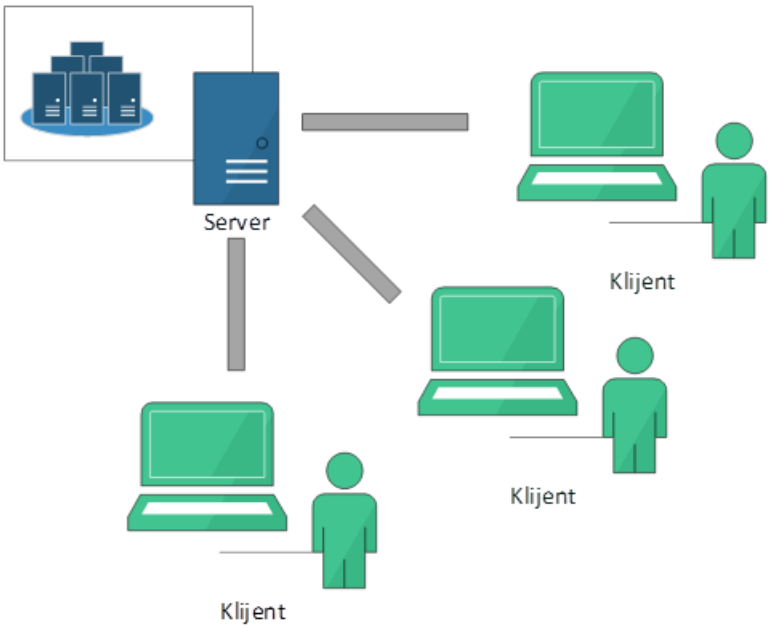
Uvod u računarske mreže

Računarske mreže predstavljaju skup nezavisnih računara i drugih uređaja (štampači, skeneri, eksterni hard diskovi, ruteri itd.) povezanih jedinstvenom tehnologijom koja omogućuje razmenu podataka i deljenje resursa. Uređaji na mreži se često nazivaju čvorovima. Čvorovi mogu biti povezani na različite načine: bakarnim, optičkim i koaksijalnim kablom, bežičnom vezom, radio i mikro talasima, infracrvenim zracima itd.

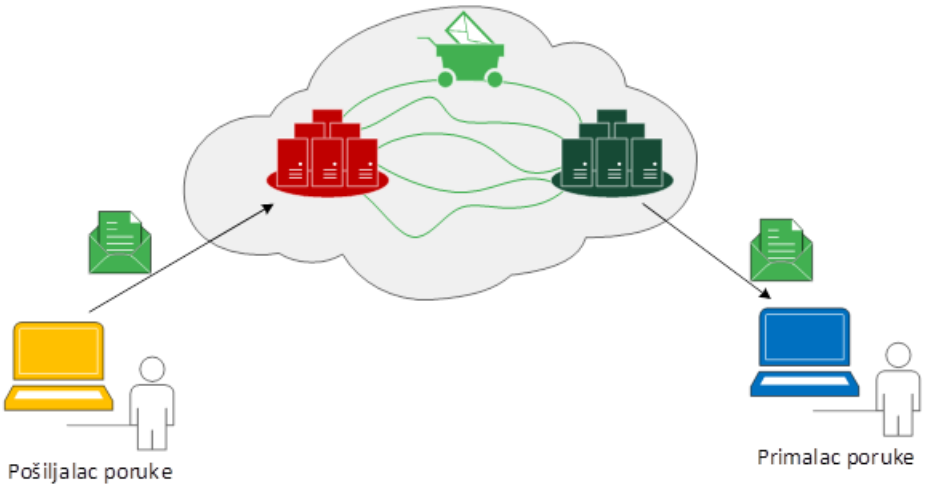
Potreba za masovnim umrežavanjem potekla je prvenstveno od firmi koje su na taj način želele da dele informacije i hardverske resurse. Ideja je bila da se na moćnim računarima, koji su se nazivali serveri, uskladište podaci, a da im korisnici pristupaju sa slabijih, a time i jeftinijih, računara tako što će izdavati zahteve na koje serveri odgovaraju. Ovakva organizacija sistema se naziva klijent-server arhitektura i danas je u širokoj upotrebi (slika 1.). Pored deljenja resursa, firme su imale potrebu i za efikasnom komunikacijom. Računarska mreža omogućava da se na jednostavan način razmeni elektronska pošta i obave telefonski i video razgovori, što značajno smanjuje troškove. Poslednjih godina elektronsko poslovanje doživljava ekspanziju, gde firme preko mreže nude svoje usluge i proizvode korisnicima.



slika 1

Računarske mreže predstavljaju skup nezavisnih računara i drugih uređaja (štampači, skeneri, eksterni hard diskovi, ruteri itd.) povezanih jedinstvenom tehnologijom koja omogućuje razmenu podataka i deljenje resursa. Uređaji na mreži se često nazivaju čvorovima. Čvorovi mogu biti povezani na različite načine: bakarnim, optičkim i koaksijalnim kablom, bežičnom vezom, radio i mikro talasima, infracrvenim zracima itd.

Potreba za masovnim umrežavanjem potekla je prvenstveno od firmi koje su na taj način želele da dele informacije i hardverske resurse. Ideja je bila da se na moćnim računarima, koji su se nazivali serveri, uskladište podaci, a da im korisnici pristupaju sa slabijih, a time i jeftinijih, računara tako što će izdavati zahteve na koje serveri odgovaraju. Ovakva organizacija sistema se naziva klijent-server arhitektura i danas je u širokoj upotrebi (slika 2.). Pored deljenja resursa, firme su imale potrebu i za efikasnom komunikacijom. Računarska mreža omogućava da se na jednostavan način razmeni elektronska pošta i obave telefonski i video razgovori, što značajno smanjuje troškove. Poslednjih godina elektronsko poslovanje doživljava ekspanziju, gde firme preko mreže nude svoje usluge i proizvode korisnicima.



slika 2

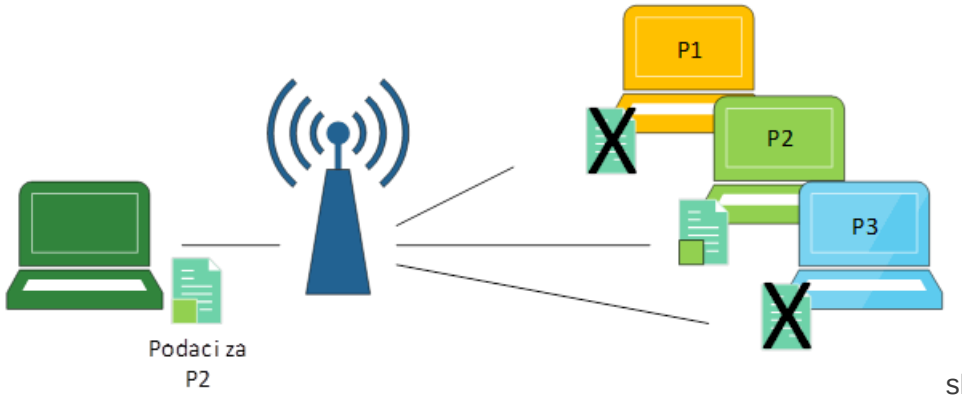
KLASIFIKACIJA MREŽA

Zvanično prihvaćena podela mreža ne postoji. Ipak, sve mreže se mogu podeliti na osnovu više kriterijuma od kojih su najvažnija dva: tehnologije prenosa i veličine.

Klasifikacija na osnovu tehnologije prenosa

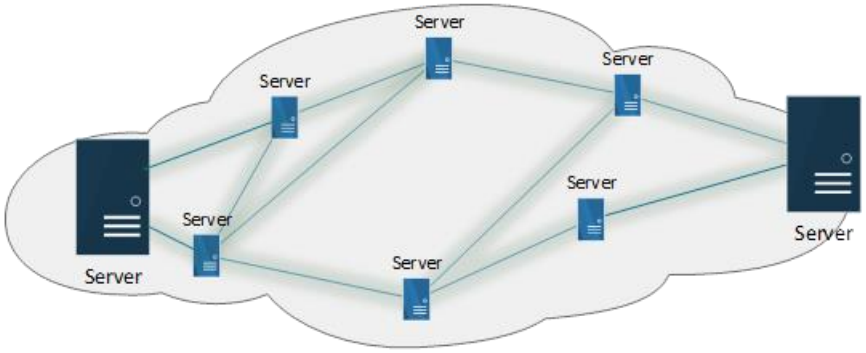
Na osnovu tehnologije prenosa mreže se mogu podeliti na emisione mreže (broadcast networks) i mreže „od tačke do tačke“ (point-to-point networks).

Kod emisionih mreža pretpostavka je da su svi računari koji učestvuju u komunikaciji povezani na jedinstveni komunikacijski kanal. Ovaj kanal služi za razmenu poruka koje može da šalje bilo koji računar, a te poruke primaju svi ostali računari. Svaka poruka ima adresno polje u kome se navodi primalac. Kada poruka stigne do računara, računar najpre proverava adresno polje pa ukoliko je poruka njemu namenjena, pristupa se obradi te poruke, inače se poruka zanemaruje. Bežična mreža je tipičan primer emisione mreže (slika 3.).



slika 3

Mreže od tačke do tačke se zasnivaju na vezama između parova računara (slika 4.). Ukoliko ne postoji direktna veza između računara pošiljaoca i računara primaoca, tokom svog puta poruka prolazi kroz jedan ili više čvorova – tačaka. Obično postoji više različitih mogućnosti za putanju poruke, pa je pronalaženje optimalne jedan od problema matematičke optimizacije.



slika 4

Klasifikacija na osnovu veličine

Na osnovu veličine mreže se dele na: lične, lokalne, gradske i regionalne mreže. Povezivanjem dve ili više mreža dobija se kombinovana mreža (internetwork). Internet je primer najveće kombinovane mreže.

