

Računalniško omrežje

A) Računalniško omrežje

V osnovnem pomenu lahko omrežje predstavlja skupino, lahko tudi ljudi, ki imajo nekaj skupnega. Naštujemo lahko primer omrežja iz vsakdanjega sveta: skupina otrok, ki obiskuje tečaj tujega jezika; skupina prijateljev, ki igra nogomet ob torkih zvečer; skupina dijakov enega razreda ali učitelji šole oz. zavoda. Eno najbolj znanih omrežji ustvarjenih pred računalniškimi omrežji je telefonsko omrežje. Vsi telefoni so med seboj povezani s kabli in žicami (danes tudi že brezžično), tako da med seboj povezujejo govorce iz različnih strani sveta.

Računalniško omrežje je skupina med seboj povezanih računalnikov z namenom, da si delijo informacije in opremo. Ti računalniki so lahko v isti sobi, isti stavbi, na različnih koncih mesta ali sveta. Računalnike povezujemo v omrežja z namenom deljenja skupnih virov (podatkovnih, procesorskih), poenotenje dela, zmanjšanje cene vzdrževanja in popravil, centralni nadzor in administracija poslovnih aktivnosti, poglobljeno sodelovanje med ponudniki in kupci. Gre za povezavo računalniške tehnologije (strojna oprema, operacijski sistemi, programi) in komunikacijske tehnologije (prenos - transport podatkov)

Kako veliko je lahko omrežje?

Lahko je poljubne velikosti: mala, sestavljena iz dveh računalnikov, ali pa povezuje več milijonov računalnikov.

Če povežeš med seboj dva računalnika na kakršenkoli način, si naredil mrežo. Vsi, med seboj povezani računalniki v šoli, so del večjega računalniškega omrežja. Največjemu računalniškemu omrežju, v kateri je več milijonov računalnikov, pravimo Internet.

Po velikosti in z vidika gledanja števila med seboj povezanih računalnikov jih delimo na:

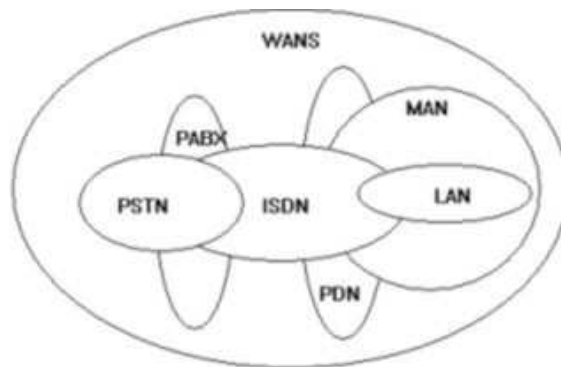
LAN (Local Area Network)/lokalno omrežje – lokalna omrežja ponavadi omejena na eno ali več stavb, popularno Campus (število naprav v omrežju je omejeno; prenosne hitrosti so nižje; naprave so cenejše).

MAN (Metropolitan Area Network)/mestno omrežje – ima vse lastnosti lokalnih omrežij, pokriva pa še širše območje (npr. velikost mesta).

WAN (Wide Area Network)/javno (komunikacijsko) omrežje – omrežje širšega obsega, razprostrto omrežje. Značilno je veliko število zapletenih in dragih naprav, večkrat pokriva območje več držav ali celo celin, sestavlja ga množica lokalnih omrežij LAN.

GLOBALNO OMREŽJE – Internet, pravijo mu tudi omrežje omrežji.

Običajno imamo vse te tipe med seboj povezane in prepletene, kot prikazuje spodnja slika:



Prepletanje različnih tipov omrežji

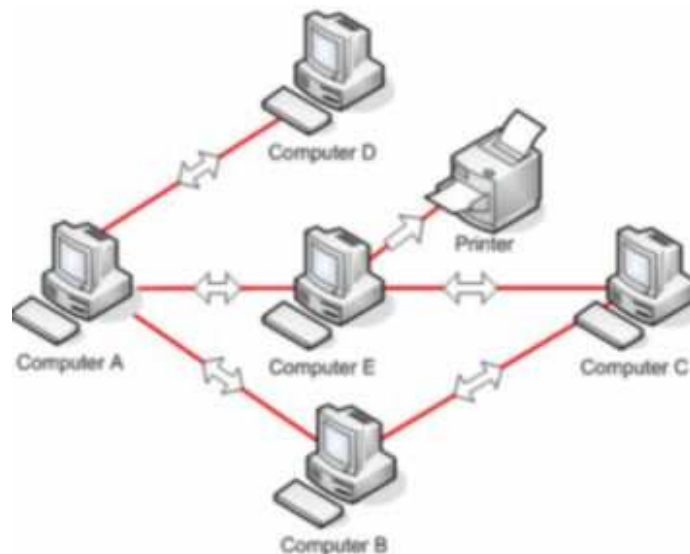
Ali obstaja več tipov omrežji?

Kljub temu, da obstaja več različnih načinov za povezavo računalnikov, poznamo v glavnem dva tipa računalniških omrežji: peer-to-peer and client/server.

Peer-to-peer ali omrežje enakovrednih partnerjev

Značilno za to omrežje je, da so računalniki in naprave v omrežju enakovredne in med seboj izmenjujejo podatke. Vsaka naprava lahko komunicira s katerokoli napravo v omrežju in izkorišča sredstva le-te (pogoni, diski, tiskalniki...), vse pa so med seboj enakovredne. Če imate doma računalnik in vaši starši ali prijatelji na svojem domu, se lahko med seboj povežete v omrežje "peer-to-peer". Če imajo starši ali prijatelji tiskalnik, se lahko povežete z njim in tiskate preko njega, torej uporabljate njegove periferne naprave. Vsi računalniki v načinu "peer-to-peer" so med seboj enakovredni.

Običajno "peer-to-peer" omrežje nima več kot 10, med seboj povezanih računalnikov. Prikaz na spodnji sliki 1:



Slika 1:Prepletanje različnih tipov omrežji

Client/server ali odjemalec/strežnik

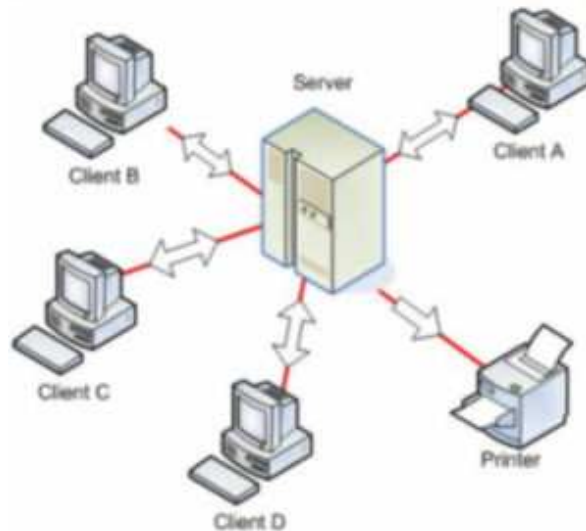
Je struktura - omrežje, pri kateri imajo računalniki v omrežju nalogo strežnika in odjemalca. Strežnik je računalnik, ki za odjemalce upravlja določene naloge (servise), skrbi za omrežje, hrani skupne podatke, upravlja tiskalnik, razdeljuje pošto ipd. Odjemalec je delovna postaja (osebni računalnik), ki te skupne servise izkorišča.

Takšno omrežje se običajno uporablja v poslovnih okoljih, podjetjih, šolah.

Ko želite na primer pridobiti informacije z določene spletne strani, deluje vaš računalnik v tem trenutku kot client/odjemalec. Ta dobi podatke od serverja/strežnika po omrežju, ki nudi usluge v obliki prikazovanja spletnih strani – www.

Odjemalec/strežnik omrežje se uporablja za povezovanje večjega števila računalnikov. Je mnogo dražje

od "peer-to-peer" omrežja, vendar enostavnejše za vzdrževanje in uporabo.



Slika 2: Client - Server

Omrežja – topologija

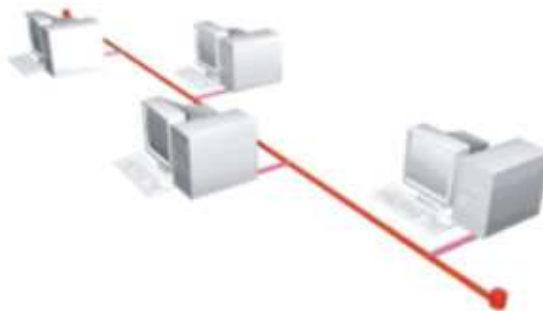
Topologija je geometrijski načrt - oblika prenosnega medija. Sestavljeni so iz vozlišča, ki so aktivni elementi, ker izvajajo usmerjanje prometa in prenosni kanali, ki so pasivni elementi, saj podatke le pasivno prenašajo. Topologija omrežja močno vpliva na lastnosti omrežja.

