IP-MANZILLASH VA MARSHRUTLASH ASOSLARI

Nosirov Mansurjon
Farg‘ona davlat texnika universiteti

Annatatsiya. Ushbu maqola kompyuter tarmoqlarining ikki asosiy tushunchasi — IP-manzillash va marshrutlash — ni ilmiy asosda va keng qamrovda tahlil qiladi. Maqolada IPv4 manzillarining tuzilishi, subnet mask va CIDR notatsiyasi, xususiy va umumiy manzillar kategoriyalari, shuningdek IPv6 ning paydo bo‘lish sabablari va texnik xususiyatlari batafsil yoritilgan. Marshrutlash qismida statik va dinamik marshrutlash usullari, asosiy routing protokollari (RIP, OSPF, EIGRP, BGP), longest prefix match qoidasi va NAT texnologiyasining amaliy roli ko‘rib chiqilgan. VLSM va supernetting orqali IP-manzillardan samarali foydalanish tamoyillari ham o‘z aksini topgan. Maqola kompyuter tarmoqlari sohasini o‘rganuvchi talabalar, tarmoq muhandislari va IT sohasidagi mutaxassislarga mo‘ljallangan bo‘lib, nazariy bilimlarni amaliy misollar bilan mustahkamlashga xizmat qiladi. Manba sifatida IETF RFC hujjatlari va xalqaro darajadagi darsliklar asos qilib olingan.

Kalit so‘zlar: IP-manzil, IPv4, IPv6, subnet mask, CIDR, marshrutlash, routing protokoli, OSPF, BGP, NAT, VLSM.

Kirish

Tasavvur qiling: siz Toshkentdan turib, Nyu-Yorkdagi serverga so‘rov yuboryapsiz. Bu so‘rov atigi bir necha yuz millisekund ichida o‘nlab mamlakatlardan o‘tib, to‘g‘ri manzilga yetib boradi va javob qaytaradi. Bu qanday sodir bo‘ladi? Javob — IP-manzillash va marshrutlash tizimlarida.

Internet bugungi kunda yer yuzidagi eng murakkab muhandislik inshootlaridan biridir. Uning asosida esa ikkita fundamental tushuncha yotadi: har bir qurilmaga yagona manzil berish (IPmanzillash) va ma'lumotlarni to‘g‘ri yo‘nalishda harakatga keltirish (marshrutlash). Ushbu maqolada biz shu ikki tushunchaning mohiyatini, texnik asoslarini va amaliy ahamiyatini chuqur ko‘rib chiqamiz.

IP-Manzil Nima va U Qanday Ishlaydi?

Tarixiy kontekst. Internet Protocol — ya'ni IP — 1970-yillarning boshida ARPANET loyihasi doirasida ishlab chiqilgan. 1981-yilda RFC 791 hujjati orqali rasmiylashtirилган IPv4 standarti o‘sha davrda dunyodagi barcha qurilmalarni qamrab olish uchun yetarli deb hisoblangan. Ammo internet shunchalik tez rivojlandiki, bu manzillar zaxirasi 2011-yilga kelib amalda tugadi — bu holat yangi avlod protokoli IPv6 ning keng joriy etilishiga zamin yaratdi.

IPv4: Klassik manzillash tizimi

IPv4 manzili 32 bitdan iborat bo‘lib, odatda to‘rtta o‘nlik sonni nuqta bilan ajratish orqali ifodalanadi.

Masalan: **192.168.1.1**

Bu to‘rtta son — oktet deb ataladi — har biri 0 dan 255 gacha qiymat olishi mumkin. Demak, nazariy jihatdan IPv4 tizimi taxminan 4,29 milliard (2^{32} = 4 294 967 296) ta unikal manzilni qo‘llab-quvvatlaydi.

Har bir IP-manzil ikki qismdan iborat:

- Tarmoq qismi (Network portion) — qurilma qaysi tarmoqqa tegishli
- ekanligini bildiradi.

Xost qismi (Host portion) — o‘sha tarmoq ichidagi aniq qurilmani belgilaydi.

