**PROTOKOLI**

Komunikacija među dvjema stranama, pa bili to i uređaji, moguća je jedino ukoliko obje strane „govore“ istim jezikom. Stoga se definira formalni skup pravila koja „razumiju“ i koriste obje strane kad međusobno „razgovaraju“. Takva pravila nazivaju se protokoli. Mrežnim je protokolom određen „jezik“ mreže.

Mrežni protokol ima više razina. Tijekom komunikacije svaka razina obavlja određeni zadatak.

TCP/IP (Transmission Control Protocol/Internet Protocol) je mrežni protokol koji se danas najviše koristi. Ovaj protokol ima četiri razine:

1. **APLIKACIJSKA RAZINA** – Ovosno o primjeni, programi „razgovaraju“ na različite načine, stoga je u ovoj razini definirano više aplikacijskih protokola.

FTP (File Transfer Protocol) – protokol za razmjenu datoteka putem interneta.

HTTP (HyperText Transfer Protocol) – protokol za prijenos web stranica s poslužiteljskog do korisničkog računala. Primjenjuje se od 1990. godine pojavom usluge interneta WWW - World Wide Web.

**Kodiranje znakova (engl. character set)** - HTTP koristi MIME definiciju skupa znakova i omogućava razmjenu dokumenata koji sadrže znakove različitih svjetskih jezika definiranjem skupa znakova primijenjenog u dokumentu. Kodiranje znakova se primjenjuje kako bi se slijed okteta mogao ispravno protumačiti kao slijed znakova. Oznake skupova znakova definira IANA. Ako nije navedena oznaka za tip znakova, podrazumijeva se ISO-8859-1. Znakovlje hrvatskog jezika definirano je kao

ISO-8859-2. Danas se najčešće koristi UTF-8.

HTTP se razlikuje od ostalih TCP protokola kao što je npr. [FTP](https://hr.wikipedia.org/wiki/FTP), po tome što se konekcija i komunikacija sa serverom prekida odmah nakon izvršenja zahtjeva klijenta (isporučenog paketa traženih podataka).

*HTTP protokolom definira se, između ostalog:*

1. Forma komunikacije između klijenta i poslužitelja, tj. način postavljanja upita i odgovora i njihov format
2. Kodiranje znakova karakterističnih za brojne jezike (engl. character set)
3. Kodiranje sadržaja (engl. content coding)
4. Pristup dokumentima za različite tipove protokola
5. Pristup dokumentima uz provjeru identiteta (autorizacija i autentikacija)
6. Pohrana dokumenata u privremenu memoriju (engl. caching)
7. Sigurnosne aspekte - osjetljive točke u komunikaciji između klijenta i poslužitelja, odnosno, u procesu dostave podataka korisniku.

**HTTPS** je sigurna verzija HTTP protokola, koja koristi SSL/TLS za zaštitu i skrivanje prometa, odnosno podataka koji se razmjenjuju između klijenta i poslužitelja. Ovaj protokol obično koristi TCP port 443. SSL (donekle) omogućava zaštitu komunikacije, čak i u slučaju kada je samo jedna strana (obično poslužitelj) autentificirana.

**HTTP kolačići (cookies)** su male datoteke koje internetski preglednici spremaju na naše računalo pri pristupanju pojedinim web-sjedištima kako bi se omogućila dodatna funkcionalnost tih stranica.

 Najčešći je primjer brži pristup stranicama pamćenjem prijave - kolačić sadrži podatke za prijavu pa se preskaču postupci ponovnog prijavljivanja na stranicu.

Dolaze li kolačići od strane reklamnih stranica ili stranica neprovjerenog sadržaja, mogu narušiti korisnikovu privatnost. Kolačići su napravljeni s namjerom da budu jednostavni mehanizam za stranice koje bi ih koristile za pamćenje ključnih informacija (uključujući artikle dodane na popis kupovine u online trgovinama) ili pamćenje korisnikove internetske povijesti (uključujući klikanje nekih gumbova, prijavljivanje na račun, ili stranice koje smo posjetili u povijesti). Također mogu biti korišteni u svrhu pamćenja informacija koje smo unosili u određena polja (imena, adrese, lozinke, broj kreditne kartice...)