Najznačilnejše oblike topologij so:

Topologija skupnega vodila (bus):

Računalniki so priključeni na en skupni in neprekinjen del podatkovnega medija, ki predstavlja mnogotočkovno povezavo. Osnovni komunikacijski medij je na obeh straneh zaključen s končnimi členi ali terminatorji, ki določajo pomembne impendanci lastnosti glavnega kabla. Sporočilo oddano glavnemu prenosnemu mediju je takoj dostopno vsem vozliščem na omrežju.

Značilnosti: preprosto priključevanje novih uporabnikov, niso potrebna posebna vozlišča, težko je lokalizirati napako na vodilu v primeru prekinitve ali kakšne druge napake, omejena je dolžina prenosnega medija. (slika3)

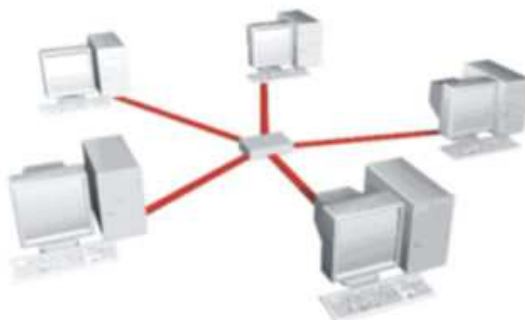


Slika 3: Skupno vodilo -bus

http://www.cisco.com/global/TH/networking/network/what_network.shtml

Zvezdna topologija:

Zvezdna topologija ima samo eno vozlišče. Njena prednost je enostavnost, saj so usmerjevalni postopki trivialni: med katerimakoli pristopnima točkama vodi namreč le ena pot. Posledica enostavnosti je vrsta pomanjkljivosti: zelo je občutljiva na izpad vozlišča, saj v tem primeru noben par ne more več komunicirati. Vozlišče z velikim številom priključenih končnih računalnikov postane počasno, zato se omejuje število priključkov na vozlišče. Topologija ni primerna za večja omrežja. (slika 4)

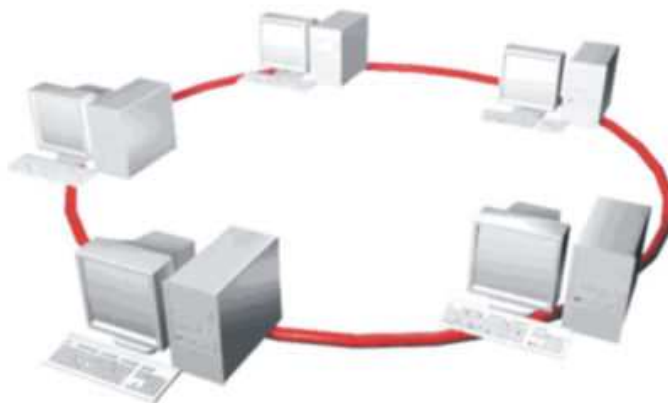


Slika 4: Zvezdno vodilo -star

http://www.cisco.com/global/TH/networking/network/what_network.shtml

Topologija obroča

Več vozlišč nanizamo drugo za drugim v obroč. Primerjamo obroč z zvezdo. Usmerjevalni postopki so nekoliko kompleksnejši, med vsakim parom sta možni dve možni poti. Omrežje je bolj trdoživo, saj so ob izpadu vozlišča prizadeti le lokalni uporabniki. Ob izpadu dveh vozlišč lahko omrežje razpade na dva dela. (slika5)



Slika 5: Topologija obroča - ring

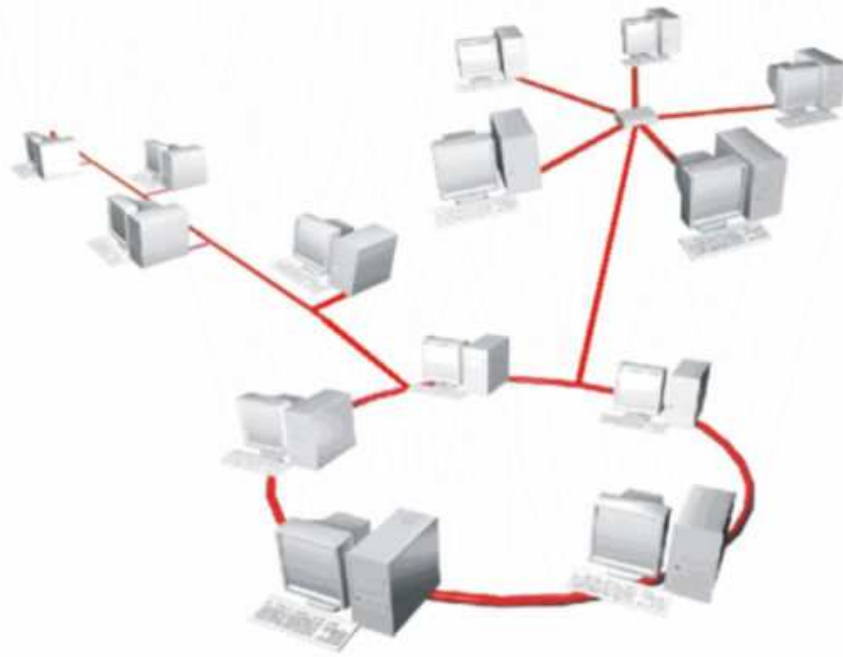
http://www.cisco.com/global/TH/networking/network/what_network.shtml

Druge oblike:

Drevesna topologija: zagotavlja enostavne usmerjevalne postopke. Predstavljamo si jo lahko kot večnivojsko zvezdo. V praksi se redko uporablja, navadno v omrežjih lokalnega dostopa.

Polna topologija: zahteva neposredne povezave med vsemi pari vozlišč. Usmerjevalni postopki so zelo zahtevni, saj število možnih poti strmo narašča s številom vozlišč. Uporablja se le v omrežjih s posebnim namenom.

Kombinacije topologij: je v praksi najpogostejša. Vsebuje poljubno izmed podmnožic povezav popolne topologije, ki še zagotavljajo povezanost omrežja. Običajno je tako v praksi kombinacija med funkcionalnostjo in stroški, da to dosežemo. Tako kombiniramo različne tipe topologij. Eno izmed možnih kombinacij je predstavljeno na sliki 6



Slika 6: Kombinacija topologija

Kako se računalniki med seboj pogovarjajo - komunicirajo?

Omrežje deluje, ker so vsi deli in naprave omrežja med seboj povezani. Vsak računalnik in del opreme, kot so tiskalniki, prenosniki, čitalci in drugi, so povezani s kabli, brezžično v omrežju WiFi, brezžično preko satelita, telefonske linije ali kako drugače.

Vsako omrežje je torej sestavljeno iz medija za prenos (kabli, brezžično) in seveda tudi vmesniki, ki tvorijo povezavo z računalnikom in med računalniki. To imenujemo tudi informacijsko komunikacijski sistem. Informacijsko komunikacijski sistem je funkcionalno porazdeljen v več nivojev ali plasti, kjer vsaka plast predstavlja in združuje sorodne storitve. V grobem delimo informacijsko komunikacijski sistem na tri funkcionalne plasti:

- plast informacijskega sistema
- plast transportnega sistema (npr. vzpostavlja zvezo med oddajnim in sprejemnim računalnikom)
- plast prenosnega kanala (npr. zagotavlja prenos podatkov od vozlišča do vozlišča)

Malo podrobneje, na področju komunikacijskih sistemov zasledimo dva močna trenda standardizacije:

1. sedemplastni ISO OSI (International Standard Organization Open System Interconnection) referenčni model in
2. štiriplastni TCP/IP (Transmission Control Protocol / Internet Protocol) model.

ISO OSI

ISO OSI predpisuje vmesnike med lokalno informacijsko infrastrukturo in transportnim sistemom.

Funkcionalnost posameznih plasti je naslednja:

1. Fizična plast skrbi za prenos bitov preko prenosnega medija in zagotavlja standardno aparaturno priključevanje sistemov na prenosni medij.
2. Povezovalna plast prenaša podatkovne okvire med dvema točkama. Osnovna naloga je odkrivanje napak, ki se zgodijo med prenosom po fizičnem prenosnem mediju.
3. Omrežna plast skrbi za usmerjanje paketov skozi topologijo omrežja - izvaja usmerjevalne algoritme.
4. Transportna plast poskrbi za storitve, ki omogočajo prestop uporabniških - informacijskih

podatkovnih enot v transportni sistem in nazaj. Izvaja transport podatkov med dvema končnima računalniškima aplikacijama.