Bu ikki qism o‘rtasidagi chegara subnet mask (qo‘shimcha tarmoq niqobi) orqali aniqlanadi.

Subnet Mask va CIDR Notatsiyasi

Subnet mask IPv4 manzili bilan birgalikda ishlatiladi va qaysi bitlar tarmoqqa, qaysilari xostga tegishli ekanligini ko‘rsatadi. Masalan:

IP-manzil	Subnet mask	CIDR	Tarmoq manzili
192.168.1.100	255.255.255.0	/24	192.168.1.0
10.0.0.50	255.255.0.0	/16	10.0.0.0
172.16.5.20	255.255.255.128	/25	172.16.5.0

CIDR (Classless Inter-Domain Routing) notatsiyasi 1993-yilda RFC 1519 bilan standartlashtirildi.

Bu tizimda manzil yoniga "/" belgisidan keyin tarmoq qismidagi bitlar soni yoziladi. Masalan, /24 degani — manzilning birinchi 24 biti tarmoqni, qolgan 8 biti esa xostni ifodalaydi. Bu holda bir tarmoqda maksimal 254 ta xost qurilmasi bo‘lishi mumkin (256 manzildan 2 tasini — tarmoq manzili va broadcast manzilini — chiqarib tashlaganda).

IP-Manzillarning Maxsus Kategoriyalari

Barcha IP-manzillar teng yaratilmagan. Ularning bir qismi maxsus maqsadlar uchun ajratilgan:

Xususiy manzillar (Private addresses) — RFC 1918 ga asosan, quyidagi diapazonlar faqat ichki tarmoqlarda ishlatiladi va internetda yo‘naltirilmaydi:

10.0.0.0/8 — yirik korporativ tarmoqlar uchun

172.16.0.0/12 — o‘rta tarmoqlar uchun

192.168.0.0/16 — uy va kichik ofis tarmoqlari uchun

Loopback manzil: 127.0.0.1 — qurilmaning o‘zini sinovdan o‘tkazish uchun. Bu manzilga jo‘natilgan paket hech qayerga bormaydi, faqat o‘sha qurilmaning o‘zida qayta ishlanadi.

Broadcast manzil: Tarmoqdagi barcha qurilmalarga bir vaqtda xabar yuborish uchun ishlatiladi.

Masalan, 192.168.1.255 — 192.168.1.0/24 tarmog‘idagi barcha qurilmalarga murojaat.

Multicast manzillar: 224.0.0.0/4 diapazoni — bir vaqtda bir guruh qurilmalarga ma'lumot yuborish uchun. Video translatsiya va routing protokollarida keng qo‘llaniladi.

IPv6: Kelajak Allaqachon Kelgan

Nima uchun IPv6 kerak bo‘ldi?

2011-yil 3-fevral kuni IANA (Internet Assigned Numbers Authority) oxirgi IPv4 bloklarini regional registrlarga tarqatdi. Bu sanadan boshlab yangi IPv4 manzillarini

olish amalda imkonsiz bo‘lib qoldi. Vaziyatni vaqtincha NAT (Network Address Translation) texnologiyasi yengillashtirgan bo‘lsa-da, uzoq muddatli yechim zarur edi.

IPv6 bu muammoni tubdan hal etdi: u 128 bitli manzillash tizimini joriy qilib, 340 undetsillion ($3{,}4 \times 10^{38}$) ta unikal manzilni ta'minlaydi. Bu raqam yer yuzidagi qum donachalari sonidan ham ko‘p.