Ostali tipovi kolačića igraju bitnu ulogu u modernom internetu. Vjerojatno najvažniji, **autentikacijski kolačići** su najčešća metoda korištena od strane servera kako bi znali je li korisnik prijavljen ili nije. Sigurnost autentikacijskog kolačića ovisi o sigurnosti te web-stranice, te o sigurnosti korisnikovog web-preglednika, isto kao i jeli sadržaj kolačića kriptiran ili nije. Ranjivost sigurnosnog sustava može štetiti korisniku ukoliko haker može pročitati njegove informacije zapisane na kolačiću.

**Session cookie**

Session kolačić postoji samo u trenutnoj memoriji dok korisnik pregledava neku web-stranicu. Web-preglednici obično izbrišu session cookie kad korisnik zatvori web-preglednik. Za razliku od ostalih kolačića, session kolačići nemaju u sebi zapisan datum isteka trajanja, stoga ih web-preglednici odmah izbrišu.

**Sigurnosni kolačić**

Sigurnosni kolačić može se jedino nalaziti na stranicama sa kriptiranom vezom (npr. HTTPS), ne mogu biti emitirani preko ne kriptiranih veza (npr. HTTP). To čini kolačić sigurnijim i manje su šanse da će biti izložen cookie lopovima.

**Ustrajan kolačić**

Ustrajni kolačić nije izbrisan nakon zatvaranja web-preglednika, nego u sebi ima datum isteka trajanja. To znači da će u kolačić u cijelom "životnom vijeku" slati informacije serveru svaki put kada korisnik posjeti tu stranicu. Iz tog razloga, često se ovi kolačići nazivaju i pratećim kolačićima jer mogu biti korišteni od strane reklama koje sakupljaju informacije o korisnikovim pretraživanjima na internetu.

**HTTPOnly kolačić**

HTTPOnly kolačiću ne mogu pristupiti korisnikovi aplikacijski i programski protokoli. Ova zabrana eliminira prijetnju kolačić lopovima preko XSS-a, no svejedno kolačić ostaje ranjiv na Cross-site\_tracing XST i Cross-site\_request\_forgery XSRF.

**Superkolačić**

Superkolačići mogu biti potencijalno opasni za sigurnost korisnika i stoga su često blokirani od strane web-preglednika. Ukoliko korisnik ili web-preglednik odblokira superkolačić, haker koji kontrolira malicioznu web-stranicu može postaviti superkolačić da promjeni zahtjeve korisnika koje je stavio na neku drugu stranicu s istom domenom (npr. promjena internet kupovine).

**Zombi kolačić**

Zombi kolačić je kolačić koji se automatski rekreira nakon što je izbrisan. To je omogućeno zbog spremanja kolačića na nekoliko mjesta na računalu, stoga ukoliko se jedan kolačić izbriše, drugi se kopira na to isto mjesto.

**Drugi značajniji internetski protokoli na aplikacijskoj razini su: FTP, HTTP, HTTPS, IMAP, IRC, NNTP, POP3, RTP, SIP, SMTP, SNMP, SSH, SSL, Telnet, UUCP, BitTorrent ...**

**File Transfer Protocol (FTP)** je standardni mrežni protokol koji se koristi za premještanje datoteka s jednog hosta na drugi putem mreže temeljene na TCP-u, kao što je Internet.

Izvorni tehnički opis za FTP je napisao **Abhay Bhushan** i objavljen je kao RFC 114 16.4.1971. godine te poslije zamijenjen RFC 765 (lipanj 1980.g.) pa je zamijenjen s današnjim tehničkim opisom RFC 959 (listopad 1997.g.). Nekoliko standarda dopuna je predloženo RFC 959, npr. RFC 2228 (lipanj 1997.g.) predlaže sigurnosno proširenje i RFC 2428 (rujan 1998.g.) dodaje podršku za IPv6 i definira novi tip pasivnog načina rada.

**Internet Message Access Protocol (IMAP**) ime je za popularni protokol za preuzimanje elektronske pošte preko interneta, drugi popularni protokol je **Post Office Protocol (POP).**

**IRC je kratica za Internet Relay Chat** - doslovni prijevod je "razgovor putem Interneta", koji je nastao 1988. godine. Kao što postoje poslužitelji web stranica (npr. Apache ili IIS), tako postoje i IRC poslužitelji, na koje se korisnici spajaju putem irc klijenata, biraju kanal ili kanale koje će koristiti, te potom komuniciraju s ostalim korisnicima IRC-a koji se nalaze na istom kanalu.

