Računari, komponente i skladištenje podataka

Računar se sastoji iz komponenata, ralizličitih delova koji imaju neku ulogu. U komponente spadaju softver i hardver. Softver daje instrukcije dok je hardver taj koji izvršava radnje. Zajedno čine sistem u kojem svaka komponenta saradjuje sa drugom. Međusobno su zavisne, ako jedna ne radi kako treba niz ostalih će biti na neki način uslovljene neispravnom komponentom.

Hardverske komponente se dele na unutrasne i sporedne. Unutrašnje se nalaze u kućištu ili telu laptopa a sporedne van računara. Komponente unutar kućišta realizuju sam rad računara i svi računari ih poseduju. Sporedni ili ulazno-izlazni uređaji mogu imati razne funkcije i većina je neobavezna.

Hardver tj. njegova elektronska kola izvršavaju programe na mašinskom jeziku. Kod računara jako su bitna logička kola koja su izgrađena od tranzistora i predstavljaju najmanju jedinicu. Svako kolo ima jedan ili više digitalnih ulaza (na koje prima signale u vidu jedinica i nula) i izlaz na kome se pojavljuje neka funkcija ulaznih podataka na primer AND (konjukcija) i OR (disjunkcija).

Računar

Kada kažemo računar često mislimo na najčešće korišteni lični računar (PC) koji svako poseduje kod kuće. Ovi računari često nisu skupi i zadovoljavaju potrebe korisnika. Pošto ne obrađuju veliu količinu podataka, akcenat je na korisničkom interfejsu i jednostavnosti korišćenja. Laku navigaciju i za najmanje upućene korisnike omogućavaju savremeni intuitivni operativni sistemi.

Lični računari sa savremenim operativnim sistemom omogućavaju i višekorisnički rad poput serverskih sistema.

Pored ličnog postoje i mejnfrejm (mainframe) računari koji su mnogo većih dimenzija jer obrađuju industrijki i državni nivo količine podataka. Ti računari moraju imati puno snage za brzo rešavanje složenih zadataka. Koriste se za popis stanovništva, industrijske i potrošačke statistike, planiranje resursa preduzeća i obradu transakcija. Pored brzine, zahteva se visoki nivo sigurnosti zbog vrste podataka, zato mora da ima složen sistem enkripcije za koji je potrebna velika procesorska moć.

Super kompijuteri su vrsta računara koji su slični mejnfrejmovima. Za razliku od mejnfrejm računara, nisu za komercijalnu upotrebu već se prave za specifične zadatke. Ovi računari dostižu i definišu rekorde za brzinu obrađene informacije. Koriste se u naučne svrhe za numerička izračunavanja. Simuliraju razne fizičke procese kojima doprinose najsloženijim naučnim divizijama poput kvantne mehanike. Njihova brzina se meri posebnom jedinicom zvanom LINPACK. Meri se brzina izvršavanja složenih funkcija, tačnije FLOPS (floating point operations per second.)

IBM-ov Summit, trenutno(2019.) najbrži superkompjuter na svetu

Unutrašnje komponente računara

Unutrašnje komponente imaju svakakve osetljive delove, zato su predviđene da stoje unutar kutije koja je namenjena da drži sve delove sigurno i štiti komponente od spoljašnjih smetnji.

Ta kutija se naziva kućište, ali se tim nazivom često misli na kutiju sa svim komponentama unutra. Savremeno kućište treba da ima rezervisano mesto za:

- Matičnu ploču,
- Napajanje,
- Grafičku karticu,
- Uređaje za skladištenje podataka i
- Optičke uređaje

Kućište i komponente

Kompakt diskovi su se pojavili 80-ih godina i polako dolazi do kraja njihove upotrebe. Ovakav tip fizički prenosivog skladišta podataka se pokazao neefikasnim pojavom klaud drajvova i praktičnijih USB stikova. Zato se i u novim računarima često izostavlaju optički čitači.

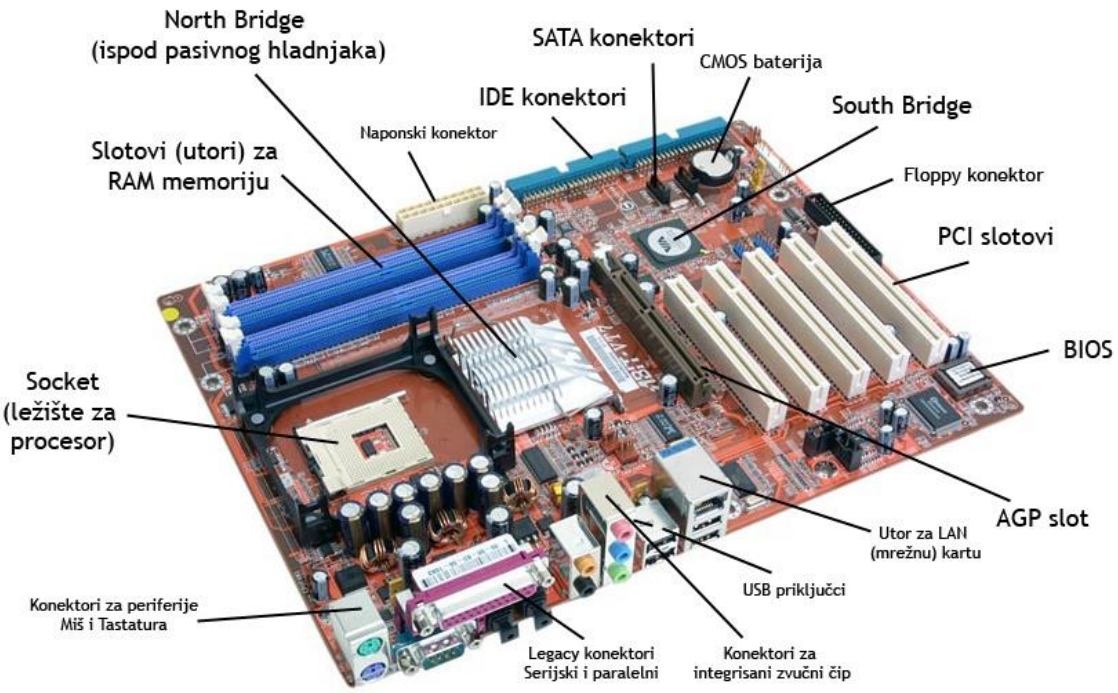
Sistem za napajanje računara (Power Supply Unit - PSU) pretvarač je koji od naizmenične struje pravi jednosmernu, slično punjaču za mobilne uređaje. Međutim, ono što ga razlikuje od ostalih „adaptera", jer ima izlaze na više od jednog napona. Bez obzira na to što se na krajevima „pramena žica" četvrtaste kutije nalazi nekoliko vrsta konektora, svaki od njih može da ima nekoliko napona. Dakle, napajanje računara prevodi naizmeničnu struju na 220 V u jednosmernu struju na tri (tačnije rečeno pet) naponskih nivoa.

Matična ploča

Drži i pruža komunikaciju među najvažnijim delovima sistema, kao što su procesor i memorija, i sadrži ulaze za povezivanje drugih ulazno-izlaznih uređaja. Iako služi za držanje komponentata, njena izrada, magistrale, čipset i soketi, su veoma bitni i utiču na performansu celog sistema. Izrađuju se prema različitim standardima. Form Factor je standard koji određuje oblik i veličinu matične ploče. Prilikom kupovine ili unapređivanja računara bitno je obratiti pažnju na kompatibilnost sa procesorom. Zato što se matične ploče izrađuju prema različitim standardima i procesor se mora poklapati sa tim standardom, podrazumeva se da proizvođač navede te detalje.

Delovi matične ploče:

- **Čipset** - Glavni deo koji vezuje sve ostale delove sa procesoromte šalje CPU informacije ostalim delovima, sastoji se od dva dela: NorthBridge i SouthBridge.
  - NorthBridge: NorthBridge je direktno konektovan sa procesorom (CPU) preko FSB-a (Front Side Bus ili Sabirnica) što omogućava brzu dostupnost podataka iz memorije i grafičke. Od njega najviše zavise performanse matične ploče te je integrisan na matičnu ploču što znači da se ne može menjati.
  - Southbridge: Southbridge je sporiji od Northbridge-a te sve informacije iz CPU-a idu prvo preko Northbridge-a pa tek onda na Southbridge koji je sabirnicama spojen na PCI, USB, zvučni čip, SATA i PATA konektore itd.
- **Socket**: Socket određuje koju vrstu procesor možemo staviti u matičnu ploču. Postojao je univerzalni soket ali njega Intel napušta praveći sopstveni socket čime dolazi do današnje podele na sockete za Intel (i VIA ga koristi) i AMD. Danas je nemoguće staviti AMD-ov procesor u matičnu ploču koja podržava Intel socket (i čipset). Ispod ćemo nabrojati neke od najpoznatijih socketa:
  - Socket 7 - Zadnji univerzalni socket za PC kompjutere
  - Socket 478 - Za starije Pentium i Celeron procesore
  - Socket LGA775 - Za nove Intel Pentium 4 proceosore
  - Socket A - Za stare AMD procesore
  - Socket 754 - Za AMD procesore
  - Socket 939 - Za AMD procesore
  - Socket AM2 - Za AMD procesore
- **BIOS**: Basic Input/Output System (BIOS) kontroliše primitivne fukncije računara i svaki put proverava svoje stanje kod paljenja računara.
- **Memorijski slotovi**: Služe kao dom za RAM memoriju, obično ih ima više.
- **PCI slotovi**: PCI (Peripheral Component Interconnect) konektori za zvučne, TV, mrežne pa i grafičke karte.
- **AGP port**: Accelerated Graphics Port (AGP), konektor namenjen za grafičke karte, karakteriše ga veća brzina od PCI-a.
- **IDE konektori**: Integrated Drive Electronics (IDE), služi za spajanje PATA hard diskova, optičkih uređaja (DVD/CD-ROM/RW), obično nalazimo dva konektora.
- **SATA konektori**: Serial Advanced Technology Attachment (SATA) je nešto noviji od PATA, služi za konektovanje SATA hard diskova, i logično donosi bolje mogućnosti, sam konektor je nešto manji i praktičniji.
- **USB priključci**: Universal Serial Bus (USB) služi za priključivanje spoljašnjih uređaja (štampača, USB stikova,...).
- **Legacy konektori**: Reč je o stvarno ostarelim i prevaziđenim konektorima (Serijskom i Paralelnom), još su uvek tu radi podrške starih uređaja iako se sve manje koristi, odlikuje ga mala brzina.
- **Konektori za periferije**: Konektori za miš i tastaturu su takođe veoma dugo s nama i nisu se previše mijenjali. Danas se sve više miševi i tastature prave za USB standard.
- **CMOS baterija**: Pamti neke vitalne i osvnovne postavke, takođe sadrži u sebi sistemski sat.
- **Integrisani delovi**: Večina ploča danas ima već ugrađene audio (zvučne), mrežne pa i grafičke čipove.
- **Naponski konektor**: Preko njega matična ploča dobija struju (od napojne jedinice), te je raspodeljuje ostalim delovima na matičnoj ploči.



Matična ploča

Procesor

Procesor, centralna procesorska jedinica ili CPU (Central Processing Unit) je srce računara. CPU preveden je u procesor, ali to ne znači da postoji samo jedan tip u računaru. Grafička karta sadrži procesor drugačije arhitekture.

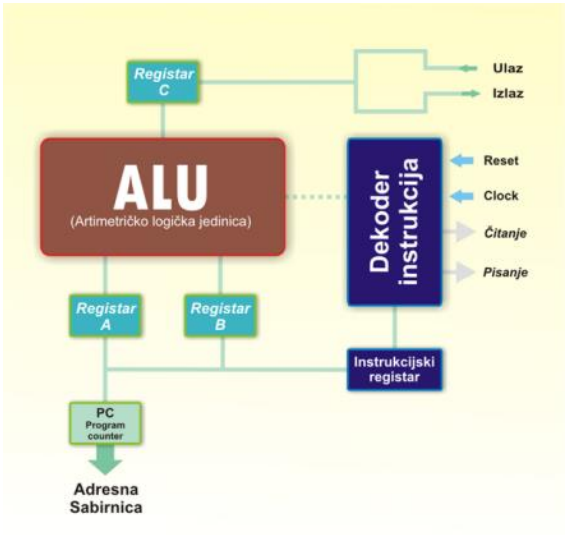
Njegova glavna uloga je da radi sa programima iz glavne memorije, uzimajući njihove instrukcije, ispitujući ih i izvršavajući ih jednu za drugom. Komponente u računaru povezane su magistralom odnosno sabirnicom.

Procesor se sastoji iz upravljačkih jedinica, aritmetičko-logičke jedinece, male memorije velike brzine koja se koristi za skladištenje privremenih resurasa i upravljačkih podataka.

Najvažniji registar je programski brojač. On ukazuje na instrukciju koje treba sledećada se preuzme za izvršavanje.

Putanja podataka tipičnog Von Njumanovog procesora sastoji se od registara, ALU imagistrala koje povezuju komponente.

Dva vodeća proizvođača koja se bore za tržište su Intel i AMD. Oba proizvođača imaju svoje linije procesora koje zadovoljavaju različite korisnike. Obično Intelov procesor je bolji od AMD-ovog ekvivalenta po performancama i potrosnji energije, ali ima veću cenu.



Šematski prikaz najjednostavnijeg procesora

Grafička kartica

Moderne grafičke kartice ili video kartice su opremljene snažnim grafičkim procesorima koji svojom procesorskom snagom i brojem tranzistora gotovo nadmašuju glavne procesore. Grafički procesor obrađuje podatke koje dobija posredstvom neke sabirnice.Grafička kartica se ugrađuje u matičnu ploču, obično u AGP ili PCI Express slot.Pretvara binarni kod u vidljivu sliku na nekom grafičkom izlaznom uređaju(monitor). Sama arhitektura čipa je najbitnija, što znači da njegove instrukcije i brzina izvođenja istih su glavne odlike jednog GPU-a.

Neki procesori sadrže integrisanu grafičku karticu koja uklanja potrebu za posebnom komponentom, sve dok se koristi za poslove koji nisu grafički zahtevni. Integrisana grafička je ustvari deo procesora (jezgro ili tred) rezervisan za procesiranje grafičkog sadržaja. Taj rezervisani deo je mnogo slabiji od samostalnih grafičkih kartica. Iako se nalazi u kućištu, samostalna kartica je tehnički periferna komponenta jer se ne nalazi u direktnom sastavu sa matičnom pločom.

Većina podataka koji dolaze za obradu se privremeno smešta na memoriju koja se nalazi na grafičkoj kartici. Time se obezbeđuje brz protok i samim time brža obrada grafike, što na kraju daje veći broj slika u sekundi čineći grafički proikaz čistijim i lepšim. Zbog toga proizvođači nastoje poboljšati brzinu RAM-a na kartici koja je davno prevazišla brzinu sistemskog RAM-a. Brzina memorije na grafičkoj kartici je već odavno prešla gigahercne granice.

Moderna grafička kartica

Spoljašnje komponente računara

Periferni uređaj je bilo koji uređaj koji se povezuje i radi sa računarom da bi preneo ili preuzeo informacije od njega.

Povezuju se kablom (USB, hdmi,VGA) ili bežično(Bluetooth) sa matičnom pločom. Procesor obrađuje informacije koje sprovode PCI, VESA local(VL) i ISA magistrale.

Periferni uređaji se često nazivaju i spoljašnje periferije, integrisane periferije, pomoćne komponente ili ulazno- izlazni (I/O) uređaji.

Obično reč periferni se odnosi na spoljašnje uređaje (poput skenera) ali, po definiciji, periferni uređaji se nalaze i u kućištu računara. Periferni uređaji doprinose funkionalnosti računara, ali nisu deo glavne grupe komponenata poput procesora matične ploče i sistema za napajanje. Iako ne učestvuju u glavnim procesima ne znači da nisu obavezni delovi sistema.

Periferni uređaji se mogu kategorisati u tri grupe: ulazni, izlazni i ulaznjo izlazni.

Ulazni, ulazno-izlazni i izlazni uređaji

Ulazni uređaji se tako zovu jer računar od njih dobija informaciju. Uređaji koji spadaju u tu grupunajčešće dozvoljavaju korisniku da upravlja sistemom. Za upravljanje se koriste tastasture i razni ručni uređaji poput miša, džojstika i grafičkih tabla. Informacije koje mogu preneti računaru dolaze u različitim oblicima. Postoje razni senzori koji prenose podatke iz neke sredine na primer senzor za temeraturu,pritisak itd. U ulazne uređaje spadaju i mikrofoni, kamere skeneri.

Kod **izlaznih uređaja** informacije putuje u suprotnom smeru, računar je taj koji ih šalje. Najčešće ti uređaji daju sadržaj u video ili audio formatu. Tu spadaju monitori, video bimovi, štampači, zvučnici i slušalice.

Skladištenje podataka

Memorija je deo računara u kome se čuvaju podaci i programi. Oni se skladište u memoriju i iščitavaju iz nje na zahtev korisnika.

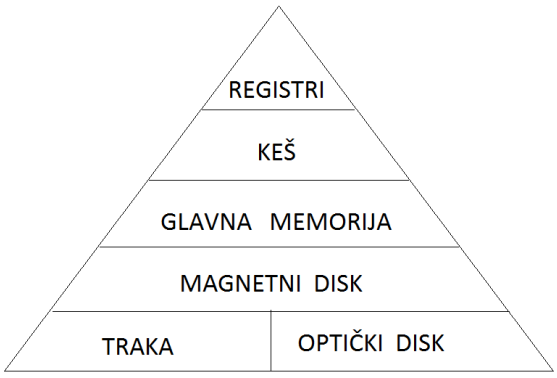
Osnovna jedinica memorije jebiti može da ima vrednost 0 ili 1.Memorija se sastoji od ćelija i lokacija od kojih svaka čuvainformaciju. Svakoj ćeliji je pridružen broj nazvan adresa, pomoću koje mogu programida je nađu.

Hierarhija

Rešenje za skladištenje velike memorije je hijerarhijsko organizovanje memorije.

Na vrhu se nalaze registri procesora kojima procesor može pristupati punom brzinom. Ispod njih je keš memorija čija je veličina trenutno od 32kb do nekoliko mb. Zatim glavna memorija od 16Mb do 10Gb. Onda idu magnetni diskovi za trajno skladištenje podataka. Na kraju magnetne trake i optički diskovi za arhivu podataka.

Primećujemo da od vrha pa na niže raste kapacitet memorije, a takođe raste i vreme pristupanja memoriji.



Hierarhija memorije

Keš memorija

Mala memorija velike brzine. Keš je načinjen da bi se u njemu čuvale najčešće korišćene reči.

Procesor pristupa glavnoj memoriji samo ako traženu reč ne nađe u kešu. Ima ulogu bafera između procesora i glavne memorije. Ako se u kešu nalazi bitan deo najčešće korišćenih reči, prosečno vreme pristupanja se skraćuje.

Poštujući princip, glavne i keš memorije se dele u blokove fiksne veličine. Kada govorimo o takvim blokovima unutar keša, obično ih zovemo redovi keša. Kada dođe do promašaja u kešu, iz glavne memorije se u keš učitava čitav red.

Projektovanje keša postaje važnije za visoke performanse. Što je veći, bolje su mu performanse ali i skuplji.

Glavna ili primarna memorija – ram i rom memorija

Glavna memorija zadržava samo one podatke i instrukcije koje računar trenutno koristi. Ima mali kapacitet(danas najčešće 4 do 8 gigabajta) ali je brža od sekundarne(spoljašnje memorije) i podaci se gube pri isključivanju računara. Glavna memorija se deli u dve podgrupe: ram i rom memorija.

RAM memorija je memorija sa direktnim pristupom, omogućava čitanje i upisivanje podataka. Postoje dve vrste ram memorije: statička i dinamička.

Statička RAM memorija (SRAM) – interno se konstruiše pomoću logičkih kola. Ova vrsta memoirje čuva podatke sve dok postoji napajanje (nekoliko sekundi, minuta). SRAM su vrlo brze. Tipično vreme pristupanja iznosi nekoliko nanosekundi. Zbog toga je statička ram memorija popularna i kao keš memorija drugog nivoa.

Za dinamičku ram (DRAM) memoirju ne koriste se flip flopovi(logička kola). Za razliku od statike ona se sastoji od niza ćelija, a svaka sadrži jedan tranzistor i mali kondenzator. Kondenzator se može ispuniti i prazniti čime se omogućava čuvanje logičkih nula i jedinica. Svaki bit u dinamičkoj memoriji se mora osvežavati na nekoliko milisekundi da bi se odgovarajući kondenzator pnovo punio. Zbog toga se DRAM složenije realizuje od statike memorije. DRAM je spora memorija, kombinacija SRAM za keš memoriju i DRAM za glavnu memoirju je optimalno rešenje jer se iskorišavaju dobra svojstva obe memorije.

ROM memorija je memorija čiji se sadržaj ne mže promeniti niti obrisati. Podaci se u rom unose tokom njegove proizvodnje.Ovi cipovi su mnogo jeftiniji od RAM cipova , takodje su i manje fleksibilni jer se ne mogu menjati po izlasku iz proizvodnje.

Glavna memorija

Sekundarna memorija

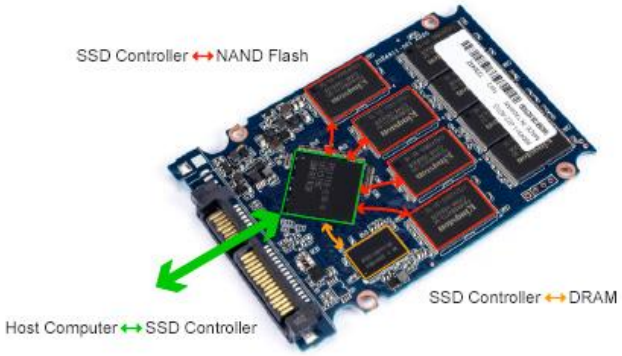
Ova memorija je poznata kao spoljašnja ili pomoćna. Spada u računarske periferije. Sporija je od glavne i koristi se za stalno skladištenje. Podaci ostaju na njoj dok se ne obrišu manuelno. Procesor ne pristupa ovoj komponenti direktno već preko ulazno izlaznih magistrala. Sadržaj spoljašnje memorije se prebacuje prvo u glavnu memoriju i onda procesor može da pristupi podacima. U početku, 60-ih godina, sekundarnu memoriju su predstavljale bušene kartice koje je računar mogao da izčitava. Od 80-ih do danas najkorišćeniji su magnetni diskovi, magnetne trake i optički diskovi.

Magnetni diskovi – sastoji od 1 ili nekoliko aluminijumskih ploča presvučenih slojem koje se namagnetišu. Ploče su prečnika od 3 do 12 cm dok je prečnik diskova za prenosive računare već manji od 3 cm. Glava diska koja sadrži indukcioni kalem, klizi neposredno iznad njegove površine na vazdušnom jastuku. Kada kroz glavu prolazi struja u jednom ili drugom smeru, ona magnetizuje površinu neposredno ispod sebe, usmeravajući magnetne čestice ulevo ili udesno. Kada glava prelazi iznad namagnetisanih područja u njoj se indukuje struja jednog ili drugog smera, što joj omogućava da pročita ranije uskladištene bitove informacija.

HDD ili hard disk driveje sačinjen od više aluminijumskih ploča naslaganih na osovini. Ovaj tip pomoćne memorije je najpopularniji zbog svog kapaciteta i relativno niske cene.

SSD(solid state drive) za razliku od HDD diskova nemaju pokretnih delova koji su osetljivi, i možda je najlakše da se zamisle kao velike "USB fleš memorije", mada treba imati u vidu da se memorijski čip u SSD disku razlikuje po tipu i brzini od onog u USB fleš memoriji. Ovakva konstrukcija SSD diskova omogućava znatno brže čitanje podataka sa njih što korisniku omogućava da se znatno brže učitava operativni sistem, startuju aplikacije i ukupno gledano ubrza rad računara.

Govor o SSD-u je počeo još 70-ih godina ali 2014. je stekao veliku popularnost na tržištu i SSD sve češće zamenjuje HDD u ličnim računarima. Od kada je ova tehnologija za skladištenje podataka postala pristupačnija i povoljnija, korisnici imaju mogućnost da još više ubrzaju rad svojih računara, ako imaju računar koji nije stariji od 4 godine.



Arhitektura SSD-a

Serveri

Prvobitno reč server se odnosi na računarski program ili proces. Odatle uređaj koji vodi jedan ili više serverskih procesa dobija isto ime. U svojoj mreži taj uređaj je host(domaćin).

