ЛЕКЦІЯ 3

Ethernet у мережах операторів

Агрегування каналів EtherChannel

Слайд 2. Пригадуємо лекцію 2 та план лекції 3

Спочатку коротко пригадаємо, що ми розглянули на минулій лекції. Ми з'ясували, що протокол IP — це універсальний «клей» мереж, який об'єднує різнорідні канальні технології. Розглянули дві версії IP: IPv4 з 32-бітною адресою і заголовком змінної довжини 20–60 байтів, та IPv6 з 128-бітною адресою і фіксованим заголовком 40 байтів. Побачили три типи адрес IPv6 — unicast, multicast, anycast; розібрали механізм фрагментації та PMTUD. Останнє — окремо зупинилися на безкласовій адресації CIDR та масках змінної довжини VLSM, які роблять сучасний Інтернет із його понад 950 тисячами префіксів у BGP-таблиці технічно можливим.

Сьогодні ми переходимо на канальний рівень і в новий контекст — операторські мережі. Почнемо з еволюції Ethernet — як він за півстоліття виріс з локальної технології 10 Мбіт/с у магістральну технологію 400 Гбіт/с. Далі — концепція Carrier Ethernet і п'ять атрибутів MEF, які роблять його придатним для операторських мереж. Розберемо три ключові інтерфейси Carrier Ethernet — UNI, NNI та EVC. Далі — три базові послуги MEF: E-Line, E-LAN та E-Tree. І друга частина лекції — уся присвячена EtherChannel: принцип роботи, протоколи LACP та PAgP, алгоритми балансування навантаження, відмовостійкість та концепція Multi-Chassis EtherChannel.

Слайд 3. Еволюція Ethernet від LAN до операторських мереж

Щоб зрозуміти, чому Ethernet сьогодні домінує в операторських мережах, треба подивитися на його еволюцію. Технологія народилася в 1973 році в дослідницькому центрі Xerox PARC як експериментальна система на 3 мегабіти за секунду. У 1983 з'явився офіційний стандарт IEEE 802.3 — 10 мегабіт на секунду по коаксіальному кабелю. Це була суто локальна технологія.

У 1995 стандарт 802.3u — Fast Ethernet, 100 мегабіт на секунду по витій парі, з підтримкою повного дуплексу. У 1998 — Gigabit Ethernet, 802.3z — гігабіт на секунду. Ще донедавна це вважалося магістральною швидкістю. Ключовий момент — 2002 рік, стандарт 802.3ae, 10 Gigabit Ethernet. Це коли Ethernet вперше вийшов ЗА МЕЖІ LAN — почав використовуватися в MAN, метрополітенських мережах, і в WAN, глобальних. Це і стало переломним моментом, коли Ethernet почав конкурувати з традиційним TDM.

У 2010 з'явився 100 Gigabit Ethernet — стандарт 802.3ba, і в 2017 — 400 Gigabit Ethernet, 802.3bs. Сьогодні ці швидкості використовуються в

магістралях найбільших операторів, дата-центрах, транспорті для 5G. Уже стандартизується 800GbE, розробляється і 1.6TbE.

Тепер важливе: чому оператори масово переходять з TDM-технологій (SDH, SONET, Frame Relay, ATM) на Ethernet? Погляньте на верхню частину слайда — там чотири основні причини. Перша — єдина технологія від LAN до WAN. Клієнт має Ethernet у себе в офісі, і оператор надає Ethernet-канал — не потрібно нічого перетворювати. Це спрощує архітектуру і зменшує затримки. Друга — обладнання Ethernet дешевше за TDM у кілька разів при тій же смузі. Це серйозна економія і на CAPEX (закупівлі), і на OPEX (експлуатації). Третя — гнучке масштабування: від 10 мегабіт до 400 гігабіт можна нарощувати швидкість без заміни базової платформи. І четверта — широка екосистема виробників: Cisco, Juniper, Huawei, Arista, HP — усі роблять Ethernet-обладнання. Це створює конкуренцію і знижує ціни. Тоді як TDM-обладнання виробляє обмежене коло постачальників з відповідною ціновою політикою.