Lična mreža (Personal Area Network – PAN) je računarska mreža koja služi za komunikaciju između računara i drugih uređaja. Neki od uređaja koji se mogu naći u PAN-u su računari, štampači, skeneri, telefoni itd. Domet lične mreže je obično do 10 metara. Na primer, povezivanjem prenosivog računara i mobilnog telefona obrazuje se PAN. Često se to povezivanje ostvaruje bežičnim putem i tada se ova mreža naziva bežični PAN (Wireless PAN – WPAN).

Lokalna mreža (Local Area Network – LAN) je mreža koja povezuje računare i uređaje na ograničenom području poput kuće, škole, zgrade itd. Ova mreža je pogodna za deljenje resursa kao što su dokumenti, štampači, a koristi se i za igre. Mnoge LAN mreže povezuju računare sa radnim stanicama (*workstations*). Radne stanice su posebni računari sa boljim performansama koji obično izvršavaju vremenski i prostorno zahtevne procese. Oni se često koriste za čuvanje velikih količina podataka.

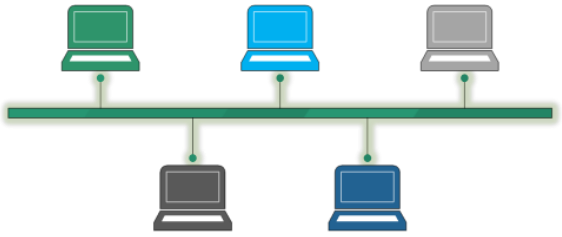
LAN mreže su ograničenih dimenzija što olakšava njihovo projektovanje, povezivanje i obično omogućava veoma brz prenos podataka.

Postoje različite vrste LAN mreža koje se generalno mogu razlikovati po sledećim karakteristikama:

- Topologija – predstavlja prostornu uređenost mreže.
- Protokoli – određuju pravila i specifikacije kodiranja za razmenu podataka. Protokoli još određuju da li mreže koriste arhitekturu „od korisnika do korisnika“ (*peer-to-peer* – P2P) ili klijent-server arhitekturu. Kod P2P arhitekture mrežu čine čvorovi istog ranga (odgovornosti, sposobnosti), što se razlikuje od klijent-server arhitekture gde neki računari obezbeđuju usluge drugim.
- Tehnologija za povezivanje uređaja može biti: bakarni, koaksijalni i optički kabl, ili bežična tehnologija. Ako se koristi bežična tehnologija, tada se radi o bežičnom LAN-u (*Wireless LAN* – WLAN).

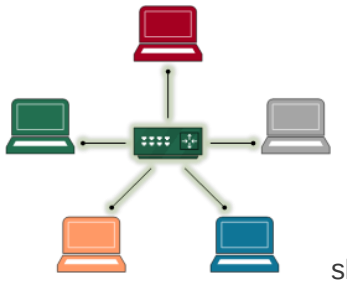
Topologija može biti fizička i logička. Fizička topologija odnosi se na raspored uređaja na mreži i može biti:

- Bus topologija – podrazumeva da su svi uređaji povezani na jedinstveni centralni kabl (Slika 5.). Ova topologija je jeftina, jednostavna za održavanje i često se koristi za male LAN mreže.



slika 5

- Topologija zvezde – svi uređaji su povezani na centralni uređaj (*hub*) koji ima više utičnica (portova). Slika 6. ilustruje mrežu koja odgovara topologiji zvezde. Kada poruka stigne na jednu utičnicu, ona se prosleđuje kroz sve ostale utičnice. Mreža sa topologijom zvezde se relativno jednostavno implementira i održava. Prednost je i to što gubitak jednog računara ne utiče na ostatak mreže. Međutim, otkazivanje centralnog uređaja onesposobljava kompletnu mrežu, a može se javiti problem uskog grla jer sve poruke prolaze kroz centralni uređaj.

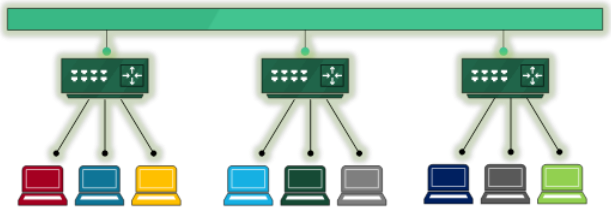


slika 6

- Topologija prstena – svaki uređaj je povezan sa susedna dva uređaja formirajući tako zatvorenu kružnicu (slika 7.). Poruke putuju od čvora do čvora, a svaki čvor čita samo poruke koje su njemu namenjene. Mreže sa ovom topologijom nije jednostavno implementirati, i relativno su skupe za održavanje. Međutim, one imaju veći protok i mogu pokriti veće udaljenosti.

slika 7

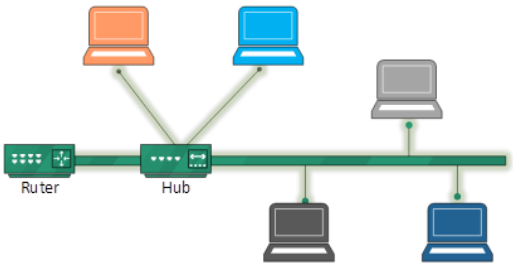
- Topologija drveta – kombinuje karakteristike bus topologije i topologije zvezde. Sastoji se od grupe čvorova organizovanih u topologiji zvezde koji su povezani na centralni kabl (slika 8.).



slika 8

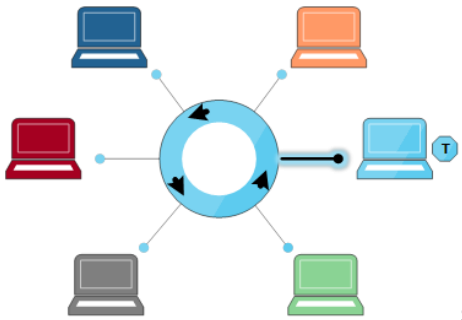
Logička topologija se često naziva i topologija signala. Ovom topologijom se definiše kako će podaci putovati kroz mrežu, ne uzimajući u obzir fizičku povezanost uređaja na mreži. Postoje dve vrste logičke topologije:

- Topologija deljenog medija – podrazumeva da svi čvorovi dele sve fizičke medije unutar mreže (slika 9.). Prednost ove topologije je u tome što čvorovi imaju neograničeni pristup svim medijima. Međutim, problem koji se često javlja je kolizija poruka. Kolizija nastaje kada dva računara u isto vreme pokušaju da emituju poruke. Postoje posebni protokoli koji služe za izbegavanje kolizije.



slika 9

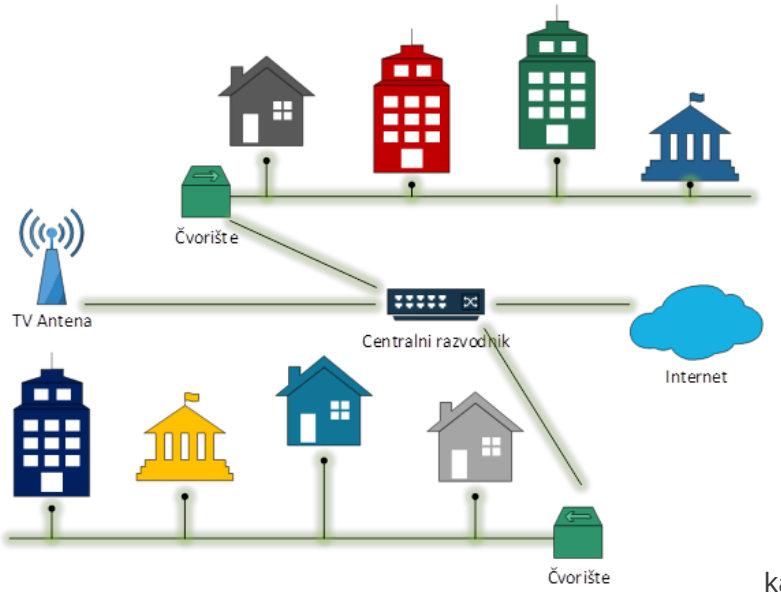
- Topologija žetona (token) – koristi žeton pristupa (ili samo žeton) kojim određuje koji računar ima pravo da emituje poruke (slika 10.). Žeton putuje kroz mrežu, i ukoliko računar želi da emituje poruke, najpre mora da dohvati žeton sa mreže. Zajedno sa porukama računar šalje i žeton odredišnom računaru, koji u odgovoru taj žeton vraća nazad. Nakon emitovanja poruka, računar oslobađa žeton tako da može da ga koristi neki drugi računar. Mreže sa topologijom žetona nemaju problem sa kolizijom poruka, jer na osnovu žetona u jednom trenutku samo jedan računar može da emituje poruke. Problem kod ovih mreža je nastanak kašnjenja, jer svaki računar mora da čeka da dobije žeton. Najčešće se mreže sa topologijom žetona implementiraju kao mreže sa fizičkom topologijom prstena. Tada žeton putuje u krug kroz sve računare.