IPv6 manzilining tuzilishi

IPv6 manzili sakkizta 16 bitlik guruhdan iborat bo‘lib, ikki nuqta (kolon) bilan ajratiladi:

2001:0 db 8:85 a3:0000:0000:8 a2e:0370:7334

Yozuvni soddalashtirish uchun bir nechta qoida mavjud:

- Har bir guruh boshidagi nollarni tushirib qoldirish mumkin: 0db8 → db8
- Ketma-ket nol guruhlarini :: bilan almashtirish mumkin (faqat bir marta): yuqoridagi

manzil → 2001:db8:85a3::8a2e:370:7334

IPv6 ning afzalliklari

IPv6 nafaqat kattaroq manzil makonini taqdim etadi. Uning arxitekturaviy yangiliklari ham muhimdir:

- IPSec majburiyligi — IPv6 ning asosiy spetsifikatsiyasida xavfsizlik protokollari o‘rnatilgan.
- NAT shart emas — har bir qurilma haqiqiy global manzil olishi mumkin.
- Autoconfiguration (SLAAC) — qurilmalar DHCP serverisiz ham avtomatik manzil olishi mumkin.
- Yaxshilangan multicast — broadcast o‘rniga multicast keng qo‘llaniladi, bu tarmoq yukini kamaytiradi.

Marshrutlash: Ma'lumotlar Yo‘l Topadi

Marshrutlash nima?

Agar IP-manzillash "kimga yetkazish kerak"ni belgilasa, marshrutlash "qanday yo‘l bilan yetkazish kerak"ni aniqlaydi. Marshrutlash — bu tarmoqlar orasida ma'lumot paketlarini to‘g‘ri yo‘nalishda uzatish jarayoni.

Bu jarayonni amalga oshiradigan qurilma router (marshrutizator) deb ataladi. Router har bir kelgan paketni ko‘rib chiqib, uning manzilini o‘zining marshrutlash jadvaliga (routing table) solishtirib, keyingi yo‘nalishni belgilaydi.

Marshrutlash jadvali

Marshrutlash jadvali routerning "xaritasi"dir. U quyidagi asosiy ustunlarni o‘z ichiga oladi:

Tarmoq manzili	Subnet mask	Gateway (keyingi hop)	Interfeys	Metric
192.168.1.0	/24	Directly connected	eth0	0
10.0.0.0	/8	172.16.0.1	eth1	10
0.0.0.0	/0	203.0.113.1	eth2	20

Oxirgi qator — 0.0.0.0/0 — "default route" (standart yo‘l) deb ataladi. Router boshqa mos yozuvlarni topolmagan taqdirda barcha paketlarni shu yo‘nalishga yuboradi. Uy routerlarida bu odatda internet provayderiga olib boruvchi yo‘l bo‘ladi.

Marshrutlash turlari

Marshrutlash ikki asosiy usulda amalga oshiriladi:

Statik marshrutlash (Static routing) — tarmoq administratori yo‘llarni qo‘lda kiritadi. Bu usul kichik, o‘zgarmaydigan tarmoqlar uchun mos, ammo katta tarmoqlarda boshqarish qiyinlashib ketadi.

Dinamik marshrutlash (Dynamic routing) — routerlar bir-biri bilan ma'lumot almashib, tarmoq topologiyasini avtomatik o‘rganadi va yo‘nalishlarni yangilab turadi. Agar tarmoqda biror aloqa uzilsa, dinamik routing protokollari alternativ yo‘lni topadi.

Marshrutlash protokollari

Dinamik marshrutlash uchun turli xil protokollar ishlab chiqilgan. Ularni ikkita asosiy guruhga bo‘lish mumkin:

IGP (Interior Gateway Protocols) — bir tashkilot ichidagi tarmoqlar uchun:

- RIP (Routing Information Protocol) — eng sodda protokollardan biri. "Distance vector" algoritmiga asoslanadi: har bir router qo‘shnilariga o‘z jadvalini

yuboradi. Maksimal 15 hop cheklovi bor, bu esa katta tarmoqlarda qo‘llanilishini cheklaydi.

- OSPF (Open Shortest Path First) — RFC 2328 ga asosan standartlashtirilgan. "Link-state" algoritmidan foydalanadi: har bir router butun tarmoqning xaritasini o‘zida saqlaydi va Dijkstra algoritmidan foydalanib eng qisqa yo‘lni hisoblaydi. Katta korporativ tarmoqlarda keng qo‘llaniladi.
- EIGRP (Enhanced Interior Gateway Routing Protocol) — Cisco tomonidan ishlab chiqilgan, ammo keyinchalik RFC 7868 orqali ochiq standartga aylangan. Distance vector va link-state yondashuvlarini birlashtiradi.