Server je deo klijent-server modela, gde server raspolaže keširanim podacima za klijente. Način komunikacije između klijenta i servera je zahtev i odgovor. U principu svaki računarski proces koji može da se pozove od strane drugog procesa je server. Tako da svaki obični računar povezan na neku mrežu može da vodi(host) servere. Na primer ako se podaci dele preko nekog procesa, taj proces je server datoteka. Slično internet server softver može da radi na svakom osnovnom računaru, zato mogu laptop ili lični računar da vode internet server bez tegoba.

Hardver servera nema standardni oblik i organizaciju. U potpunosti zavisi od njegove uloge. Većina servera imaju zajedničko to što mogu da rade bez konstantnog nadgledanja i nemaju način za direktno upravljanje sistemom. Normalno je da nemaju monitor, zvučne uredjaje i USB interfejs. Često jedini vid povratne informacije i manipulacije preko programa poput Microsoft Menagement Console(MMC) koji dozvoljava administratoru da nadgleda i konfiguriše sistem samo kada je to potrebno.

Tradicionalni serveri bi trebali da rade neprekidno duži niz godina. Snose veliku odgovornost i postoji šansa da organizacija ne može da funkcioniše bez rada servera. Zato je kod hardvera naglasak na sigurnost i izdržljivost. Koristi se hardver specijalizovan sa niskom verovatnoćom kvara. Radi sprečavanja prekida koriste se takozvani neprekidni sistemi za napajanje. Ti sistemi čuvaju višak energije za neopčekivan gubitak struje. Serveri tipično imaju hardverske redudancije radi sigurnosti kao što su dvojni sistemo za napajanje, RAID diskovi i ECC memorija. Trebali bi da sadrže komponente koje mogu da sa zamenjuju na mestu, bez potrebe za prekidanjem sistema. Serverska kućišta su široka i niska, pločastog oblika dizajnirana da stoje kao polica naslagana jedno iznad drugog. Često su im dodeljene posebne sobe sa uslovima za rad servera. Serverske sobe ili data centri moraju da imaju dobru kontrolu temperature pošto uređaji za hlađenje koje ima svaki pojedinačni server ponekad nisu dovoljni. Zbog opasnosti pregrevanja serveri često koriste vodene sisteme hlađenja.

Serveri u data centru

Glavnauloga servera je da deli podatke i resurse. U zavisnosti od vrste podatka potrebna korisniku i uloge postoje više vrsta servera.

Server baznih podatakaodržava i deli sve oblike baze preko neke mreže. Podaci su organizovani u tabele sa predefinisanim odlikama.Klijent je softver namenjen upravljanjem i čitanjem baza podataka pogotovo u velikim količinama koje koriste državne organizacije, banke itd.

Proxy Server predstavlja posrednika između klijenta i nekog drugog servera. Klijent se povezuje na proxy server, tražeći neke podatke ili konekciju od nekog servera, proxy onda ocenjuje taj zahtev pre nego što ga prosledi. Tako smanjuje teret na serveru sa resursima i daje strukturu distribuiranim sistemima.

Web(internet) serverisu ti koji realizuju konekciju sa internet mrežom. Jedan server može držati jednu ili više web stranica. Obrađuje dolazne mrežne zahteve preko HTTP protokola. Klijent dobija najčešće informaciju u formi HTML dokumenta koji može da sadrže slike preglede i druge vidove tekstualnog sadržaja.

BACKUP I STORAGE SISTEMI

Skladištenje podataka je jedna od najvažnijih funkcija svakog IT okruženja kod korisnika bilo koje veličine. Generalno posmatrano samo smeštanje podataka se najčešće može podeliti na 3 nivoa:

– **Primarno smeštanje podataka**

podaci koji se svakodnevno koriste u produkciji se smeštaju na jedan ili više uređaja

–

Backup (rezervnakopija) podataka

kao medijum se koriste trake ili u zadnje vreme diskovi ili kombinacija

–

Arhiviranje podataka

čuvanje podataka na duži rok po određenim polisama. Podaci se mogu arhivirati na trake, diskove ili magneto-optičke medije.

U svim katastrofičnim scenarijima je bekap podataka i aplikacija, te njihov brzi povratak i oporavak od ključnog značaja za brzo vraćanje funkcionalnosti. Izrada rezervne kopije backup je potreba kako pojedinčnih korisnika i malih preduzeća , tako najvećih I najavažnijih sisteme kao što su banke i finansijske organizacije, država itd. U kućnom okruženju, držanje backup-a na udaljenoj lokaciji znači samo jedno – upotrebu servisa zasnovanih na cloud-u, kao što su Dropbox ili Microsoft OneDrive.

Izbor uređaja za backup

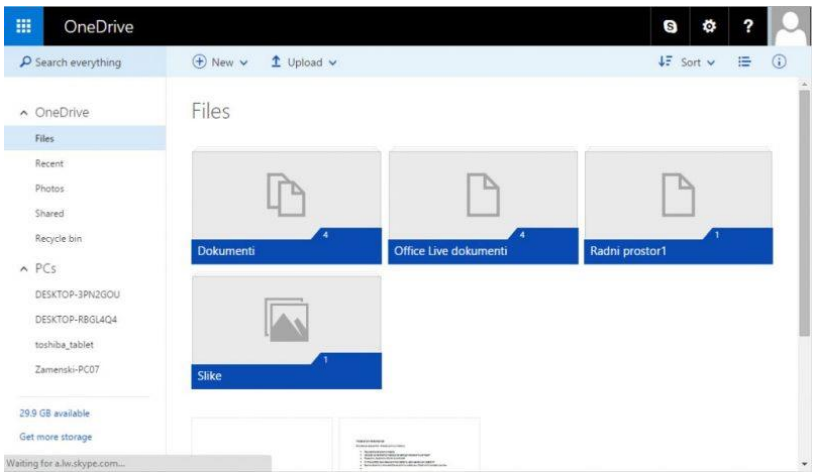
Bilo bi idealno da se backup podataka radi na dva različita medija istovremeno. Prvo pada na pamet dodatnidisk; eksterni ili interni. Preporučujese da se on koristi za image kompletnog sistema. U tu svrhu moguće je koristiti alat koji dolazi uz operativni sistem ili neki od nezavisnih (besplatnih) programa, kao što je Macrium Reflect Free.

Mrežni hard-disk je sekundarno rešenje. Može se čuvati na nekoj udaljenoj lokaciji ili u lokalnoj kućnoj mreži. Čuvanje podataka u cloud-u takođe je česta varijanta, a najpoznatiji servisi tog tipa jesu Dropbox, Microsoft OneDrive i Google Drive. Bezbednost možete da poboljšate upotrebom servisa Viivo za šifrovanje podataka pre slanja na pomenute sisteme. Ako vam ni to nije dovoljno sigurno, onda je pravo rešenje za vas lični cloud storage sistem kao što je OwnCloud.

Dobar izbor za čuvanje rezervnih kopija podataka jesu i drugi računari. Ukoliko posedujete više računara, možete da sinhronizujete podatke na njima. Bonus koji se dobija ovim načinom pravljenja rezervnih kopija jeste to što su svi podaci koje koristite uvek dostupni na svim računarima.

Još jedno dobro rešenje, o kojem verovatno niste razmišljali, jeste razmena slobodnog prostora na hard-diskovima s rođacima ili prijateljima u koje imate poverenja – na vašem računaru možete da čuvate njihove backup-e, a oni na svojim vaše. Malo „paranoje“ nije naodmet, pa se pre nego što razmenite podatke pobrinite da oni budu šifrovani, ako ništa drugo Winzip-om.

Backup podataka



Windows 10 nudi dva osnovna načina za backup podataka – Backup and Restore i File History. Oba se fokusiraju na kreiranje rezervnih kopija bitnih dokumenata, fotografija i drugih ličnih podataka, kao i fajlova iz operativnog sistema koji mogu da se prekopiraju na bilo koji drajv vidljiv na računaru, uključujući i mrežne diskove.

Osnovno pravilo backup-a jeste da se napravi više kopija na različitim lokacijama. Ni File History ni Backup and Restore ne dozvoljavaju backup na alternativne lokacije, ali ukoliko koristite Windows 10, možete da prevaziđete to ograničenje. Konfigurišite File History tako da podatke kopira jednu lokaciju, recimo na drajv koji je fizički povezan na računar, a Backup and Restore podesite da podatke kopira na neku drugu lokaciju, recimo, u šerovani folder na mrežnom disku. File History konstantno prati promene na sistemu i pravi backup po potrebi, dok Backup and Restore može da se podesi da kreira backup u redovnim intervalima (nedeljnim, mesečnim…) ili u vreme kada znate da nećete raditi na računaru.

Kopija operativnog sistema

Svako ko je makar jednom reinstalirao sistem od nule zna koliko je to mukotrpan posao i da su potrebni dani da se svi programi, drajveri i alati dovedu u funkcionalno stanje. Za takve slučajeve idealna je tzv. slika sistema (drive image), koji pomenuti posao skraćuje na jedan sat. Windows će ponuditi da napravi image fajl prilikom setovanja Backup and Restore alata, ali u njemu postoje slabosti. Prvo, svaki backup takvog tipa zahteva desetine, pa i stotine gigabajta prostora na hard-disku. Drugi, mnogo važniji problem jeste to što tako kreirani image fajlovi nisu verifikovani i ne postoje garancije da su ispravni. Najzad, image fajlovi se čuvaju samo na jednom drajvu.

Pomoću nezavisnog programa Macrium Reflect eliminišu se sve tri slabosti. Besplatnu verziju možete da preuzmete sa adrese www.macrium.com/reflectfree.asp. Problem prevelikog zauzimanja prostora on rešava upotrebom diferencijalnog image fajla, koji zauzima mnogo manje mesta zahvaljujući tome što snima samo izmene koje su napravljene od poslednjeg backup-a.

Preporučujemo da na mesečnoj bazi kreirate kompletan backup, a da na dnevnoj bazi uključite Differential Backup Setšablon. Napravite još jedan šablon sa istim podešavanjima, ali pozicionirajte backup fajl na neku drugu lokaciju. I na kraju, kada vas program upita za kreiranje Rescue medija, odgovorite potvrdno i napravite DVD ili USB flash drajv koji će vam pomoći da oporavite sistem čak i ako nakon Windowshavarije ne uspeva da se startuje.

Sve se ovo može uraditi u besplatnoj verziji Macrium Reflect programa. Ukoliko vam je potrebno nešto više, kao što su inkrementalni backup-i ili backup pojedinačnih fajlova i foldera, razmislite o komercijalnoj verziji programa Macrium Reflect Home Edition.

Cloud rešenja

Danas se cloud nameće kao glavna lokacija za backup podataka, pošto čuvanje podataka u oblaku osigurava da će jedna od kopija podataka biti na sigurnoj, udaljenoj lokaciji, što je važno u slučaju krađe, požara ili neke druge katastrofe. Većina ljudi opredeljuje se za backup u cloud prostor koji se nalazi u vlasništvu neke poznate kompanije, kao što je Microsoft i njegov OneDriveservis, koji je još i uključen u Windows 10. Često korišćene alternative kojima se veruje jesu Dropbox (www.dropbox.com) i Google Drive (drive.google.com).

Zajednička mana svih ovih servisa jeste to što u osnovnoj (besplatnoj) varijanti nude veoma ograničen prostor, između 5 i 15 GB. Ako vam to nije dovoljno, svi ovi servisi nude mesečne ili godišnje pretplate.

Podaci u cloud-u se šifruju, a ako sumnjate u kvalitet enkripcije, možete sami da ih šifrujete pre nego što ih pošaljete. Verovatno najbolji alat za tu namenu jeste servis Viivo (www.viivo.com), koji radi s različitim cloud provajderima i poseduje mogućnosti za deljenje pristupa s prijateljima i familijom. Ovaj servis je i dalje besplatan za privatnu upotrebu.

Data Centri

Data centar se može definisati kao mesto gde su smešteni ra;unarski sistemi, sistemi za skladištenje podataka i telekomunikaciona oprema. Data centri uklju;uju i sisteme za napajanje, sisteme za backup napajanja (baterije, agregati), protivpožarne sisteme, sisteme za održavanje uslova radne okoline i bezbednosne sisteme. Data centri treba da omoguće kompanijama smeštaj i funkcionisanje njihove IT infrastructure.

Od izbora pravog data centra uveliko zavisi bezbedno, pouzdano i nesmetano poslovanje kompanije. Naravno da ne treba zanemariti ni cenu. Data centar treba da nudi potpunu fleksibilnost u pogledu skalabilnosti, modularnosti, bezbednosti, konektivnosti, nadzora i pristupa. Zatim, treba da ima redundantnu, pouzdanu i otvorenu infrastrukturu, zaštitu za sve kriti ne komponente sistema, kvalifikovano i posvećeno osoblje za podršku 24 sata, 7 dana u nedelji, garantovan stepen i kvalitet usluge. Data centri se danas mogu graditi bilo gde u svetu, jer im se može pristupati preko Internet mreže. Ali se mora voditi računa o nekoliko faktora prilikom izgradnje Data centra. Zbog lakšeg pristupa izvorima elektri ne energije, treba izabrati lokaciju sa dobrom energetskom infrastrukturom. Data centar u oblasti sa hladnijom klimom omogućava prirodno hlađenje i potencijalno niže troškove-izacije.

Savremeni Data centri predstavljaju osnovu današnjeg poslovanja velikih kompanija. Sa uvođenjem tehnika virtuelizacije u Data centre, dolazi se do evolucije samih Data centara, a samim tim i do evolucije u savremenom poslovanju. Virtuelizacija dobija na zna aju i ima najve eg smisla upravo u Data centrima. Rad gotovo svake će kompanije u najvećoj meri zavisi od pouzdanosti i raspoloživosti njenog informacionog sistema. Protok i dostupnost podataka neophodnih za funkcionisanje firme su od krucijalne važnosti i ti podaci se moraju prenositi i skladištiti bez gubitaka. Stoga je svaka karika u lancu prenosa podataka, njihovog skladištenja i procesiranja od kritičnevažnosti. Data centri su jedna od najbitnijih karika u procesrianju podataka, jer informacije i podaci moraju biti dostupni sistemu u pravo vreme, a to e biti mogu e jedino ako se obezbedi pouzdana i bezbedna IT infrastruktura.

OPERATIVNI SISTEMI, SERVERI I SERVERSKI SOFTVER

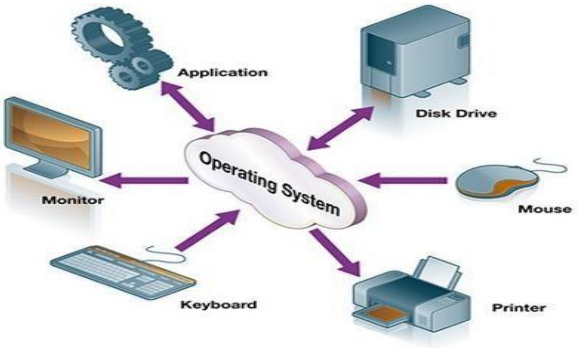
Računarski sistem se grubo može podeliti u dva dela: softver i hardver. Hardver, čiji su najvažniji sastavni delovi procesor, memorija, magistrala i ulazno-izlazni uređaji, obezbeđuje osnovne resurse za funkcionisanje sistema. Pod softverom se podrazumevaju operativni sistem i aplikativni softver. Operativni sistem upravlja hardverom i koordinira njegovo deljenje između različitih aplikacija i korisnika, dok aplikativn programi rešavaju probleme korisnika. U računarstvu, server je program ili uređaj koji puža funkcionalnost drugim programima ili uređajima koji se nazivaju klijenti. Ova arhitektura naziva se model klijent-server. Serveri mogu da pružaju različite funkcionalnosti, poput deljenja podataka ili resursa između više klijenata. Jedan server može služiti više klijenata, a jedan klijent može koristiti više servera. Postupak klijenta može se pokrenuti na istom uređaju ili se može povezati preko mreže na server na drugom uređaju. Tipični serveri su: serveri baza podataka, serveri datoteka , serveri e - pošte, serveri štampača, web - serveri, serveri igara i serveri aplikacija.

Operativni sistemi

Operativni sistem je kompleksan programski sistem sastavljen od skupa programa koji treba da obezbedi lako i efikasno korišćenje računara. Operativni sistem objedinjuje u jedinstvenu funkcionalnu celinu hardver (delove računara) i softver (programe na računaru). U opštem smislu, operativni sistem se može definisati kao skup programa koji upravlja resursima računarskog sistema i obezbeđuje interfejs ka korisniku. Da bi zadovoljio sve ove zahteve, operativni sistem ima funkcije:

- upravljanje perifernim jedinicama,
- upravljanje memorijom,
- upravljanje mikroprocesorom,
- upravljanje podacima iprogramima,
- kontrola funkcije (uključujući otkrivanje i otklanjanje grešaka).

Operativni sistem mora stalno da prati akcije programa i promene u stanju hardvera i da deluje u skladu sa tim promenama. Ovo delovanje operativnog sistema odvija se pozivanjem odgovarajućih sistemskih programa u sastavu operativnog sistema kojima se izvršavaju različiti zadaci, a u skladu sa komandama koje mu je zadao korisnik .



Operativni sistem

Podela operativnih sistema

Operativni sistemi mogu se podeliti na osnovu:

- broja programa koji mogu istovremeno da budu u memoriji,
- broja korisnika koji mogu istovremeno da koriste računar,
- načina zadavanja komandi i
- prenosivosti na različite arhitekture.

Na osnovu broja programa koji istovremeno mogu biti u memoriji, operativni sistemi se dele na:

- Monoprogramske (jednoprocesne)/MS DOS - omogućavaju da računar u memoriji drži i izvršava samo jedan program.
- Multiprogramske (višeprocesne) - omogućavaju da se u centralnoj memoriji računara nalazi više programa istovremeno, od kojih se samo jedan izvršava u jednom trenutku, a vreme i redosled izvršavanja programa određuje operativni sistem.

Na osnovu broja korisnika koji istovremeno koriste računar operativni sistemi se dele na:

- *Jednokorisničke (singleuser)* – naziva se još i desktop operativni sistem budući da je namenjen za rad jednog korisnika (na jednom računaru) i optimizaciju rada korisničkih aplikacija u takvom jednokorisničkom okruženju.
  Primer monoprogramskog operativnog sistema je MSDOS.
- *Višekorisničke (multiuser)* - mrežni operativni sistemi se često nazivaju i serverski operativni sistemi, budući da se instaliraju na server mašinama u klijent – server arhitekturi, omogućavajući korisnicima i njihovim aplikacijama pristup svim resursima povezanim u mrežu.
  Primeri višekorisničkih operativnih sistema su: Novell Net Ware, Windows NT (Now Technology), Windows 2000,Linux.

Na osnovu zadavanja komandi operativni sistemi se dele na:

- *Operativne sisteme komandnog tipa* - Kod operativnih sistema komandnog tipa komande se zadaju ukucavanjem naredbi sa svojim parametrima. Posle uključenja računara na ekranu se dobija određen znak koji se naziva prompt. Ovim znakom operativni sistem obaveštava korisnika da je spreman da primi komandu. Komanda se zadaje ukucavanjem teksta a pritiskom na taster enter na tastaturi naredba se prihvata i započinje njeno izvršenje. Dok se naredba izvršava promt se ne vidi na ekranu, a kada se naredba izvrši na ekranu se prikažu dobijeni rezultati i nakon toga prompt, čime računar obaveštava korisnika da je spreman za prihvatanje nove komande. Najpoznatiji operativni sistemi ovog tipa jesu DOS, UNIX i njemu sličan LINUX.
- *Operativne sisteme sa grafičkim okruženjem* - Kod grafičkih operativnih sistema komande se najčešće zadaju pokazivanjem na nju. Komande su u obliku sličica koje predstavljaju određene komande. Najpoznatiji operativni sistemi sa grafičkim okruženjem su Windows i Linux.

Na osnovu prenosivosti na različite tehnologije operativni sistemi se dele na:

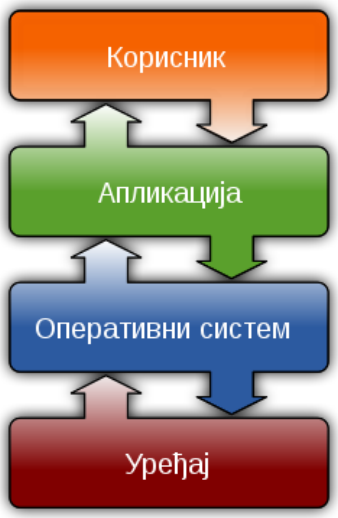
- *Prenosive (portable)* - Prenosivi operativni sistemi, kako im i ime kaže, mogu da se koriste sa malim izmenama na različitim arhitekturama računara.
- *Neprenosive (proprietary-vlasnički)* - Neprenosivi operativni sistemi su projektovani tako da mogu da rade samo na određenom modelu računara.

Programi i podaci sa kojima programi rade moraju biti u centralnoj memoriji računara. Kod prvih računara, ako programi i podaci nisu mogli da stanu u centralnu memoriju računara, program nije mogao da radi. *Virtuelna memorija* je tehnika koju operativni sistem koristi da upravlja lokacijama segmentiranog programa. Prilikom instalacije, operativni sistem rezerviše deo hard diska za smeštanje segmenata programa i podataka (virtuelna memorija).

Ona može biti fiksna (tačno određena vrednost kapaciteta memorije) ili dinamička (operativni sistem menja veličinu virtuelne memorije shodno svojim potrebama).

Keš (cache) memorija je vrlo brza memorija koja se nalazi u samom procesoru (interni keš) ili uz njega na matičnoj ploči (eksterni keš). Ova memorija ima višestruko brže vreme pristupa od obične memorije. Zbog toga se u njoj drže podaci koji se često koriste. Prilikom prvog zahteva za podacima oni se kopiraju iz RAM memorije u keš memoriju. Kada su sledeći put potrebni isti podaci procesor ih prvo potraži u ovoj memoriji. Ako su podaci tu procesor im pristupa mnogo brže, a ako nisu moraju da se ponovo preuzmu iz RAM memorije. Veličina interne keš memorije je danas obično 512MB ili1GB.

Baferi (buffers) su delovi RAM memorije koje neki programi alociraju (rezervišu) za svoje potrebe. Jedna od čestih primena je prilikom ulaza i izlaza podataka. Ako računar ne može dovoljno brzo da obrađuje podatke koji mu pristižu on ih trenutno deponuje u bafer, dok ne stignu na obradu da se ne bi prekidao proces unošenja. Slično, ako štampač ne može da dovoljno brzo odštampa podatke on ih šalje u bafer (spooler) gde čekaju u red zaštampu.



Hijerarhija korišćenja računara

Moderni operativni sistemi

Najveći broj današnjih operativnih sistema za računare može se svrstati udve velike grupe:

Unix i Windows. Unix predstavlja čitavu porodicu operativnih sistema koji vuku poreklo iz originalnog Unix operativnog sistema koji je 1969. godine razvila Bell laboratorija. U ove sisteme spadaju Version 7 Unix ili System V Unix (koji se deklarišu kao tradicionalni Unix sistemi), ali i BSD i Linux. Unix sistemi se koriste na korporacijskim serverima, ali i na radnim stanicama u npr. akademskim ustanovama. Danas je verovatno najpoznatija verzija Unix-a operativni sistem Linux. Linux je sistem čiji kernel je besplatan (u javnom vlasništvu). Razvio ga je Linus Torvalds 1991. godine dok je studirao na Univerzitetu u Helsinkiju, bazirajući se na tada popularnoj MINIX verziji Unix-a.

Danas se svi operativni sistemi koji uključuju Linux kernel nazivaju "Linux". Korisnici danas dolaze do Linux sistema kroz takozvane „distribucije“, koje u stvari predstavljaju pakete koji uključuju kernel i GNU sistem, verzije grafičkog korisničkog interfejsa i određen broj korisničkih programa. Proces instalacije neke od distribucija može varirati od jednostavnih, do onih koje zahtevaju dobro poznavanje Linux-a/Unix-a i računara. Trenutno postoji preko 200 aktivnih distribucija za PC računare, a neke od najpoznatijih su Red Hat, Debian, Ubuntu, SuSE, Fedora, CentOS, Mint i sl. Distribucije obično nisu skupe ili su potpuno besplatne i dostupne na Internetu. Linux je veoma fleksibilan operativni sistem, pa tako svaki korisnik može na osnovu kernela sastaviti sopstvenu verziju. Čak se i izgled korisničkog interfejsa može razlikovati budući da postoje različita grafička okruženja (najpoznatija su svakako Gnome i KDE) koja se mogu koristiti. Trenutno najpopularnija Linux distribucija, namenjena krajnjim korisnicima je Ubuntu, kompanije Canonical. Ubuntu je besplatan, lak za instalaciju i korišćenje. Dolazi "napakovan" korisničkim programima, a instalacija novih aplikacija je maksimalno pojednostavljena zahvaljujući softverskom centru. Razvijen je na osnovu poznate Debian distribucije, a po izgledu se razlikuje od svih ostalih Linux sistema, pošto koristi sopstveno korisničko okruženje Unity.