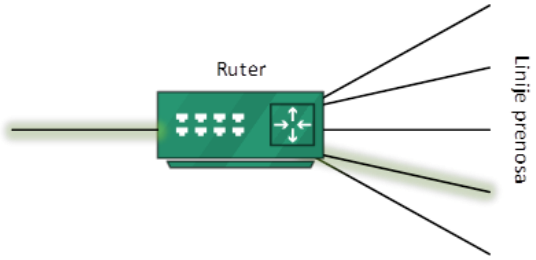
slika 10

Gradska mreža (Metropolitan Area Network – MAN) je velika mreža koja pokriva područje veličine jednog grada ili opštine. MAN obično povezuje više lokalnih mreža pomoću optičkog kabla čime ostvaruje veoma brzu i efikasnu mrežu. MAN mreža takođe obezbeđuje i vezu ka regionalnim mrežama i internetu. Na primer, jedna kompanija može imati kancelarije na više adresa u jednom gradu. Ukoliko je potrebno omogućiti komunikaciju između računara u tim kancelarijama, potrebno je implementirati gradsku mrežu. Još jedan primer gradske mreže je mreža kablovske televizije (slika 11.). Ova mreža postoji u mnogim gradovima i predstavlja sistem kablova koji povezuje korisnike do centralnog razvodnika odakle se emituje televizijski i internet signal.

Regionalna mreža (*Wide Area Network* – WAN) – povezuje velike geografske oblasti kao što su države, regioni ili kontinenti. Primer WAN mreže je sistem rezervacija karata u vazdušnom saobraćaju, gde se terminali mogu naći širom države. Na terminalima se obavlja sama rezervacija, a oni putem WAN mreže pristupaju podacima iz centralnog računara. Regionalna mreža povezuje manje mreže u jednu celinu, a deo mreže koji obavlja to povezivanje naziva se komunikaciona podmreža, ili samo podmreža. Uloga podmreže je da omogući razmenu poruka (podataka) između dva računara koji su povezani udaljenim LAN (ili MAN) mrežama. Podmreža je izgrađena od dva osnovna elementa: prenosnih linija i rutera (mrežnih usmerivača). Prenosne linije služe za prenos bitova između računara i to su najčešće bakarni, koaksijalni i optički kablovi, ali i bežične veze. Ruteri spajaju tri ili više linija prenosa i njihov zadatak je da prispele podatke usmere dalje nekom od prenosnih linija (slika 12.).

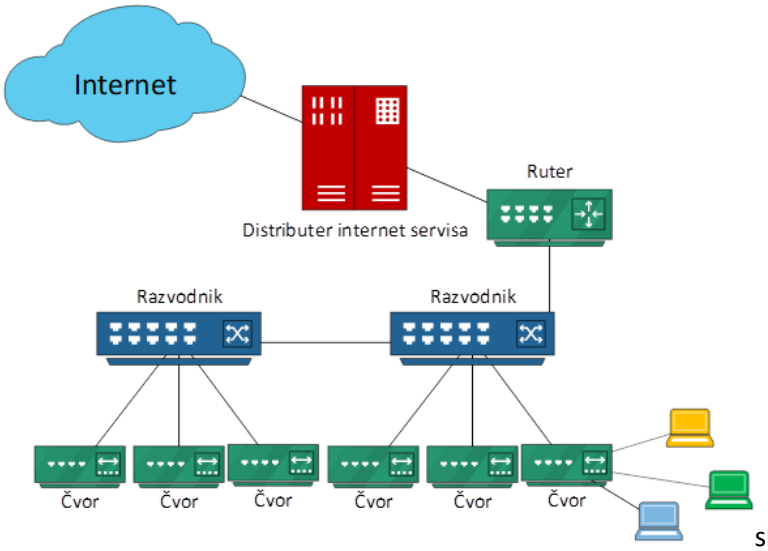


kablovska tv (slika 11)



slika 12

Kombinovana mreža (internetwork ili internet) – predstavlja skup međusobno povezanih jasno razgraničenih mreža. Ova mreža povezuje manje mreže (LAN, MAN, WAN) kreirajući mrežu globalnih razmera. Implementacija kombinovane mreže je veoma kompleksan zadatak zbog velikog broja tehnologija koje se koriste za implementaciju manjih mreža. Ipak, ruteri (*routers*), mostovi (*bridges*) i mrežni prolazi (*gateways*) su uređaji koji to omogućavaju. Mostovi su uređaji koji povezuju dve LAN mreže koje koriste isti protokol (npr. Eternet). Mrežni prolazi su uređaji koji služe da premoste različitosti u mrežnim tehnologijama. U slučaju servera koji sadrži veb stranice, mrežni prolaz je računar koji usmerava saobraćaj sa servera na spoljnu mrežu, čime omogućuje dostupnost tih stranica. Često mrežni prolaz ima ulogu servera posrednika (proxy server). U kućnoj varijanti mrežni prolaz predstavlja dobavljač internet usluga (*Internet Servise Provider* – ISP). Engleski termini *internetwork* i internet su nastali od fraze *interconnected networ*ki odnose se na kombinovanu mrežu u opštem smislu. Sa druge strane, internet je jedan konkretan primer kombinovane mreže (slika 13.).



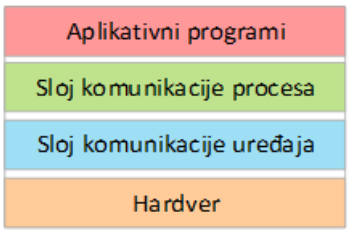
slika 13

ARHITEKTURA MREŽE

Od mreža se zahteva da obezbede brzu, efikasnu i robusnu vezu između velikog broja uređaja. Potrebno je da mreže poseduju određenu fleksibilnost kako bi se obezbedila mogućnost tehnološkog unapređenja i fizičkog proširenja. Takođe, mora se voditi računa o tome da će mreže održavati ljudi različitih nivoa stručnosti.

Dizajniranje mreže, koja zadovoljava sve ove uslove, nije jednostavan zadatak. Jedno od rešenja je apstrakcija mreže u više slojeva u cilju smanjenja kompleksnosti zadatka (slika 14.). Osnovna ideja ovog pristupa je da se usluge koje nudi mrežni hardver organizuju kao jedan (najniži) sloj i da se na njega dalje nadovežu viši slojevi, gde svaki viši sloj predstavlja viši stepen apstrakcije. Najniži sloj se sastoji od funkcionalnosti koje nudi mrežni hardver. Sloj iznad njega koristi te funkcionalnosti i sloju iznad obezbeđuje mogućnost konekcije između dva uređaja. Na osnovu tih mogućnosti sledeći sloj kreira servis koji ostvaruje međuprocesnu komunikaciju. Na samom vrhu nalazi se aplikacija koja se na

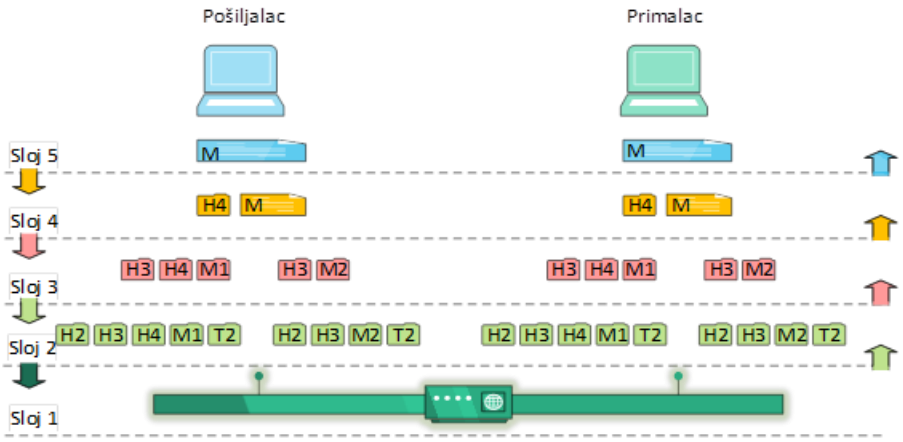
osnovu sloja ispod povezuje sa procesom na udaljenom računaru. Važno je napomenuti da broj slojeva nije fiksiran i zavisi od konkretne implementacije mreže. Takođe, apstrakcija mreže u više slojeva nije jedino moguće rešenje problema implementacije mreže, ali jeste najčešće korišćeno. Neki od razloga česte primene ovog pristupa su modularnost i učaurivanje (enkapsulacija) koji upravo proističu iz apstrakcije mreže u više slojeva. Modularnost omogućuje menjanje (poboljšanje) ili čak zamenu pojedinačnog sloja bez uticaja na ostale slojeve. Ukoliko su potrebne izmene u mreži, jednostavnije je to uraditi na jednom sloju. Enkapsulacija se odnosi na činjenicu da su detalji implementacije sloja skriveni unutar njega, tj. nisu vidljivi izvan sloja.



slika 14

Svaki sloj definiše dva interfejsa. Prvi je servisni interfejs i on obuhvata sve operacije koje taj sloj nudi sloju iznad sebe. Drugi interfejs definiše komunikaciju između dva ista sloja na različitim mašinama i naziva se protokol sloja. Jedan sloj može imati više protokola koji definišu različite načine komunikacije. Arhitekturu mreže čini skup slojeva i protokola. Stek protokola je niz koji se sastoji od po jednog protokola po sloju počevši od najvišeg pa do najnižeg sloja.