EGP (Exterior Gateway Protocols) — turli tashkilotlarning tarmoqlari orasida:

- BGP (Border Gateway Protocol) — RFC 4271 da belgilangan va internetning "orqamuya"si hisoblanadi. Hozirgi kunda dunyodagi barcha yirik internet provayderlar, content delivery networklar va korporatsiyalar BGP orqali bir-biri bilan bog‘langan. BGP "path vector"

protokoli bo‘lib, nafaqat eng qisqa yo‘lni, balki siyosat va tijorat kelishuvlarini ham hisobga oladi.

VLSM va Supernetting

VLSM — Moslashuvchan Tarmoq Bo‘linishi

Variable Length Subnet Masking (VLSM) texnologiyasi tarmoq muhandislariga turli o‘lchamdagi quyi tarmoqlarni yaratish imkonini beradi. Bu IP-manzillar resursidan tejamkorlik bilan foydalanishga yordam beradi.

Misol: sizga 192.168.10.0/24 tarmoqi berildi va siz undan quyidagilarni tashkil etishingiz kerak:

- ta katta bo‘lim: 100 ta xost
- ta o‘rta bo‘lim: 50 ta xost
- 4 ta kichik bo‘lim: 10 ta xost

VLSM yordamida:

192.168.10.0/25 → 126 ta xost uchun (katta bo‘lim)

192.168.10.128/26 → 62 ta xost (birinchi o‘rta bo‘lim)

192.168.10.192/26 → 62 ta xost (ikkinchi o‘rta bo‘lim)

192.168.10.0/28 diapazonlardan kichik bo‘limlar uchun

Supernetting va Route Aggregation

Supernetting — bu bir nechta kichik tarmoqlarni bitta yirik tarmoqda birlashtirish. Bu amaliyot marshrutlash jadvallarini kichraytiradi va routerlarning yuklama hajmini kamaytiradi.

Masalan, quyidagi to‘rtta tarmoqni:

200.10.0.0/24 200.10.1.0/24 200.10.2.0/24 200.10.3.0/24

Bu amaliyot "route summarization" yoki "route aggregation" deb ham ataladi.

NAT: Manzillar Kamligining Muvaqqat Yechimi

NAT nima?

Network Address Translation (NAT) — xususiy IP-manzillarni umumiy (public) manzillarga tarjima qilish jarayoni. RFC 1631 da tavsiflanган bu texnologiya IPv4 manzillarining kamligini bartaraf etishda muhim rol o‘ynadi.

NAT tufayli bitta tashqi IP-manzil orqali yuzlab yoki minglab qurilmalar internetga chiqishi mumkin. Uy yoki ofis routeri xususiy tarmoqdagi barcha qurilmalarning so‘rovlarini o‘z tashqi manzili nomidan yuboradi va javoblarni tegishli qurilmalarga qaytaradi.

NAT turlari

- Static NAT — bitta xususiy manzilni bitta umumiy manzilga doimiy moslashtirish. Server xizmatlarida ishlatiladi.
- Dynamic NAT — xususiy manzillarni umumiy manzillar havzasidan dinamik taqsimlash.

PAT (Port Address Translation) — eng keng tarqalgan usul. Bitta umumiy IP-manzilga turli port raqamlari orqali ko‘plab xususiy manzillarni moslashtiradi. "NAT overload" deb ham ataladi.

NAT ning kamchiliklari

NAT ba'zi muammolarni ham keltirib chiqaradi:

- End-to-end ulanish buziladi — tashqaridan to‘g‘ridan-to‘g‘ri ichki qurilmaga murojaat qilib bo‘lmaydi.
- VoIP va ba'zi P2P ilovalar NAT bilan muammolarga duch keladi.

- Tarmoqni disk raskachka qilish murakkablashadi.

Aynan shu sabablarga ko‘ra IPv6 ning keng joriy etilishi va NAT dan voz kechish uzoq muddatli maqsad hisoblanadi.

