

ЛЕКЦІЯ 2

Протокол IP у глобальних мережах

Технології адресації IPv4 та IPv6

Основна частина лекції

Слайд 2. Пригадаємо лекцію 1 та план лекції 2

Перед тим як зануритись у нову тему, коротко пригадаємо, що ми розглянули на минулій лекції. Ми з'ясували, що WAN — це глобальна мережа на тисячі кілометрів; познайомилися з п'ятьма критеріями класифікації WAN; побачили, що комутація пакетів домінує в сучасних глобальних мережах; розглянули базові топології; ввели важливу концепцію розділення underlay і overlay; та розібрали ієрархію інтернет-провайдерів — Tier 1, 2, 3 — і роль протоколу BGP і точок обміну трафіком IXP.

Сьогодні ми детально розглянемо власне «мову», якою розмовляє Інтернет, — протокол IP. Логіка викладу така: почнемо із загальної ролі IP адреси у мережах; потім розберемо старшу версію — IPv4: формат заголовка, адресний простір, історичні класи; далі перейдемо до наступної версії — IPv6: розглянемо, чому і як її створено, які типи адрес вона підтримує; проведемо систематичне порівняння двох версій; окремо зупинимось на важливих інженерних питаннях — фрагментації, MTU, а також безкласовій адресації CIDR та масках змінної довжини VLSM; і на завершення обговоримо, як відбувається перехід від IPv4 до IPv6 у реальних мережах.

Слайд 3. Роль протоколу IP у глобальних мережах

Отже, почнімо з головного: що таке протокол IP і навіщо він потрібен? Формально, IP — це протокол мережевого, третього рівня моделі OSI, що входить до стеку TCP/IP. Він забезпечує адресацію вузлів і маршрутизацію пакетів у глобальних мережах. Але за цим сухим визначенням стоїть дуже потужна ідея.

Ключова ідея: протокол IP виконує роль універсального «клею», що поєднує різноманітні каналні технології — Ethernet, MPLS, PPP, Frame Relay і десятки інших — у єдину глобальну мережу. Уявіть: ваш ноутбук під'єднаний по Wi-Fi, роутер — по оптиці, магістраль провайдера — по MPLS, підводний

кабель через океан — по DWDM. Кожна з цих технологій має свою логіку роботи, свої заголовки, свої правила. Але поверх них усіх, як універсальний конверт, лежить IP-пакет. Це те, що робить Інтернет Інтернетом — можливість передати дані з будь-якої точки в будь-яку іншу, незалежно від того, які саме каналні технології задіяні на шляху.

На сьогодні паралельно функціонують дві версії IP: IPv4, визначена у стандарті RFC 791 створений ще у 1981 році, і IPv6, визначена у RFC 8200. Обидві версії мають істотні відмінності — за обсягом адресного простору, форматом заголовка, механізмами розширення. І фахівець з комп'ютерної інженерії та кібербезпеки повинен добре знати обидві. Ще одна важлива деталь: IP забезпечує так звану негарантовану дейтаграмну доставку. Це означає, що кожен пакет маршрутизується самостійно, послідовно надіслані пакети можуть іти різними шляхами й прибувати в довільному порядку. Гарантії надійності — це не робота IP, а робота протоколів транспортного рівня, насамперед TCP.

Слайд 4. IPv4: формат заголовка пакета

Тепер деталі. На слайді ви бачите структуру заголовка IPv4-пакета. Довжина заголовка змінна — від 20 до 60 байтів. Мінімум 20 байтів — це коли немає опціональних полів; максимум 60 — коли додано розширення через поле Options. Розберемо ключові поля.

Version — 4 біти, для IPv4 завжди дорівнює 4. Це поле дозволяє мережевим пристроям одразу зрозуміти, з якою версією IP вони працюють. IHL, Internet Header Length — довжина заголовка у 32-бітних словах. Потрібне саме тому, що заголовок змінної довжини — маршрутизатор має знати, де закінчується заголовок і починаються дані. DSCP/ECN — 8 бітів, використовуються для класифікації трафіку та підтримки QoS. Спочатку ці 8 бітів називалися Type of Service, але з розвитком технологій пріоритезації трафіку їх переосмислили: 6 бітів DSCP для маркування класу трафіку, 2 біти ECN для сигналізації про перевантаження.

