МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Марія КОЛОЩУК
Ольга ДЯЧУК

ГЛОБАЛЬНІ МЕРЕЖІ

Навчальний посібник

Житомир
2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

◆

Марія КОЛОЩУК
Ольга ДЯЧУК

ГЛОБАЛЬНІ МЕРЕЖІ

Навчальний посібник

Житомир
2026

УДК 004.7.075.8
К61

Рекомендовано до друку Вченою радою
Державного університету «Житомирська політехніка»
(протокол №10 від 5 червня 2026 року)

Рецензенти:

Я.Ю. Дорогий – доктор технічних наук, професор, завідувач кафедри прикладної математики та інформатики Донецького національного технічного університету;

М.М. Делембовський – кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури;

В.В. Воротніков – доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

Колощук М.С.

К61 Глобальні мережі : навч. посібник / М.С. Колощук, О.Ю. Дячук. – Електронні дані. – Житомир : Державний університет «Житомирська політехніка», 2026. – 180 с.

ISBN 978-966-683-737-3

Навчальний посібник присвячено теоретичним і прикладним засадам побудови, функціонування та захисту глобальних комп'ютерних мереж, що є основою сучасної цифрової інфраструктури.

У виданні послідовно висвітлено основні теоретичні та практичні аспекти побудови глобальних мереж. Розглянуто підходи до класифікації WAN, їхні архітектурні особливості, принципи функціонування операторських мереж. Окрему увагу приділено механізмам забезпечення якості обслуговування, технологіям Metro Ethernet, Carrier Ethernet та MPLS. Також розкрито особливості організації мереж доступу, використання протоколу BGP, технологій VPN та EVPN, а також засобів захисту, моніторингу й оптимізації глобальної мережевої інфраструктури.

Матеріал навчального посібника структуровано відповідно до логіки вивчення дисципліни «Глобальні мережі» та спрямовано на формування цілісного уявлення про принципи проєктування, функціонування, адміністрування й захисту сучасних телекомунікаційних та комп'ютерних мереж великого масштабу.

Навчальний посібник призначено для здобувачів вищої освіти, які навчаються за спеціальностями у галузях комп'ютерної інженерії, кібербезпеки, телекомунікацій, комп'ютерних наук та інформаційних технологій, а також для викладачів і всіх, хто цікавиться питаннями побудови та експлуатації глобальних мереж.

УДК 004.7.075.8

ISBN 978-966-683-737-3

СПИСОК СКОРОЧЕНЬ

AES	Advanced Encryption Standard — стандарт симетричного блочного шифрування
AS	Autonomous System — автономна система в Інтернеті
ASN	Autonomous System Number — номер автономної системи
ATM	Asynchronous Transfer Mode — асинхронний режим передачі
BFD	Bidirectional Forwarding Detection — двонаправлене виявлення збоїв
BGP	Border Gateway Protocol — протокол граничного шлюзу
CIDR	Classless Inter-Domain Routing — безкласова міждоменна маршрутизація
CPE	Customer Premises Equipment — обладнання у приміщенні клієнта
CSPF	Constrained Shortest Path First — алгоритм найкоротшого шляху з обмеженнями
DDoS	Distributed Denial of Service — розподілена атака на відмову в обслуговуванні
DNS	Domain Name System — система доменних імен
DPI	Deep Packet Inspection — глибокий аналіз пакетів
DSCP	Differentiated Services Code Point — код диференційованого обслуговування
DSL	Digital Subscriber Line — цифрова абонентська лінія
DWDM	Dense Wavelength Division Multiplexing — щільне хвильове мультиплексування
ECMP	Equal-Cost Multi-Path — багатошляхова маршрутизація з рівною вартістю
EVPN	Ethernet VPN — Ethernet-орієнтована VPN-технологія
FCAPS	Fault, Configuration, Accounting, Performance, Security — модель управління мережею
FEC	Forwarding Equivalence Class — клас еквівалентної пересилки
FHRP	First Hop Redundancy Protocol — протокол резервування першого шлюзу
FRR	Fast Reroute — швидке перемикання / швидке відновлення маршруту
FTTH	Fiber to the Home — оптичне волокно до помешкання
GLBP	Gateway Load Balancing Protocol — протокол балансування шлюзів

GPON	Gigabit Passive Optical Network — гігабітна пасивна оптична мережа
GRE	Generic Routing Encapsulation — загальна інкапсуляція маршрутизації
GSLB	Global Server Load Balancing — глобальне балансування серверного навантаження
HA	High Availability — висока доступність
HSRP	Hot Standby Router Protocol — протокол гарячого резерву маршрутизаторів
IDS	Intrusion Detection System — система виявлення вторгнень
IEEE	Institute of Electrical and Electronics Engineers — Інститут інженерів електротехніки та електроніки
IGP	Interior Gateway Protocol — протокол внутрішнього шлюзу
IP	Internet Protocol — міжмережевий протокол
IPFIX	IP Flow Information Export — стандарт експорту інформації про IP-потоки
IPS	Intrusion Prevention System — система запобігання вторгненням
IPsec	Internet Protocol Security — набір протоколів захисту IP-трафіку
IS-IS	Intermediate System to Intermediate System — протокол маршрутизації
ITU-T	International Telecommunication Union — Telecommunication Standardization Sector — Сектор стандартизації електрозв’язку МСЕ
L2VPN	Layer 2 VPN — VPN канального рівня
L3VPN	Layer 3 VPN — VPN мережевого рівня
LAG	Link Aggregation Group — група агрегованих каналів
LAN	Local Area Network — локальна мережа
LDP	Label Distribution Protocol — протокол розподілу міток
LSP	Label Switched Path — шлях з комутацією міток
LSR	Label Switch Router — маршрутизатор з комутацією міток
LTE	Long Term Evolution — стандарт мобільного зв’язку 4G
MAC	Media Access Control — управління доступом до середовища
MEF	Metro Ethernet Forum — індустріальна асоціація з Carrier Ethernet
MIB	Management Information Base — база керуючої інформації
MITM	Man-in-the-Middle — атака «людина посередині»
MLAG	Multi-Chassis Link Aggregation — агрегація каналів між кількома шасі

MPLS	Multiprotocol Label Switching — багатопротокольна комутація за мітками
NAT	Network Address Translation — трансляція мережевих адрес
NetFlow	Технологія Cisco для експорту статистики мережевих потоків
NFV	Network Functions Virtualization — віртуалізація мережевих функцій
NMS	Network Management System — система управління мережею
NTP	Network Time Protocol — протокол синхронізації часу
OAM	Operations, Administration, Maintenance — операції, адміністрування, обслуговування
OID	Object Identifier — ідентифікатор об’єкта в SNMP/MIB
OLT	Optical Line Terminal — оптичний лінійний термінал
ONT	Optical Network Terminal — оптичний мережевий термінал
OSPF	Open Shortest Path First — протокол маршрутизації за найкоротшим шляхом
OTN	Optical Transport Network — оптична транспортна мережа
PBB	Provider Backbone Bridges — магістральні мости провайдера
PDH	Plesiochronous Digital Hierarchy — плезіохронна цифрова ієрархія
PE	Provider Edge — граничний маршрутизатор провайдера
PON	Passive Optical Network — пасивна оптична мережа
PTP	Precision Time Protocol — протокол точної синхронізації часу
QinQ	IEEE 802.1ad VLAN stacking — подвійне тегування VLAN
QoS	Quality of Service — якість обслуговування
RFC	Request for Comments — серія стандартів IETF
RPKI	Resource Public Key Infrastructure — інфраструктура відкритих ключів для маршрутизації
RR	Route Reflector — рефлектор маршрутів у BGP
RSVP-TE	Resource Reservation Protocol — Traffic Engineering — протокол резервування ресурсів
SD-WAN	Software-Defined WAN — програмно визначена WAN
SDH	Synchronous Digital Hierarchy — синхронна цифрова ієрархія
SDN	Software-Defined Networking — програмно визначена мережа
SIEM	Security Information and Event Management — управління інформацією про безпеку

SLA	Service Level Agreement — угода про рівень обслуговування
SNMP	Simple Network Management Protocol — простий протокол управління мережею
SPoF	Single Point of Failure — одинична точка відмови
STP	Spanning Tree Protocol — протокол кістякового дерева
TCP	Transmission Control Protocol — протокол управління передачею
TLS	Transport Layer Security — безпека транспортного рівня
TTL	Time to Live — час життя пакета
UDP	User Datagram Protocol — протокол користувацьких дейтаграм
UNI	User-Network Interface — інтерфейс користувач-мережа
VLAN	Virtual LAN — віртуальна локальна мережа
VPLS	Virtual Private LAN Service — віртуальний приватний LAN-сервіс
VPN	Virtual Private Network — віртуальна приватна мережа
VRF	Virtual Routing and Forwarding — віртуальна маршрутизація та пересилка
VRRP	Virtual Router Redundancy Protocol — протокол резервування маршрутизаторів
VXLAN	Virtual Extensible LAN — віртуальна розширювана LAN
WAN	Wide Area Network — глобальна мережа

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційного суспільства, цифровізація економіки та широке впровадження хмарних, мобільних і кіберфізичних сервісів зробили глобальні мережі ключовою складовою сучасної телекомунікаційної інфраструктури. Інтернет, корпоративні WAN, операторські магістралі та програмно-визначені мережі сьогодні забезпечують функціонування державних інституцій, фінансової системи, промисловості, освіти та повсякденного життя мільярдів користувачів. Здатність проєктувати, експлуатувати та захищати такі мережі стала однією з фундаментальних професійних компетентностей фахівців у галузі інформаційних технологій, комп'ютерної інженерії та кібербезпеки.

Дисципліна «Глобальні мережі» посідає важливе місце у системі підготовки здобувачів вищої освіти за спеціальностями галузей знань F «Інформаційні технології». Вона забезпечує формування у студентів цілісного уявлення про принципи побудови та функціонування мереж великого масштабу, технології передавання й комутації даних, протоколи міждоменної маршрутизації, а також про сучасні підходи до забезпечення якості обслуговування, відмовостійкості та безпеки телекомунікаційних систем. Опанування цієї дисципліни є необхідною передумовою для подальшої професійної діяльності у сфері проєктування, адміністрування та супроводу телекомунікаційних мереж.

Курс «Глобальні мережі» логічно продовжує та поглиблює знання, отримані студентами під час вивчення дисциплін циклу професійної підготовки, зокрема «Комп'ютерні мережі», «Архітектура комп'ютерів», «Операційні системи» та «Основи інформаційної безпеки». Знання, набуті у процесі вивчення глобальних мереж, є підґрунтям для подальшого засвоєння спеціалізованих дисциплін магістерського рівня та для виконання кваліфікаційних робіт інженерного й науково-дослідного спрямування.

Навчальний посібник «Глобальні мережі» підготовлено з метою систематизованого викладу теоретичних засад і прикладних аспектів побудови, функціонування та експлуатації мереж глобального масштабу. У виданні послідовно розглянуто фундаментальні принципи побудови WAN, архітектурні рішення сучасних операторських мереж, моделі надання послуг та механізми забезпечення якості обслуговування (QoS); первинні транспортні мережі (PDH, SDH, DWDM, OTN) і концепцію накладених (overlay) мереж; особливості функціонування протоколів IPv4 та IPv6 у глобальному середовищі, технології керування трафіком і MPLS Traffic Engineering; принципи маршрутизації між автономними системами на основі протоколу BGP, побудову L2VPN, L3VPN та EVPN; питання інформаційної безпеки глобальних мереж — від класифікації кіберзагроз і протидії DDoS-атакам до архітектури Zero Trust і захисту BGP; а також сучасні засоби моніторингу, управління та забезпечення високої доступності телекомунікаційних систем.

Структура посібника побудована за принципом «від загального до конкретного»: спочатку формуються базові теоретичні поняття та класифікаційні схеми, після чого розглядаються конкретні технології, протоколи та інженерні рішення, які реалізують ці концепції на практиці. Кожен розділ супроводжується ілюстративними рисунками, порівняльними таблицями та контрольними запитаннями, що дозволяє читачеві не лише засвоїти теоретичний матеріал, а й перевірити рівень його опанування.

