TCP/IP PROTOKOLLAR TO‘PLAMI

Mamajonova Gulmox Misratulla qizi
Farg‘ona davlat texnika universiteti
732-23(21) guruh talabasi

Tillaboyev Muhiddinjon Ganijonovich
Farg‘ona davlat texnika universiteti o‘qituvchisi
Email: gulmohmamadjanova601@gmail.com

Annotatsiya. Ushbu maqola zamonaviy raqamli infratuzilmaning asosini tashkil etuvchi TCP/IP protokollar to‘plamini har tomonlama ilmiy va amaliy nuqtai nazardan o‘rganadi. Internet tufayli insoniyat tarixida misli ko‘rilmagan ma’lumot almashinuv tezligi va ko‘lami paydo bo‘ldi — 2024-yil ma’lumotlariga ko‘ra global Internet trafigi kuniga taxminan 400 eksabaytni tashkil etmoqda. Bu astronomik raqamning zamirida esa oddiy, lekin ulug‘vor g‘oyaga asoslangan protokollar majmuasi yotadi: TCP/IP.

Kalit so‘zlar: TCP/IP, protokol, tarmoq qatlami, IPv4, IPv6, routing, encapsulation, congestion control, sliding window, three-way handshake.

Kirish

1969-yil 29-oktabr kuni soat 22:30 da UCLA dan SRI (Stanford Research Institute) ga birinchi ARPANET xabari yuborildi. Yuboruvchi "LOGIN" yozmoqchi edi, ammo tizim "L" va "O" harflaridan so‘ng ishdan chiqdi. Shunday bo‘lsa-da, bu "LO" — dunyo tarixidagi birinchi tarmoq xabari bo‘lib, Internet erasining boshlanishini belgiladi.

ARPANET bir muammo atrofida qurilgan edi: yadroviy urush bo‘lsa ham aloqa uzilmasin. Buning uchun markazlashtirilgan tizim emas, balki har bir tugun mustaqil yo‘l topa oladigan tarqatilgan tarmoq kerak edi. Bu g‘oya "paket kommutatsiyasi" (packet switching) deb atalgan texnologiyada mujassamlashdi — ma’lumot kichik bo‘laklarga (paket) bo‘linib, har bir bo‘lak mustaqil ravishda tarmoq orqali yo‘l topadi.

Dastlabki ARPANET NCP (Network Control Program) protokolida ishladi. Biroq 1970-yillar o‘rtasiga kelib tarmoq kengaydi va turli xil kompyuter tizimlari paydo bo‘ldi — ularni bog‘lash uchun universal til kerak edi. 1974-yilda Vint Serf (Vinton Cerf) va Bob Kan (Robert Kahn) "A Protocol for Packet Network Intercommunication" maqolasini nashr etdi. Bu maqola TCP ning ilk ta’rifini o‘z ichiga olardi. 1978-yilda TCP va IP ikki alohida protokolga ajratildi — shunday qilib TCP/IP juftligi tug‘ildi.

1983-yil 1-yanvar "Flag Day" deb atalib, ushbu kunda barcha ARPANET tugunlari NCP dan TCP/IP ga ko‘chdi. Bu zamonaviy Internetning rasmiy tug‘ilgan kuni hisoblanadi. Keyingi o‘n yilliklarda Tim Berners-Li (Tim Berners-Lee) ning WWW ixtirosi (1989), brauzerni ommalashtirgan Mosaic (1993), Google (1998) va hozirgi raqamli ekotizim — barchasi TCP/IP ustida qurildi.

TCP/IP Falsafasi va Dizayn Prinsiplari

TCP/IP ning muvaffaqiyati tasodifiy emas — u puxta o‘ylangan falsafiy prinsiplar asosida qurilgan. Bu prinsiplarni tushunmay turib protokolning kuchini to‘liq anglab bo‘lmaydi.

End-to-End printsipi (Ulanish uchlarida aql): Tarmoqning o‘zi iloji boricha sodda bo‘lishi, murakkab logika esa ulanishning ikki uchida — manba va qabul qiluvchi — joylashishi kerak. Bu printsip tarmoqni turli ilovalar uchun universal qiladi.

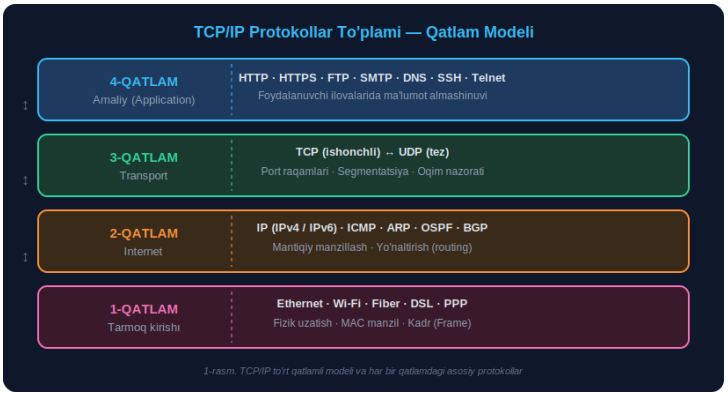
Best-effort yetkazib berish: IP protokoli paketni yetkazib berishga harakat qiladi, lekin kafolat bermaydi. Ishonchlilik yuqori qatlamlarga (TCP) yuklatiladi. Bu yondashuv tarmoqni sodda va tez saqlaydi.

Modulyarlik va qatlamlilik: Har bir qatlam faqat o‘z vazifasini bajaradi. Bu texnologik yangilashni osonlashtiradi — Wi-Fi Ethernet o‘rnini oldi, lekin IP qatlami o‘zgarmadi.

Ochiqlik: TCP/IP spetsifikatsiyalari RFC hujjatlari orqali barchaga ochiq. Har qanday kompaniya yoki dasturchi ularga rioya qilgan holda mahsulot yaratishi mumkin. Bu raqobat va innovatsiya uchun zamin yaratdi.