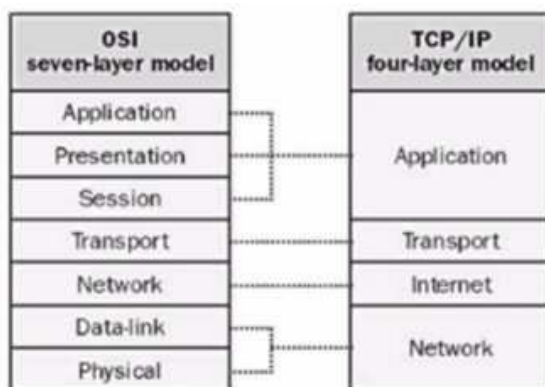
5. Plast seje je namenjena storitvam, ki podpirajo logično povezovanje oddaljenih procesov med seboj.
6. Predstavitvena plast skrbi za združljivost predstavitve podatkov v računalniških okoljih in za zaščito podatkov.
7. Aplikacijska plast vsebuje vrsto standardnih aplikacij, brez katerih si danes ne moremo več predstavljati komunikacijskih sistemov.

TCP/IP

TCP/IP družina protokolov je bila razvita med leti 1973 in 1981 v okviru DARPA (Defence Advance Research Projects Agency). TCP/IP danes predstavlja standard odprtih protokolov. Iz stališča uporabnika je TCP/IP množica aplikacijskih programov, ki uporabljajo omrežje za izvršitev uporabnih komunikacijskih nalog. Večina uporabnikov izvaja aplikacijske programe, ne da bi razumeli TCP/IP tehnologijo, strukturo podmrežja, ali celo po kateri poti gredo podatki do cilja; te podrobnosti prepustijo aplikacijskim programom.

Referenčni model Interneta je sestavljen iz štirih nivojev:

1. Fizični nivo skrbi za prenos datagrama do ponora. Na ponoru fizični nivo poda glavo in paket IP nivoju. Ta iz glave ugotovi, če je zanj. Če se podatki ne ujemajo s ponorjem, potem pošlje paket transportnemu nivoju. Ta še enkrat preveri, če je paket na pravem naslovu in pošlje potrditev prejema, nato pa preda podatke aplikacijskemu nivoju.
2. Internetni nivo (mrežni nivo) doda paketu poleg glave in zaporedne številke še IP naslov izvora in ponora. Ta nivo tvori fizičen naslov ponora. Za osnovno komunikacijsko enoto uporablja datagram, ki vsebuje paket in fizični naslov ponora. Njegova naloga je poslati datagram na fizični nivo.
3. Transportni nivo razdeli tok podatkov na več TCP paketov, jih opremi z glavo in jim dodeli zaporedne številke ter jih pošlje internet nivoju.
4. Aplikacijski nivo pošilja in prevzema toke podatkov od oz. do transportnega nivoja. V aplikacijski nivo sodijo protokoli Telnet, FTP (File Transfer Protokol), SMTP (Simple Mail Transfer Protocol) in še množica drugih. Aplikacijski nivo je edini, s katerim ima uporabnik neposreden stik



Slika 7:ISO-OSI in TCP/IP

Poglejmo si nekatere fizične vmesniki in naprave za povezavo in tvorjenje omrežji. Med seboj se razlikujejo po funkcionalnosti (logični in fizični) in glede na katerem nivoju ali plasti ISO/OSI modela delujejo.

Mrežne Kartice/Network Interface Cards (NICs)

Network interface card (NIC) ali mrežna kartica je tisti vmesnik v računalniku ali napravi, ki nam omogoča, da se preko nje naš računalnik ali naprava poveže v omrežje (seveda pod to smatramo tudi

druge vmesnike s katerimi se lahko povezujemo). Na računalniku ali napravi potrebujemo nato še programsko opremo za svojo mrežno kartico, da ta pod operacijskim sistemom, kateri je nameščen na računalniku, uspešno deluje in nam omogoča povezavo z ostalimi.

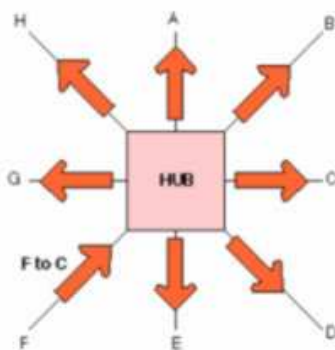
Komunikacija med računalniki poteka po določenih pravilih in načinu, ki mu pravimo **protokol**. Protokol je računalniški jezik, strukturiran v obliki različnih pravil, dogovorov in postopkov, ki vodijo in opravljajo prenos informacij. Protokol je potreben, da ne pride do napak pri komuniciranju. S protokolom natančno določimo pošiljanje in sprejemanje informacij. Omrežni protokoli so potrebni zaradi istega razloga kot drugi protokoli (npr. pogovor po telefonu, prihod predsednika države na obisk, način rokovanja – na Tajskem se ne rokujejo ipd.).



Slika 8: Mrežna kartica - NIC

Hub - Ponavljalnik

Hub - Ponavljalnik je naprava v (računalniškem) omrežju, ki omogoča prenos podatkov med več linijami. V bistvu je nekakšen multiplekser – signal iz enega vmesnika razdeli na poljubno število vseh drugih vmesnikov. Torej je njegova naloga, da signal, ki ga sprejme na enem vmesniku, ojači in obnovi ter preusmeri na vse preostale vmesnike.



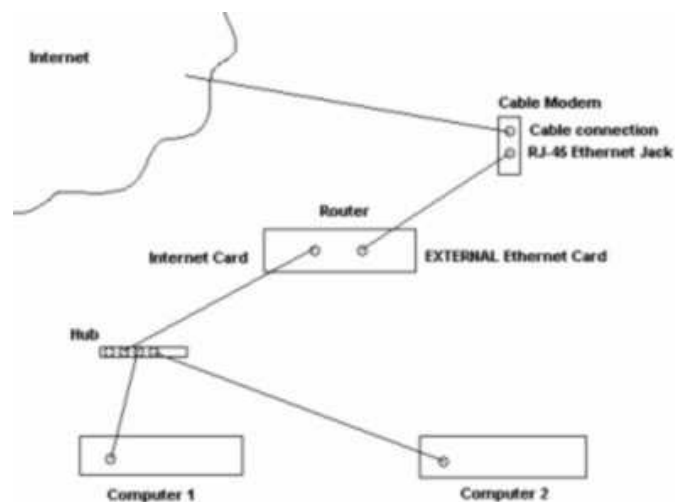
Slika 9 – Prenos paketov ali podatkov iz vmesnika F do C pomeni na ponavljalniku prenos podatkov na vse ostale vmesnike



Slika 10 HUBi s označenimi povezovalnimi vmesniki. Več ponavljalnikov lahko med seboj povezujemo.

Router – Usmerjevalnik

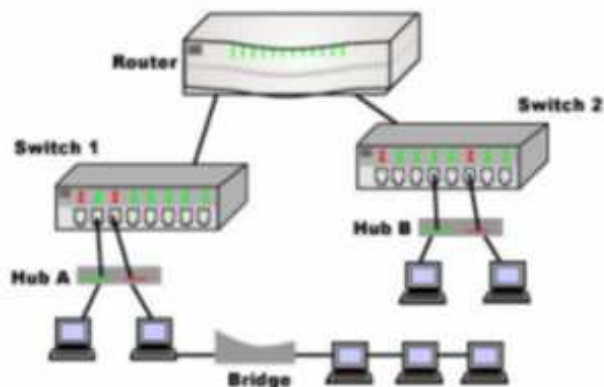
Je naprava s katerim povezujemo lokalna omrežja s zunanjimi omrežji. Usmerjevalniki imajo vgrajene funkcije za filtriranje prometa, omogočajo prenos paketov po vzporednih poteh, s čimer povečamo prepustnost omrežja, omogočajo delitev omrežij na podomrežja na podlagi omrežnih naslovov. Promet se tako usmerja iz enega vmesnika na točno določenega drugega.



Slika 11- Prikaz postavitve usmerjevalnika

Bridge – Most

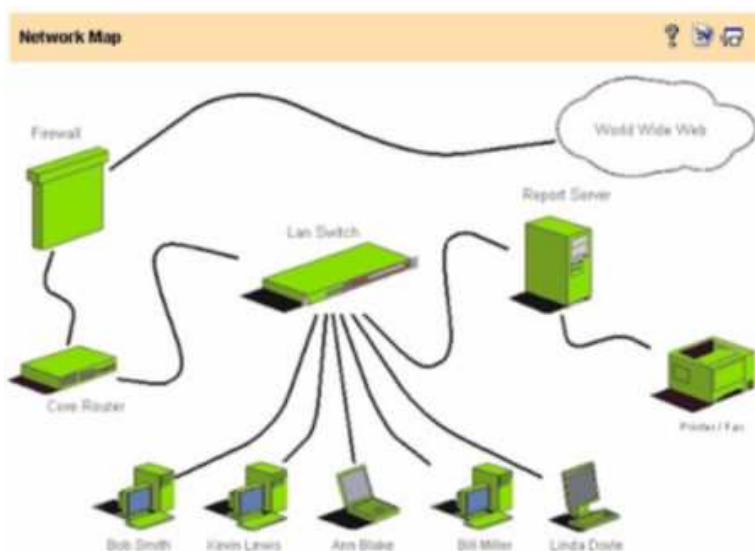
Naprava, ki povezuje in prepušča pakete med dvema deloma - segmentoma omrežja, ki uporabljata enak komunikacijski protokol. Bridge-most podatke ali pakete ojači, shrani, in preveri v medpomnilniku. Most v medpomnilniku pregleda vsak paket in na podlagi tega se odloča kaj bo naredil s paketom.