**Network News Transfer Protocol (NNTP)** je internetski aplikacijski protokol koji služi za prenošenje Usenet članaka (netnews - mrežne vijesti) između poslužitelja kao i za čitanje i slanje vijesti od strane krajnih korisnika. Ovaj protokol je opisan sa internetskim standardom RFC 997 1986., a njeni glavni autori su Brian Kantor s University of California, San DiegoPhil Lapsley s University of California, Berkeley.

**POP3**, od engl. Post Office Protocol version 3, uobičajeni je protokol za preuzimanje elektroničke pošte sa poslužitelja na mrežama koje koriste internet protokol.

**Real-time Transport Protocol (RTP)** ime je za standardizirani paket informacija koje služe za prijenos zvuka i pokretnih slika preko IP mreža.

**Protokol za pokretanje sesije (eng. SIP - Session Initiation Protocol)** je signalizacijski protokol koji se rabi radi uspostave, modificiranja i raskidanja višemedijskih sesija u mrežama zasnovanim na internetskom protokolu (IP networks). Razvilo ga je i standardiziralo Radno tijelo za razvoj Interneta (IETF - Internet Engineering Task Force), i ostala značajna međunarodna tijela prihvatila su ga kao glavni protokol u višemedijskim domenama 3G mobilnih sustava (višemedijski podsustav utemeljen na protokolu IP, IMS - IP Multimedia Subsystem) i kao okosnicu mreže sljedeće generacije (NGN - Next Generation Network).

Ovaj je aplikacijski protokol za signale koji je definirao IETF, koji se široko primjenjuje za upravljane multimedijskom komunikacijom kao zvuk ili video preko mreža koje koriste IP. Ovaj protokol se koristi za stvaranje, mijenjanje i prekidanje protoka komunikacija između dvije stranke (unicast) ili između više stranaka (multicast). Mijenjanje se odnosi na mijenajnje adrese ili porta, pozivanje više sudionika, dodavanje ili oduzimanje medijskih prikaza. Aplikacije koje koriste SIP su: video konferencija, instantne poruke, online igre. Glavni dizajneri SIP-a su Henning Schulzrinne i Mark Handley, i rad su započeli 1996. Zadnja inačica SIP specifikacije je RFC 3261. U studenom 2000, SIP je prihvaćen kao signalni protokol za 3GPP, i kao stalni dio IP Multimedia Subsystem (IMS) arhitekture za multimedijske service u mobilnim sistemima.

**SMTP, od engl. Simple Mail Transfer Protocol**, uobičajeni je način (de facto standard) za prijenos elektroničke pošte na internetu. Formalno je definiran u RFC 821, a novija inačica poznata kao ESMTP u RFC 2821.

**SNMP (Simple Network Management Protocol**, slobodni prijevod: jednostavni mrežni protokol za nadzor i upravljanje) jednostavni je protokol koji se danas najčešće koristi za nadzor i upravljanje mrežnim uređajima u TCP/IP mrežama. SNMP omogućava mrežnim administratorima da upravljaju mrežnim performansama, nalaze i rješavaju mrežne probleme te planiraju potrebe za rastom mreže.

**SSH - (Secure Shell)** je mrežni protokol koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem nesigurne računalne mreže.

SSH protokol svoj rad bazira na korištenju kombinacije simetrične i asimetrične kriptografije, metode enkripcije koja omogućuje sigurniji prijenos podataka računalnom mrežom.

**SSL skraćenica je od eng. složenice Secure Sockets Layer**, ili slobodno prevedeno sigurnosni sloj utikača i ime je za transportni protokol unutar TCP/IP stoga. SSL omogućava sigurnu komunikaciju preko interneta za razne aplikacije: e-pošta, web preglednik, trenutne komunikacije (instant messaging) te za druge aplikacije koje koriste TCP/IP stog.

**Telnet j**e mrežni protokol unutar IP grupe protokola koji se koristi na Internetu ili u lokalnim mrežama. Namjena ovog protokola je uspostava dvosmjernog 8-bitnog komunikacijskog kanala između dva umrežena računala. Najčešće se koristi da osigura korisniku jednog računala sesiju za korištenje tzv. sučelja komandne linije na drugom računalu. Sam naziv protokola dolazi od kratice engleskog naziva TELephone NETwork iz kojeg se vidi da je protokol dizajniran s namjerom povezivanja jednog terminala na udaljeno računalo.

