

* Sve sa prezentacija i iz zbirke (bez zadatka) i bitni delovi iz knjige

* Crvenom je oznaceno ono sto je dolazilo ranije i 100 pitanja, predlog je da se samo to uci ☺

8. Baze podataka

8.1 Uvod u baze podataka

- **Baze podataka** – predstavljaju skup povezanih i struktuiranih podataka i njihovih opisa.
- **Tri komponente baza podataka** su:
 - Tabele ili datoteke,
 - Veze (relacije) između vrsta u tabelama,
 - Metapodaci tj podaci o podacima.
- Nad bazama podataka se izvršavaju aplikacije ili sistemi aplikacija. **Komponente sistema aplikacija** su:
 - Krajnji korisnik,
 - Aplikacija (program, izveštaj, upit...),
 - Baza podataka,
 - Sistem za upravljanje bazom podataka (DBMS).
- **Model podataka**– predstavlja specifične teorije pomoću kojih se specificira i projektuje neka konkretna baza podataka ili informacioni sistem. Modeli podataka su intelektualni alati za opisivanje sistema kao skupa objekata, njihovih atributa i medjusobnih veza. Najzastupljeniji je relacioni model (kod njega je najbitnija ta relacija između tabela).
 - Tri komponente modela podataka su:
 - Logička struktura svih podataka u bazi,
 - Skup operatora,
 - Skup ograničenja nad podacima.
- **Enkapsulacija** - Dodavanje informacija postojećim u toku prelaza sa viših na niže slojeve u OSI modelu.
- **Četiri komponente modela podataka**:
 - struktura modela (skup koncepata za opis objekata sistema, njihovih atributa i njihovih međusobnih veza)
 - ograničenja na vrednosti podataka u modelu
 - operacije nad konceptima strukture (preko kojih je moguće prikazati i menjati vrednosti podataka u bazi)
 - dinamička pravila integriteta (definišu osnovno dinamičko ponašanje modela)
- **Model podataka se može dekomponovati na tri dela**:
 - Logički model:
 1. Eksterni nivo – kako korisnici vide podatke,
 2. Konceptualni nivo – logička struktura podatka,
 - Fizički model:
 3. Interni nivo – fizička definivija podataka.
- **Šema** – je opis određenog skupa podataka korišćenjem datog modela podataka.
- **Podšema** – planovi korišćenja delova baze podataka uz korišćenje aplikativnih programa.

- **Fizička šema** – plan fizičke baze. Sadrži podatke kojima se opisuje realni sistem i podatke o podacima.
- **Konceptualna šema** – plan konceptualne baze. Definiše logički opis baze podataka, predstavlja apstraktan model baze podataka. Kreira se u toku planiranja i systemske analize.
- **Fizička nezavisnost podataka** – izmene u fizičkoj strukturi podataka ne dovode do promena u šemama, podšemama i aplikativnih programa. Nezavisnost između konceptualne šeme i interne šeme.
- **Logička nezavisnost podataka** – izmene konceptualne šeme ne utiču na izmene šema i podšema pod uslovom da se ne menjaju obeležja podataka koji se koriste. Samo se menja preslikavanje šeme u podšeme. Nezavisnost između konceptualne šeme i podšema.
- Termini logički i fizički označavaju različite aspekte struktuiranja podataka.
- **Funkcionalna zavisnost** – kada je svakoj vrednosti a (atributa) moguće pridružiti samo jednu vrednost b (atributa), kažemo da je a zavisno od b.
- **Potpuna funkcionalna zavisnost** – atribut je potpuno zavisan od ključa ako je funkcionalno zavisan od celog ključa. Odnosno kada je ključ sastavljen od više atributa.

- **UML** – je standardni grafički jezik za specifikaciju, projektovanje i dokumentovanje softverskih sistema.
 - Dijagrami slučajeva korišćenja (namenjeni za specifikaciju zahteva datog softverskog sistema.)
 - Dijagrami klase (namenjeni za specifikaciju strukture datog sistema.)
 - Dijagrami kolaboracije (namenjeni za specifikaciju dinamike datog sistema)
 - Dijagrami komponenti (specifikacija implementacije datog softverskog sistema.)
 - Dijagrami sekvenci su namenjeni za opis ponašanja datog softverskog sistema za izdvojeni scenario slučaja korišćenja.

- Baza podataka se **projektuje** u dve faze: u prvoj fazi se projektuje logicka struktura, a u drugoj fizička struktura baze podataka. Rezultat prve faze su konceptualna šema i podšeme baze podataka. Rezultat druge faze je interna šema baze podataka.

• **Osnovne vrste modela baza podataka:**

- **Hijerarhijski** – veze su ugrađene u strukturu podataka. Ne postoji granica između fizičke i logičke strukture podataka. Nedostaci su složenost i redundandnost podataka.
- **Mrežni** – isto kao i kod hijerarhijskih.
- **Model objekti-veze** – namenjen za specifikovanje statičke strukture baze podataka i osnovnih dinamičkih ograničenja. Koristi se za projektovanje baze podataka. Ovaj model se dalje transformiše direktno u opis baze podataka u nekom sistemu za upravljanje bazama podataka.
- **Relacioni** – jednostavna struktura i jednostavni jezik za korišćenje SQL

Operacije nad relacijama:

1. Unija
 2. Presek
 3. Razlika
 4. Selekcija – (unarna operacija) izdvajaju se n-torke koje zadovoljavaju uslov
 5. Projekcija – (unarna operacija) biraju se kolone zadate relacije čiji se nazivi navode u oznaci operacije i upisuju u novu relaciju
 6. Dekartov proizvod
 7. Kontrolisano ili uslovno spajanje
- **Objektno-relacioni** – može se raditi i nad objektima i nad tabelama.
 - **Objektni** – sve se radi nad objektima. Podržava modelovanje složenih struktura.
 - **Aktivne baze podataka** – proširuju relacioni model sa skupom koncepata za ugrađivanje dinamike sistema u bazu. Ovde se koriste triggeri.

Trigger – pravilo "događaj – uslov – akcija".

- **Normalne forme:**

1. Prva normalna forma – relacija je u ovoj formi ako su atributi nedeljivi i funkcionalno nezavisni od ključa.

2. Druga normalna forma – relacija je u ovoj formi ako je u prvoj normalnoj formi i ako svi njegovi atributi (koji nisu ključevi) potpuno funkcionalno zavise od ključa.

3. Treća normalna forma – relacija je u ovoj formi ako je u drugoj normalnoj formi i ako su svi njeni atributi (koji nisu ključevi) funkcionalno nezavisni.

Normalizacija baza podataka rešava:

- Problem redundantnosti i integriteta
- Moguće neusklađenosti u izrazima
- Smanjuje kompleksnost obrade
- Pojednostavljuje održavanje
- Smanjuje veličinu potrebnog memorijskog prostora

8.1.1 Nivoi apstrakcije

- **Apstrakcija** – kontrolisano i postepeno uključivanje detalja u opis sistema, “sakrivanje” detalja u opisu sistema, odnosno izvlačenje i prikazivanje opštih, a odlaganje opisivanja detaljnih osobina. Postoje:

- **Tipizacija** (klasifikacija) – objekti koji imaju isti skup osobina i isto dinamičko ponašanje mogu se predstaviti jednim tipom ili klasom podataka.

- **Generalizacija** – skup sličnih tipova objekata predstavlja se opštim generičkim tipom, odnosno nadtipom.

- **Agregacija** – apstrakcija u kojoj se skup podataka tretira kao novi, jedinstveni, agregirani tip.

8.2 Sistemi za upravljanje bazama podataka DBMS

- **DBMS (Sistem za upravljanje bazom podataka)** – softverski sistemi koji obezbeđuju osnovne funkcije obrade velikih količina podataka. To je softverski sistem projektovan za jednostavno i efikasno memorisanje i upravljanje bazama podataka.

- Namena DBMSa:

1. Skladištenje podataka sa minimumom redundanse,
2. Pouzadnost podataka pri nekim otkazima,
3. Pouzdano paralelno korišćenje podataka od strane ovlašćenih lica,
4. Logičku i fizičku nezavisnost podataka,
5. Jednostavno komuniciranje sa bazom putem upita.

- **Sistem baze podataka = baza podataka + DBMS**

- **Prednosti rada sa bazom podataka:**

1. Integrisanost podataka – centralizovana kontrola svih podataka i upravljanje podacima na sistematizovan način,
2. Nezavisnost podataka od programa koji ih obrađuju,
3. Razdvajanje fizičkog zapisa i logičke organizacije podataka.

- **Pouzdanost podataka** – ostvaruje se očuvanjem integriteta podataka i kontrolom pristupa podacima.

- **Integritet podataka** – tačnost ili korektnost podataka.

8.3 Osnove SQL jezika

• **Jezici:**

1. **DDL** – Data Description Language – jezik za opis podataka koji je neproceduralan i njime se definišu: slogovi, atributi, logičke veze, domen.
2. **DMCL** – Device Media Control Language – ovim jezikom se opisuje kako se podaci nanose na medijume za memorisanje.
3. **DML** – Data Manipulation Language – jezik za rad sa podacima.
4. **QL** – Query Language – jezik za realizaciju upita nad relacijama u relacionim bazama.
- **SQL** – Structured Query Language – najpoznatiji relacioni jezik upita.