Poseban kuriozitet su tzv. live distribucije koje ne zahtevaju čak ni instalaciju na računaru, već se pokreću sa nekog uređaja spoljne memorije (CD-a, USB flash memorije i sl). Ove distribucije su idealne za početnike koji bi želeli da isprobaju Linux, bez rizika po svoj računar i postojeći operativni sistem. Zbog toga što zahtevaju malo veći nivo znanja i zbog toga što za Linux i dalje ne postoje verzije velikog broja popularnih Windows programa i igara, ovi sistemi čak i potpuno besplatni i dalje nisu dovoljno zastupljeni na kućnim računarima. Sa druge strane, slika je drugačija kada su u pitanju serverski računari na kojima je Linux cenjen zbog svoje stabilnosti i bezbednosti - i to besplatno. Iza Linux-a danas stoji veliki broj programera iz celog sveta koji pojedinačno ili organizovano razvijaju i održavaju korisničke programe ili delove sistema. Većina tog softvera jebesplatna.

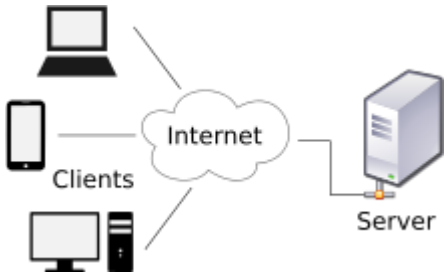
Windows operativni sistemi predstavljaju proizvod firme Microsoft. Prve verzije Windows-a su bile samo grafička nadogradnja starog MS-DOS operativnog sistema. Tek kasnije verzije Windows-a prerastaju u samostalni operativni sistem. Iako komercijalan, Windows je danas najrasprostranjeniji operativni sistem, pre svega zahvaljujući jednostavnom korisničkom interfejsu i dobrom marketingu. Microsoft već godinama razvija dve glavne linije Windows-a: verziju namenjenu radnim stanicama, odnosno računarima u svakodnevnoj upotrebi (Windows 3.11, 95, 98, ME, XP, Vista, Windows 7, Windows 8, Windows 10) i verziju namenjenu serverima (Windows NT, 2000, 2003, 2008...). I unutar ove dve linije postoje različite verzije Windows-a koje se razlikuju po ceni i komponentama koje uključuju (npr. Windows 7 ima nekoliko verzija: Starter, Home Basic, Home Premium, Professional, Enterprise i Ultimate).

Osim ova dva najrasprostranjenija, različiti računari mogu imati različite operativne sisteme. Među poznatima su OS X (nekadašnji Mac OS), koji se koristi na Apple Macintosh računarima i Solaris (SunOS), koji je na osnovu Unix-a razvila kompanija Sun za svoje radne stanice. Stariji operativni sistemi koji se još uvek upotrebljavaju (a neki od njih se čak i dalje razvijaju) su IBM- ov OS/2, Amiga OS, HP-ov OpenVMS. Osim Windows i raznih operativnih sistema na bazi Unix-a, postoje i sistemi koji ne spadaju ni u jednu od ove dve velike grupe. To su sistemi za velike računare, za specijalne namene ili za posebne uređaje kao što su mobilni telefoni i tableti. Primeri ovih operativnih sistema su PalmOS, Symbian, Android i iOS.Posebno bi trebalo pomenuti i Google Chrome OS, operativni sistem koji je namenjen Internetu i korišćenju web aplikacija

Serveri

U oblasti informacionih tehnologija ***server*** je računarski sistem koji pruža usluge drugim računarskim sistemima – klijentima. Komunikacija između servera i klijenta odvija se preko računarske mreže. Naziv server najčešće se odnosi na ceo računarski sistem, ali se ponekada koristi i samo za hardver ili softver takvog sistema. Klijent i server zajedno obrazuju klijent-server mrežnu arhitekturu.
Kada se pod pojmom server podrazumeva računar, to se uglavnom odnosi na računar koji obavlja serverske poslove. Server se može sastojati od standardnih hardverskih komponenti koje se ugrađuju u obične desktop računare (PC – *personal computer*) u slučaju da programi (aplikacije) koji se izvršavaju na serverima nisu složeni odnosno hardverski zahtevni. Serveri koji opslužuju složene programe ili veliki broj korisnika zahtevaju specijalizovan hardver koji je optimizovan za upotrebu u serverima. Poseban hardver podrazumeva i hard diskove visokih performansi, prvenstveno brzine i pouzdanosti. Procesorska brzina nije od ključne važnosti za servere pošto se većina servera bavi uzlazno/izlaznim (I/O – *input/output*) operacijama i ne koristi grafički korisnički interfejs (GUI – *graphic userinterface*).
Pod serverom se podrazumeva program koji od klijenta preko mreže prima zahteve, obrađuje ih i opet preko mreže šalje odgovore klijentu. Programi koji se koriste na serverima su posebno razvijani za serverske operativne sisteme i potrebe server/klijent okruženja. Primeri serverskih programa su DHCP, DNS, mail server, ruter i drugo.

Klijent – server model



Na server može, a ne mora bitiinstaliran serverski operativnisistem.
Ovo zavisi od uloge server i broja računara, odnosno korisnika koji će koristiti server.
Na primer, za malu kancelariju sa 4-5 racunara u mreži koja ima potrebu za računarom koji će olakšati pristu prazličitim dokumentima I internetu, može biti sasvim dovoljan Windows ili neki Linux.
Sa drugestrane u slučaju velikog broja korisnika koji moraju imati računar koji omogućava pristup programu za poslovanje u svakom trenutku biće neophodan serverski operativni sistem kao što je Windows Server, linux .
Serverski operativni sistemi su robusniji i sigurniji od operativnih sistema za radne stanice.
Ono štotrebaimati u vidu jeste da nabavka serverskog operatinog sistema znači skup operativni sistem, skup hardver i skupe programe koji se instaliraju na serverskim operativnim sistemima.

Operativni sistemi koji se koriste na serverima su specijalno dizajnirani za servere. Na serverima se najviše koriste Linux, Solaris i FreeBSD operativni sistemi koji su razvijeni po uzoru na operativni sistem UNIX. Koriste se i serveri iz Microsoft Windows porodice: Windows NT, Windows 2000, Server 2003 Windows Server 2012.

Za operativne sisteme za servere karakteristična je:

- bezbednost i pouzdanost
- mogućnost rekonfigurisanja softvera i hardvera bez zaustavljanja sistema (ograničeno)
- fleksibilnost mrežnog povezivanja

Većina server programa radi u pozadini i ne očekuje ulazne podatke od korisnika niti ispisuje informacije na ekranu. Ovo je posledica toga da serveri komuniciraju samo sa klijent - računarima preko računarske mreze. Zbog toga na serverima vrlo često nema potrebe za postojanjem grafičkog radnog okruženja. A nekorišćenje takvog okruženja značajno oslobađa procesor servera za svoje namenske zadatke.

Skoro cela Internet struktura bazira se na klijent - server modelu. Milioni spojenih servera čine Internet i rade neprekidno opslužujući zahteve korisnika. Internet serveri pružaju usluge kao sto su Web, e-mail, transfer podataka, chat i mnoge druge..

Podela servera

U zavisnosti od toga kakvu funkcionalnost obavljaju postoje sledeće vrste servera:

- **Server za identifikaciju korisnika (Identifikacioni server) -** Zadatak ovakvog servera jeste da omogući korisniku kontrolisan pristup mreži. Ovo se realizuje tako što korisnik mora da ukuca svoje korisničko ime i lozinku svaki put kada želi da radi koristeći radni stanicu. Najpoznatiji program koji ovo omogućava je MS ActiveDirectory.

- **Server koji omogućava pristup štampačima (Print server) -** Ovakav server omogućava svim radnim stanicama korišćenje štampača koji su priključeni na njega. Danas se ovakvi serveri sve manje koriste jer postoje štampači koji se direktno priključuju na mrežu i koji u sebi već imaju instaliranu ovu funkciju. To su tzv. mrežni štamapči.

- **Serveri za deljene dokumenata (File server) -** Često korišćen server koji na sebe smešta dokumenta koja koriste zaposleni prema svojim potrebama. Može se ograničiti pristup nekim dokumentima u smislu da samo odredeni korisnici mogu da im pristupaju ili da ihmenjaju.

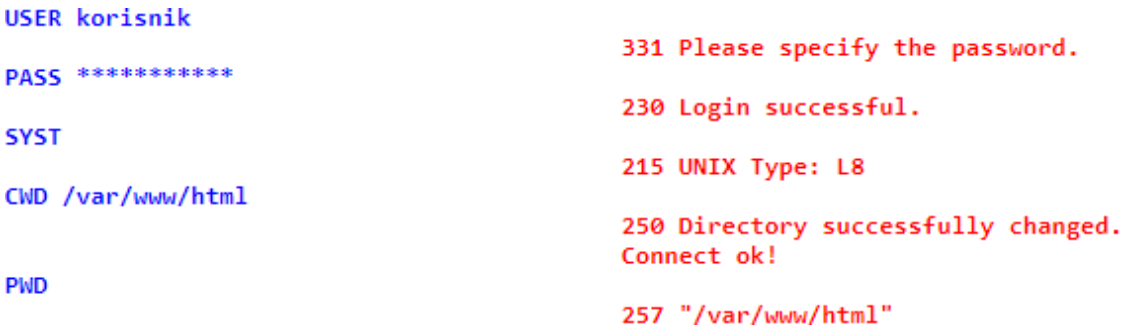
- **Serveri za pogon web aplikacija (Web server) -** Ukoliko imate internet stranicu ili program kome treba da pristupa veliki broj korisnika sa različitih lokacija potreban vam je server na kome će se postaviti vaš sajt ili vaša aplikacija i kome će onda korisnici moći da pristupaju kada su povezani na Internet koristeći neki od pregledača Internet sadržaja, kao što su Google Chrome ili MozillaFirefox.

- **Server za deljenje dokumenata preko Interneta (FTP Server) -** Kao što se pomoću servera za deljenje dokumenata dele dokumenta u okviru lokalne mreže, ovakav server omogućava deljenje dokumenata prekoInterneta.

- **Server za elektronsku poštu (Mail server) -** Kada se instalira server za elektronsku poštu, dogadja se to da sva elektronska pošta namenjena zaposlenima u firmi prvo dolazi na server nakon čega im se distribuira. Isto se dešava kada zaposleni žele da pošalju nekom elektronsku poštu. Ona prvo dolazi na server, a server je šalje kome jepotrebno.

- **Serveri baze podataka (Database server) -** Ovakvi serveri skladište podatke i omogućavaju aplikacijama instairanim na drugim računarima da ovakve podatkekoriste.

- **Serveri za daljinski pristup (VPN serveri) -** Ovi serveri vam omogućavaju da pristupite sopstvenoj mreži sa bilo koje lokacije na kojoj imate pristup Internetu. Jednostavno rečeno, omogućava vam da koristite sve resurse kao da ste u kancelariji, a ne na nekoj udaljenojlokaciji.



Primer FTP – File Transfer Protokola

U primeru prikazanom na slici broj 9 dat je deo komunikacije između klijenta i server putem FTP protokola koji se koristi za prenos fajlova. Sa leve strane prikazane su komande koje klijent upućuje serveru, a sa desne odgovoriservera.

Karakteristike server računara

Primarna funcija servera je da podrži višestruke i istovremene zahteve klijenata, koji zahtevaju servisiranje svojih zahteva. Serveri moraju da omoguče podršku za multitasking kao i da omoguće nesmetanu podelu i dodelu svog memorijskog prostora Kao server platforme mogu se koristiti jači PC računari, RISC računari ili veliki računari ako je u pitanju upravljanje velikim bazama podataka .Od njih se očekuje da prihvate spoljašnje zahteve, da ih obrade i vrate klijentima tražene podatake i to u potpunoj sinhronizaciji. Sve to mora da prati potpuna bezbednost i nezavisnost u prihvatanju i slanju potrebnih podataka kako bi se sačuvao njihov integritet.Razvoj objektno orjentisanih tehnologija (OOT) diktira razvoj OS i razvojnih okruženja, pa su serveri postali “svuda prisutni”. Serveri treba da budu potpuno transparentni da ne zavise od tehnologije izrade, mesta gde se oni postavljaju tj. gde se nalaze korisnici (users) ili razvoj (developers) i da budu uvek dostupni.

Jedan računarski proces može se jasno podeliti na klijent i server komponente, tako za server procese kažemo da važe sledeći principi:

- Lokaciona nezavisnost - server proces može biti smešten bilo gde
- Optimizacija resursa - server proces mogu deliti više klijenata.
- Skalabilnost - server proces može biti startovan na više platformi

Server procesi bi trebalo da rade u plug-and-play okruženju.

Od savremenih serverskih mašina zahteva se podrška: multiprocesiranju (multi-core CPU), disk poljima (RAID strukture), mehanizmima obrade višestrukih niti (multithreading) upravljanju memorijskih podsistema (ECC mehanizam), Potrebna je i zaštita od problema u napajanju električnom energijom što se obično obezbeđuje uređajem za neprekidno napajanje (UPS). Obezbediti mogućnost za proširenje CPU-a,memorije,diska i periferija.,

Za operativni sistem servera se najčešće bira operativni sistem sa mrežnom podrškom i sistemima zaštite podataka. Ide se na to da se odvoje server procesi i mrežni opertivni sistem jer se tada server računar rasterećuje od izvršavanja zahteva koji do njega stižu sa mreže.

Radne stanice, sofver i njihove karakteristike

Bilo koju radnu stanicu (desktop workstation) koju koristi jedan korisnik smatramo klijentskom radnom stanicom ili samo klijentom.U klijent server modelu ne postoje neke tehnološke razlike, sa stanovništva računara, između klijenta i servera. Performanse radnih stanica su dramatično napredovale performanse CPU povećale su se 850 puta (4,7MHz → 4GHz), veličina RAM-a memorije 16 000 puta (256kB → 4GB) kapacitet hard diskova 100 000 puta (10MB → 1TB). Napredak tehnologije učinio je da aplikacije koje su se izvršavale na desktop računarima postanu jako sofisticirane (pametne) tj. napredne -Sa druge strane ovakav veliki razvoj tehnologije desktop računara prouzrokovao je i veliki razvoj drugih računarskih tehnologija a pre svega komunikacionih (razvoj velikog broja protokola) a one su dovele do razvoja mrežnih tehnologija (LAN, WAN i Internet mreže). Danas je nezamislivo da imamo desktop računar koji nije umrežen.

Klijent je bilo koji proces koji zahteva usluge od serverskog procesa. Osobine hardverske i softverske komponente klijent računara:

- Ne toliko snažan hardver ali dovoljne radne memorije,
- Operativni sistem koji je sposoban da podrži multitasking,
- Grafički korisnički interfejs (GUI – Graphic User Interface) ,

Komunikacione sposobnosti (mrežnu karticu). Hardver klijenta je obično PC računar a u poslednje vreme se koristi i X-terminal koji jedan deo potrebnog klijent/server softvera drži u ROM-u, a ostatak se puni u RAM memoriju sa servera preko mreže. Postoji široki opseg različitih OS koji mogu da zadovolje minimalne zahteve klijentskih OS (DOS/Windows, WinXP, Win7, Win10 ,Linux,..). Hardver i OS mora obezbediti adekvatno povezivanje sa mrežnim OS. Klijent aplikacije su uglavnom zasnovane na grafičkom korisničkom interfejsu, čija je uloga da sakrije kompleksnost od krajnjeg korisnika. Klijent aplikacija interaguje sa OS radi korišćenja multitaskinga, GUI interfejsa i sa mrežnom komponentom komunikacionog posrednika Dok se zahtev izvršava na serveru, klijent je potpuno slobodan.

Klijent je osnovni korisnik servisa koji se izvršavaju na serverima.Postoji jasna podela funkcija između klijenta i servera .Jedan od osnovnih servisa koji se izvršavaju na klijent radnoj stanici je prezentacioni servis, kontroliše prihvatanje i prikazivanje podataka. Današnje tehnologije omogućile su pored GUI interfejsa i multimedijalni pristup podacima

putem audio-vizuelnog pristupa. Tehnika višestrukih prozora (windowing enviroment) omogućuje klijentu da istovremeno bude uključen u nekoliko simultanih sesija. Unošenje teksta, praćenje E-maila, gledanje nekog filma ili slušanje muzike, mogu potpuno simultano da se odvijaju na jednom klijentu.

Klijentski softver podržava napredne mogućnosti kao što su:

- DDE (Dynamic Data Echange) dinamička razmena podataka,
- OLE (Object Level Embedding)
- CORBA (Communicating Object Request Broker Architecture)

One omogućuju prostu operaciju cut and paste (premeštanje podataka) između različitih aplikacija: tekst procesora, baza podataka, tabelarnih prikaza, grafičkih prikaza i to u različitim višestrukim prozorima. Klijent radna stanica zahteva neki servis od servera a NOS (Netware Operating System) softver prenosi ili dodaje specificirani zahtev od izvora do ciljnog servera na kome se izvršava neka aplikacija. Uvek kada je taj server isti kao i radna stanica ili pak predstavlja neki mrežni, fizički odvojeni server, aplikacioni format zahteva je uvek isti. IPC (Inter Process Communication) predstavlja generički izraz koji se koristi da opiše komunikaciju između dva ili više procesa. U klijent server modelu ti procesi mogu biti na istom računaru, na računarima koju su povezani u LAN, WAN ili Internet mreze. Najćešći servis koji NOS pokreće je servis redirekcije. Ovaj servis prihvata pozive od klijentskog OS i prenosi ih prema NOS. Dugi niz godina programeri su se trudili da razvijaju modularni kod koristeći strukturnu tehniku i logiku poziva podprograma. Danas se zahteva da ti podprogrami (subroutines) budu i zapamćeni negde kao objekti koji će sada biti dostupni svima ko želi da ih koristi

Održavanje softvera radnih stanica obuhvata instalacije, reinstalacije, podešavanje i redovnu kontrolu operativnih sistema radnih stanica. Cilj održavanja radnih stanica su unificirane instalacije, redovno ažuriran softver i zaštita od virusa i ostalog malicioznog softvera. Radne stanice se podešavanju u skladu sa idejnim rešenjem mreže. Ovo obuhvata podešavanje TCPIP mreže, imenovanje radnih stanica na mreži, instalaciju potrebnih mrežnih štampača i mapiranje mrežnih diskova.
Radne stanice se personalizuju u skladu sa dogovorom i politikom firme.

RAČUNARSKE MREŽE

Osnovni pojmovi i klasifikacija

Tehnološku podlogu za elektronsko poslovanje čine računarske mreže. Računarska mreža je skup više računara, perifernih jedinica i drugih uređaja, koji su međusobno povezani sa ciljem razmene informacija i deobe mrežnih resursa. Računari u mreži se nazivaju čvorovi. Čvorovi mogu biti serveri i radne stanice. Radna stanica je računar na kojem se izvršavaju poslovi, a server računar koji opslužuje radne stanice na osnovu njihovih zahteva i dozvoljava korišćenje mrežnih resursa u skladu sa pravima korisnika. Komunikacija između čvorova u mreži vrši se na osnovu protokola. Protokoli su pravila po kojima uređaji u računarskoj mreži međusobno komuniciraju. TCP/IP (*Transmision Control Protocol / Internet Protocol*) je najpoznatija grupa protokola koja je u početku razvijana u okviru više projekata koje je finansirala američka vojska. TCP/IP protokol [Comer2001] je namenjen komunikaciji i povezivanju računara u heterogenim sredinama. Stavljen je u javno vlasništvo, široko je prihvaćen i skoro da nema mreže koja ne podržava TCP/IP. Internet, mreža svih mreža, zasnovana je na TCP/IP grupi protokola. Prednosti korišćenja računarske mreže, u odnosu na samostalne računare, ogledaju se u boljoj iskorišćenosti resursa sistema. Pod resursima se podrazumevaju softverske i hardverske komponente kao što diskovi, štampači, datoteke, aplikacije i sl.

Jedan od kriterijuma za klasifikaciju računarskih mreža je klasifikacija prema dometu ili rasprostranjenosti mreže u okviru jedne oblasti [Tanenbaum2003]. Tri najzastupljenije kategorije prema toj podeli su:

- LAN mreže (*Local Area Networks*) – mreže lokalnog područja. LAN mreže pokrivaju ograničeno područje kao što je jedna zgrada ili deo zgrade.
- WAN mreže (*Wide Area Networks*) – mreže širokog područja. WAN mreže pokrivaju područje jedne ili više država ili područje celog sveta (Internet).
- MAN mreže (*Metropolitan Area Networks*) – mreže gradskog područja. Mreže ove vrste pokrivaju područje grada ili većeg kampusa.

Postoje i druge kategorije:

- CAN mreže (*Campus Area Networks*) – mreže univerzitetskog kompleksa koje povezuju veći broj LAN mreža na udaljenim lokacijama.
- PAN mreže (*Peronal Area* Networks) – personalne mreže malog dometa, namenjene povezivanju prenosivih uređaja kao što su laptop računari, PDA, palmtop računari i dr. Za povezivanje ovakvih mreža koriste se USB, FireWire, Bluetooth i druge tehnologije.

LAN mreže

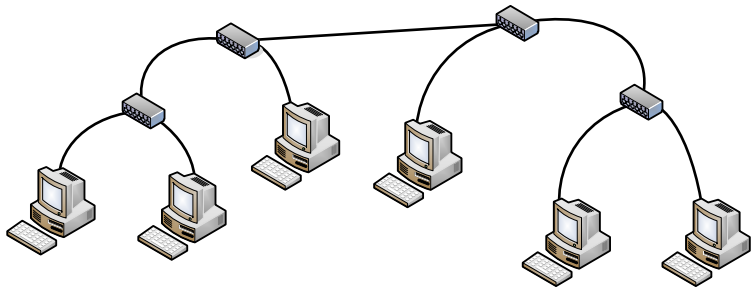
Računarske mreže koje obuhvataju samo deo zgrade, čitavu zgradu ili više zgrada na manjem rastojanju, tj. manje ograničeno područje, nazivaju se lokalne računarske mreže – LAN (*Local Area Networks*). Takve mreže se koriste za povezivanje računara i drugih mrežnih uređaj unutar privatnih prostorija kao što je kuća, stan ili poslovnih prostora kao što su kancelarija, zgrada preduzeća, zgrada škole ili neke druge institucije. U današnje vreme

najdominantnija arhitektura koja se koristi u povezivanju LAN mreža zove se *Ethernet* [Spurgeon2000].

Nastanak Ethernet-a se vezuje za projekat ALOHA, koji je realizovan na Univerzitetu na Havajima kasnih 60-ih godina, ali je komercijalno dostupan tek 80-ih godina prošlog veka. *Ethernet* je danas najpopularnija i najzastupljenija mrežna arhitektura. U početku, *Ethernet* je projektovan za prenos podataka od 10 Mbps (megabita po sekundi). Kasnije je došlo do razvoja standarda za prenos od 100 Mbps, 1, 10 i više Gbps (gigabita po sekundi). Postoji nekoliko varijanti *Ethernet* arhitekture. Pored starijih vatijanti (10Base5, 10Base2, 10BaseT, 10BaseF) u današnje vreme se koriste sledeće varijante Etherneta.

- Fast Ethernet (100 Mbit/s)
- Gigabit Ethernet
- 10 Gigabit Ethernet
- 40 Gigabit Ethernet
- 100 Gigabit Ethernet

Fast Ethernet ili 100Base-X Ethernet je standard za brzine prenosa podataka od 100 Mbps. I pored velikog broja podvarijanti ovog standard postoje dve glavne podvarijante: 100Base-TX (varijanta koja koristi UTP cat 5 kablove) i 100BaseFX (koja koristi optičke kablove). Za povezivanje računara se u obe varijante *Etherneta* koriste *se* mrežni uređaji nazvani *hub* i *switch*. Povezivanje računara se vrši kao na slici. Fast Ethernet 100Base-TX je trenutno najrasprostranjeniji standard, prvenstveno zbog niskih cena potrebne opreme i velike brzine prenosa.



