

ЛЕКЦІЯ 1

Вступ до глобальних мереж

Класифікація та архітектура WAN

Основна частина лекції

Слайд 3. План сьогоднішньої лекції

Тепер про сьогоднішню лекцію. У нас п'ять логічних блоків, кожен з яких — це відповідь на конкретне запитання. Перший блок: що взагалі таке WAN і чим вона відрізняється від інших типів мереж — LAN, MAN, кампусних мереж. Другий блок: які існують способи класифікації глобальних мереж, і чому їх стільки різних. Третій блок — це вже про архітектуру: топології, віртуальні приватні мережі, концепція розділення на underlay і overlay, і сучасна архітектура SD-WAN. Четвертий блок присвячений операторським мережам — тому, як побудований Інтернет як такий: ієрархія провайдерів, магістральні мережі, точки обміну трафіком. І п'ятий, короткий, — підсумок, де ми зафіксуємо ключові поняття.

Слайд 4. WAN — Wide Area Network

Отже, перше і головне: що таке глобальна мережа? Формальне визначення таке: Wide Area Network, або WAN — це мережа, що забезпечує обмін даними між різними локальними мережами і віддаленими вузлами на великих відстанях. Але за цим сухим формулюванням ховається дуже проста ідея.

Уявіть, що ви відкриваєте на смартфоні відео на YouTube. Ваш телефон під'єднаний до Wi-Fi роутера — це локальна мережа, LAN. Роутер — до кабельного модему провайдера — це вже вихід до міської мережі. А сам YouTube фізично розташований на серверах у США або Європі. І коли ви дивитесь відео, ваш трафік проходить через десятки різних мереж різних власників у різних країнах. Ось цю глобальну «мережу мереж» і забезпечують технології WAN. Найвідоміший приклад глобальної мережі — це, звісно, Інтернет.

Ключова відмінність від LAN — масштаб. Локальна мережа — це один офіс або будинок. WAN — це десятки, сотні або тисячі кілометрів. І цей

масштаб докорінно змінює всі підходи: інші протоколи, інша вартість, інші вимоги до надійності. Локальна мережа Ethernet у вас 'просто працює'; побудова WAN — це складна інженерна та економічна задача, у якій задіяні оператори зв'язку, регулятори, міжнародні угоди.

Слайд 5. Класифікація глобальних мереж — огляд

Оскільки WAN — поняття дуже широке, для зручності класифікації їх ділять за різними критеріями. Ми виділимо п'ять основних, які найчастіше зустрічаються в літературі.

Перший — територіальне охоплення. Це найпростіший критерій: за розміром. Другий — технологія передачі даних: які саме протоколи використовуються — X.25, Frame Relay, MPLS, Ethernet і так далі. Третій — тип комутації: канална, пакетна або віртуальних каналів. Четвертий — форма власності і призначення: публічні, приватні, гібридні мережі. І п'ятий — середовище передачі: оптоволокно, мідь, радіо, супутник.

Важливо розуміти: ці критерії не виключають один одного. Кожна реальна мережа одночасно потрапляє в кілька категорій. Наприклад, Інтернет — це одночасно і публічна WAN за призначенням, і пакетно-комутувана за типом комутації, і гібридна за середовищем — там є і оптика, і бездротові радіоканали останньої милі, і супутникові сегменти. Далі ми пройдемо по кожному критерію окремо.

Слайд 6. За територіальним охопленням

Погляньмо на ієрархію мереж за розміром. На діаграмі бачите шість рівнів — від найменшого до найбільшого. PAN, персональна мережа, — це відстань до 10 метрів: наприклад, ваш ноутбук через Bluetooth під'єднаний до навушників. LAN — до одного кілометра, це офісна або домашня мережа на базі Ethernet 802.3 або Wi-Fi 802.11. CAN, кампусна мережа, — до 5 кілометрів. Класичний приклад — університетський кампус: кілька будівель, зазвичай одна організація, високошвидкісні магістральні з'єднання між корпусами. Далі MAN — міська мережа від 5 до 50 кілометрів. Metro Ethernet і WiMAX — типові технології цього рівня.

