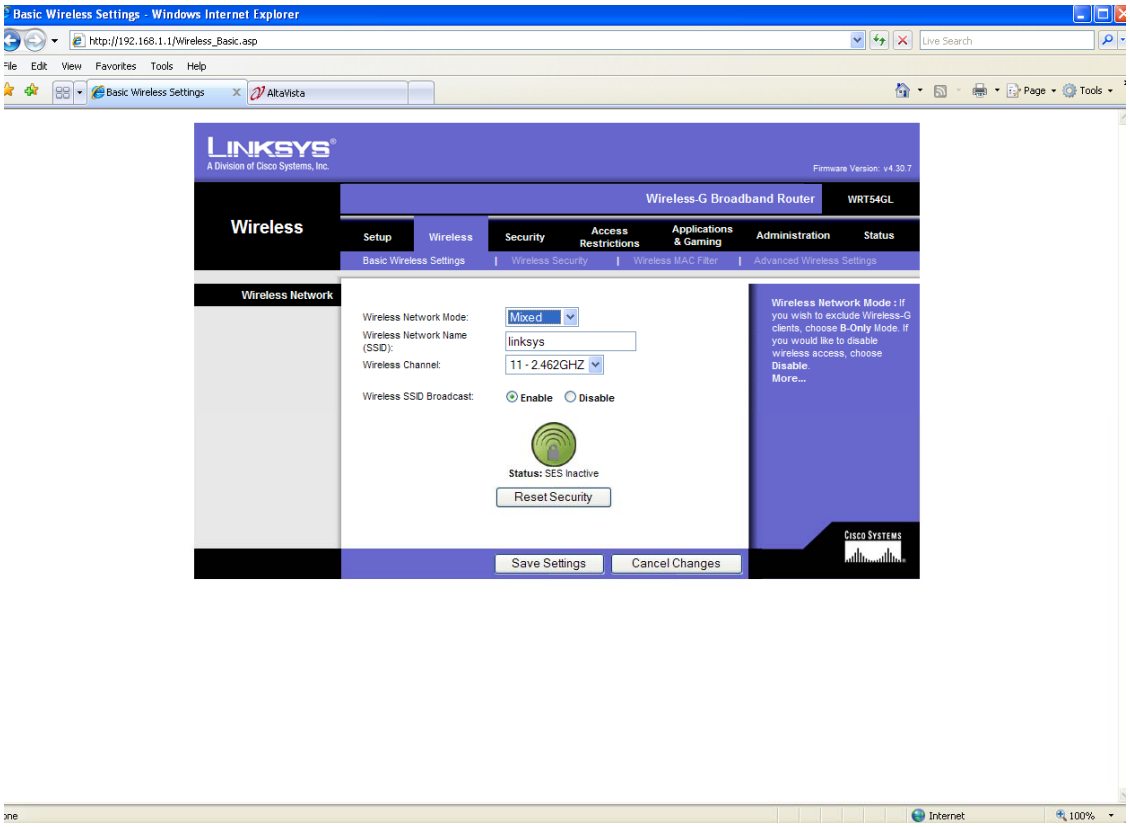
Slika 8

V brskalniku vtipkajte http://192.168.1.1/ in pod uporabniško ime (password) vpišite admin, za uporabniško ime pa pustite prazni mesto. Pojavi se vam uporabniški vmesnik, v katerem je potrebno vpisati IP naslov, itd. Uporabljen usmerjevalnik ima vgrajen DHCP strežnik in v tem razdelku lahko določimo število uporabnikov oz. št. IP naslovov, ki jih DCHP strežnik ustvari.



Slika 9

Usmerjevalnik omogoča tudi brezžičen dostop, pri katerem si moramo nastaviti osnovno konfiguracijo in varnost. V razdelku Wireless Security si lahko nastavimo način dostopa do brezžičnega usmerjevalnika (prost ali zaščiten). Dandanes se veliko pomena daje varnosti v omrežjih, zato lahko nastavimo pri brezžičnem usmerjevalniku nastavimo, kateri računalnik se lahko pridruži našemu omrežju z nastavitvijo MAC naslova računalnika. Na ta način omejimo dostop do našega usmerjevalnika.



Slika 10

Konfiguracija stikala

Pri tej vaji bomo uporabili stikalo SRW 2024 s 24. priključki oz. porti.