Aloqa yo‘llari mustaqilligi: Paketlar istalgan yo‘l orqali borishlari mumkin. Agar bir yo‘nalish ishlamasa, paketlar boshqa yo‘ldan o‘tadi. Bu "resilience" — chidamlilik xususiyatini ta’minlaydi.

Ushbu prinsiplar birgalikda TCP/IP ni yadroviy hujumga chidamli (dastlabki maqsad), va shu bilan birga — global tijorat, ijtimoiy aloqa va ilmiy hamkorlik uchun universal platforma sifatida shakllantirdi. Dizayn maqsadi va yakuniy natija o‘rtasidagi bu paradoks texnologiya tarixining eng qiziqarli sahifalaridan biridir.



1-rasm. TCP/IP to‘rt qatlamli modeli va har qatlamdagi asosiy protokollar

Metodologiya

Ushbu tadqiqot asosan tahliliy-deduktiv va qiyosiy uslublarga tayanadi. Birlamchi manbalar sifatida IETF tomonidan nashr etilgan RFC hujjatlaridan foydalanildi. Ilmiy adabiyot sifatida Tanenbaum va Wetherall "Computer Networks" (5-nashr), Kurose va Ross "Computer Networking: A Top-Down Approach" (8-nashr), Stevens "TCP/IP Illustrated" (3 jild), Forouzan "Data Communications and Networking" (5-nashr) ishlatildi. Amaliy ma’lumotlar uchun Cisco, Cloudflare va Google texnik bloghlaridan, shuningdek Wireshark tarmoq tahlil vositasi natijalaridan foydalanildi.

Har bir protokol quyidagi mezonlar bo‘yicha baholandi: (1) funktsional to‘liqlik — protokol o‘z vazifasini to‘liq bajara oladimi; (2) samaradorlik — sarlavha overhead nisbati; (3) ishonchlilik — xato aniqlash va tuzatish mexanizmlari; (4) xavfsizlik — o‘rnatilgan va qo‘shimcha himoya choralari; (5) moslashuvchanlik — yangi texnologiyalarga moslanish qobiliyati.

Port Raqamlari Tizimi

Transport qatlamida portlar — bu dasturning tarmoqdagi "eshigi". IP manzil kompyuterga yo‘l ko‘rsatsa, port raqami qaysi dasturga etkazilishini belgilaydi. Port raqamlari 0 dan 65535 gacha bo‘lib, uch guruhga bo‘linadi:

1-jadval. TCP/UDP port raqamlari diapazoni va ularning vazifalari

Diapazon	Nomi	Tavsifi
0 – 1023	Well-Known	Tizim protokollari: HTTP(80), HTTPS(443), SSH(22), DNS(53), FTP(21), SMTP(25)
1024 – 49151	Registered	Ro‘yxatdan o‘tgan ilovalar: MySQL(3306), PostgreSQL(5432), Redis(6379), RDP(3389)
49152 – 65535	Dynamic/Private	Vaqtinchalik portlar: mijoz dasturlari tomonidan operatsion tizim tomonidan avtomatik tayinlanadi

Muhokama

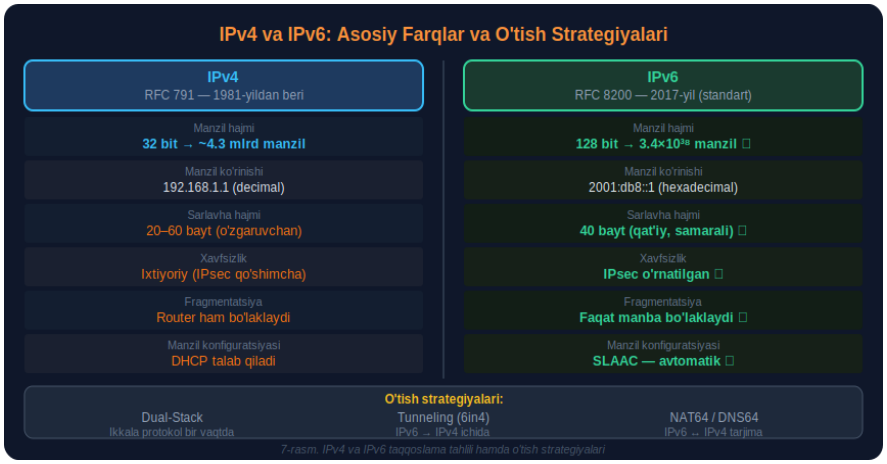
Internet Protokoli (IP) — TCP/IP tuzilishining "asab tizimi". U paketlarni manba tarmoqdan manzil tarmoqqa yo‘naltirish (routing) uchun javobgardir. IPv4, RFC 791 (1981) da belgilangan, 32 bitli manzillash tizimidan foydalanadi va "best-effort" printsipida ishlaydi — paketni yetkazib berishga harakat qiladi, lekin yetkazilishini, tartibini yoki kechikmasligini kafolatlamaydi.

TTL maydoni 8 bitdan iborat va paket nechta "sakrash" (hop) qilishi mumkinligini belgilaydi. Har bir router bu qiymatni 1 ga kamaytiradi. Agar TTL 0 ga teng bo‘lsa, router paketni yo‘q qiladi va ICMP "Time Exceeded" xabarini manbaga yuboradi. Linuxda standart TTL = 64, Windowsda = 128. Bu farq tarmoq diagnostikasida qurilma turini aniqlashda ishlatiladi.

Tarmoqning MTU (Maximum Transmission Unit) — bu bir kadrda uzatilishi mumkin bo‘lgan maksimal ma’lumot hajmi. Ethernet uchun MTU = 1500 bayt. Agar IP paketi bu chegaradan katta bo‘lsa, router uni kichik bo‘laklarga (fragment) ajratadi. Har bir fragment mustaqil paket sifatida uzatiladi va qabul qiluvchi tomonda IP qatlami ularni qayta yig‘adi. IPv6 da fragmentation faqat manbada bajarilishi — bu routerlarni soddalashtiradi va unumdorlikni oshiradi.