Total Length — загальна довжина пакета в байтах. Оскільки поле 16-бітне, максимальний розмір IP-пакета — 65 535 байтів. Далі йдуть три поля фрагментації — Identification, Flags, Fragment Offset. Про них окремо

поговоримо на слайді 6. TTL, Time To Live — «час життя» пакета. Це 8-бітове поле, яке кожен маршрутизатор на шляху зменшує на одиницю. Коли TTL досягає нуля — пакет відкидається. Мета — не допустити нескінченної циркуляції пакета в мережі у разі виникнення петлі маршрутизації.

Protocol — 8 бітів, ідентифікатор протоколу верхнього рівня. Значення 6 означає, що всередині IP-пакета — TCP-сегмент; 17 — UDP-датаграма; 1 — ICMP-повідомлення. Header Checksum — контрольна сума заголовка для виявлення пошкоджень. І, нарешті, дві найважливіші IP-адреси — Source Address, адреса відправника, і Destination Address, адреса одержувача, кожна по 32 біти. Саме ці два поля роблять IP протоколом маршрутизації.

Ще раз наголошу на важливому моменті внизу слайда: модель доставки IPv4 — негарантована дейтаграмна передача. Це означає: маршрутизатор може відкинути пакет під час перевантаження, пакети можуть прибути не в тому порядку, деякі можуть загубитися взагалі — і IP-протокол ніяк не намагається це виправити. Виправляти має TCP, який працює вище.

Слайд 5. IPv4: адресний простір та класи

Тепер про адресний простір IPv4 та його історичну структуру. Оскільки адреса IPv4 має довжину 32 біти, загальна кількість можливих адрес — 2 у степені 32, або приблизно 4,3 мільярда. Це дуже велика цифра — але, як показав час, її виявилося недостатньо для сучасного Інтернету з мільярдами підключених пристроїв, серед яких смартфони, розумні годинники, датчики IoT.

Історично, з початку 1980-х років, адресний простір IPv4 поділявся на п'ять класів — A, B, C, D і E. Класи A, B і C — це унікальні одноадресні мережі; клас D — це мультикастові адреси, для розсилок; клас E — зарезервований, ніколи не використовувався для звичайних цілей. Розберемо перші три.

Клас A — це діапазон 1 до 126 у першому байті. Одна мережа класу A містить близько 16 мільйонів адрес. Це надзвичайно багато — така мережа була б надмірною навіть для найбільшої корпорації. Тому мереж класу A виділили дуже мало. Клас B — діапазон 128 до 191, це приблизно 65 тисяч адрес у мережі. Уже прийнятніше, але для середнього підприємства зазвичай забагато. Клас C — діапазон 192 до 223, це лише 254 адреси на мережу — часто

цього недостатньо для середнього підприємства, і доводиться брати кілька мереж.

У чому проблема класової адресації? Проблема — у жорсткості й неефективності. Уявіть організацію, якій потрібно 300 адрес. Клас С — це 254 адреси, недостатньо. Клас В — це 65 тис., надмірно. У результаті організації брали клас В і використовували лише малу частину — а решта адрес просто «пропадала». Такий нерівномірний розподіл швидко призвів до вичерпання адресного простору.

Рішенням стала безкласова адресація CIDR, яку ми детально розглянемо у другій половині лекції. А зараз просто зафіксуємо: сьогодні класи А/В/С у чистому вигляді практично не використовуються. Але їхня спадщина проглядається — наприклад, приватні адресні діапазони RFC 1918, які ви знаєте, — 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 — це, відповідно, історично блок класу А, частина класу В і блок класу С.

Слайд 6. Фрагментація пакетів та MTU

Тепер поговоримо про важливу інженерну тему — фрагментацію пакетів. Щоб зрозуміти, навіщо вона потрібна, треба ввести поняття MTU — Maximum Transmission Unit, максимальний розмір блоку даних, який може бути переданий за одним кадром канального рівня. Кожна канальна технологія має своє значення MTU.