SQL jezik – je upitni jezik koji se koristi za postavljanje upita, modifikaciju podataka i upravljanje relacionim bazama podatak

Osnovne operacije u SQL su:

- **INSERT** – Sintaksa: INSERT INTO; VALUES
- **SELECT** – Sintaksa: SELECT, FROM, WHERE*
- **UPDATE** – Sintaksa: UPDATE, SET, WHERE
- **DELETE** – Sintaksa: DELETE FROM, WHERE

Osnovne funkcije agregacije (koriste se u SELECT upitima:
SUM, AVERAGE, MAX, MIN, COUNT (*))

- Primarni ključ ne može biti nepoznat
- Spoljni ključ može imati null vrednost

9. Računarske mreže

9.1 Uvod u računarske mreže

• **Računarske mreže** – čine dva ili više povezanih računara koji dele resurse kao što su datoteke sa podacima, aplikacije i dr. Računarske mreže su kombinacija hardvera i softvera koja omogućava korisnicima da razmenjuju informacije. (Hardver: fizička veza između dve mašine. Softver (skup protokola): omogućava da aplikacije koriste hardver.)

Protokol – definiše formalni jezik između različitih komponenata.

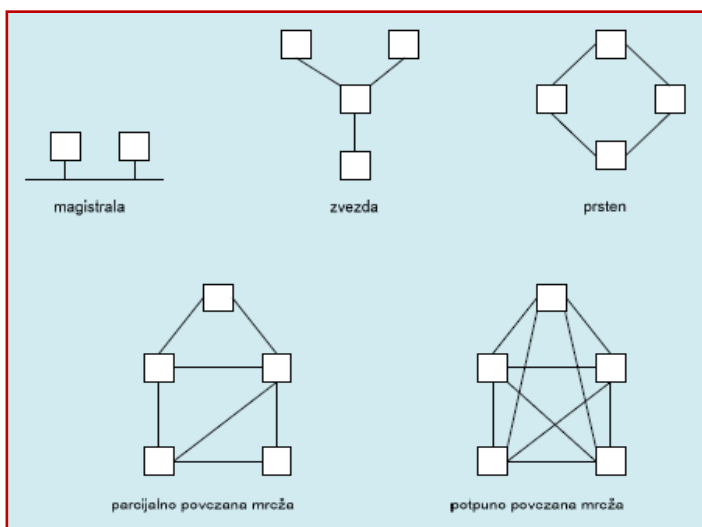
• Postoje dva tipa povezanosti računara:

1. **Potpuna povezanost** – svaki čvor je povezan direktno sa ostalim čvorovima na mreži.
2. **Delimična povezanost** – veze postoje između nekih, ali ne između svih parova u mreži.

• **Topologija** – označava fizički izgled ili oblik računarske mreže. Kriterijumi: osnovna cena, cena komunikacije, pouzdanost.

Vrste topologije:

- Magistrala – tipična za Ethernet mreže
- Zvezda – (npr. šest radnih stanica i 1 server su povezani na hub)
- Prsten – token ring mreža
- Mesh – najrobustniji tip mreže. Samo kod nje prekid kabla ne dovodi do prekida rada bilo kog računara u mreži jer uvek postoje redundantni kablovi.
- Hibridne (kombinovane)



9.2 Osnovni tipovi računarskih mreža

• Tipovi mreža:

- Od tačke do tačke (Point to Point)



- Difuzna mreža (Broadcast Network)



- Komutirana mreža (Switched Network)



- Internet



- Računarske mreže se dele na sledeće kategorije:

- PAN – Private Area Network
- LAN – Local Area Network
- MAN – Metropolitan Area Network, primer kablovska tv
- WAN – Wide Area Network, primer host računari, lan mreže i podmreže

- Protokoli koji se koriste u WAN mrežama X.25, Frame Relay, ISDN (Integrated Services Digital Network), DSL (Digital Subscriber Line), SONET/SDH, ATM (Asynchronous Transport Mode), MPLS (Multiprotocol Label Switching)

• Primeri vrsta bežičnih mreža:

1. **WiFi** – IEEE 802.11 standard (WLAN)
2. **Bluetooth** – IEEE 802.15 standard (WPAN)
3. **WiMAX** – IEEE 802.16 standard

- **Načini rada u mreži:**

- Centralizovana obrada
- Obrada u mreži ravnopravnih računara
- Obrada u klijent-server okruženju
- Obrada u višeslojnom okruženju
- "Peer to peer" model
- Distribuirana obrada

- **Mrežni uređaji:**

- **NIC** - potreban da bi računar mogao da se poveže u računarsku mrežu
- **Bridge**(most) – koristi se za segmentiranje date mreže u više segmenata

9.3 Uređaji u računarskim mrežama

9.3.1 Modemi – uređaj koji se koristi za povezivanje računara sa drugim računarima. On konvertuje digitalne signale u analogne koji se mogu prenositi dalje. Postoje interni i eksterni modemi.

Prema načinu rada modemi se dele na:

a. Analogne

b. Kablovske

c. Xdsl

Razlika između kablovskih i xDSL sa analognima je u tome što kablovski i xDSL konvertuju digitalne podatke u digitalne.

9.3.2 Habovi – mrežni uređaj koji može imati više priključaka na koje se priključuju računari i drugi uređaji. Osnovni zadatak je da prosleđuju signale koji do njih stižu. Takođe, pojačavaju signale, vrše interno rutiranje...

9.3.3 Ruteri – mrežni uređaj ima glavnu ulogu u povezivanju računara na internet. Oni se mogu povezivati na mreže koje koriste različite tehnologije, medijume prenosa itd. Ruteri imaju **centralni procesor, memoriju, više U/I interfejsa za različite mreže. Ruteri mogu da povežu dve LAN mreže, dve WAN mreže, ili LAN i WAN mrežu.**

- Kada ruter primi IP paket, tada on čita adresu odredišta paketa:

- ako je paket za udaljenu mrežu ruter prosleđuje paket do sledećeg rutera na osnovu tabele rutiranja

- ako je paket za lokalni računar ruter ga prosleđuje direktno do odredista

- ako mreža nije unutar tabele rutiranja, ruter prosleđuje paket do "default" rutera koji ima vecu tabelu rutiranja

- svaki ruter ima evidenciju susednih mreža/rutera i lokalnih "host"-ova

9.3.4 Serveri – računar u mreži koji ima zadatak da servisira zahteve klijenta koji se odnose na pristup mrežnim i aplikativnim resursima. Postoje različiti tipovi.

- Kategorije (tipovi) servera:

- serveri datoteka

- aplikacioni serveri

- serveri baza podataka

- web serveri

- serveri e-pošte

- serveri štampača

- faks serveri

- serveri za udaljeni pristup

- „backup“ serveri

9.4 Internet kao sistem virtuelne mreže

- **Internet** – je sistem virtuelne mreže. Prvi put definisan 1982. Pojavom TCP/IP.
- **Internet protokol** se sastoji iz:
 - sistema adresiranja za host računare
 - definicije formata IP paketa
 - pravila koja definišu slanje i prijem paketa
- **Postoje dve verzije IP:**
 - **IPv4** – IP adresa je napisana kao **32bitni** ceo broj napisan kao niz od četiri broja razdvojena tačkom u opsegu [0,255]. To se zove decimalna notacija sa tačkama. Ona se zapisuje u obliku aaa.bbb.ccc.ddd, gde je aaa dekadna vrednost bajta najveće težine, bbb je drugi po redu po težini itd.
 - **IPv6** – je **128bitni** broj napisan kao 16 osmobarbitnih brojeva razdvojenih dvotačkom.
- Svaka IP adresa ima 2 dela. Prefiks i sufiks.
- **Prefiks** identifikuje mrežu i dodaje se globalno a **sufiks** identifikuje ruter i njegovu vrednost dodeljuje lokalni administrator mreže.

- **Klase IP adresa na internetu i opseg vrednosti prvog bajta IP adrese:**

Klasa	Opseg vrednosti
A	Od 0 do 127
B	Od 128 do 191
C	Od 192 do 223
D	Od 224 do 239
E	Od 240 do 255

- **Namena klasa IP adresa:**

A klasa – za države ili velike firme
B klasa – firme srednje velicine
C klasa – manje organizacije i firme

- **Objasnjenje klasa:**

- **A** – sve adrese koje imaju fiksiran prvi deo, npr. 10.bbb.ccc.ddd
- **B** – sve adrese koje imaju fiksirana prva dva dela, npr. 10.200.ccc.ddd
- **C** - sve adrese koje imaju fiksirana prva tri dela, npr. 10.200.1.ddd
- **D** - sve adrese koje imaju fiksirana sva četiri dela, npr. 10.200.1.10

- **CIDR** (Classless Inter-Domain Routing) - Šema IP adresiranja koja zamenjuje adresiranje zasnovano na klasama. To je strategija za dodelu IP adresa na internetu. IP adresa se zapisuje u obliku **a.b.c.d/x** gde je x broj bitova u prvom delu adrese.

Klasa mreže	Broj bita u prefiksu	Maksimalan broj mreža	Broj bita u sufiksu	Maksimalan broj host računara po mreži
A	7	128 ili 2^7	24	16777216 ili 2^{24}
B	14	16384 ili 2^{14}	16	65536 ili 2^{16}
C	21	2097152 ili 2^{21}	8	256 ili 2^8

• **ICANN – Internet Corporation for Assigned Names and Numbers** – Internet korporacija koja upravlja IP adresama.

• **Opsezi adresa koji su namenjeni isključivo za privatno korišćenje:**

- 10.0.0.0 – 10.255.255.255

- 172.16.0.0 – 172.31.255.255

- 192.168.0.0 – 192.168.255.255

• IP adresa **255.255.255.255** je namenjena za difuzno emitovanje, kada računar šalje poruku sa ovom adresom odredišta tada se poruka isporučuje svim računarima u istoj podmreži.