Routerlar (yo‘riqchilar) IP manzillariga asoslanib paketlarni keyingi tugunga yo‘naltiradi. Har bir routerda routing jadvali (routing table) mavjud bo‘lib, u qaysi manzil qaysi interfeysga yo‘naltirilishini ko‘rsatadi. Routing protokollari esa bu

jadvallarni dinamik yangilab turadi. Ichki tarmoqlarda OSPF (Open Shortest Path First) va IS-IS, tarmoqlar orasida BGP (Border Gateway Protocol) ishlatiladi. BGP — Internetning "asosiy yo‘riqchi protokoli" va u har kuni millionlab routing yo‘nalishlarini boshqaradi.



2-rasm. IPv4 va IPv6 taqqoslamasi va o‘tish strategiyalari

IPv6 ning 128 bitli manzil maydoni nafaqat manzil tanqisligini hal qiladi — u tarmoq arxitekturasini qayta shakllantiradi. IPv6 manzili sakkizta 16 bitli blokdan iborat, ikki nuqta bilan ajratilgan hexadecimal formatda yoziladi: masalan, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Ketma-ket kelgan nol bloklari :: bilan qisqartirish mumkin: 2001:db8::1.

IPv6 ning muhim texnik yangiliklari:

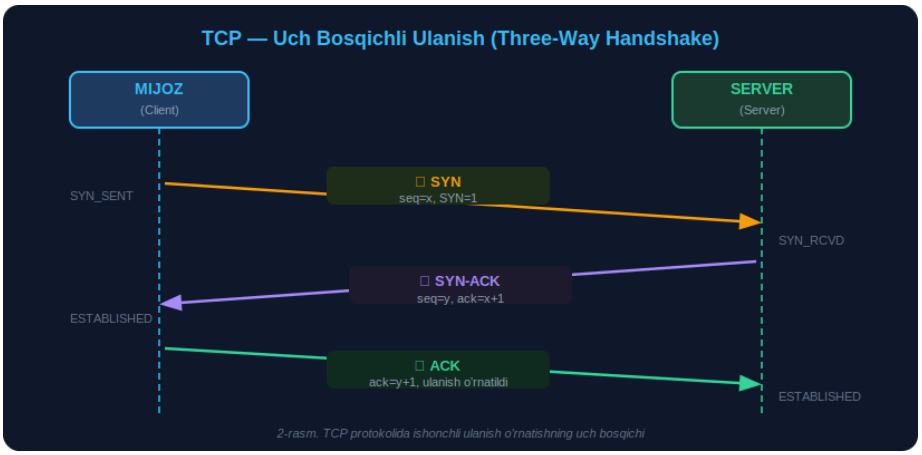
SLAAC (Stateless Address Autoconfiguration): Qurilma DHCP serverisiz o‘z IPv6 manzilini avtomatik yaratadi. Router Advertisement xabaridan tarmoq prefiksini olib, o‘zining MAC manzilidan interface identifikatorini hosil qiladi.

Anycast manzillash: Bir xil manzilga ega bir nechta server bo‘lishi mumkin — paket ulardan eng yaqiniga yo‘naltiriladi. Bu CDN (Content Delivery Network) va DNS tizimlarida keng qo‘llaniladi.

Kengaytirilgan sarlavhalar (Extension Headers): IPv4 da "Options" maydoni o‘rniga IPv6 da alohida "extension header"lar qo‘llaniladi. Bu asosiy sarlavhani soddalashtiradi va kelajakda yangi funksiyalarni qo‘shishni osonlashtiradi.

Flow Label: 20 bitli ushbu maydon bir xil oqimga tegishli paketlarni belgilaydi. QoS (Quality of Service) tizimlarida muhim ahamiyat kasb etadi.

Hop-by-Hop Options: Yo‘ldagi barcha routerlar o‘qishi kerak bo‘lgan maxsus parametrlar uchun ishlatiladi — masalan, RSVP (Resource Reservation Protocol) uchun.



3-rasm. TCP protokolida uch bosqichli ulanish o‘rnatish va holat diagrammasi

TCP ning oqim nazorati (flow control) "siljuvchi oyna" (sliding window) algoritmi orqali amalga oshiriladi. Qabul qiluvchi o‘zining bufer hajmini — rwnd (receiver window) — TCP sarlavhasidagi "Window Size" maydoni orqali uzatuvchiga bildiradi. Uzatuvchi jo‘natilgan lekin tasdiqlanmagan (unacknowledged) ma’lumot hajmini shu chegaradan oshirolmaydi.

Masalan, qabul qiluvchi rwnd = 65535 bayt desa, uzatuvchi tasdiqlanmagunicha jami 65535 baytdan ko‘p yuborolmaydi. Qabul qiluvchining buferi to‘lganda rwnd = 0 bo‘ladi va uzatuvchi kutadi. Bufer bo‘shaganda qabul qiluvchi "Window Update" yuboradi va uzatish davom etadi. Bu mexanizm tez uzatuvchining sekin qabul qiluvchini "bosib ketishiga" yo‘l qo‘ymaydi.

Tarmoqning umumiy yuklanishi — tiqilinch (congestion) — barcha foydalanuvchilarga ta’sir qiladi. TCP ning tiqilinchni boshqarish algoritmlari bu muammoni hal qiladi. Zamonaviy Linux kernelida standart algoritm TCP Cubic bo‘lsa, Google tomonidan ishlab chiqilgan BBRv3 tobora keng qo‘llanilmoqda.