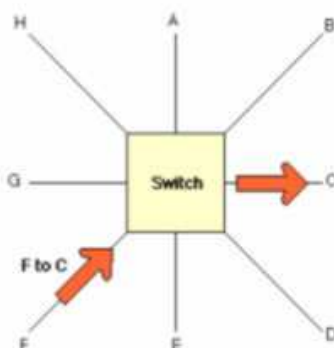
Slika 12 Bridge- most http://www.gactr.uga.edu/idl/webid/portfolio/graphics/illustrations/hub_bridge_switch_router.jpg

Switch - Preklopnik

Je podoben hubu ali ponavljalniku le, da je način delovanja v osnovi enak bridge-mostu. Namenjeni so predvsem povečanju prepustnosti znotraj lokalnega omrežja (arhitektura hitrega vodila). Zaradi boljših lastnosti in bistveno nižje cene na posamezni priključek vse bolj zamenjujejo usmerjevalnike in mostove.



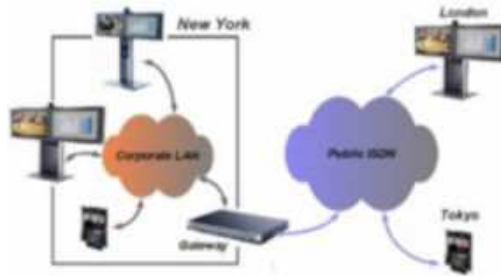
Slika 13 Prikaz uporabe switch-stikala <http://www.solarwinds.net/images/Orion/Maps>



Slika 14 Prenos paketov na Switchu- stikali poteka iz vmesnika F do C

Gateway - Prehod

Naprava ali računalnik preko katerega lokalno omrežje prehaja v drugo ali večje globalno omrežje.



Slika 15 Uporaba Gatewaya – prehoda

V praksi je običajno v eni napravi združena funkcionalnost vseh naprav. Tako lahko danes uporabimo napravo v kateri so združene funkcije in lastnosti switca-stikala, routerja-usmerjevalnika, gatewaya-prehoda, brezžične dostopkovne točke, požarnega zidu, protivirusne zaščite in še kaj. Največkrat se takšne univerzalne naprave uporabljajo za manjša podjetja ali domačo uporabo.

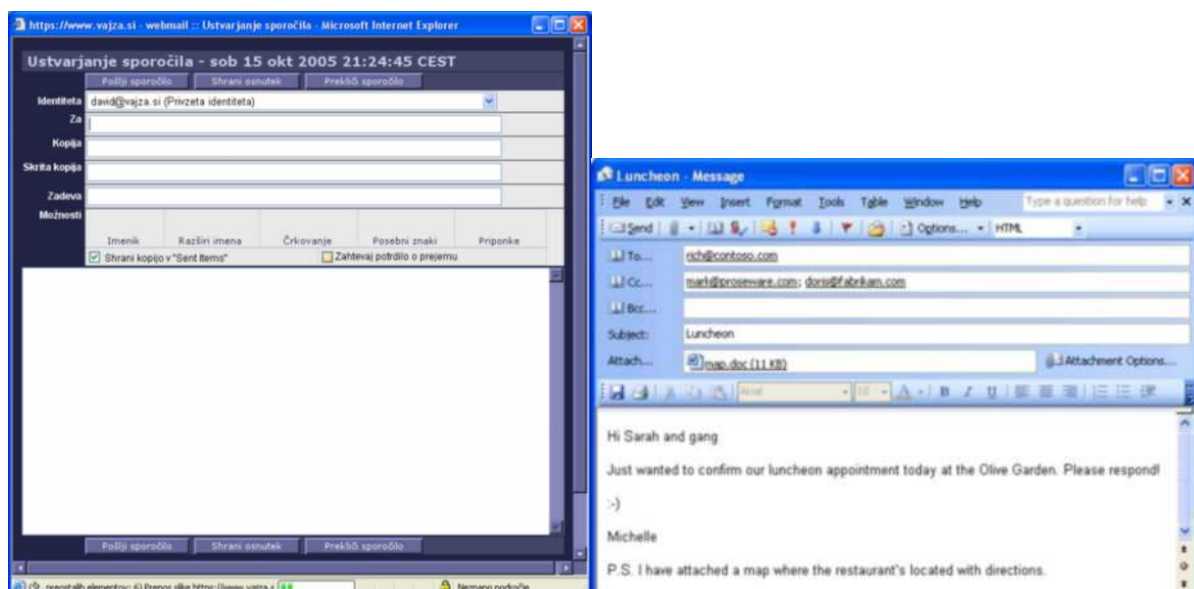
b) Oblike izmenjave sporočil v računalniškem omrežju

Omrežje vsebuje ali nudi več uslug. Najbolj pogosto uporabljeni so:

- World Wide Web – svetovne spletne strani ali krajše www oz. splet so posebne informacije shranjene v obliki, ki jih lahko pregledujemo z Web browser/ spletnim brskalnikom (InternetExplorer, Mozilla, Opera ...). Spletni brskalniki so programi, s katerimi lahko pregledujemo in obiskujemo spletne strani, ki vsebujejo besedilne, grafične ali multimedijske vsebine in programe.
- E-mail ali elektronska pošta omogoča pošiljanje elektronskih sporočil po omrežju Internet, na podoben način kot navadna pošta, brez poštarjev seveda. Več o tem v nadaljevanju.
- File transfer ali prenos datotek pomeni prenašanje ali kopiranje datotek med računalniki. Obstaja poseben protokol za prenos datotek v omrežju Internet, znan kot File Transfer Protocol (FTP).
- Usenet News ali novice sestavljajo računalniki, ki si v omrežju delijo in izmenjujejo članke za posamezno področje, nudijo podporo izdelkom, odgovarjajo na vprašanja in podobno. Takšni skupini računalnikov s skupnimi interesi za posamezno področje pravimo newsgroups ali novičarska skupina.

c) Elektronska pošta

Elektronska pošta ali e-mail je najbolj “obremenilna” usluga omrežja Internet. Vsak dan je poslanih milijone sporočil. Zakaj so sporočila pomembna? Kako izgleda e-pošta in kaj je?



Kako deluje elektronska pošta?

Elektronska pošta deluje na podoben način kot navadna pošta. Obstaja poštna služba, poštni nabiralnik (poštni strežnik), naslovi (email ali elektronski naslov) in sporočila. Elektronsko sporočilo se odpošlje in prispe že v "naslednjem" trenutku.

Za upravljanje z elektronskimi sporočili potrebujemo samostojen program ali pa ga upravljamo preko spletnega brskalnika. V obeh primerih je delo s programom podobno in se običajno izvaja po naslednjih korakih (pogledali si bomo oba primera uporabe):

- Najprej sestavimo sporočilo.
- S klikom na gumb pošlji/send nam program za elektronsko pošto pretvori sporočilo v digitalni format.
- Digitalno sporočilo se po omrežju prenese do poštnega strežnika.
- Ustrezni poštni strežnik obdela prihajajoča sporočila in jih posreduje naslovniku.

Kako oblikujemo elektronski poštni naslov?

Za delo z elektronskimi sporočili potrebujete elektronski naslov, e-mail. Običajno ga dobite od podjetja v katerem ste zaposleni, ponudnika internetnih storitev (Internet Service Provider - ISP) ali pa ga brezplačno oblikujete sami preko spletnih strani (Hotmail.com, Email.si ...).

Vsak elektronski naslov je podobno sestavljen. Običajno se začne z imenom in priimkom, uporabniškim imenom ali vzdevkom, nato sledi posebni znak @ (afna) in na koncu še ime domene.

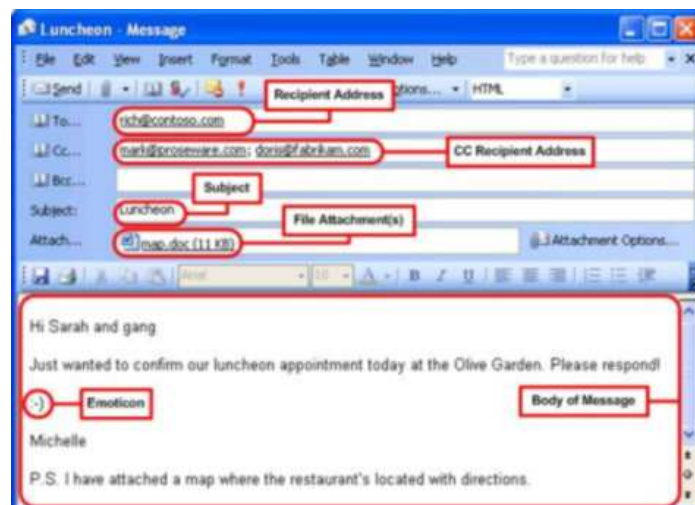
Primer: fred.sefovic@hotmail.com ali dasa@email.si ali ime.priimek@scptuj.si

Za vsak elektronski naslov potrebujete elektronski račun z edinstvenim uporabniškim imenom in geslom, ki ga potrebujete vedno, kadar želite pregledati vašo pošto oz. vaš elektronski poštni nabiralnik.