На слайді ви бачите чотири приклади. Ethernet — 1500 байтів. Це стандарт для локальних і більшості глобальних мереж на базі Ethernet. PPP — теж 1500 байтів; це протокол послідовних каналів зв'язку, який ми розглянемо в лекції 5. ATM — 53 байти; це зумовлено фіксованим розміром комірки ATM. I Jumbo frames — 9000 байтів; це збільшений розмір, який використовується у сучасних дата-центрах для покращення продуктивності при передачі великих обсягів даних.

Виникає проблема: маршрутизатор отримує IPv4-пакет розміром, скажімо, 1400 байтів по Ethernet-інтерфейсу, і йому потрібно передати цей пакет далі по інтерфейсу з меншим MTU. Що робити? Ось тут і використовуються поля фрагментації в заголовку IPv4 — Identification, Flags і Fragment Offset. Маршрутизатор розбиває пакет на кілька менших фрагментів, кожен з яких не

перевищує MTU наступного каналу. Всі фрагменти отримують однакове значення Identification — щоб отримувач знав, що вони належать до одного оригінального пакета; Fragment Offset вказує позицію фрагмента в оригінальному пакеті; а прапорець MF (More Fragments) — чи є ще фрагменти після цього.

Проблема фрагментації: вона суттєво збільшує навантаження на мережу. Кожен фрагмент — це окремий пакет зі своїм заголовком, отже, накладні витрати зростають. Гірше того, якщо втратився хоча б один фрагмент, отримувач не може зібрати оригінальний пакет — і треба повторно передавати весь пакет цілком. Це неефективно.

Тому сучасна практика — не фрагментувати пакети, а знайти оптимальний розмір заздалегідь. Для цього використовується механізм Path MTU Discovery, PMTUD, визначений у RFC 1191. Як він працює? Відправник виставляє в кожному IP-пакеті прапорець DF — Don't Fragment. Це говорить маршрутизаторам: не фрагментувати, а якщо не вміщається — відкинути пакет і повідомити відправника. Маршрутизатор, який стикається з такою ситуацією, відкидає пакет і відсилає ICMP-повідомлення «Fragmentation Needed» або в IPv6 — «Packet Too Big», вказуючи максимально дозволений MTU. Відправник отримує це повідомлення, зменшує розмір своїх пакетів і намагається знову. У результаті через кілька спроб визначається реальний MTU шляху, і далі всі пакети йдуть без фрагментації.

У IPv6, як побачимо далі, фрагментація суттєво спрощена: транзитні маршрутизатори взагалі не мають права фрагментувати пакети. Це роблять тільки вузли-відправники. Такий підхід прискорює обробку пакетів у ядрі мережі — маршрутизатору не потрібно займатися складною логікою фрагментації.

Слайд 7. IPv6 — нове покоління IP-протоколу

Переходимо до IPv6 — сучасної версії протоколу IP, визначеної в стандарті RFC 8200. Головна причина створення IPv6 — вичерпання адресного простору IPv4. Робота над новим протоколом розпочалася ще на початку 1990-х років, коли стало зрозуміло, що при темпах зростання Інтернету 4,3 мільярда адрес вичерпаються дуже швидко. Спочатку його називали IPng — IP next generation.

Прогнози справдилися: у лютому 2011 року офіційно вичерпалися вільні IPv4-адреси у IANA — центральному розподільнику; після цього регіональні реєстри — RIPE NCC для Європи, ARIN для Америки — почали поступово вичерпувати свої запаси.

Головна відмінність IPv6, яку ви бачите ліворуч на слайді: довжина адреси — 128 бітів, тобто 16 байтів. Це в чотири рази більше за IPv4. Але кількість можливих адрес зростає не в чотири рази, а в 2 у степені 96 разів — це приблизно 3,4 помножити на 10 у 38-му степені адрес. На 96 порядків більше за IPv4. Це справді астрономічна цифра — деякі автори жартують, що кожному атому на планеті можна виділити власну IPv6-адресу.

Запис IPv6-адрес суттєво відрізняється від IPv4. Замість десяткової нотації з крапками використовується шістнадцяткова нотація, де кожен 16 бітів (4 шістнадцяткові цифри) розділяються двокрапкою. Приклад бачите внизу: 2001:0db8:0000:0000:0000:0000:0000:0001. Оскільки такі адреси незручні, дозволено скорочення: провідні нулі в кожній групі можна опустити, а найдовшу послідовність нульових груп можна замінити подвійною двокрапкою. Тому та ж адреса скорочено записується як 2001:db8::1 — це та сама адреса. Важливе правило: подвійну двокрапку можна використати лише один раз в адресі — інакше буде неоднозначно, скільки нульових груп замінено.