Elementi povezivanja 100BaseTX Ethernet
mreže i način povezivanja hostova

Gigabit Ethernet (GbE ili 1 GigE) je brži standard za Ethernet mreže i podržava brzine prenosa podataka od 1 Gbps (gigabita u sekundi). Postoji u nekoliko podvarijanti od kojih su najpoznatije sledeće: 1000Base-SX i 1000Base-LX za rad sa optikom i 1000Base-T koji koristi UTP kablove kategorije. Osnovna karakteristika bržih standarda Etherneta je veoma velika brzina prenosa podataka. Pogodan je za implementaciju na najopterećenijim segmentima mreže, kao što su veze između servera.

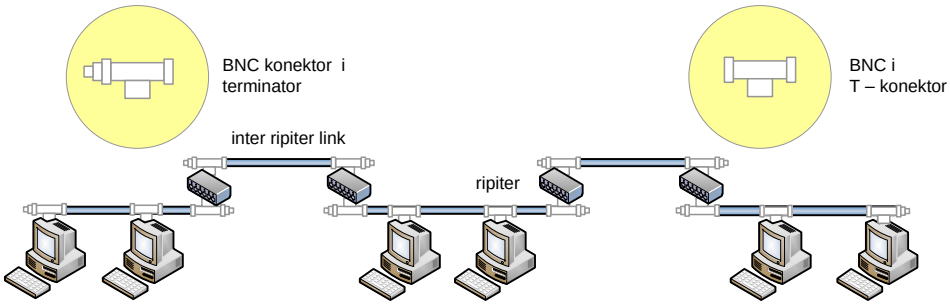
U novije vreme doloazi do nastanka i sve veće upotrebe novih standarda znatno većih brzina. 10 gigabit Ethernet (10GE, 10GbE ili 10 GigE) je standard prvi put objavljen 2002. 40 Gigabit Ethernet (40GbE) i 100 Gigabit Ethernet (100GbE) su standardi na objavljeni 2010.

Mrežni uređaji

Mrežni uređaji su specijalizovani uređaji koji su potrebni da bi se računari mogli međusobno povezati u okviru LAN mreža. Mrežni uređaji takođe služe za povezivanje različitih LAN mreža na udaljenim lokacijama kao i za povezivanje LAN mreža sa WAN mrežom. Postoji veći broj mrežnih uređaja od kojih su najavažnije tri grupe uređaja [Donahue 2007]:

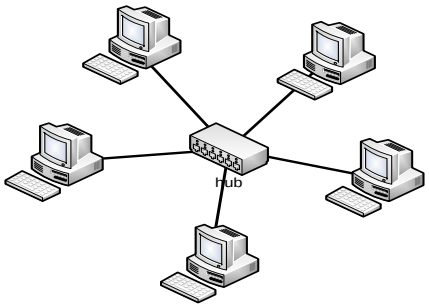
- *Layer 1* uređaji – *hub* ili *repeater*
- *Layer 2* uređaji - *switch* ili *bridge*
- *Layer 3* uređaji - ruter i *Layer 3 switch*

Repeater (repetitor) je uređaj koji radi na fizičkom sloju OSI (Open Systems Interconnection) modela, referentnog modela za otvoreno povezivanje sistema. Fizički sloj je prvi sloj OSI modela, te otuda i naziv *Layer 1* uređaji. Ovi uređaji povezuju dva mrežna segmenta istog tipa (npr. *Ethernet* – *Ethernet*) u topologiji magistrale [slika 57]. Njihova namena je pojačanje i prosleđivanje signala i potrebni su za produženje mrežnih segmenata. Pošto se koriste u kombinaciji sa tankim ili debelim koaksijalnim kablom, upotrebljavaju se za starije mrežne *Ethernet* arhitekture kao što su 10Base5 i 10Base2 *Ethernet*.



Elementi 10Base2 Ethernet mreže i način povezivanja pomoću repeater-a

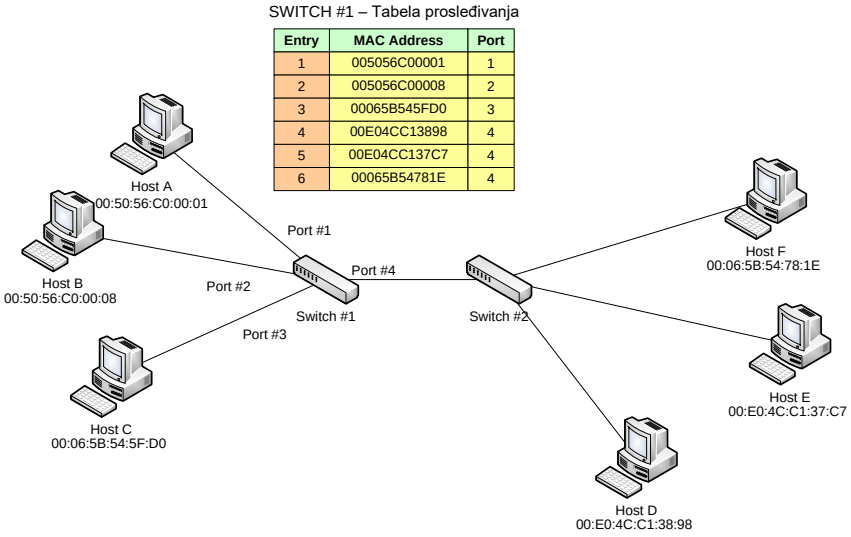
Hub (koncentrator) je uređaj sličan *repeater*-u. Radi na fizičkom sloju OSI modela, ali za razliku od svog prethodnika ima veći broj portova, pa se koristi u topologiji zvezde. Nalazi se u središtu mreže, tj. ostali računari su vezani na njega i na taj način komuniciraju sa drugim računarima [slika 53]. Ako je potrebno, radi proširenja, ovaj uređaj se može povezati i sa drugim *hub*-om ili *switch*-em. *Hub* se koristi u kombinaciji sa UTP ili STP kablovima ili optikom. Sve savremenije varijante *Ethernet*-a koriste *hub* za povezivanje računara.



Položaj hub-a u mreži sa topologijom zvezde

Bridge (most**)** je uređaj koji radi na sloju veze podataka OSI modela. Sloj veze podataka je drugi sloj OSI modela, te otuda i naziv *Layer 2* uređaj. *Bridge* služi za povezivanje mreža istog i različitih arhitektura, npr. *Ethernet – Ethernet* ili *Ethernet – Token Ring*. Radi na principu prosleđivanja okvira podataka na osnovu fizičke adrese računara (MAC adresa), kojem su okviri namenjeni. Tabela prosleđivanja sadrži MAC adrese računara u mreži i port iza koga se ti računari nalaze. Pošto *bridge* radi na ovaj način, to dovodi i do filtracije okvira podataka. *Bridge* neće prosleđivati u drugi segment mreže okvire koji nisu namenjeni računarima u tom segmentu. Na taj način se smanjuje nepotreban saobraćaj i mogućnost nastajanja kolizije (sudara okvira podataka koji se šalju) što utiče na poboljšanje rada mreže. *Bridge* se koristi u kombinaciji sa tankim i debelim koaksijalnim kablom, a samim tim i za starije mrežne arhitekture *Ethernet* tipa.

Switch (komutator) je uređaj sličan *bridge*-u. Radi na drugom sloju OSI modela, a za razliku od prethodnika ima veći broj portova. Takođe radi na principu prosleđivanja okvira podatka na osnovu MAC adrese. Prosleđivanje se vrši na osnovu tabele prosleđivanja koja se automatski kreira u samom *switch*-u [slika 56]. Tabela prosleđivanja i u ovom slučaju sadrži MAC adrese računara i brojeve portova iza kojih se ti računari nalaze. *Switch* deli mrežu na kolizione segmente. Pošto *switch* ne prosleđuje okvire podataka na sve portove, kao *hub*, nego samo na onaj port iza koga se nalazi računar kome je okvir podataka namenjen, smanjuje se mogućnost pojave kolizije, što kao u prethodnom slučaju, utiče na poboljšanje rada mreže. Koristi se isto kao i *hub*, u topologiji zvezde kao centralno čvorište, a svi ostali računari se povezuju na njega. Radi proširenja mreže, moguće je povezati ga sa drugim *switch*-em ili nekim drugim uređajem [slika 56]. Kao i *hub*, *switch* se koristi u kombinaciji sa UTP ili STP kablovima ili optikom. Sve savremenije varijante *Etherneta* koriste ovaj uređaj.



Sadržaj tabele prosleđivanja na levom od dva switch-a koji povezuju dva mrežna segmenta

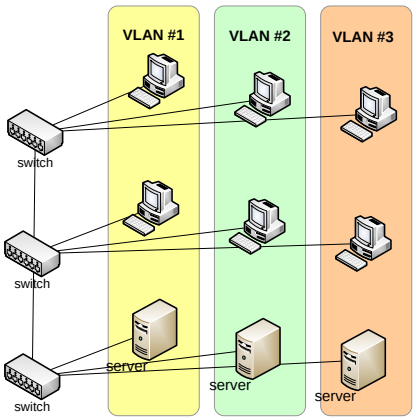
Ruter ili mrežna skretnica je uređaj koji radi na sloju mreže OSI modela. Pošto se radi o trećem sloju, ti uređaji se nazivaju *Layer 3* uređaji. Ovi uređaji služe za usmeravanje mrežnog saobraćaja na više istih ili različitih tipova mreža. Ruter usmerava pakete na mreži na osnovu logičke adrese koja se koristi u zavisnosti od protokola. U TCP/IP mrežama u koje spada i

Internet, paketi se usmeravaju na osnovu IP adrese. Prosleđivanje se vrši pomoću pravila koja se nalaze u tabeli rutiranja. U tabeli rutiranja se kao ulaz za pojedinu rutu nalaze ciljna adresa mreže ili adresa hosta, mrežna maska, adresa sledećeg rutera na putanji do cilja (*gateway*) i izlazni mrežni interfejs. Ruter karakteriše veliki broj interfejsa (najmanje dva) koji mogu da budu istog ili različitog tipa. Npr. ruter može imati više LAN interfejsa za *Fast Ethernet* mrežu u kombinaciji sa više WAN interfejsa različitog tipa.

Layer 3 Switch je uređaj koji objedinjuje funkcije *switch*-a i rutera, tako da pored osobine i mogućnosti da vrši prosleđivanje okvira podataka na osnovu MAC adrese, može da vrši i usmeravanje paketa na osnovu IP adrese. Zbog sve nižih cena nalazi se u sve većoj upotrebi.

VLAN mreže

Standardna LAN konfiguracija deli korisnike na mrežne segmente po njihovom fizičkom rasporedu (rasporedu po prostorijama i povezivanjem na određene *hub*-ove ili *switch*-eve). Pri tome se ne obraća pažnja na pripadnost specifičnoj radnoj grupi ili potreba za određenim propusnim opsegom. VLAN mreže omogućavaju logičku podelu fizičkog LAN-a na različite podmreže ili domene, što pruža mogućnost kontrole saobraćaja i bolje organizacije.



Podela jedne fizičke računarske mreže na tri VLAN mreže

VLAN ili Virtualna LAN mreža je logička grupa uređaja ili korisnika koja je logički grupisana nezavisno od njihove fizičke lokacije. Ti uređaji mogu biti grupisani po funkciji, odseku firme ili aplikaciji koju koriste, bez obzira na lokaciju njihovih fizičkih segmenata [slika 59]. Konfiguracija VLAN mreža se vrši na *switch*-evima pomoću njihovog sofvera (Layer 2 upravljivi *switch*-evi i Layer 3 *swich*-evi koji imaju podršku za VLAN).

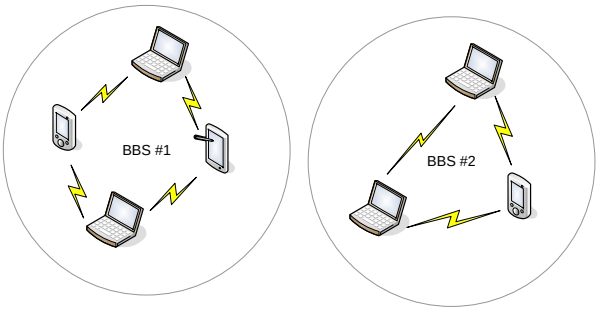
Podelom korisnika u različite VLAN-ove postiže se kontrola saobraćaja jer se slanje okvira vrši samo u okviru iste vituelne mreže. Na taj način sprečava se slanje okvira podataka u delove mreže kojima ti okviri nisu namenjeni. Takav pristup, sa jedne strane, dovodi to toga da se drugi segmenti ne opterećuju nepotrebnim saobraćajem, a sa druge strane, povećava sigurnost mreže, jer se okviri podataka ne šalju računarima koji nisu deo grupe. Dodatno, mogućnost kreiranja VLAN-ova nezavisno od fizičke lokacije dozvoljava laku prekonfiguraciju u slučajevima kada jedan zaposleni promeni radno mesto, tj. njegovu fizičku lokaciju [Shay2004].

Wireless LAN mreže

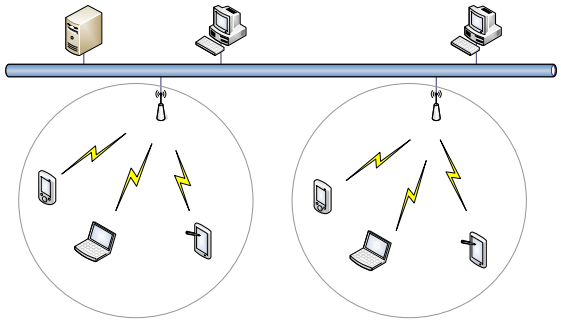
Bežične lokalne računarske mreže (*Wireless Local Area Networks*) predstavljaju pravac razvoja u oblasti lokalnih računarskih mreža popularan u zadnjih desetak godina. Za razliku od standardnih mreža koje prenose podatke preko bakarnih i optičkih medijuma, WLAN mreže koriste radio talase. Radio komunikacija se kod WLAN mreža odvija u najčešće u 2.4 GHz ili 5 GHz opsegu. Postoje dve dominantne arhitekture bežičnih LAN-ova:

Nezavisne WLAN mreže (*Independent WLANs*) su privremeno konfigurisane *peer-to peer* mreže. Nazivaju se još i ad-hoc mrežama. Njih čini grupa bežičnih uređaja koji međusobno komuniciraju na istoj frekvenciji [slika ispod levo.]. Uređaji u bežičnim LAN mrežama su mobilni i fiksni računari, PDA, palmtop računari i drugi prenosivi uređaji sa odgovarajućim hardverom (mrežne kartice sa antenama).

Infrastrukturni WLAN (*Infrastructure WLAN*) – predstavlja arhitekturu WLAN mreža u kome se mobilni uređaji povezuju sa klasičnim ožičenim LAN mrežama. Za povezivanje stanica sa ožičenim LAN mrežama koriste se namenski uređaji koji se nazivaju *access point* - AP [slika ispod desno].



Dve nezavisne WLAN mreže koje se sastoje od većeg broja mobilnih klijenata (laptop računari, PDA itd.)



Povezivanje dve WLAN mreže sa ostatkom ožičene mreže Ethernet arhitekture. Povezivanje se vrši posredstvom access point uređaja.

Postoji veći broj standarda za WLAN mreže. Najveću rasprostranjenost na tržištu imaju standardi iz serije IEEE 802.11 koji su se razvili u nekoliko varijanti. IEEE 802.11 standardi su razvijeni za upotrebu na ograničenom području kao što je kuća, zgrada ili Situacija po kontinentima je sledeća. Severna Amerika ima 266,224,500 miliona Internet korisnika (što predstavlja 13.5% ukupne svetska populacije), Evropa 475,069,448 miliona (24.2 %), Azija 825,094,396 miliona (42.0 %), Južna Amerika 204,689,836 miliona (10.4 %), Okeanija 21,263,990 milion (1.1 %), a Afrika ima 110,931,700 miliona korisnika (5.6 %).

Adresiranje na Internetu

Na internetu se koriste IP adrese kao logičke adrese računara i mrežnih uređaja. Da bi neki uređaj mogao da komunicira sa drugim uređajima na Internetu mora da ima sopstvenu IP adresu. IP adresa se sastoji od četiri decimalna broja razdvojena tačkama. Na primer - 192.168.0.1

Svaki od tih brojeva može imati vrednost od 0 do 255. U stvarnosti IP adresa je sačinjena od četiri grupe od po osam bita, što ukupno predstavlja 32 bita. Ovo je stariji format IP adrese koji se još uvek koristi i oznaka za ovu stariju verziju je IPv4. Zbog nedostatka adresnog prostora došlo je do razvoja novije verzije protokola IPv6.

Osnovna razlika između IPv4 i IPv6 protokola je dužina adrese. IPv6 adrese se sastoje od 128 bita, dok se IPv4 adrese sastoje od 32 bita. Adresni prostor IPv4 protokola ima otprilike 4 milijardi adresa, dok IPv6 ima prostora za $3.4 \cdot 10^{38}$ jedinstvenih adresa. IPv6 adresa se predstavlja kao osam grupa od po četiri heksadecimalne cifre rezdvojenih dvotačkama (:).

Na primer,

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Adrese se mogu pisati i u pojednostavljenom obliku tako što se jedna ili više grupa nula (0000) mogu izostaviti i zameniti dvostrukim dvotačkama (::), npr, adresa

8000:0000:0000:0000:0123:0067:89AB:CDEF

se može predstaviti kao

8000::0123:0067:89AB:CDEF

Vodeće nule se takođe mogu obrisati (npr. 0123 se može skraćeno prikazati kao 123)

8000::123:67:89AB:CDEF

Svaka spojena grupa nula (0000) može se smanjiti na dve dvotačke samo jedan put u adresi, tj. nije dozvoljeno imati dva ili više puta po dve dvotačke. Primer nedozvoljenog skraćivanja adrese ja kada se adresa

8000:0000:0000:0123:0067:0000:89AB:CDEF

Skrati na

8000::0123:0067::89AB:CDEF

Raspodela IP adresa

Svaki računar na Internetu mora da ima jedinstvenu IP adresu i jedinstveni alfanumerički naziv – FQDN (*Fully Qualified Domain Name*). Internet Assigned Numbers Authority (IANA) nadgleda globalnu raspodelu IP adresa, root zona za Domain Name System (DNS) i drugih brojeva i simbola u vezi sa Internet protokolom. IANA organizacijom upravlja Internet Corporation for Assigned Names and Numbers - ICANN.

Poslove oko dodele tih informacija vrše specijalizovane institucije – Internet registri koji vrše koordinaciju poslova na nivou svetskih regiona. Internet registri se formiraju kod Internet provajdera, u većim kompanijama ili državnim ustanovama, a njihov rad koordiniraju pet regionalnih centara:

- African Network Information Centre (AfriNIC) – Afrika
- American Registry for Internet Numbers (ARIN) – USA, Kanada i deo Kariba
- Asia-Pacific Network Information Centre (APNIC) – Azija, Australija, Novi Zeland i Okeanija
- Latin America and Caribbean Network Information Centre (LACNIC) – Latinska Amerika, deo Kariba,
- Réseaux IP Européens Network Coordination Centre (RIPE) - Evropa, Srednji Istok i Centralna Azija

InterNIC je centralni Internet registar koji vrši sve ostale globalne koordinacione poslove.

DNS i domeni

Računari međusobno razmenju pakete na osnovu njihove IP adrese. Za korisnike Interneta potrebno je neko jednostavnije adresiranje. Zbog toga se vrši hijerarhijsko simboličko adresiranje računara. Niz znakova razdvojenih tačkama koje predstavljaju računar naziva se domen. To su oznake koje se nalaze na kraju *e-mail* adresa (npr: @telekom.rs, @yahoo.com) ili u *web* adresama (npr yahoo.com, telekom.rs). Domen (*domain*) bi se mogao prevesti i kao oblast.

Postoje generički i nacionalni domeni najvišeg nivoa (TLD – *Top - Level Domains*). Generički ili međunarodni domeni (gTLD) su: com (trgovačke i industrijske organizacije), org (nekomercijalne organizacije), net (ustanove koje pružaju mrežne usluge), gov (civilna vladina udruženja), edu (univerzi-teti i druge obrazovne ustanove), mil (vojne ustanove), int (međunarodne organizacije) i dr. Primeri za imena računara koji su imenovani u okviru ovakvih domena su: www.mercedes.com, www.w3.org itd.

Nacionalni domeni ili nTLD su: rs (naša zemlja), hr (Hrvatska), ba (Bosna i Hercegovina), si (Slovenija), mk (Makedonija), ru (Rusija), hu (Mađarska), it (Italija), fr (Francuska), uk (Velika Britanija), de (Nemačka), ca (Kanada) itd. Na nacionalnom nivou postoje i poddomeni. Za našu zemlju karakteristični su sledeći poddomeni: ac.rs (akademske institucije), co.rs (komercijalne organizacije), org.rs (nekomercijalne organizacije) edu.rs

(obrazovne institucije) i dr. Primeri za imena računara koji su definisani u sklopu ovakvih domena su www.kss.rs, www.spc.org.rs itd.

DNS (*Domain Name System*) ili sistem imena domena [Comer2001] je hijerarhijski sistem koji mapira domenskih imena u IP adrese. Drugim rečima, koristi se za usmeravanje informacija na osnovu IP adrese, pretvarajući IP adrese u domenska imena i obrnuto. DNS serveri se izvršavaju na tačno određenim računarima i obično postoji jedan primarni DNS server i jedan ili više sekundarnih servera po domenu.

Internet servisi

Glavna odlika Interneta je pristup nesagledivoj količini informacija multimedijalnog karaktera (tekst, slike, zvuk, video materijal). Druga karakteristika Interneta prisutna je u poboljšanim mogućnostima komunikacije i razmene informacija (elektronska pošta, video konferencije). Sve ove pogodnosti dostupne su korisnicima Interneta posredstvom njegovih servisa i aplikacija.

WWW (World Wide Web)

World Wide Web ili skraćeno *web* predstavlja arhitekturu koja omogućava pristup povezanim dokumentima koji se nalaze na serverima širom Interneta. Može se opisati kao distribuirani hipermedijalni servis jer korisniku omogućuje pristup multimedijalnim sadržajima. Predstavlja svakako najatraktivniji servis Interneta i samim tim servis koji se najviše razvija.

Web je nastao marta 1989. na CERN-u, evropskom centru za nuklearna istraživanja, kao inicijalna ideja Tim Berners-Lija. Prototip je nastao 18 meseci kasnije, a prva javna demonstracija je izvršena decembra 1991. god. Februara 1993. god. je razvijen je na univerzitetu Ilinois prvi grafički *browser* – Mosaic (Mark Andersen). Andersen uskoro osniva kompaniju Netscape Communications Corp., koja razvija klijente, servere i drugi *web* softver. Uskoro kompanija Micrososft lansira svoj proizvod - *Internet Explorer*. 1994. god. CERN i M.I.T. su potpisali sporazum sa W3C (World Wide Web Consortium), organizacijom koja se posvetila daljem razvoju *web*-a i njegovom standardizacijom. Danas se nekoliko stotina univerziteta i kompanija se pridružilo tom konzorcijumu.

Web omogućuje pristup informacijama u obliku slike, teksta, zvuka i video materijala. Informacije se nalaze na računarima specijalne namene, nazvanim *web* serveri, koji su priključeni na Internet. Skup informacija koji sačinjava *web* prezentaciju (npr. prezentaciju kompanije ili pojedinca) naziva se *web* sajt. *Web* sajtovi se sastoje od niza povetanih dokumeanata koji se nazivaju *web* stranice. Svaki *web* sajt ima jedinstvenu *web* adresu. Prezentovani materijal sadrži linkove (veze) ka drugim informacijama. Linkovi mogu da pokazuju na druge prezentacije (koje se nalaze na serverima bilo gde u svetu) ili na drugi deo iste prezentacije, a takođe i na informacije drugog sadržaja (npr. slike). Pristup *web* sajtovima moguć je pomoću specijalizovanih programa koji se nazivaju *browser*-i. Najviše korišćeni programi te vrste su *Microsoft Internet Explorer, Mozzila Firefox* i *Opera*. *Browser*-i

omogućuju pristupanje *web* sajtovima na osnovu unete adrese. Primer za adresu softverske kompanije kao što je *Microsoft* je www.microsoft.com.