Slow Start (Sekin boshlash): Ulanish boshlanishida cwnd (congestion window) = 1 MSS (Maximum Segment Size) bo‘ladi. Har bir ACK kelganda cwnd ikki barobar ortadi — bu eksponensial o‘sish ssthresh (slow start threshold) ga yetgunicha davom etadi.

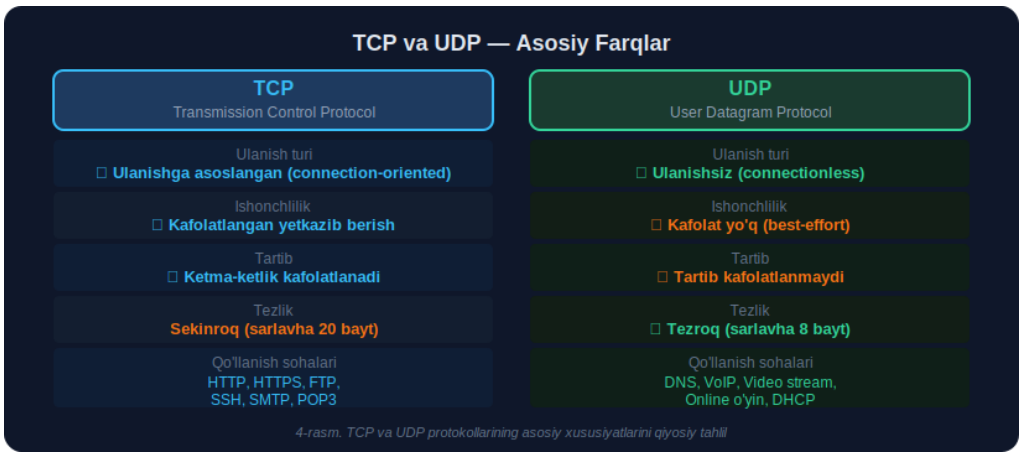
Congestion Avoidance (Tiqilinchdan qochish): ssthresh dan keyin cwnd har RTT (round-trip time) da faqat 1 MSS ga oshadi — bu chiziqli o‘sish.

Fast Retransmit: Agar 3 ta takrorlangan ACK kelsa (duplicate ACK), TCP paket yo‘qolganligini tushunadi va timeout kutmasdan qayta yuboradi.

Fast Recovery: Paket yo‘qotilganda ssthresh yarim qilinadi, cwnd yangi ssthresh ga tushadi va Congestion Avoidance davom etadi.

TCP ulanishni yopganda, faol taraf (active closer) TIME_WAIT holatiga kiradi va 2×MSL (Maximum Segment Lifetime, odatda 60-120 sekund) kutadi. Buning sababi — tarmoqda hali "ko‘chib yurgan" eski paketlar bo‘lishi mumkin. TIME_WAIT davri ularning muddati o‘tib yo‘q bo‘lishini ta’minlaydi. Yuqori yuklamali serverlarda TIME_WAIT holatlari juda ko‘payib ketishi mumkin — bu "TIME_WAIT exhaustion" deb atalib, port tanqisligiga olib keladi.

Bu muammo SO_REUSEADDR va SO_REUSEPORT socket optsiyalari orqali hal qilinadi.



4-rasm. TCP va UDP protokollarining asosiy xususiyatlari va qo‘llanish sohalari

UDP ning sarlavhasi faqat 8 bayt: manba port (2 bayt), manzil port (2 bayt), uzunlik (2 bayt), nazorat summasi (2 bayt). Bu minimalizm UDP ni ba’zi vaziyatlarda TCP dan ancha afzal qiladi. Qaysi holatlarda UDP tanlash to‘g‘riroq?

Kechikishga sezgir ilovalar: VoIP (Voice over IP) da 150 ms dan ortiq kechikish suhbat sifatini sezilarli pasaytiradi. TCP ning qayta uzatish mexanizmi bu kechikishni yanada ko‘paytirishi mumkin — UDP da esa yo‘qolgan tovush paketi shunchaki o‘tkazib yuboriladi, kechikish esa minimal qoladi.

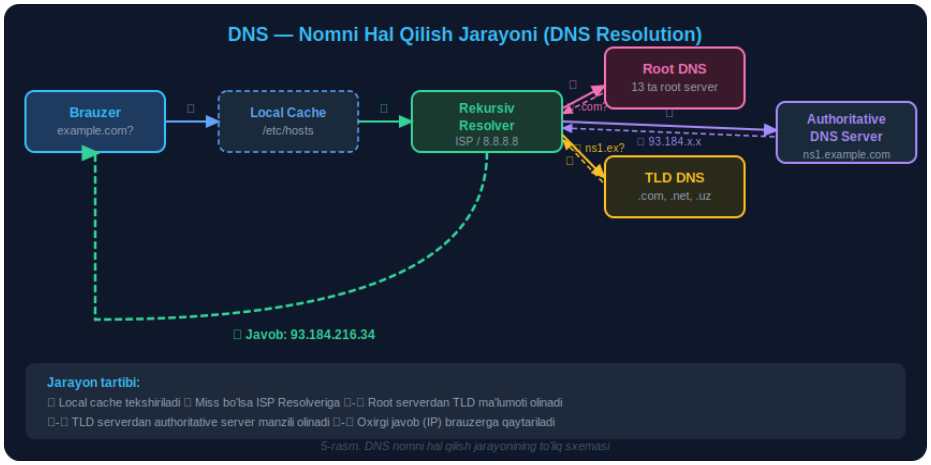
Multicast va broadcast: UDP bir paketni bir vaqtda ko‘p qabul qiluvchiga yuborish imkonini beradi. IPTV (internet televiziyasi) va jonli efir shu sababdan UDP ishlatadi.

Qisqa so‘rov-javob: DNS so‘rovi bitta UDP paketga sig‘adi va javob ham bitta paketda keladi. TCP ulanish o‘rnatishi (3-way handshake) keraksiz kechikish qo‘shardi.