Але IPv6 — це не просто більше адрес. Це комплексне переосмислення протоколу для нових реалій. На правій частині слайда — головні причини його створення й переваги: мільярди пристроїв IoT потребують адрес; вбудований IPsec забезпечує безпеку прямо на рівні протоколу — не як опція, а як стандартна частина; фіксований заголовок дозволяє швидшу апаратну обробку; і відсутність NAT — це повернення до справжньої end-to-end зв'язності, коли будь-який пристрій може напряму спілкуватися з будь-яким іншим.

Слайд 8. Структура глобальної адреси IPv6

Розглянемо, як побудована глобальна унікальна адреса IPv6, або Global Unicast Address. Її 128 бітів логічно поділені на чотири рівні ієрархії. На діаграмі показано три основні частини.

Перша частина — префікс глобальної маршрутизації, зазвичай 48 бітів. Він виділяється провайдером, і саме він визначає, куди в глобальному Інтернеті маршрутизуватиметься трафік. Ієрархія розподілу така: IANA виділяє великі блоки регіональним інтернет-реєстрам (для Європи це RIPE NCC), ті виділяють блоки локальним інтернет-реєстрам (LIR) — тобто провайдерам, а провайдери вже виділяють префікси /48 своїм клієнтам. Тобто організація зазвичай отримує від провайдера префікс типу 2001:db8:1234::/48.

Друга частина — ідентифікатор підмережі, 16 бітів. Це кількість, якою організація може розпоряджатися самостійно для внутрішнього поділу на підмережі. 16 бітів — це до 65 536 різних підмереж або VLAN у межах однієї організації. Для більшості це надмірно, і це чудово — можна структурувати мережу за будь-якою логікою: за поверхами, відділами, типами трафіку — не турбуючись про економію адрес.

Третя частина — ідентифікатор інтерфейсу, 64 біти. Він унікально ідентифікує пристрій у межах підмережі. 64 біти — це приблизно 18 квінтильйонів адрес у кожній підмережі. Цей величезний простір дозволяє автоматично формувати ідентифікатор інтерфейсу з MAC-адреси мережевої карти за алгоритмом EUI-64 — це так звана автоконфігурація без збігів. З міркувань приватності частіше використовують випадкові ідентифікатори — це визначено у стандарті RFC 8981, Privacy Extensions.

І ще важлива концепція: у IPv6 стандартна довжина префікса підмережі — це /64. Тобто типовий запис адреси мережі виглядає як 2001:db8:1234:5678::/64 — де перші 64 біти визначають підмережу, а наступні 64 — ідентифікатор інтерфейсу.

Слайд 9. Три типи адрес IPv6

У IPv6 визначено три основні типи адрес: unicast, multicast та anycast. Це принципова відмінність від IPv4, у якому були unicast, multicast і broadcast — а в IPv6 broadcast'a немає взагалі. Розберемо кожен тип.

Unicast — індивідуальна адреса, ідентифікує один конкретний інтерфейс. Пакет, надісланий на unicast-адресу, доставляється саме цьому одному інтерфейсу. Це звичайна адреса хоста, з якою ми маємо справу найчастіше.

Класичний приклад — коли ваш браузер підключається до сервера сайту: використовується unicast-адреса цього сервера.

Multicast — групова адреса. Вона ідентифікує групу інтерфейсів, і пакет, надісланий на неї, доставляється всім членам групи. Multicast адреси у IPv6 починаються з ff00::/8. Особливо важливі системні мультикастові адреси. Наприклад, ff02::1 — це група «всі вузли на локальному каналі». Якщо потрібно доставити повідомлення всім пристроям у сегменті — надсилаємо на ff02::1, і його отримають усі. Це, до речі, і є заміна колишнього broadcast'a у IPv4. Ще один приклад: ff02::2 — це «всі маршрутизатори на локальному каналі», використовується протоколом Neighbor Discovery для пошуку маршрутизаторів.