Za razvoj *web* stranica koriste se neke od sledećih tehnologija

- HTML (Hypertext Markup Language)
- JavaScript
- VBScript
- Java applet
- JSP (Java Server Pages)
- PHP
- XML (Exstensible Markup Language)
- ASP (Active Server Pages)
- Perl

E-mail

E-mail ili elektronska pošta je namenjena za prenos tekstualnih dokumenata koji sadrže poruke. Prenos poruka se vrši pomoću programa za distribuciju pošte (*mail server*) do elektronskog sandučića (*mailbox*) neke osobe. Poruke je moguće čuvati i prosleđivati. Pored obične razmene poruka između dve osobe, servis obuhvata i neke proširene usluge, kao to su mailing i diskusione liste, slanje datoteka i slika sa tekstualnom porukom (attachment) i dr. Poruka se šalje korisniku na osnovu njegove e-mail adrese. E-mail adresa je tipa imekorisnika@domen (npr. peric@ptt.rs ili peter@microsoft.com).

E-mail sistemi imaju dve bitne komponente. To su korisničke klijentske aplikacije ili MUA (Mail User Agent) i mail serveri ili MTA (Message Transfer Agent). Mail serveri se koriste za prenos elektronskih poruka između računara na kojima se nalaze korisnički poštanski sandučići upotrebom klijent-server arhitekture. Za prenos poruka između mail servera koristi se SMTP (The Simple Mail Transfer Protocol) protokol.

Korisnička klijentska aplikacija je program koji se koristi za prijem pošte, sastavljanje i slanje pošte, odgovaranje na pristigle poruke i manipulaciju sa korisničim poštanskim sandučićima. Za pristupanje mail serveru i korisničkom mail boksu koriste se POP3 i IMAP4 protokoli. Popularni program ove vrste su Microsoft Outlook, Windows Live Mail, Mozilla Thunderbird i Pegasus Mail.

Danas, u veoma popularan način pristupa elektronskoj pošti spada i pristup upotrebom *web* tehnologije. Takav način pristupa se naziva *webmail*. Neki *web* sajtovi, kao Gmail, Hotmail i Yahoo, omogućavaju besplatnu e-mail uslugu na ovaj način i imaju veliki broj korisnika.

Multimedija

U skorije vreme dolazi do sve šire upotrebe novijih tehnologija na Internetu koje omoguću razne vidove prenosa multimedijalnih sadržaja.

Internet telefonija spade u komunikacione usluge novije generacije koje su našle svoju primenu na Internetu. VoIP (Voice-over-IP ili Internet Protocol) upućuje na način prenosa glasa preko računarskih mreža uz pomoć IP protokola, jednog od najvažnijih protokola Interneta. VoIP sistemi današnjice postali su laki za upotrebu i mogu da zamene klasične telefone. Za implementaciju VoIP sistema koriste se tehnologije kao što su:

- Real-time Transport Protocol (RTP)
- H.323
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)

RTP (Real-time Transport Protocol) je projektovan za prenos digitalizovanih zvučnih i video signala preko IP mreža i Interneta. H.323 je standard koji je prvobitno projektovan za prenos govora preko LAN mreža, ali je ubrzo proširen i prilagođen za prenos preko IP protokola i Interneta. Osim što omogućuje prenos govora i videa u realnom vremenu, H.323 omogućuje i prenos podataka. Npr, dva učesnika u video konferenciji mogu istovremeno da koriste i "tablu za pisanje" na ekranu, da šalju statične slike ili razmenjuju kopije dokumenata. U kasnijem periodu, razvijen je SIP (Session Initiation Protocol) protokol koji je zamišljen kao alterantiva H.323 protokolu. U današnje vreme ovaj protocol zauzima sve veći udeo u VoIP tržištu [Comer2001].

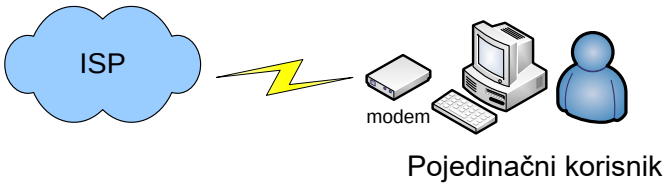
Streaming media sistemi predstavljaju još jedan vid distribucije multimedijalnog sadržaja na Internetu. Mnoge radio i TV kompanije pružaju prenose uživo i emitovanje njihovih emisija. Korisnici ove sadržaje mogu da prate na računarima i drugim uređajima koji imaju pristup Internetu. Jedan od najpopularnijih sajtova za besplatni video streaming je YouTube. Sistemi za streaming digitalnih medija imaju potrebu za velikim brzinama Internet linkova. U ostale oblike distibucije i pristupa multimedijalnim sadržajima spadaju *Web* kamere, video chat sobe i video konferencije.

Priključenje na Internet

Pristup Internetu omogućen je svim korisnicima (uključujući preduzeća i pojedince), koji plate specijalizovanim kompanijama za pružanje Internet usluga – nazvanim ISP (*Internet Service Providers*).

Pojedinačni korisnici se mogu priključiti na Internet posredstvom ISP sistema i upotrebom neke od sledećih tehnologija:

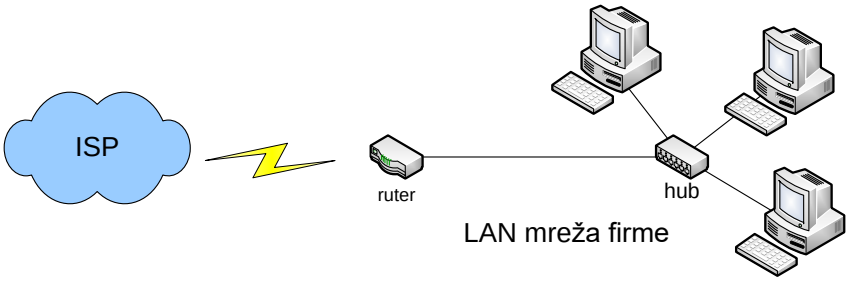
- Kablovski Internet
- ADSL
- Dial-up ISDN ili analogni modemski pristup
- Wireless pristup



Šema povezivanja pojedinačnih korisnika
na Internet modemskom vezom

Slična rešenja mogu da budu pogodna i za manje firme, sa manjim brojem računara koje nemaju potrebu za većim protokom ili stalnim priključenjem na Internet. Povezivanje većih korisnika (kompanije i druge organizacije) može se izvršiti upotrebom sledećih tehnologija kao što je prikazano na slici [slika 77]:

- ADSL
- Ethernet
- Iznajmljene linije (leased-line)



Načini povezivanja na Internet LAN mreža preko iznajmljenih linija

Intranet

Unutrašnja mreža jedne organizacije, zasnovana na Internet tehnologiji naziva se Intranet. Osnovna namena Intraneta je optimizacija poslovnih procesa i efikasna razmena informacija unutar kompanije. S obzirom da sadrži informacije od vitalnog značaja za kompaniju, pristup Intranetu je ograničen i kontrolisan tako da samo ovlašćene osobe mogu da koriste informacije. Gotovo sve velike kompanije u svetu koriste Intranet sa velikim uspehom.

Koncept Intraneta uslovljen je napretkom računarske tehnologije i razvojem personalnih računara. Veliki broj "glupih" terminala (*dumb terminals*), koji su se do tada koristili u lokalnim mrežama kompanija, zamenjen je modernijim personalnim računarima (PC, *Macintosh* i druge platforme). Interni *Web* serveri kompanija preuzeli su ulogu servera aplikacija. Tako da se sa radnih stanica, korišćenjem *Web browser*-a, može pristupati *Web* serveru bez obzira na tip računara i njegov operativni sistem (platformski nezavistan softver).

Intranet sistem se ne mora koristi samo unutar kompanije koja se nalazi na jednoj fizičkoj lokaciji. On se može koristi i za proširenje komunikacije sa drugim udaljenim odeljenjima

kompanije ili sa partnerima za razmenu vitalnih informacija za poslovanje. VPN (*Virtual Private Networks*) mogu da prošire Intranet sistem.

Zaštita računarskih mreža

Firewall sistemi

U današnje vreme, sigurnost mreža i zaštita podataka predstavljaju veoma važan faktor. Povezivanje mreže na Internet i direktna veza sa svetom, predstavljaju stalnu pretnju za sistem i pružaju mogućnost hakerima, da koristeći različite bezbednosne propuste, provale u sistem.

Firewall predstavlja mehanizam zaštite u računarskim mrežama. To je softverski proizvod koji proverava pakete koji dolaze do njega i na osnovu unetih pravila, propušta ili odbija te pakete. Na tržištu postoji veoma mnogo *firewall* proizvoda.

Firewall se obično nalazi na ulazu u mrežu, tj. između unutrašnje i spoljašnje mreže, tako da se celokupan saobraćaj mora odvijati preko njega. On štiti mrežu na svim softverskim slojevima OSI modela – od sloja veze podataka, do aplikacionog sloja.

U *firewall* sistemima se koriste tri osnovna metoda zaštite:

- filtriranje paketa (*packet filtering*) – metod pomoću koga se odbija pristup TCP/IP paketa koji dolaze sa neovlašćenih hostova i na neovlašćene servise.
- translacija adresa ili NAT (*Network Address Translation*) – metod koji prevodi IP adrese unutrašnjih hostova u neku od spoljašnjih (javnih) adresa i tako omogućava hostovima iz unutrašnje mreže pristup Internetu. Za ovaj metod se često koristi i termin IP *masquerading*.
- *proxy* servisi – metod koji radi pomoću aplikacija višeg sloja, koje omogućavaju hostovima iz interne mreže pristup servisima na javnim serverima.

Sve ove funkcije mogu se obavljati na jednom hostu, ali i na više njih. Ostale funkcije koje firewall sistem može da pruži su:

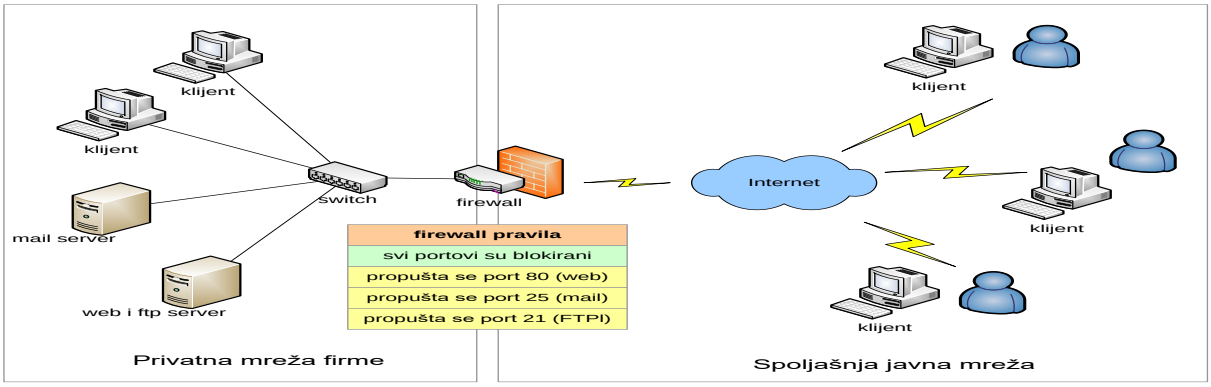
- kriptovana autentifikacija – omogućava korisnicima da sa spoljašnje, pristupe unutrašnjoj mreži, ako se identifikuju.
- podrška za virtualne privatne mreže ili VPN (*Virtual Private Networking*) – tehnologija koja pruža mogućnost uspostavljanja sigurne veze između dve privatne, preko javne mreže, npr. Interneta. VPN mreže se takođe nazivaju enkriptovani tuneli.
- skeniranje virusa – mogućnost da se vrši skeniranje dolaznih podataka da bi se otkrili i uklonili virusi.
- filtriranje sadržaja (*content filtering*) – mogućnost da se vrši blokiranje pristupa pojedinim servisima na osnovu sadržaja kojem se pristupa.

Filtriranje paketa

Prvi firewall sistemi su bili jednostavni filteri paketa. Filtriranje paketa (*packet filtering*) ostaje ključna i osnovna funkcija današnjih *firewall* sistema. Filtriranje je proces u kome se proveravaju paketi mrežnog protokola, kao što je IP, ili transportnog protokola, kao što je TCP. Paketi se upoređuju sa pravilima na osnovu kojih se vrši filtriranje. Pravila se nalaze u tabeli i mogu se naći na ruteru ili nekom od računara sa odgovarajućim softverom za filtriranje.

Filteri sprečavaju prolaz sumljivih paketa u unutrašnjost mreže. Upotreba *firewall* softvera na ruteru ima svojih prednosti. Ruteri se obično nalaze na ulazu u mrežu [slika 96], kao čvorovi

kroz koji mora da prođe ceo saobraćaj upućen na tu mrežu. Filteri koji su podignuti na njima mogu da kontrolišu pristup celoj mreži, delu mreže ili samo ka specifičnom hostu.



Prikaz zaštićene mreže u kojoj firewall blokira nepoželjan saobraćaj sa spoljašnje mreže

Filteri se mogu podići i na pojedinim hostovima. Ti filteri mogu obično da kontrolišu pristup samo onim hostovima na kojima se nalaze. Zbog toga se upotreba filtera na hostovima preporučuje samo kao dodatak i u kombinaciji sa filterima na ulaznim ruterima, a nikako kao jedinstveno rešenje.

Tipična pravila za filtriranje paketa mogu biti raznovrsna. Jedno od osnovnih je sprečavanje pokušaja uspostavljana dolazne konekcije (*inbound*) na neki od hostova unutrašnje mreže. To se postiže odbacivanjem paketa (*drop*). Takođe se može vršiti i sprečavanje pristupa određenom opsegu IP adresa, tj. većem broju hostova. Zatim postoji mogućnost dozvoljavanja uspostavljana izlazne konekcije (*outbound*).

Firewall može da vrši i sprečavanje pristupa onim portovima na unutrašnjim računarima, na kojima se nalaze servisi koji ne bi trebali da budu vidljivi na Internetu (npr. NetBIOS *session port*), a da dozvoli pristup za pakete upućene na portove na kojima se nalaze servisi koji treba da su dostupni sa spoljne mreže (SMTP za servis elektronske pošte ili HTTP za *Web* servis). Obično se dozvoljava pristup preko SMTP protokola (port 25) samo mail serveru, tj. samo onom hostu u mreži na kome se nalazi taj servis.

Napredniji paket filteri proveravaju stanje svake konekcije koja se uspostavlja preko njih, u potrazi za nekim znacima napada. Ti znaci napada mogu biti *source routing*, ICMP redirekcija i IP *spoofing*. Konekcije koje pokazuju slične znake se blokiraju.

Unutrašnjim klijentima se obično dozvoljava izlaz sa mreže. Ako unutrašnji klijent inicira uspostavljanje veze sa spoljašnjim hostom, tada se spoljašnjim hostovima dozvoljava uspostavljanje povratne konekcije sa unutrašnjim hostom, koji je inicirao konekciju. Naime, kada host unutar mreže pokuša da uspostavi TCP konekciju, šalje TCP poruku na IP adresu odredišnog hosta i broj porta javnog servera na tom hostu. U inicijalnoj poruci se naznači IP adresa udaljenog servera i port koji će služiti za uspostavljanje povretne konekcije (npr. port 2050).

Spoljašnji server šalje nazad podatke na naznačeni port. Pošto *firewall* proverava ceo saobraćaj između dva hosta, on zna da je konekcija inicirana sa hosta koji se nalazi unutar mreže, tj. hosta koji je priključen na njegov unutrašnji interfejs. Takođe, *firewall* zna IP adresu unutrašnjeg hosta i port na kojem očekuje konekciju. Na osnovu tih podataka, dozvoljava se konekcija na unutrašnji host sa odgovarajućom IP adresom i samo na predviđeni port.

Kada host koji je inicirao konekciju, zatvori TCP konekciju, *firewall* otklanja ulaz u tabeli koji dozvoljava konekciju spoljnog hosta na unutrašnji. Ako računar, koji je inicirao uspostavljanje konekcije, prestane da komuncira usled pada ili neke druge nepredviđene situacije pre zatvaranja TCP konekcije, *firewall* uklanja ulaz u tabelu posle isteka unapred određenog vremena čekanja.

Filtriranje se može vršiti i na operativnim sistemima. Serverske UNIX i Windows platforme imaju *packet filtering* ugrađen u okviru TCP/IP protokola. Taj softver za filtriranje može se koristiti kao dodatak *firewall* softveru na ruterima.

Filtriranje paketa ima svoja bezbednosna ograničenja. Ta ograničenja bi se mogla nazvati i nedostaci *firewall*-a. Pošto su IP adrese računara iz unutrašnje mreže prisutne u odlaznim paketima, bezbednosni problem se ne može rešiti u potpunosti, jer to pruža mogućnost potencijalim napadačima da otkriju broj i tip hostova unutar mreže i da na njih usmere napade. Filtriranje, znači, ne skriva identitet hostova unutar firewall sistema.

Takođe, filteri ne proveravaju fragmente IP poruka zasnovane na protokolima viših slojeva, kao što su TCP zaglavlja. To omogućava pojavu propusta u filtriranju i dozvoljava komunikaciju sa *Trojan horse* virusima unutar mreže. Noviji *firewall* softveri imaju rešenje za ovakav problem.

Na kraju, filteri nisu dovoljno kompleksni da bi proverili ispravnost protokola unutar paketa mrežnog sloja. Na primer, filteri ne proveravaju HTTP pakete unutar TCP paketa da bi proverili da li je to uobičajeni HTTP zahtev ili napad na *Web browser* ili *Web* server na drugom kraju konekcije. Pošto su firewall softveri skoro eliminisali napade na mrežnom sloju, danas se mnogi napadi usmeravaju na servise viših slojeva, tako da ovaj nedostatak može predstavljati problem.

Filtriranje paketa na operativnim sistemima treba da se koristiti tako da se dozvoli prolaz samo onim paketima koji su potrebni, tj. onim paketima koji su upućeni na postojeće servise na određenom hostu. OS filtriranje omogućava definisanje kriterijuma za propuštanje paketa na osnovu:

- broja IP protokola,
- broja TCP porta i
- broja UDP porta

Filtriranje se obično ne primenjuje na odlaznu konekciju (*outbound connection*), tj. konekciju koja potiče sa samog servera. Ako postoji više mrežnih adaptera, filteri se definišu za svaki mrežni adapter na sistemu.

Postavlja se pitanje, koji su portovi obično otvoreni na različitim tipovima servera. Tipičan server ima podignute servise na sledećim portovima [tabela 23] i oni moraju biti otvoreni da bi servisi radili kako treba:

Tabela1: Tipični servisi potrebni za rad servera

Port	TCP/IP Service
7	Echo
9	Discard
13	Daytime
17	Quote of the Day
19	Character Generator

Internet serveri obično imaju otvorene dodatne portove [tabela 2]:

Tabela 2: Tipični servisi potrebni za rad Internet servera

Port	Server
21	File Transfer Protocol (FTP)
22	Secure Shell
23	Telnet
80	World Wide Web (HTTP)
119	Net News (NNTP)
443	Secure HTTP (HTTPS)

Fajl serveri imaju otvorene sledeće portove [tabela 3]:

Tabela3: Tipični servisi potrebni za rad file *servera*

Port	Service
53	Domain Name Service (DNS servis, ako postoji)
137	NetBIOS Name Service (WINS serveri)
139	NetBIOS Session Service (Windows mreža i SMB/CIFS klijenti)
530	Remote Procedure Call (RPC koristi Windows NT i aplikacije višeg sloja)
3389	Windows Terminal Services prihvata konekcije pomoću RDP protokola

Mail serveri imaju otvorene portove [tabela 4]:

Tabela 4: Tipični servisi potrebni za rad mail *servera*

Port	Mail Server
25	Simple Mail Transfer Protocol (za međuserversku razmenu pošte)
110	Post Office Protocol version 3 (za preuzimanje pošte sa servera)
143	Internet Mail Access Protocol (za pristup klijenta mail serveru)

Potrebno je napomenuti da se pri svakoj instalaciji novog servisa na računaru *firewall* mora podesiti da dozvoli pristup portu na kome se servis nalazi. U suprotnom, taj servis neće raditi. Ovo se ne odnosi i na server i na ulazni *firewall*.

Postoje dva osnovna principa za postizanje sigurnosti. Prvi je sprečavanje svake vrste saobraćaja osim one koja je potrebna i drugi, koji dozvoljava svaku vrstu saobraćaja osim one za koju se zna da predstavlja pretnju za sigurnost sistema. Prvi način je sigurniji, jer drugi podrazumeva da se pretnja može predvideti unapred, što nije sasvim tačno. Stoga će se opširnije opisati prvi princip.

Kada se postavljanju filteri, potrebno je zabraniti pristup svim protokolima i adresama. Nakon toga treba dozvoliti pristup pojedinim servisima i hostovima, ali samo onim za koje je to potrebno. Dalje je potrebno zabraniti sve pokušaje uspostavljanja konekcije u unutrašnjost mreže, jer dozvoljavanjem uspostavljana veze sa spoljne strane može se dozvoliti hakerima prolaz ka *Trojan horse* virusima ili bagovima u softveru. Nakon toga je potrebno zabraniti odgovor na ICMP *redirect* i *echo* (*ping*) poruke. Na kraju, treba odbaciti sve TCP *source* rutirane pakete, pošto se *source routing* retko koristi za uobičajenu komunikaciju.

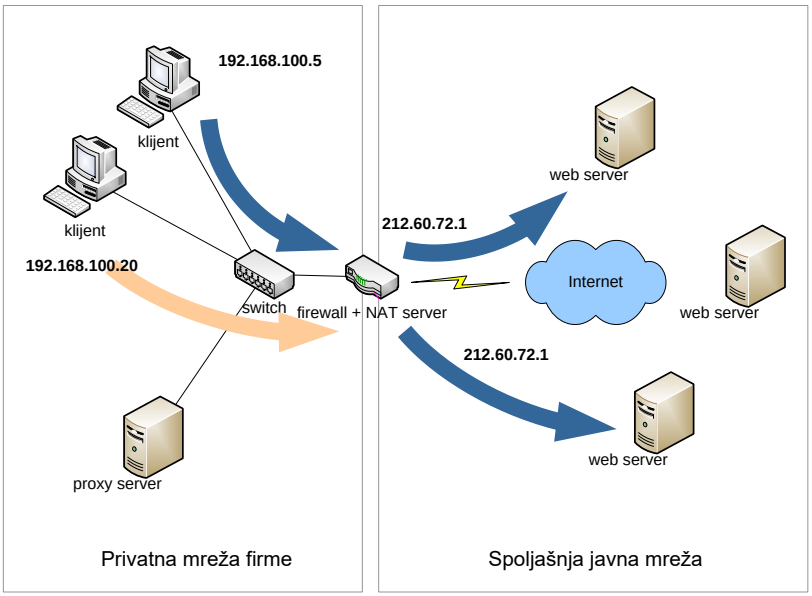
Ako se u mreži nalaze serveri za *Web* i *mail* servis, njih je potrebno postaviti ispred filtera paketa, radije nego da se zbog njih propušta saobraćaj kroz sam firewall.

Na kraju treba imati da na umu da filtriranje paketa nije i jedini način zaštite mreže i da se ne treba samo na to osloniti.

NAT (Network Address Translation)

NAT predstavlja rešenje problema skrivanja internih hostova i informacija o njima od potencijalnih napadača. NAT je zastupnički servis mrežnog sloja. Suština ovog servisa je da jedan host, nazvan NAT server, ostvaruje konekcije iz unutrašnje, prema spoljašnjoj mreži i prema javnim serverima u ime ostalih hostova. Na taj način ih krije od ostatka sveta. Windows 2000, Windows XP, Linux i ostali UNIX operativni sistemi podržavaju NAT u sklopu distribucije operativnog sistema.

NAT krije unutrašnje IP adrese pretvaranjem njihovih adresa u adresu *firewall* sistema. Kada primi zahtev za uspostavljanje konekcije prema spoljašnjoj mreži, *firewall* to čini koristeći svoj broj TCP porta za uspostavljanje veze sa javnim hostom. Na Internetu, ovaj zahtev za uspostavljanje veze izgleda kao da saobraćaj dolazi sa jednog računara, u ovom slučaju NAT servera [sl. 97].



NAT server pretvara adresu hostova u svoju adresu i prosleđuje zahtev hostova na Web server

NAT efikasno krije sve informacije TCP/IP sloja o unutrašnjim hostovima. Adresna translacija takođe dozvoljava upotrebu privatnih IP adresa, koje bez tog servisa ne bi mogle da pristupe Internetu. To može da pomogne u slučajevima kada administrator ne raspolaže dovoljnim brojem javnih IP adresa i kada se ne bi moglo izvršiti adresiranje svih hostova koji treba da pristupaju Internetu.