Stateless protokollar: DHCP, SNMP (Simple Network Management Protocol) va TFTP (Trivial File Transfer Protocol) UDP ishlatadi, chunki ular holat saqlashni talab qilmaydi.

QUIC protokoli: HTTP/3 ning ostida ishlaychi QUIC protokoli UDP ustida qurilgan, lekin o‘zi TCP ning ko‘plab funksiyalarini (ishonchlilik, oqim nazorati, xavfsizlik) amalga oshiradi.

Muhokama: Amaliy Qatlam Protokollari



5-rasm. DNS nomni hal qilish jarayonining to‘liq bosqichli sxemasi

DNS (Domain Name System) 1983-yilda Paul Mockapetris tomonidan ixtiro qilingan va bu ixtiro Internet tarixidagi eng muhim qarorlardan biri bo‘ldi. Undan oldin barcha tarmoq nomlari bitta HOSTS.TXT faylida saqlangan edi — tarmoq kengayishi bilan bu holat boshqarib bo‘lmas edi.

DNS ierarxik tuzilishga ega. "www.example.com" manzilini o‘ngdan chapga o‘qisak: "." (ildiz yoki root) — "com" (TLD — Top Level Domain) — "example" (ikkinchi darajali domen) — "www" (subdomen). Bu ierarxiya DNS ma’muriyatini

ham aks ettiradi: ICANN ildiz domenlarni boshqaradi, domeny registraturalar TLD lar bilan shug‘ullanadi, tashkilotlar o‘z domenlarini o‘zlari boshqaradi.

DNS kesh mexanizmi tizimni ishlashini ta’minlaydi. Har bir DNS yozuvida TTL (Time to Live) qiymati bo‘lib, u ushbu yozuvning necha sekundgacha keshlashini ko‘rsatadi. Google ning 8.8.8.8 va 8.8.4.4 DNS serverlari, Cloudflare ning 1.1.1.1 serveri — bu public recursive resolver lar global DNS kesh infrastrukturasining bir qismi.

DNS xavfsizligi alohida mavzu. DNS so‘rovlari an’anaviy ravishda ochiq matn (plaintext) sifatida UDP/53 orqali uzatiladi — bu "DNS spoofing" va "Man-in-the-Middle" hujumlariga imkon beradi. DNSSEC (DNS Security Extensions) raqamli imzolar orqali javoblar autentifikatsiyasini ta’minlaydi. DoH (DNS over HTTPS) va DoT (DNS over TLS) esa DNS so‘rovlarini shifrlaydi.

HTTP/HTTPS — Webning Tili

HTTP (Hypertext Transfer Protocol) 1991-yilda Tim Berners-Li tomonidan ixtiro qilingan va o‘shandan beri veb ning asosiy protokoli sifatida xizmat qilmoqda. HTTP so‘rov-javob (request-response) modelida ishlaydi: mijoz so‘rov yuboradi, server javob qaytaradi.

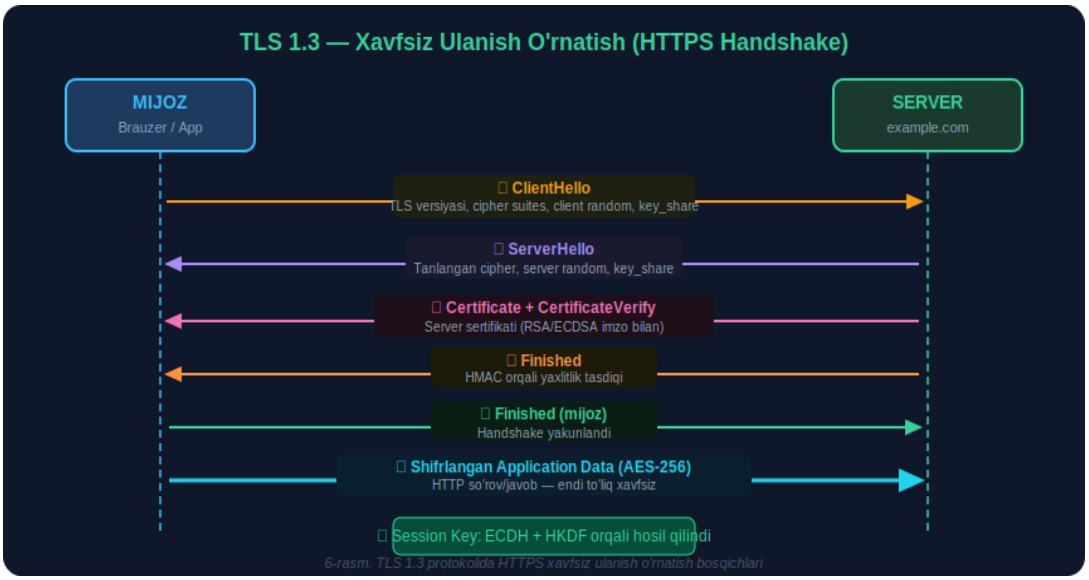
2-jadval. HTTP protokolining versiyalari va har versiyaning asosiy yangiliklari

Versiya	Asosiy xususiyatlar	O‘zgarish
HTTP/1.0	Har so‘rov uchun yangi TCP ulanish	1996, RFC 1945
HTTP/1.1	Persistent connection, pipelining	1997, RFC 2616 — 20 yil standart
HTTP/2	Multiplexing, header compression (HPACK), server push	2015, RFC 7540 — TCP ustida
HTTP/3	QUIC ustida, 0-RTT ulanish, head-of-line blocking yo‘q	2022, RFC 9114 — UDP ustida

HTTP/2 ning eng muhim yangiligi — multiplexing. HTTP/1.1 da "head-of-line blocking" muammosi bor edi: bitta yo‘qolgan paket barcha keyingi so‘rovlarni to‘xtatib qo‘yardi. HTTP/2 da bitta TCP ulanish orqali bir vaqtda ko‘plab so‘rovlar parallel yuboriladi. HTTP/3 esa bu muammoni QUIC yordamida tubdan hal qildi —

har bir so‘rovning o‘z mustaqil QUIC stream i bor, bittasining yo‘qolishi boshqalarga ta’sir qilmaydi.