І, нарешті, WAN — це вже тисячі кілометрів, країна або континент. Технології — MPLS, SD-WAN, історично Frame Relay. Окремо часом

виділяють GAN — глобальну мережу нового покоління, планетарного масштабу з супутниковим зв'язком. Хочу підкреслити: термін GAN не є формально стандартизованим у документах IETF, ITU чи IEEE. Це радше умовна категорія, яку використовують, коли говорять про такі системи, як Starlink чи OneWeb — низькоорбітальні супутникові сузір'я, що покривають усю поверхню Землі.

І ще одна важлива теза, яку я хочу, щоб ви запам'ятали з цього слайда: чим ширший масштаб мережі, тим складніше нею керувати. Локальна мережа Ethernet — це, як правило, «розгорнув і забув». WAN потребує постійного моніторингу, керування смугою, договорів з операторами, SLA — угод про рівень обслуговування. Про них ми окремо говоритимемо в шостій лекції.

Слайд 7. Ключові відмінності: LAN та WAN

Тепер порівняймо LAN і WAN за конкретними параметрами — це на слайді у вигляді таблиці. Проходжу по кожному рядку.

Географія: LAN — можуть займати будівлю або поверх; WAN — в свою чергу це може бути країна, континент, планета. Відстань між вузлами: у LAN — метри, максимум кілометр; у WAN — десятки і тисячі кілометрів. Швидкість: у сучасній LAN типово 1–100 гігабіт за секунду, і кожен пристрій «свій» гігабіт зазвичай має. У WAN діапазон значно ширший — від скромних кілобіт на секунду в старих технологіях до терабіт на секунду на магістралях провайдерів. Але важливо розуміти: цю смугу ділять багато користувачів одночасно.

Затримка: у LAN це мікросекунди — мілісекунди, у WAN — десятки і сотні мілісекунд, а для супутникового зв'язку — навіть сотні мілісекунд. Це критично важливо для інтерактивних застосунків: голосу, відеозв'язку, ігор. Технології: LAN — це переважно Ethernet 802.3 і Wi-Fi 802.11, дві-три стандартизовані технології, які «розмовляють» між собою. У WAN — цілий зоопарк: MPLS, SD-WAN, Frame Relay, Carrier Ethernet, багато варіантів.

Власник: локальна мережа належить одній організації — школі, компанії, вам особисто вдома. WAN — це майже завжди інфраструктура операторів зв'язку, провайдерів. І, як наслідок, вартість каналу WAN незрівнянно вища.

Купити гігабітний свіч для офісу — це кількасот доларів. А орендувати гігабітний канал між двома містами — це десятки тисяч доларів на рік.

І ще раз повторю ключову думку внизу слайда: складність управління і забезпечення якості обслуговування зростає зі збільшенням масштабу мережі. Тому побудова WAN — це не просто «більша LAN». Це принципово інша інженерна дисципліна.

Слайд 8. Історичний розвиток технологій WAN

Щоб краще розуміти, чому сучасні технології WAN такі, якими вони є, корисно подивитися на еволюцію. На таймлайні бачите ключові віхи.

Все почалося у 1976 році з протоколу X.25 — першої стандартизованої технології пакетної комутації для глобальних мереж. Швидкість — до 64 кілобіт за секунду. Головна перевага X.25 — вбудований механізм виявлення і виправлення помилок на кожному вузлі. Це було критично важливо, бо тодішні аналогові канали зв'язку були дуже шумними. Технологія довго використовувалась у банківських і транспортних системах.

У 1991 з'явилася Frame Relay — до 45 мегабіт за секунду. Це вже було серйозно, і Frame Relay широко використовувалась для об'єднання локальних мереж до початку 2010-х. У 1995 — АТМ, асинхронний режим передачі. Цікава технологія з фіксованим розміром комірки 53 байти, з гарантованою якістю обслуговування. Спочатку її вважали майбутнім телекомунікацій, але з часом вона програла битву IP-технологіям.