Komunikacija između dva procesa (aplikacije) na umreženim računarima počinje tako što prvi proces prosleđuje poruku najvišem nivou mreže (slika 15.). Najviši nivo obrađuje poruku (npr. deli je na manje poruke, kompresuje) i prosleđuje je nivou ispod sebe, koji nastavlja ovaj proces sve do najnižeg nivoa. Najniži nivo je taj koji fizički prenosi poruku do drugog računara. Svaki nivo na dospelu poruku dopisuje zaglavlje koje sadrži potrebne podatke (npr. redni broj poruke, vreme slanja, ime protokola koji se koristi itd.). Kada poruka stigne na određenu destinaciju, ona prolazi kroz sve slojeve mreže, ali u obrnutom redosledu. Svaki sloj čita zaglavlje i koristi informacije koje su u njemu zapisane, nakon čega ga odstranjuje i sloju iznad prosleđuje podatke. Kada poruka stigne do procesa na vrhu, kome je poslata, sva zaglavlja su odstranjena i proces dobija originalnu poruku.

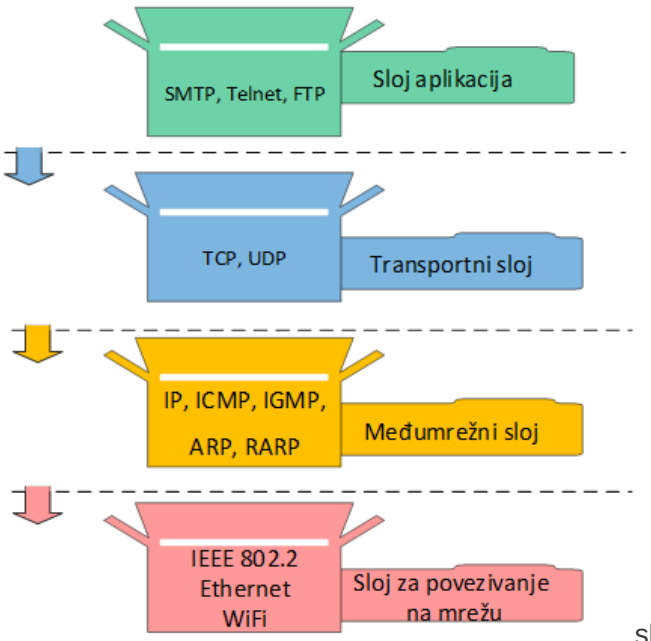


slika 15

REFERENTNI MODEL TCP/IP

TCP/IP je nastajao u više iteracija i istorija njegovog razvoja prepliće se sa istorijom interneta. Zapravo, ovaj model je omogućio nastanak interneta. TCP/IP je dobio ime po svoja dva najvažnija protokola: TCP (Transmission Control Protocol) i IP (Internet Protocol). Osnovni cilj modela bio je da omogući komunikaciju unutar kombinovane mreže (*internetwork* ili *internet*). Svaka mreža ima svoj komunikacioni interfejs. TCP/IP predstavlja apstrakciju komunikacionih mehanizama svih mreža tako što sakriva njihove specifičnosti i obezbeđuje jedinstveni interfejs nezavisan od fizičke mreže.

TCP/IP model se sastoji od 4 sloja (slika 16.): sloj aplikacija, transportni sloj, međumrežni sloj i sloj za povezivanje na mrežu.



slika 16

Kod TCP/IP modela najviši sloj je sloj aplikacija, dok slojevi prezentacije i sesije ne postoje. Same aplikacije su zadužene za predstavljanje podataka i upravljanje sesijama. Sloj aplikacija sadrži razne protokole višeg nivoa, kao što su: HTTP, FTP, TELNET, SMTP, POP3, DNS.

Srž transportnog sloja kod TCP/IP modela su protokoli TCP i UDP. TCP (Transmission Control Protocol) je pouzdan protokol, tj. garantuje prenos podataka bez greške. Podatke dobijene iz sloja aplikacija TCP deli na pakete određene veličine koje prosleđuje međumrežnom sloju. Za svaki paket se očekuje potvrda o pristizanju. Ukoliko potvrda ne stigne u određenom periodu, ponavlja se slanje paketa. Pored toga, TCP podržava kompresiju podataka, kontrolu zagušenja i kontrolu toka. Zbog svojih osobina TCP je najčešće korišćeni protokol transportnog sloja. UDP protokol (User Datagram Protocol) je daleko jednostavniji, ali zato ne garantuje pouzdan prenos. Obično se UDP koristi u situacijama kada brzina prenosa podataka ima prednost u odnosu na tačnost (određenog broja) bitova, kao npr. kod video prenosa.

Međumrežni sloj je zadužen za prenos paketa na željenu destinaciju, pri čemu paketi putuju nezavisno. Zbog toga se može desiti da paketi ne stignu u redosledu kojim su poslati. Viši slojevi su zaduženi za pravilno raspoređivanje pristiglih paketa. Osnovni protokol ovog sloja je IP (*Internet Protocol*) koji je odgovoran za rutiranje paketa. IP je protokol bez uspostavljanja konekcije, nije pouzdan, ne podržava kontrolu toka i oporavak od greške. Ukoliko je to potrebno, ove funkcionalnosti moraju biti pokrivene u višim slojevima. Ostali protokoli ovog sloja su: ICMP, IGMP, ARP, RARP.

Najniži sloj TCP/IP modela je sloj za povezivanje na mrežu. Zapravo, to i nije pravi sloj, već je to skup interfejsa postojećih mreža. TCP/IP model ne definiše nikakav protokol na ovom sloju, ali može koristiti gotovo sve poznate interfejse mreža kao što su: IEEE 802.2, Ethernet, WiFi, Token Ring mreža itd.

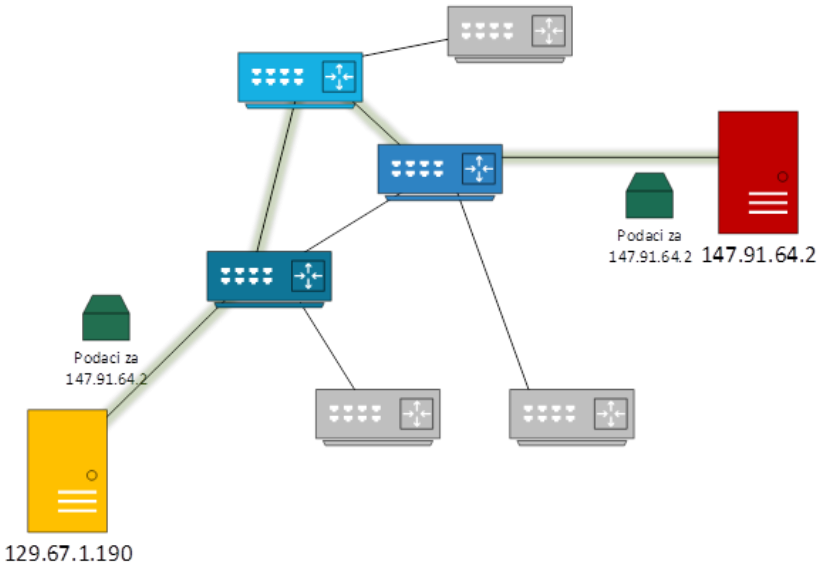
IP adresiranje i rutiranje

Kombinovana mreža (*internetwork* ili *internet*) predstavlja kolekciju međusobno povezanih različitih mreža. IP protokol je zaslužan za sakrivanje osobine fizičke mreže čime kreira prividno jedinstvenu mrežu. Podaci koji se razmenjuju IP protokolom nazivaju se IP datagrami. Datagrami su poruke specifičnog formata i sastoje se od dva osnovna dela – zaglavlja i tela datagrama. Zaglavlje datagrama sadrži podatke kao što su:

- Verzija IP protokola – 4 bita, moguće vrednosti su IPv4 i IPv6;
- Veličina zaglavlja u 32-bitnim rečima – 4 bita;
- Ukupna veličina datagrama u bajtovima – 2 bajta, pa je najveća veličina datagrama 65535 bajtova;
- Protokol transportnog sloja – 1 bajt, a neke od mogućih vrednosti su TCP ili UDP;
- IP adresa pošiljaoca datagrama;
- IP adresa primaoca datagrama itd.

IP adresa služi za identifikovanje (lociranje) svakog računara na mreži. Da bi računar bio dostupan na mreži, mora imati svoju IP adresu. Mašine koje su povezane na više različitih mreža imaju po jednu IP adresu za svaku mrežu. Prema tome, ruteri imaju više IP adresa jer su povezani na više mreža. Da bi ruter mogao da pošalje poruku odgovarajućoj mreži, on mora da zna na osnovu IP adrese (tj. njenog mrežnog dela) kroz koju „žicu“ treba dalje proslediti poruku. Svaki ruter u sebi sadrži tabelu rutiranja (*routing table*) koja mu obezbeđuje ove podatke. Prilikom slanja poruka na veće udaljenosti, one najčešće prolaze kroz veći broj rutera (slika 17.). Tom prilikom svaki ruter određuje dalji put poruke na osnovi njene IP adrese i svoje tabele rutiranja. Proces određivanja putanje poruke od pošiljaoca do primaoca naziva se IP rutiranje.