Anycast — це найцікавіший, «розумний» тип адреси. З точки зору структури й запису anycast-адреса виглядає точнісінько як unicast. Але вона одночасно призначена кільком інтерфейсам, зазвичай розташованим у різних географічних локаціях. Пакет, надісланий на anycast-адресу, доставляється лише одному з цих вузлів — тому, який найближче до відправника за метрикою маршрутизації. Так працюють, наприклад, кореневі DNS-сервери Інтернету — від А до М. Кожен з них насправді реалізований десятками фізичних серверів по всьому світу, які мають одну й ту ж anycast-адресу. Коли ваш DNS-запит іде до сервера F, він потрапляє на найближчу до вас копію — з мінімальною затримкою. Anycast також широко використовується для балансування навантаження в CDN — мережах доставки контенту типу Cloudflare.

І окремо про спеціальні адреси IPv6 — унизу слайда чотири найважливіші. Link-local адреси, префікс fe80::/10 — це адреси, які автоматично призначаються кожному інтерфейсу і дійсні лише в межах одного канального сегмента. Кожен пристрій з увімкненим IPv6 має link-local адресу — це база для роботи протоколів пошуку сусідів. Unique local, префікс fc00::/7, переважно fd00::/8 — це аналог приватних адрес RFC 1918 з IPv4, призначені для внутрішніх мереж, не маршрутизуються в глобальному Інтернеті. Адреса ::1 — це loopback, аналог 127.0.0.1, для локальних з'єднань всередині одного пристрою. І адреса :: (просто дві двокрапки без нічого) — це невизначена адреса, аналог 0.0.0.0.

Слайд 10. Заголовок IPv6 та Extension Headers

Тепер про заголовок IPv6. Ліворуч на слайді ви бачите структуру: заголовок IPv6 має фіксовану довжину 40 байтів — і це принципова відмінність від IPv4 з його змінною довжиною 20–60 байтів. Спрощення заголовка — це усвідомлене архітектурне рішення. Фіксована довжина дозволяє маршрутизаторам обробляти пакет швидше, бо позиція наступного заголовка завжди відома і немає потреби парсити змінні поля.

Заголовок IPv6 містить вісім полів. Version — 4 біти, значення 6. Traffic Class — 8 бітів, аналог поля DSCP/ECN з IPv4, використовується для QoS. Flow Label — 20 бітів, це нове поле, якого не було в IPv4. Воно дозволяє позначати потік пакетів з однаковими вимогами до обробки — наприклад, усі пакети одного відеозв'язку. Маршрутизатори можуть використовувати Flow Label для швидкого прийняття однакових рішень для всіх пакетів одного потоку без глибокого аналізу.

Payload Length — 16 бітів, довжина корисного навантаження (не включаючи основний заголовок). Next Header — це найцікавіше поле, до нього повернемося за хвилину. Hop Limit — 8 бітів, аналог TTL з IPv4. Source Address і Destination Address — по 128 бітів кожна.

На панелі праворуч показано, що вилучено з IPv4 порівняно з IPv6. Поле IHL — не потрібне, бо заголовок фіксованої довжини. Поля Identification, Flags, Fragment Offset — не в основному заголовку; фрагментація винесена в окремий розширений заголовок. Header Checksum — прибрано, бо контроль цілісності забезпечують канальний рівень (наприклад, CRC у кадрі Ethernet) і транспортний рівень (наприклад, checksum у TCP). Постійно перераховувати контрольну суму на кожному маршрутизаторі при зменшенні TTL — це витрата ресурсів, від якої відмовились.

Тепер про механізм Extension Headers — заголовків розширення. Замість опціональних полів у заголовку, як було в IPv4, у IPv6 використовується ланцюжок окремих заголовків. Поле Next Header в основному заголовку вказує на тип наступного заголовка. Це може бути один із стандартних заголовків розширення: Hop-by-Hop Options — обробляється кожним маршрутизатором на шляху; Routing — визначає шлях через задані проміжні вузли (аналог source routing з IPv4); Fragment — для фрагментації; Authentication Header і

Encapsulating Security Payload — для механізмів IPsec; Destination Options — для одержувача. Кожен наступний заголовок теж має власне поле Next Header, і так формується ланцюжок аж до заголовка транспортного рівня — TCP або UDP.