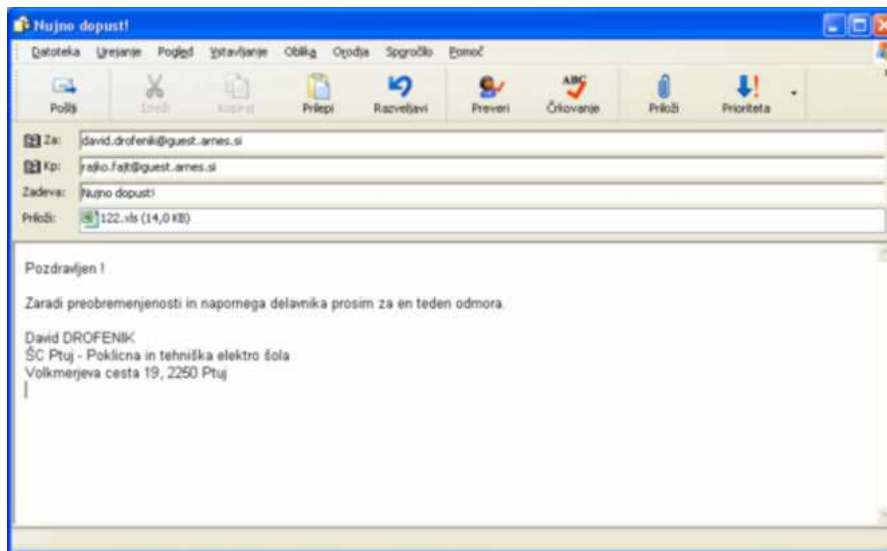
Za vsak elektronski naslov potrebujete elektronski račun z edinstvenim uporabniškim imenom in geslom, ki ga potrebujete vedno, kadar želite pregledati vašo pošto oz. vaš elektronski poštni nabiralnik.

Kako pošiljamo in sprejemamo elektronsko pošto?

Slika 17 in 18 prikazujeta osnovne dele sporočila:



Slika 17 Elektronsko sporočilo s svojimi sestavnimi deli angleška varianta



Slika 18 Elektronsko sporočilo s svojimi sestavnimi deli slovenska varianta

Te sestavine vsebujejo:

- Recipient's Name and Address (to) ali prejemnikov elektronski naslov (za)

Tako kot pri navadnem pismu potrebujemo naslov osebe, kateri pošljamo sporočilo.

- Sender's Name and Address ali pošiljatelj elektronski naslov

Naslov pošiljatelja se avtomatsko doda vsakemu elektronskemu sporočilu.

- Subject ali zadeva

Naslov osnovne zadeve sporočila, ki bo prikazan naslovniku.

- Time and Date ali čas in datum sporočila

Čas se avtomatsko doda vsakemu sporočilu v trenutku, ko je bilo sporočilo poslano.

- Main Body ali telo sporočila

Prostor, v katerega vpisujemo besedilo sporočila.

- Attachments ali priponke

Pripnemo poljubne datoteke, ki vsebujejo poljubno vsebino. Pazite na velikost priponke!

- Carbon Copy (cc) ali dodatna kopija (kp)

Isto sporočilo lahko istočasno pošljemo več osebam hkrati, če vpišemo elektronski naslov v c/kp polje.

Ostali prejemniki vidijo naslov teh oseb.

- Blind carbon copy (bcc) ali skrita kopija sporočila

Isto sporočilo lahko istočasno pošljemo več osebam hkrati, če vpišemo elektronski naslov v bcc polje, vendar ostali prejemniki iz polja to/za tega ne vidijo.

Ko smo sporočilo sestavili, ga lahko pošljemo. Prejemnik dobi elektronsko pošto v svoj poštni nabiralnik.

Navodila pravega obnašanja pri uporabi e-pošte

V običajnem pogovoru s sogovornikom poteka tako verbalna kot neverbalna komunikacija, kar pri elektronskem prenašanju sporočil ne moremo doseči. Odziv sogovornika na določeno stvar, kot so jeza, dolgčas, veselje ipd. je viden le iz povratnega pisnega sporočila.

Pri elektronskem pisanju sporočil veljajo nekatera osnovna pravila, znana kot netiquette ali predpisi dobrega obnašanja:

- Uporabljajte vrstico zadeva! V njej jasno povejte kaj je bistvo sporočila oz. za kaj gre. Ne puščajte okenca za zadevo praznega.
- Nikoli ne pišite vse z velikimi črkami. V računalniškem jeziku to pomeni, da na nekoga kričite.
- Uporabljajte pravila pravopisa, slovnice in slovarjev. Deloma si lahko pomagata z vgrajenimi orodji.
- Pazite na oblikovanje. Nekomu vaše kričeče barve, čudna ozadja ter menjava malih in velikih črk ne bodo všeč. Različni programi za elektronsko pošto imajo popolnoma različne dodatne funkcije. Tako se lahko zgodi, da vsega dodatnega oblikovanja prejemnik ne bo videl in slika bo popačena.

- V elektronska sporočila ne vpisujte števil kreditne kartice, gesla in ostalih zaupnih podatkov.
- Ko odgovarjate na sporočila, vstavite le najpomembnejše informacije osnovnega sporočila, da vas bo oseba razumela. Ne pošiljajte celotnega osnovnega sporočila nazaj.
- Vključite signature line ali vrstico s vašim podpisom na koncu vsakega sporočila. Ta običajno vključuje vaše ime, elektronski naslov in ostale pomembne informacije. Vrstica s vašim podpisom naj ne presega štirih vrstic.
- Elektronska sporočila naj bodo kratka in v odstavkih. Med odstavki je priporočljivo pustiti eno vrstico prazno.
- Uporabite zvezdico/asterisks, ko poudarjate neko besedo, npr. this can be **extremely** helpful.
- Uporabite podčrtovalnik/underscore, npr. Romeo and Juliet.
- Uporabite lahko znake čustev/emoticons in kratic/acronyms, ki naredijo sporočilo bolj osebno.

Kaj še lahko delamo z e-pošto?

V nadaljevanju pošiljanja elektronske pošte posameznikom ali skupinam se lahko pridružimo tudi seznamu razprav (discussion list). To je skupini ljudi, ki med seboj komunicirajo preko elektronske pošte. Druži jih skupen interes. Na glavni naslov skupine lahko pošljete elektronsko pošto in strežnik vam bo avtomatsko poslal kopijo vseh članov skupine.

Elektronska pošta olajša razpravo o skupnih interesih. Če skupina študentov, na primer, obiskuje poletni tečaj, lahko organizacija, ki je ta tečaj organizirala, oblikuje seznam vseh sodelujočih. Posamezniki se bodo na seznam naročili in tako prejeli ali poslali sporočila. Če pošljete eno sporočilo na glavni seznam, bodo kopijo dobili vsi naročniki in razprava steče.

Takšnih seznamov je na Internetu na tisoče in pokrivajo raznolika področja. Obstaja toliko seznamov, da so celo ustvarili seznam seznamov. Ko enkrat najdete željen seznam, pošljete sporočilo za naročilo.

Glede na vrsto seznama, boste običajno dobili sporočilo nazaj, ki bo sporočalo, ali ste avtomatsko postali član seznama ali pa boste potrebovali dovoljenje nekoga, ki vas bo dodal na seznam naročnikov. Vsak seznam ima zbir navodil. Preberite pogoje in jim natančno sledite.

d) Iskanje podatkov v globalnem omrežju

V ta namen uporabljamo iskalnike.