Слайд 4. Carrier Ethernet — що це таке

Але щоб Ethernet міг замінити TDM у мережах операторів, його треба було суттєво доопрацювати. Звичайний LAN Ethernet, який ви маєте вдома чи в офісі, не годиться для комерційних телекомунікаційних послуг. Він працює за принципом «best effort» — «найкращих зусиль» — і нічого не гарантує. Пакет може загубитися, затриматися, прийти не в тому порядку — і Ethernet це не турбує.

Ключова ідея сьогоднішньої першої частини лекції ось у чому. Carrier Ethernet — це набір стандартів і специфікацій, які перетворюють традиційну локальну технологію Ethernet на повноцінне рішення операторського класу. Ключове слово тут — «операторського класу», carrier grade. Це означає рівень надійності, масштабованості й якості обслуговування, які раніше давали тільки SDH і SONET.

Стандартизацію Carrier Ethernet здійснює міжнародна галузева організація, яка називається Metro Ethernet Forum, або MEF. Вона заснована у 2001 році і зараз об'єднує понад 200 членів — це оператори зв'язку, виробники обладнання, системні інтегратори з усього світу.

Погляньте на три картки внизу слайда — вони показують, де саме Carrier Ethernet знаходиться між традиційним LAN Ethernet і TDM-мережами SDH/SONET. Ліворуч — LAN Ethernet: доставка best effort, немає QoS, STP-конвергенція десятки секунд, домен зазвичай одна організація. Праворуч — SDH/SONET (TDM): гарантована смуга завжди, але жорсткі TDM-канали, дуже дороге обладнання. І в центрі — Carrier Ethernet: SLA-гарантії доступності 99,999%, вісім класів QoS, кільцевий захист ERPS з переключенням менше 50 мілісекунд, мільйони EVC і MAC-адрес у одному

домені. Це і є «золота середина»: дешевизна й простота Ethernet плюс надійність TDM.

Слайд 5. П'ять атрибутів Carrier Ethernet за MEF

MEF визначає п'ять ключових атрибутів, яким має відповідати мережа, щоб класифікуватися як Carrier Ethernet. Розберемо кожен з них.

Перший атрибут — стандартизовані сервіси. Мережа повинна підтримувати стандартні типи послуг, визначені MEF — E-Line, E-LAN, E-Tree, E-Access — з чітко описаними параметрами й інтерфейсами. Це забезпечує сумісність обладнання різних виробників. Клієнт, наприклад, може купити E-Line у одного оператора і бути впевненим, що це буде працювати так само, як E-Line іншого оператора.

Другий атрибут — масштабованість. Мережа повинна підтримувати мільйони Ethernet-сервісних інстанцій (EVC) та мільйони MAC-адрес в одному домені. У звичайній корпоративній LAN VLAN'ів десятки або сотні. В операторській мережі — десятки тисяч клієнтів, кожен зі своєю структурою. Тобто мільйони EVC — це реальна цифра, яку операторська мережа має витримувати.

Третій атрибут, і, мабуть, найважливіший — надійність. Мережа повинна забезпечувати доступність на рівні 99,999%, «п'ять дев'яток». У практичних термінах — не більше 5,26 хвилин простою на рік. Плюс — час перемикання при відмові має бути менше 50 мілісекунд. Це стандарт «carrier grade» від класичних TDM-мереж. Для порівняння: класичний STP при відмові каналу перебудовує топологію 30–50 секунд, тобто в тисячу разів повільніше. Тому у Carrier Ethernet замість STP використовують спеціальний механізм — ERPS, стандарт ITU-T G.8032, який забезпечує переключення саме за менш ніж 50 мілісекунд.