Основними завданнями, що стоять перед студентом у процесі вивчення дисципліни «Глобальні мережі», є: засвоєння принципів класифікації, проєктування та функціонування мереж WAN-рівня; розуміння архітектури сучасних операторських мереж і моделей надання телекомунікаційних послуг; набуття навичок аналізу та налаштування протоколів маршрутизації, технологій MPLS, SD-WAN і Carrier Ethernet; формування здатності застосовувати механізми QoS, забезпечення відмовостійкості та високої доступності; опанування методів захисту глобальних мереж від сучасних кіберзагроз і атак на інфраструктурному рівні; вироблення вмінь використовувати сучасні засоби моніторингу, управління та діагностики мережі.

Видання призначене для здобувачів вищої освіти першого (бакалаврського) і другого (магістерського) рівнів, а також буде корисним викладачам, аспірантам, інженерам-практикам та широкому колу читачів, які цікавляться питаннями побудови й експлуатації сучасних телекомунікаційних мереж. Матеріали посібника можуть бути використані як для аудиторної роботи, так і для самостійного опрацювання.

Автори висловлюють сподівання, що пропонований навчальний посібник сприятиме формуванню у студентів цілісного й системного уявлення про сучасні глобальні мережі, допоможе поєднати фундаментальні теоретичні знання з практичними інженерними навичками та стане надійною основою для подальшого професійного зростання у галузі мережевих технологій.

РОЗДІЛ 1

ОСНОВИ ПОБУДОВИ ГЛОБАЛЬНИХ МЕРЕЖ

У першому розділі розглядаються фундаментальні принципи побудови глобальних мереж, починаючи від класифікації та архітектурних рішень і завершуючи механізмами забезпечення якості обслуговування. Особлива увага приділяється сучасним технологіям, таким як MPLS, SD-WAN, хмарні сервіси та моделі надання послуг, що визначають обличчя телекомунікаційної галузі на сьогодні.

Глобальні мережі (Wide Area Network, WAN) забезпечують обмін даними між різними локальними мережами та віддаленими вузлами на великих відстанях. Вони є основою сучасної цифрової інфраструктури, що підтримує бізнес-процеси, хмарні сервіси, електронну комерцію та глобальну комунікацію.

Ключова ідея

Глобальні мережі об'єднують віддалені системи та користувачів, забезпечуючи надійний обмін даними та доступ до ресурсів незалежно від географічних відстаней.

1.1. КЛАСИФІКАЦІЯ ГЛОБАЛЬНИХ МЕРЕЖ

Глобальні мережі являють собою складні телекомунікаційні системи, що забезпечують передачу даних на значні відстані — від десятків до тисяч кілометрів. На відміну від локальних мереж (LAN), які обмежені територією одного будинку або групи будинків, глобальні мережі охоплюють міста, країни та континенти. Розуміння різноманітних типів глобальних мереж та їхніх характеристик є необхідною передумовою для грамотного проєктування та експлуатації мережевої інфраструктури.

Класифікація глобальних мереж може здійснюватися за багатьма критеріями, серед яких найбільш важливими є: територіальне охоплення, технологія передавання даних, тип комутації, форма власності та призначення мережі.

1.1.1. За територіальним охопленням

За географічним масштабом мережі поділяються на такі типи:

- PAN – персональна мережа (до 10 м).
- LAN – локальна мережа (будівля, офіс, кампус).
- MAN – міська мережа (місто або регіон).
- WAN – глобальна мережа (країна, континент).
- GAN – глобальна мережа нового покоління (міжконтинентальний та супутниковий зв'язок). Зазначимо, що термін GAN не є стандартним у документах IETF, ITU чи IEEE та використовується переважно як умовна категорія для глобальних мереж планетарного масштабу.

Локальні мережі (Local Area Network, LAN) забезпечують з'єднання пристроїв у межах обмеженої території — зазвичай одного приміщення, поверху або будівлі. Типова відстань між вузлами LAN становить від кількох метрів до кількох кілометрів. Технологічною основою LAN є стандарти Ethernet (IEEE 802.3) та Wi-Fi (IEEE 802.11).

Міські мережі (Metropolitan Area Network, MAN) охоплюють територію міста або агломерації, забезпечуючи зв'язок між різними будівлями та локальними мережами в межах міста або регіону.

Глобальні мережі (Wide Area Network, WAN) є найбільш масштабним рівнем мережевої інфраструктури. Вони об'єднують мережі нижчих рівнів (LAN та MAN), забезпечуючи передачу даних між географічно віддаленими точками. WAN можуть охоплювати територію окремої країни, континенту або навіть усієї земної кулі. Найвідомішим прикладом глобальної мережі є Інтернет.

Окрему категорію становлять **кампусні мережі** (Campus Area Network, CAN), які займають проміжне положення між LAN та MAN. Кампусна мережа об'єднує кілька будівель, розташованих на одній обмеженій території, — наприклад, комплекс будівель університету, промислове підприємство або військова база. Кампусні мережі зазвичай належать одній організації та використовують високошвидкісні магістральні з'єднання між будівлями.

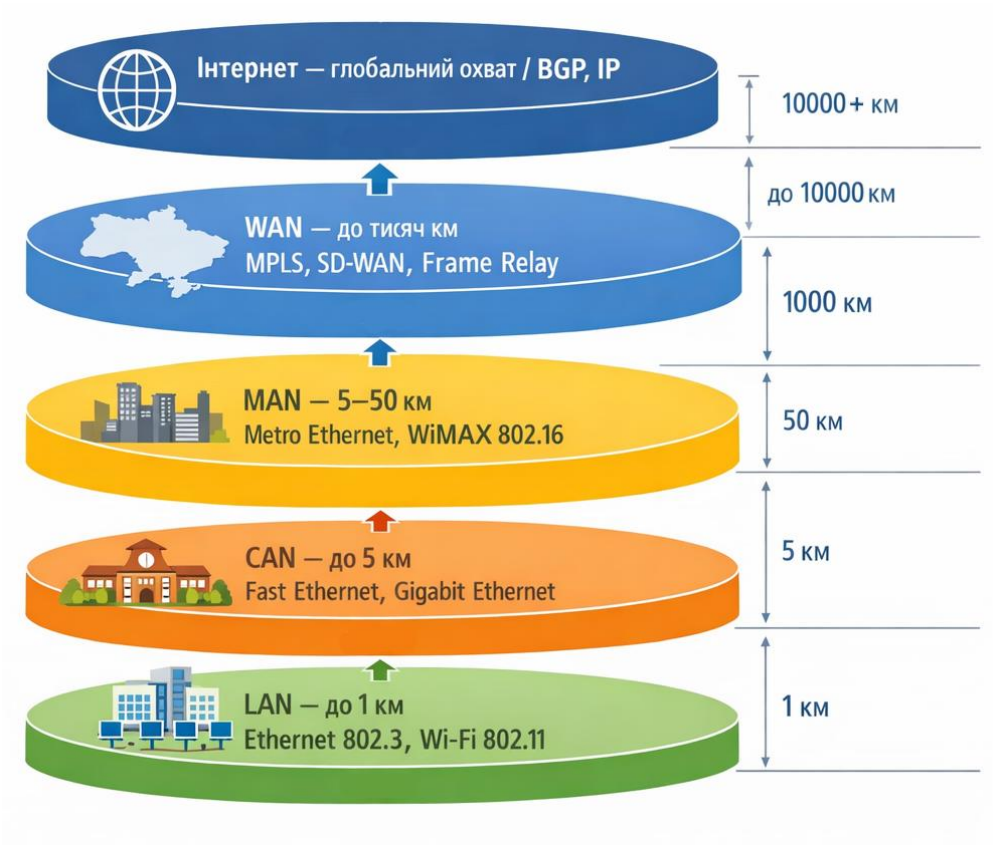

Рисунок 1.1 – Ієрархія мереж за територіальним охопленням

> **Важливо**
> *Чим ширший масштаб мережі, тим складніше її управління та забезпечення якості обслуговування (SLA).*

1.1.2. За технологією передачі даних

Технологія передавання даних є одним із ключових критеріїв класифікації глобальних мереж, оскільки саме вона визначає швидкість, надійність та вартість мережевих послуг. За середовищем і способом передавання даних виділяють:

- Дротові мережі (оптоволокно, мідні лінії, кабельні системи).
- Бездротові мережі (радіоканал, мікрохвильовий зв'язок, супутниковий зв'язок).
- Гібридні мережі (комбінація дротових і бездротових технологій).

Технологія X.25, розроблена у 1976 році, стала однією з перших стандартизованих технологій пакетної комутації для глобальних мереж. Головною

перевагою X.25 є вбудовані механізми виявлення та виправлення помилок. Однак швидкість передачі даних у мережах X.25 зазвичай не перевищує 64 кбіт/с.

Технологія Frame Relay забезпечує значно вищу пропускну здатність — до 45 Мбіт/с — і орієнтована на використання каналів зв'язку високої якості. Frame Relay широко використовувалася для об'єднання локальних мереж до початку 2010-х років.

Технологія ATM (Asynchronous Transfer Mode) розроблена як універсальне рішення для передачі різнорідного трафіку — голосу, відео та даних — з гарантованою якістю обслуговування. ATM підтримує швидкості передачі 155 Мбіт/с (OC-3) та 622 Мбіт/с (OC-12).

Технологія MPLS (Multiprotocol Label Switching) поєднує переваги маршрутизації на основі IP-протоколу та високопродуктивної комутації на основі міток. MPLS залишається однією з основних технологій у магістральних мережах операторів зв'язку.

Технології Carrier Ethernet являють собою розширення стандартів Ethernet для використання у глобальних мережах. Carrier Ethernet підтримує швидкості від 1 Мбіт/с до 100 Гбіт/с та забезпечує механізми OAM для управління мережею операторського класу.

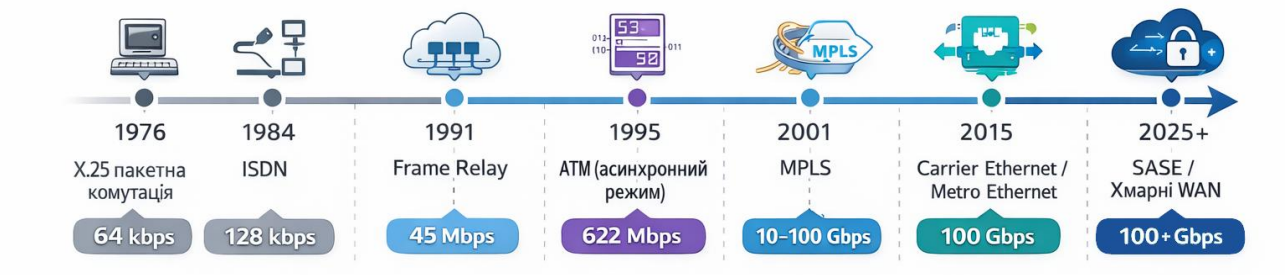

Рисунок 1.2 – Історичний розвиток технологій глобальних мереж

Таблиця 1.1 — Порівняння технологій глобальних мереж

Параметр	X.25	Frame Relay	ATM	MPLS	Carrier Ethernet
Швидкість	До 64 кбіт/с	До 45 Мбіт/с	155–622 Мбіт/с	До 100 Гбіт/с	До 100 Гбіт/с
Рівні OSI	1–3	1–2	1–2	2.5	1–2
Тип комутації	Вірт. канали	Вірт. канали	Комірки 53 Б	Мітки	Кадри Ethernet
QoS	Обмежений	CIR, Bc, Be	5 класів	DiffServ, TE	MEF CoS
Статус	Застаріла	Застаріла	Обмежене	Широко вик.	Зростає

1.1.3. За типом комутації

Тип комутації є фундаментальною характеристикою будь-якої мережі, яка визначає спосіб встановлення з'єднання між джерелом та отримувачем даних. У глобальних мережах використовуються три основні типи комутації: комутація каналів, комутація пакетів та комутація комірок.

Комутація каналів (circuit switching) передбачає встановлення фізичного або логічного з'єднання між двома абонентами перед початком передачі даних. Це з'єднання зберігається протягом усього сеансу зв'язку та забезпечує постійну пропускну здатність каналу. Класичним прикладом є традиційна телефонна мережа (PSTN).

Комутація пакетів (packet switching) є домінуючим підходом у сучасних глобальних мережах. При комутації пакетів дані поділяються на окремі блоки (пакети),

кожен з яких самостійно маршрутизується через мережу від джерела до одержувача. Розрізняють дейтаграмний режим (протокол IP) та режим віртуальних каналів (X.25, Frame Relay, MPLS).