Hostovi unutar mreže se mogu adresirati sa bilo kojim IP adresama, ali to može dovesti do problema ako se neovlašteno dodele adrese koje već postoje na Internetu. Zbog toga se preporučuje upotreba privatnih IP adresa iz nekog, za tu svhu, preporučenih rezervisanih opsega (npr. 192.168.0.0 ili 10.0.0.0 adrese).

NAT takođe dozvoljava pristup Internetu sa većeg broja računara iz unutršanje mreže preko jedne javne IP adrese. To je veoma važno za kompanijske mreže koje ne raspolažu dovoljnim adresnim prostorom i u slučaju kada se deli jedna *dial-up* konekcija ili jedan pristup preko kablovskog modema.

Kao i u prethodnom slučaju NAT, koji se implementira samo na TCP/IP sloju, ne može u potpunosti da zaštiti sistem. Informacije protokola viših slojeva mogu biti skrivene za *firewall*, tako da paketi mogu koji kroz njega prođu ponovo mogu da se iskoriste za napad na bagoviti softver ili komunikaciju sa *Trojan horse* virusima. *Firewall* neće proveravati takve pakete. Da bi se postigla potpuna zaštita i da bi se sprečili takvi napadi, i potrebno je koristiti servise viših slojeva. To se postiže upotrebom *proxy* servisa.

Pored ovog nedostatka, moguće je da dođe do problema u radu nekih servisa. Problem sa NAT sistemima se javlja kod nekih protokola koji stavljaju IP adresu hosta u deo za podatke. Kada se adresa zameni za javnu adresu, što se događa pri prolasku paketa kroz NAT, ranije upisana adresa u tom delu postaje nevalidna što može da izazove probleme u komunikaciji. To se dešava kod FTP, H.323 ili IPSec komunikacije.

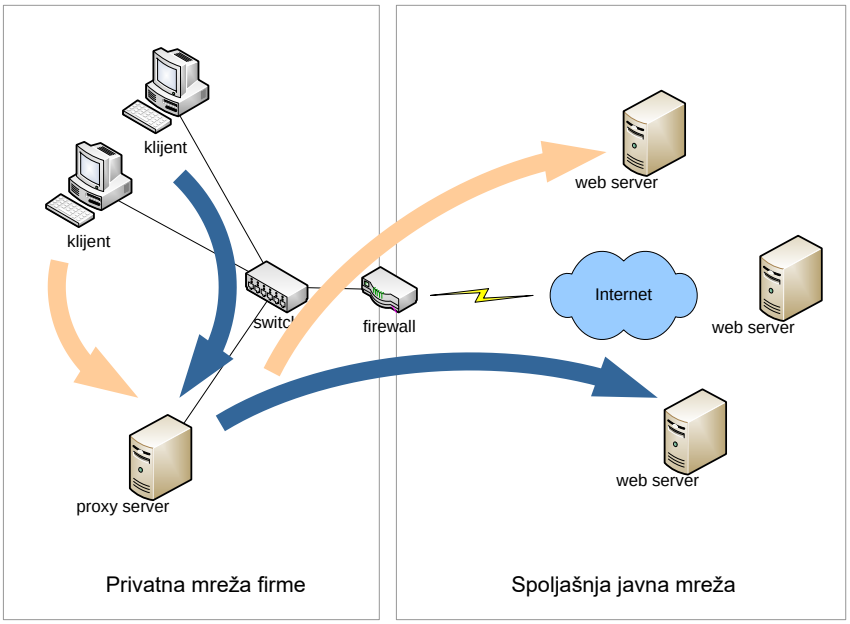
NAT stvara problem administratorima koji hoće da se povežu na klijente iza NAT servera, u slučaju udaljene administracije. To se dešava pošto NAT ima jednu IP adresu, te nema načina da se odredi interni klijent kojem želimo da pristupimo. Ovo sprečava hakere od direktnog povezivanja na unutrašnji klijent, ali i legitimne korisnike da pristupe mreži u slučaju potrebe. Srećom, mnogi savremeni NAT servisi dozvoljavaju redirekciju, tj. propuštanje konekcija koje dođu na server na određeni host sa određenom IP adresom i odgovarajućim portom u unutrašnjoj mreži (*port-forwarding*).

Proxy servisi

NAT rešava probleme koji se mogu javiti kod direktnog pristupa računara na Internet, ali ne može da kontroliše i sprečava protok paketa kroz *firewall*. I dalje postoji mogućnost da potencijalni napadač, sa *monitoring* softverom, analizira saobraćaj koji dolazi iz pravca naše mreže. Tako se može saznati da *firewall* vrši translaciju adresa za ostale hostove. Ta se informacija može iskoristiti za pokretanje napada na mrežu.

Proxy softver koji radi na sloju aplikacije sprečava takvu zloupotrebu. On omogućava da se u potpunosti zabrani protok, na sloju mreže, kroz *firewall* i da se dozvoli saobraćaj samo sa protokolima višeg sloja kao što su HTTP, FTP i SMTP.

Proxy softver aplikacionog sloja je kombinacija servera i klijenta za specifični protokol. Na primer, *Web proxy* je kombinacija *Web* servera i *Web* klijenta. Serverska strana *proxy* servisa prima konekciju sa klijenta u unutrašnjoj mreži, klijentska strana *proxy* servera uspostavlja vezu ka *Web* serveru na javnoj mreži. Kada klijentski deo *proxy* servera primi podatke od javnog servera, serverska strana ga prosleđuje klijentu [slika 98].



Proxy server prima zahtev na privatnoj mreži i šalje ga ka Web serveru na javnoj mreži. Sadržaj koji je dobijen sa Web servera prosleđuje se klijentu

Proxy povezuje dve mreže između kojih je zabranjena komunikacija. Kada klijent na zaštićenom delu mreže uspostavi konekciju na javni server, *proxy* prima zahtev za tu konekciju i uspostavlja konekciju u ime zaštićenog klijenta. *Proxy* tada prosleđuje odgovor javnog servera na unutrašnju mrežu. Može se reći da *proxy* ima ulogu posrednika za hostove u unutrašnjoj mreži.

Aplikacioni *proxy* servisi (kao što *Microsoft Proxy Server* ili *squid*), za razliku od NAT servera i paketnih filtera, koriste se samo ako se u korisničkoj aplikaciji to navede. Na primer, u *Internet Exploreru* treba da se podesi upotreba *proxy* servera navođenjem njegove IP adrese (ili domenskog imena) i porta na kojem se servis nalazi (obično 8080). Tako *Internet Explorer* šaje sve svoje zahteve na *proxy* server, a ne direktno na Internet ka *Web* sajtovima.

Bilo koji server, unutrašnji ili spoljašnji, može da izvrši ulogu *proxy* servera. Bez upotrebe *firewall*-a, upotrebom samo *proxy* servera, mreža se ne može zaštiti, tako da je potrebno implementirati oba servisa. Paketni filter mora biti instaliran, barem da bi sprečio *denial-of-service* napad na *proxy* server (napad kao što je "ping smrti"). Ako se *proxy* nalazi iza firewall-a, mora se dozvoliti prolaz kroz postojeći ulazni *firewall*.

Idealno bi ipak bilo da *firewall* može da izvršava *proxy* funkciju. Neka *proxy - firewall* rešenja imaju mogućnost IP filtriranja i maskiranja (IP *masquerade*). To im omogućava da blokiraju izlazne konekcije, npr. konekcije sa unutrašnjih hostova na port 80 u slučaju HTTP protokola, i posle preusmere sve korisničke zahteve na *proxy*. U tom slučaju ne bi bilo potrebno unositi *proxy* za svakog klijenta ponaosob, već bi se *Web* zahtev klijenta automatski preusmeravao na *proxy*. *Firewall - proxy* bi se nakon toga povezao sa udaljenim serverom i tražio bi podatke u ime blokiranog klijenta. Povratni podaci bi se vraćali klijentu. Ovakav *proxy* se naziva *transparent proxy* i potpuno je nevidljiv za korisika.

Sigurnosni *proxy* može da izvrši i filtriranje paketa na aplikacionom sloju. Na pimer, *firewall* HTTP *proxy* može da proverava tagove u HTML stranicama i tako pronađe one stranice sa *Java* ili *ActiveX* apletima. Apletima se može zabraniti prolaz. Ovo sprečava da se aplet izvršava na klijentskim računarima, a samim tim smanjuje rizik od preuzimanja *Trojan horse* i sličnih virusa.

Što su mrežni slojevi viši, sigurnosni servisi su sve specifičniji. Specifičnost proxy servera je to, što rade samo sa specifičnom aplikacijom. Na primer, za *Web* servis je potreban HTTP *proxy* modul, za FTP je potreban FTP *proxy* modul itd. Mnogi protokoli su retki, pa za njih ne postoji sigurnosni *proxy*. SOCKS je specifični *proxy*, koji se nekad naziva *circuit-level gateway*.

Na kraju se može preporučiti da se u zaštićenim mrežama ne dozvoli korišćenje servisa za koje ne postoje *proxy* serveri. Takođe se preporučuje upotreba *proxy* servera koji mogu da spreče ulazak *ActiveX* ili *Java* apleta na korisničke računare.

Zaštita podataka na Internetu

Da bi se pretnje po integritet i tajnost podataka efikasno otklonile, i time Internet, od izuzetno nebezbednog, postao prirodan i siguran medij za osetljivu delatnost poput elektronskog poslovanja, bilo je neophodno razviti odgovarajuće sigurnosne protokole. Ti protokoli se izvršavaju na različitim nivoima OSI mrežnog modela TCP/IP protokol steka, i možemo ih podeliti na **aplikativne sigurnosne protokole**: SSL, SSH, S/MIME, PGP, i tzv. **protokole za tunelovanje** (*tunneling*) kojima se ostvaruju različite vrste virtuelnih privatnih mreža: MPLS, PPTP, L2TP, GRE, IPSEC. Ovi protokoli se delom zasnivaju na kriptografskim tehnikama zaštite informacija, čije usluge koriste i mehanizmi za pouzdano dokazivanje identiteta – digitalni potpisi i sertifikati.

Osnove kriptografije

Kriptografija je nauka o tajnom pisanju (zapisivanju), i bavi se metodama očuvanja tajnosti informacija. Kriptografski algoritam transformiše čitljiv tekst P (od *plaintext*) u nečitljiv tekst C (od *ciphertext*). Kriptoanaliza je, suprotno, nauka o dobijanju čitljivog teksta P (ili ključeva, ...), tako da napad na privatnost kriptovanih podataka predstavlja pokušaj kriptoanalize. Kriptologija je nauka koja obuhvata i kriptografiju i kriptoanalizu.

Osnovni elementi kriptografske metode za zaštitu su:

- šifrovanje – transformacija čitljivog teksta u nečitljiv oblik,
- dešifrovanje – postupak vraćanja šifrovanog teksta u čitljiv oblik,
- ključ – početna vrednost algoritma kojim se vrši šifrovanje; može biti reč, broj ili fraza,
- *plaintext* – generalno, informacija koju želimo da zaštitimo, i
- *ciphertext* – kriptovan tekst, nečitljiv, onaj koji treba dekriptovati

Namena kriptografije je zaštita memorisane informacije čak i u slučaju da neko neovlašćen pristupi podacima.

Kriptografski algoritmi predstavljaju matematičke funkcije koje se koriste za šifrovanje i/ili dešifrovanje, a mogu biti:

- Ograničeni algoritmi: bezbednost se zasniva na tajnosti algoritma, i
- Algoritmi zasnovani na ključu: bezbednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati (algoritam je javno poznat, a ključ se čuva tajnim).

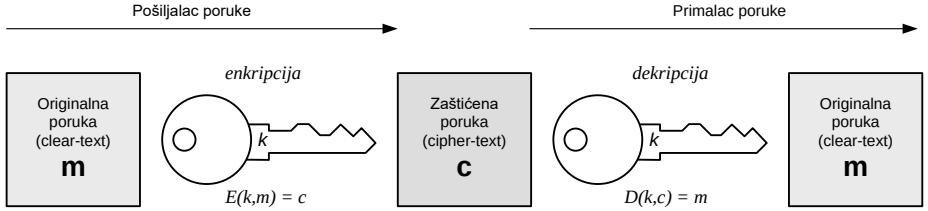
Moderna kriptografija koristi algoritme zasnovane na ključu, zbog njihovih praktičnih prednosti u odnosu na ograničene algoritme. Konkretan skup koji se sastoji iz kriptografskih algoritama, protokola koji omogućuju njihov rad i svih mogućih ključeva, naziva se *kriptosistem*.

Kriptografski postupci

Kriptografski algoritmi zasnovani na ključu dele se na simetrične (često se nazivaju i *konvencionalnim*) i asimetrične. Prvi koriste isti tajni ključ za enkripciju i dekripciju (*shared secret key cryptography*), dok se drugi baziraju na korišćenju različitih ključeva za enkripciju i dekripciju, od kojih je jedan javni i poznat svima, a drugi tajni i poznat samo jednom od učesnika u komunikaciji (*public key cryptography*).

Simetrična kriptografija

Kod simetrične kriptografije postupak enkripcije i dekripcije zasniva se na dve matematički srodne funkcije:



Simetrična kriptografija

Enkripciona funkcija *E*, na osnovu ključa *k* i ulazne poruke *m*, kreira zaštićenu poruku *c*. Dekripciona funkcija *D*, na osnovu *istog* ključa *k* i zaštićene poruke *c*, restaurira originalnu poruku *m*.

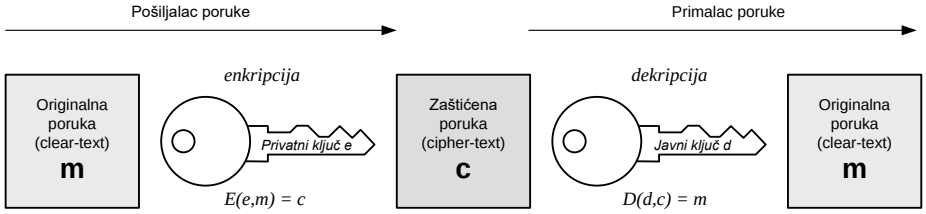
Osnovna prednost ovog načina kriptografije u odnosu na asimetričnu kriptografiju jeste ta što je manje računski intenzivna, tako da se veće količine podataka brže enkriptuju/dekriptuju. Velika mana je činjenica da moramo pronaći bezbedan način za distribuciju tajnog ključa, tj. neophodno je osigurati bezbedan kanal za razmenu ključeva između zainteresovanih strana. Ukoliko bismo već imali tako besprekoran siguran kanal, kriptografija nam ne bi bila ni potrebna: jednostavno bismo preko takvog kanala poslali same podatke. Takođe, u današnjim intenzivnim razmenama podataka preko Interneta, izuzetno je nepraktično generisati ogroman broj ključeva koji su neophodni za komunikaciju: kad god komuniciramo sa nekom drugom stranom, moramo imati ključ koji je jedinstven samo za komunikaciju sa dotičnim klijentom / serverom.

Najpoznatiji simetrični enkripcioni algoritmi:

- DES *(Data Encryption Standard)* – ključ je dužine 56 bita,
- Triple DES, DESX, GDES, RDES – ključ je dužine 168 bita,
- (*Rivest*) RC2, RC4, RC5, RC6 – promenljiva dužina ključa do 2048 bita,
- IDEA (*International Data Encryption Algorithm*) – osnovni algoritam za PGP (*Pretty Good Privacy*) – ključ je dužine 128 bita,
- *Blowfish* – promenljiva dužina ključa do 448 bita,
- AES (*Advanced Encryption Standard*) - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita.
- *Rijndael* - kriptografski postupak se izvršava nad blokovima od 128, 192 ili 256 bita, a tolika može biti i dužina ključeva. Tako se može definisati 2^{128}, 2^{192} ili 2^{256} ključeva.

Asimetrična kriptografija

Algoritmi za asimetričnu kriptografiju su razvijeni znatno kasnije u odnosu na konvencionalnu kriptografiju, a njihov koncept je prvi put prikazan u radovima *Whitfielda Diffieja* i *Martina Hellmana*, 1975. godine (mada postoje indicije da je britanska tajna služba prva došla do mogućnosti ovakve zaštite, nekoliko godina ranije, ali je postupak smatran vojnom tajnom).



Asimetrična kriptografija

Proces enkripcije i dekripcije se kod ovih algoritama takođe zasniva na dve funkcije – imamo enkripcionu funkciju *E* i dekripcionu funkciju *D*. One ponovo manipulišu originalnom porukom *m*, odnosno zaštićenom porukom *c*, ali se ovog puta za enkripciju i dekripciju koriste dva ključa - jedan za enkripciju (ključ *e*), a drugi za dekripciju (ključ *d*). Jedan od ovih ključeva se naziva javni ključ (*public key*) i poznat je svima, a drugi se zove privatni ključ (*private key*), i poznat je samo jednoj strani (slika Asimetrična kritptografija).

Enkripcija podataka asimetričnom kriptografijom može se obaviti na dva načina:

1. *enkripcija originalne poruke javnim ključem* – samo vlasnik privatnog ključa može dekriptovati poruku, ali ne može biti siguran ko je poruku poslao, jer je javni ključ dostupan svima;
2. *enkripcija originalne poruke privatnim ključem* – ovog puta je poreklo poruke nedvosmisleno, kao i nemogućnost poricanja vlasnika javnog ključa da je poruku poslao, ali je tajnost poruke kompromitovana – svako ko ima javni ključ koji odgovara tajnom ključu korišćenom za enkripciju, može videti poruku. Ova osobina se koristi u mehanizmu *digitalnih potpisa,* za dokazivanje identiteta.

Osnovna prednost korišćenja asimetrične kriptografije jeste da strane koje nikada do tog momenta nisu komunicirale, niti su pravile bilo kakve bezbednosne konstrukcije za zaštićeni prenos podataka, mogu bez problema tajno komunicirati jer nije potreban siguran kanal za distribuciju ključeva. Takođe, potrebno je znatno manje ključeva za komunikaciju – tačno dva, od kojih se jedan slobodno prenosi, a drugi čuva. Međutim, enkripcija korišćenjem asimetričnih postupaka je mnogo sporija (praktično oko hiljadu puta, u zavisnosti od konkretnih algoritama) nego zaštita korišćenjem konvencionalnog (simetričnog) kriptografskog postupka, tako da ih ne treba koristiti za šifrovanje velikih količina podataka (tzv. *bulk-encryption*). Najšire korišćeni algoritmi za asimetrično šifrovanje su RSA algoritam (*Ron Rivest, Adi Shamir* i *Leonard Adleman*, 1978), sa dužinama ključa od 512 do 1024 bita, i *Diffie-Hellman* algoritam.

Moderna kriptografija - hibridni pristup

U današnjim modernim enkripcionim sistemima koristićemo i simetričnu i asimetričnu kriptografiju za postizanje potrebnog nivoa zaštite informacija – najpre ćemo asimetričnom kriptografijom razmeniti tajni ključ za ostvarivanje simetrične kriptografije, koju ćemo kasnije koristiti za prenos velike količine podataka.

Kriptografski ključevi

Pored same poruke koju štitimo, moderni kriptografski algoritmi zahtevaju upotrebu jednog ili više kriptografskih ključeva radi zaštite poverljivih informacija. U osnovi, ti ključevi su veoma veliki brojevi, čija se dužina se meri u bitima. Što je dužina ključa veća, zaštićena informacija je sigurnija. Međutim, poređenje veličine ključeva kod asimetrične i simetrične (konvencionalne) kriptografije nije moguće, jer se zbog specifičnosti algoritama sličan stepen zaštite postiže različitim dužinama ključeva: ključ za simetričnu kriptografiju dužine 80 bita ima približnu jačinu zaštite kao ključ za asimetričnu zaštitu od 1024 bita; simetrična zaštita od 128 bita odgovara 3000-bitnom javnom ključu koji bi se koristio u asimetričnim tehnikama, itd.

Kod asimetrične kriptografske tehnike ključevi su matematički povezani. Iako je iz javnog ključa veoma teško izračunati privatni, uz dovoljno vremena i procesorske moći uvek je moguće izvesti ovaj zaštićeni deo informacije, a samim tim i razbiti zaštitu. Zbog toga je prilikom projektovanja jačine zaštite neophodno razmotriti kakve napade očekujemo, i koliko vremena je neophodno da naša zaštita odoleva. Ukoliko uzmemo dužinu ključa koja je premala, rizikujemo da informacije budu otkrivene; u obrnutom slučaju ćemo imati izuzetno vremenski zahtevne proračune i proizvod (zaštićenu informaciju), koji je količinski znatno veći nego originalna informacija. Pošto se u današnjim hibridnim kriptosistemima asimetrična kriptografija pre svega koristi za siguran transfer simetričnih sesijskih ključeva, smatramo da uz odabir dovoljne dužine ključa ova karika kriptografskog lanca nije kritična.

Hashfunkcije

U *hash* funkcije spadaju matematičke funkcije koje na osnovu ulazne poruke generišu vrednost fiksne dužine, tzv. *hash vrednost, message digest* ili *message fingerprint* – "otisak prsta" ulazne poruke. Često korišćena tehnika *One-Way-Hash* omogućava da se utvrdi eventualna izmena podataka. Ova tehnika koristi OWF (*One-Way-Functions*), čiji je rezultat "*digest*" - obično 128 ili 160 bita. Praktično je nemoguće proizvesti dokument koji odgovara *digest*-u drugog dokumenta, tako da je ova tehnika provere integriteta podataka veoma pouzdana (detaljnije u opisu funkcionisanja mehanizma digitalnih potpisa). Danas se koriste sledeći *hash* algoritmi:

- *Message Digest* (128-bit digest); MD2, MD4 i MD5,
- *Secure Hash Algorithm* (160-bit digest); SHA i SHA-1,
- *Digital Signature Algorithm* (DSA),
- *Hash Message Authentication Code* (HMAC).

Upravljanje mrežama, Protokoli: SNMP, (MBI) Management Information Base, (SMI)

Upravljanjemrežom je širokspektarfunkcija, uključujućiaktivnosti, metode, procedure iupotrebualata za administriranje, upravljanjeipouzdanoodržavanjemrežnihsistema.

Uslugekojepruža ova disciplina jeste analiza grešaka, upravljanjeperformansama, obezbedjivanje mreža i održavanje kvaliteta usluge.

Softver koji omogućava administratorima mreže da obavljaju svoje funkcije naziva se softver za upravljanje mrežom. Upravljanje mrežom omogućava da se nadgledaju mrežne komponente unutar velike mreže.

Upravljanje mrežom poziva na kontinuirano, u realnom vremenu poznavanje celokupne mrežne infrastrukture. Vodi se računa o dostupnosti, performansama i upotrebi u celoj mrezi i njegovim različitim uredjajima, ublažavajući rizike i rešavajući probleme.

Neke od glavnih oblasti u sistemu upravljanja mrežama su:

Administracija mreže:

Ovo uključuje praćenje i inventorisanje mnogih mrežnih resursa, kao što su nadgledanje prenosnih linija, čvorišta, prekidača, rutera i servera.

To takodje uključuje praćenje njihovog rada i ažuriranje njihovog povezanog softvera, posebno mrežnih operativnih sistema i distributivnih softverskih aplikacija koje koriste korisnici mreže.

Mrežne operacije:

Ovo uključuje funkcionisanje mreže kao što je dizajnirano i namenjeno, uključujići pražljivo praćenje aktivnosti za brzo i efikasno rešavanje problema.

Održavanje mreže: Ovo uključuje pravovremenu popravku i neophodne nadogradnje svih mrežnih resursa, kao i preventivne mere kroz blisku komunikaciju i saradnju sa mrežnim andministratorima.

Omogućavanje mreže:

Ovo podrazumeva konfigurisanje mrežnih resursa da podrže zahteve odredjenje usluge.

Inženjeri koriste sistem za upravljanje mrežom da bi upravljali različitim operacijama, medju kojima su:

Performanse monitora:

Prikupljanjem operativnih metrika kroz seriju fizičkih pipaka, softverskih agenata ili interfejsa jednostavnog mrežnog protokola, sistem za upravljanje mrežom može da obezbedi vidljivost potrebnu da se utvrdi da li mrežni elementi rade ispravno.

Otkrivanje uredjaja:

Sistem za upravljanje mrežom se koristi za otkrivanje uredjaja na mreži i za obezbedjivanje da se uredjaji prepoznajui ispravno konfigurišu.

Analiziranje performansi:

Sistem za upravljanje mrežom se koristi za praćenje indikatora podataka o performansama, uključujući korišćenje propusnog opsega, kašnjenje, dostupnost, i vreme rada rutera, prekidača kao i drugih mrežnih komponenti.