У 2001 з'явилася MPLS — і це справжня революція. MPLS поєднав переваги IP-маршрутизації та швидкої комутації на основі міток. І, забігаючи наперед — MPLS досі залишається основною технологією у магістральних мережах операторів. Ми цій тематиці присвяtimo цілу лекцію трохи згодом. Далі — Carrier Ethernet і Metro Ethernet, які принесли швидкості до 100 гігабіт. І сучасний тренд — це SD-WAN та SASE: програмно-визначені мережі з інтегрованою безпекою і хмарними сервісами. Швидкості — 100+ гігабіт, і, головне, зовсім інший підхід до управління.

Отже, тенденція очевидна: швидкості ростуть у мільйони разів за півстоліття, а фокус зміщується з апаратної реалізації на програмну.

Слайд 9. Порівняння технологій глобальних мереж

На цьому слайді — та ж інформація, але у вигляді порівняльної таблиці. Зверну вашу увагу на найважливіше.

По-перше, зверніть увагу на рядок «Рівні OSI». MPLS — єдина технологія, для якої вказано «2.5». Це не жарт: MPLS формально не належить ні до канального рівня (другого), ні до мережевого (третього). Вона працює між ними, використовуючи мітки замість IP-адрес для швидкої пересилки — звідси і назва «technology of layer 2.5». Це важлива концептуальна річ, до якої ми повернемося.

По-друге, подивіться на нижній рядок «Статус» — тут я спеціально виділила кольорами. Червоним — застарілі технології: X.25 і Frame Relay. Ви їх у нових проєктах уже не побачите, але, працюючи з успадкованими системами, іноді ще стикатиметесь. Помаранчевим — ATM, обмежене використання, зберігається у деяких магістралях. Зеленим — MPLS, який широко використовується, і Carrier Ethernet, який швидко зростає.

Загальний тренд, який зарезюмовано внизу: сучасний вибір — це MPLS для операторів та Carrier Ethernet для міських і корпоративних мереж. І понад все — конвергенція з SD-WAN.

Слайд 10. Три типи комутації у WAN

Перейдемо до наступного критерію класифікації — тип комутації. Це фундаментальне поняття. Спосіб, у який мережа встановлює з'єднання між двома точками, визначає майже всі її подальші характеристики: як швидко, наскільки надійно і скільки коштує передавати дані.

Розглянемо на прикладі. На діаграмі — комп'ютер А зліва хоче передати дані комп'ютеру Б справа через мережу з маршрутизаторів.

У випадку комутації каналів — це верхня схема, червона лінія — між А і Б перед початком передачі встановлюється фізичний або логічний канал, який зберігається протягом усього сеансу. Класичний приклад — традиційна телефонна мережа PSTN. Ви набираєте номер — станція «прокладає» канал через комутатори — і поки ви говорите, цей канал вважається зайнятим, навіть якщо ви мовчите. Плюс: гарантована пропускна здатність. Мінус: неефективне використання ресурсу.

Комутація пакетів — це друга схема, з різнокольоровими пунктирами. Дані діляться на невеликі шматки — пакети — і кожен пакет самостійно вирішує, яким шляхом іти. Пакет 1 пішов верхнім маршрутом, пакет 2 — нижнім, пакет 3 — ще іншим. У пункті призначення вони збираються назад у правильному порядку. Це домінуючий підхід у сучасних WAN, зокрема в Інтернеті. Плюс: ефективне використання ресурсу, стійкість до відмов — якщо один канал відмовляє, пакети йдуть іншими шляхами. Мінус: немає гарантій швидкості.

Третій різновид — Комутація віртуальних каналів — це гібридний підхід (наприклад, у мережах ATM або Frame Relay), який поєднує логіку обох методів. Перед передачею даних між А і Б створюється фіксований логічний маршрут (віртуальний канал), яким послідовно йдуть абсолютно всі пакети, але сама лінія зв'язку фізично не монополізується і ділиться з іншими користувачами. Плюс: гарантований порядок доставки пакетів та висока швидкість. Мінус: затримка на створення каналу перед стартом і вразливість — якщо один вузол на шляху «впаде», доведеться перебудовувати весь канал заново..