Комутація комірок (cell switching) є різновидом комутації пакетів, що використовує пакети фіксованого розміру — комірки. Цей підхід реалізований у технології ATM, де розмір комірки становить 53 байти.

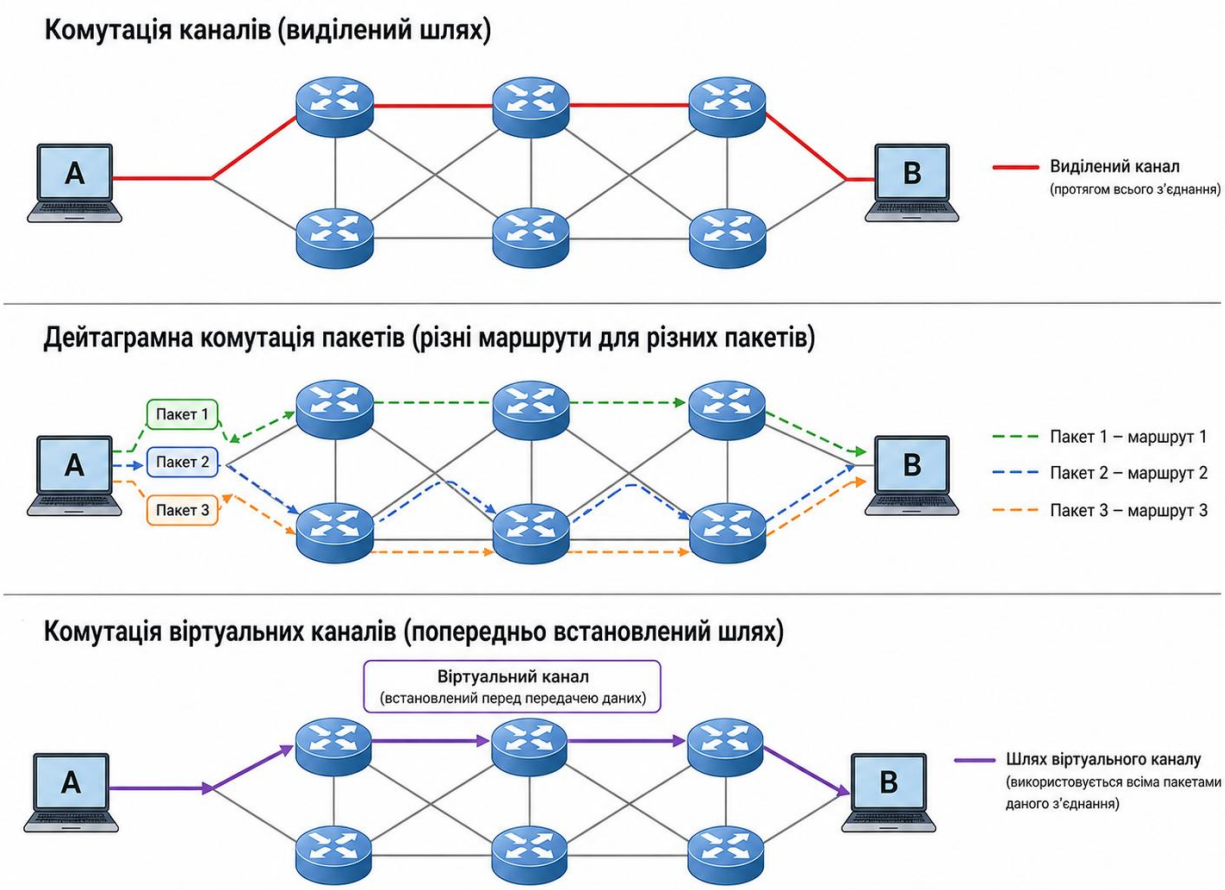

Рисунок 1.3 – Типи комутації у глобальних мережах

1.1.4. За формою власності та призначенням

За формою власності глобальні мережі поділяються на публічні (public), приватні (private) та гібридні. **Публічні мережі** належать операторам зв'язку і надають послуги широкому колу користувачів. Найбільшою публічною мережею є Інтернет.

Приватні мережі створюються та експлуатуються окремими організаціями для власних потреб. Перевагами є повний контроль над інфраструктурою та високий рівень безпеки. **Гібридні мережі** поєднують елементи публічних та приватних мереж, типовим прикладом є VPN.

За призначенням глобальні мережі класифікуються на мережі загального користування, корпоративні мережі, науково-освітні мережі (GEANT у Європі, Internet2 у США) та мережі спеціального призначення.

1.1.5. За середовищем передачі

Волоконно-оптичні кабелі є основним середовищем передачі даних у сучасних магістральних мережах. Вони забезпечують надзвичайно високу пропускну здатність (до терабітів на секунду), низький рівень загасання та невразливість до електромагнітних завад.

Мідні кабелі (вита пара, коаксіальний кабель) використовуються переважно на ділянках «останньої милі». Технології xDSL дозволяють використовувати існуючу телефонну інфраструктуру для доступу зі швидкостями до кількох сотень мегабітів на секунду.

Радіорелейні лінії зв'язку забезпечують передачу даних за допомогою мікрохвильового випромінювання між наземними станціями у прямій видимості.

Супутникові канали зв'язку забезпечують глобальне покриття, включаючи віддалені райони. Сучасні системи LEO (Starlink, OneWeb) зменшують затримку до 20–40 мс.

1.2. АРХІТЕКТУРИ WAN

Архітектура глобальної мережі визначає принципи організації фізичних та логічних з'єднань між вузлами мережі, розподіл функцій між мережевими елементами та загальну структуру мережевої інфраструктури. Правильний вибір архітектури WAN є критично важливим для забезпечення необхідної продуктивності, надійності, масштабованості та вартості мережевого рішення.

1.2.1. Фізичні та логічні топології WAN

Топологія мережі описує спосіб з'єднання вузлів та визначає шляхи передачі даних. У контексті глобальних мереж розрізняють фізичну топологію (реальне розташування обладнання) та логічну топологію (шляхи передачі даних).

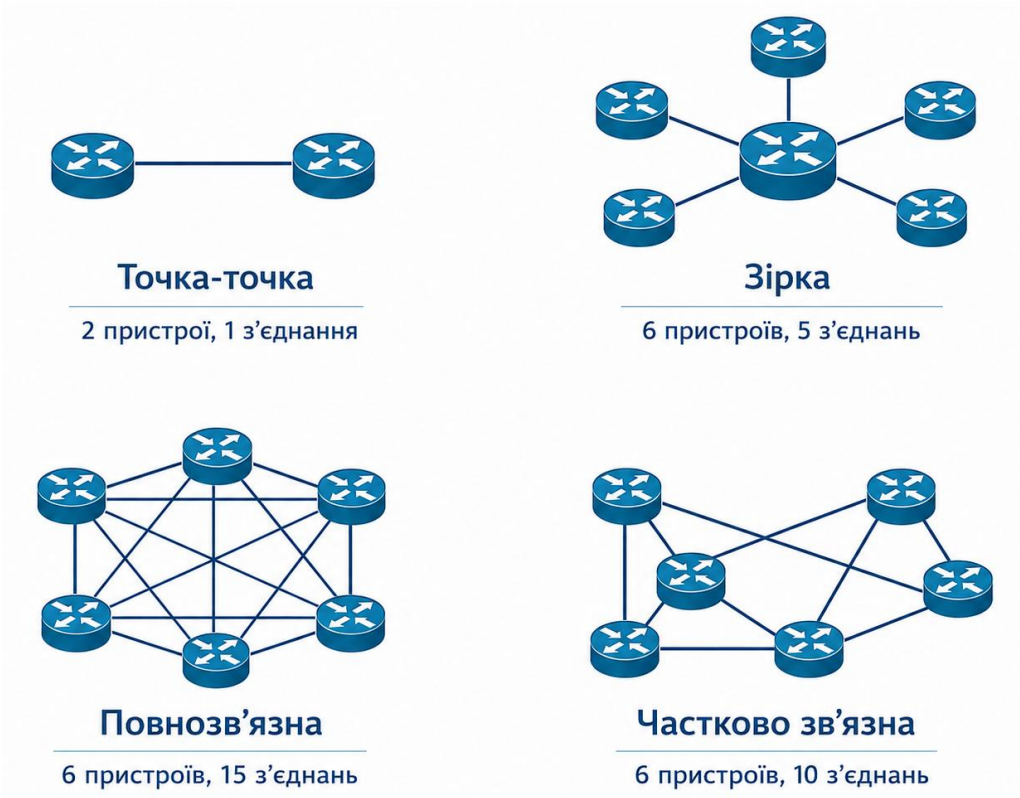

Рисунок 1.4 – Топології WAN

Топологія **«точка-точка»** (point-to-point) є найпростішою формою з'єднання у WAN, що забезпечує прямий зв'язок між двома вузлами. Перевагами є простота конфігурації, гарантована пропускна здатність та мінімальна затримка.

Топологія **«зірка»** або **«втулка та спиці»** (hub-and-spoke) передбачає наявність центрального вузла (hub), через який здійснюється зв'язок між периферійними вузлами (spokes). Ця топологія є найбільш поширеною у корпоративних WAN.

Повнозв'язна топологія (full mesh) забезпечує пряме з'єднання між кожною парою вузлів мережі. Ця топологія має найвищу відмовостійкість, але кількість необхідних з'єднань зростає квадратично: N(N-1)/2.

Частково зв'язна топологія (partial mesh) є компромісним рішенням між «зіркою» та повнозв'язною топологією. Прямі з'єднання встановлюються лише між тими вузлами, які потребують інтенсивного обміну даними.

1.2.2. Віртуальні приватні мережі (VPN)

Віртуальна приватна мережа (Virtual Private Network, VPN) — це технологія, що дозволяє створити захищене логічне з'єднання (тунель) через публічну мережу, зазвичай Інтернет. VPN забезпечує конфіденційність, цілісність та автентичність переданих даних за допомогою криптографічних протоколів.

Протокол IPsec (Internet Protocol Security) є одним із найпоширеніших протоколів для побудови VPN. IPsec підтримує два режими роботи: транспортний (шифрується лише вміст пакета) та тунельний (шифрується весь пакет разом із заголовком).

MPLS VPN є технологією побудови віртуальних приватних мереж на основі інфраструктури MPLS оператора зв'язку. Розрізняють L3VPN (маршрутизація на мережевому рівні) та L2VPN (прозоре з'єднання на канальному рівні).

SSL/TLS VPN використовують протоколи SSL/TLS для побудови захищених з'єднань. На відміну від IPsec, SSL VPN може працювати через стандартний веб-браузер, що спрощує розгортання для мобільних користувачів.

1.2.3. Концепція Overlay та Underlay мереж

Сучасна архітектура глобальних мереж часто базується на концепції розділення на два рівні: underlay (базова мережа) та overlay (накладена мережа). Ця концепція є фундаментом для побудови VPN, SD-WAN та інших сучасних рішень.

Underlay мережа — це фізична або логічна мережева інфраструктура, яка забезпечує базову зв'язність між вузлами. Вона включає фізичні канали зв'язку, мережеве обладнання та протоколи маршрутизації (OSPF, IS-IS, BGP).

Overlay мережа — це логічна мережа, побудована поверх underlay мережі за допомогою механізмів тунелювання та інкапсуляції. Технології VPN, VXLAN та GRE є прикладами механізмів побудови overlay мереж.

1.2.4. Програмно-визначені глобальні мережі (SD-WAN)

SD-WAN (Software-Defined Wide Area Network) є сучасною архітектурою глобальних мереж, яка застосовує принципи програмно-визначених мереж (SDN) до архітектури WAN. SD-WAN відокремлює площину управління від площини передачі даних (Data Plane), забезпечуючи централізоване управління WAN-інфраструктурою.

SD-WAN забезпечує інтелектуальне управління трафіком через кілька типів з'єднань одночасно: MPLS, широкосмуговий Інтернет, LTE/5G та інші. Контролер SD-WAN аналізує стан кожного з'єднання у реальному часі та динамічно обирає оптимальний маршрут для кожного потоку даних.

Ключові функції SD-WAN: централізоване управління через єдину консоль; динамічна маршрутизація на основі політик застосунків; автоматичне створення захищених тунелів із шифруванням AES-256; нульова конфігурація (zero-touch provisioning). SD-WAN дозволяє знизити витрати порівняно з традиційними MPLS-архітектурами.