І ще раз наголошу на принципово важливому: фрагментацію в IPv6 виконує лише вузол-відправник. Транзитні маршрутизатори у IPv6 не мають права фрагментувати пакети — якщо пакет не вміщається, вони його просто відкидають і надсилають ICMPv6-повідомлення «Packet Too Big». Це змушує використовувати PMTUD, про який ми говорили. Такий підхід прискорює обробку пакетів у ядрі мережі.

Слайд 11. Порівняння IPv4 та IPv6

Тепер зведемо все, що дізналися, у порівняльну таблицю. Це Таблиця 3.1 з навчального посібника. Пройдемо по ключових рядках.

Довжина адреси: 32 біти проти 128 бітів. Адресний простір: 4,3 мільярда проти 3,4 помножити на 10 у 38-му. Заголовок: 20–60 байтів змінної довжини проти 40 байтів фіксованої. Фрагментація: у IPv4 виконують і маршрутизатори, і хости; у IPv6 — тільки хости.

Контрольна сума заголовка: у IPv4 є, у IPv6 — немає. Broadcast: підтримується в IPv4, замінений мультикастом у IPv6. IPsec: у IPv4 опціональний, у IPv6 — вбудований, рекомендований до використання, хоч на практиці й не завжди застосовується. Автоконфігурація: у IPv4 — через DHCP-сервер; у IPv6 є новий механізм SLAAC — Stateless Address Autoconfiguration, коли вузол сам генерує собі адресу без централізованого сервера, використовуючи інформацію від найближчого маршрутизатора. Це принципово нова можливість — plug and play на рівні мережі.

NAT — це, мабуть, найважливіша практична відмінність. У IPv4 NAT став необхідністю через нестачу адрес — саме тому у вас удома роутер має одну публічну адресу і роздає внутрішні приватні адреси всім вашим пристроям. У IPv6 адрес настільки багато, що NAT просто не потрібен. Це повертає нам концепцію справжньої end-to-end зв'язності — кожен пристрій може напряму спілкуватися з кожним, без «посередників» типу NAT. Це і плюс, і мінус: з одного боку, спрощує роботу P2P-протоколів, WebRTC, серверів у домашній

мережі; з іншого — вимагає ретельнішого підходу до безпеки, бо кожен пристрій прямо доступний з Інтернету.

І, нарешті, поле Flow Label у IPv6, якого не було в IPv4 — 20 бітів для позначення потоків трафіку, що спрощує роботу з QoS.

Головна ідея, що IPv6 — це не «просто більше адрес». Це комплексне переосмислення протоколу для мереж XXI століття.

Слайд 12. CIDR — безкласова адресація

Тепер переходимо до однієї з найважливіших практичних тем — CIDR та VLSM. Це те, що ви безпосередньо використовуватимете на лабораторних роботах.

CIDR — Classless Inter-Domain Routing — безкласова міждоменна маршрутизація, визначена у стандарті RFC 4632. Основна ідея CIDR — відмова від жорсткого поділу адресного простору на класи фіксованого розміру. Замість класів A/B/C з фіксованою межею на 8, 16 або 24 бітах, CIDR дозволяє встановлювати межу між мережевою і хостовою частиною адреси в будь-якій позиції.

Це виражається у вигляді нотації з косою рисою. Наприклад, запис 192.168.10.0/22 означає мережу з 22-бітним префіксом. Тобто перші 22 біти адреси — це номер мережі, а решта 10 бітів — номер хоста в цій мережі. Скільки це дає адрес? 2 у степені $10 = 1024$. Це вдвічі більше, ніж давав клас C (256 адрес), але вчетверо менше, ніж клас B (65 536). Тобто CIDR дозволяє точно підбирати розмір мережі під реальні потреби.

Ключова перевага CIDR — можливість агрегації маршрутів, її ще називають *supernetting*. Це процес заміни кількох окремих маршрутних записів одним узагальненим. Приклад бачите на слайді праворуч: чотири мережі — 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 — можна агрегувати в один маршрут 192.168.0.0/22. Замість чотирьох записів у таблиці маршрутизації — один. Це істотно зменшує розмір таблиць маршрутизації магістральних маршрутизаторів.