Dozvoljavanje obaveštenja:

U slučaju prekida rada sistema, sistem će obavestiti administratore o svim problemima u performansama.

Mrežni protokoli

Mrežni protokol je skup uspostavljenih pravila koji diktiraju kako formatirati, prenositi, i primate podatke tako da računarski mrežni uredjaji mogu komunicirati bez obzira na njihovu razliku u infrastrukturama, dizajnu ili standardima.

Podrška za mrežne protokole može biti ugradjena u hardver, softver ili oba.

Bez standardizovanih mrežnih protokola računari izmedju sebe ne bi mogli da funkcionišu osim u slučajevima specijalno izgradjenih mreža za specifičnu strkturu. Najpoznatiji protokoli su: (SNMP) Simple Network Management Protocol, (MBI) Management Information Base, (SMI) Structure of Management Information, …

SNMP

SNMP (Simple Network Management Protocol) je prvi standard napravljen za upravljanje mrežama. Dolazi iz de facto bazirane pozadine TCP/IP komunikacije i predstavlja protocol aplikativnog sloja. Protokol olakšava razmenu upravljačkih informacija izmedju mrežnih uredjaja.

Jedna ili više upravljačkih stanica konfigurišu, nadgledaju i primaju poruke od čvorova unutar mreže.

SNMP je relativno jednostavan i razumljiv, zbog čega je postao popularan protokol za upravljanje mrežom. Postao je standard jer su proizvodjači razvili aplikacije za upravljanje zasnovane na SNMP-u. Smatralo se da je brzo dizajnirano rešenje za pomoć pri radu na mreži, dok su drugi većiibolji protokoli bili dizajnirani. Ali zbog činjenice da nije objavljeno boljerešenje, SNMP je postao izborni protkol upravljanja mrežom.

Na ovom protokolu možemo razlikovati dva tipa upravljačkih jedinica, SNMP menadžeri i agenti. Stanica za upravljanje mrežom (NMS) je radna stanica na kojoj se pokreću višestruke aplikacije za upravljanje mrežom.

NMS se koristi za prikupljanje informacija iz upravljanih čvorova preko agenata i predstvalja ih korisniku na pogodan način. Agenti imaju zadatak da nadgledaju jedan ili više mrežnih čvorov ai prikupljaju informacije o tome št arade i kakav status imaju.

Postoje dve tehnike koje se koriste za komunikaciju izmedju upravljanih uredjaja i NMS-a, a to su anketiranje i izveštavanje od ogadjajima. Anketiranje je interakcija izmedju zahteva i odgovora izmedju menadžera i agenta. Izveštavanje o dogadjajima je akcija koju inicira agent. On šalje infromacije menadžeru, koji onda čeka na dolazne podatke.

Uticaj performasni na upravljane uradjaje i agente potrebno je minimizirati, iz razloga što su resursi čvora često ograničeni u smislu performansi CPU-a ili ograničene memorije.

Postoje različiti tipovi čvorova, neki upravljaju i mogu biti upravljani, neki razumeju različite verzije SNMP protokola, neki nisu upravljivi, itd…

SNMP poruk ekoje se razmenjuju preko mreže sadrže dva dela, zaglavlje poruke i protokolne jedinice podataka.

Zaglavlje poruke sadrži broj verzije i naziv zajednice, dok protokolne jedinice podataka sadrže specificirane SNMP operacije. Ukupno imamo pet različitih protokolnih jedinica podataka, dva čitaju podatke o terminalu, dva podašavaju podatke o terminalu, a jedan se koristi za nadgledanje mrežnihdogadjaja.

SNMP V1 se zasniva na jednostavnom principu zahtev-odgovor. On obezbedjuje četiri operacije a to su: Komande za čitanje (get) omogućavaju mrežnom menadžeru da nadgleda upravljane uredjaje, a komande za pisanje (set) NMS koriste za kontrolu promenljivih koje su uskladištene upravljanim uredjajima. Operacije ‘get-next’ odredjuju koje varijable podržavaju podršku za upravljane uredjaje i mogu sekvencijalno prikupljati informacije. I na kraju naredba ‘trap ’izveštava o odredjenim dogadjajima NMS-u.

SNMP funkcioniše preko UDP-a bez povezivanja pre svega što je to nepouzdan provajder transporta, u kome se podaci mogu izgubiti. Provajder je orijentisan na povezivanje isporučuje ili sve podatke ili ništa. Na menadžeru je da otkrij egubitak podataka. Dok je druga implikacija za UDP je da menadžeri moraju da izvrše provere da bi otkrili da li su agenti još uvek operativni. Za razliku od provajdera orijentisanih na povezivanje, koji imaju funkcije kontrole u toku života da bi proverili da li je agent operativan ili ne, menadžer ima odgovornost da se pobrine za ovaj problem.

SNMP definiše samo kako se informacije o upravljanju razmenjuju preko mreže, a ne k je informacije uopšte postoje.

Postoje tri verzije SNMP protokola čiji su nedostaci i benefiti dati u nastavku:

SNMP v1:

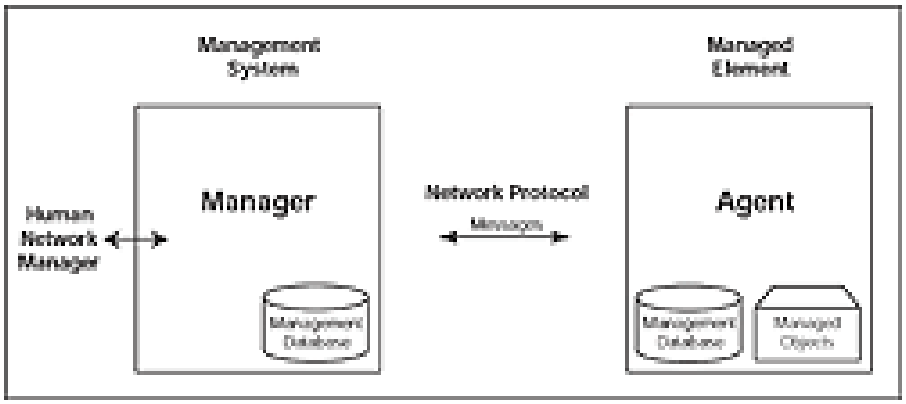
Najstarija verzija ovog protokola. Lako se podešava- zahteva samo zajednicu čistog teksta. Najveće mane su što ne podržava 64-bitne brojace, samo 32-bitne, i ima malu sigurnost.

SNMP v2:

U praktičnom smislu druga verzija protokola je ista kao i prva verzija osim što ima podršku za 64-bitne brojače, što je bitno, posebno za interfejse. Većina uredjaja danas podržava druguverziju SNMP-a. Nisu primećeni nedostatci u ovoj verziji.

SNMP v3:

Dodaje sigurnost 64-bitnim brojačima. SNMP verzija 3 dodaje i enkripciju i autentifikaciju, koja se mogu koristiti zajedno ili odvojeno. Podešavanje je složenije nego samo definisanje string zajednice.



SNMP

MIB

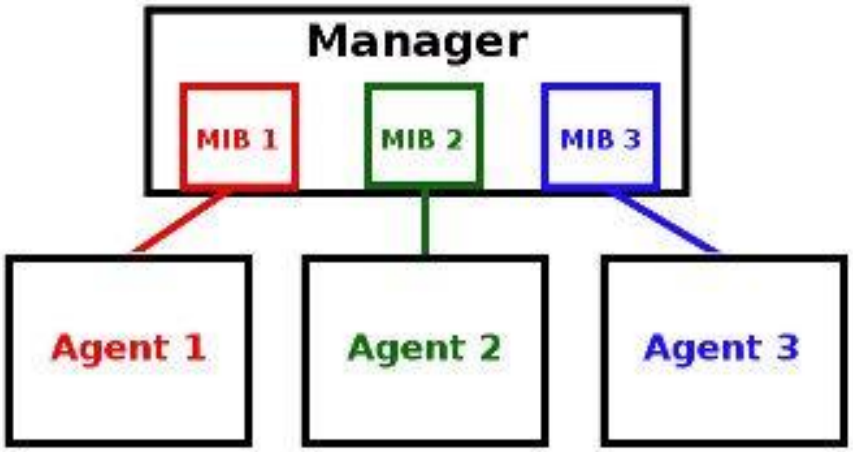
Management Information Base (MIB), je hirearhijska virtuelna bazapodataka o mrežnim objektima koji opisuju uredjaj koji se nadzire sistemom upravljanja mrežom (NMS).

Ovi objekti su logički prikaz fizičkih mrežnih komponenti koje su omogućene za SNMP (kao što su računari, čvorišta, ruteri, prekidači i softver za umrežavanje). MIB-ovi sadrže informacije o konfiguraciji tih mrežnih komponenti, kao što su verzija softvera koji se izvodi na komponenti, IP adresa ili broj porta i količina dostupnog prostora na disku. MIB se koristi pomoću protokola SNMP. MIB baza podataka je namenjena za referenciranje kompletne zbirke upravljačkih informacija o entitetu, medjutim često se koristi za upućivanje na podskup baze podataka i često se naziva MIB modul.

Pošto je svaki MIB član MIB hirearhije, može se jedinstveno identifikovati MIB za svaku mrežnu komponentu. Svaki MIB je adresiran ili identifikovan pomoću identifikatora objekta (OID), koji je često postavka ili status uredjaja. OID jedinstveno identifikuje upravljani objekat u MIB hirearhiji.

Da bi uklonili dvosmislena značenja i popravili nedostatke podataka, MIB-ovi se ažuriraju, ali te promene moraju biti u skladu sa odredjenim pravilima. SNMP protocol koristi MIB, i sakuplja podatke iz jednog MIB-a.

Postoje dva tipa upravljanih objekata, a to su skalarni i tabularni objekti. Oni definišu pojedinačnu instance objekta ili višestruke srodne instance objekta grupisane u MIB tabele.



-MIB

MIB je u suštini šifarnik koji prevodi numeričke nizove, koje šalje SNMP, u tekst koji je moguće čitati.

Elementi definisani u MIB-u mogu biti veoma široki kao i svi objekti kreirani od strane privatnih preduzeća.

Dok je svaki OID jedinstven, prvih nekoliko delova svakog OID-a je ista. Ovi nivoi gornje lokacije su definisani serijom standardnih reference unutar MIB-a. Pojedini proizvodjači kreiraju sopstvene MIB-ove koji uključuju samo OID-ove koje se spicifično odnose na njihov uredjaj.

Ova struktura čini SNMP MIB obejktno orijentisanim, maksimalno efikasnim načinom pohranjivanja informacija.

MIB fajlovi se sastoje od ASCII teksta i mogu se pregledati pomoću bilo kog programa za obradu teksta. Kada se čita MIB, nije potrebno čitati svaku pojedinačnu liniju teksta. Medjutim potrebno je poznavati neke od koncepata ugradjenih u MIB medju kojima su:

- Koje karakteristike uredjaja mogu da se kontrolišu daljinski pomoću SNMP menadžera,
- Koje izveštaje o dogadjajima uredjaj može da pošalje SNMP menadžeru,
- Koje informacije SNMP menadžer može da zatraži od uredjaja,
- Koji MIB-ovi su otvorenog koda i mogu se naći i preuzeti pomoću jednostavne veb pretrage.

SMI

Stucture of Management Information (SMI) protokol se u osnovi koristi za standardizaciju raličitih atributa objekata kao što su identifikatori objekata, tip objekta i metode kodiranja objekta.

SMI definiše okvir koji opisuje osnovne tipove informacija koje mogu biti manipulisane od strane SNMP-a.

On obezbedjuje skelet koji specificira osnovni format i hirearhiju upravljačkih podataka, ali ne opisuje objekte kojima se može upravljati. Umesto toga, on opisuje gradjevinske blokove od kojih se upravljaju objekti.

Identifikatori objekta: Svaki SNMP objekat ima jedinstven identifikator objekta, SMI dozvoljava da identifikatori objekta budu ili u obliku imena ili u obliku broja, medjutim oba oblika imaju hirearhijsku infrastrukturu.

Tipovi objekata:

SMI definiše osnovne tipove podataka koji olakšavaju opisivanje upravljanih objekata. Ovi tipovi su: Integer, ipAdress, Counter, Octet_String, Object_Identifier, Gauge, TimeTicks, NetworkAddress, Opaque.

Metoda kodiranja objekata: SMI koristio snovnapravila za kodiranje (BER) koja se sastoji od tipa/oznake, dužine i vrednosti, da bi se kodirali objekti zajedno sa njihovim vrednostima, za prenos unutar SNMP paketa.

SMI ne specificira listu objekata za odredjeni mrežniprotokol/ entitet, niti specificira tip objekata koji će se koristiti za odredjeni mrežni protokol. Ove aspekte vodi MIB.

Upravljanje adresama

Upravljanje Internet Protokol adresama (IPAM) je metoda praćanja i modifikovanja informacija povezanih sa prostorom mrežnog Internet Protokola (IP adresa). Pomoću IPAM-a, administrator mogu osigurati da inventar IP adresa koje se mogu dodeliti ostane aktuelan i dovoljan. Obično ne pruža DNS (Domain Name System) iDinamic Host Configuration Protocol (DHCP) usluge, ali upravlja informacije za ove komponente.

Mrežni administrator koriste IPAM da identifikuju i ažuriraju razne detalje o svojim mrežama, kao što su:

- Koliko slobodnog prostora IP adrese postoji,
- Koje podmreže su u upotrebi, koliko su velike i ko ih koristi,
- Stalni naspram privremenog statusa za svaku IP adresu,
- Podrazumevani ruteri koji koriste različite mrežne uredjaje,

- Ime hosta povezano sa svakom IP adresom,
- Specificni hardver povezan za svakom IP adresom.

Centralizovano prikupljanje ovih podataka možepomoći u istraživanju problema i zloupotrebe. IPAM alati su sve važniji jer se nove IP mreže koriste sa velikim bazama podataka.

Maske podmreže, VLSM, privatno adresiranje i NAT mogu omogućiti efikasnije korištenje IP adresa. Takodje i hirearhijsko adresiranje omogućava efikasnu alokaciju adresa i smanjen broj unosa tabele rutiranja. Posebno VLSM-ovi pružaju mogućnost uključivanja više od jedne podmrežne maske unutar mreže.

Mrežni fajl sistem

Mrežni fajl sistem (NFS) je klijent/server aplikacija koja korisničkom računaru omogućava pregled i opciono skladištenje i ažuriranje datoteka na udaljenom računaru kao da su na korisnikovom računaru. NFS protocol jedan je od nekoliko standard distribuiranog sistema datoteka za skladištenje u mreži (NAS).

NFS omogućava korisniku ili administrator sistema da montiraju (odrede kao pristupne) sve ili deo fajl sistema na serveru. Delu instaliranog fajl sistema klijenti mogu pristupiti bez obzira na privilegije dodeljene svakoj datoteci (samo za čitanjeili za čitanje-pisanje). NFS koristi pozive daljinskog postupka (RPC) za usmeravanje zahteva između klijenata i servera. NFS su prvobitno razvili Sun Microsystems 1980-ih, a sada im upravlja Internet inženjerskaradnagrupa (IETF). NFSv4.2 (RFC-7862) potvrđen je u novembru 2016. kaoskupproširenjana NFSv4 (RFC-3530).

NFS okruženje se može implementirati na različitim operativnim sistemima jer NFS definiše apstraktni model fajl sistema, a nearhitektonsku specifikaciju. Svaki operativni sistem primenjuje NFS model na semantiku fajlsistema. Ovaj model znači da su operacije ovog sistema poput funkcije čitanja i pisanja kao da operacije pristupaju lokalnoj datoteci. Usluga NFS ima sledeće prednosti:

- Omogućuje više računara da koriste iste datoteke, tako da svi u mreži mogu da pristupe istim podacima
- Smanjuje troškove skladištenja tako što računari dele delove aplikacija umesto da im je potreban proctor na disku za svaku korisničku aplikaciju
- Omogućava konzistentnost i pouzdanost podataka jer svi korisnici mogu čitati isti skup datoteka
- Čini montažu fajl sistema transparentnom za korisnike
- Pristup udaljenim datotekama čini preglednim za korisnike
- Podržava heterogena okruženja
- Smanjuje režijske troškove sistema

NFS usluga fizičku lokaciju datotečnog sistema čini nevažnom za korisnika. Može se koristiti NFS implementacija da bi se omogućila korisnicima da vide sve relevantne datoteke bez obzira na lokaciju. Umesto da se stave kopije najčešće korišćenih datoteka na svakisistem, NFS usluga omogućava da se stavi jedna kopija na disk jednog računara. Svi ostali sistemi pristupaju datotekama širom mreže. Pod operacijom NFS, daljinski sistem datoteka gotovo se ne razlikuje od lokalnog sistemadatoteka.

Sistemi datoteka koji se dele putem NFS servisa mogu se aktivirati automatskim montiranjem. Autofs, usluga na strani klijenta, je struktura fajl sistema koja omogućava automatsku montažu. Sistem datoteka autofs se pokreće automatski kada se sistem pokrene. Automatsko pokretanje radi neprekidno, montirajući i demontirajući udaljene direktorijume po potrebi. Kad god klijentski računar koji radi automatski, pokušava da pristupi udaljenoj datoteci ili udaljenom direktorijumu, automatski se aktivira udaljeni sistem datoteka (fajl sistem). Ovaj daljinski sistem datoteka ostaje montiran onoliko dugokoliko je potrebno. Ako nekom udaljenom fajl sistemu nije dostupan određeni vremenski period, sistem datoteka se automatski isključuje. Montaža ne treba da se vrši u vreme pokretanja, a korisnik više ne mora da zna lozinku super usera za postavljanje direktorijuma. Korisnici ne moraju da koriste komande mount i umount. Auto fs servis montira i demontira sisteme datoteka po potrebi bez ikakve intervencije od strane korisnika. Montaža nekih hijerarhija datoteka sa automountd-om ne isključuje mogućnost postavljanja drugi hhijerarhija pomoću mount-a. Računar bez diska mora da montira / (root), / usri / usr / kvm prekoko mande mount i / etc / vfstab datoteke.

Daljinskipristup

Udaljeni ili daljinski pristup je mogućnost udaljenog pristupa računaru ili mrež iputem mrežne veze. Udaljeni pristupom ogućava korisnicima pristup sistemima koji su im potrebni ako se fizički ne mogu direktno povezati; drugim rečima, korisnici pristupaju sistemima na daljinu koristeći telekomunikacijske ili internetske veze.

.

Udaljenim pristupom ogućava udaljenim korisnicima da pristupaju datotekama i drugim sistemskim resursima na bilo kojim uređajima ili serverima koji su povezani na mrežu u bilo kojem trenutku, povećavajući produktivnost zaposlenihi omogućavajući im bolju saradnju sa kolegama širom sveta.

Jedan uobičajeni način pružanja udaljenog pristupa je putem VPN veze sa daljinskim pristupom. VPN stvara sigurnui šifrovanu vezu preko manje sigurnemreže, kao što je internet. VPN tehnologija razvijena je kao način da se udaljenim korisnicima i poslovnicama omogući sigurno prijavljivanje u korporativne aplikacije i druge resurse.

Preduzeća takođe mogu koristiti udaljene radne površine da bi se korisnicima omogućilo daljinsko povezivanje sa njihovim aplikacijama i mrežama. Udaljene radne površine koriste aplikativni softver – ponekad ugrađen u operativni sistem udaljenog domaćina – koji omogućava aplikacijama da se daljinski pokreću na mrežnom serveru i istovremeno prikazuju lokalno. Korisnici mogu bezbedno pristupati lokalnim i oblačnim aplikacijama i serverima sa bilo kog mesta, na bilo kom uređaju sa raznim metodama provere identiteta, uključujući udaljeno jednokratno prijavljivanje, što korisnicima omogućava lak i siguran pristup aplikacijama koje su im potrebne bez konfigurisanja VPN-ova ili izmene zaštitnog zida politike. Pored toga, organizacije mogu koristiti višefaktornu proveru identiteta za proveru identiteta korisnika kombinujući više jedinstvenih dokumenata za jednu osobu.

Softveri za upravljanje mrežama

Postoje mnogi softveri za upravljanje softvera, medju kojima se nalaze sledeći koji su okarakterisani kao najbolji u 2019 godini:

Solarwinds Network Performance Monitor je jednostavan za podešavanje i može biti spreman za kratko vreme. Alat automatski otkriva mrežne uredjaje i njegov jednostavan pristup nadgledaju čitave mreže čini ga jednim od najlakših za upotrebu i najintuvnijim korisničkim interfejsima.

Proizvod je veoma prilagodljiv i interfejs se lako upravlja i menja veoma brzo, može se prilagoditi veb-bazirane kontrolne table, grafikone i prikaze. takodje se može i dizajnirati prilagodjen u topologiju za celu mrežnu infrastrukturu.

PRTG Network Monitor from Paessler je poznat po svojim naprednim mogućnostima upravljanja infrastrukturom. Svi uredjaji, sistemi, saobraćaj i aplikacije u vašoj mrežim ogu se lako prikazati u hirearhijskom pogledu koji sumira performance i upozorenja. PRTG prati IT infrastrukturu koristeći tehnologije kao što su SNMP, VMI, HTTP, itd…

To je jedan od najboljih izbora za organizacije sa niskim iskustvom u nadgledanju mreže. Korisnički interfejs je zaista moćan i veoma jednostavan za upotrebu.

ManageEngine OpManager u svojoj osnovi ovaj softver je upravljanje infrastrukturom, nadgledanje mreže i upravljanje performansama aplikacije APM softverom. Softver je dobro izbalansiran kada su u pitanju funkcije praćenja i analize. Rešenje može da upravlja mrežom, serverima, mrežnom konfiguracijom, greškama i performansama. Ovaj proizvod sadrži unapred konfigurisanim šablonima uredjaja za nadzor mreže koji sadrže unapred definisane parametre praćenja i intervale za odredjene tipove uredjaja.

Nagios XI Nagios KSI je namenjen širokoj publici, od slobodnih novinara, malih i srednjih preduzeća, do velikih korporacija. Ovo čini Nagiosov KSI cenovni model jednim od najfleksibilnijih.

Imaju besplatnu verziju, open-source, jednokratnu licencu i pretplatu. To je jedan od retkih alata koji omogućava ekstremnu fleksibilnost (zbog svoje prilagodljivosti plug-inovima) na ono što se prati i upozorava na niske troškove.

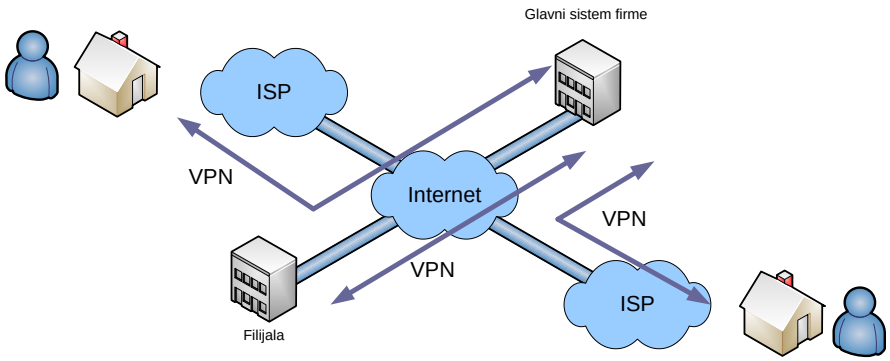
Nagios KSI je softver koji se fokusira na monitoring. Ključne IT komponente koje Nagios KSI koristi su mreža, infrastruktura i baza podataka. Iako je softverj ednostavan za instalaciju, potrebno je malovremena da se prilagodi vašim potrebama. To je zato što Nagios KSI ne otkriva automatski uredjaje. Morate da konfigurišete svaki uređaj koji treba da se nadgleda pomoću konfiguracione datoteke.

Virtuelne privatne mreže (VPN)

VPN (*Virtual Private Networks*) su virtuelne privatne mreže. VNP koncept omogućuje kreiranje sigurnih, privatnih mreža, korišćenjem javne mreže kao što je Internet. To se može postići upotrebom odgovarajućeg softvera, hardvera ili njihovom kombinaciom u cilju uspostavljana sigurne veze između dve lokacije preko javne mreže. To se može postići uz enkripciju, autentifikaciju, tuneliranje i uz upotrebu firewall sistema [Scott1999].