Четвертий атрибут — якість обслуговування, QoS. Мережа повинна підтримувати диференційоване обслуговування трафіку. Різні типи трафіку мають різні вимоги: голос — мінімальна затримка (менше 150 мс end-to-end) і джитер (менше 30 мс); відео — висока пропускна здатність і мінімальні втрати; звичайні дані — гарантована доставка. MEF визначає до 8 класів обслуговування, кожен зі своїми гарантіями.

І п'ятий атрибут — управління сервісами. Оператор має можливість комплексного моніторингу, діагностики й управління Ethernet-сервісами через стандартні механізми OAM — Operations, Administration, and Maintenance. Тут працюють два основні стандарти: IEEE 802.1ag, який називається Connectivity Fault Management (CFM), для виявлення й локалізації відмов; і ITU-T Y.1731, який розширює CFM механізмами вимірювання продуктивності — Frame Delay, Frame Delay Variation (тобто джитер), Frame Loss Ratio. Це дозволяє

оператору в реальному часі контролювати дотримання SLA для кожного клієнта.

Слайд 6. Інтерфейси Carrier Ethernet: UNI, NNI, EVC

Тепер про архітектуру Carrier Ethernet — три ключові поняття, які треба чітко розрізняти. Це UNI, NNI та EVC.

UNI — User-to-Network Interface, інтерфейс «користувач-мережа». Це демаркаційна точка, де фізично зустрічаються мережа клієнта та мережа оператора. По один бік — обладнання клієнта, яке називається CE, Customer Edge; по інший — обладнання оператора, PE, Provider Edge. Фізично UNI зазвичай реалізується як звичайний Ethernet-порт на маршрутизаторі або комутаторі оператора, до якого клієнт підключає свій пристрій. Але важливо — UNI це не просто «шматок кабелю». Це формально визначена точка, де узгоджуються всі параметри послуги: швидкість підключення (UNI bandwidth), кількість і тип EVC, параметри QoS. MEF визначає різні типи UNI залежно від конфігурації: UNI з одним EVC (all-to-one bundling); UNI з кількома EVC (service multiplexing) — коли клієнт через один фізичний порт має кілька логічних сервісів.

NNI — Network-to-Network Interface. Це інтерфейс між мережами. Розрізняють два підтипи. E-NNI (External) — інтерфейс між мережами РІЗНИХ операторів. Це критично важливо для мультиоператорських Ethernet-послуг — коли клієнтський трафік має пройти через мережі кількох операторів, щоб дійти до віддалених сайтів. Наприклад, ваш офіс у Києві підключений через провайдера А, а філія у Львові — через провайдера Б. І між ними побудовано E-Line через два оператори — вони узгоджують параметри послуги через E-NNI. I-NNI (Internal) — інтерфейс між різними доменами ОДНОГО оператора. Наприклад, різні технологічні платформи в одній мережі, або мережі різних регіонів одного оператора.

І третє, найважливіше поняття — EVC, Ethernet Virtual Connection, Ethernet-віртуальне з'єднання. Це логічне з'єднання між двома або більше UNI, яке забезпечує передачу Ethernet-фреймів між сайтами клієнта. EVC — це аналог віртуального каналу PVC у старих технологіях типу Frame Relay. Клієнт «купує» саме EVC, а не фізичний канал. Кожен EVC має набір атрибутів: тип (point-to-point або multipoint-to-multipoint); параметри QoS у вигляді bandwidth profile; правила обробки клієнтських VLAN-тегів; клас обслуговування CoS (до восьми); параметри OAM. Особлива увага до параметра CoS — Class of Service. Це три біти в тегу 802.1Q, які визначають до восьми класів обслуговування — від найвищого пріоритету для голосу і сигналізації до найнижчого для фонового трафіку типу резервного копіювання.

Слайд 7. Три базові послуги MEF

Тепер про типи послуг Carrier Ethernet. MEF визначає три базові типи Ethernet-сервісів. Кожен з них показаний на діаграмі ліворуч. Розберемо їх по черзі.