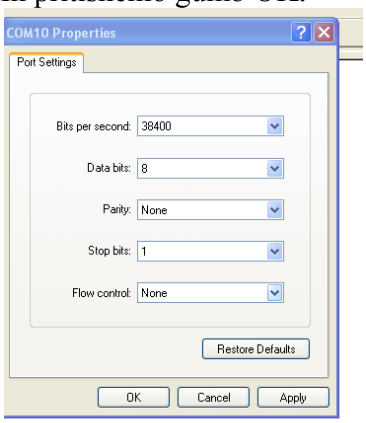
Slika 11

Najprej moramo stikalo nastaviti s pomočjo programa Telnet preko serijskega vmesnika. Program Hyperterminal zaženemo pod Start->All Programs->Accessories->Communications->Hyperterminal.

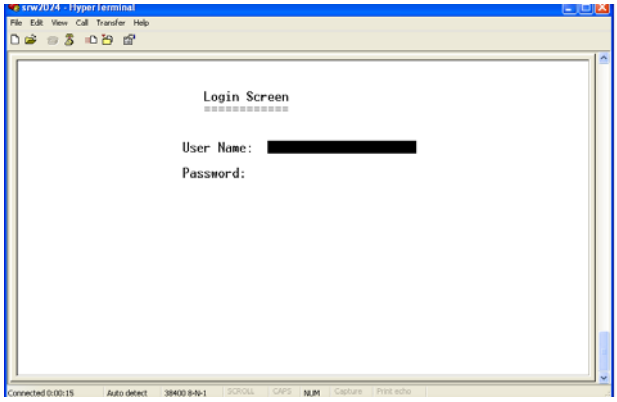
Izberemo ime za povezavo npr. srw2024 in pritisnemo ok.

Nato izberemo komunikacijska vrata, kamor je stikalo povezano s pomočjo RS232 vmesnika.

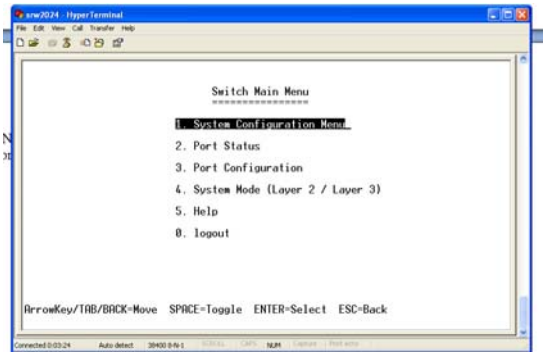
Nato nastavimo nastavitve ra serijsko komunikacijo RS232 in izberemo
Bits per second 38400
Data bits 8
Parity None
Stop bits 1
Flow control None
In pritisnemo gumb OK.



Pojavi se nam Telnet okno

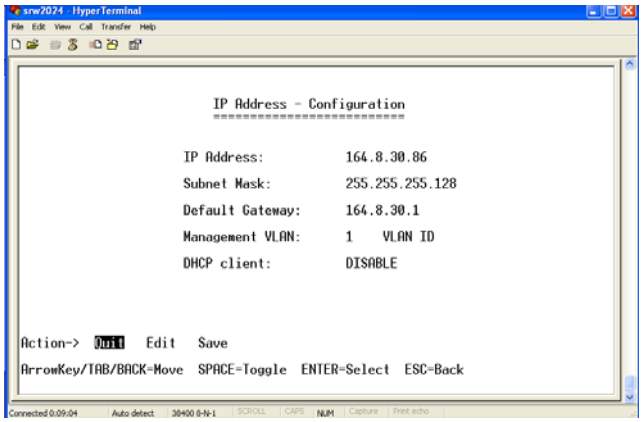


Pod User Name (Uporabniško ime) vtipkamo admin, pod password (geslo) pa pustimo prazno in pritisnemo enter in pojavi se nam uporabniško okno uporabljenega stikala.