TLS/HTTPS — Xavfsiz Aloqa



6-rasm. TLS 1.3 protokolida HTTPS xavfsiz ulanish o‘rnatishning bosqichlari

TLS (Transport Layer Security) — SSL ning merosxo‘ri — amaliy va transport qatlami orasida ishlaydi. TLS 1.3 (RFC 8446, 2018) oldingi versiyalarga nisbatan jiddiy yaxshilanishlar olib keldi:

Handshake qisqartirish: TLS 1.2 da handshake 2 RTT (round-trip time) talab qilardi. TLS 1.3 da bu 1 RTT gacha qisqardi. 0-RTT (Zero Round Trip Time Resumption) bilan esa oldindan ma’lum serverga ulanishda dastlabki so‘rov handshake bilan birga yuboriladi.

Eskirgan algoritmlarni olib tashlash: TLS 1.3 RC4, DES, 3DES, MD5, SHA-1, RSA key exchange kabi zaif algoritmlarni butunlay olib tashladi. Faqat zamonaviy, xavfsiz suitlar qoldi: AES-GCM, ChaCha20-Poly1305, ECDHE.

Forward Secrecy majburiy: Har bir sessiya uchun yangi vaqtinchalik kalit yaratiladiki (ECDHE), hatto uzoq muddatli server kaliti o‘g‘irlansa ham, o‘tgan sessiyalar shifrini ochib bo‘lmaydi.

Encrypted SNI: TLS 1.3 da Server Name Indication (SNI) — qaysi domen bilan ulanilayotgani — ham shifrlangan holda uzatiladi. Bu xususiyat tarmoq kuzatuvchilardan qo‘shimcha himoya beradi.

DHCP — Avtomatik Manzil Berish

DHCP (Dynamic Host Configuration Protocol) qurilma tarmoqqa ulanganda avtomatik ravishda IP manzil, subnet mask, default gateway va DNS server manzillarini beradi. Bu jarayon to‘rtta bosqichdan iborat — "DORA" qisqartmasi bilan eslab qolinadi:

3-jadval. DHCP DORA jarayonining to‘rtta bosqichi va har bosqichdagi xabar mazmuni

#	Xabar	Qabul qiluvchi	Mazmuni
1	DISCOVER	Broadcast (255.255.255.255)	Tarmoqda DHCP server bormi?
2	OFFER	Mijozga	Mana bu IP manzilni olishingiz mumkin
3	REQUEST	Broadcast	Taklif qilingan manzilni qabul qilaman
4	ACK	Mijozga	Tasdiqlandi, manzil va parametrlar berildi

DHCP lease (ijara) tushunchasi: DHCP server IP manzilni doimiy emas, balki muddatli beradi. Uy routerlari odatda 24 soatlik lease beradi. Muddat tugashidan oldin qurilma lease ni yangilaydi (RENEW). Bu mexanizm IP manzillarni samarali boshqarish imkonini beradi — tarmoqdan chiqib ketgan qurilmalarning manzillari boshqalarga qayta beriladi.

SMTP va Elektron Pochta Protokollari Zanjiri

Elektron xabar yuborish jarayoni aslida bir necha protokolning muvofiqlashtirilgan ishini talab qiladi:

SMTP (Simple Mail Transfer Protocol, port 25/587): Xabarni yuborish protokoli. Sizning mail client ingiz SMTP orqali mail server ingizga xabar yuboradi, u esa manzil domen ning MX (Mail Exchange) yozuvini DNS orqali topib, uning SMTP serveriga xabarni uzatadi.

IMAP (Internet Message Access Protocol, port 143/993): Xabarlarni server da saqlab, har xil qurilmadan ko‘rish imkonini beradi. Xabar faqat o‘chirilganda serverdan ketadi — shu sababdan Gmail, Outlook kabi xizmatlar IMAP ishlatadi.

POP3 (Post Office Protocol 3, port 110/995): Xabarlarni serverdan yuklab oladi va odatda serverdan o‘chiradi. Eski, hozir IMAP bilan almashtirilgan.

SPF, DKIM, DMARC: Spam va fishing hujumlaridan himoyalanish mexanizmlari. SPF (Sender Policy Framework) qaysi serverlar ushbu domendan xabar yuborishi mumkinligini DNS orqali belgilaydi. DKIM (DomainKeys Identified Mail) xabarni raqamli imzolaydi. DMARC esa SPF va DKIM ishlamaganida nima qilish kerakligini belgilaydi.

Kelajak: Protokollarning Yangi Avlodi

QUIC (Quick UDP Internet Connections) — Google tomonidan 2012-yilda ishlab chiqilgan, 2021-yilda IETF tomonidan RFC 9000 sifatida standartlashtirilgan yangi transport protokoli. QUIC UDP ustida ishlab, TCP ning barcha kamchiliklarini bartaraf etadi:

0-RTT ulanish: Ilgari ulanilgan server bilan yangi sessiya boshlashda hech qanday handshake kechikmasdan darhol ma’lumot yuborish mumkin.

Connection ID: QUIC ulanish IP manzil va port o‘rniga noyob "Connection ID" ga asoslanadi. Wi-Fi dan 4G ga o‘tganda IP manzil o‘zgarsa ham ulanish uzilmaydi — bu mobil ilovalar uchun inqilobiy.

Stream multiplexing: Har bir QUIC stream mustaqil — bittasida yo‘qotish bo‘lsa, boshqalar kutmaydi. HTTP/2 dagi TCP darajasidagi head-of-line blocking muammosi yo‘q.