E-Line, Ethernet Line Service — це послуга типу «точка-точка», яка з'єднує ДВА UNI через один EVC. E-Line є прямим аналогом виділеного каналу — leased line — але на основі Ethernet. Реалізацій E-Line є дві. EPL, Ethernet Private Line — виділена лінія з повною ізоляцією трафіку: увесь UNI використовується виключно для одного EVC. EVPL, Ethernet Virtual Private Line — з мультиплексуванням кількох сервісів через один фізичний порт UNI; це дозволяє клієнту через один порт мати з'єднання з кількома віддаленими сайтами. E-Line — найпростіша послуга, використовується для з'єднання двох офісів клієнта, підключення клієнта до дата-центру або для побудови WAN-каналів.

E-LAN, Ethernet LAN Service — це послуга типу «багато-до-багатьох». З'єднує множину UNI через multipoint-to-multipoint EVC. E-LAN емулює Ethernet-комутатор: фрейм від будь-якого UNI може бути доставлений будь-якому іншому UNI в тому ж EVC. По суті — це віртуальний Ethernet-комутатор на всю територію міста або країни. Реалізації — EP-LAN (з виділеними UNI) та EVP-LAN (з мультиплексуванням). Технологічно E-LAN базується на VPLS — Virtual Private LAN Service, RFC 4761 та 4762 — або на новішій технології EVPN, Ethernet VPN, RFC 7432. Використовується для об'єднання множини офісів клієнта в єдину корпоративну мережу без побудови повнозв'язної мережі точка-точка.

E-Tree, Ethernet Tree Service — це послуга типу «корінь-листки», rooted multipoint. Один або кілька кореневих UNI (root) можуть обмінюватися кадрами з усіма листковими UNI (leaf); але листкові UNI можуть обмінюватися кадрами ЛИШЕ з кореневими, а МІЖ СОБОЮ — не можуть. E-Tree ідеально підходить для сценаріїв «головний офіс — філії»: філії мають доступ до центру, але не мають прямої зв'язності між собою — це і безпека, і контроль трафіку. Також E-Tree використовується для розсилки контенту (content distribution) — коли головний вузол розсилає інформацію багатьом одержувачам; і для доступу до Інтернету — коли клієнти можуть спілкуватися з роутером провайдера, але не між собою напряму (це запобігає багатьом типам атак у мережі провайдера).

Слайд 8. Проблема одного каналу — рішення LAG

Ми розглянули загальний операторський контекст. Тепер переходимо до конкретної технології — агрегації каналів. Це і буде основною темою другої

половини лекції. Але спочатку — навіщо взагалі потрібна агрегація каналів? Розглянемо типову ситуацію в мережі оператора.

Уявіть: між двома комутаторами прокладено гігабітний Ethernet-канал. Трафік між ними — три гігабіти на секунду. Що робити? Перший варіант — купити 10 Гбіт/с обладнання. Але 10-гігабітні модулі та порти суттєво дорожчі, часто вимагають заміни цілої платформи, це дорого і повільно розгортається. Другий варіант — прокласти паралельно ще один гігабітний канал. Але тут виникає проблема: STP заблокує один з двох паралельних каналів, щоб уникнути петлі. Тобто два фізичні канали є, а трафік іде тільки одним.

Плюс — окремий канал завжди є єдиною точкою відмови, SPOF, Single Point Of Failure. Якщо його порізали або обладнання відмовило, зв'язок припинився повністю, а конвергенція STP займе десятки секунд.

Рішення обох проблем одразу — агрегація каналів, Link Aggregation. Ідея дуже проста: об'єднати кілька фізичних каналів в один логічний. Що це дає? Погляньте на чотири картки внизу. Перше — пропускна здатність зростає як сума. Два по гігабіту — це вже два гігабіти. Друге — відмовостійкість: якщо один канал падає, трафік автоматично йде іншими; STP при цьому нічого не помічає. Третє — спрощення. STP і протоколи маршрутизації бачать один логічний порт, а не декілька — це спрощує конфігурацію й аналіз. І четверте — економія. Не треба міняти платформу на швидшу, можна нарощувати смугу поступово, докладаючи канали в існуючу групу.