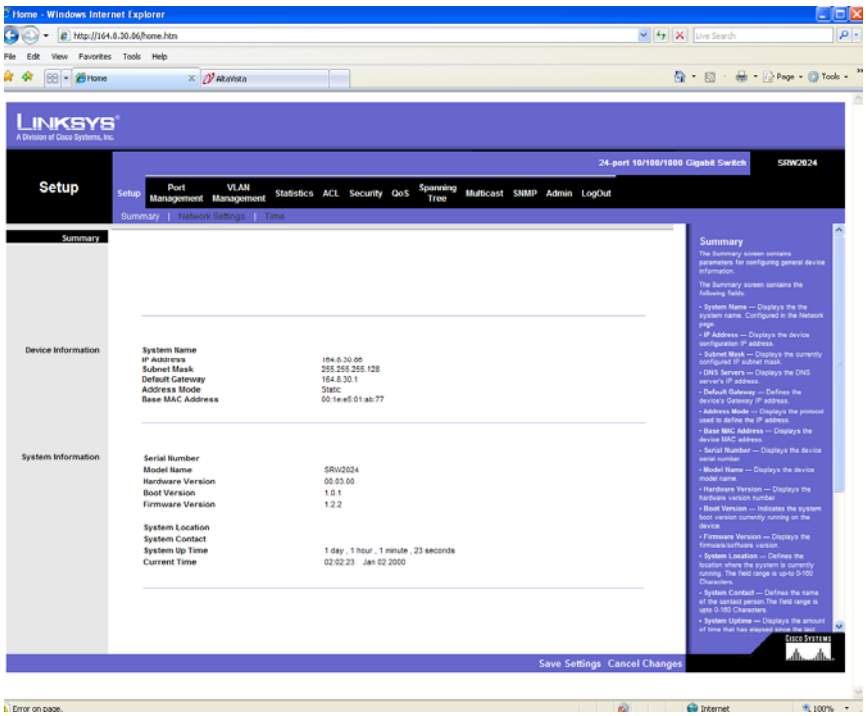
Na vajah si bomo podrobneje pogledali kaj vsak meni pomeni, za podrobnosti lahko pogledate pdf datoteko z navodili, ki jo najdete na spletni strani proizvajalca www.linksys.com.

Sedaj je naš cilj, da nastavimo IP naslov stikala. Tukaj lahko izbiramo, ali bo imelo stikalo statičen IP ali pa dinamičen. V zadnjem primeru ga dodeli strežnik DHCP. Pritisnemo tipko 1 in nato enter (System Configuration menu), nato tipko 5 in enter (IP Configuration menu), ter 1+enter (IP address settings). Če želimo, da se IP naslov dodeli dinamično gremo na polje DHCP client (pod Action s kurzorskimi tipkami gremo na polje Edit in pritisnemo enter) in s tipko space omogočimo DHCP. Nato pritisnemo tipko Esc in s kurzorskimi tipkami posnamemo (Save) nastavitve.



S tem smo nastavili stikalo in sedaj zapustimo Telnet aplikacijo z ustreznim zaporedjem tipk Esc in numerične tipkovnice. Kako se stikalo nastavi bomo pogledali v spletnem brskalniku. Privzemimo, da ima stikalo IP naslov 164.8.30.86 in ta IP naslov vtipkamo v spletni brskalnik. Nato pod username (uporabniško ime) vtipkamo admin in pritisnemo gumb ok.

Prikaže se nam grafičnu uporabniški vmesnik, kjer lahko spreminjamo in nadzorujemo nastavitve. Na vajah si bomo ogledali nekaj najbolj tipičnih nastavitev za posamezen vtič na stikalu.