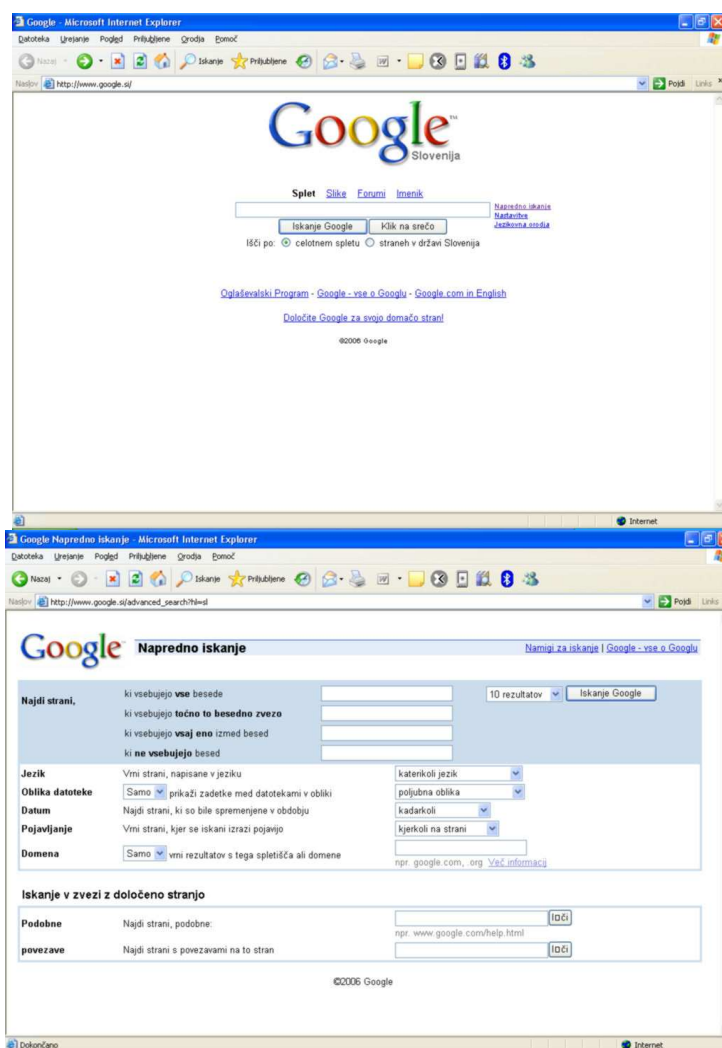
Iskalniki so spletne strani, na katerih lahko iščemo informacije. Obstaja ogromno iskalnikov spletnih strani, kjer lahko iščemo informacije (spisek vseh iskalcev najdemo na <http://www.searchenginecolossus.com/>). Vsi pa uporabljajo podobne prijeme, da si napolnijo svojo bazo strani, po katerih iščemo:

- Program imenovan pajek je avtomatski program, ki raziskuje omrežje Internet in dodaja oz. odvzema s spletnih strani ustrezne informacije.
- Indeksni program organizira in uredi vse dobljene informacije po različnih ključih.
- Podatkovna baza je zbirka vseh informacij, ki jih lahko dobimo od iskalnika in je potrebna za njegovo delovanje, to je dajanje iskalnih rezultatov.
- Vmesnik je običajno spletno okno, preko katerega uporabnik zahteva iskani niz ali besedilo.

Obstajajo trije osnovni tipi iskalnikov:

- Meta iskalniki: njihova lastnost je zajemanje rezultatov več iskalnikov hkrati, njihovo optimiziranje glede na našo zahtevo in podajanje le-teh kot rezultatov.
 - o MSN Search: <http://search.msn.com>
 - o Ask Jeeves: <http://www.ask.com>
 - o Dog Pile: <http://www.dogpile.com>
 - o Yahoo!: <http://www.yahoo.com>
 - o Alta Vista: <http://www.altavista.com>
 - o Excite: <http://www.excite.com>
- Splošno-namenski iskalniki: za začetek najboljši in najenostavnejši iskalniki.
 - o Google: <http://www.google.com>
 - o Teoma: <http://www.teoma.com>
 - o Webmyway: <http://www.webmyway.com>
- Iskalni agentis: programska oprema za zahtevnejše iskanje.
 - o Bot Spot: <http://bots.internet.com>
 - o Copernic: <http://www.copernic.com>

Večina spletnih iskalnikov je zasnovana iz osnovne strani, kamor vstavite iskani niz in sprožite iskanje. Posamezni iskalniki vrnejo različno število možnih rešitev. Uporabljajte napredne funkcije iskanja in dodatni parameter, s katerimi boste zmanjšali število zadetkov.



Slika 19 Iskalnik Google in njegovo naprednejše iskanje

Namizni iskalniki

Medtem ko spletni iskalni iščejo iskano informacijo na spletu, jo namizni iščejo na vašem osebнем računalniku. Za uspešno in hitro izvedeno iskano operacijo je treba najprej ustvariti indeks ali kazalo podatkov. Tako namesto vedno znova iskanja po datotekah iščemo znotraj indeksa, ki je nekakšna baza podatkov o datotekah, njihovi vsebini ali njihovih meta podatkov. Indeksiranje je torej potrebno opraviti preden želimo začeti s iskanjem in ga je potrebno redno ponavljati. (npr. ob zagonu računalnika, ob prijavi ali tudi večkrat dnevno).

Trenutno so najbolj razširjeni namizni iskalniki, ki se razen v imenu proizvajalca in zunanem izgledu razlikujejo predvsem v podpori različnih zapisov datotek znotraj katerih so sposobni iskati:

- Microsoft Windows Desktop Search
- Google Desktop – <http://desktop.google.com/>
- Copernic Desktop Search – <http://www.copernic.com/en/products/desktop-search/>
- Yahoo Desktop Search – <http://desktop.yahoo.com/>

e) Značilnosti računalniške obdelave podatkov

f) Pomen zaščite in varovanja podatkov

g) Pisno kodiranje podatkov

Ali je to kodiranje in šifririni algoritmi ?

h) Nevarnosti računalniških virusov

skok na

i) Načini varovanja ter zdravljenja podatkov

V prejšnjih poglavjih smo spoznali čudovite stvari, ki so dosegljive v omrežju Internet in drugih omrežji. Potrebno pa je opozoriti na možne nevarnosti in načine zaščite.

Na omrežje se vpisuje mnogo različnih ljudi in težko ugotovimo, kakšne so njihove namere. Kadarkoli smo povezani v omrežje, obstaja možnost, da na naš računalnik pride nepovabljen gost (program, oseba). Zato je dobro, da smo seznanjeni vsaj z osnovnimi možnostmi zaščite in splošni pojmi varovanja.

Pojmovanje računalniške varnosti v podjetjih je nekoliko drugačno od tistega doma oz. računalnika za osebno – domačo uporabo. Medtem, ko se doma poskušamo zavarovati predvsem pred lastnimi napakami in zlorabami v omrežju, je dojemanje računalniške varnosti v podjetjih precej celovitejše in zahtevnejše. Čeprav so mnoge uporabljene tehnologije iste, se pogosto uporabljajo v druge namene. V tem poglavju bomo spoznali načine ogrožanja računalnika in možnosti zaščite.

Varnostne vrzeli

Računalniški sistem je toliko varen koliko je ranljiva njegova najšibkejša točka. Ranljivost je slabost v računalniškem sistemu, ki lahko povzroči izpad ali poškodbo računalniškega sistema. Poznamo štiri vrste ogrožanja varnosti računalniškega sistema:

1. Prekinitev-motnja (interruption) del računalniškega sistema se lahko pokvari, izgubi, je neupraben ali nedosegljiv
 2. Prisluskovanje-prestrezanje (interception) pomeni dostop nepooblaščenega vstopa v naš računalniški sistem. To je lahko iz strani osebe, programa ali drugega računalniškega sistema.
 3. Sprememba-prikrojitev (modification) podatkov s spreminjanjem vrednosti, kakor tudi sprememba strojne opreme.
 4. Ponarejevanje (fabrication) ali dodajanje lažnih podatkov ali prilagajanje le teh.
- [Pflege3]

Bistvo varnosti računalniških sistemov

Računalniško varnost računalniških sistemov ocenjujemo s treh medsebojno dopolnjujočih se vidikov:

- zaupnost (confidentiality)
- celostnost, celovitost (integrity)
- dostopnost (availability)

Z zaupnostjo mislimo zaščito delov računalniškega sistema samo pooblaščenim delom. Varovanje zaupnosti ne vključuje le celostnih podatkov, temveč tudi posamezni informacije, ki so same zase videti nedolžne, vendar bi z njihovo pomočjo lahko prišlo do zlorabe drugih, zaupnih informacij.

Celostnost pomeni da posamezne dele lahko spreminjajo samo pooblašчени deli na pooblaščen način. Celostnost podatkov vključuje zaščito le teh pred brisanjem ali spremembami v kakršnikoli obliki brez dovoljenja lastnika ali pooblaščene strani.

Dostopnost poskrbi da so posamezni deli dostopni in na razpolago samo pooblaščenim delom. Predvsem v zadnjem času, ko se vse več dejavnosti seli v internet, postaja dostopnost teh informacij izredno pomembna, dostopnost naj bi skrbela tudi za računalniško varnost s tega vidika.

Ti trije vidiki predstavljajo bistvo varnosti v računalniških sistemih. Poglejmo si jih podrobneje.

Zaupnost

Strjeno pomeni zaupnost: »samo pooblaščene osebe lahko vidijo oz. imajo dostop do zaščitene podatkov«.

Zaupnost pomeni omogočanje dostopa do podatkov in računalniških virov ter delov računalniškega sistema le pooblaščenim osebam. Omejevanje dostopa dosežemo s pooblaščenim dostopom in kodiranjem podatkov.