• **Protokoli na internetu** (daju vam skracenice, a vi da napisete puno ime):

- IP (Internet Protocol)- obezbeđuje upravljanje stvarnom isporukom paketa

- TCP (Transmission Control Protocol)- radi sa individualnim paketima

* TCP/IP – Skup protokola. Podaci se grupišu u **pakete** i svaki paket se šalje kroz odgovarajuću putanju.

- ARP (Address Resolution Protocol)

- DHCP (Dynamic Host Configuration Protocol)

- NAT (Network Address Translation)

• **TCP/IP-slojevi (nivoi)= TCP/IP-OSI arhitektura:**

Sloj 5 – Aplikacijski sloj

Sloj 4 – Transportni sloj

Sloj 3 – Mrežni sloj (internet nivo)

Sloj 2 – Sloj veze podataka (mreže pristupa)- Ethernet i PPP

Sloj 1 – Fizički sloj

• Paralelni prikaz TCP/IP i OSI arhitekture

Sloj aplikacije	Sloj aplikacije
	Sloj prezentacije
	Sloj sesije
Transportni sloj	Transportni sloj
Mrežni sloj	Mrežni sloj
Sloj veze podataka	Sloj veze podataka
Fizički sloj	Fizički sloj

• **DNS** - TCP/IP usluga koja pretvara IP adresu u ime hosta

• **ARP** – TCP/IP protokol za prevodjenje logičkih u fizičke adrese

• **TCP** – TCP/IP protokol koji omogućava pouzdanu, end-to-end komunikaciju između hostova

• **IETF – Internet Engineering Task Force** – razvila je četvoroslojni protokol koji se naziva TCP/IP.

- **Upravljanje mrežom** uključuje isporuku, integraciju i koordinaciju hardverskih, softverskih i ljudskih resursa radi nadgledanja, testiranja, konfiguracije, analize i upravljanja mrežom i osnovnim resursima da bi se ostvarili zahtevi rada u realnom vremenu i kvalitet servisa po razumnoj ceni.

- Standardi za upravljanje mrežom:

1. SNMP (Simple Network Management Protocol): deo TCP/IP protokola, Internet koreni, danas: SNMP V3, *de facto* standard za upravljanje mrežama

- **SNMP: 4 ključna dela:**

1. Baza za upravljanje informacijama (MIB):
 - Distribuirano skladište informacija sa podacima o upravljanju mrežom
2. Struktura upravljackih informacija (SMI):
 - Jezik za definisanje podataka za MIB objekte
3. SNMP protokol
 - informacije o objektima kojima se upravlja, komande
4. Zaštita, mogućnosti administriranja
 - glavni dodaci u SNMPv3
 - o Šifrovanje-dešifrovanje SNMP poruke
 - o Autentikacija-izračunavanje, slanje MIC(m,k)
 - o Kontrola pristupa

2. OSI CMIP (Common Management Information Protocol): projektovan 1980-ih, standard za unifikaciju upravljanja mrežama

- **Dva načina za prikupljanje MIB informacija :**

- način rada tipa zahtev/odgovor

- način rada sa prekidima

- Protokoli na **aplikativnom nivu**: TELNET, FTP, HTTP, SHTTP, SMTP/MIME (e-mail), SSH...

- Čemu služi TELNET?

- Telnet i FTP – korisni alati za udaljeni pristup
- Telnet komunikacija se ostvaruje TCP vezama.
- Telnet – omogućava logon na udaljenu mašinu i rad na lokalnim terminalima.
- Telnet – ne omogućava prenos audio ili video podataka (samo ASCII ili EBCDIC podaci).

- Čemu služi FTP (File Transfer Protocol)?

- FTP – omogućava prenos datoteka ("file transfer").
- FTP koristi TCP protokol.

- **FTP sesija** obuhvata pet softverskih elemenata:

- Korisnički interfejs
- Interpreter protokola
- Proces na strani klijenta
- Interpreter protokola na strani servera
- Proces na strani servera za prenos podataka
- put Ispit.txt – FTP komanda za prenos sa lokalnog na udaljeni računar (upload)
- get Ispit.txt – FTP komanda za prenos sa udaljenog na lokalni računar (download)

9.5 Raspoloživost i pouzdanost uređaja i sistema

- **Raspoloživost** je verovatnoća da će komponenta ili sistem biti raspoloživi u toku fiksnog perioda vremena.

Raspoloživost% = (ukupno raspoloživo vreme – Downtime)/ukupno raspoloživo vreme

Downtime – vreme kada sistem ne radi uopšte

- **Pouzdanost** se računa po formuli:

$$R(t) = e^{-bt},$$

gde je $b=1/MTBF$ i

t je vreme trajanja date operacije.

MTBF= mean time before failure

- Standardi iz serije 802:

- 802.3 – odnosi se na Ethernet
- 802.11 – odnosi se na bežičnu tehnologiju
- IEEE 802.11 – odnosi se na bežične Ethernet i WiFi mreže

*Sistemi obeležavanja (prezentacija)

- **Karakteristike sistema obeležavanja:**

- Primenjena metoda
- Izabrana obeležja
- Postupnost
- Nivo detalja

- **Sistem obeležavanja** – standardizacija informacione podrške

• **Nomenklatura ili šifarnik** – daje strukturu i značenje obeležja. Za kodiranje obeležja najčešće se koriste cifre i slova.

- **Obeležja** – za identifikaciju i klasifikaciju.

• **Identifikaciona obeležja**- koriste se za formiranje primarnih ključeva i za identifikaciju odabranih objekata ili pojmova bez obzira na svrhu korišćenja i korisnike. (najčešće su numericka).

- **Dužina obeležja** prema formuli :

$l = \log_a N$; gde je a -osnova sistema obeležavanja a N – broj objekata obeležavanja.

- **Koje su prednosti i nedostaci identifikacionog sistema obelezavanja?**

- Prednost: obeležja nisu dugačka
- Nedostatak: identifikaciona obeležja služe samo za identifikaciju i ne daju pouzdane informacije o objektima obeležavanja

• **Klasifikacija** – raspoređivanje po klasama objekata date vrste na osnovu neke opšte karakteristike koju poseduju.

- **Formalno-logicka pravila klasifikacije:**

- Objekti se mogu istovremeno deliti samo po jednoj osnovi,
- Deljenje na podklase mora da bude proporcionalno i kontinualno i
- Dobijene klase i podklase isključuju jedna drugu.

• **Struktura obeležja** može biti grupa, podgrupa i identifikacioni broj

• Identifikacioni broj – odnosi se na elemente podgrupe.

• Klasifikacioni deo obeležja – može da se koristi kao sekundarni ključ.

• “Govoreće” šifre – mogu biti klasifikacione i informativne

• Informativne – specifični podaci o objektima

• Sistemi paralelnog obeležavanja – sadrže identifikaciona i klasifikaciona obeležja.

- **Prednosti paralelnog sistema obeležavanja su:**
relativno jednostavno šifriranje;
relativno lako održavanje sistema obeležavanja;
dobro iskorišćenje memorijskog prostora;
mogućnost proširenja i trajnost sistema;
mogućnost izgradnje celovitog sistema obeležavanja;
mogućnost jedinstvenog obeležavanja;
- Klasifikacioni deo obeležja – nezavisan i paralelan sa identifikacionim.
- **Struktura obeležja paralelnog sistema obeležavanja:** Identifikacioni broj, klasifikaciono obeležje, informativno obeležje
- Identifikacioni broj – nepromenljiv deo. Klasifikacioni i informativni deo se mogu menjati i proširivati.
- **UPC** (Universal Product Code) – univerzalni kod artikala
UPC-A, 12 cifara. Dve identifikacione šifre (svaka po pet cifara)
Prva šifra – šifra proizvođača
Druga šifra – šifra proizvoda
Dvanaesta cifra je kontrolna
- **EAN sistem** - Evropsko numerisanje artikala (razvijen je iz UPC sistema)
Postoje dve verzije: EAN – 13 i EAN – 8
Standardizovana je struktura šifre:
 - Prve dve cifre – oznacavaju šifru zemlje,
 - Sledećih 5 – identifikovanje proizvođača,
 - Sledećih 5 – identifikovanje proizvoda,
 - Poslednja – kontrolni broj.
- **QR (Quick Response) Codes** je dvodimenzionalni bar-kod koji omogućava brzo dekodiranje sadržaja koda (npr. URL). Mobilni telefon sa kamerom i instaliranim odgovarajućim softverom može da se koristi za skeniranje slike QR koda.