O‘rnatilgan shifrlash: QUIC da TLS 1.3 ajralmas qism bo‘lib, shifrlanmagan QUIC ulanish mumkin emas.

Cloudflare statistikasiga ko‘ra, 2024-yilda barcha veb-trafikning 30% dan ko‘prog‘i HTTP/3 (QUIC) orqali uzatilmoqda. Bu o‘tish tezligi TCP/IP ning 1983-yildan beri ko‘rgan eng tezkor protokol yangilanishi hisoblanadi.

IoT va Kichik Qurilmalar Uchun Protokollar

Milliardlab IoT qurilmalari — aqlli termostatlar, tibbiy sensorlar, sanoat avtomatsiyasi — TCP/IP ning to‘liq stekini ko‘tara olmaydi. Buning uchun maxsus "engil" protokollar ishlab chiqilgan:

MQTT (Message Queuing Telemetry Transport, port 1883/8883): Publish-subscribe modeli. Sensor ma’lumotlarini broker ga yuboradi, ilovalar broker dan oladi. Telekommunikatsiya tarmoqlarida, neft quvurlari monitoringida keng qo‘llaniladi.

CoAP (Constrained Application Protocol): HTTP ga o‘xshash, lekin UDP ustida va juda kichik sarlavha (4 bayt). Batareya bilan ishlaydigan sensorlar uchun ideal.

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks): IPv6 ni kichik, kam quvvatli qurilmalarda ishlatish imkonini beradi. IEEE 802.15.4 (Zigbee) standartida ishlaydi.

Matter protokoli (2022): Apple, Google, Amazon va Samsung birgalikda ishlab chiqqan aqlli uy qurilmalari standarti. IPv6, Thread va Wi-Fi ustida ishlaydi — turli brendlar qurilmalari bir-biri bilan muloqot qiladi.

SDN va Dasturiy Ta’minot Bilan Boshqariladigan Tarmoqlar

SDN (Software Defined Networking) — tarmoq boshqaruvini (control plane) ma’lumot uzatishdan (data plane) ajratish g‘oyasi. An’anaviy routerlarda ikkala funksiya bir qurilmada joylashgan. SDN da esa markaziy SDN kontroller tarmoqning "miyasi" bo‘lib xizmat qiladi, qurilmalar esa faqat uning ko‘rsatmalarini bajaradi. Bu yondashuv tarmoqni dastur kabi boshqarish, tez yangilash va avtomatlashtirish imkonini beradi. OpenFlow —ng keng tarqalgan SDN protokoli.

Network Function Virtualization (NFV) esa an’anaviy tarmoq funktsiyalari — firewall, load balancer, VPN gateway — ni maxsus hardware o‘rniga oddiy serverda dastur sifatida bajarish imkonini beradi. Bu operator xarajatlarini keskin kamaytiradi.

Xulosa

TCP/IP protokollar to‘plami yetmish yillik tarixga ega bo‘lishiga qaramay, nafaqat o‘z ahamiyatini yo‘qotmagan, balki jahon iqtisodiyoti va madaniyatining asosiy infratuzilmasiga aylangan. Bu uning dizayn falsafasining g‘alabasi — qatlamlilik, ochiqlik, "best-effort" printsipi va "uch uchlarida aql" (end-to-end) konsepsiyasi texnologik inqiloblarga bardosh berdi.

Ushbu tadqiqot natijasida quyidagi asosiy xulosalar chiqarildi: birinchidan, TCP ning oqim nazorati va tiqilinchni boshqarish algoritmlari Internetning "o‘z-o‘zini tartibga solish" qobiliyatini ta’minlaydi — markazlashtirilgan nazorat bo‘lmay turib

milliardlab qurilmaning hamjihatligi shu mexanizmlar orqali ta’minlanadi. Ikkinchidan, DNS ierarxiyasi — ildizdan autentifikativ serverlargacha bo‘lgan zanjir — Internetning nom tizimini boshqarish uchun ajoyib miqyoslanuvchi (scalable) yechim bo‘ldi.

Uchinchidan, IPv6 ga o‘tish zaruriyati nafaqat texnik, balki geosiyosiy muammodir. IPv4 manzillari Osiyo va Afrika da yanada tezroq tugab borayotgani, bu hududlardagi raqamli rivojlanishga to‘siq bo‘lmoqda. To‘rtinchidan, QUIC va HTTP/3 ning paydo bo‘lishi ko‘rsatadiki, TCP/IP arxitekturasi yangi protokollarga mo‘ljallangan: QUIC UDP ustida TCP ning funksiyalarini bajaradi, ya’ni mavjud infratuzilmadan foydalanib tubdan yangi yondashuv taqdim etadi.

Amaliy tavsiyalar sifatida quyidagilar ilgari suriladi. Tarmoq muhandislari uchun: IPv6 dual-stack ni bugun joriy etish — bu ertangi muammodan hozir qutulish. Dasturchilar uchun: HTTP/3 va QUIC ni qo‘llab-quvvatlash, TLS 1.3 va zamonaviy cipher suitlaridan foydalanish. Tizim ma’murlar uchun: DNS over HTTPS va DNSSEC ni faollashtirish, tarmoq monitoringida NetFlow va sFlow protokollarini qo‘llash.

Kelajakka nazar solsak, 6G tarmoqlari (2030 yillar), kvant kommunikatsiyasi va sun’iy intellekt bilan boshqariladigan tarmoqlar yangi protokol paradigmalarini talab qiladi. Biroq hozirgi TCP/IP ning tamoyillari — modulyarlik, ochiqlik va tarqatilgan arxitektura — bu kelajak protokollarining ham asosini tashkil etishi muqarrar. Vint Serfning so‘zlari bilan aytganda: "Biz Internetni qurishda uning bugungi ko‘lamini tasavvur ham qilmagan edik — lekin uni kengayishi uchun mo‘ljallagan edik."