Povezava v internet so vrata v podjetje prav tako kot je fizičen vhod za ljudi. Tako kot fizičen vhod za ljudi je tudi povezavo v internet potrebno ustrezno zaščititi. (požarni zidovi, programskimi pripomočki, kot so različni ovijalni programi – tcpwrapper, s katerimi blokiramo dostop v naše omrežje). Potrebno je omejiti povezave in pregled znotraj podjetja. Ustrezno zaupnost in varnostno politiko je potrebno postaviti pri podjetjih, ki imajo več prostorsko dislociranih podružnic (z postavitvijo navidezno najeto omrežje virtual private network VPN in IPSec).

Celostnost - celovitost

Celostnost po mišljenju avtorja Welke in Mayfield lahko pomeni-predstavlja različne stvari znotraj različnega konteksta. Nekateri pomeni celostnosti so:

- natančnost
- točnost, vestnost
- nespremenljivost
- spremenljivost na dopusten način
- spremenljivost samo pooblaščenim osebam
- spremenljivost samo pooblaščenim procesom
- skladnost
- notranjo konsistentnost
- razumljivost in točnost rezultatov

Avtorja Welke in Mayfield ločita tri vidike celostnosti: pooblaščene akcije, ločeni in zaščiteni sistemski viri ter zaznava in odprava napak.

Celostnost računalniških sistemov pomeni, da se vedejo tako, kakor od njih pričakujejo pooblašчени uporabniki. Celostnost podatkov pa, da jih ne morejo brisati ali spreminjati nepooblašчени uporabniki.

Dostopnost

Dostopnost se kaže tako v dostopnosti do podatkov, kakor tudi do servisov računalniškega sistema. Različni pogledi na dostopnost vsebujejo:

- prisotnost objektov ali servisov v uporabni obliki
- zmožnost dostopa do servisa, ki ga potrebujejo
- napredovanje, razvijanje omejevanje čakalni čas

- primeren časovni odziv servisov

Glavne stvari dostopnosti so:

- časovna odzivnost
- uporabnost
- kontrolirana istočasnost; podpora hkratnemu dostopu, mrtvi objem, ekskluzivni dostop

Dostopnost vseh informacijskih virov v računalniškem sistemu je vse pomembnejša. Verjetnost, da bi bila storitev onemogočena ali da bi bila njena uporaba močno okrnjena, mora biti zmanjšana na minimum.

Ranljivost računalniških sistemov

Ranljivost računalniškega sistema gledamo z vidika njegovih sestavnih delov : strojne opreme, programske opreme in podatkov. Na sliki 20 je prikazana ranljivost računalniškega sistema na njegove sestavne dele.



Slika 20 Ranljivost rač. sistemov

Grožnja, ranljivost strojne opreme

Strojna oprema predstavlja fizičen del računalniškega sistema in je tako dovzetna na fizične poškodbe. Strojna oprema mora biti ustrezno varovana in zaščitena (varovani prostori, zaklepanje računalnikov, nedostopnost ipd). Ne smemo zanemariti tudi čiščenje in ustrezno vzdrževanje ter rokovanje (občutljivost na prah, tekočine, spremembo temperature ipd).

Grožnje, ranljivost programske opreme

Strojna oprema ne deluje brez programske opreme. Spremembe na strojni opremi so hitro opazne, medtem, ko se spremembe programske opreme težko ali sploh ne opazijo. Kot obliko ranljivosti in groženj programske smatramo:

- brisanje programske opreme; namerne ali nenamerno
- spreminjanje, prikrojevanje programske opreme med katere prištevamo tudi Trojanske konje, viruse, stranska vrata, informacije o slabosti programske opreme.
- kraja in nelegalno kopiranje programske opreme

Grožnje, ranljivost podatkov

Podatki so podobno kot programska in strojna oprema dovzetni na napake, izgube, zlorabe in druga. Iztiskani podatki so predmet fizične zaščite in so kot taki vsem vidni.

Z vidika groženj in varovanja podatkov je pomembna tudi časovna pomembnost podatkov, ki jih imamo. (Zastareli, nepomembni podatki ne potrebujejo več enake stopnje varovanja kot trenutno aktualni –

odvisnost).

Podatke uporabljajo ljudje, programska in strojna oprema, zato grožnje na njihovo varnost ogrožajo tudi varnost podatkov:

- shranjevanje podatkov na shranjevalni pomnilniške medije (trakovi, CD-zgoščenke, MO diski, in podobno);
- podatki služijo v največji meri ljudem in za njihovi ogrožanje varnosti predstavljajo leti izredno pomemben faktor dostop do podatkov.

Kako se lahko zaščitim pred neželjenimi posegi v moj računalnik?

Obstajajo različni načini nevarnosti za vas in vaš računalnik. Nekateri bi želeli od vas vaše osebne informacije in navade, drugi pa samo onemogočiti ali izrabit vaš računalnik.

Pred čem je potrebno varovati računalnik? Kdo želi nepovabljeno priti na naš računalnik?

- Napadi hekerjev
 - o trojanski konji - Trojan horses
 - o odpoved storitve - Denial of service
 - o zamenjava DNS naslova - DNS spoofing
 - o nadzor paketov, prometa - Packet sniffers
 - o pridobivanje osebnih podatkov - Social engineering
 - o zamenjava prave spletne strani z lažno - Web page defacement
- virusi - virus
- črvi - worms
- neželena okna - pop-ups
- neželena pošta - spam
- škodljiva programska oprema - malware
- vohunska programska oprema - spyware
- fizična zaščita računalnika pred ljudmi in drugimi nevarnostmi

Hekerji ali Hackers

Beseda heker/hacker je izraz za računalniškega entuziasta. Običajno besedo heker povezujemo z osebo, ki želi nepooblaščen dostopiti do tujih računalnikov z namenom uničiti ali zlorabiti podatke. Mnogi hekerji se raje imenujejo krekerji/ crackers.

Hekerji uporabljajo mnogo načinov da vplivajo na delovanje vašega računalnika. Poglejmo si najbolj znane metode:

- Programi trojanski konji/Trojan horse programs
so majhni programi, ki jih "nevede" prenesemo (download) v svoj računalnik z mislijo, da so potrebni za naše delovanje. So škodljivi programi, ki se pretvarjajo, da so nekaj drugega, kot v resnici so. Se ne razmnožujejo samodejno.

- Odpoved storitve/Denial of service attacks
so narejeni z namenom, da onemogočijo določene storitve npr. spletno stran, poštne storitve ali da oslabijo delovanje omrežja. Heker izdelava program, ki neprestano zahteva informacijo od posamezne storitve in tako onemogoča normalno delovanje strežnika in omrežja.

- Zamenjava DNS naslova/DNS spoofing

Hekerji spremenijo DNS številko in tako URL naslov pošlje uporabnika na popolnoma drugo spletno stran. Npr. www.microsoft.com kot URL naslov vas namesto na spletno stran podjetja Microsoft preusmeri na lažno spletno stran, kjer prodajajo avtomobile.

- Pregledovanje paketov/Packet sniffers

je program, ki nadzoruje promet na omrežju. Tako želi iz njega pridobiti informacije, s katerim bi nato lažje prišel v omrežje (na primer uporabniško ime in geslo).

- Pridobivanje osebnih podatkov/Social engineering

je izraz, s katerim se označuje ravnanje hekerjev, ko želijo pridobiti osebne podatke uporabnikov in tako preko njih vstopiti v omrežje.

- Zamenjava prave spletne strani z lažno/Web page defacement

Hakerji zamenjajo pravo spletno stran z lažno in preko nje zbirajo informacije o vas, kreditnih karticah, navadah, osebnih podatkih ipd. (Primer - The CIA, The Republican National Committee, The New York Times).

Virusi ali viruses in črvi ali worms

Obstajajo programi, ki preko omrežja “okužijo” druge računalnike. Delimo jih v dve skupini: virusi/viruses in črvi/worms.

Danes obstaja več tisoč različnih virusov in črvov, ki se aktivirajo in razširjajo oz. razmnožujejo na različne načine.

- Virusi na računalnikih so dobili imena od navadnih bioloških virusov. So mali, samostojno se kopirajo, nekateri mutirajo in ne morejo obstajati brez prenašalca-gostitelja. Virus je torej programska koda, ki “okuži” datoteke na računalniku, lahko zbrise podatke na disku na določen dan, lahko se “igra” z računalnikom, ali pa ne dela čisto nič. Širi se s kopiranjem in zagonom okuženih datotek.
- Črvi so, podobno kot virusi, majhni programi, ki se samostojno kopirajo, vendar za razliko od virusa, ne potrebujejo gostitelja. So bolj nevarni kot virusi. Najbolj znani črvi: Blaster, Sasser, I LOVE YOU.

Nezaželjena elektronska pošta ali E-mail Spam

Nezaželjena elektronska pošta je danes eden najbolj nadležnih problemov. Spam ali nezaželjeno elektronsko pošto predstavljajo tista elektronska sporočila v našem elektronskem nabiralniku, ki jih ne želimo dobiti.