Longest Prefix Match: Marshrutlashning Oltin Qoidasi

Routerlar bir paketning manzili bir nechta marshrutlash jadvali yozuvlariga mos kelganda qaysi yo‘lni tanlaydi? Javob: eng uzun prefix match (longest prefix match) qoidasi.

Bu qoidaga ko‘ra, router doimo eng aniq — ya'ni eng uzun subnet maskga ega — yozuvni tanlaydi.

Misol: marshrutlash jadvalida quyidagilar bor:

10.0.0.0/8 → Router A 10.1.0.0/16 → Router B 10.1.1.0/24 → Router C

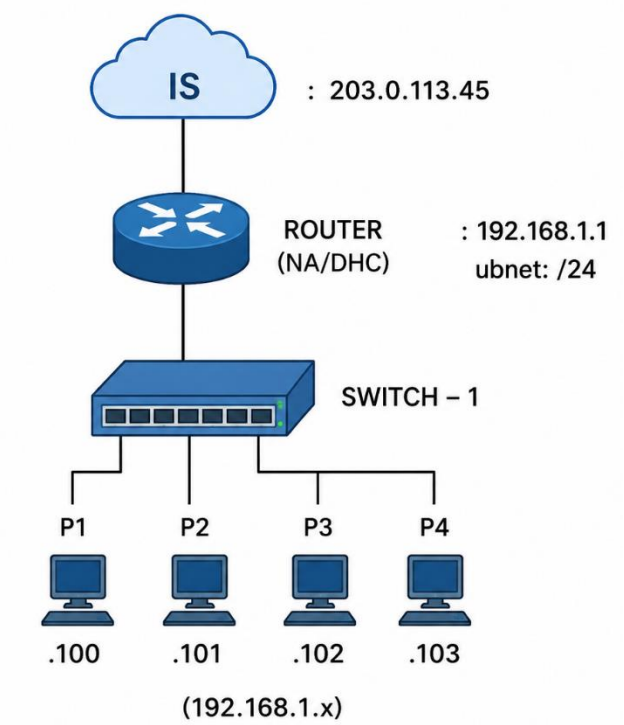
10.1.1.50 manzilga kelgan paket uchun:

/8 mos keladi ✓ /16 mos keladi ✓ /24 mos keladi ✓

Router /24 — eng uzun (aniqroq) match bo‘lgani uchun Router C ni tanlaydi. Bu mantiqiy: qanchalik aniq yo‘l bo‘lsa, shunchalik to‘g‘ri manzilga etib borish ehtimoli yuqori.

Amaliy Misollar va Muhandislik Nuqtai Nazari

Uy tarmog‘i: Oddiy uy tarmog‘ini ko‘rib chiqaylik:



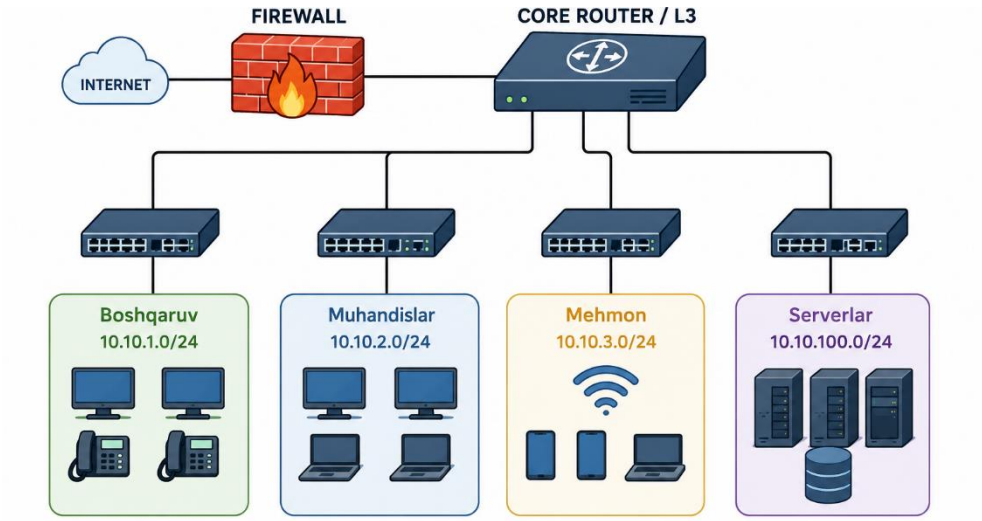
Bu holda router ikki xil manzilga ega:

- WAN interfeysi: 203.0.113.45 — internetga chiqish uchun
- LAN interfeysi: 192.168.1.1 — ichki tarmoq uchun default gateway

Barcha ichki qurilmalar 192.168.1.1 ni gateway sifatida ishlatib, internet so‘rovlarini routerga yuboradi. Router ularni NAT orqali o‘z WAN manzili nomidan tashqariga jo‘natadi.

Korporativ tarmoq: Segmentatsiya

Yirik tashkilotlarda tarmoq xavfsizlik va boshqaruv maqsadida segmentlarga bo‘linadi (VLAN va subnet yordamida):



Bu segmentatsiya tarmoq muhandislariga har bir bo‘lim uchun alohida xavfsizlik siyosatini joriy etish imkonini beradi.

Xulosa

IP-manzillash va marshrutlash — bu shunchaki texnik mavzu emas, balki zamonaviy sivilizatsiyaning asosiy infratuzilmasi. Har kuni milliardlab odamlar tomonidan yuborilayotgan trillionlab paketlar aynan shu tizimlar orqali yo‘l topmoqda.

IPv4 dan IPv6 ga o‘tish jarayoni hali ham davom etmoqda va bu soha mutaxassislari uchun katta imkoniyatlar ochmoqda. Dinamik routing protokollari esa tobora murakkablashayotgan internet muhitida tarmoq barqarorligini ta'minlashning asosiy vositasiga aylangan.

Tarmoq muhandisligini o‘rganuvchi har bir mutaxassis uchun IP-manzillash va marshrutlash asoslarini chuqur tushunish — bu nafaqat imtihon uchun kerakli bilim, balki real muammolarni hal eta oladigan muhandis bo‘lishning zarur sharti. Chunki internet "ishlaydi" deganda, aslida bu minglab routerlar va millionlab marshrutlash qarorlari ortida yashiringan ulkan matematik va muhandislik aqlining natijasidir.

Foydalanilgan adabiyotlar

1. Postel, J. (1981). Internet Protocol. RFC 791. IETF. https://www.rfc-editor.org/rfc/rfc791

2. Rekhter, Y., Li, T., & Hares, S. (2006). A Border Gateway Protocol 4 (BGP-4). RFC 4271. IETF. https://www.rfc-editor.org/rfc/rfc4271

3. Moy, J. (1998). OSPF Version 2. RFC 2328. IETF. https://www.rfc-editor.org/rfc/rfc2328

4. Fuller, V., & Li, T. (2006). Classless Inter-Domain Routing (CIDR): The Internet Address

5. Assignment and Aggregation Plan. RFC 4632. IETF. https://www.rfc-editor.org/rfc/rfc4632

6. Deering, S., & Hinden, R. (2017). Internet Protocol, Version 6 (IPv6) Specification. RFC 8200. IETF. https://www.rfc-editor.org/rfc/rfc8200

7. Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). Address

8. Allocation for Private Internets. RFC 1918. IETF. https://www.rfc-editor.org/rfc/rfc1918

9. Egevang, K., & Francis, P. (1994). The IP Network Address Translator (NAT). RFC 1631. IETF. https://www.rfc-editor.org/rfc/rfc1631

10. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Prentice Hall. ISBN: 978-0-13-212695-3.

11. Forouzan, B. A. (2012). Data Communications and Networking (5th ed.). McGraw-Hill. ISBN: 978-0-07-337622-9.

12. Cisco Systems. (2023). Routing Protocols Configuration Guide. Cisco Press. https://www.cisco.com/c/en/us/tech/ip/ip-routing/index.html