10. Programski jezik JAVA

10.1 Java tehnologija

- **Java** je objektno-orijentisani programski jezik opšte namene pogodan za pisanje konkurentnih, mrežnih i distribuiranih programa. Zasnovan na jeziku C i C++, portabilan je.
- **Karakteristike Java:** jednostavan programski jezik, objektno orijentisan, distribuiran, koristi interpreter, robustan je, siguran, neutralan od arhitekture, ima odlične performance, multithreaded je.
- **Verzije Java:**
 - **JDK** (način imenovanja 1995-2006)
JDK izdanja:
 - J2SE (Java Standard Edition) se koristi za razvoj standalone klijent aplikacija ili applet-a.
 - J2EE (Java Enterprise Edition) se koristi za razvoj serverskih aplikacija kao što su Java servleti i Java ServerPages.
 - J2ME (Java Micro Edition) se koristi za razvoj aplikacija za mobilne uređaje, kao što su mobilni telefoni.
 - **J SE** (promenjen nacin imenovanja 2011-traje još uvek)

Java “bytecode” - “Mašinski jezik” za Java virtuelnu mašinu

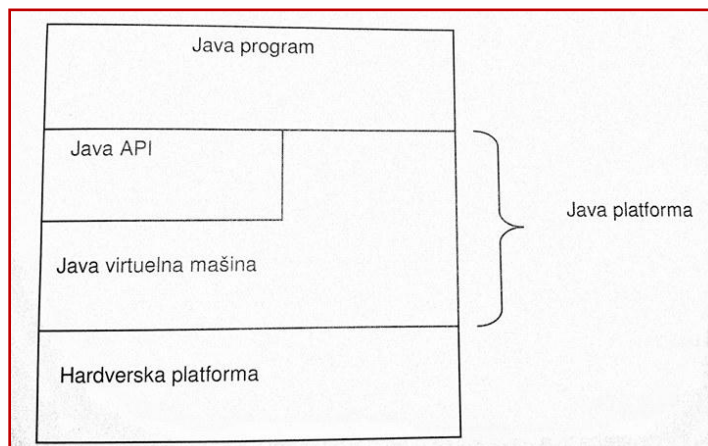
- **Objekat** je osnovni koncept objektno-orijentisane paradigme u modelovanju sistema.
- **Dva osnovna tipa podataka:** primitivni tipovi i objekti.
- Java programi – sastoje se od klasa. Klase sadrže metode za izvršavanje zadataka.
- **Klasa** – predstavlja model objekta koji obuhvata atribute i metode. Objekat je jedan primerak svoje klase.
- **“Source” kod** – zasniva se na klasama. U opštem slučaju jedna “public” klasa se definiše u jednoj datoteci.
- **Operatori koji se koriste za kreiranje java izraza:**
 - Aritmetički (+, -, *, /, ++, --)
 - Relacioni (<, >, <=, >=, ==, !=)
 - Logički (!, &&, ||)
 - Bit operateri (!, &, |)
 - Operatori dodele vrednosti (=)
 - Operatori pomeranja (<<, >>, >>>)
 - Konverzije tipova (npr. long)
- **Karakteristike upravljanja Javom:**
 - Dinamičko upravljanje memorijom (garbage collection)
 - Niti (“threads”)
 - Upravljanje greškama
 - Podrška radu u mreži
 - Zaštita

10.1.2 Java alati

- **Java SDK alati:**
 - **javac** – java prevodilac, čita “source” i generiše “bytecode”
 - **java** – java interpreter, izvršava “bytecode”
 - **jdb** – java “debugger”, pokreće se sa komandne linije
 - **javadoc** - kreiranje dokumentacije iz koda
 - **jar** – Java program za arhiviranje
 - **javakey** – kreiranje digitalnih potpisa
 - **javap** – deasembliranje Java bytecode-a
 - **javah** – kreiranje datoteka zaglavlja
 - **appletviewer** – pokretanje i izvršavanje **applet**-a (Java koda koji se poziva iz HTML datoteke)

10.1.1 Java programski jezik i Java platforme

- **Java platforma:**



- **Tri platforme Java:**

- Java SE (Standard Edition)
- Java EE (Enterprise Edition)
- Java ME (Micro Edition)

• **U Javi se mogu uraditi sledeće aplikacije (tipovi aplikacija):**

- Appleti
- Aplikacije
- "Bean"-ovi
- Servleti
- Midleti (za mobilne uređaje)
- Serverski programi

• **JDBC** (Java Database Connectivity) – omogućen je uniformni pristup širokom opsegu relacionih baza podataka

Višeslojna aplikacija ima :

- Klijentski sloj
- Srednji sloj
- Sloj podataka

• **Program za punjenje** prebacuje Java klase u primarnu memoriju.

• **Verifikator bajtkoda** Java programa potvrđuje validnost koda i potvrđuje da nije narušena zaštita.

• **Interpreter** Java programa čita bajtkod i prevodi ga u jezik koji mašina razume.

• **Pet logičkih operatora:**

1. Logičko "I" (operator &)
2. Uslovno "I" (operator &&)
3. Logičko "ILI" (operator |)
4. Uslovno "ILI" (operator ||)
5. Logička negacija (operator !)

• **Razlika između logičkog "I" i uslovnog "I"** – kod uslovnog "I" operatora (&&) vrednost desnog operanda ne izračunava ako je vrednost levog operanda false, jer je tada vrednost izraza određena i jednaka false.

Logički operator "I" se koristi kada je potrebno da se i vrednost desnog operanda izračuna. Prema tome, kod logičkog operatora "I" vrednost celog izraza se uvek izračunava.

• **Break komanda** – omogućava izlaz iz loop petlje ili bloka komandi u kojima se nalazi.

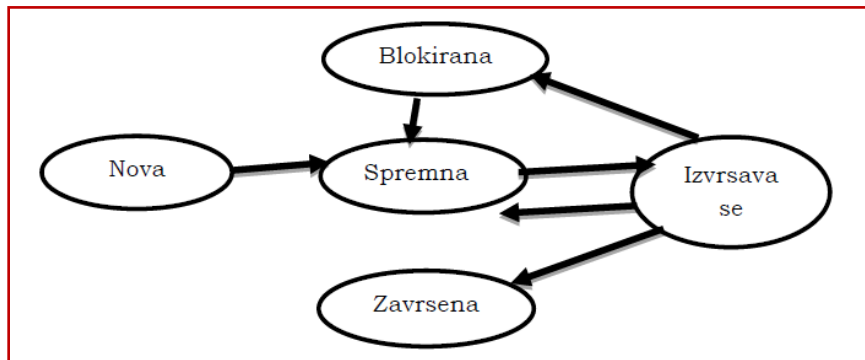
• **Prednosti rada u Javi:**

- Brz početak pisanja programa
- Manja veličina koda
- Brže pisanje programa
- Nezavisnost od platforme
- Pisanje programa jednom, izvršavanje bilo gde
- Lakša distribucija softvera

Polimorfizam – koncept koji omogućava objektima da ispolje različito ponašanje.

• **Nit ("thread")** – sekvencijalni tok kontrole unutar programa. Java podržava rad sa nitima. Element niza u Javi može takođe da sadrži niz.

• **Životni ciklus niti :**



• **Nit je završena kada :**

- run metoda završi sa radom
- kada se pojavi neki neuhvacen izuzetak
- kada neko pozove metod niti stop (koji se u novijim verzijama Jave ne koristi)

Blokirana nit – kada nit sama sebe dovede u fazu čekanja.

• **Ključne reči:**

- public = svako ima pristup (datoj metodi se može pristupiti izvan date klase)
- private = niko izvan date klase nema pristup
- protected = podklase imaju pristup

• **Tipovi podataka u Javi i njihove veličine u bajtovima:**

- byte = 1
- short = 2
- int = 4
- long = 8
- char = 2
- float = 4
- double = 8

11. Komunikacioni sistemi

11.1 Podaci i signali

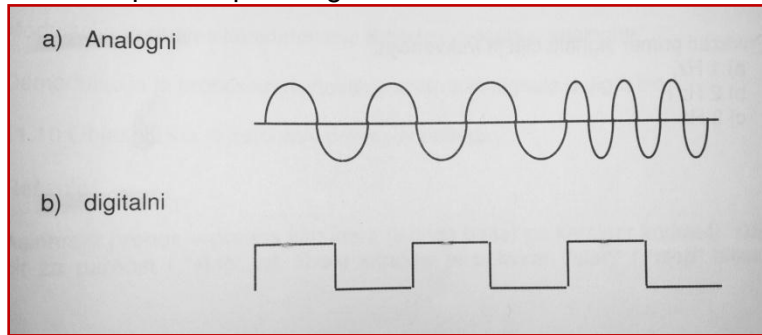
- **Podaci** – su entiteti koji prenose neko značenje. Digitalni podaci se prenose brže, jeftinije i sa manje grešaka.
- **Signali** – električne ili elektromagnetne reprezentacije podataka.
- **Telekomunikacije** – centralna komponenta većine današnjih informacionih sistema

- Podaci i signali mogu biti analogni i digitalni.

Analogni signali – kontinualni talasi tokom vremena. Pozitivan napon je binarno 1 a negativan napon je binarno 0. Kod ovih signala je potrebno da svi detalji signala budu tačno reprodukovani.

Digitalni signal – diskretne vrednosti električnih impulsa sa mogućim vrednostima 1 i 0. Kod ovih signala potrebno je da samo diskretni nivoi signala budu reprodukovani.

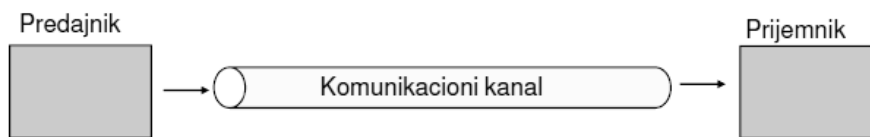
- Grafički prikaz tipova signala kod telekomunikacionih sistema:



- **Tri komponente signala:**

- **Amplituda** – mera jačine signala odnosno rastojanje od horizontalne linije do vrha talasa.
- **Frekvencija** – mera učestalosti signala, tj. Fizička veličina koja se meri u Hz.
- **Faza** – predstavlja poziciju signala relativno u odnosu na dati vremenski trenutak ili u odnosu na nulu. Vrednost može biti bilo koji broj od 0 do 360.

- Apstraktni prikaz prenosa podataka kod telekomunikacionih sistema:



- **Komunikacioni kanal** – fizička veza koja se koristi za prenos podataka.