Uobičajeno je da se izraz telnet koristi i kao naziv interaktivnog klijentskog programa koji omogućava spajanje na drugo računalo protokolom telnet. Taj je klijentski program pod tim nazivom standardno dostupan na gotovo svim UNIX i Linux operacijskim sustavima gotovo od samih početaka, a u novije vrijeme i na svim drugim operacijskim sustavima. Stoga je poznat i izraz telnetirati se na drugo računalo, što označava korištenje klijenta telnet i protokola telnet za povezivanje na drugo računalo.

**BitTorrent ima dva značenja:**

 - to je naziv peer to peer protokola za dijeljenje i razmjenu datoteka. Svaka datoteka koja se želi dijeliti mora se indeksirati (datoteka se dijeli na jednake dijelove, od 16kB pa sve do 4MB, radi se SHA-1 checksum svih dijelova, i rezultirajuća datoteka se snima na poslužitelj torrent datoteka). Potom se osoba koja dijeli datoteku prijavljuje na tracker poslužitelj i tad je moguće da svi oni koji su našli torrent na indeks-poslužitelju počnu dijeliti datoteku, prvo od izvora, a poslije i međusobno.

- to je naziv programa pomoću kojega možemo dijeliti (bilo skidati bilo uploadati) sadržaje sa interneta, poput filmova i glazbe. Postoji više vrsta indeks-torrent poslužitelja koji pružaju tu uslugu besplatno, bez registracije. Moguće ih je skinuti sa interneta, s bilo koje stranice orijentirane na tu temu. Torrent inače znači mlaz ili bujica, u ovom slučaju, podataka.

2. **PRIJENOSNA RAZINA** - Današnje su mreže paketne što znači da su poruke dijele na manje dijelove ujednačene duljine koje zovemo paketima. Svaki paket sadrži sve podatke: adresu računala koje šalje poruku, adresu računala koje poruku prima, ukupni broj paketa u poruci te svojem mjestu (rednom broju paketa u poruci. Paketi se neovisno jedan o drugome šalju prema odredištu pa stoga mogu doći i putovima i redoslijedom različitim od onih kojima su odaslani.

Prijenosna razina zadužena je za dijeljenje poruka na pakete pri odašiljanju poruke, odnosno za rekonstrukciju poruke od pristiglih paketa pri prijamu. Ova razina najčešće je definirana TCP protokolom.

|  |  |
| --- | --- |
| [**Transportni**](https://hr.wikipedia.org/w/index.php?title=Transportni_sloj&action=edit&redlink=1) | : [TCP](https://hr.wikipedia.org/wiki/TCP), [UDP](https://hr.wikipedia.org/wiki/UDP), [DCCP](https://hr.wikipedia.org/wiki/DCCP),[SCTP](https://hr.wikipedia.org/wiki/SCTP), [IL](https://hr.wikipedia.org/w/index.php?title=IL_(protokol)&action=edit&redlink=1), [RUDP](https://hr.wikipedia.org/w/index.php?title=RUDP&action=edit&redlink=1), |

Protokoli (prijenosni ili transportni):

**TCP** je jedan od osnovnih protokola unutar IP grupe protokola. Naziv je kratica od engleskog naziva Transmission Control Protocol. Korištenjem protokola TCP aplikacija na nekom od hostova umreženog u računalnu mrežu kreira virtualnu konekciju prema drugom hostu, te putem te ostvarene konekcije zatim prenosi podatke. Stoga ovaj protokol spada u grupu tzv. spojnih protokola, za razliku od bespojnih protokola kakav je primjerice UDP. TCP garantira pouzdanu i isporuku podataka u kontroliranom redoslijedu od pošiljatelja prema primatelju. Osim toga, TCP pruža i mogućnost višestrukih istovremenih povezivanja prema jednoj aplikaciji više klijenata na jednom hostu više klijenata, gdje su najčešći primjeri za to web ili poslužitelji e-pošte.

TCP podržava neke od najčešće korištenih aplikacijskih protokola na Internetu, kao što su HTTP (protokol za pregled web stranica), SMTP (protokol za razmjenu elektroničke pošte), telnet i SSH (protokole za udaljeni rad na računalu) i brojne druge.