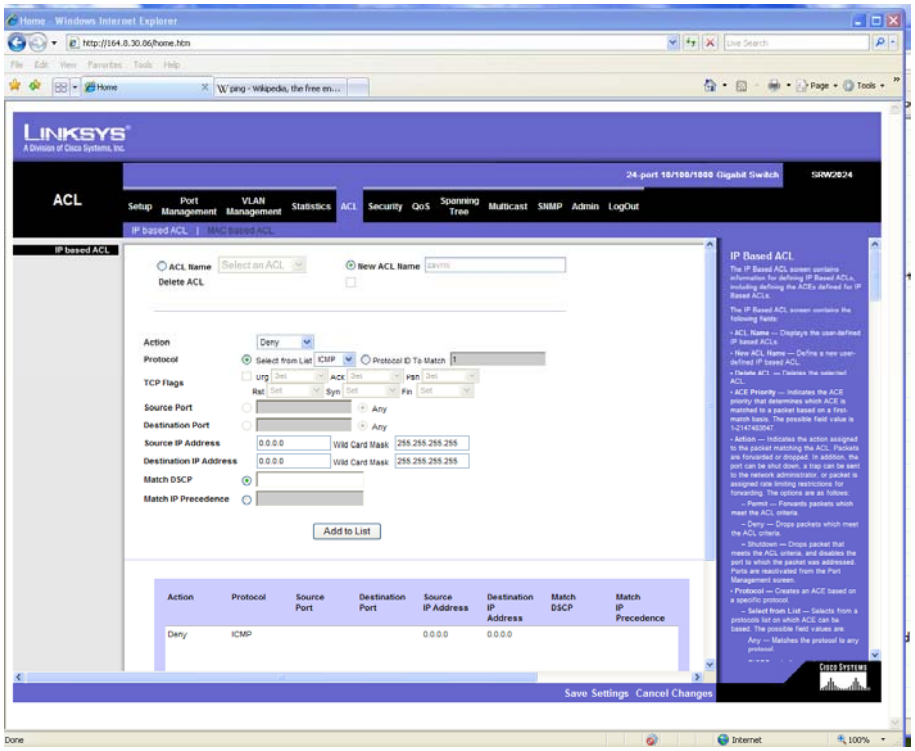


Varnost

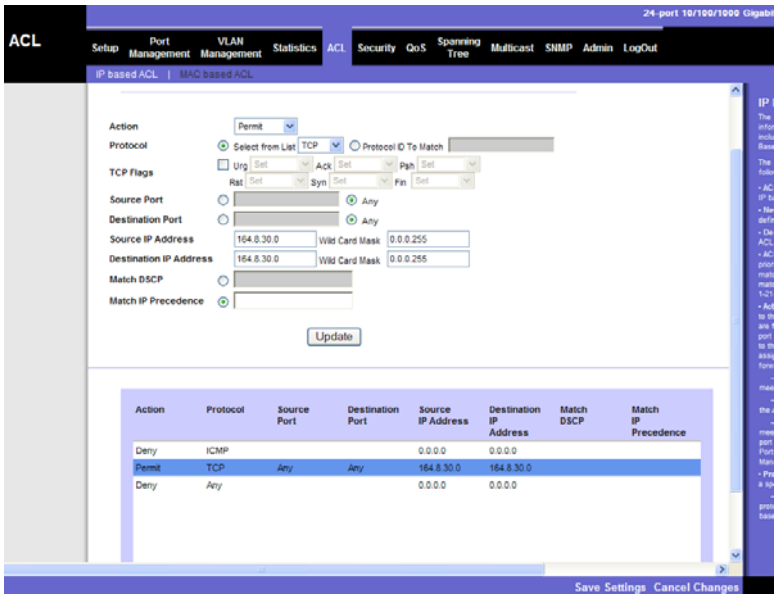
V tem poglavju bomo uporabili ACL (Access Control List) ali dostopno nadzorovane table, ki je namenjene za implementacijo varnosti na stikalu ali usmerjevalniku in se obnašajo kakor požarni zid. ALC uporabljamo za zavrnitev določenega prometa, identificiranje paketov po prioriteti, omejitev in zmanjšanje prometa na stikalu ali usmerjevalniku, identificiranje paketov za enkripcijo.
Obstajata dve tipični dostopni listi in sicer, standardna dostopna lista za preverjanje IP naslova, kjer se dovoli ali zavrne celoten protokol na posameznem omrežju ali pod omrežju ali uporabniku. Razširjene liste pa preverijo izvor in cilj naslovov, kamor se pošiljajo paketi. Preverijo se lahko posamezni protokoli, številka vtiča (port number). Paketi se lahko spustijo ali zavrnejo, zavrne se lahko tudi celoten protokol.

ACL se nastavijo s pomočjo pravil, ki določajo vrsto protokola in IP naslova uporabnika. Primer ACL liste si bomo pogledali na primeru, kjer želimo

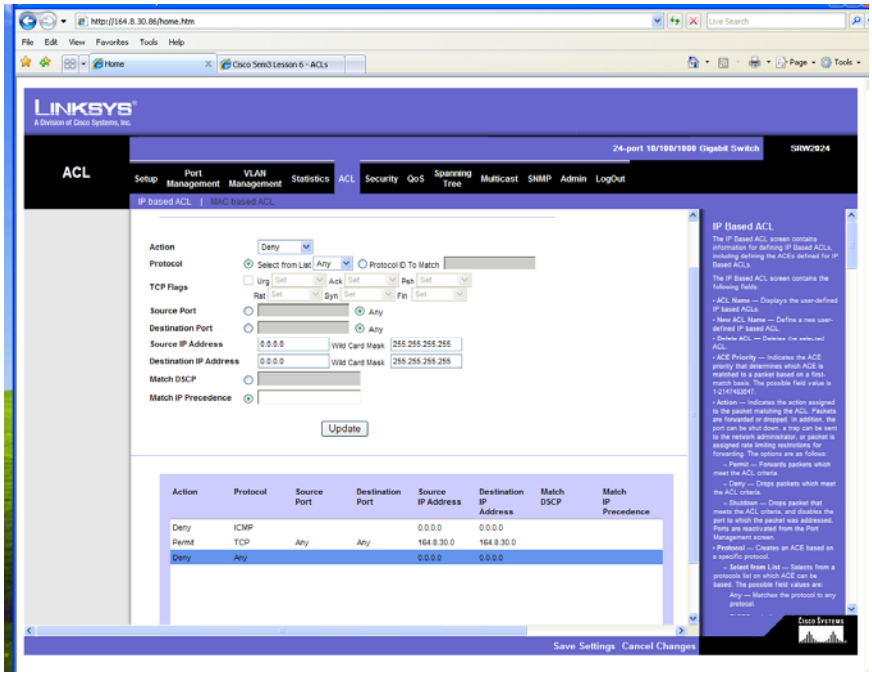
- onemogočiti aplikacijo PING, ki deluje s pomočjo Internet Control Message Protocol (ICMP). V ta namen si moramo ustvariti novo ACL ime (npr zavrni) in vnesti parametre, kot prikazuje spodnja slika. Ker bodo nastavitve veljale za vse naprave v našem podomrežju moramo vnesti Source IP 0.0.0.0 in masko 255.255.255.255, podobno za destination IP. Na koncu dodajmo nastavitve na tabelo (Add to list)