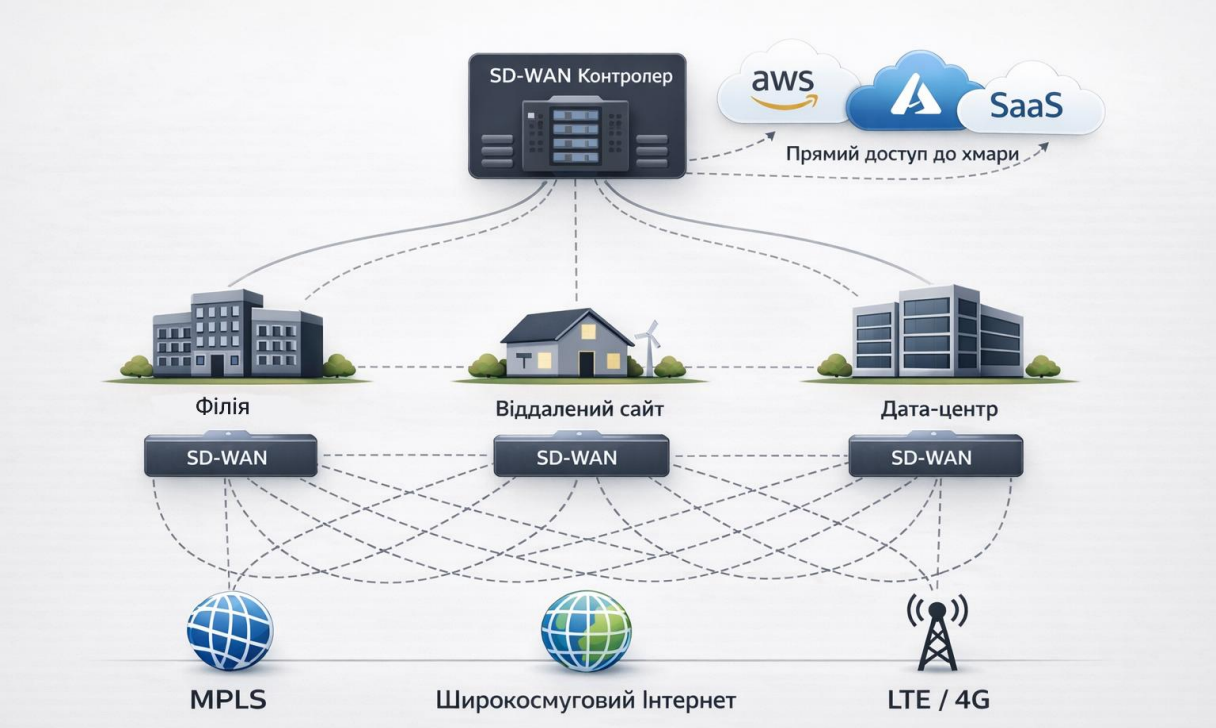

Рисунок 1.5 – Архітектура SD-WAN

1.2.5. Масштабованість та відмовостійкість WAN

Масштабованість мережі може бути горизонтальною (додавання нових вузлів) та вертикальною (збільшення пропускної здатності). Ієрархічна архітектура, що складається з ядра (core), рівня розподілу (distribution) та рівня доступу (access), забезпечує найкращу масштабованість.

Відмовостійкість WAN досягається шляхом резервування критичних компонентів: резервні канали різними маршрутами, дублювання обладнання, протоколи динамічної маршрутизації OSPF/BGP для автоматичного відновлення зв'язності після відмови. Для критичних застосунків вимагається доступність 99,99% («чотири дев'ятки») — не більше 52,6 хвилин простою на рік.

1.3. ОПЕРАТОРСЬКІ МЕРЕЖІ

Операторські мережі складають основу глобальної телекомунікаційної інфраструктури. Вони забезпечують транспортування даних між кінцевими користувачами, корпоративними мережами та центрами обробки даних, формуючи багаторівневу ієрархічну систему взаємоз'єднаних мереж.

1.3.1. Ієрархія провайдерів інтернет-послуг (ISP)

Структура глобальної мережі Інтернет базується на ієрархії провайдерів інтернет-послуг (ISP) трьох рівнів. Ця ієрархія відображає масштаб мережі провайдера, його роль у глобальній зв'язності та характер комерційних відносин.

Провайдери першого рівня (Tier 1) становлять вершину ієрархії та забезпечують глобальну зв'язність Інтернету через безкоштовні пірингові угоди. Серед

найвідоміших — Lumen Technologies, NTT Communications, Cogent Communications. Їхні магістральні мережі забезпечують пропускну здатність у десятки та сотні терабітів на секунду.

Провайдери другого рівня (Tier 2) мають регіональне або національне покриття та забезпечують зв'язність через пірингові угоди та купівлю транзитних послуг у Tier 1. Прикладами є Ukrtelecom в Україні, Deutsche Telekom, Orange.

Провайдери третього рівня (Tier 3) — місцеві провайдери, які забезпечують «останню милю» — підключення кінцевих користувачів до Інтернету.

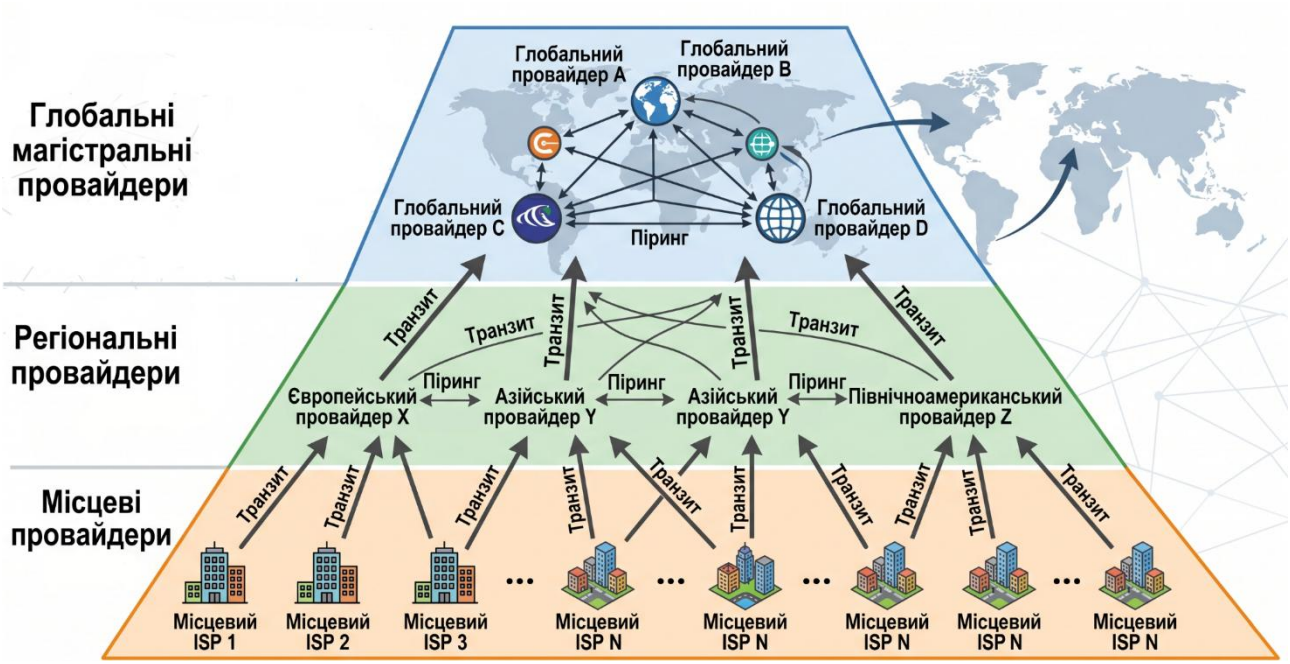

Рисунок 1.6 – Ієрархія провайдерів інтернет-послуг

1.3.2. Магістральні мережі (Backbone)

Магістральна мережа (backbone) — це високошвидкісна мережа, яка забезпечує транспортування даних між великими вузлами інфраструктури. Фізичну основу складають волоконно-оптичні кабелі з технологією DWDM, що дозволяє передавати до 96 і більше довжин хвиль із швидкістю 100–400 Гбіт/с кожна.

Підводні кабельні системи, такі як MAREA або JUPITER, мають пропускну здатність понад 200 Тбіт/с. Архітектурно магістральні мережі будуються за принципом повнозв'язної топології з потужними маршрутизаторами ядра, що обробляють мільйони пакетів на секунду.

1.3.3. Пірінг та точки обміну трафіком (IX)

Пірінг (peering) — це процес безпосереднього обміну трафіком між двома мережами без використання послуг третьої сторони. Розрізняють приватний пірінг (пряме з'єднання між маршрутизаторами) та публічний пірінг через точки обміну трафіком (IXP).

Точки обміну трафіком (IXP) зменшують затримки, знижують витрати на транзит та підвищують надійність Інтернету. Найбільшими IXP є DE-CIX у Франкфурті (понад 14 Тбіт/с), AMS-IX в Амстердамі та LINX у Лондоні. В Україні найбільшим є UA-IX (Kyiv Internet Exchange).

1.3.4. Протокол BGP та маршрутизація між автономними системами

Border Gateway Protocol (BGP) є основним протоколом міждоменної маршрутизації в Інтернеті. **Автономна система** (AS) — це сукупність IP-мереж під єдиним адміністративним контролем, що ідентифікується унікальним номером ASN. Поточна версія BGP-4 визначена у стандарті RFC 4271.

BGP належить до класу протоколів маршрутизації типу path-vector, тобто протоколів вектору шляху. Ключовим атрибутом є AS_PATH — упорядкований список номерів AS, через які проходить маршрут. Серед інших важливих атрибутів: LOCAL_PREF, MED, NEXT_HOP, COMMUNITY.

Безпека BGP є актуальною проблемою. Протокол вразливий до атак BGP hijacking та route leaks. Для підвищення безпеки розроблено механізм RPKI (Resource Public Key Infrastructure) та стандарт BGPsec (RFC 8205).

1.3.5. Транзит та мультихомінг

Транзит — це послуга, при якій один провайдер надає іншому доступ до всіх мереж Інтернету через свою інфраструктуру з оплатою за передачу трафіку.

Мультихомінг (multihoming) — це підключення мережі до двох або більше провайдерів для підвищення надійності та продуктивності. Реалізація вимагає протоколу BGP та власного блоку IP-адрес (PI-адреси) та номера AS.

1.4. МОДЕЛІ НАДАННЯ ПОСЛУГ

Модель надання послуг у глобальних мережах визначає спосіб, у який оператори та провайдери забезпечують клієнтів мережевими ресурсами. Еволюція відбулася від простої оренди виділених каналів до складних хмарних сервісів з оплатою за фактичне використання.

1.4.1. Традиційні моделі мережевих послуг

Оренда виділених каналів (leased lines) надає клієнту у постійне користування канал фіксованої пропускної здатності між двома точками з гарантованою пропускною здатністю та мінімальними затримками. Залишається затребуваною для критично важливих з’єднань.

Послуги MPLS VPN надаються на основі MPLS-інфраструктури оператора. Забезпечує ізоляцію трафіку, гарантовану QoS та масштабування без зміни архітектури клієнтської мережі. MPLS тривалий час залишався основною технологією корпоративних WAN.

Керовані мережеві послуги (Managed Network Services) передбачають, що оператор бере на себе відповідальність за управління обладнанням, моніторинг мережі та реагування на інциденти. Рівень відповідальності визначається угодою SLA.

1.4.2. Хмарні обчислення та моделі надання послуг

Хмарні обчислення (Cloud Computing) надають обчислювальні ресурси як послугу через Інтернет з оплатою за фактичне використання. NIST визначає п’ять основних характеристик: самообслуговування за запитом, широкий мережевий доступ, об’єднання ресурсів, швидка еластичність та вимірюване обслуговування.

IaaS (Infrastructure as a Service) надає базові обчислювальні ресурси: віртуальні сервери, сховища даних, мережі. Клієнт контролює ОС, додатки та мережеві налаштування. Приклади: Amazon EC2, Microsoft Azure, Google Compute Engine.

PaaS (Platform as a Service) надає платформу для розробки та розгортання застосунків без управління базовою інфраструктурою. Приклади: Google App Engine, Heroku, AWS Elastic Beanstalk.