**UDP** (User Datagram Protocol) omogućuje slanje kratkih poruka (datagram) između aplikacija na umreženim računalima

**Datagram Congestion Control Protocol (DCCP)** ime je za transportni protokol u IP mrežnom modelu, koji služi za sigurnu uspostavu, prekidanje, kontrolu začepljivanja (Explicit Congestion Notification). Standard DCCP je objavljen u RFC 4340, 2006. godine.

3. **RAZINA INTERNETSKOG protokola** dobiva pakete iz prijenosne razine i pridodaje im adresu računala koje šalje podatke te onog računala koje ih prima.

|  |  |
| --- | --- |
| [**Mrežni**](https://hr.wikipedia.org/w/index.php?title=Mre%C5%BEni_sloj&action=edit&redlink=1) | [IP](https://hr.wikipedia.org/wiki/Internetski_protokol) ([IPv4](https://hr.wikipedia.org/wiki/IPv4), [IPv6](https://hr.wikipedia.org/wiki/IPv6)), [ICMP](https://hr.wikipedia.org/wiki/ICMP),[IGMP](https://hr.wikipedia.org/wiki/IGMP), [ARP](https://hr.wikipedia.org/wiki/ARP), [RARP](https://hr.wikipedia.org/wiki/RARP), … |

**IP broj ili IP adresa** je jedinstvena brojčana oznaka računala na internetu. IP adresa je u osnovi binarni broj, koji je u slučaju trenutno važeće verzije IP protokola, IPv4, binarni broj 32 bita dug. Često se radi lakšeg pamćenja IP adrese zapisuju u dekadskoj notaciji, gdje se 32-bitni broj podijeli na četiri 8-bitna broja, koji se zatim prikazuju kao četiri decimalna broja odvojena točkom. Svaki od tih brojeva je u rasponu 0-255, što je upravo raspon brojeva koji se mogu prikazati u jednom 8-bitnom binarnom prikazu. IPv6 verzija protokola predviđa 128-bitne adrese, te se u tom slučaju može koristiti i heksadecimalni zapis, radi kraćeg oblika i jednostavnosti. Primjer IP adrese je 172.16.254.1

Kako je nužno da IP adrese budu jednoznačno dodijeljene, postoje međunarodne organizacije koje se brinu o raspodjeli IP adresnog prostora. Takva je organizacija **The Internet Assigned Numbers Authority (IANA)**. IANA zatim za određen raspon adresa zadužuje regionalne Internet registre, pa je za područje Europe zadužen **RIPE Network Coordination Centre.**

Ono što bi se moglo nazvati IPv5om je postojalo samo kao eksperimentalni ne-IP protokol u realnom vremenu nazvan ST2 i opisan u RFC 1819. Ovaj protokol je napušten u korist RSVPa.

IP adrese se dijele na statičke ( imaju ih poslužitelji) i dinamičke (dobivaju ih klijentska računala).

**U IPv6**, novi standardni internet protokol, gdje su adrese 128 bita široke, što bi, čak i sa velikim dodjelama netblokova, trebalo zadovoljiti blisku budućnost. Teoretski, postojalo bi točno 2128, ili 3.403×1038 unikatnih adresa. Kada bi zemlja bila sačinjena kompletno od zrna pijeska od 1cm³, onda bi se mogla dodijeliti jedinstvena adresa svakom zrnu u 300 milijuna planeta veličine zemlje. Veliki prostor za adrese će biti rijetko popunjen, što omogućava ponovno kodiranje više informacija. Globalne adrese koje se šalju k jednom odredištu sastoje se iz dva dijela: 64-bitni dio za rutiranje i 64-bitni identifikator domaćina. Netblokovi se određuju kao moderne alternative IPv4: broj mreže, kojega prati kosa crta i broj značajnih bitova (u decimalnom zapisu). Primjer je 12AB::CD30:0:0:0:0/60 uključuje sve adrese koje počinju s 12AB00000000CD3. IPv6 ima dosta poboljšanja u odnosu na IPv4, pored samo većeg prostora za adrese, uključujući i samostalno ponovno odbrojavanje i obveznu upotrebu IPsec-a.

P-adrese se pišu i prikazuju u formatu koji je ljudima lahko čitljiv, npr. 172.16.254.1 (IPv4) i 2001:db8:0:1234:0:567:8:1 (IPv6).