Отже, у сучасних WAN абсолютно домінує комутація пакетів на основі IP. Комутація каналів залишилася переважно у телефонії, ATM — у нішевих застосуваннях.

Слайд 11. За формою власності та призначенням

Ще один критерій класифікації — форма власності. Всі глобальні мережі діляться на три групи. Публічні мережі — це ті, що належать операторам зв'язку і надають послуги широкому колу користувачів. Найбільша публічна мережа — це, звісно, Інтернет.

Приватні мережі — це мережі, які створюються і експлуатуються окремими організаціями для власних потреб. Приклад — корпоративна мережа великого банку або оборонного відомства, побудована на власних або орендованих виділених каналах. Переваги приватних мереж: повний контроль над інфраструктурою і високий рівень безпеки. Недолік: висока вартість.

Гібридні мережі поєднують елементи публічних і приватних. Найтипівіший приклад — VPN, віртуальна приватна мережа. Коли ви з дому підключаєтеся до корпоративної мережі роботодавця, ви фактично створюєте

зашифрований тунель через публічний Інтернет — і використовуєте публічну інфраструктуру для передачі приватних даних. Ми детально розглянемо VPN у чотирнадцятій лекції.

Крім поділу за власністю, мережі класифікують також за призначенням — це нижня частина слайда. Виділяють мережі загального користування (той самий Інтернет), корпоративні (мережі бізнесу), науково-освітні і мережі спеціального призначення.

На науково-освітніх мережах зупинюся окремо, бо це цікавий приклад. У Європі це GÉANT — загальноєвропейська наукова мережа, яка з'єднує університети і дослідницькі центри понад сорока країн зі швидкостями до кількох терабіт на секунду. У США — Internet2. Ці мережі мають унікальні вимоги: наприклад, передавати гігантські обсяги даних з експериментів CERN або з радіотелескопів. Це те, чого звичайний Інтернет не потягне з розумною ціною.

Слайд 12. Топології WAN

Переходимо до другого великого блоку сьогоднішньої лекції — архітектура WAN. І першою в ньому розглянемо топології — тобто способи з'єднання вузлів мережі.

Тут корисно розрізнити два поняття: фізична топологія — це реальне розташування кабелів і обладнання; логічна топологія — це шляхи, якими передаються дані. Вони можуть не збігатися. Наприклад, у сучасній корпоративній мережі фізично може бути «зірка» — всі філії підключені до центрального дата-центру. А логічно — «повнозв'язна»: у SD-WAN всі філії «бачать» одна одну через віртуальні тунелі-overlay поверх цієї зірки.

На слайді — чотири базові топології. Точка-точка — найпростіша, два пристрої, одне з'єднання. Плюс — гарантована смуга, немає з ким її ділити. Використовується для виділених каналів між критично важливими вузлами.

Зірка, вона ж hub-and-spoke — «втулка і спиці». Центральний вузол-hub, до нього підключені периферійні spoke. Це найпоширеніша топологія в корпоративних WAN — простота управління, легко масштабувати, додаючи нові філії. Мінус — центральний вузол є єдиною точкою відмови.

Повнозв'язна, або full mesh, — кожен вузол напряду з'єднаний з кожним. Максимальна відмовостійкість — навіть якщо кілька зв'язків впадуть, мережа працюватиме. Але зверніть увагу на формулу в правому нижньому куті: у мережі з N вузлами потрібно N в квадраті мінус N поділити на два з'єднань. Тобто зростання квадратичне. Для 5 вузлів це 10 зв'язків, для 10 — вже 45, а для 100 вузлів — 4950. У реальних мережах повнозв'язна топологія використовується тільки на найвищому рівні — між магістральними маршрутизаторами ядра.

І компромісне рішення — частково зв'язна топологія. Прямі з'єднання є тільки між тими вузлами, які інтенсивно обмінюються даними. Це найпоширеніший вибір для великих провайдерських мереж — розумний баланс вартості та надійності.