- Internet omogućava višekanalni pristup. **Kanali koji su danas raspoloživi:** Kablovski sistemi, telefonski sistemi, radio mreze, televizijske mreze i bezicne tehnologije (mobilni telefoni, PDA uređaji i sateliti)

- **Shannonova jednačina** - izračunavanje maksimalne brzine prenosa podataka:

$$S(f)=f*\log_2(1+W/N)$$

W – snaga signala

N – snaga šuma

F – frekvencija signala

- Signali se mogu reprodukovati u **vremenskom domenu** i **frekvencijskom domenu**.

- **Period se izračunava:**

$$T= 1/f_1$$

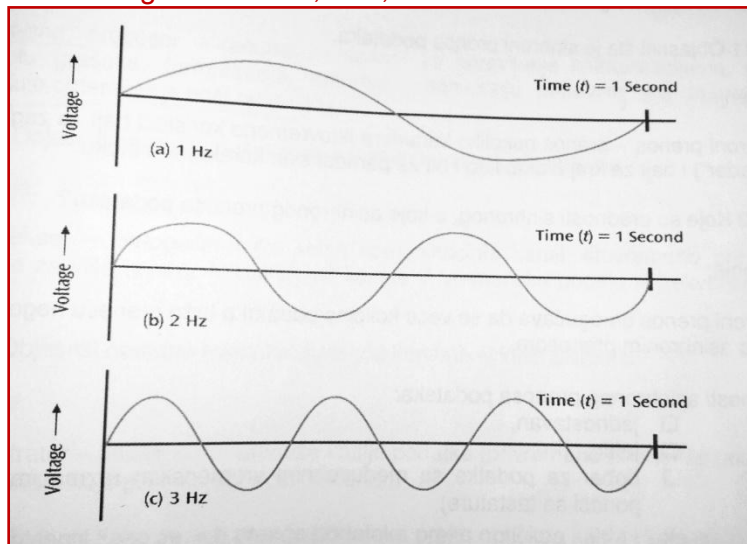
- **Frekvencija se izračunava:**

$$V=1/T$$



- **Spektar signala**– prikaz signala u frekvencijskom domenu.
- **Modulacija** – promena komunikacionog signala nastala promenom njegove amplitude, frekvencije ili faze. Postoje fazna, frekvencijska i amplitudna modulacija. Dakle, proces konvertovanja digitalnih signala u analogne.
- **Demodulacija** – proces konvertovanja analognih signala u digitalne.
- **Komponente telekomunikacionih sistema su:**
 - Računari i ulazno-izlazni uređaji
 - Komunikacioni procesori – modemi, kontoleri, multiplekseri, koncentratori.
 - Front end procesor – računar namenjen za upravljanje komunikacijama, vrši kontrolu grešaka, formatiranje, rutiranje i konverziju podataka i na taj način smanjuje opterećenje host računara.
 - **Telekomunikacioni softver** – upravljanje i podrška uređajima i aktivnostima u mreži. Koristi se za upravljanje mrežom, kontrolu pristupa, upravljanje prenosom, detekciju i korekciju grešaka i zaštitu.
 - **Protokoli**– skup pravila koja se koriste da se omogući komunikacija različitih komunikacionih uređaja.
 - **Najčešće telekomunikacione mreže:**
 - LAN – za povezivanje mikroracunara kako bi delili informacije i uređaje.
 - WAN –regionalna računarska mreža.
 - PBX – privatna centrala, omogućava korisnicima unutar organizacije uzajamno pozivanje bez izlaska na javnu telefonsku mrežu.
 - VAN – mreža sa dodatnim uslugama koje se naplaćuju.
 - Klijent-server procesiranje – serveri datoteka mogu se koristiti za skladištenje aplikativnih programa i podataka.
 - **ISDN** – je međunarodni standard čiji je cilj da zameni današnju telefonsku mrežu, koja zahteva digitalno-analogne konverzije, uređajima koji su namenjeni isključivo uređajima za digitalnu komutaciju i prenos. Mogućnost prenošenja govora, računarskih podataka, muzike, slike.
 - ISDN se zasniva na dva osnovna tipa komunikacionih kanala: B kanal (64 Kb u sekundi) i D kanal za prenos upravljačkih informacija (od 16 do 64 Kb u sekundi).

- Primer signala od 1Hz, 2Hz, 3Hz



11.2 Opšti model komunikacija

- **Protokoli za prenos podataka** – skup pravila kojima se upravlja prenosom podataka između 2 komponente u komunikacionoj mreži. Osnovne funkcije su:
 - Identifikovanje uređaja na komunikacionoj putanji
 - Verifikacija tačnog prijema podataka koji se prenose
 - Utvrđivanje da li je potrebno ponovo slanje usled grešaka
 - Oporavak komunikacije ako su se pojavile greške

11.3 Načini prenosa podataka

- Prema kriterijumu **smera prenosa podataka** razlikujemo sledeće načine prenosa podataka:
 - **Simpleks** – podaci mogu da se prenose samo u jednom smeru u bilo koje vreme. Uređaj može da primi podatke ali ne i da ih šalje. (TV)
 - **Poludupleks** – podaci mogu da se prenose u oba smera ali u datom trenutku samo u jednom smeru. Oba uređaja mogu da šalju i primaju podatke ali u različito vreme. (toki-voki)
 - **Potpuni dupleks** – podaci mogu da se prenose u oba smera istovremeno. Oba uređaja mogu da šalju i primaju podatke istovremeno. (telefon)
- Prema kriterijumu **broja bitova koji se istovremeno prenose** razlikujemo sledeće prenose podataka:
 - **Paralelni** prenos – prema broju bitova koji se istovremeno prenose, ovaj je brži, ali je potreban veći broj linija preko kojih se prenose podaci.
 - **Serijski** – takođe prema broju bitova koji se istovremeno prenose, samo što je ovde dovoljna jedna linija za podatke.
- Prema kriterijumu **sinhronizacije pošaljioca i primaoca** razlikujemo sledeće prenose podataka:
 - **Asinhroni** – prenos karaktera po karakter koristeći start bit, bit za parnost i stop bit. Svaki karakter je uokviren sa start bitom i stop bitom koji označavaju početak i kraj bita. Bit za parnost se koristi za kontrolu grešaka. Niz bitova se segmentira u male grupe od 5-8 bitova. Na početku se javlja start bit i na kraju stop bit. Formiraju se okviri. Između 2 karaktera može biti razmak proizvoljne dužine.

- **Sinhroni** – prenos nekoliko karaktera istovremeno koristeći bajt za zaglavlje i bajt za kraj bloka, kao i bit za parnost svih karaktera u bloku. Niz bitova se segmentira u velike grupe ili blokove. Za svaki blok se dodaju kontrolni bitovi na početku i kraju bloka. Formiraju se okviri. Ne postoji razmak.

• **Koje su prednosti sinhronog, a koje asinhronog prenosa podataka?**

- Sinhroni prenos omogućava da se veće količine podataka brže prenesu nego što bi to bilo asinhronim prenosom.
- Prednosti asinhronog prenosa podataka: jednostavan, jeftin, dodatno 2-3 bita po karakteru (dodatno oko 20%), dobar za podatke sa međusobnim vremenskim razmacima (npr. podaci sa tastature).

11.4 Uređaji u komunikacionim sistemima

• **Repetitor** – uređaj koji se u komunikacionim kanalima koristi za smanjivanje izobličenja pojačavanjem ili regenerisanjem signala tako da signal može da se pošalje dalje sa svojom prvobitnom jačinom i u prvobitnom obliku.

• **Modem** - uređaj koji se koristi za konvertovanje digitalnog u analogni signal kod slanja podataka radi prenosa preko telefonske linije, a zatim za konvertovanje analognog u digitalni signal kod prijema.

• **Multiplexeri** – omogućava da jedan komunikacioni kanal istovremeno prenosi podatke za više izvora. Koriste ili vremensku ili frekvencijsku podjelu.

• **Koncentrator** – uređaj koji memoriše i šalje podatke.

• **Kontroler** – nadgleda komunikacioni saobraćaj između centralnog procesora i drugih uređaja, kao što je štampač, usmerava izlaz ka odgovarajućim uređajima i upravlja tokom ulaznih podataka do centralnog procesora.

• **Bluetooth** – omogućava bežični prenos podataka. Mikročip sa radio predajnikom se ugrađuje u elektronske uređaje i na taj način se prenose podaci bez kablova.

11.5 Medijumi za prenos podataka

- **Uparena žica** – ovde se koriste dva izolovana bakarna provodnika debljine oko 1mm koji su spiralno upredeni. Imaju nisku cenu ali spor prenos podataka. Osnova telefonskog analognog sistema. Brzina prenosa je od 500 bita u sekundi do 10mb. Brzina zavisi od debljine kablova i udaljenosti između predajnika i prijemnika.

- **Koaksijalni kabl** – njega čini izolovana bakarna žica, odnosno dva bakarna provodnika koja nisu postavljena paralelno, već koncentrično. Brzina prenosa je od 56kb do 200mb u sekundi. Koristi se za prenos signala visokih frekvencija.

- **Optički kabl** – ovde se podaci transformišu u svetlosne impulse i svaki svetlosni impuls predstavlja 1 bit. Medijum je debljine vlakna kose. Brzina je od 500kb do 10 GB u sekundi. Teže je raditi sa ovim medijum a i skuplji je. Ovo je najbolja tehnologija za prenos velikih količina podataka na velika rastojanja.