Наскільки це важливо? Погляньте на нижню частину слайда — станом на 2024–2025 роки глобальна BGP-таблиця в Інтернеті містить понад 950 000

IPv4-префіксів. Без CIDR і агрегації ця цифра була б у мільйони або десятки мільйонів — обладнання магистральних маршрутизаторів просто не витримало б такого навантаження. Кожен маршрутизатор Інтернету зберігає повну таблицю BGP в оперативній пам'яті, і чим більше префіксів — тим більше пам'яті потрібно, тим повільніше йде пошук маршрутів.

Ще одна важлива умова — ієрархічність розподілу. Щоб агрегація працювала, суміжні адресні блоки повинні виділятися одному провайдеру або організації. Ієрархія розподілу така: IANA — це центральний орган — виділяє великі блоки регіональним інтернет-реєстрам, RIR. Для Європи це RIPE NCC, для Північної Америки — ARIN, для Азії — APNIC. Далі RIR виділяють блоки локальним інтернет-реєстрам, LIR — це, як правило, великі провайдери. І вже LIR розподіляють адреси кінцевим клієнтам. За такої ієрархії суміжні адреси природно потрапляють до одного власника, і агрегація стає можливою.

Слайд 13. VLSM — маски змінної довжини

Тепер про VLSM — Variable Length Subnet Mask, маски змінної довжини. Це техніка, яка тісно пов'язана з CIDR, але вирішує внутрішнє завдання організації — ефективний поділ виділеного адресного блоку на підмережі різного розміру.

До впровадження VLSM протоколи маршрутизації типу RIPv1 вимагали, щоб у межах однієї мережі всі підмережі мали однакову маску. Це призводило до значних втрат адрес — якщо у вас є одна велика підмережа на 500 хостів і десять маленьких на 2 хости кожна, всі вони мали б мати однакову маску, розраховану на найбільшу з них. VLSM дозволяє використовувати різні маски для різних підмереж — точно під реальні потреби.

Розберемо конкретний приклад, показаний на діаграмі і в таблиці справа. Уявіть, організація отримала мережу 10.1.0.0/16 — це 65 534 адреси (загальний розмір мінус адреса мережі і broadcast). Організація має різні підрозділи: головний офіс — 500 хостів; два регіональні офіси — по 120 хостів; п'ять філій — по 25 хостів; і десять з'єднань point-to-point між маршрутизаторами — на кожному потрібно лише 2 адреси, для двох кінців каналу.

Як би це виглядало при фіксованій масці /24 (тобто 254 адреси на підмережу)? Для головного офісу на 500 хостів довелося б виділити ДВІ

мережі /24, бо одна не вміщає. Для регіональних, філій і навіть point-to-point — по цілій мережі /24 з 254 адрес. Тобто на кожному point-to-point каналі витрачалося б 252 адреси марно.

Тепер з VLSM. Для головного офісу на 500 хостів беремо маску /23 — це 510 корисних адрес, вміщає. Для регіональних офісів беремо /25 — це 126 адрес, вміщає 120 хостів. Для філій беремо /27 — це 30 адрес, вміщає 25 хостів. І, найголовніше, для point-to-point з'єднань беремо /30 — це рівно 2 корисні адреси, точно потрібна кількість. Внаслідок цього ми ефективно використовуємо адресний простір і залишається великий резерв для майбутнього зростання.

На діаграмі ліворуч ви бачите приклад такого розподілу на базі мережі 192.168.0.0/22: великий офіс отримує 192.168.0.0/23 із 512 адресами; середні офіси — 192.168.2.0/25 і 192.168.2.128/25 по 128 адрес; малі офіси — /27 підмережі; а point-to-point канали — /30. Праворуч на слайді — ієрархічна схема того ж поділу у вигляді дерева, яка показує, як з базового блоку /22 послідовно виділяються підблоки.