SaaS (Software as a Service) надає готові програмні додатки через Інтернет. Провайдер повністю відповідає за всю інфраструктуру. Приклади: Microsoft 365, Google Workspace, Salesforce, Zoom.

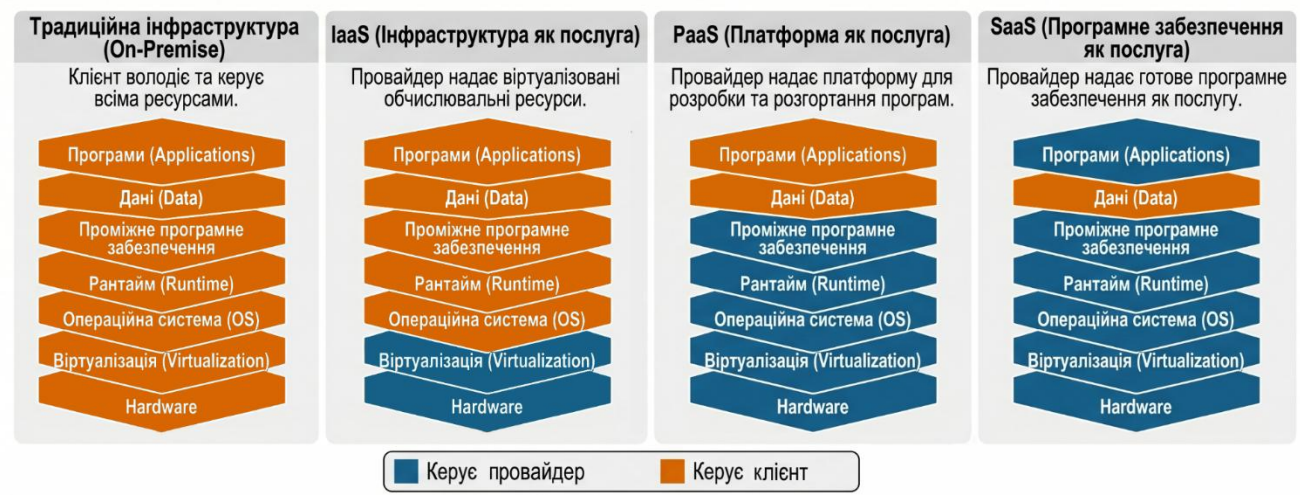

Рисунок 1.7 – Порівняння моделей хмарних послуг

Таблиця 1.2 — Порівняння моделей хмарних послуг

Характеристика	IaaS	PaaS	SaaS
Контроль клієнта	ОС, додатки, дані	Додатки, дані	Лише дані
Відп. провайдера	Обладнання, вірт.	+ОС, середовище	Все, крім даних
Гнучкість	Висока	Середня	Низька
Складність	Висока	Середня	Мінімальна
Типовий користувач	IT-адміністратори	Розробники	Бізнес-користувачі

1.4.3. Концепція XaaS та нові моделі послуг

Концепція XaaS (Everything as a Service) відображає тенденцію до надання будь-яких IT-ресурсів у формі хмарних сервісів.

NaaS (Network as a Service) надає мережеву інфраструктуру як хмарний сервіс. Клієнт отримує віртуальні мережеві ресурси без придбання фізичного обладнання.

SECaaS (Security as a Service) надає послуги кібербезпеки через хмару: захист від DDoS, моніторинг, управління вразливостями. Концепція SASE об'єднує SD-WAN та SECaaS.

UCaaS (Unified Communications as a Service) надає інтегровані комунікаційні сервіси: VoIP, відеоконференції, обмін повідомленнями. Приклади: Microsoft Teams, Zoom, Cisco Webex.

1.4.4. Угоди про рівень обслуговування (SLA)

Угода про рівень обслуговування (Service Level Agreement, SLA) — це формальний документ, який визначає параметри якості послуг та відповідальність сторін. SLA є ключовим елементом будь-якої моделі надання послуг.

Типова SLA для мережевих послуг включає: параметри доступності (наприклад, 99,95% — не більше 4 год 22 хв простою на рік); параметри продуктивності (пропускна здатність, затримка, джитер, втрати пакетів); параметри підтримки (час реагування, час відновлення); механізм компенсації (service credits — від 5% до 100% місячної плати).

1.5. QoS У ГЛОБАЛЬНИХ МЕРЕЖАХ

Якість обслуговування (Quality of Service, QoS) у глобальних мережах — це сукупність технологій та механізмів, що забезпечують диференційоване обслуговування різних типів мережевого трафіку відповідно до їхніх вимог. Без механізмів QoS мережа обробляє всі пакети однаково за принципом «найкращих зусиль» (best effort).

1.5.1. Основні параметри якості обслуговування

Пропускна здатність (bandwidth / throughput) визначає максимальний обсяг даних, який може бути переданий через канал за одиницю часу. Для голосового трафіку кодек G.711 потребує 64 кбіт/с, G.729 — 8 кбіт/с. Для HD-відеоконференції — від 4 до 8 Мбіт/с.

Затримка (latency / delay) — час передачі пакета від джерела до одержувача. Складається з затримки серіалізації, поширення, обробки та черги. Стандарт ITU-T G.114 рекомендує одностороннє значення не більше 150 мс для голосу.

Джитер (jitter) — варіація затримки між послідовними пакетами. Критичний параметр для голосового та відео трафіку. Рекомендоване значення для голосу — не більше 30 мс.

Втрати пакетів (packet loss) — відсоток пакетів, які не досягли одержувача. Для голосового трафіку допустимий рівень — не більше 1%. Для TCP-трафіку компенсується механізмом повторної передачі.

Таблиця 1.3 — Рекомендовані параметри QoS для різних типів трафіку

Тип трафіку	Затримка	Джитер	Втрати	Пропускна здатність
VoIP	< 150 мс	< 30 мс	< 1%	30–128 кбіт/с
Відеоконференція	< 200 мс	< 30 мс	< 1%	1–8 Мбіт/с
Критичні дані	< 300 мс	N/A	< 0,1%	Залежить від застосунку
Веб-трафік	< 500 мс	N/A	< 5%	Залежить від потреб
Передавання файлів	Некритична	N/A	< 5%	Максимальна

1.5.2. Моделі QoS: IntServ та DiffServ

Модель **IntServ** (RFC 1633) забезпечує гарантовану QoS для окремих потоків шляхом попереднього резервування ресурсів через протокол RSVP. IntServ визначає два класи: Guaranteed Service (верхня межа затримки) та Controlled Load. Головний недолік — проблема масштабованості у великих мережах.

Модель **DiffServ** (RFC 2474, 2475) є масштабованою альтернативою. Класифікує пакети за обмеженою кількістю класів на основі поля DSCP (6 біт у заголовку IP-пакета, до 64 класів). Ключова концепція — PHB (Per-Hop Behavior).

Стандарт DiffServ визначає: Default PHB (best effort); Expedited Forwarding (EF, DSCP 101110) — для голосового трафіку; Assured Forwarding (AF1–AF4, по 3 рівні відкидання); Class Selector (CS0–CS7) — для зворотної сумісності.

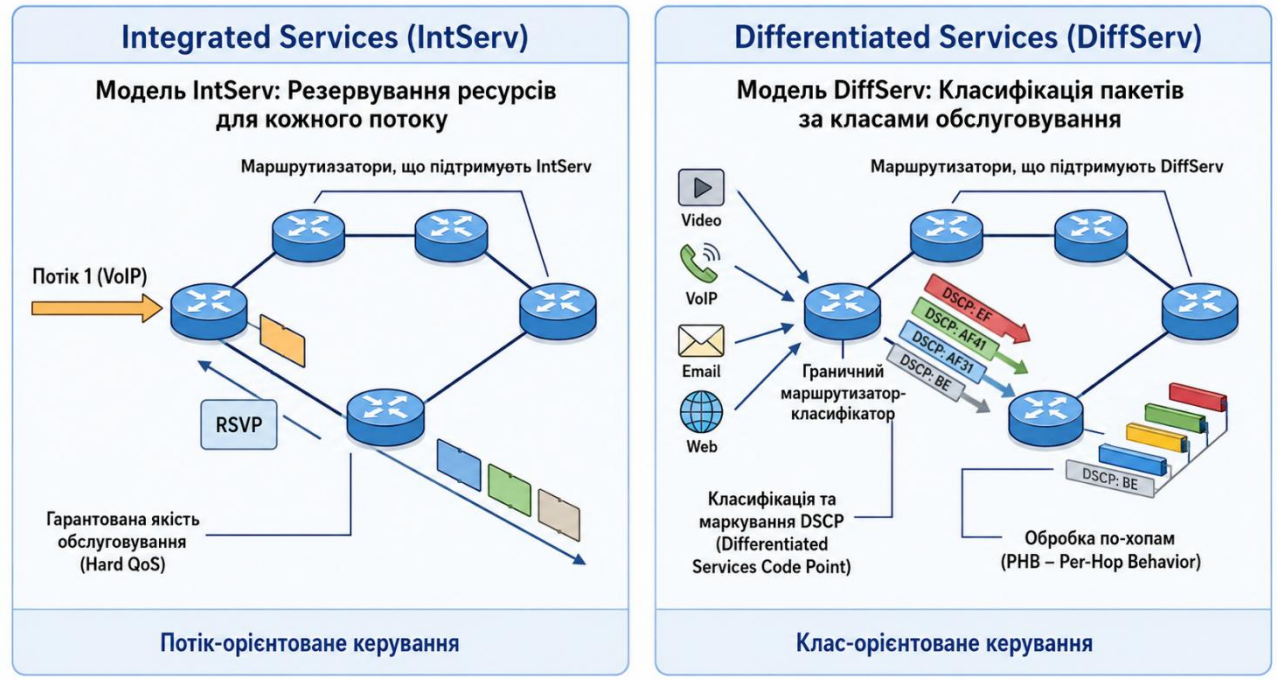

Рисунок 1.8 – Порівняння моделей QoS: IntServ та DiffSer

1.5.3. Механізми реалізації QoS

Реалізація QoS базується на комплексі механізмів: класифікація та маркування, управління перевантаженнями, запобігання перевантаженням та формування трафіку.

Управління перевантаженнями (congestion management): FIFO (без пріоритетів); Priority Queuing (абсолютний пріоритет); WFQ (зважене справедливе обслуговування); CBWFQ (окрема черга для кожного класу); LLQ — найпоширеніший механізм, поєднує пріоритетну чергу з CBWFQ.

Запобігання перевантаженням: Tail Drop (відкидає пакети при переповненні черги); WRED (Weighted Random Early Detection) — випадкове відкидання до переповнення з урахуванням пріоритету.

Формування трафіку (traffic shaping) згладжує піки за алгоритмом Token Bucket. Обмеження трафіку (traffic policing) відкидає або перемарковує надлишкові пакети — застосовується на вхідних інтерфейсах.

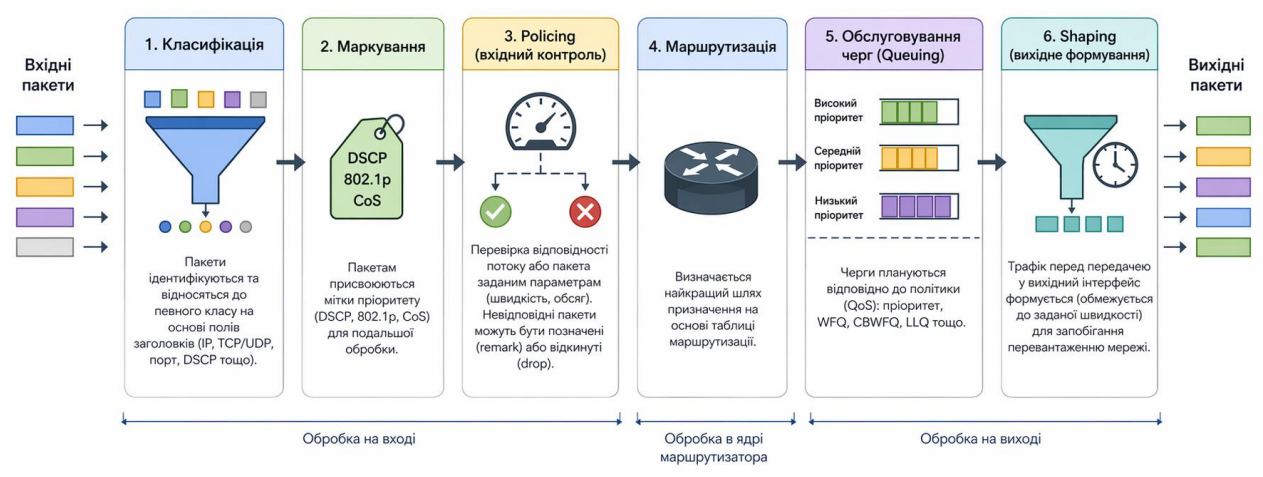

Рисунок 1.9 – Механізми QoS у мережевому обладнанні

1.5.4. QoS у технології MPLS

MPLS надає розширені можливості для QoS завдяки 3-бітному полю TC у заголовку MPLS, аналогічному DSCP. MPLS Traffic Engineering (MPLS-TE) дозволяє явно визначати шляхи проходження трафіку через мережу за допомогою протоколу RSVP-TE.