- **Vazduh** – bežični prenos

• **Bežični prenos može imati nekoliko oblika:**

- **Mikrotalasni** - komunikacioni prenos sa korišćenjem radio veze tipa od tačke do tačke na frekvencijama većim od 1 ghz. Ova vrsta prenosa je ograničena linijom vidljivosti. Koristi se u kombinaciji sa satelitima. Brzina prenosa od 256kb do 100mb u sekundi.

- **Satelitski** – slično kao i mikrotalasni prenos, samo su pozicionirani u prostoru. Brzina im je ista.

- **Prenos korišćenjem mobilnih mreža**

- **Prenos korišćenjem bežičnih lokalnih mreža.**

- **Komunikacioni linkovi** – služe za povezivanje računara i krajnjih sistema.
- **Mrežni linkovi:**
 - **linkovi od tačke do tačke** – odnose se na 1 pošaljioca na jednom kraju i 1 primaoca na drugom kraju
 - **difuzni linkovi** – može da ima više pošaljioca i primaoca is vi dele isti difuzni kanal
- **Ruta** – je put kojim se paket prenosi do krajnjeg sistema koji ga je poslao, kroz niz komunikacionih linkova i rutera do krajnjeg sistema kome je namenjen.

11.6 WiMAX mreže

WiMAX mreže – zasnovane na standardu IEEE 802.16. Ova mreža omogućava:

- Širokopolasni pristup internetu (broadband bezicni pristup Internetu)
- VoIP
- Prenos video i audio sadržaja
- Prenos video konferencija.

12. Elektronska trgovina

12.1 Sistemi elektronske trgovine i Internet tehnologije

• **E trgovina** – proces kupovine, prodaje i razmene proizvoda, servisa ili informacija korišćenjem računarskih mreža. Primena e-trgovine smanjuje cenu proizvoda u poređenju sa standardnom trgovinom.

• **Faze u evoluciji e-trgovine:**

- 1.faza- telegraf, telefon, faks
- 2.faza- EDI – elektronska razmena podataka
- 3.faza- Internet, www
- 4.faza- Integracija konvencionalnih i bežičnih mreža
- 5.faza- Integracija i upravljanje kanalima i sadržajem

• **E-trgovina danas:** naručivanje proizvoda i usluga, plaćanje, popunjavanje formulara, servisi i tehnička podrška.

• **Transakcija** – grupa operacija koje se izvršavaju u potpunosti pri čemu se trajni efekat tih operacija trajno i beleži.

• **Bitne karakteristike transakcija u e-trgovini su:**

- Atomnost – izvršavanje u potpunosti ili se uopšte ne izvršava.
- Konzistentnost
- Izolovanost
- Trajnost

• **Vrste transakcija u e-trgovini:**

- Ravne – sastoje se od niza operacija
- Ugnježdene – sastoje se od više podtransakcija
- Distribuirane – nedeljive, tj. ravne transakcije koje pristupaju podacima distribuiranim po različitim čvorovima mreže.

• **Replikacija** je pravljenje kopije podataka.

- **Dva osnovna razloga za korišćenje replikacije:**

- Povećanje pouzdanosti
- Pобољшanje performansi sistema

- **Tri osnovna tipa replikacije:**

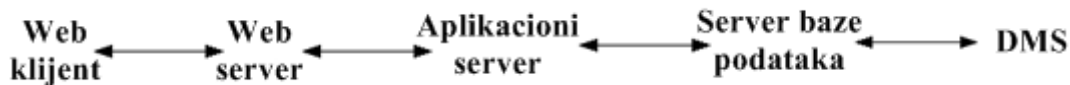
- Permanentne replikacije
- Privremene – kada dođe do naglog povećanja zahteva od strane klijenata
- “keš klijenta” – replika koja se inicira od strane korisnika

- **Autentikacija** – provera autentičnosti korisnika-Lozinke, sertifikati, digitalni potpisi, smart kartice, biometrijske tehnike

- **Integritet podataka** je zaštita od modifikacije od strane neautorizovanih strana.

- **Detektovanje** – je izveštavanje o bilo kom riziku, napadu, lažnoj transakciji.

- **EBPP sistem**- je sistem za online plaćanje mesečnih računa.



Višeslojna arhitektura sistema e-trgovine zasnovane na Web-u

12.2 Osnovne vrste e-trgovine

1. B2C – bussiness to consumer- ovde su učesnici kompanije koje prodaju svoje proizvode i pojedinačni kupci koji elektronski kupuju te proiizvode. Primer je: walmart web site.

2. BCB – bussiness to bussiness – ovde su učesnici kompanije koje svoje proiuvode prodaju drugim kompanijama. Primer je: grainger web site.

3. C2C – consumer to consumer – omogućava e-trgovinu potrošačima, odnosno da fizička lica međusobno trguju preko centralnog Web servera. Primer je: eBay.

4. C2B – consumer to bussiness – ovde korisnici koriste online agente za traženje proizvoda ili usluga. Primer je: priceline.

5. B2G – bussiness to government – učesnici su kompanije koje svoje prooizvode prodaju državnim institucijama i agencijama. Primer : CA.gov

6. P2P – peer to peer – omogućava internet korisnicima da dele fajlove i resurse direktno bez centralnog Web servera. Primer je: paypal

7. M Trgovina – se odnosi na korišćenje bežičnih digitalnih uređaja pomoću kojih se prenose transakcije na webu. Ovde korisnici mogu da rezervišu putovanja, porede cene.. primer: mbill.

12.3 Web tehnologije u sistemima e-trgovine

URL – adresa koja se koristi za pristup datoj WEB stranici.

HTTP – protokol koji se koristi za prenos Web stranice preko Interneta.

HTML – programski jezik koji se koristi za formiranje web stranica. Uvek počinje sa <html> i završava se </html> tagom.

XML – standard za razmenu podataka i informacija na webu fokusiran na struktuiranje sadržaja podataka i informacija.

WEB KLIJENTI – računarski uređaji povezani na internet i koji mogu da šalju HTTP zahteve i da prikazuju HTML stranice.

WEB BROWSER – program koji se koristi za prikazivanje web stranica.

12.4 Internet servisi u sistemima e-trgovine

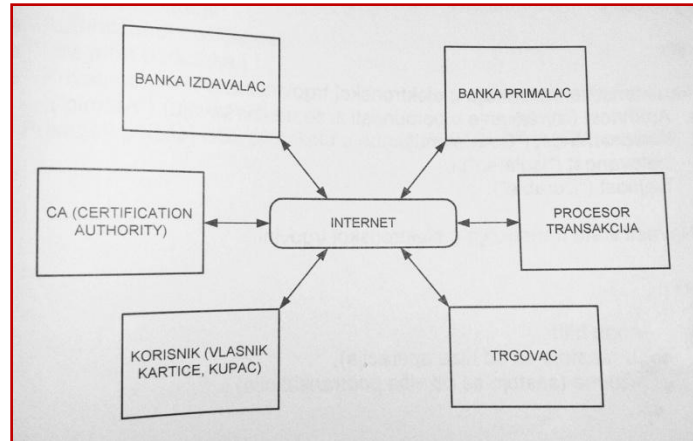
- **BLOG** – personalne web stranice koje tipično sadrže niz hronoloških informacija publikovanih od strane autora.
- **RSS** – really simple syndication – program koji omogućava korisnicima da imaju multimedijalni digitalni sadržaj koji uključuje tekstove, multimedijalne dokumente, bllogove, video i audio prezentacije.
- **ONLINE SOFTVER I SERVISI** – web aplikacije, widgeti, gadgeti, distribucija softvera.
- **WIKI** – web aplikacija koja omogućava korisnicima da lako dodaju ili promene sadržaj na nekoj web strani
- **PODCASTING** – audio prezentacija koja se skladišti kao audio file i koja je raspoloživa preko interneta.
- **APLIKACIJE M-TRGOVINE** – aplikacije koje omogućavaju mobilnim potrošačima da izvrše kupovinu i plaćanje proizvoda i usluga putem telefona.
- **INTERNET TELEFONIJA** – servis koji koristi VoIP za prenos audio komunikacije preko Interneta.
- **IPTV** – internet televizija koja koristi kompresiju podataka primenom standarda kao što su MPEG2 i MPEG4.
- **VIDEO KONFERENCIJE** – zasnovane na internetu koj kojih se koriste širokopojasne internet konekcije i web kamera.
- **SERVISI MUZIKE I VIDEO ZAPISA** – servisi namenjeni za isporuku muzike i video zapisa. Pr. Itunes, dvd.