Слайд 13. Концепція Underlay та Overlay мереж

А тепер — одна з найважливіших концепцій сучасних мереж. Це розділення мережі на два шари: underlay і overlay.

Underlay — це базова, фізична мережа. Реальні кабелі, реальні маршрутизатори, реальні комутатори. Це те, куди можна прийти в машинному залі і буквально помацати рукою. У underlay працюють протоколи IP-маршрутизації: OSPF, IS-IS, BGP. Їхнє завдання — забезпечити базову IP-зв'язність між усіма фізичними вузлами.

Overlay — це логічна мережа, побудована ПОВЕРХ underlay за допомогою механізмів тунелювання та інкапсуляції. Тобто ми беремо пакет і «загортаємо» його в інший пакет, який передається через underlay так, ніби це звичайний трафік. Технології overlay: VPN, VXLAN, GRE, Geneve, MPLS L3VPN.

Найкраща аналогія — з транспортом. Underlay — це дороги: фізична інфраструктура міста. Overlay — це маршрути громадського транспорту, які по цих дорогах ходять. По одних і тих самих дорогах можуть їздити десятки різних маршрутів автобусів. Одна фізична мережа може обслуговувати сотні незалежних overlay-мереж — приватних, ізольованих одна від одної.

Що це дає? По-перше, ізоляцію трафіку різних клієнтів або відділів. По-друге, гнучкість — можна створювати нові логічні мережі без прокладання нових кабелів. По-третє, безпеку — overlay-тунелі шифруються. По-четверте,

незалежність — при заміні фізичного обладнання логічні мережі продовжують працювати.

Ця концепція — фундамент і для VPN, і для SD-WAN, і для сучасних мереж дата-центрів на VXLAN. Ми повернемося до неї у восьмій лекції, коли будемо говорити про транспортну інфраструктуру.

Слайд 14. SD-WAN

Про SD-WAN варто сказати окремо, бо це сучасний магістральний тренд у корпоративних мережах. Аббревіатура розшифровується як Software-Defined WAN — програмно-визначена глобальна мережа.

Ідея SD-WAN у чому. У традиційних мережах керування і передача даних тісно перемішані — кожен маршрутизатор сам приймає рішення про маршрутизацію на основі локальної інформації. У SD-WAN ці дві функції розділяють. З'являється центральний SD-WAN контролер, який має повну картину мережі: стан кожного каналу, завантаженість, затримка, втрати пакетів. І цей контролер централізовано керує потоками трафіку.

Погляньте на схему — типова SD-WAN використовує кілька фізичних з'єднань одночасно. У прикладі це MPLS, широкосмуговий Інтернет і LTE або 4G — тепер уже і 5G. Контролер аналізує стан кожного каналу в реальному часі і динамічно обирає оптимальний маршрут для кожного потоку. Наприклад: голосові дзвінки VoIP — по каналу з найменшим джитером; резервне копіювання файлів — по найдешевшому широкосмуговому інтернету; критичні бізнес-застосунки — по гарантованому MPLS.

Права частина слайда — ключові функції. Централізоване управління через єдину консоль — адміністратор бачить усю мережу і керує нею з одного місця. Динамічна маршрутизація на основі політик — можна написати правило типу «весь трафік до Salesforce йде через LTE, якщо MPLS перевантажений». Автоматичне створення захищених тунелів з шифруванням AES-256 — нам не треба вручну налаштовувати IPsec на кожному пристрої. Zero-touch provisioning — нульова конфігурація на місці: пристрій приходить на нову філію, вмикається, автоматично зв'язується з контролером і отримує всі налаштування.

I — з практичної точки зору — головна економічна перевага: SD-WAN дозволяє замінити частину дорогих MPLS-каналів на дешевий широкосмуговий Інтернет без втрати якості обслуговування. Це реальна економія, тому останні роки десяти SD-WAN дуже активно впроваджується у бізнесі.

Слайд 15. Масштабованість та відмовостійкість WAN

Ще дві критичні характеристики будь-якої WAN — масштабованість і відмовостійкість. Розберемо кожну.