DiffServ-Aware MPLS-TE поєднує DiffServ та MPLS-TE, резервуючи пропускну здатність на LSP для кожного класу окремо: голосовий трафік отримує пріоритетне обслуговування, бізнес-критичні дані — гарантовану смугу, best-effort — ресурси що залишилися.

1.5.5. QoS у SD-WAN

SD-WAN використовує Application-Aware Routing — ідентифікацію конкретних застосунків за допомогою Deep Packet Inspection та застосування індивідуальних політик маршрутизації.

Контролер SD-WAN безперервно здійснює моніторинг стану кожного WAN-каналу (затримка, джитер, втрати) та динамічно обирає оптимальний канал для кожного застосунку. При погіршенні якості Інтернет-каналу голосовий трафік автоматично переключається на MPLS.

SD-WAN підтримує оптимізацію WAN: Forward Error Correction (FEC) для зменшення втрат; дуплікацію пакетів для критичних застосунків; оптимізацію TCP для каналів з високою затримкою; стиснення та дедуплікацію даних.

Контрольні питання

1. Дайте визначення поняття «глобальна мережа» (WAN). Чим WAN відрізняється від LAN та MAN?
2. Назвіть основні критерії класифікації глобальних мереж та охарактеризуйте кожен із них.
3. Порівняйте технології X.25, Frame Relay, ATM та MPLS за основними параметрами.
4. Опишіть основні топологічні рішення для WAN: переваги та недоліки кожного.
5. Що таке SD-WAN? Які переваги вона надає порівняно з традиційною MPLS-архітектурою?
6. Поясніть концепцію overlay та underlay мереж на прикладі VPN.
7. Охарактеризуйте ієрархію провайдерів інтернет-послуг (Tier 1, 2, 3).
8. Що таке IXP? Яку роль точки обміну трафіком відіграють в архітектурі Інтернету?
9. Порівняйте моделі хмарних послуг IaaS, PaaS та SaaS за ключовими характеристиками.
10. Назвіть основні параметри QoS та рекомендовані значення для голосового трафіку.
11. Порівняйте моделі QoS IntServ та DiffServ. Чому DiffServ є найбільш поширеним підходом у глобальних мережах завдяки кращій масштабованості?
12. Опишіть механізми реалізації QoS у SD-WAN. Що таке Application-Aware Routing?
13. Поясніть різницю між фізичною та логічною топологіями WAN. Наведіть приклад, коли вони не збігаються.
14. У чому полягає принципова відмінність між комутацією каналів, комутацією пакетів та комутацією комірок? Наведіть приклади технологій для кожного типу.
15. Опишіть архітектуру магістральної мережі (backbone). Яку роль у ній відіграє технологія DWDM та підводні кабельні системи?
16. Поясніть призначення протоколу BGP. Що таке автономна система (AS) та атрибут AS_PATH?
17. Що таке мультихомінг? Які вимоги він пред’являє до мережі організації та які переваги забезпечує?
18. Порівняйте традиційні моделі мережевих послуг: оренду виділених каналів, MPLS VPN та керовані мережеві послуги (Managed Network Services).
19. Опишіть концепцію XaaS (Everything as a Service). Чим відрізняються NaaS, SECaaS та UCaaS? Що таке концепція SASE?
20. Назвіть основні параметри типової SLA для мережевих послуг. Що означає доступність 99,95% у годинах простою на рік та як визначається механізм компенсації (service credits)?

РОЗДІЛ 2

ПЕРВИННІ ТА НАКЛАДЕНІ МЕРЕЖІ

У другому розділі увагу зосереджено на двох фундаментальних концепціях, що визначають архітектуру сучасних глобальних мереж: первинних (транспортних) мережах та накладених мережах.

Первинні мережі утворюють фізичний фундамент, на якому будуються всі інші мережеві сервіси. Вони забезпечують транспортування великих обсягів даних на значні відстані за допомогою оптичних технологій, таких як SDH та DWDM. Накладені мережі, у свою чергу, використовують ресурси первинних мереж для створення логічних структур із заданими властивостями — ізоляцією, гнучкістю, безпекою та масштабованістю. Взаємодія цих двох рівнів визначає ефективність, надійність та безпеку всієї глобальної мережевої інфраструктури.

Ключова ідея

Первинні (транспортні) мережі забезпечують фізичну основу передачі даних, тоді як накладені (overlay) мережі створюють логічні структури з потрібними властивостями. Розуміння взаємодії цих рівнів — ключ до проєктування сучасних телекомунікаційних систем.

2.1. ПЕРВИННІ МЕРЕЖІ (SDH, DWDM)

Первинні мережі (primary networks), також відомі як транспортні мережі (transport networks), становлять нижній рівень телекомунікаційної інфраструктури та забезпечують передачу даних між великими вузлами мережі. Їхньою головною функцією є формування високошвидкісних каналів зв’язку, якими користуються мережі вищих рівнів — мережі передачі даних IP/MPLS, мережі рухомого зв’язку, мережі кабельного телебачення та інші. Первинні мережі оперують цифровими потоками даних та оптичними сигналами, забезпечуючи мультиплексування, комутацію та захист каналів зв’язку на фізичному та канальному рівнях моделі OSI.

Історично еволюція первинних мереж відбувалася від аналогових систем передачі до цифрових плезіохронних систем (PDH), потім до синхронних цифрових систем (SDH/SONET) і, нарешті, до оптичних транспортних мереж (OTN) на базі технології DWDM. Кожен наступний етап забезпечував суттєве збільшення пропускної здатності, підвищення надійності та спрощення управління транспортною інфраструктурою. Сьогодні первинні мережі великих операторів зв’язку переважно побудовані на технологіях DWDM та OTN, хоча обладнання SDH залишається в експлуатації в багатьох регіонах світу.

2.1.1. Плезіохронна цифрова ієрархія (PDH)

Для розуміння принципів побудови сучасних транспортних мереж доцільно коротко розглянути їхнього попередника — **плезіохронну цифрову ієрархію** (Plesiochronous Digital Hierarchy, PDH). PDH стала першою масово розгорнутою технологією цифрової передачі в телекомунікаційних мережах, замінивши аналогові системи передачі на початку 1970-х років. Термін «плезіохронний» (від грецького «плезіо» — близький та

В основі PDH лежить принцип **мультиплексування з поділом за часом** (Time Division Multiplexing, TDM). Базовим каналом є цифровий канал зі швидкістю 64 кбіт/с, що відповідає одному оцифрованому телефонному каналу (кодування PCM із

частотою дискретизації 8 кГц та розрядністю 8 біт). Мультиплексування кількох базових каналів у канали вищого порядку утворює ієрархію швидкостей передачі. Існують дві незалежні ієрархії PDH — європейська (E1/E2/E3/E4) та північноамериканська (T1/T2/T3), які використовують різні коефіцієнти мультиплексування та швидкості.

Європейська ієрархія PDH починається з потоку E1 зі швидкістю 2,048 Мбіт/с, що об'єднує 30 телефонних каналів та 2 службових канали (всього 32 канали по 64 кбіт/с). Потік E2 зі швидкістю 8,448 Мбіт/с утворюється мультиплексуванням чотирьох потоків E1. Потік E3 зі швидкістю 34,368 Мбіт/с об'єднує чотири потоки E2, а потік E4 зі швидкістю 139,264 Мбіт/с — чотири потоки E3. Північноамериканська ієрархія базується на потоці T1 (DS1) зі швидкістю 1,544 Мбіт/с, що об'єднує 24 канали.

Головним недоліком PDH є відсутність прямого доступу до компонентних потоків нижчого порядку без повної демультиплексації агрегатного потоку. Наприклад, для вилучення одного потоку E1 із потоку E3 необхідно послідовно демультиплексувати E3 в чотири потоки E2, потім один із E2 — у чотири потоки E1, після чого вилучити потрібний E1, а решту — мультиплексувати назад. Ця процедура вимагає значної кількості обладнання, є енергоємною та ускладнює управління мережею. Крім того, PDH має обмежені можливості резервування та автоматичного перемикання у разі аварій. Саме ці обмеження стали причиною розробки синхронної цифрової ієрархії SDH.

2.1.2. Синхронна цифрова ієрархія (SDH)

Синхронна цифрова ієрархія (Synchronous Digital Hierarchy, SDH) — це стандартизована технологія транспортних мереж, розроблена ITU-T у кінці 1980-х років як наступник PDH. Паралельно в Північній Америці було розроблено аналогічний стандарт SONET (Synchronous Optical NETwork), який відрізняється деталями реалізації, але базується на тих самих принципах. SDH визначена серією стандартів ITU-T G.707, G.708, G.709 та іншими, які охоплюють формати передачі, архітектуру обладнання, механізми захисту та управління.

Фундаментальною відмінністю SDH від PDH є те, що всі елементи мережі SDH синхронізовані від єдиного джерела тактової частоти. Це забезпечує точне позиціонування компонентних потоків всередині агрегатного потоку та уможливлює пряме вставляння та вилучення (Add/Drop) будь-якого компонентного потоку без повної демультиплексації. Ця можливість реалізується за допомогою спеціального елемента мережі SDH — **мультиплексора вставляння-вилучення** (Add-Drop Multiplexer, ADM).

Базовим модулем передачі в SDH є синхронний транспортний модуль першого рівня STM-1 (Synchronous Transport Module level 1) зі швидкістю 155,52 Мбіт/с. Структура кадру STM-1 має вигляд матриці розміром 9 рядків на 270 стовпців (байтів), загальна тривалість кадру становить 125 мікросекунд, що відповідає частоті 8000 кадрів на секунду. Перші 9 стовпців кожного рядка відведені під секційний заголовок (Section OverHead, SOH), який поділяється на заголовок регенераторної секції (RSOH) та заголовок мультиплексної секції (MSOH). Решта 261 стовпець кожного рядка утворюють область корисного навантаження.

Рисунок 2.1 – Структура кадру STM-1 (SDH)

Ієрархія швидкостей SDH побудована на основі байт-інтерлівного мультиплексування кадрів STM-1. Модуль STM-4 утворюється мультиплексуванням чотирьох STM-1 та має швидкість 622,08 Мбіт/с. Модуль STM-16 — 2488,32 Мбіт/с (приблизно 2,5 Гбіт/с), STM-64 — 9953,28 Мбіт/с (приблизно 10 Гбіт/с), а STM-256 — 39813,12 Мбіт/с (приблизно 40 Гбіт/с). Слід зазначити, що рівні STM-64 та STM-256 практично не отримали широкого розповсюдження, оскільки на цих швидкостях більш ефективною виявилася технологія DWDM.

Таблиця 2.1 — Ієрархія швидкостей SDH та відповідність SONET

Рівень SDH	Рівень SONET	Швидкість, Мбіт/с	Кількість каналів E1
STM-1	OC-3 / STS-3	155,52	63
STM-4	OC-12 / STS-12	622,08	252
STM-16	OC-48 / STS-48	2 488,32	1 008
STM-64	OC-192 / STS-192	9 953,28	4 032
STM-256	OC-768 / STS-768	39 813,12	16 128

Для розміщення компонентних потоків PDH та інших даних у кадрі SDH використовується система контейнерів та віртуальних контейнерів. Контейнер (Container, C) визначає обсяг корисного навантаження для потоку певної швидкості: C-12 для потоку E1 (2 Мбіт/с), C-3 для потоку E3 (34 Мбіт/с) та C-4 для потоку E4 (140 Мбіт/с). **Додавання до контейнера заголовка маршруту** (Path OverHead, POH) **формує віртуальний контейнер** (Virtual Container, VC). Заголовок маршруту забезпечує наскрізний контроль якості передачі від точки формування до точки прийому віртуального контейнера.