12.5 Interakcija sa kupcem i aktivan sadržaj

- **CGI** – interfejs za razmenu podataka između WWW servera i WWW klijenta
- **ASP** – script na strani servera koji se koristi za Microsoft-ove Web servere
- **Java JSP i Java Script** – programski jezici koji rasterećuju računar servera, tako što omogućavaju programerima da kreiraju interaktivan i aktivan sadržaj na računaru klijenta
- **Active X i VBScript** – Microsoft-ovi programski jezici koji su konkurentni Javi i Java Script-u
- **Cold Fusion**

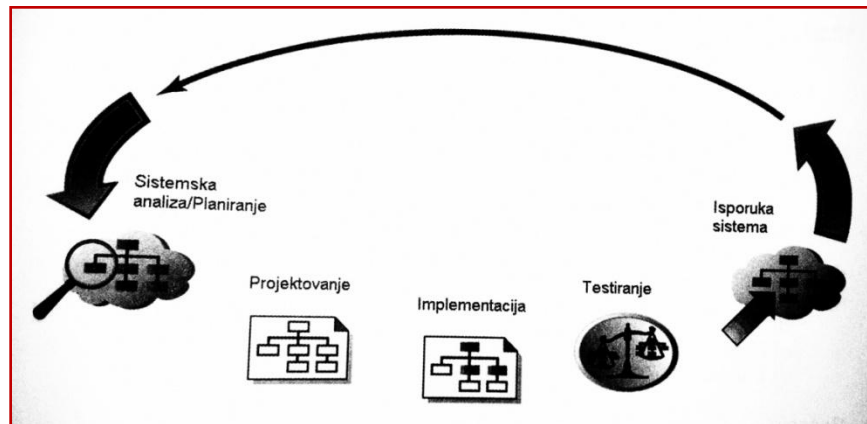
12.6 Elektronski sistemi plaćanja

- **Prema iznosu pojedinačne transakcije** dele se na:
 - sisteme za mikroplaćanja
 - sisteme za makroplaćanja.
- **Prema načinu poravnanja** dele se na:
 - bilateralne, poravnanje je uzajamno
 - multilateralne, postoji poravnanje između svaka dva učesnika
 - sistemi sa posrednikom, vrsta usluge koju posrednik naplaćuje.



Arhitektura elektronskih sistema za plaćanje preko Interneta

- **SET protokol** – je protokol za obavljanje transakcija kreditnim ili debitnim karticama preko Interneta. Vršiti proveru identiteta kupaca, trgovaca i banaka.
- **SSL protokol obezbeđuje:** autentičnost pošiljaoca, integritet podataka, privatnost pošiljaoca.
- **Mogućnosti za kreiranje i održavanje web site-a uz inhouse i outsource:**
 - Kompletno inhouse
 - Kompletno outsourced
 - Kreiranje in house, održavanje outsourced
 - Kreiranje outsourced, održavanje in house
- **WWW-** je skup povezanih resursa koje čine dokumenti, video zapisi, zvučni zapisi koji se nalaze na računarima kojima se može pristupiti preko interneta.

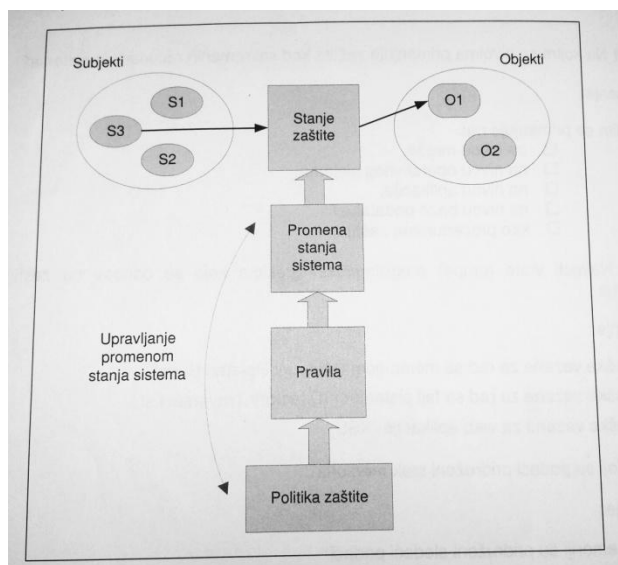


Osnovne aktivnosti u toku životnog ciklusa razvoja Web site-ova

13. Zaštita podataka

13.1 Problem zaštite

- **Zaštita** je skup metoda, tehnika i pravnih normi kojima se kontroliše pristup podacima od strane programa i ljudi i štiti fizički integritet celokupnog računarskog sistema, bio on distribuiran ili ne, centralizovan ili decentralizovan.
- Zaštita se sa tehnickog aspekta primenjuje na:
 - na nivou računarske mreže,
 - na nivou operativnog sistema,
 - na nivou aplikacije,
 - na nivou baze podataka i
 - kao proceduralna zaštita.
- Vrste programerskih grešaka koje se odnose na zaštitu sistema:
 1. Greške vezane za rad sa memorijom
 2. Greške vezane za rad sa fajl sistemom
 3. Greške vezane za web aplikacije
- **Ransomware** je vrsta napada kod koje napadač kriptuje podatke na napadnutom računaru i nakon toga zahteva od vlasnika podataka plaćanje određenog iznosa radi dostavljanja ključa za dešifrovanje podataka. Prenosi se preko priloga e-pošte, zaraženih programa, kao i kompromitovanih web sajtova.
- **MAC adresa** ima 6 bajtova (na primer: 00-AA-00)
- Tipovi **spoofing** napada:
 1. *IP address spoofing* (promena izvorne IP adrese podataka IP adresom napadnutog računara)
 2. *ARP spoofing* (ARP je protokol koji se koristi za preslikavanje logičke IP adrese u fizičku MAC adresu.)
 3. *DNS server spoofing* (DNS je sistem koji vezuje imena domena sa IP adresama. Ova vrsta napada se koristi za širenje virusa i računarskih crva.)



Opšti model zaštite računarskih mreža

• **SQL Injection** je tehnika modifikacije (promene) SQL upita najčešće sa eksterne lokacije. Može se izvesti na jednostavan način, npr. iz browser-a.

• Stek memoriji su pridruženi sledeći podaci:

1. Pokazivac steka
2. Povratna adresa
3. Pokazivac okvira

• Modeli za kontrolu pristupa korisnika datog sistema:

- **MAC** (Mandatory Access Control) – primenjuje se hijerarhijski model za kontrolu pristupa resursima. Korisnici ne mogu da menjaju kontrolu pristupa resursima. Kontrolu obavlja sistem administrator.

- **DAC** (Discretionary Access Control) – model koji dozvoljava svakom korisniku da direktno kontroliše pristup sopstvenim resursima.

- **RBAC** (Role Based Access Control) – model koji omogućava kontrolu pristupa resursima datog sistema na osnovu poslovne uloge korisnika u datoj organizaciji ili kompaniji.

- **RBAC** (Rule Based Access Control) – model koji omogućava kontrolu pristupa na osnovu skupa pravila koje definiše sistem administrator.

• Klasifikacija **neovlašćenog pristupa** prema načinu dejstva:

- Pasivni – osmatranje protoka informacija u nekoj tacki sistema (bez izmene podataka), oni se ne mogu detektovati ali se mogu sprečiti.

- Aktivni – dejstvo ili interakcija sa sistemom od strane infiltratora (promena paketa, brisanje paketa, unošenje kašnjenja, dupliranje, zagušenje, ...), oni se ne mogu sprečiti ali se mogu detektovati.

• Primeri napada ”**spolja**“:

- Pasivno prisluškivanje
- Aktivno prisluškivanje
- Lažno predstavljanje
- Zaobilaženje mehanizama kontrole pristupa
- Ometajuća emitovanja

• Primeri napada s ”**iznutra**“:

- Kada se poznati korisnici sistema ponašaju na neplaniran ili neovlašćen način
- Narušavanje sistema sigurnosti iznutra
- Direktna zavisnost rešenja zaštite podataka od stepena osetljivosti podataka i raspoloživosti finansijskih sredstava.

13.2 Vrste napada na operative sisteme

13.2.1 Virusi

Virus – program koji se može sam reprodukovati tako što dodaje sopstveni kod nekom drugom programu. Rezultat može biti ispisivanje neke poruke, prikaz slike na ekranu, menjanje i brisanje neke datoteke...

Polimorfni virusi – virusi koji mutiraju.

• Skoro svi virusi su manji od **4 KB**.

“Memory resident” virusi – su virusi koji ostaju u operativnoj memoriji i nakon završetka rada programa u okviru koga su bili dodatak.

Parazitni virusi – virusi koji postaju dodatak nekom izvršnom programu.

“Boot sector” virusi – virusi koji su memorisani unutar “master boot” sektora. Boot sektor je mali deo memorijskog prostora na hard disku ili drugom eksternom memorijskom uređaju koji BIOS prvo učitava u RAM memoriju nakon uključanja napajanja računara.

Antivirusni softver– program za zaštitu od virusa.

Retrovirusi – su programi koji su namenjeni blokiranju antivirusnih programa. Često se nazivaju i anti-antivirusi, oni mogu blokirati rad antivirusnih programa čime se sistem otvara za nove, manje opasne viruse.

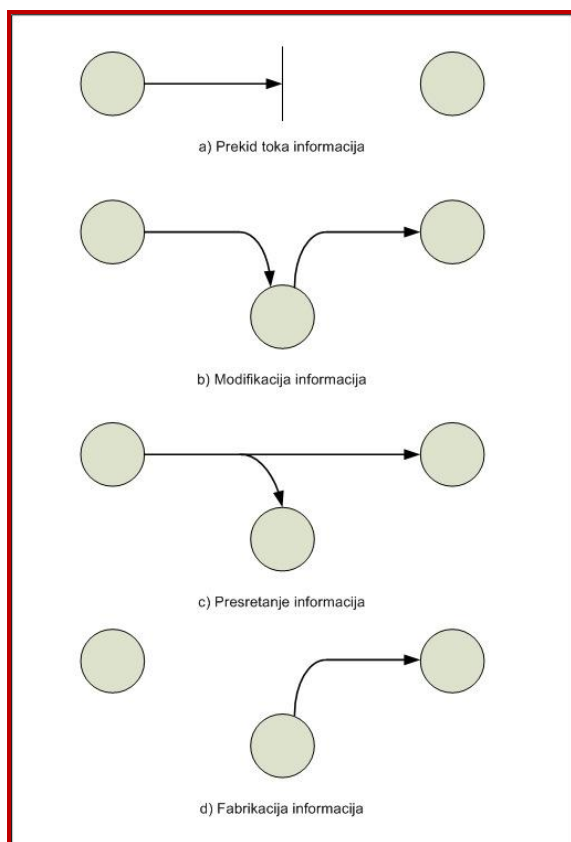
13.2.2 Crvi

Crvi– računarski program koji kopira samog sebe sa jednog računara na drugi. Mogu se koristiti za prenošenje virusa ili za zamenu postojećih datoteka verzijama datoteka koje predstavljaju Trojanske konje. Crvi su slični virusima ali postoji razlika a to je da za aktiviranje crva nije potreban korisnik i oni skrivaju svoje širenje na druge računare.