Слайд 9. EtherChannel — принцип роботи

Тепер — про саму технологію EtherChannel. Це реалізація ідеї агрегації каналів у Cisco-термінології. Стандарт має кілька синонімів: EtherChannel — це маркетинговий термін Cisco; Link Aggregation — загальний технічний термін; Port-Channel або Port Channel — назва інтерфейсу в Cisco IOS; LAG — Link Aggregation Group — ще одна синонімічна назва. Всі вони означають одне й те саме.

Формально EtherChannel стандартизовано в IEEE 802.1AX. До 2008 року стандарт називався IEEE 802.3ad, потім перейменували на 802.1AX. Технологія дозволяє об'єднати від двох до восьми фізичних Ethernet-портів в один логічний порт — Port Channel. Дуже важлива умова: усі порти в групі мають бути однакові за швидкістю, дуплексом, VLAN-конфігурацією та типом. Не можна об'єднати, наприклад, гігабітний порт і 10-гігабітний. Не можна об'єднати access-порт і trunk-порт.

Логічний канал EtherChannel сприймається всіма протоколами верхнього рівня як один інтерфейс. STP бачить один порт — і не блокує його як «зайвий», навіть якщо фізично там кілька каналів. Протоколи маршрутизації (OSPF, EIGRP) теж працюють з одним інтерфейсом — обчислюють метрики,

встановлюють суміжності. Це і є те, чому EtherChannel таке зручне рішення: воно прозоре для верхніх рівнів.

EtherChannel підтримується у різних сценаріях: між двома комутаторами (switch-to-switch — найпоширеніший випадок); між комутатором і сервером (switch-to-server — для критичних серверів з двома або чотирма мережевими картками); між комутатором і маршрутизатором (switch-to-router).

Тепер — принцип роботи. На нижньому банері слайда він у стислому вигляді. Як пакет попадає в один з фізичних каналів групи? Комутатор обчислює хеш-функцію від певних полів кадру або пакета — MAC-адрес, IP-адрес, TCP/UDP портів. Результат хешування визначає, через який саме фізичний канал буде надіслано цей кадр. Ключова властивість: усі пакети одного потоку (з тими самими значеннями полів хешу) завжди йдуть через ОДИН і ТОЙ САМИЙ фізичний канал. Це гарантує збереження порядку кадрів — це критично важливо, бо якщо TCP-пакети прийдуть у неправильному порядку, TCP розцінить це як втрату і буде переспитувати. Тому агрегація зроблена так, щоб порядок пакетів в потоці не порушувався.

Діаграма на слайді ілюструє обидві ключові властивості EtherChannel — розподіл трафіку по каналах у нормальному режимі (ліва частина внизу) і автоматичне переключення при відмові каналу (права частина внизу).

Слайд 10. Протоколи агрегації: LACP та PAgP

Щоб два комутатори могли встановити EtherChannel-групу, вони мають узгодити між собою параметри агрегації — які порти включити в групу, чи сумісні їхні швидкості, дуплекси і так далі. Для цього використовуються два протоколи узгодження. Розберемо обидва.

LACP, Link Aggregation Control Protocol — це стандартний протокол, визначений в IEEE 802.1AX. Він відкритий, вендоронезалежний і підтримується обладнанням практично всіх виробників — Cisco, Juniper, Huawei, HP, Arista, Mellanox і так далі. Тобто якщо у вас у мережі обладнання різних виробників (multi-vendor environment) — треба використовувати саме LACP. Це стандарт для операторських мереж і для більшості корпоративних. LACP підтримує два режими налаштування портів. Active — активний режим: порт активно ініціює LACPDU (Link Aggregation Control Protocol Data Units) — спеціальні кадри для узгодження. Passive — пасивний: порт тільки відповідає на LACPDU, які отримує, але сам не ініціює.