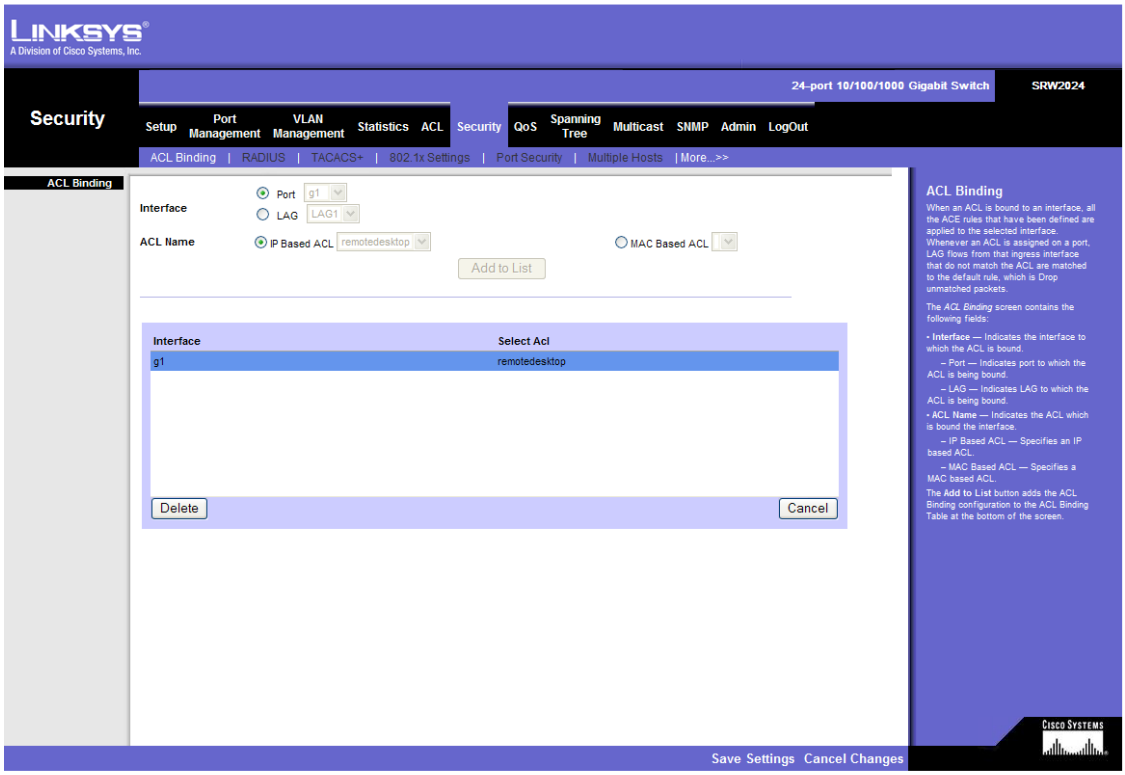
Če želimo omejiti dostop samo do našega omrežja moramo vnesti enak Source in Destionation IP naslov in omejiti z masko 0.0.0.255. Na ta način omejimo TCP samo znotraj našega podomrežja.



Onemogočiti še moramo vse ostale dostope izven našega podomrežja.



Na koncu še moramo naše nastavitve nastaviti za določena vrata na stikalu. To naredimo v razdelku Security->ACL Binding in izberemo ustrezna vrata (na katera imamo priključenega klienta, ki mu želimo onemogočiti dostop) ter ustrezen IB base ACL ter kliknemo na Add to List.



Spremenite tabelo ACL tako, da bo mogoče uporabljati samo TCP protokol in samo ICMP protokol.