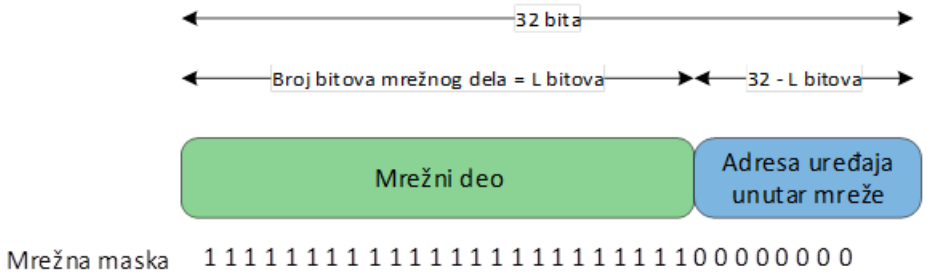
Postoje različite vrste IP adresa od kojih su najznačajnije: IPv4 i IPv6. IPv4 adresa je 32-bitni neoznačen ceo broj. Dužina IPv6 adrese je 6 bajtova, a u nastavku ove sekcije adresiranje i rutiranje će biti predstavljeno sa IPv4 adresama. Zapis IP adrese se sastoji od 4 decimalna cela broja koji su razdvojeni tačkama. Svaki od tih brojeva predstavlja jedan bajt 32-bitne adrese što znači da može imati vrednost od 0 do 255. Primer jedne validne IP adrese je 147.91.66.10. Ovaj zapis se koristi radi lakše čitljivosti, dok računari koriste bitovski zapis. Primer još čitljivijeg zapisa je *myhost.example.com*. Iza svakog ovakvog zapisa nalazi se IP adresa, a DNS (*Domain Name System*) serveri su zaduženi za njihovu međusobnu konverziju.



slika 17-rutiranje

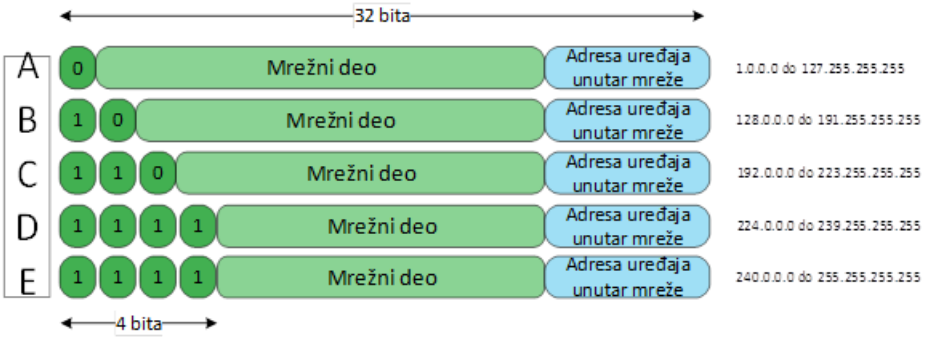
IP (IPv4) adresa se sastoji od dva dela. Prvi je mrežni deo i određuje adresu čitave mreže. Drugi deo se odnosi na adresu uređaja unutar mreže. To znači da sve mašine koje su povezane na jednu mrežu imaju isti mrežni deo. Posebne RIR (*Regional Internet Registries*) organizacije se bave dodeljivanjem mrežne adrese mrežama u različitim delovima sveta. Broj bitova mrežnog dela u IP adresi varira i ne može se dobiti iz same adrese, pa su protokoli rutiranja zaduženi za prenos ove informacije. Često se prilikom zapisa IP adrese ističe veličina mrežnog dela tako što se na zapis adrese nadoveže „/L“, gde je L broj bitova mrežnog dela. Na primer, zapis 147.91.66.10/16 označava da prvih 16 bitova navedene adrese predstavlja njen mrežni deo. Izdvajanje mrežnog dela iz IP adrese omogućuje mrežna

maska (*subnet mask*). To je 32-bitni broj kod koga L viših (prvih) bitova ima vrednost 1, dok ostali bitovi imaju vrednost 0. Kada se izvrši bitovska konjunkcija adrese i mrežne maske dobija se mrežni deo IP adrese (slika 18.).



18 – mrezna maska

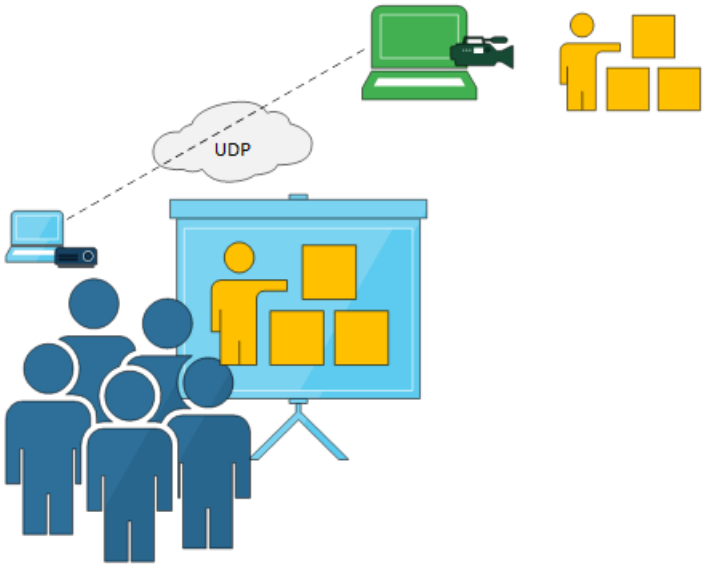
Postoji pet klasa IP adresa i one su prikazane na Slici 9.19. Klase A, B i C mogu imati respektivno 128 mreža sa (oko) 16 miliona uređaja, 16 384 mreža sa 65 536 uređaja, i (oko) 2 miliona mreža sa 256 uređaja. Klasa D je rezervisana za višesmerno slanje datagrama (*multicasting*), dok su adrese iz klase E rezervisane za istraživanja u budućnosti.



19-klase IP adresa

UDP protokol

UDP je protokol transportnog sloja u TCP/IP modelu dizajniran za korišćenje sa IP protokolom. Ovaj protokol omogućava programima da razmenjuju poruke minimalnim mehanizmom, bez uspostavljanja konekcije. To znači da program pošiljalac pre slanja poruka ne proverava da li je program primalac dostupan i spreman za prihvatanje poruka. Zbog toga UDP ne garantuje isporuku poruka, pravilan redosled prilikom pristizanja poruka, a ne poseduje ni zaštitu od dupliranja poruka. Da bi postigao bolje performanse, UDP dozvoljava da pojedine poruke budu odbačene (bez zahteva za ponovnim slanjem) i da poruke mogu pristizati u proizvoljnom redosledu.



slika 20 - primena UDP protokola

UDP poruka se sastoji od zaglavlja i korisničkih podataka. Zaglavlje UDP poruke ima 4 polja od po 2 bajta, i to su:

- Port pošiljaoca;
- Port primaoca;
- Dužina UDP poruke;
- Kontrolna suma (*checksum*).

UDP portovi omogućavaju da različite aplikacije na jednom računaru koriste (istu) mrežu. Svakoj aplikaciji se dodeljuje poseban port – broj na osnovu koga se može identifikovati aplikacija na računaru. Da bi jedna aplikacija poslala poruku drugoj na udaljenom računaru, ona mora tu poruku da pošalje na adresu udaljenog računara sa odgovarajućim portom aplikacije. Portovi su 16-bitni brojevi, pa mogu imati vrednost od 0 do 65535. Vrednosti od 0 do 1023 su rezervisane za privilegovane servise. Na primer, SMTP protokol koristi port 25, HTTP koristi port 80, a POP3 koristi port 110. Dužina UDP poruke odnosi se na broj bajtova zajedno sa zaglavljem, dok se kontrolna suma koristi kao vid zaštite od neželjenih promena u poruci nastalih tokom transporta. Kontrolna suma je rezultat posebnog algoritma koji radi sa 16-bitnim rečima. Ulaz za algoritam se sastoji od bitova kompletne UDP poruke i bitova dela IP zaglavlja. Ako broj bitova nije deljiv sa 16, onda se UDP dopunjuje nulama. Promena bitova tokom transporta izaziva i promenu kontrolne sume na osnovu čega primalac može da odredi da li je primio konzistentne podatke ili ne.

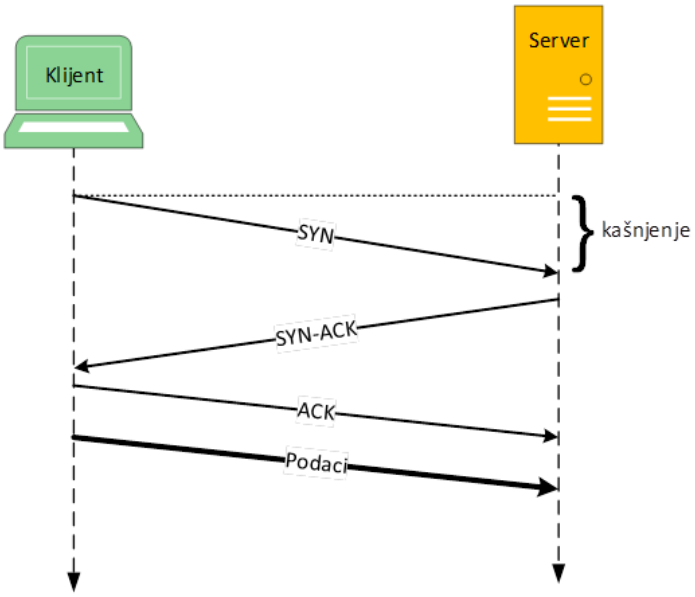
UDP je transakciono orijentisan, tj. pogodan za jednostavne protokole tipa zahtev-odgovor. Primeri takvih protokola su DNS i NTP (*Network Time Protokol*). Zbog svoje jednostavnosti, UDP se koristi kod aplikacija u realnom vremenu gde je brzina bitnija od ispravnosti pristiglih podataka. Neke od njih su aplikacije za video konferencije (slika 20.), video igre, IPTV (*IP Television*) i VoIP (*Voice over IP*) sistemi itd.