Тепер важлива технічна деталь: щоб VLSM працював, протокол маршрутизації повинен передавати інформацію про маску підмережі разом із мережевою адресою. Це так звані classless-протоколи. На нижній панелі слайда — список тих, що підтримують: OSPFv2, IS-IS, EIGRP, RIPv2, BGP-4. І один, який не підтримує — RIPv1. Він передає лише мережеву адресу без маски, тому з ним неможливо мати підмережі різних розмірів. Саме через це RIPv1 вважається застарілим і в сучасних мережах не використовується.

Слайд 14. Механізми переходу від IPv4 до IPv6

Ми з вами розглянули обидві версії протоколу. Але як на практиці відбувається перехід від однієї до іншої? Це не миттєвий процес — Інтернет як глобальна інфраструктура не може одномоментно перейти на IPv6. Тому розроблено кілька механізмів співіснування двох версій. Розглянемо три основні підходи.

Перший підхід — Dual Stack, або подвійний стек. Це найпростіший і рекомендований для більшості випадків метод. Ідея — кожен мережевий пристрій одночасно підтримує обидва протоколи. Кожен інтерфейс має

щонайменше одну IPv4-адресу і одну IPv6-адресу. Коли пристрій хоче встановити з'єднання з якимось сервером, він робить DNS-запит. Якщо DNS повертає запис AAAA — це IPv6-адреса, використовується IPv6. Якщо тільки A — використовується IPv4. Якщо є обидва — використовується той, який швидше встановить з'єднання. Для оптимізації цього вибору використовується механізм Happy Eyeballs, визначений у RFC 8305. Він паралельно ініціює з'єднання обома протоколами і використовує те, яке встановилося раніше, з невеликим пріоритетом на IPv6. Dual Stack — це найпоширеніший підхід для сучасних мереж, бо забезпечує повну сумісність.

Другий підхід — тунелювання. Він використовується, коли IPv6-мережі розділені IPv4-інфраструктурою. Наприклад, у вас є два IPv6-острова, які треба з'єднати через глобальний Інтернет, який ще працює переважно на IPv4. Ідея тунелювання: IPv6-пакет інкапсулюється в IPv4-пакет (як пасажир в конверт) і передається як звичайний IPv4-трафік. На вихідному кінці тунелю IPv4-заголовок знімається, і далі йде «чистий» IPv6-пакет. Існує кілька механізмів: 6to4 — це автоматичні тунелі; 6in4 — ручні; ISATAP — для корпоративних мереж; Teredo — навіть через NAT з UDP-інкапсуляцією.

Третій підхід — трансляція протоколів. Це рішення для випадків, коли одна сторона працює тільки на IPv6, а інша — тільки на IPv4. Основна технологія тут — NAT64, визначена у RFC 6146. Вона працює у парі з DNS64, RFC 6147: DNS64 синтезує AAAA-записи для доменів, що мають лише A-записи, додаючи спеціальний префікс типу 64:ff9b::/96 до IPv4-адреси. А NAT64 перетворює пакети IPv6 у IPv4 і навпаки. Комбінація NAT64/DNS64 використовується у сучасних чисто-IPv6 мережах, наприклад, у мобільних мережах T-Mobile у США.

Слайд 15. Підсумок лекції

Підбиваємо підсумки. За цю лекцію ми з вами покрили шість ключових ідей. Перше: протокол IP — це універсальний «клей» мереж, єдиний мережевий рівень для всіх канальних технологій; існує у двох версіях — IPv4 (RFC 791) і IPv6 (RFC 8200). Друге: IPv4 має 32-бітну адресу і 4,3 мільярда унікальних адрес, змінний заголовок 20–60 байтів, а історична класова адресація застаріла. Третє: IPv6 має 128-бітну адресу і майже безмежний

адресний простір, фіксований заголовок 40 байтів, broadcast скасовано, його роль виконує multicast.

Четверте: IPv6 підтримує три типи адрес — unicast для одного інтерфейсу, multicast для групи, і anycast — розумний механізм доставки до найближчого з групи. П'яте: фрагментація — у IPv4 роблять і маршрутизатори, і хости, у IPv6 — тільки хости; сучасна практика — уникати фрагментації через PMTUD. Шосте: CIDR і VLSM — це фундаментальні технології сучасної адресації, які дозволяють гнучко ділити адресний простір і агрегувати маршрути; без них у нас не було б сучасного Інтернету з понад 950 тисячами префіксів у BGP-таблиці.