13.2.3 Trojanski konji

Trojanski konj – program koji se najčešće prenosi na ciljni računar kao nevidljivi dodatak uz neki drugi program, a zatim dolazi do njegovog aktiviranja. Mogu se preneti kopiranjem

programa, “download”-ovanjem sa Interneta i otvaranjem “attachment”-a iz maila. Oni su najopasniji jer se izvršavaju u okviru kernela iliti jezgra operativnog sistema.



13.3 Napadi u distribuiranim sistemima

• Osnovne vrste napada koje postoje na Internetu:

1. Prekid
2. Modifikacija
3. Presretanje
4. Fabrikacija

13.4 Mehanizmi zaštite

Mehanizmi zaštite kod distribuiranih sistema su:

- Fizička zaštita
- Sistem lozniki
- Uvođenje prava pristupa

13.5 Principi projektovanja zaštite

Principi projektovanja zaštite:

- Princip zabrane – pristup nekom objektu je zabranjen i to je default stanje
- Princip kompletnosti – svaki pristup mora biti kontrolisan
- Princip najmanje privilegije – po ovom principu svakom subjektu se dodeljuje samo dozvola koja je potrebna za rešavanje konkretnog zadatka
- Princip otvorenosti – svaki korisnik može da zna mehanizme zaštite
- Princip bezbednog kernela – potrebno je izvršiti izolaciju sistemskih servisa koji su bitni za zaštitu sistema od ostatka sistema
- Princip jednostavnosti – sistem zaštite mora biti jednostavan
- Princip višenivoske zaštite – potrebno je primeniti zaštitu na više nivoa kako bi sistem bio sigurniji i otporniji u slučajevima narušavanja zaštite na nekom nivou

13.6 Zaštita u distribuiranim sistemima

- Osnovni principi za zaštitu računarskih mreža:
 - Kontrolisati spoljašnju vidljivost mreže.
 - Kontrolisati pristup svim sistemima u mreži.
 - Kontrolisati prenos podataka preko svih zaštitnih granica.
 - Nadgledati, detektovati i reagovati na sva sumnjiva ponašanja unutar mreže
- Mere zaštite – **hardverske kontrole**
 - Brave
 - Pristupni uređaji
 - Citaci “smart” kartica,
 - Biometrijski senzori: otisak prsta, skener zenice oka, ...
- Mere zaštite – **softverske kontrole**
 - Operativni sistem
 - Zaštita unutar aplikacije
 - Zaštita unutar baze podataka
 - Standardi za razvoj aplikacija
 - Pregled log-ova
- Mere zaštite – **kontrolni sistemi**
 - “Firewall”-ovi
 - Izlazni ruteri
 - Detektori napada i upada (“Intrusion detectors”)
 - Skeneri virusa (antivirusni softver)
 - Analiza log-ova baza podataka, centralizovano prikupljanje log file-ova.
- **NONCE** (u sistemima zaštite) – slučajna vrednost, timestamp ili vrednost brojača koja se dodaje datoj poruci da bi se obezbedila jedinstvenost.
- **Autorizacija** (kod kontrole pristupa) – pravo datog subjekta da pristupi datom objektu.
- **Provera autentičnosti** (kod kontrole pristupa) - verifikacija datog subjekta ili izvora date poruke.

13.6.1 Autentikacija

Autentikacija – je proces utvrđivanja identiteta korisnika. Ona se može uraditi na više načina ali se zasniva na 3 principa:

- Nešto što korisnik zna
- Nešto što korisnik ima
- Nešto što korisnik jeste

13.6.2 Kriptografija

• **Kriptografija**– Posiljalac koristi algoritam za kriptovanje, a primalac inverzni algoritam za dekriptovanje.

• **Osnovne grupe algoritama u kriptografiji:**

1. Kriptografija sa asimetričnim algoritmima ima 2 ključa:

-**Javni** – poruka koju želi da pošalje (velika prednost na Internetu- ne postoji potreba da se ključevi razmene privatno)

-**Tajni** – poruka koju primi

2. Kriptografija sa simetričnim ključem:

Posiljalac i primalac koriste isti ključ

• Najpoznatiji simetrični algoritmi: DES, 3DES algoritam, AES

• Najpoznatiji asimetrični algoritam: RSA algoritam

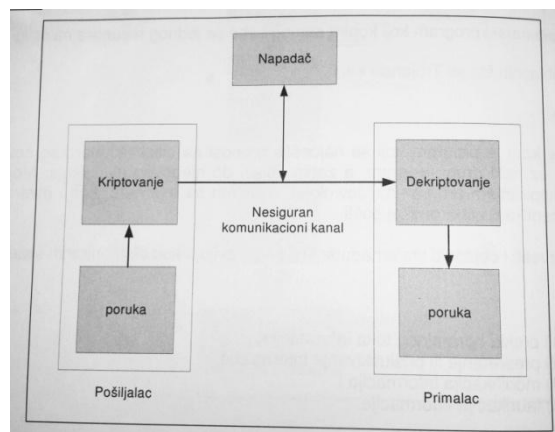
• **Dužine ključeva kod primene AES algoritma:** 128, 192, 256 bitova.

• Mere zaštite – kriptografske kontrole

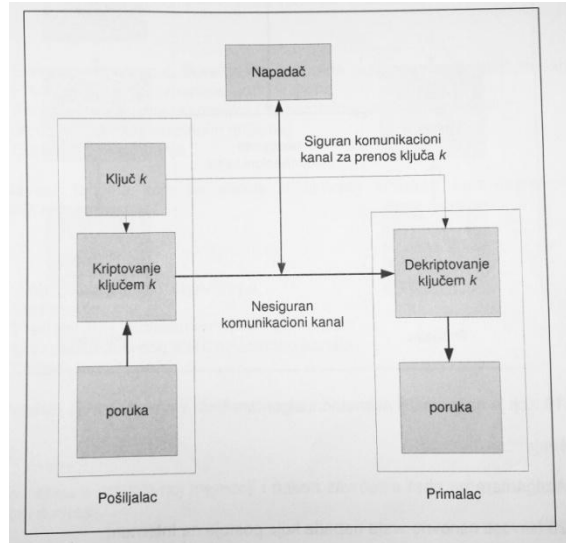
- Šifrovanje podataka je najzastupljeniji mehanizam sprovođenja sigurnosnih servisa računarskih komunikacija.

- Šifrovanje ("encryption") – simetričnim i asimetričnim algoritmima

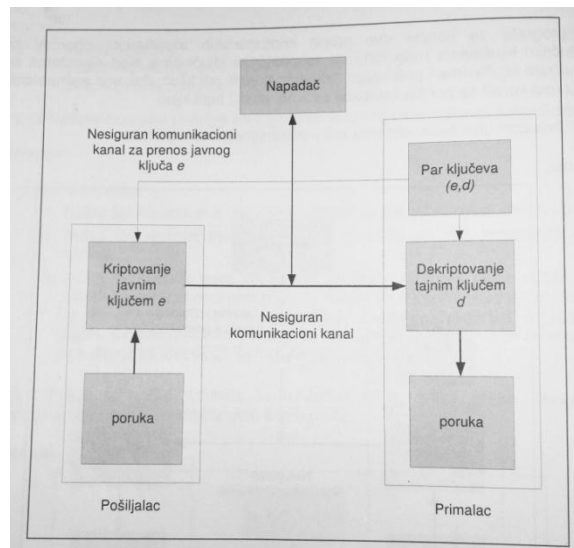
- dešifrovanje ("decryption")



Prikaz komunikacije 2 korisnika preko nesigurnog kanala korišćenjem kriptografije



Blok šema sistema za rad sa simetričnim algoritmima



Blok šema sistema za rad sa asimetričnim algoritmima

13.6.3 Digitalni potpis

• **Digitalni potpis garantuje:**

1. Autentikaciju pošiljaoca
2. Proveru da li je poruka izmenjena u prenosu
3. Nemogućnost negiranja poslate poruke

• **X.509 Sertifikat** - preduslov za rad sa digitalnim potpisom jeste posedovanje ovog sertifikata. Ovo je dokument koji obezbeđuje potvrdu identiteta datog entiteta u sistemima za rad sa javnim ključevima. Dominantna verzija je 3 X.509 sertifikata.

• **Digitalna envelope** – bezbedan elektronski kontejner koji se koristi za zaštitu date poruke ili dokumenta (primenjuje se simetrična enkripcija poruke ili dokumenta i asimetrična enkripcija simetričnog ključa).

Prikazati strukturu adrese resursa na Internetu (URL)?

Service://HostComputer/Path/ResourceName

- Service-Internet protokol koji resurs koristi
- http je servis koji se koristi za pristup Web stranicama (ftp i smtp su takođe primeri servisa)
- HostComputer-IP adresa ili ime domena Web servera sa kojim ste povezani
- Path-Direktorijum relativan u odnosu na Internet "root" na datom Web serveru
- ResourceName-Ime resursa