TCP protokol

TCP je jedan od najvažnijih protokola transportnog sloja u TCP/IP modelu, koji se koristi u kombinaciji sa IP protokolom. Kao i UDP, TCP koristi portove da bi omogućio korišćenje mreže većem broju aplikacija na jednom računaru. Za razliku od UPD protokola, ovaj protokol pruža aplikacijama više pogodnosti. TCP je pouzdan protokol, što znači da omogućuje uspostavljanje konekcije između procesa i garantuje da će podaci biti preneti bez greške na određenu destinaciju.

Da bi se omogućila pouzdanost, zaglavlje TCP paketa se u odnosu na UDP proširuje dodatnim poljima i kontrolnim bitovima. Kontrolni bitovi sadrže kontrolne signale koji su potrebni za uspostavljanje pouzdane komunikacije. Postoji ukupno 6 kontrolnih signala (i za svaki od njih po jedan bit), a najčešće korišćeni su SYN (*Synchronization*) i ACK (*Acknowledgment*) signali. Signal SYN se koristi za početak komunikacije, dok signal ACK služi da potvrdi da je paket uspešno primljen.

Komunikacija dva procesa počinje uspostavljanjem konekcije. Konekcija se uspostavlja međusobnom razmenom praznih paketa koji sadrže SYN i ACK kontrolne signale. Na primer, neka je potrebno da klijent pošalje podatke serveru (slika 21.). Klijent prvo šalje prazan paket sa postavljenim SYN signalom. Server potvrđuje da je primio paket ACK signalom i šalje SYN signal. Ove signale nije neophodno slati u odvojenim paketima, zato server šalje jedan prazan paket sa postavljenim SYN i ACK signalima. Kada klijent primi ovaj paket, on odgovara praznim paketom sa postavljenim ACK signalom, nakon čega počinje da šalje podatke. Pošto je za uspostavljanje konekcije potrebno razmeniti 3 paketa, ovaj proces se još naziva i trostruko rukovanje (*Three-Way Handshake*).



slika 21- TCP protokol

Podatke pristigle sa aplikativnog sloja TCP deli u pakete određene veličine i svakom pridružuje redni broj. Na osnovu rednih brojeva primalac može da organizuje pakete i regeneriše poruku, ali i da utvrdi da li neki paket nedostaje. Od primaoca se očekuje da pošalje potvrdu (ACK) o poslednjem uspešno primljenom paketu. Tom prilikom primalac šalje i broj bajtova koji u tom trenutku može da primi. Ako potvrda (ACK) ne stigne u određenom vremenskom periodu, paket se ponovo šalje.

Da bi se bolje iskoristio protok mreže, koristi se poseban tzv. mehanizam prozora. Zagušenje se može izbeći ako bi se paketi slali jedan po jedan, pri čemu bi se svaki sledeći paket slao tek po primljenoj potvrdi o uspešnom transferu prethodnog paketa. Ovakav način slanja ne koristi najbolje protok mreže. Mehanizam prozora dozvoljava da se šalje veći broj paketa istovremeno čime se povećava propusnost mreže, odnosno količina podataka koji se mogu preneti mrežom u jedinici vremena. Mehanizam prozora radi na nivou bajtova, ali će radi lakšeg razumevanja biti predstavljen na nivou paketa. Osnovna karakteristika prozora je veličina i ona predstavlja broj paketa koje pošiljalac može da šalje bez čekanja potvrde.

ISTORIJA INTERNETA

Sa razvojem računara pedesetih godina dvadesetog veka javila se potreba za njihovom međusobnom komunikacijom. Krajem pedesetih u Sjedinjenim Američkim Državama osnovana je agencija ARPA (*Advanced Research Projects Agency*) sa primarnim ciljem da razvija informacione tehnologije otporne na nuklearne napade. Godine 1967. predstavnici ARPA-e i stručnjaci iz privatnog sektora sastali su se sa predstavnicima Ministarstva odbrane (*Department of Defense*) Sjedinjenih Američkih Država. Tema sastanka bila je diskusija o protokolima za razmenu podataka između računara. Tako je 1969. godine nastala mreža ARPANET koja je koristila NCP protokol (*Network Control Protocol*).

ARPANET je trebalo da omogući razmenu podataka između vojnih centara, državnih institucija i univerziteta u SAD-u. Ova mreža je na početku povezivala 4 lokacije (Univerzitet Kalifornija u Los Anđelesu, Univerzitet Kalifornija u Santa Barbari, Centar za istraživanja Stenford i Univerzitet Juta), ali se taj broj brzo uvećao. Ubrzo se javljaju i druge manje mreže čiji su tvorci želeli da se povežu sa ARPANET-om. Međutim, istraživanja su pokazala da protokoli ARPANET-a nisu bili pogodni za komunikaciju između različitih mreža pa je ARPA u međuvremenu nastavila istraživanja sa ciljem da napravi pogodnije protokole. Tako je nastao skup protokola TCP/IP (*Transmission Control Protocol – TCP*, *Internet Protocol – IP*).

TCP/IP je nastao 1978. godine. Prva implementacija interneta javila se 1980. kada je ARPA krenula sa menjanjem protokola ARPANET-a na TCP/IP. Uporedo sa tim, u cilju širenja novog protokola, ARPA je potpisala ugovor sa kompanijom BBN (*Bolt, Beranek, Newman*) da implementira TCP/IP protokol za svoj *Berkeley UNIX* operativni sistem (drugi naziv za ovaj operativni sistem je BSD – *Berkeley Software Distribution*). Slični ugovori potpisani su i sa ostalim vodećim kompanijama (kao što su IBM i HP) koje su implementirale TCP/IP na svojim platformama. Prva verzija BSD-a sa TCP/IP protokolom objavljena je 1983. godine. Iste godine ARPA je završila zamenu protokola na svim mašinama u ARPANET-u i objavila da svi uređaji koji žele da se priključe na ARPANET moraju koristiti TCP/IP.

Tokom 1980-tih nove i postojeće mreže (naročito LAN mreže) povezivane su sa ARPANET-om. Da bi se omogućila komunikacija između mašina, dodeljivani su im određeni brojevi koji su predstavljali njihove adrese unutar mreže tzv. IP adrese (videti deo 9.5.1). Sa porastom mreže, pronalaženje konkretne mašine u njoj nije bilo jednostavno zbog velikog broja adresa. Zato se uporedo sa adresama (brojevima) mašine označavaju i nazivima, a napravljen je i DNS sistem (*Domain Name System*) koji je zadužen za konverziju naziva računara u njegovu adresu. Od tada, DNS se razvio u generalizovanu distribuiranu bazu za čuvanje raznih podataka vezanih za nazive mašina.

Povezivanje sa ARPANET-om nije bilo jednostavno. Da bi se neka mreža povezala sa ARPANET-om morala je da ima odobrenje od Ministarstva odbrane SAD-a, a mnoge to nisu imale. Organizacija NFS (*National Science Foundation*) je uvidela koliko je uticaj ARPANET imao na naučna istraživanja pa je odlučila da napravi glavnu (*backbone*) mrežu koja će povezati 6 super-računarskih centara: San Dijego, Boulder, Šampanj, Pitsburg, Itaka i Prinston. Pored svakog super-računara nalazio se jedan manji računar. Ti manju računari su koristili TCP/IP, bili su međusobno povezani i formirali su podmrežu. Pored šest super-računarskih centara, NFS je u tu mrežu uključio i mnoge regionalne mreže. Kompletna mreža, uključujući glavnu i regionalne, nazvana je NSFNET i ona je bila povezana sa ARPANET-om.

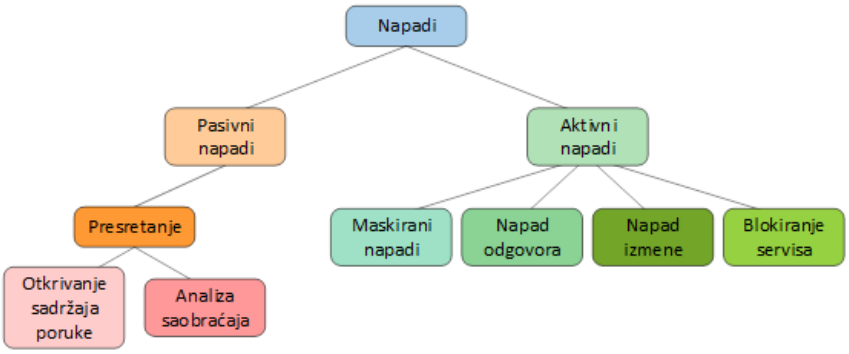
Tokom 1990-tih mnoge druge države i regioni su formirali slične mreže kao što su ARPANET i NSFNET. Neke od njih u Evropi su EuropaNET i EBONE. Povezivanjem tih mreža nastao je internet koji se brzo razvijao od samog početka. Pravu ekspanziju internet je doživeo pojavom veba (*World Wide Web*) ranih devedesetih.

BEZBEDNOST RAČUNARSKIH MREŽA

Kada je koncept računarskih mreža bio relativno nov, bezbednost mreža se nije mnogo razmatrala. Čak se smatralo da bezbednost mreža nije neophodna. Takvo razmišljanje je bilo opravdano jer i da je postojao neko ko bi želeo da zloupotrebi mrežu, nije imao tehnologiju i znanje da to uradi. Danas je situacija drugačija. Postoji mnogo ljudi koji su stekli određen nivo znanja o mrežama a mogli bi da ga zloupotrebe. Skoro svakog dana u medijima se može čuti neka vest o zloupotrebama na internetu, kao što su krađa identiteta ili poverljivih finansijskih podataka. Tačno je da su oni najčešća meta napada, ali nisu samo podaci na mreži ugroženi. Vrlo često se dešavaju napadi „sabotaže“ koji imaju za cilj da onemoguće pojedine servise. Zbog svega navedenog, bezbednost na mrežama je danas primarna tema u tehnološkoj industriji sa ciljem da se smanji, ako ne i potpuno ukloni mogućnost napada na mreži. Da bi se računarske mreže zaštitile od neželjenih napada, neophodno je različite vrste napada razumeti i proučiti.