PAgP, Port Aggregation Protocol — це пропрієтарний протокол Cisco. Він працює лише між пристроями Cisco і зберігається переважно для сумісності з існуючими мережами. У новій техніці Cisco також підтримується, але не є переважним вибором. Режими у PAgP аналогічні: desirable — аналог active, порт активно ініціює узгодження; auto — аналог passive, тільки відповідає.

Дуже важливе правило, показане у нижньому банері слайда: щоб EtherChannel-група утворилася, хоча б один із двох комутаторів має бути в активному режимі. Тобто працюють такі комбінації: active + active, active + passive, desirable + desirable, desirable + auto. НЕ утворюють групу такі комбінації: passive + passive, auto + auto — обидва пасивні, ніхто не ініціює, обидва «мовчать» і чекають один одного.

Ще існує так званий статичний режим — «mode on». У ньому агрегація конфігурується примусово, без будь-якого протоколу узгодження. Порти просто оголошуються членами групи, і комутатор починає їх використовувати. Цей режим НЕ рекомендується до використання. Чому? Бо він не перевіряє параметри на іншій стороні. Якщо на другому кінці налаштування помилкові — наприклад, там взагалі немає EtherChannel — це може призвести до петлі в мережі. Тому у виробничих мережах завжди використовуйте LACP або PAgP.

І ще одна цікава особливість LACP, якої немає в PAgP: механізм «hot standby». Він дозволяє додати до групи до 16 портів, з яких лише 8 будуть активними, а решта 8 — у стані очікування, standby. При виході з ладу активного порту один із standby-портів автоматично активується і бере на себе трафік. Це гарантує швидке відновлення повної пропускної здатності без ручного втручання.

Слайд 11. Балансування навантаження в EtherChannel

Тепер про балансування навантаження — тему, з якою ви безпосередньо стикнетеся на лабораторній роботі. Комутатор має вирішити, через який з декількох фізичних каналів надіслати кожен кадр. Це рішення приймається за допомогою хеш-функції: обчислюється хеш від певних полів, і результат визначає канал. Питання — від яких саме полів?

У таблиці на слайді — сім основних алгоритмів балансування. Розберемо кожен та коли який доцільний.

src-mac — хешується MAC-адреса джерела. Доцільно, коли у нас багато клієнтів, які спілкуються з одним сервером — тоді кожен клієнт піде через свій канал. Наприклад: множина комп'ютерів у офісі → один файловий сервер.

dst-mac — MAC-адреса призначення. Доцільно у зворотній ситуації: один клієнт (наприклад, той самий файловий сервер) відправляє відповіді багатьом клієнтам. Тоді кожна відповідь піде через свій канал відповідно до MAC різних отримувачів.

src-dst-mac — обидві MAC-адреси. Для загального L2-трафіку в мережі з різноманітним трафіком.

src-ip і dst-ip — аналогічно, але за IP-адресами замість MAC. Доцільно для L3-трафіку — коли трафік проходить через маршрутизатор і MAC-адреси змінюються, а IP залишаються.

src-dst-ip — обидві IP-адреси. Це рекомендований варіант за замовчуванням, який ви бачите виділеним у таблиці. Дає найбільш рівномірний розподіл хешів для загального L3-трафіку. Це та настройка, яку ви побачите на більшості реальних мереж і яку зазвичай ставлять на лабораторних.

src-dst-port — обидві IP-адреси плюс TCP/UDP порти. Найдетальніший розподіл: кожне окреме TCP-з'єднання може піти через свій канал. Використовується там, де потрібен найточніший баланс — наприклад, у мережах з великою кількістю однотипних потоків між одними й тими самими вузлами.

І критично важливий момент, виділений у нижньому лівому банері: EtherChannel НЕ ГАРАНТУЄ рівномірного розподілу трафіку по каналах. Один потік завжди йде через один канал. Якщо у вас є «слон-потік», elephant flow — наприклад, велике резервне копіювання по мережі — він завантажить свій канал, поки інші канали залишатимуться майже вільними. Тому оператор має моніторити утилізацію КОЖНОГО фізичного каналу в групі окремо і при потребі — змінювати алгоритм балансування або перерозподіляти трафік.