**Internet Assigned Numbers Authority (IANA)** rukovodi dodjeljivanjem adresnog prostora IP-adresa širom svijeta i daje ovlaštenje petorici regionalnih internetskih registrara (RIR-a) da lokalnim internetskim registrima (dobavljačima internetskih usluga) dodjeljuju adresne blokove:

African Network Information Center (AFRINIC)[1] for Africa

American Registry for Internet Numbers (ARIN)[2] for the United States, Canada, several parts of the Caribbean region, and Antarctica.

Asia-Pacific Network Information Centre (APNIC)[3] for Asia, Australia, New Zealand, and neighboring countries

Latin America and Caribbean Network Information Centre (LACNIC)[4] for Latin America and parts of the Caribbean region

Réseaux IP Européens Network Coordination Centre (RIPE NCC)[5] for Europe, Russia, the Middle East, and Central Asia

**ICMP (engl. Internet Control Message Protocol)** – komunikacijski protokol koji je ugrađen u svaki IP modul da bi omogućio mrežnim prolazima (usmjerivačima) ili računalima slanje kontrolnih poruka o greškama. Zadužen je samo za prijavljivanje grešaka, ali ne i za njihovo ispravljanje.

**Internet Group Management Protocol (IGMP)** je komunkacijski protokol koji koriste nositelji i granični usmjerivači na IP mreži pri izgrađivaju članstva multicast skupina.

**ARP (engl. Address Resolution Protocol)** – komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese. Najraširenija njegova primjena danas je na Ethernetu gdje se IP adrese povezuju s MAC adresama.

Arp je također i naredba kojom se može pregledavati i mijenjati sadržaj tablice u operacijskom sustavu u kojoj se nalaze informacije dobivene ovim protokolom (tzv. ARP cache).

Arp naredba omogućava mapiranje fizičke adrese poznate kao IPv4 adrese. Ova metoda uključuje slanje ARP requesta. Uređaj za koji su potrebni podatci upućuje ARP zahtjev na mrežu, a lokalni uređaji odgovarju natrag ARP odgovorom koji sadrži njegovu IP-MAC par.

RARP (engl. Reverse Address Resolution Protocol) mrežni je protokol kojim je moguće iz poznate fizičke MAC adrese saznati IP adresu, što je obrnuto od uloge ARP-a. Najčešća primjena RARP-a je kod sustava bez diska koji prilikom pokretanja ne znaju vlastitu IP adresu pa je dobivaju pomoću RARP upita.

4**. MREŽNO SUČELJE** – dobije pakete iz prethodne razine te ih šalje kroz mrežu ili prima iz mreže. Protokol ove razine ovisi o mreži koja se koristi.

|  |
| --- |
|  |
| [**Podatkovni**](https://hr.wikipedia.org/w/index.php?title=Podatkovni_sloj&action=edit&redlink=1) | Ethernet, [Wi-Fi](https://hr.wikipedia.org/wiki/Wi-Fi%22%20%5Co%20%22Wi-Fi),[Token ring](https://hr.wikipedia.org/wiki/Token_ring%22%20%5Co%20%22Token%20ring), [PPP](https://hr.wikipedia.org/wiki/PPP), [SLIP](https://hr.wikipedia.org/wiki/SLIP),[FDDI](https://hr.wikipedia.org/wiki/FDDI), [ATM](https://hr.wikipedia.org/wiki/ATM), [DTM](https://hr.wikipedia.org/w/index.php?title=DTM&action=edit&redlink=1),[Frame Relay](https://hr.wikipedia.org/wiki/Frame_Relay%22%20%5Co%20%22Frame%20Relay), [SMDS](https://hr.wikipedia.org/w/index.php?title=SMDS&action=edit&redlink=1), … |

Ethernet ili IEEE standard 802.3 je danas najčešće korištena tehnologija za lokalne mreže (LAN).

**Wi-Fi** je zaštitni znak koji se postavlja na certificirane proizvode za bežičnu lokalnu računalnu mrežu (WLAN) zasnovane na specifikacijama IEEE 802.11, a neformalno često i sinonim za cijelu takvu tehnologiju.

Certifikat izdaje istoimena neprofitna udruga proizvođača Wi-Fi Alliance sa svrhom poticanja međusobne kompatibilnosti i promoviranja svojih proizvoda.

Token ring ime je za LAN protokol koji nalazi u podatkovnom sloju OSI modela mreže. Token ring koristi posebni tri bajtni okvir koji se zove token (žeton) koji putuje u krugu do svake stranice lokalne mreže. Računalo domačin koje posjeduje taj tro bajtni žeton ima pravo isproučiti podatke preko medija.