Масштабованість — це здатність мережі рости. Розрізняють горизонтальну масштабованість — додавання нових вузлів у мережу; і вертикальну — збільшення пропускної здатності існуючих каналів. Найкращу масштабованість забезпечує ієрархічна архітектура з трьох рівнів: ядро мережі (core) — потужні магістральні маршрутизатори, рівень розподілу (distribution) — агрегація трафіку від рівня доступу, і рівень доступу (access) — куди підключаються кінцеві користувачі. Ця трирівнева модель — класика мережевого дизайну, її запропонувала Cisco ще у 1990-х, і вона працює й досі.

Відмовостійкість — це здатність мережі продовжувати роботу при відмові окремих компонентів. Досягається кількома способами. По-перше, резервування каналів — до кожного важливого вузла ведуть щонайменше два незалежні маршрути, часто фізично різними шляхами — навіть різними операторами. По-друге, дублювання обладнання — критичні пристрої встановлюють у парі. По-третє, використання протоколів динамічної маршрутизації OSPF і BGP, які автоматично перебудовують шляхи при відмовах — часто за секунди. По-четверте, протоколи резервування першого хопу FHRP — VRRP і GLBP, які ми будемо детально розглядати в дев'ятій і десятій лекціях, і робити практичні лабораторні по них.

I, нарешті — та цифра, яка на слайді: 99,99%. «Чотири дев'ятки». Це цільовий рівень доступності для критичних застосунків. Що це означає у практичних термінах? Це не більше 52,6 хвилини простою на рік. Для порівняння: 99,9% — це вже майже дев'ять годин простою на рік. А для найбільш критичних систем — банкінг, авіа перельоти — цільовий рівень 99,999%, «п'ять дев'яток» — це менше п'яти хвилин простою на рік.

Провайдери гарантують такі показники в SLA — угодах про рівень обслуговування, до яких ми окремо розглянемо в наступних лекціях.

Слайд 16. Ієрархія провайдерів інтернет-послуг ISP

Тепер про операторські мережі — четвертий великий блок лекції. Головне, що я хочу, щоб ви зрозуміли: Інтернет — це не одна централізована мережа. Це радше «мережа мереж» — сотні тисяч автономних систем, що належать різним операторам і з'єднані між собою угодами. І серед цих операторів існує чітка ієрархія трьох рівнів.

На вершині — провайдери першого рівня, Tier 1. Це такі собі «магістральні гіганти» глобального масштабу. Їхня особливість: вони не платять нікому за транзит, а обмінюються трафіком між собою за безкоштовними піринговими угодами. Це елітний «клуб» — увійти туди дуже складно. Приклади: Lumen Technologies (колишній CenturyLink), NTT Communications, Cogent Communications. Їхні магістралі мають пропускну здатність десятки та сотні терабіт за секунду.

Другий рівень, Tier 2 — це регіональні або національні провайдери. Мають велике охоплення в межах країни чи континенту, з деякими Tier 1 мають безкоштовний піринг, але для повного доступу до Інтернету купують транзитні послуги у Tier 1. Приклади: Укртелеком в Україні, Deutsche Telekom у Німеччині, Orange у Франції.

Третій рівень, Tier 3 — це місцеві провайдери. Вони забезпечують так звану «останню милю» — фізичне підключення кінцевих користувачів до Інтернету. Це домашні провайдери у ваших містах, невеликі міські ISP, що дають вам оптичний кабель у квартиру.

У чому практична цінність цієї ієрархії? По-перше, коли ваш пакет іде до сервера на іншому континенті, він, як правило, проходить: ваш Tier 3 → регіональний Tier 2 → Tier 1 → інший Tier 1 → Tier 2 у тій країні → Tier 3 → кінцевий сервер. По-друге, це пояснює економіку Інтернету: гроші за трафік течуть знизу вгору. І, по-третє, ця ієрархія дозволяє Інтернету масштабуватися — кожен рівень бачить лише «своїх» сусідів, ніхто не тримає в голові карту всієї мережі.

Слайд 17. Магістральні мережі та точки обміну трафіком

Тепер — про два ключові елементи інфраструктури: магістралі (backbone) і точки обміну трафіком (IXP).