Практична порада — праворуч. Для більшості випадків використовуйте src-dst-ip. Для маршрутизаторів — src-dst-ip або src-dst-port для точнішого балансу. Змінити алгоритм в Cisco IOS можна командою: port-channel load-balance із зазначенням алгоритму. Ця команда — глобальна для всього комутатора, тобто вона впливає на всі EtherChannel-групи на цьому пристрої.

Слайд 12. Відмовостійкість та Multi-Chassis EtherChannel

Розглянемо детальніше, як працює відмовостійкість. Уявімо сценарій: у нас група з чотирьох каналів по 1 гігабіту, і один канал раптово падає — наприклад, розірваний оптоволоконний кабель.

Ліворуч на слайді — покрокова процедура. Крок перший: комутатор миттєво виявляє втрату несучої сигналу (link down). Це відбувається на фізичному рівні — практично одразу. Крок другий: порт видаляється з групи агрегації. Крок третій: трафік, який раніше йшов через цей канал, перерозподіляється між трьома каналами, що залишились працездатними. Це знову відбувається за допомогою переобчислення хеш-функції — потоки, які раніше «прив'язувались» до відмовшого каналу, тепер прив'язуються до працюючих. Крок четвертий: уся процедура займає кілька мілісекунд. І, найголовніше, крок п'ятий — STP і протоколи маршрутизації нічого не помічають. Логічний порт залишається активним, поки хоча б один фізичний канал у групі працює.

Це надзвичайно швидко. Для порівняння: класичний STP при відмові каналу перебудовує топологію 30–50 секунд; RSTP — кілька секунд.

EtherChannel — мілісекунди. Тому кажуть, що EtherChannel забезпечує failover у сотні і тисячі разів швидше за STP.

Тепер про Multi-Chassis EtherChannel, MCEC. Це важлива еволюція концепції агрегації, показана у правій частині слайда. Проблема звичайного EtherChannel: якщо весь комутатор виходить з ладу — а не окремий канал — то усі канали в групі стають недоступними. Тобто відмовостійкість каналів є, а відмовостійкості комутатора немає.

Рішення — MCEC. Ідея: підключений пристрій (наприклад, сервер, або комутатор доступу) встановлює EtherChannel не до одного, а до двох фізичних комутаторів, які виглядають з боку сервера як один логічний. Для сервера це прозоро — він бачить звичайний Port-Channel. Але фізично його канали йдуть до двох незалежних пристроїв, і навіть якщо один з них повністю відмовляє, з'єднання зберігається.

У Cisco реалізовано дві технології MCEC. vPC, Virtual Port Channel — для комутаторів серії Nexus (дата-центрові платформи). VSS, Virtual Switching System — для комутаторів серії Catalyst (кампусні платформи). Обидві технології роблять одне й те ж — об'єднують два фізичні комутатори в один логічний з точки зору Port-Channel. MCEC — це фактично стандарт для сучасних мереж дата-центрів. Кожен важливий сервер підключається до двох top-of-rack комутаторів через vPC, і це захищає одночасно від відмови каналу, відмови мережевої картки і відмови комутатора.

Слайд 13. Порівняння: EtherChannel vs окремі канали

Зведемо все, що ми дізналися про EtherChannel, у порівняльну таблицю. Це Таблиця 5.2 з навчального посібника. Пройдемо швидко по рядках.

Пропускна здатність. EtherChannel — сума каналів у групі, максимум 8 портів по 10 гігабіт, тобто до 80 гігабіт. Окремі канали — тільки один канал за раз.

Відмовостійкість. EtherChannel — автоматичне перемикання за мілісекунди. Окремі канали — покладаються на STP, який працює секунди чи десятки секунд.

STP. EtherChannel — один логічний порт, STP не блокує. Окремі канали — STP розглядає кожен порт окремо і, якщо між двома комутаторами є кілька шляхів, блокує зайві, залишаючи лише один активний.