Teorijska podela napada

Napadi se grubo mogu podeliti na pasivne i aktivne (slika 22.).



slika 22

Kod pasivnih napada napadač presreće poruke i pretražuje ih sa ciljem da sazna nešto više o mreži, učesnicima u komunikaciji ili samoj komunikaciji. Termin „pasivni“ označava da napadač ne vrši nikakvu izmenu podataka. Zbog toga je veoma teško prepoznati ovu vrstu napada. Iako pasivni napadi deluju bezopasno, potencijalna šteta može biti velika, jer se podaci dobijeni iz pasivnih napada koriste za aktivne napade. Postoje dva osnovna tipa pasivnih napada, a to su otkrivanje sadržaja poruka i analiza saobraćaja.

Napad otkrivanja sadržaja poruka (Release of message content) je prilično jednostavan. Elektronska pošta ili neki drugi vidovi komunikacije često sadrže osetljive podatke. Ovi napadi se sastoje od praćenja nezaštićene komunikacije ili dešifrovanja slabo šifrovanih poruka (dobijenih nedovoljno kompleksnim algoritmom šifrovanja) da bi se došlo do poverljivih podataka kao što su podaci za autentifikaciju. Više o autentifikaciji se može videti u delu 9.7.4. Osnovnu zaštitu od ovakvih napada pruža kriptografija.

Kod analize saobraćaja (Traffic analysis) sadržaj poruke nije bitan. Na osnovu frekventnosti poruka napadač pokušava da sazna nešto više o sistemu. Na primer, ako napadač primeti da je razmena poruka sa određenim računarom u mreži učestalija, on može zaključiti da određeni računar ima važnu ulogu u mreži (npr. ulogu servera). Sledeće akcije napadača mogu biti usmerene ka izvršavanju aktivnog napada sa ciljem da se navedeni računar onesposobi.

Osnovna karakteristika aktivnih napada je pokušaj nedozvoljene promene sistema koji se napada. To može biti izmena ili uništavanje podataka koji se prenose kroz mrežu, izmena ili uništavanje podataka koji se čuvaju na određenom računaru, neovlašćeno kreiranje novih podataka, obaranje pojedinih servisa sistema ili čitavog sistema itd. Ovi napadi se lakše prepoznaju zbog izmena na sistemima i štete koju prouzrokuju. Aktivni napadi se mogu podeliti u 4 podvrste:

- Maskirani napadi;
- Napad odgovora;
- Napad izmene;
- Blokiranje servisa.

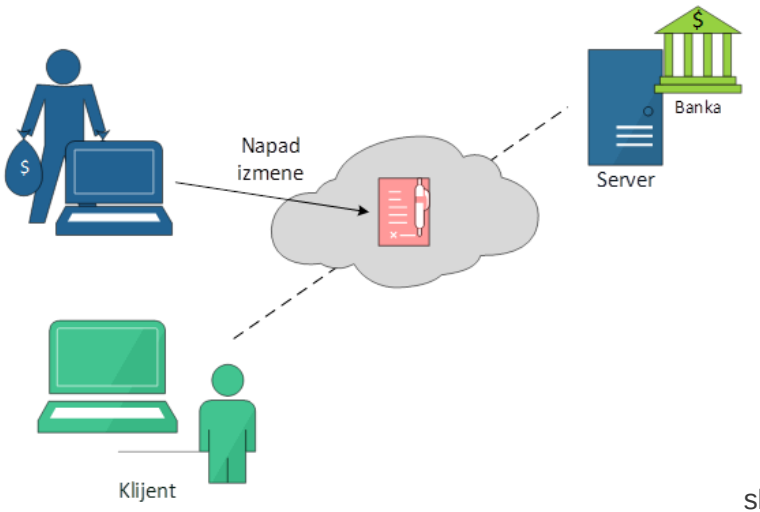
Maskirani napad (Masquerade attack) se odnosi na situaciju u kojoj se napadač predstavlja kao neko drugi sa ciljem da dobije privilegovan status unutar sistema. Maskirani napadi se mogu realizovati na različite načine. Krađa autentifikacionih podataka nekog legalnog korisnika je uobičajeni slučaj. Drugi način je pronalaženje bezbednosnih slabosti ili izbegavanje autentifikacionog postupka nekog sistema.

Napad odgovora (Replay message attack) podrazumeva da napadač poseduje kopije šifrovanih poruka upućenih nekom računaru. Na primer, kopije se mogu dobiti prisluškivanjem i presretanjem komunikacije dva računara na mreži. Napadač kasnije može poslati navedenom računaru presretnute poruke očekujući da će dobiti odgovor. Na taj način napadač pokušava da dođe do zaštićenih podataka.

Napad izmene (Alteration message attack) se dešava kada napadač presretne i izmeni poruku (slika 23.). Na primer, napadač može u zaglavlju izmeniti adresu primaoca da bi je preusmerio. Takođe, može izmeniti sadržaj poruke da bi ostvario ličnu korist.

Blokiranje servisa (Denial-of-Service attack – DoS) služi da onemogući normalno funkcionisanje sistema. Najčešće, meta napada su veb servisi i serveri za elektronsku poštu, ali to mogu biti bilo koji uređaji povezani na mrežu. Ideja ovih napada je da se servis optereti velikim brojem zahteva. To dovodi do usporenja u funkcionisanju servisa, a često i do pada servisa. Najčešći primer DoS napada je preopterećenje mreže beskorisnim podacima od strane napadača. Isto tako, veliki broj (regularnih) zahteva za prijavljivanje može izazvati blokadu servisa.

Popularna vrsta DoS napada u prošlosti bio je tzv. ping smrti (Ping-of-Death – PoD). Ping je posebna funkcionalnost operativnih sistema koja se obično koristi za testiranje ispravnosti računarskih mreža. Ping je program koji šalje pakete na određenu adresu, a kao odgovor očekuje iste te pakete. U zavisnosti od pristiglih paketa, program će ispisati statističke podatke o eventualnim gubicima podataka, vremenu potrebnom za slanje i primanje paketa, i sl. Ping smrti se realizovao slanjem ping zahteva većeg od 65536 bajtova, što je najveći dozvoljen broj bajtova u paketu IP protokola. Zbog toga se vrši fragmentacija podataka u dva paketa. Kada paketi stignu na odredište, oni se spajaju u početnu poruku. Ta količina podataka može da izazove prepunjenost bafera i pad sistema. PoD je bio moguć zbog greške u operativnim sistemima, koja je kasnije ispravljena.



slika 23

Praktični napadi

Realni primeri napada su veoma raznovrsni i nije jednostavno razvrstati ih prema navedenim kategorijama. Neki od njih se mogu rasporediti u više kategorija. Zbog ovoga biće navedeni najznačajniji primeri realnih napada bez njihove stroge klasifikacije.

- Skeniranje portova (Port scanning) je napad koji nije u potpunosti pasivan jer zahteva određene akcije napadača, ali se ne može ni svrstati u aktivne. Ovaj napad je moguće realizovati na sistemima koji koriste TCP ili UDP portove. Skeniranjem portova napadač pokušava da pronađe portove preko kojih bi mogao da izvrši aktivne napade. Napadač ispituje redom sve portove tako što pokušava da uspostavi TCP/IP konekciju na tom portu. Ukoliko se na nekom portu uspostavi konekcija, može se pokušati sa pronalaženjem dodatnih slabosti procesa koji koristi taj port.