Nezaželjeno elektronsko pošto lahko dobimo na več načinov:

- avtomatsko, preko raznih spletnih čitalcev ali pajkov, ki so izsledili naš elektronski naslov nekje na spletnih straneh;
- prijavili smo se v neko knjigo gostov in tam pustili naš elektronski naslov;
- sodelovali v nekem nagradnem kvizu ali igri;
- enostavno odgovorili na eno izmed nezaželenih sporočil, ki so prispeli na naš naslov;
- naš elektronski naslov je na rumenih straneh oz. v telefonskem imeniku;
- smo člani novičarskih skupin;
- preko spletnih strani, kjer smo vstavili svoj elektronski naslov;
- dobili smo jo od nekoga drugega.

Kdo me nadzoruje?

Obstajajo programi, ki se “pritajijo” v naš računalnik in prevzamejo nadzor in programi, ki takšne odkrivajo. Ti programi so znani kot vohunska programska oprema/adware ali spyware. Ti programi uporabljajo stvari, kot so piškotki/cookies, nadzor/surveillance control in stvari za omejitev dostopa/blocking software. Programi tako spremljajo delo uporabnika in jih javljajo tistim, ki so ta program napisali ali podtaknili v sistem.

Adware tipi programov nas običajno motijo z občasnim pojavljanjem reklamnih sporočil na zaslonu. Ti pa upočasnijo delovanje našega računalnika.

Spyware tipi so pravi vohunski programi, ki zbirajo informacije o nas z namenom, da jih posredujejo nekomu drugemu. Programi upočasnijo delovanje in lahko povzročijo izpad delovanja.

Piškotki ali Cookies

Piškotki so majhne tekstovne datoteke, ki se shranijo v naš računalnik in vsebujejo podatke, kot je prikazano na sliki 21



Slika 21 Datoteka cookies-piškotek

Orodja za nadzor ali Surveillance Tools

Razne institucije želijo imeti nadzor nad uporabniki Interneta in tudi podjetja želijo nadzor nad delom zaposlenih pri uporabi računalnika. Takšne programe za nadzor uporabljajo tudi varnostne službe (FBI DCS 1000 – Carnivore). Nekatera podjetja tudi zanima, katere spletne strani odpirajo njihovi uporabniki ali kaj z računalnikom počnejo. Tako na njihove računalnike namestijo programe, ki spremljajo njihovo delovanje in celo katere tipke in kaj na tipkovnici računalnika so pritisnili (keystroke loggers).

Programi za preprečevanje in blokiranje programov ali vsebin

Popolne zaščite na omrežju Internet ni. Največkrat pa podjetja, starši ali šole želijo preprečiti dostop do programov ali spletnih strani z določeno vsebino.

Obstajajo programi, s katerimi lahko preprečimo zaganjanje drugih programov, ali omejimo upravljanje s računalnikom, tako da lahko uporabnik uporablja samo točno določene programe.

Druga skupina programov pa skrbi za blokado pregleda določene vsebine, tako da definiramo posebne filter, v katerih povemo, kaj se lahko prikaže in kaj ne.

Kako lahko sam pripomore k svoji varnosti?

Katere programe lahko uporabljam?

Dobro je, če ste seznanjeni z možnostmi, ki ga ponuja omrežje Internet. Za kontrolo dostopa, varovanja računalnika in elektronske pošte uporabljamo v glavnem sledeče vrste programov:

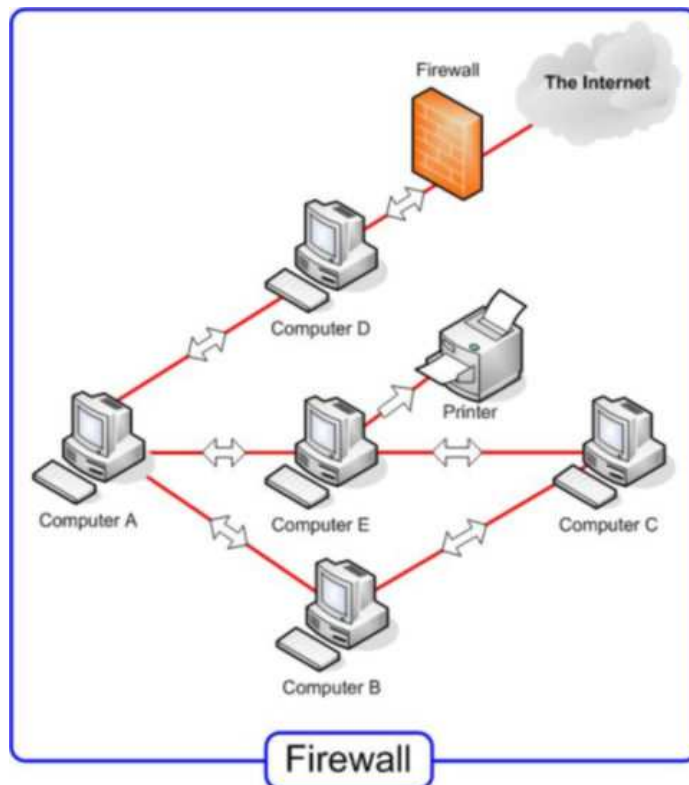
- požarni zidovi/firewalls
- protivirusni programi/anti-virus software
- programi proti nazaželjeni pošti/anti-spam software
- anti ADWARE

Požarni zidovi ali Firewalls

Požarni zid je prepreka – ovira, ki blokira neželjene vsebine. Koncept delovanja požarnega zidu prikazuje slika 22. Običajno je požarni zid sestavljen iz strojne in programske opreme.

Najbolj znani proizvajalci programskih požarnih zidov so:

- Zone Alarm Personal Firewall: <http://www.zonelabs.com/>
- Symantec Firewall: <http://www.symantec.com>
- McAfee Personal Firewall: <http://us.mcafee.com>
- Kerio Personal Firewall: <http://www.kerio.com>



Slika 22 Požarni zid- Firewall

Protivirusni programi ali Anti-virus software

Ena največjih groženj računalniških sistemov predstavljajo virusi. Proti njim se borimo s protivirusnimi programi, ki varujejo naše datoteke, ki so shranjene v našem računalniku preko CD-pogona, diskete, elektronske pošte ali drugega prenosnega pomnilniškega medija.

Nekateri so mnenja, da viruse in protivirusne programe pišejo iste osebe, kar v določenih primerih morda tudi drži. Proizvajalcev protivirusnih programov je veliko. V čem in kako se razlikujejo?

Programi proti nazaželjeni pošti ali Anti-spam software

So običajno dodatki poštnih programov in tako razširjajo svoje funkcije. Sestavljeni so iz naprej definiranih ali lastno narejenih filtrov, s pomočjo katerih preprečujemo nezaželjeni pošti dostop v naš računalnik (na strežniku ali odjemalcu).

Kako se torej obvarujemo pred virusi in nezaželjeno pošto in drugimi nevarnostmi?

Popolnega zagotovila, da smo zaščiteni pred virusi, ni. Lahko pa stopnjo zaščite pred njimi zvišamo z upoštevanjem naslednjih napotkov:

- Redno posodabljanje protivirusnega programa – najbolje nastaviti avtomatsko, če imate to možnost.
- Ne odpirajte priponk v elektronski pošti, ki ste jo dobili, razen če ste sami zahtevali to priponko in veste od koga ste jo dobili.
- Uporabljajte in prenašajte programe od zaupljivega vira. Niso vsa podjetja, ki imajo spletne strani, resnična.
- Izklopite predogled opcijo v poštnem programu.
- Redno posodablajte svoj operacijski sistem. <http://v4.windowsupdate.microsoft.com/en/default.asp>

Kaj pa uporaba varnih spletnih strani?

Največkrat jih srečamo pri povezavah na spletne strani, kjer je varnost na prvem ali višjem mestu.

Predvsem so to bančne transakcijske spletne strani, davčne spletne strani in tiste, pri katerih vstavljamo

podatke, in bi želeli, da na kodiran in varen način prispejo do spletne strani in ponudnika. Kako opazimo, da smo na “varni” ali bolje, varnejši spletni strani? URL naslov se začne s HTTPS in v desnem spodnjem delu okna je ključavnica spletnega brskalnika, kar označuje, da je stran v načinu prenosa SSL -Secure Sockets Layer.

Nekaj napotkov za varnejše brskanje po spletnih straneh

- Nikoli ne dajajte več informacij kot je potrebno.
- Na varnejših spletnih straneh morate pogosto uporabljati uporabniško ime in geslo. Pazite, kako in kaj si izberete (Kaj je dobra izbira?).
- Uporabljajte zadnje verzije spletnih brskalnikov, ker vsebujejo zadnje verzije varnostnih in drugih mehanizmov.
- Preberite varnostno politiko. Najbrž ne želite vaših zaupnih informacij na spletni strani, ki jih bo prodala dalje.
- Hranite zapise vseh vaših internetnih transakcij.

avtor: David Drofenik, ŠC Ptuj

Del gradiva je nastalo 2005 za potrebe višje strokovne šole smer Mehatronika in je bil nadgrajen 2006 v sklopu projekta E-gradiva za računalništvo in informatiko

© 2005-2006, David DROFENIK