Foydalanilgan adabiyotlar

1. Olimov O. O., Saparbayev R. K. Network traffic queue analysis //Educational Research in Universal Sciences. – 2024. – T. 3. – №. 2. – p. 311-318.
2. N.Y. Ye, R.K. Saparbaev, I.I Omonov . A brief review of machine learning algorithms O‘zbekistonda Fanlararo Innovatsiyalar va Ilmiy Tadqiqotlar Jurnali, 2 (15) (2023), pp. 411-417.
3. Saparbaev Rakhmon, Analog to digital conversion process by matlab simulink // Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali ISSN 2181-4252 Tom: 1 | Son: 4 | 2023-yil.

4. Umarovich, I. U., Mukhammadyunusovich, K. M., Rustambekovich, D. L., & O‘G‘Li, N. R. M. (2020). Methods of reducing the probability of signal loss on optical fiber communication lines. Наука, техника и образование, (6 (70)), 27-31.

5. Salimjon, O., Juraev, N., & Khalilov, M. (2019). Creation of photodetectors based on film heterostructure p–membranous CdTe–ZnSe C deep impurity levels. Euroasian Journal of Semiconductors Science and Engineering, 1(3), 6.

6. Azamat o‘g‘li, K. J., & Xalilov, M. M. (2026). IoT protokollari va tarmoqlari iot qurilmalarining aloqa protokollari va tarmoq texnologiyalari. Zamonaviy taraqqiyot va fan: 21-asr yondashuvlari, 5(1), 392-398.

7. Makhmudov, I. A., & Isroiljonova, G. S. (2021). The package multiservice services in NGN. Academic research in educational sciences, 2(6), 989-994.

8. Juraev, N., & Toshpulatov, S. (2025). Design of an optical–digital system for noninvasive detection of myeloblasts. Collection of scientific papers «SCIENTIA», (October 17, 2025; London, England, UK), 264-271.

9. Onarqulov, K., Maxmudova, A., Toshpulatova, F., & Toshpulatov, S. (2025). Noinvaziv usulda mieloblast hujayralarni diagnostika qilish uchun optik raqamli tizim ishlab chiqish. Engineering problems and innovations, 3(3), 6-11.

10. Onarkulov, K., Juraev, N., Toshpulatova, F., & Toshpulatov, S. Analysis OF the Diagnostic Effectiveness OF Infrared Spectroscopy AND Traditional Laboratory Methods in Early Diagnosis. Grail of Science, (57), 806-812.

11. АХМЕДОВ, Х., & ДАЛИБЕКОВ, Л. (2026). Актуальные вопросы общества, науки и образования. Москва, 2, 10-12.

12. АХМЕДОВ, Х., & ДАЛИБЕКОВ, Л. (2026). Наука сегодня: актуальные вопросы теории и практики. Москва, 2, 8-10.

13. Rustambekovich, D. L. (2025). Raqamli tasvirlarni qayta ishlashda shovqinni kamaytirish usullar. Tadqiqotlar, 76(4), 347-352.

14. Далибеков, Л. (1839). Исследование аномальных фото напряжений как индикаторов сетевых проблем. In Conference on Digital Innovation:" Modern Problems and Solutions". извлечено от https://fer-teach. uz/index. php/codimpas/arti cl e/vi ew.

15. Ergasheva, M. (2026, March). Ma’lumotlarni integratsiyalash algoritmlari asosida konveyer tizimlarida materialni boshqarishni kontaktsiz intellektual olchashni ta’minlash. In International Online Multidisciplinary Conference (pp. 62-64).

16. Ergasheva, M., & Ismoilov, X. (2026, March). Pochta aloqasi xizmat sifatini avtomatlashtirish tizimini shakllantirish. In International Online Multidisciplinary Conference (pp. 32-34).

17. Ergasheva, M. E. (2022). Innovatsion ta’lim texnologiyalari asosida bo‘lajak o‘qituvchilarni ma’naviy axloqiy sifatlarini rivojlantirish. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), (Special Issue 1), 120-124.

18. Madaminov, M. R. (2023). Classification and operating modes of backup energy supply sources of mobile networks. Best Journal of Innovation in Science, Research and Development, 2(12), 32-38.

19. Madaminov, M. R. (2023). Experimental study of operating modes of an uninterruptible power supply source using a wind generator as the primary source. International Journal of Advance Scientific Research, 3(10), 125-131.

20. Madaminov, M. R., & Yuldashev, X. T. (2022). Inverter modeling in improving the energy efficiency of a mobile uninterrupted supply source. International Journal of Advance Scientific Research, 2(11), 77-82.

21. Хосилов, Д. Д., Мадаминов, М. Р., & Йулдашев, Х. Т. (2021). Исследование вольт–амперная характеристика в системе полупроводник–газоразрядный промежуток. Oriental renaissance: Innovative, educational, natural and social sciences, 1(10), 625-634.

22. Muxammadyunusovich, X. M. (2025). Software-defined networking (sdn) va uning kommutatsiya-marshrutizatsiyadagi o‘rni. Ustozlar uchun, 85(4), 128-137.

23. Mahammadjonov, H., Najmiddinov, M., & Xalilov, M. (2026). Axborot va kodlash nazariyasining zamonaviy aloqa tizimlaridagi ahamiyati. Research and Implementation, 4(4/2), 154–156. извлечено от https://rai-journal.uz/index.php/rai/article/view/2935.

24. Xalilov, M., & Raxmatxonov, B. (2026). IPTV va OTT platformalarida media kontentni yetkazib berishda kechikishlarni (latency) kamaytirish usullari. Research and Implementation, 4(4/2), 97–99. извлечено от https://rai-journal.uz/index.php/rai/article/view/2919.

25. Komilov, D. R., & Tajibayev, I. B. (2023). Improving the use of virtual lan (vlan) technology. Web of Discoveries: Journal of Analysis and Inventions, 1(7), 6-11.