Nazivaju se i enkriptovani tuneli. VPN može da omogući sigurnu komunikaciju za povezivanje dve fizički odvojene mreže preko Interneta. Te mreže mogu komunicirati bez izlaganja podataka neautorizovanom pristupu i eventualnom prisluškivanju. U toku uspostavljanja tunela VPN mogu biti meta mnogih napada. Ako se implementiraju kao deo *firewall* sistema, *firewall* može da spreči ove napade.

Kada se tunel uspostavi, VPN mreže su bezbedne sve dok je enkripcija sigurna. Privatne mreže mogu da razmenjuju saobraćaj kao da se radi o dva segmenta iste mreže. VPN dozvoljava korisniku da pristupi hostu direktno unutar mreže, preko njegove skrivene IP adrese.



Slika 109: Povezivanje udaljenih lokacija preko VPN mreža

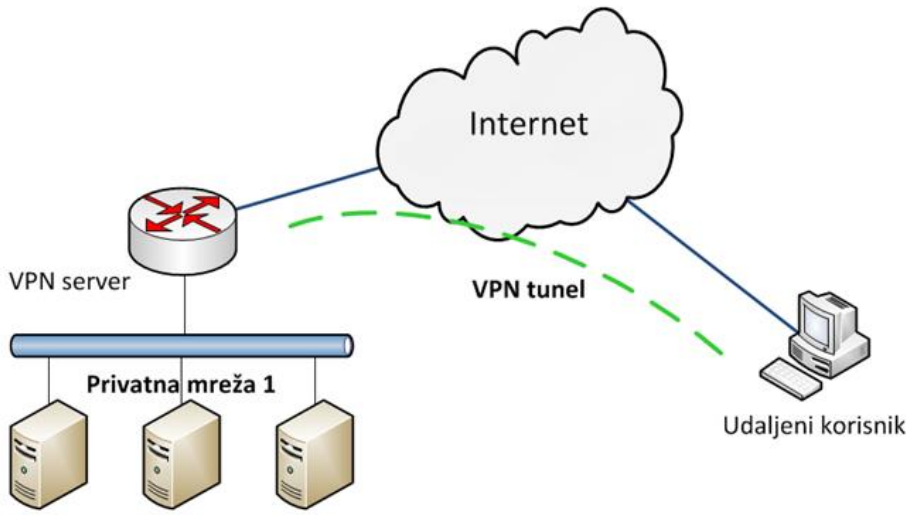
Postoji veći broj protokola koji se koristi za VPN mreže, kao na primer: VPN preko SSH, MPLS (*Multi-Protocol Label Switching*), PPTP (*Point-to-Point Tunneling Protocol*), L2TP (*Layer-2 Tunneling Protocol*), IPSec (*IP Security*) protokol, GRE (*Generic Routing Encapsulation*) itd. Linux distibucije imaju podršku za enkriptovane tunele uz upotrebu PPP *over* SSL (*Point-to-Point Protocol over Secure Socket Layer*) protokola.

Postavlja se pitanje kada treba koristiti VPN konekcije. Alternativa za povezivanje udaljenih lokacija je povezivanje posredstvom iznajmljene linije jednom od pomenutih WAN tehnologija. Kada je takvo rešenje dovoljno ekonomično i ostvarivo, za povezivanje dve udaljene mreže iste kompanije, preporučuje se upotreba i uspostavljanje iznajmljenih linija, pošto su one mnogo sigurnije. Naravno, ovo je moguće kada se te dve lokacije nalaze u istom gradu ili na relativno malim rastojanjima. Kada je potrebno povezati udaljene lokacije na većim rastojanjima, takvo povezivanje postaje veoma skupo, pa se moraju koristiti VPN mreže. VPN mreže su neophodne pošto se tada povezivanje vrši preko Interneta, pa komunikacija mora biti sigurna.

U ovom slučaju, najbolje je koristiti isti ISP sistem, pošto se VPN saobraćaj ne mora usmeravati međuprovajderskim linkovima. Interna komunikacija dve mreže preko Interneta ne sme se obavljati kroz neenkriptovani kanal. Neenkriptovani paketi sadrže korisne informacije za potencijalne napadače.

VPN je tehnologija koja omogućava **sigurno** povezivanje računara ili privatnih mreža u zajedničku virtuelnu privatnu mrežu i to kroz privatnu ili javnu mrežnu infrastrukturu (prvenstveno se to odnosi na Internet).

Za razliku od privatnih mreža koje koriste iznajmljene linije za komunikaciju, VPN može da radi i preko javne mreže uspostavljanjem sigurnog kanala između krajnjih tačaka



Osnovna zamisao VPN tehnologije je da obezbedi sigurno povezivanje privatnih mreža preko javne mrežne infrastrukture, odnosno Interneta.

To se najčešće izvodi **tuneliranjem podataka** između dve tačke. Kod tuneliranja podataka, podaci se mogu komprimovati i/ili kriptovati.

Implementacija VPN-a može biti **softverska ili hardverska** a često se koristi i kombinacija.

Po pravilu programska podrška je dovoljno brza za kriptovanje/dekriptovanje do 10Mbps podataka u realnom vremenu, a za veće brzine se koristi hardverska podrška.

VPN može obezbediti sigurnost, ali stalnu vezu ne može garantovati. Propusnost veze je jednaka najslabijoj tački u njoj.

U prednosti su iznajmljene (skuplje) linije koje po pravilu obezbeđuju stalnu vezu i pouzdan prenos podataka.

ZAHTEVI KOJE TREBA DA ISPUNI VPN:

Potrebno je da VPN tehnologija ispuni sledeće zahteve:

- **Upravljanje adresama** – VPN je zadužen za dodjeljivanje klijentskih adresa unutar privatnih mreža;
- **Mehanizme za upravljanje ključevima** – VPN mora osigurati generisanje i osvježavanje ključeva između klijenta i pružalaca usluga;
- **Podršku za razne protokole** – VPN mora podržavati standardne protokole koji se koriste u javnim mrežama (IP, IPX, itd.).

Vrlo su bitni i sigurnosni zahtevi:

- **Pravo pristupa** – Potrebno je da VPN osigura proveru identiteta korisnika i dozvoli pristup samo registrovanim korisnicima
- **Autentifikaciju** – Potrebno je da VPN osigura da podaci koji dolaze stvarno dolaze s odredišta s kojeg tvrde da dolaze i da osoba koja tvrdi da je pošiljalac podataka to stvarno i jeste.
- **Integritet podataka** – Potrebno je da VPN osigura da niko ne menja podatke dok se prenose Internetom. Za to se najčešće koristi kriptografski algoritam MD5 (Message-Digest algorithm 5), koji spada u grupu haš algoritama ili algoritama za sažimanje.
- **Poverljivost (kriptovanje)** – Potrebno je da VPN osigura kriptovanje podataka tako da ih niko, osim klijenta, odnosno pružaoca usluge, ne može pročitati. To se postiže raznim algoritmima poput DES, 3DES, RSA ili Diffie-Hellman

VRSTE VPN REŠENJA

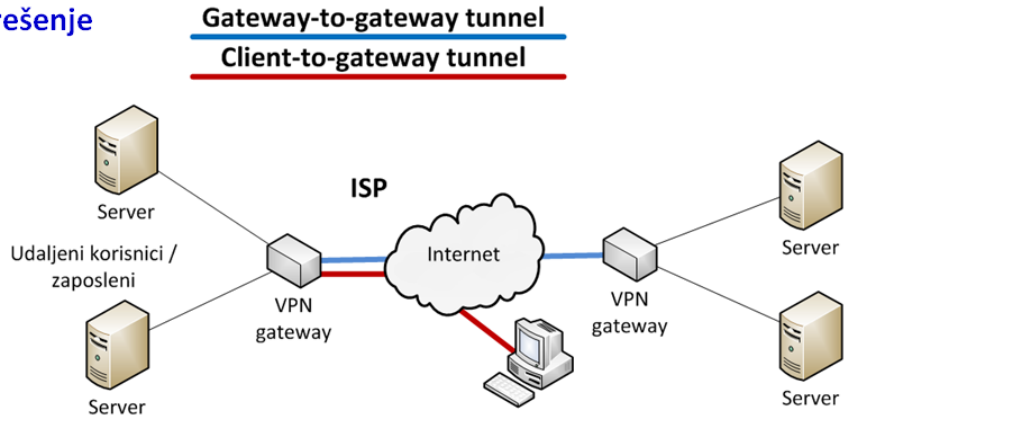
U odnosu na **mogućnost primene VPN se dele na**:

- **Intranet VPN -** Koristi se za povezivanje više lokacija unutar jedne organizacije. Za prenos podataka se koristi Internet ili WAN.
- **Extranet VPN -** Koristi se za povezivanje dva ili više dobavljača i/ili poslovnih partnera. Za prenos podataka se koristi Internet ili WAN;
- **Udaljeni pristup -** Povezuje udaljene korisnike (ili manje poslovnice) sa lokalnom mrežom preduzeća. Povezivanje se obavlja putem modemske veze preko Interneta (ponekad se to naziva VPDN = Virtual Private Dial Network).

U **zavisnosti od konfiguracije VPN se dele na** :

- **"Client-to-server" (ili "client-to-gateway") rešenje** - Koristi se kod modemskih (Dial-up) rešenja
- **"Server-to-server" (ili "gateway-to-gateway") rešenje** - Koristi se kod spajanja dve ili više odvojenih lokalnih mreža.

"Client-to-server" (ili "client-to-gateway") i "Server-to-server" (ili "gateway-to-gateway") rešenje



UREĐAJI U VPN-U

Uređaji u IP VPN-u su:

CPE *(Customer Premisses Equipment)* - odgovarajući korisnički uređaji (kompjuteri, ruteri, firewall-ovi, ili neki drugi specijalni VPN uređaji),

NAS (*Network Access Server)* - uređaj pomoću kojeg provajder usluga ISP (Internet Service Provider) obezbeđuje korisniku Internet pristup,

HG *(Home Gateway)* predstavlja kraj veze kojim se centralni deo VPN mreže povezuje na Internet preko NAS-a.

TUNELIRANJE

Tuneliranje predstavlja tehniku prenosa podataka o okviru jedne VPN mreže preko neke druge mreže za prenos. Podaci koji se šalju mogu biti formatizovani u ramove (ili pakete) a moguća je primena i nekih drugih protokola.

Tuneliranje je enkapsulacija paketa jednog protokola u pakete drugog protokola, ali pri tome je drugi protokol na istom ili višem nivou nego prvi.

Protokol, kojim se implementira tuneliranje, enkapsulira tj. dodaje originalnom ramu posebno oblikovano zaglavlje koje sadrži dodatne podatke (za usmeravanje) kako bi enkapsulirani paket stigao, kroz mrežu koja služi za prenos, do odredišta.

Enkapsulirani podaci se onda šalju između krajnjih tačaka tunela.

Tunel je logički put kojim enkapsulirani podaci prolaze kroz mrežu koja služi kao medijum za prenos.

Kad takav ram dođe do svog odredišta podaci se izdvajaju/ekstrahuju i zatim šalju na ciljno odredište.

Tuneliranje uključuje čitav navedeni proces (enkapsulacija, prenos i ekstrakcija).

VPN se može podeliti i u zavisnosti o tipu tuneliranja koji koriste na:

- **Stalno** – nisu isplativi zbog toga što traže određeni rezervisani propusni opseg za prenos podataka (bandwidth) čak i kada se podaci ne prenose, a ISP-ovi često naplaćuju prosečni garantovani protok.

- **Privremeno** – uspostavljaju se kada klijent zatraži spajanje u VPN i raskidaju se kad se komunikacija završi.

Postoje razne tehnologije koje omogućavaju tuneliranje, a najpoznatije od njih su:

- PPTP (Point-to-Point Tunneling Protocol)
- L2F (Layer 2 Forwarding)
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (Internet Protocol Security Tunnel Mode)
- Mobile IP – za mobilne korisnike
- GRE (Generic Routing Encapsulation) (CISCO)
- ATMP (Ascend Tunnel Management Protocol)
- DLSW (Data Link Switching)

INFORMACIONA BEZBEDNOST RAČUNARA NA INTERNETU

Pretnje informacionim resursima

Informacione resurse jedneorganizacije čine: računari i druga prateća oprema, kao i informacije na njima, informacioni sistemi i aplikacije, baze podataka.

Ti resursi su izloženi mnogobrojnim pretnjama.

Pretnja informacionom resursu je bilo kakva opasnost kojoj sistem može da bude izložen.

Izloženost informacionih sistema je narušavanje, gubitak ili oštećenje koje može da se desi ukoliko pretnjana ruši ta jsistem. Rizik je verovatnoća da će se pretnja pojaviti. Kontrola informacionih sistema je niz procedura, uređaja ili softvera koji služe kao prevencija da se sistem ne naruši. Informacioni sistemi su izloženi mnogim potencijalnim pretnjama i rizicima.

Vithmani Mattordsu 2003 godine klasifikovali pretnje u sledeće kategorije:

1. Nehotični postupci
2. Elementarne nepogode
3. Tehnički kvarovi
4. Greške menadžmenta
5. Namerni postupci

Nehotični postupci

Nehotični postupci su ljudske greške koje nemaju zle namere.Pretnje bezbednosti sistema od strane stalno zaposlenih:

a) Aplikativni programer(programiranje aplikacija da funkcionišu van opisa njihove specifikacije)
b) Sistemski programer (zaobilaženje mehanizma zaštite, isključivanje mehanizma zaštite, instaliranjen ebezbednih sistema)
c) operateri(kopiranje poverljivih izveštaja, pokretanjene bezbednih sistema, krađa poverljivog materijala)
d) korisnici(greške pri unošenju podataka, slabe lozinke,nedovoljna obuka)

Drugu kategoriju zaposlenih u organizaciji čine honorarni saradnici, konsultanti, domari i čuvari. Konsultantii honorarni saradnici često imaju pristup lokalnoj mreži organizacije, informacionim sistemima i informacionim sredstvima. Najčešće zloupotrebe sa njihove stranes u:

a) neovlašćeni pristup
b) krađa
c) kopiranje

Najčešće nehotične ljudske greške su:

a) „prilepljivanje“ (tehnika kojom uljez ulazi u odeljenja u koja je zabranjen ulaz i koja se obezbeđuju bravom ili karticom)
b) Gledanje preko ramena(uljez posmatra monitor računara preko ramena zaposlenog)
c) Nemaran odnos prema laptopu (gubljenje laptopa)
d) Nemarnost sa prenosivim uređajima(gubljenje prenosivih uređaja ili nemarno korišćenje omogućava da zlonamerni softver dospe do mrež eorganizacije)
e) Otvaranje sumnjive e-pošte (otvaranje poštene poznatog pošiljaoca ili klik na linkove koji su u e-pošti)
f) Nemarno pretraživanje interneta (pristupanje sumnjivim web-sajtovima može uzrokovati da zlonamerni softver ili tuđi softve rdođe do mreže organizacije)
g) Loš izbor lozinke i neoprezno korišćenje lozinke(dobra lozinka treba da je dugačka najmanje 8, a najviše 127 znakova, da ne sadrži korisničko ime, stvarno ime il imekompanije, da ne sadrži kompletnu reč, da je drugačija od prethodnih lozinki. Znakovi koje sadrži lozinka treba da budu iz svih sledećih kategorija: mala slova, velika slova, brojevi, simboli sa tastature)
h) Nemarnost na random mestu (ostavljanje otključane kancelarije i ormana sa dokumentima posle završetka radnogvremena, neodjavljivanje sa kompjuterske mreže kada zaposleni napusti svoje mesto na duži period)
i) Nemarno korišćenje privatnih uređaja(to su uređaji koji pripadaju klijentima ili poslovnimpartnerima, računari koji se nalaze u poslovnim centrima hotela is viostali koji se nalaze na javnim mestima)

Elementarne nepogode

Elementarne nepogode, kao što su poplave, zemljotresi, udar groma, uragani, tornada, ili požari, mogu dovesti do gubljenja podataka, pa kompanije moraju da isplaniraju pravljenje rezervnih kopija.

Tehnički kvarovi

Tehnički kvarovi obuhvataju problem sa hardverom i softverom. Najčešći hardverski problem je kvar hard diska. Najčešći softverski problem su greške u računarskim programima.

Greške menadžmenta

Greške menadžmenta povezane su sa nedostatkom sredstava za informacionu zaštitu i nedostataki nteresovanja da se ta zaštita sprovede.

Takav stav top menadžmenta organizacije uzrokuje nebezbednost informacionih sistema u celini.

Namerni postupci

Namerni postupci zaposlenih u samoj organizaciji ili osoba van organizacije uzrokuju veliki broj krađa informacija. Vrste takvih postupakas u:

a) Špijunaža ili upadanje u posed

b) Informaciono iznuđivanje

c) Sabotaža ili vandalizam

d) Krađa opreme ili informacija

e) krađaidentiteta

Tipovi softverskih napada:

1. **Virus**
2. **Crv**
3. **Trojanski konj**
4. **Sporedni ulaz**
5. **Logička bomba**
6. **Napadi na lozinku**
7. **Napad uskraćivanjem servisa**
8. **Distribuirani napad uskraćivanjem servisa**
9. **„Fišing“ napad**
10. **Napad metodom nultog dana**

Virus

Virus je maliciozan kod koji se pri izvršavanju samo umnožava, kopira samog sebe unutar drugog izvršnogkoda (executable code).

Virusi se umnožavaju i šire unutar jednog računara i zatim se prenose od računara do računara prenosnim medijima kao štosu CD i DVD mediji, kao i USB memorijski uređaji.

Isto tako, mogu se širitii putem deljenih datoteka u lokalnoj mreži. Svojim razvojem internet je postao glavni medijum za širenjevirusa. U većinislučajeva, virusi se prenose putem elektronskepošte. Mogu se nalaziti kao izvršne i druge datoteke u prilogu e-mail poruke ili je čak nekad dovoljno da korisnik samo otvori poruku, da se računar inficira.

Pristigla poruka može biti od neke poznate osobe jer virusi, zajedno sa brojnim drugim vrstama parazita imaju sposobnost da se sami pošalju e-mailom sa inficiranog računara na sve adrese iz e-mail adresara.

Zaštita od virusa

Štete od virusa mog biti od bezazlenih poruka koje se pojavljuju na ekranu do vrlo teških kao što je brisanje dokumenata ili podataka koje zauvek nestaju sa hard diska.

Prvi virus koji je šokirao javnost, a posebno Ministarstvoodbrane SAD i univerzitetsku sredinu, je Morris koji je inficirao mrežu institucija i izazvao štetu koja se procenjujena oko 98 miliona dolara. Mnogo je veća šteta što je Morris inicirao brojne hakere da se utrkuju u sličnim poduhvatima. Od tada je otvoren beskompromisan front borbe između hakera i proizvođača antivirus programa.

Pretpostavlja se da u svetu računar ima preti preko 50000 virusa. Oni se klasifikuju u sledeće kategorije:

- Virusi koji inficiraj uprogramske fajlove tako što se zakače obično za .COM ili .EXE fajlove i inficiraju .SYS, .PRG ili druge sistemske fajlove.
  Kreatori virusa gađaju fajlove koji se startuju prilikom podizanja sistema. Kada se sistem startuje virus se munjevitom brzinom proširi pre nego što startuje zaštita.
- Česti su virusi koji se nalaze na disket iili CD. Njihovim učitavanjem učita se i virus koji može da stvori brojnep robleme kao što su blokiranje rada hard diska, pa sistem ne može ni da se pokrene, brisanje podataka itd.
- Makro virusi su najčešći vrlo opasni. Aplikacije kao što su Microsoft Word i Excel podržavaju makro jezike koji se koriste kao sredstvo za transport virusa.
- Makro e-mail virusi koji se prenose elektronskom poštom nastoje da izbegnu zaštitu a imaju vrlo retrogradno dejstvo. “BubbleBoy” je prvi e-mail virus koji je inficirao računar a da korisnik nije otvorio e-mail ili attachement.
- Crv je vrsta virusa koji se razmnožava.Unosi se u računar u stilu “Trojanskog konja” uz neki program ili podatke. Preduzima štetne aktivnosti po računar korisnika.

Crv

Crv je naziv za maliciozni kompjuterski kod koji se samostalno kopira i inficira računare, sposoban da samostalno traži nove sisteme domaćine i inficira ih putem mreže. Mnogi često poistovećuju crve s virusima, nazivajući ih samo jednom specijalnom vrstom virusa.

Istotako, mnogi poznati maliciozni program koji su popularno prozvani virusima, trebali bi biti smatrani crvima ili hibridima tih dveju vrste štetnih programa.

Crvi imaju neke zajedničke karakteristike sa virusima. Najvažnija karakteristika koju dele je mogućnosts amoumnožavanja. Međutim, razlikuju se u samom načinu kako to čine.

Prvo, crvi ne zahtevaju domaćina da bi se širili, kao virusi koji su paraziti. Crvi su samostalni, samostalno deluju i šire se.

Druga razlika je što je osnovni medijum širenja crva - mreža.

Crv se možeu množavati beskonačno il idok se ne zaustavi internim mehanizmom tempiranja – ako postoji.

Dve najčešće metode širenja crva su:

- Elektronska pošta (e-mail)
- Iskorišćavanje bezbedonosnih slabosti i propusta na računarima spojenim na mrežu ili na internet

Trojanski konj ili "trojanac"

Termin "trojanskikonj" potiče od poznate priče iz Ilijade. Sam naziv predstavlja zamku maskiranu u nešto naizgled bezopasno. Analogija važi i u računarskom svetu.

Trojanski konj je oblik zlonamernog softver akoji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Najčešće se predstavljaju kao neki zanimljiv program ili možda i neki video ili audio sadržaj kojeg korisnik traži.

Osnovna razlika od virusa i crva je ta da se trojanski konj ne može umnožavati. Tu se oslanja na neoprezne korisnike koji svojevoljno dozvoljavaju njihovo izvršavanje na sopstvenom računaru. Trojanski konj je mnogo opasniji i maliciozniji od virusa i crva, i programi za detekciju virusa (antivirus) i slični zaštitni program neretko ne uspevaju da ih prepoznaju.

Glavni cilj trojanskog konja je da napadaču omogući pristup sistemskim datotekama. Mogu da brišu datoteke ili čitave particije, da kopiraju datoteke na inficirani računar, da preimenuju datoteke, da kradu lozinke i ostale poverljive podatke, da onemoguće bezbedonosne programe, da ugase ili resetuju računar...

Sporedniulazilizadnjavrata (backdoor)

Danas taj termin predstavlja bilo kakav mehanizam koji napadač u potajno omogućava pristup sistemu ili mreži. Obično, nakon što dođe do "upada" u neki sistem ili mrežu iskorišćenjem neke rupe ili propusta u sistemu ili nekoj aplikaciji, napadači nastavljaju s prikrivanjem tragova i instaliraju zadnja vrata. Ako vlasnik sistema ili mreže i otkrije upad i ispravi propust, napadači pak ima mogućnost ponovnog pristupa ako korisnik nije otkrio i instalirani zadnji ulaz.

Najčešće je jedini način sigurnog uklanjanja zadnjih vrata potpuno obrisati sve i reinstalirati sistem sa ranije rezervne kopije (backup), za koju je dokazano da je sigurna.

Logičkabomba

Logička bomba je segment računarskog koda koji se sačuva u postojećim računarskim programima neke organizacije, a projektovan je da aktivira i izvršava destruktivne akcije u određeno vreme ili određenog dana.

Napadinalozinku

Napadi na lozinku se dele na napad metodom rečnika (Dictionary Attack) koji isprobavaju kombinacije slova i brojeva, na primer sve reči iz rečnika i napad metodom grube sile (Brute Force Attack) napadi koji koriste ogromne računarske resurse da isprobaju sve moguće kombinacije znakova kako bi otkrili pravu lozinku.

Napad uskraćivanjem servisa

Napadač šalje toliko mnogo zahteva za informacijama ciljanom računarskom sistemu, tako da sistem ne može uspešno da ih obradi i tada se dešava da “sistem padne” (prestane da funkcioniše).

Distribuiraninapaduskraćivanjemservisa

Napadač najpre preuzima puno računara pomoću zlonamernog virusa. Takvi računari su onesposobljeni za normalnu funkciju i nazivaju se zombiji ili roboti. Napadač od njih formira mrežu kako bi preneli koordinisanu masu zahteva za informacijama ciljanom računaru, zbog čega ciljani računar prestane da funkcioniše.

“Fišing” napad

Ovakvim napadom napadač se lažno predstavlja kako bi izvukao osetljive informacije putem poruka zamaskiranih u e-poštu ili instant poruke.

Napad metodom nultog dana

Napadač koristi novootkrivenu nepoznatu slabu tačku u softveru i počinje sa napadima na nju, pre nego što proizvođač softvera stigne da je otkloni.