- Prepunjenost bafera (Buffer overflow) je napad koji koristi nedostatke programa (bagove) i pokušava da u neki od bafera sačuva količinu podataka veću od njegovog kapaciteta. Baferi služe za čuvanje ograničene količine podataka, pa će se višak podataka upisati u susednu memoriju. To može da zaustavi rad programa, ali i da dovede do složenijih neželjenih posledica ako taj višak podataka sadrži neke instrukcije. Neka je, na primer, napadač generisao (napisao) deo programa, koji je zatim preveo u mašinski kôd. Napadač može pokušati da izvrši taj kôd tako što će ulazni bafer napuniti do kraja regularnim podacima, a zatim na njih nadovezati bajtove mašinskog koda. Ovaj napad se može sprečiti jednostavnom proverom da li je veličina ulaznih podataka manja od kapaciteta bafera.
- Računarski virus je deo programa koji je umetnut u regularni program. Virus se sam umnožava (kopiranjem) i umeće u druge programe na računaru i tom prilikom može se sam menjati (mutirati). Računar se može zaraziti na razne načine: skidanjem zaraženih podataka sa interneta, pomoću poruke elektronske pošte, preko zaraženih USB diskova i drugih medija itd. Virusi ne „inficiraju“ samo programe. Oni se mogu umetnuti i u neke dokumente koji imaju izvršni sadržaj. Takvi su Microsoft Office dokumenti. U određenim delovima oni sadrže makroe koji se izvršavaju automatski prilikom otvaranja dokumenta. Virusi mogu imati razne destruktivne osobine. Oni mogu brisati dokumente na sistemu, zauzimati prostor na disku, memoriji ili procesorsko vreme, mogu snimati sve unose sa namerom da dođu do osetljivih podataka, mogu ispisivati na ekranu poruke raznog sadržaja, ili samo ukazivati na postojanje slabosti u sistemu.
- Trojanski konj, popularno trojanac, je program koji je maskiran tako da izgleda kao regularna aplikacija, ali u sebi sadrži destruktivne instrukcije. Za razliku od virusa, trojanci se ne umnožavaju sami. Trojanci se na internetu često predstavljaju kao koristan softver. Drugi često korišćeni način za širenje trojanaca je elektronska pošta.
- Računarski crvi (computer worm) su mali delovi softvera koji za širenje koriste bezbednosne propuste u mreži. Slično kao i virusi, crvi se umnožavaju tako što sami sebe kopiraju. Za razliku od virusa, koji menjaju programe ili fajlove da bi se širili, crvi su samostalni i ne zahtevaju akciju korisnika za širenje. Crvi mogu da prouzrokuju istu štetu kao i virusi. Ipak, oni najčešće ne oštećuju podatke, već samo zauzimaju memoriju ili opterećuju mrežu smanjujući njen protok. Zauzimanje resursa ima za cilj da se onemogući normalan rad pojedinih računara ili čitavih mreža.
- „Čovek u sredini“ (Man in the middle) je napad u kome napadač prisluškuje komunikaciju između dva korisnika koji u komunikaciji koriste simetrične algoritme šifrovanja. Ovi algoritmi koriste dva ključa – javni ključ koji služi za šifrovanje poruka i tajni ključ koji služi za dešifrovanje poruka. Svaki učesnik u komunikaciji zna samo svoj tajni ključ, dok su javni ključevi svima poznati. Pošiljalac šifruje poruku koristeći javni ključ primaoca i na nju nadovezuje svoj javni ključ. Primalac dešifruje poruku svojim tajnim ključem, a odgovor šifruje javnim ključem pošiljaoca koji je primio zajedno sa porukom. U opštem slučaju, napadač presreće poruku koja sadrži javni ključ pošiljaoca, zamenjuje javni ključ svojim javnim ključem i prosleđuje poruku primaocu. Zatim, napadač presreće odgovor pošiljaoca koji može da dešifruje jer je poruka šifrovana njegovim javnim ključem.

Odbrana od napada na mreži

Tokom proteklih godina sa razvojem napada unutar računarskih mreža razvijala se i odbrana od njih. Postoje različite tehnike i softveri koji sprečavaju napade. Pojedinačno, ove tehnike ne mogu obezbediti potpunu sigurnost sistema. Tek kada se one iskombinuju u nekom sistemu, onda se može pretpostaviti da je taj sistem bezbedan. Na žalost, potpuna bezbednost se ne može garantovati. Proizvođači softverskih i hardverskih alata za odbranu su u stalnom nadmetanju sa kreativnim napadačima.

Antivirus je zaštitni softver koji štiti računare od malicioznog softvera (*malicious software*). Drugi naziv za maliciozni softver je malver (*malware*) i on obuhvata viruse, trojance, crve i slične softvere. Da bi bio efikasan, antivirus je stalno aktivan u sistemu kao pozadinski proces i on sprečava, detektuje i uklanja napade malicioznog softvera. Antivirus koristi različite tehnike prepoznavanja malvera, a najčešće korišćene su detektovanje potpisa i heuristička detekcija.

Detektovanja potpisa je tehnika koja se obično koristi za prepoznavanje virusa. Potpis virusa je heš vrednost njegovog koda. Antivirus koristi heš mapu koja sadrži potpise virusa. Za vreme svog rada, antivirus skenira dokumente u računaru i pokušava da pronađe delove koda. Kada naiđe na kôd, on računa heš vrednost tog koda i upoređuje sa potpisima u heš mapi. Ako se dogodi poklapanje, antivirus može preduzeti različite akcije, kao što su brisanje dokumenta, pokušaj popravke dokumenta ili smeštanje dokumenta u karantin. Pošto se zasniva na bazi poznatih virusa, ovaj metod nije efikasan kod novih virusa. Da bi bili efikasniji, antivirusi preporučuju često ažuriranje heš mape.

Takođe, proizvođači antivirusnog softvera podstiču korisnike da dele (*upload*) nove viruse kako bi se oni proučili i njihovi potpisi dodali u heš mapu.

Heuristička detekcija virusa se zasniva na praćenju svih programa i pokušaju da se prepoznaju sumnjiva ponašanja. Ova tehnika ne koristi heš mapu i zastupljena je kod naprednijih antivirusa da bi prepoznali nove viruse ili varijacije postojećih virusa. Na primer, antivirus registruje pokušaj menjanja izvršnog fajla i o tome obaveštava korisnika koji odlučuje o daljim akcijama. Moderni komercijalni antivirusi kombinuju ove tehnike.

Iako predstavljaju veoma efikasnu zaštitu, antivirusi imaju nekoliko mana. Prva od njih je što ne obezbeđuju potpunu zaštitu od malvera. Napadi novih malvera za koje antivirusi nemaju podatke popularno se nazivaju „napadi od nultog dana“ (*zero-day attacks*). Ovi napadi mogu biti veoma uspešni u periodu od pokretanja novog virusa pa sve do njegovog registrovanja i proučavanja njegovog potpisa. Druga mana antivirusa je ta što oni zauzimaju resurse računara, što može uticati na njegove performanse.

Zaštitni zid (Firewall) je metod ili uređaj koji reguliše nivo poverenja između dve ili više mreža. To može biti softver ili hardver, mada se moderni zaštitni zidovi implementiraju kao posebne mašine koje kombinuju softver sa hardverom. Zaštitni zid štiti lokalnu mrežu od pristupa neautorizovanih korisnika sa interneta, ali može da se koristi za regulisanje saobraćaja između dve mreže iste kompanije. Sve poruke koje pristižu u lokalnu mrežu ili je napuštaju ili prolaze kroz zaštitni zid. One poruke koje ne zadovoljavaju navedeni sigurnosni kriterijum bivaju odbačene. Zaštitni zidovi ne mogu da pruže zaštitu od virusa, ali u određenim okolnostima mogu da spreče viruse da šalju podatke sa zaraženih računara.

Postoje različite vrste zaštitnih zidova:

- Zaštitni zid za filtriranje paketa (Packet filtering firewall) – ovaj zaštitni zid, u zavisnosti od konfiguracije, prihvata ili odbija pakete na osnovu informacija iz zaglavlja paketa. Filtriranje paketa se može obavljati na mrežnom i transportnom sloju i to na osnovu IP adrese pošiljaoca i/ili primaoca, portova pošiljaoca i/ili primaoca, protokola itd. Filtriranje paketa je efektivna metoda zaštite od neautorizovanog pristupa sistemu, ali je veoma zahtevna za konfigurisanje.
- Kružni prolaz (Circular-level gateway) – ova vrsta zaštitnog zida obezbeđuje sigurnost TCP konekcije. Kružni prolaz nadgleda proces uspostavljanja TCP konekcija i proverava validnost tih konekcija na osnovu zadatih pravila. Pravila za definisanje validnih sesija mogu biti vezana za IP adrese primaoca i/ili pošiljaoca, njihove portove, doba dana, protokol, korisničko ime, lozinku itd. Kada ustanovi validnost konekcije, kružni prolaz otvara sesiju i dozvoljava razmenu podataka. Kada se otvori sesija, dalje provere se ne izvršavaju. Podaci koji prolaze kroz kružni prolaz ka internetu deluju kao da potiču od samog kružnog prolaza. Zbog toga udaljeni računar ne može da odredi interne privatne IP adrese računara (npr. neke organizacije). Ova tehnika se naziva prevođenje mrežnih adresa (*Network Address Translation* – NAT) i podrazumeva pridruživanje privatnih IP adresa više uređaja jednoj javnoj IP adresi.
- Aplikacioni prolaz (Application-level gateway) – ovaj zaštitni zid čita sadržaj paketa i na osnovu njega odlučuje da li će ga propustiti ili odbaciti. Aplikacioni prolaz skenira pakete u potrazi za malverom i ukoliko ga nađe, paket se odbacuje. Zbog toga, aplikacioni prolaz pruža najveći stepen bezbednosti. Aplikacioni prolaz se implementira kao „server zastupnik“, tj. proksi server (*proxy server*). To je posebna mašina koja se nalazi između klijentskog i servisnog računara. Kada klijent želi da se poveže sa servisnim računarom, on se zapravo povezuje sa proksi serverom koji zastupa servisni računar. Čitava komunikacija se odvija preko proksi servisa. Servisni računar ostaje zaštićen jer klijent ne može da odredi njegovu adresu. Proksi server zahteva veliku količinu resursa (memorije, procesora), a javlja se i problem rutiranja paketa.

Kriptografija ima veliku ulogu u bezbednosti računarskih mreža. Reč kriptografija potiče iz grčkog jezika i znači tajno pisanje. Ona omogućuje bezbednu razmenu poruka i sprečava krađu poverljivih podataka, čak i u slučajevima kada je napadač u mogućnosti da presretne te poruke. Osnovna ideja je da pošiljalac transformiše poruku u neki nečitljivi format i pošalje primaocu, koji jedini može da izvrši inverznu transformaciju i dođe do originalne poruke. Ukoliko napadač presretne poruku, on nije u mogućnosti da otkrije njen sadržaj. Pored toga što omogućuje poverljivost podataka, kriptografija obezbeđuje i ostale kritične bezbednosne zahteve kao što su autentifikacija i integritet podataka.