Магістральна мережа, backbone — це високошвидкісна мережа, яка транспортує дані між великими вузлами глобальної інфраструктури. Фізичну основу складають волоконно-оптичні кабелі з технологією DWDM. Це технологія щільного мультиплексування довжин хвиль — по одному оптичному волокну одночасно передається сигнал на 96 і більше різних довжинах хвиль, кожна зі швидкістю 100–400 гігабіт. Тобто одна фізична оптоволоконна нитка «товщиною з волосину» може передавати десятки терабіт за секунду.

Особливо вражають підводні кабельні системи — це реальна фізична інфраструктура Інтернету, про яку зазвичай ніхто не думає. Наприклад, кабель MAREA з'єднує США та Іспанію через Атлантичний океан, кабель JUPITER — США і Азію через Тихий океан. Їхня пропускна здатність — понад 200 терабіт за секунду. Знищення такого кабелю — а таке час від часу трапляється, найчастіше через кораблі — може відчутно вплинути на роботу Інтернету цілих регіонів.

Згадайте масштабний розрив кабелів у Червоному морі (Березень 2024 та Вересень 2025)

Це були найгучніші інциденти. У першому випадку єменські хусити (або корабель, що затонув після їхньої атаки та тягнув якір) пошкодили одразу 4 ключові підводні кабелі. У вересні 2025 року ситуація повторилася — знову сталася аварія на магістралях у тому ж регіоні. Через комутацію пакетів інтернет не зник, але ми помітили величезні затримки (пінг) в іграх, довге завантаження відео на YouTube, а також глобальні збої в роботі сервісів Microsoft (зокрема Azure та Teams), які активно використовуються в українському бізнесі.

Тепер про IXP — Internet Exchange Point, точка обміну трафіком. Це фізичне місце — зазвичай серверна кімната у дата-центрі — де встановлено обладнання багатьох провайдерів, і вони обмінюються трафіком напряму, а не через транзит через Tier 1. Що це дає? Три речі: зниження затримки — трафік іде коротшим шляхом; зниження вартості — не треба платити за транзит; підвищення надійності — менша залежність від одного каналу.

На слайді — приклади найбільших IXP світу. DE-CIX у Франкфурті — це найбільший у світі IXP з пропускною здатністю понад 14 терабіт за секунду. AMS-IX в Амстердамі — другий за обсягами. LINX у Лондоні — великий європейський вузол. І UA-IX у Києві — найбільша точка обміну трафіком в Україні. Від нормальної роботи UA-IX залежить, наскільки швидко всередині країни між українськими провайдерами передається трафік — і, відповідно, наскільки комфортно нам користуватися українськими сайтами й сервісами.

Слайд 18. Що ми сьогодні дізналися — підсумок

Підбиваємо підсумки. За цю лекцію ми з вами покрили шість ключових ідей — вони на слайді у вигляді картки-шпаргалки. Пробіжимося ще раз коротко по ним.

Перше: WAN — це глобальна мережа, що об'єднує LAN і MAN на відстанях від десятків до тисяч кілометрів. Друге: існує п'ять основних критеріїв класифікації — територія, технологія, комутація, форма власності, середовище передачі. Третє: технології WAN пройшли шлях від X.25 через Frame Relay і ATM до сучасних MPLS і SD-WAN. На сьогодні MPLS домінує в магістралях операторів, а SD-WAN і SASE — новий стандарт для корпоративних мереж.

Четверте: топології мережі — точка-точка, зірка, повнозв'язна, частково зв'язна — визначають баланс між вартістю та надійністю. П'яте: сучасні мережі побудовані на концепції розділення underlay і overlay, що дозволяє гнучко створювати логічні мережі поверх фізичної інфраструктури. І шосте: Інтернет — це ієрархічна структура з провайдерів Tier 1, 2 і 3, з'єднаних піринговими та транзитними угодами. Ключовий протокол, який керує цією ієрархією, — BGP, йому ми присвяtimo цілу лекцію на одному з наступних занять.