2.1.3. Елементи мережі SDH та топології

Мережа SDH складається з кількох типів мережевих елементів. **Термінальний мультиплексор** (Terminal Multiplexer, TM) здійснює мультиплексування компонентних потоків PDH та Ethernet у агрегатний потік STM-N і навпаки. TM зазвичай розташовується на кінцях лінійного ланцюга та має один або два оптичних агрегатних порти та кілька трибутарних портів для підключення обладнання клієнтів.

Мультиплексор вставляння-вилучення (Add-Drop Multiplexer, ADM) є ключовим елементом мережі SDH. ADM підключається до двох або більше напрямків агрегатного потоку та забезпечує вставляння (add) та вилучення (drop) окремих віртуальних контейнерів без повної демультиплексації. Це означає, що з транзитного потоку STM-16, що проходить через ADM, можна вилучити, наприклад, один потік VC-12 (еквівалент E1) і направити його на трибутарний порт. Саме ця можливість є принциповою перевагою SDH над PDH.

Цифровий кросовий комутатор (Digital Cross-Connect, DXC) забезпечує неблокуючу комутацію віртуальних контейнерів між будь-якими портами. DXC використовується у вузлових точках мережі. **Регенератор** (Regenerator, REG) забезпечує відновлення форми, амплітуди та тактової частоти оптичного сигналу на протяжних ділянках. Максимальна відстань між регенераторами становить від 40 до 120 км.

Мережі SDH будуються за кількома типовими топологіями. Лінійний ланцюг (point-to-point) з'єднує два або більше вузлів послідовно. Кільцева топологія є найбільш поширеною та забезпечує вбудовані механізми захисту. У разі розриву волокна або відмови вузла трафік автоматично перемикається на резервний шлях кільця. Час перемикання згідно зі стандартом ITU-T G.841 не повинен перевищувати 50 мілісекунд.

Стандарт SDH визначає два основні типи кільцевих архітектур захисту. Однонаправлене кільце (UPSR/USHR) — топологічна схема, у якій робочий і захисний трафіки передаються по різних шляхах одного напрямку кільця. Як механізм захисту в таких кільцях зазвичай застосовують SNCP (Subnetwork Connection Protection), що забезпечує захист підмережевих з'єднань і може використовуватись як у кільцевих, так і в комірчастих топологіях. Двонаправлене **кільце з комутацією мультиплексних секцій** (MS-SPRing) використовує половину пропускної здатності кільця для робочого трафіку, а другу половину — для захисту.

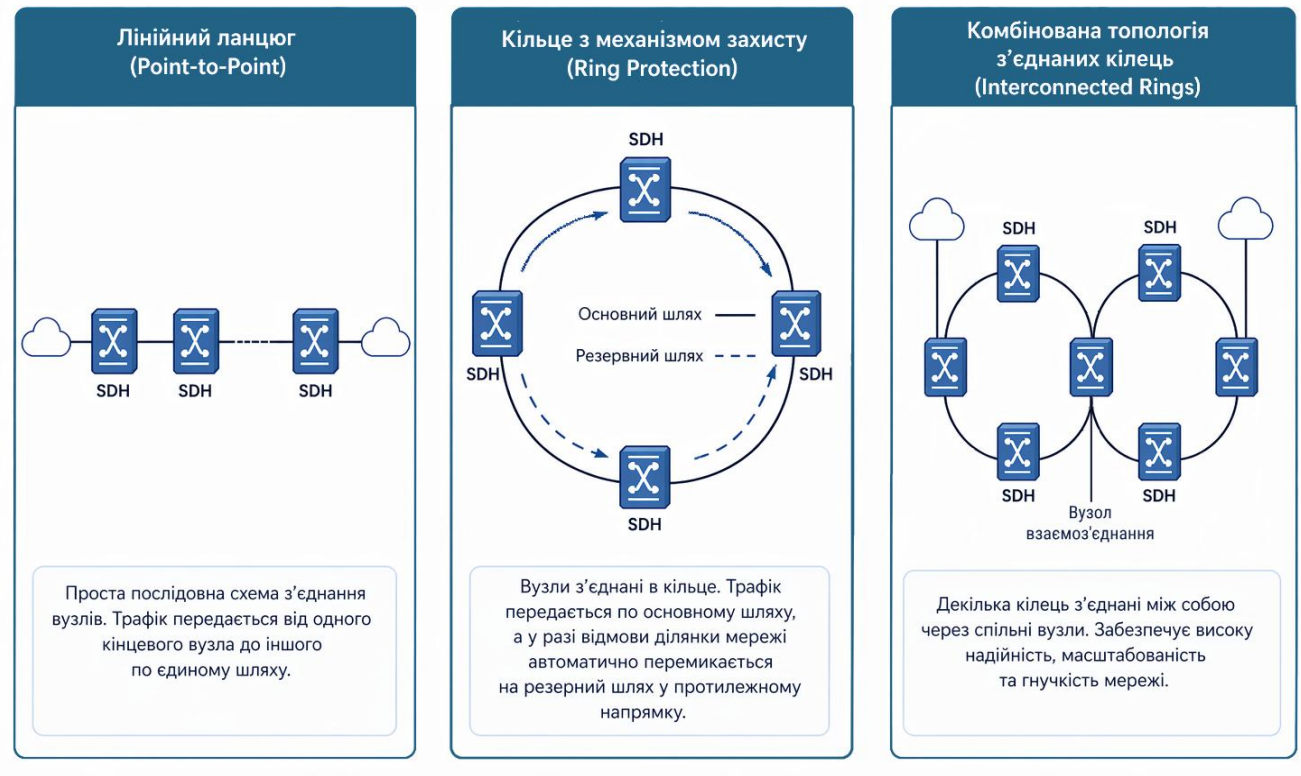

Рисунок 2.2 – Топології мережі SDH

> **Важливо**
>
> *Час перемикання SDH у разі аварії — менше 50 мс. Це стало де-факто стандартом «операторського класу» (carrier grade), якого має досягати кожна транспортна технологія.*

2.1.4. Щільне хвильове мультиплексування (DWDM)

Щільне хвильове мультиплексування (Dense Wavelength Division Multiplexing, DWDM) — це технологія оптичної передачі, що забезпечує одночасну передачу кількох оптичних сигналів різних довжин хвиль (каналів) по одному волокну. Кожна довжина хвилі утворює незалежний канал передачі, який може нести сигнал будь-якого формату — SDH, Ethernet, Fibre Channel, OTN та інші. DWDM є ключовою технологією сучасних магістральних мереж, оскільки дозволяє збільшити пропускну здатність волоконно-оптичної лінії у десятки та сотні разів без прокладання додаткових волокон.

Принцип роботи DWDM базується на тому, що оптичне волокно має широке вікно прозорості в діапазоні довжин хвиль приблизно від 1260 до 1625 нм. Стандарт ITU-T G.694.1 визначає сітку частот для каналів DWDM у діапазоні C-band (1530–1565 нм) та L-band (1565–1625 нм) з міжканальними інтервалами 100 ГГц, 50 ГГц, 25 ГГц та 12,5 ГГц. При міжканальному інтервалі 100 ГГц у діапазоні C-band розміщується до 40 каналів, а при інтервалі 50 ГГц — до 80 каналів.

Ключовими компонентами системи DWDM є оптичні транспондери, мультиплексори та демультиплексори, оптичні підсилювачі та системи управління. Транспондер (transponder) приймає оптичний сигнал від клієнтського обладнання на «сірій» довжині хвилі і перетворює його на сигнал «кольорової» довжини хвилі, що відповідає одному з каналів сітки DWDM. Сучасні когерентні транспондери підтримують швидкості 100 Гбіт/с, 200 Гбіт/с, 400 Гбіт/с та 800 Гбіт/с на один канал DWDM з використанням складних форматів модуляції, таких як DP-QPSK та DP-16QAM.

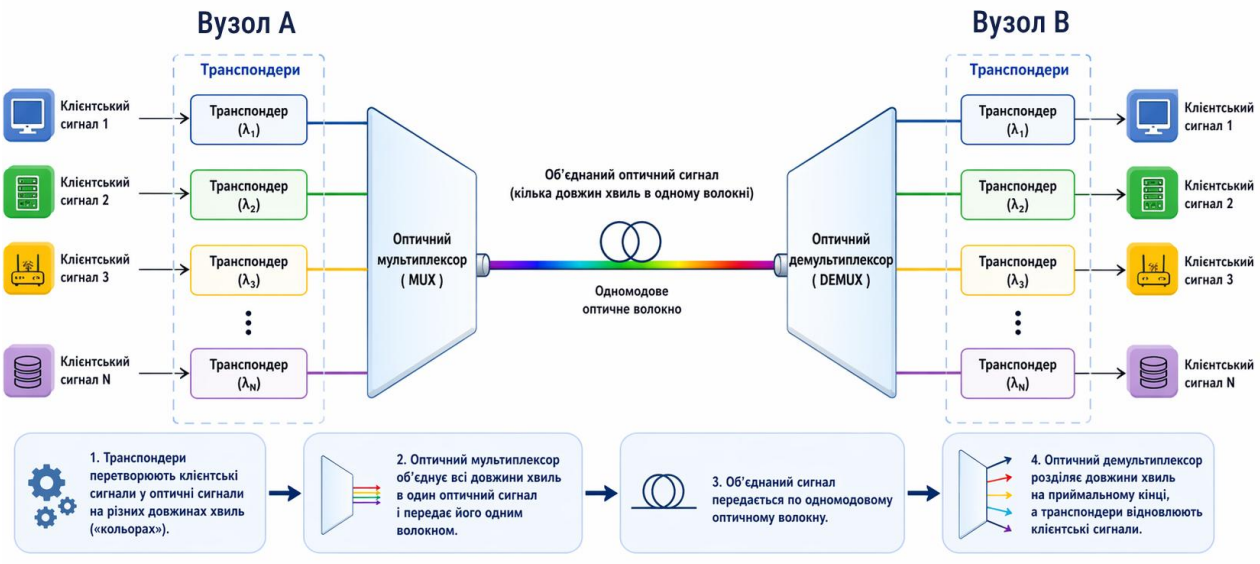

Рисунок 2.3 – Принцип роботи системи DWDM

Оптичні підсилювачі (Optical Amplifier, OA) забезпечують підсилення оптичного сигналу без перетворення в електричну форму, що є ключовою перевагою DWDM перед SDH. Найпоширенішим типом є підсилювач на основі волокна, легованого ербієм (Erbium-Doped Fiber Amplifier, EDFA), який працює у діапазоні C-band та L-band.

Один EDFA замінює десятки окремих регенераторів, необхідних у мережі SDH. Типова відстань між EDFA становить 80–120 км, а загальна дальність передачі без електричної регенерації може досягати 2000–3000 км.

Оптичні мультиплексори вставляння-вилучення (Reconfigurable Optical Add-Drop Multiplexer, ROADM) є ключовим елементом сучасних мереж DWDM. ROADM дозволяє вставляти та вилучати окремі довжини хвиль у транзитному оптичному сигналі без впливу на інші канали та без перетворення оптичного сигналу в електричний. Сучасні ROADM на основі технології WSS (Wavelength Selective Switch) підтримують гнучку конфігурацію напрямків передачі довжин хвиль між кількома волокнами.

2.1.5. Оптична транспортна мережа (OTN)

Оптична транспортна мережа (Optical Transport Network, OTN) — це технологія, визначена стандартом ITU-T G.709, яка поєднує переваги SDH (стандартизоване мультиплексування, механізми захисту, моніторинг) з можливостями DWDM (висока пропускна здатність, оптичне підсилення). OTN часто називають «цифровою обгорткою» (digital wrapper) для DWDM, оскільки вона додає до оптичних каналів DWDM стандартизовані заголовки для моніторингу якості передачі, виявлення помилок та управління.