Балансування трафіку. EtherChannel — за хешем на основі MAC, IP або портів. Окремі канали — балансування немає, увесь трафік іде через один активний.

Протоколи узгодження. EtherChannel — LACP або PAgP. Окремі канали — не потрібні.

Максимум портів у групі. Для LACP — 8 активних плюс 8 у режимі standby. Для окремих каналів — не застосовно.

І сфера застосування. EtherChannel — магістральні канали між комутаторами, uplink до критичних серверів, підключення важливих маршрутизаторів. Окремі канали — звичайні кінцеві підключення робочих станцій, некритичне обладнання.

Головний висновок, який висвітлений у нижньому банері: EtherChannel одночасно дає три речі — більшу смугу, швидку відмовостійкість і спрощення управління. Це техніка, яку варто використовувати всюди, де є хоча б два паралельні канали.

Слайд 14. Куди все це вписується: архітектура Metro Ethernet

Останній слайд перед підсумком показує, як усі теми сьогоднішньої лекції складаються в цілісну картину. Ліворуч ви бачите архітектуру Metro Ethernet — трирівневу ієрархічну модель, яка є де-факто стандартом побудови сучасних операторських мереж міського масштабу.

Найнижчий рівень — рівень доступу (access). Це саме те місце, де знаходяться UNI. Клієнтське обладнання CE підключається до комутаторів доступу оператора через ці інтерфейси. Комутатори доступу виконують класифікацію трафіку, застосовують bandwidth profiles, роблять базову QoS-обробку. Типова пропускна здатність — від 10 мегабіт до 10 гігабіт. Часто рівень доступу будується як кільце, і для його захисту використовується технологія ERPS (стандарт G.8032), яка забезпечує ті самі 50 мілісекунд переключення при обриві.

Середній рівень — рівень агрегації (aggregation). Він об'єднує трафік від множини пристроїв рівня доступу і транспортує його до ядра. На цьому рівні виконується агрегація EVC, міжвузловий OAM, складніша QoS-обробка. Саме тут переважно застосовується EtherChannel — між комутаторами агрегації і між агрегацією та ядром. Погляньте на діаграмі: два зелені комутатори агрегації з'єднані каналом, підписаним «EtherChannel».

Верхній рівень — ядро мережі (core). Це високошвидкісний транспорт між вузлами агрегації. Тут використовуються 10G, 40G, 100G Ethernet-канали, часто в повнозв'язній топології для максимальної відмовостійкості.

Отже, підсумовуючи. Ми з вами розглянули операторський контекст — Carrier Ethernet і послуги MEF. І одну з базових технологій, які роблять цю архітектуру можливою — EtherChannel. У сучасних мережах Metro Ethernet EtherChannel використовується практично повсюдно — на кожному з'єднанні, де потрібна швидка відмовостійкість або більша смуга.

Слайд 15. Підсумок лекції

Підбиваємо підсумки. Шість ключових моментів. Перше: Carrier Ethernet — це розширення технології Ethernet до операторського класу; стандартизовано у MEF; забезпечує доступність 99,999%. Друге: п'ять атрибутів MEF — стандартизовані сервіси, масштабованість, надійність, QoS, управління через OAM. Третє: три ключові поняття архітектури — UNI, NNI, EVC — інтерфейс клієнт-оператор, інтерфейс між операторами, і логічний канал як аналог PVC у Frame Relay.

Четверте: три послуги MEF — E-Line (точка-точка), E-LAN (multipoint-to-multipoint), E-Tree (root-leaf). П'яте: EtherChannel, він же LAG, стандартизований у IEEE 802.1AX; об'єднує від 2 до 8 портів у групу; для STP і маршрутизації виглядає як один логічний порт. Шосте: два протоколи узгодження — LACP (стандарт, вендоронезалежний) і PAgP (тільки Cisco); принаймні один з двох комутаторів має бути в активному режимі, інакше група не утвориться.