PPP (engl. Point-to-Point Protocol, hrv. Protokol za komunikaciju od točke do točke ) koristi se za izravno povezivanje dvaju čvorova računalne mreže. Omogućuje povezivanje računala serijskim, telefonskim ili optičkim kabelom, pomoću mobilnih telefona te posebno oblikovanom radio ili satelitskom vezom. Većina ISP (engl. Internet Service Provider) poslužitelja koristi ovaj protokol za omogućavanje pristupa Internetu preko telefonskog priključka korištenjem modema (engl. dial-up). Ugrađena (engl. encapsulated) inačica PPP protokola, tzv. PPPoE (engl. Point-to-Point over Ethernet) protokol, se na sličan način koristi kod DSL (engl. Digital Subscriber Line) pristupa Internetu. Kod ovog protokola se PPP podatkovni paketi umeću u Ethernet pakete.

**PPP** protokol se koristi na drugom, podatkovnom, sloju OSI (engl. Open System Interconnection) mrežnog modela za povezivanje preko sinkronih i asinkronih veza. Ovaj je protokol u velikoj mjeri zamijenio starije protokole, kakav je npr. SLIP (engl. Serial Line Internet Protocol) protokol, i protokole telefonskih kompanija, kao što je LAPB (engl. Link Access Procedure Balanced) protokol iz X.25 skupine protokola. PPP je građen tako da omogućuje rad s brojnim protokolima mrežnog sloja, uključujući IP (engl. Internet Protocol), IPX (engl. Internetwork Packet Exchange) i AppleTalk protokole.

**Serial Line Internet Protocol (SLIP)** je učahurenje IP koji omogućava rad preko serijskih protokola i modema.

**Fiber Distributed Data Interface (FDDI)** omogućava prijenos od 100 Mbit/s i optički je standard prijenos podataka na lokanoj mreži koja se može proteći do 200 km. Iako je topologija FDDI-a zasnovana na prestenatoj žetonskoj mreži, FDDI ne koristi IEEE 802.5 token ring protokol kao svoju osnovu; FDDI protokol je derivacija IEEE 802.4 token bus sinhroniziranog žetonskog protokola.

**ATM (engl. Asynchronous Transfer Mode**) tehnika je prijenosa u telekomunikacijama koja se zasniva na asinkronom vremenskom multipleksiranju odsječaka prometa (ćelija) veličine 53 bajta, od kojih je 48 koristan promet, a 5 čini zaglavlje.

Glavna odlika ove tehnike je da osim prijenosa podataka omogućuje i kvalitetan prijenos drugih vrsta prometa kao što su digitalizirani glas (telefon) i slika (video). To je jedan od razloga za korištenje ATM-a kod usluga zasnovanih na ADSL-u.

**Frame relay** je jedan od najpopularnijih protokola za prijenos podataka (uz Ethernet i ATM). Koristi za povezivanje LAN,SNA, Internet ili čak “voice” aplikacija.

--------------------------------------------------------------------

**RSS** (kratica od RDF Site Summary, više poznat kao Really Simple Syndication - stvarno jednostavne vijesti) je univerzalni format za razmjenu sadržaja omogućava vlasnicima web stranica prezentiranje sadržaja korisnicima u skraćenom obliku. Korisnici mogu ponuđene sadržaje pregledavati pomoću preglednika, posebnih programa ili koristiti na svojim stranicama.

**Internet Society ( ISOC )** je američka neprofitna organizacija osnovana 1992. godine kako bi osigurala povezivanje normama, obrazovanje, pristup i politiku. Njegova je misija "promicati otvoreni razvoj, evoluciju i korištenje Interneta za dobrobit svih ljudi širom svijeta".

Internetsko društvo ima svoje globalno sjedište u Restonu u Virginiji , Sjedinjenim Državama (blizu Washingtona), glavnim uredom u Ženevi , Švicarskoj , te regionalnim uredima u Bruxellesu , Singapuru i Montevideu . Ima globalnu članstvo više od 100.000 organizacijskih i individualnih članova.

**Web – katalozi** – informacije na internetu možemo pronaći i korištenjem web-kataloga. Radi se o posebnim web-sjedištima koja nude uslugu pronalaženja sadržaja na internetu pomoću uređenog kataloga web-stranica razvrstanih po kategorijama i potkategorijama.