Ієрархія OTN визначає оптичні канали різних швидкостей: OTU1 (приблизно 2,7 Гбіт/с, транспортує один потік STM-16 або GbE), OTU2 (приблизно 10,7 Гбіт/с, транспортує STM-64 або 10GbE), OTU3 (приблизно 43 Гбіт/с, транспортує STM-256 або 40GbE) та OTU4 (приблизно 112 Гбіт/с, транспортує 100GbE). Кожен рівень OTU має вбудований механізм прямої корекції помилок (Forward Error Correction, FEC), який суттєво підвищує дальність передачі та стійкість до шумів у порівнянні з «чистим» DWDM.

OTN підтримує механізм мультиплексування з поділом за часом, аналогічний SDH: кілька потоків OTU нижчого рівня можуть бути мультиплексовані в потік вищого рівня. Це забезпечує гнучке управління пропускною здатністю та ефективне використання оптичних каналів DWDM.

Таблиця 2.2 — Порівняння технологій SDH та DWDM

Параметр	SDH	DWDM
Принцип	Мультиплексування за часом (TDM)	Мультиплексування за довжиною хвилі
Макс. швидкість каналу	~10 Гбіт/с (STM-64)	400–800 Гбіт/с на канал
Макс. ємність волокна	~10 Гбіт/с	Десятки Тбіт/с
Підсилення	Електрична регенерація	Оптичне (EDFA)
Захист 50 мс	Так (стандартний)	Так (з OTN)
Гнучкість	Фіксовані швидкості	Будь-який формат у каналі
Статус	Поступово виводиться	Основна технологія

2.2. КОНЦЕПЦІЯ НАКЛАДЕНИХ МЕРЕЖ

Накладена мережа (overlay network) — це логічна мережа, побудована поверх існуючої фізичної або логічної мережевої інфраструктури (underlay network) за допомогою механізмів тунелювання та інкапсуляції. Концепція накладених мереж є одним із фундаментальних архітектурних принципів сучасних телекомунікацій, що дозволяє створювати мережеві структури із заданими властивостями — ізоляцією,

адресацією, безпекою, масштабованістю — незалежно від характеристик базової мережі. По суті, кожна наступна мережева технологія, від IP поверх Ethernet до VPN поверх Інтернету, є прикладом концепції overlay/underlay.

Як було зазначено у підрозділі 1.2 першого розділу, базова мережа (underlay) забезпечує фізичну зв'язність та транспортування пакетів між кінцевими точками, тоді як накладена мережа (overlay) додає логічну структуру, невидиму для underlay. Фундаментальним механізмом побудови overlay мереж є інкапсуляція (encapsulation): пакети overlay мережі вкладаються у пакети underlay мережі, утворюючи тунель. На вхідній точці тунелю пакет overlay мережі отримує додатковий заголовок underlay мережі, а на вихідній точці цей заголовок знімається. Таким чином, проміжні вузли underlay мережі обробляють лише зовнішній заголовок і не мають інформації про вміст тунелю, що забезпечує прозорість та ізоляцію.

2.2.1. Протоколи тунелювання

Тунелювання є ключовим механізмом побудови накладених мереж. Існує значна кількість протоколів тунелювання, кожен з яких оптимізований для конкретних завдань.

GRE (Generic Routing Encapsulation, RFC 2784) — один із найпростіших та найстаріших протоколів тунелювання, розроблений компанією Cisco. GRE інкапсулює **пакети будь-якого мережевого протоколу** (IPv4, IPv6, IPX та інших) у пакети IP. Заголовок GRE має мінімальний розмір 4 байти та може бути розширений до 16 байт з додаванням полів контрольної суми, ключа (для ідентифікації тунелю) та порядкового номера. GRE не забезпечує шифрування та автентифікації, тому для захисту даних зазвичай комбінується з IPsec.

IPsec (Internet Protocol Security, RFC 4301) у контексті накладених мереж забезпечує побудову захищених тунелів з шифруванням (протокол ESP) та автентифікацією (протокол AH) на мережевому рівні. IPsec у тунельному режимі повністю інкапсулює вихідний IP-пакет у новий IP-пакет із зашифрованим вмістом. Поєднання GRE та IPsec (GRE over IPsec) є поширеним рішенням, де GRE забезпечує інкапсуляцію різнорідного трафіку, а IPsec — його захист.

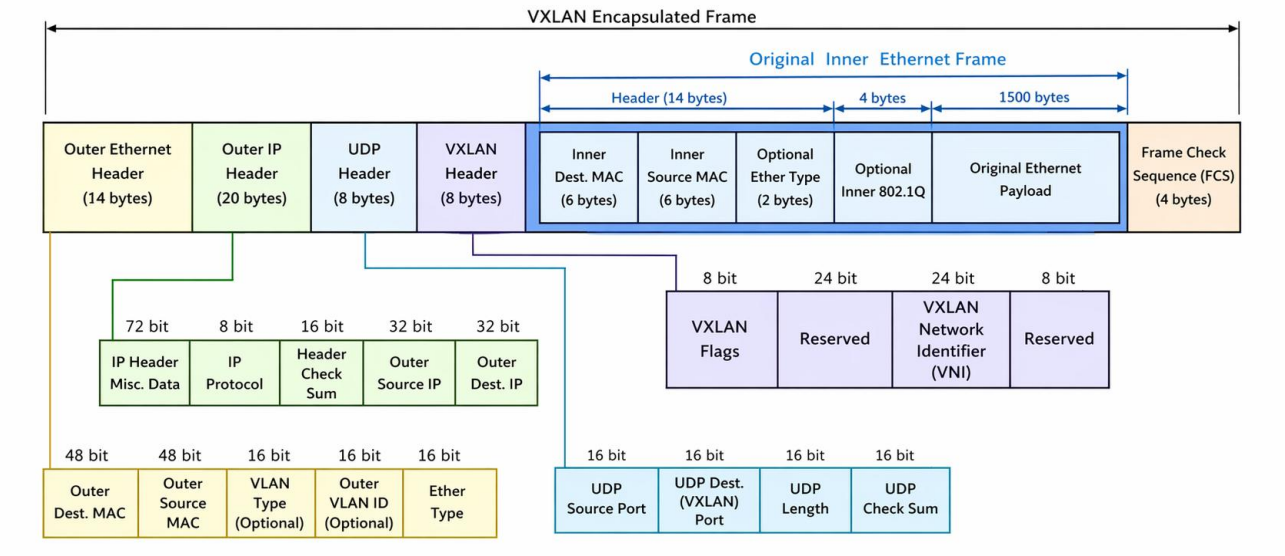

Рисунок 2.4 – Інкапсуляція кадру у VXLAN

VXLAN (Virtual Extensible LAN, RFC 7348) — це протокол тунелювання, розроблений спеціально для віртуалізації мереж у центрах обробки даних (ЦОД). VXLAN інкапсулює кадри Ethernet рівня 2 у пакети UDP/IP, дозволяючи створювати логічні мережі рівня 2, що розтягуються через мережу рівня 3. Це має ключове

значення для середовищ віртуалізації, де віртуальні машини повинні мігрувати між фізичними серверами у різних підмережах, зберігаючи свої MAC-адреси та мережеві з'єднання.

Заголовок VXLAN містить 24-**бітовий ідентифікатор мережі** (VXLAN Network Identifier, VNI), що дозволяє створити до 16 мільйонів ізольованих логічних мереж — на три порядки більше, ніж 4096 VLAN, доступних у стандарті IEEE 802.1Q. Кожна логічна мережа VXLAN (VXLAN segment) є повністю ізольованою. Кінцеві точки тунелів VXLAN називаються VTEP (VXLAN Tunnel Endpoint) і зазвичай реалізуються на комутаторах верхнього рівня (ToR) або у гіпервізорах.

NVGRE (Network Virtualization using Generic Routing Encapsulation, RFC 7637) — альтернативний протокол тунелювання для віртуалізації мереж, запропонований компанією Microsoft. NVGRE інкапсулює кадри Ethernet у пакети GRE/IP та

Geneve (Generic Network Virtualization Encapsulation, RFC 8926) — це протокол тунелювання нового покоління, розроблений як уніфікований стандарт, що об'єднує переваги VXLAN та NVGRE. Geneve використовує UDP-інкапсуляцію (як VXLAN), 24-бітовий ідентифікатор мережі (VNI) та, що найважливіше, заголовок змінної довжини з підтримкою TLV-розширень. TLV-розширення дозволяють передавати додаткову метаінформацію разом із тунельованими кадрами. Geneve поступово стає переважним протоколом тунелювання у нових розгортаннях, зокрема у рішеннях VMware NSX.

2.2.2. Віртуалізація мережевих функцій (NFV)

Концепція накладених мереж тісно пов'язана з віртуалізацією мережевих функцій (Network Functions Virtualization, NFV). NFV передбачає реалізацію мережевих функцій — маршрутизації, комутації, міжмережевого екранування, балансування навантаження, оптимізації WAN та інших — у вигляді програмного забезпечення, що виконується на стандартних серверах замість спеціалізованих апаратних пристроїв. NFV використовує накладені мережі для з'єднання віртуальних мережевих функцій (VNF — Virtual Network Functions) між собою та з фізичною інфраструктурою.

Архітектура NFV, визначена ETSI NFV ISG, складається з трьох основних компонентів. Інфраструктура NFV (NFVI) включає фізичні та віртуальні обчислювальні, мережеві та сховищні ресурси. **Віртуальні мережеві функції** (VNF) реалізують конкретні мережеві сервіси. **Менеджмент та оркестрація** (MANO) забезпечують автоматизоване розгортання, масштабування та управління VNF. Overlay мережі є критичним елементом NFVI, оскільки забезпечують гнучке з'єднання VNF між собою та з зовнішніми мережами незалежно від фізичного розташування серверів.

2.2.3. Програмно-визначені мережі та overlay

Програмно-визначені мережі (Software-Defined Networking, SDN) використовують концепцію overlay/underlay як основний архітектурний принцип. У моделі SDN контролер мережі має глобальне уявлення про топологію та стан мережі і програмує правила пересилки пакетів у мережевих пристроях через стандартизовані інтерфейси, такі як OpenFlow. Overlay мережі у SDN створюються контролером шляхом встановлення тунелів між вузлами мережі та налаштування правил інкапсуляції та маршрутизації.

Одним із найвідоміших практичних втілень концепції SDN overlay є VMware NSX — платформа мережевої віртуалізації для центрів обробки даних. NSX створює overlay мережу рівня 2 та рівня 3 поверх існуючої фізичної інфраструктури, використовуючи протоколи VXLAN або Geneve для тунелювання. У межах overlay мережі NSX реалізує повний набір мережевих функцій: розподілену маршрутизацію,

розподілений міжмережевий екран, балансування навантаження та VPN. Всі ці функції виконуються безпосередньо у гіпервізорі на кожному фізичному сервері, що забезпечує мікросегментацію та мінімальну затримку.

Іншим прикладом є Cisco ACI (Application Centric Infrastructure), яка поєднує SDN-**контролер** (APIC) із спеціалізованими комутаторами Nexus 9000 для побудови мережевої фабрики (fabric) ЦОД. ACI використовує протокол VXLAN для побудови overlay мережі та забезпечує автоматизоване управління мережевими **політиками на основі профілів застосунків** (Application Network Profiles, ANP).

Таблиця 2.3 — Порівняння протоколів тунелювання overlay мереж

Параметр	GRE	IPsec	VXLAN	NVGRE	Geneve
Рівень	L3	L3	L2 over L3	L2 over L3	L2 over L3
Транспорт	IP (47)	IP (50/51)	UDP:4789	GRE	UDP:6081
Ід. мережі	Key (32 біт)	SPI (32 біт)	VNI (24 біт)	VSID (24 біт)	VNI (24 біт)
Шифрування	Ні	Так (ESP)	Ні	Ні	Ні (зовн.)
Розширюваність	Обмежена	Ні	Ні	Ні	TLV-опції
Застосування	WAN VPN	Secure VPN	ЦОД overlay	ЦОД overlay	ЦОД overlay

2.2.4. Взаємозв’язок overlay та underlay мереж

Розуміння взаємозв’язку між overlay та underlay мережами є критично важливим для проєктування та експлуатації сучасних мережевих інфраструктур. Overlay мережа повністю залежить від underlay з точки зору базової зв’язності, пропускної здатності та надійності: якщо underlay мережа втрачає зв’язність між двома точками, тунелі overlay мережі між ними також перестають функціонувати. Тому проєктування underlay мережі повинно враховувати потреби всіх overlay мереж, що будуть на ній розгорнуті.

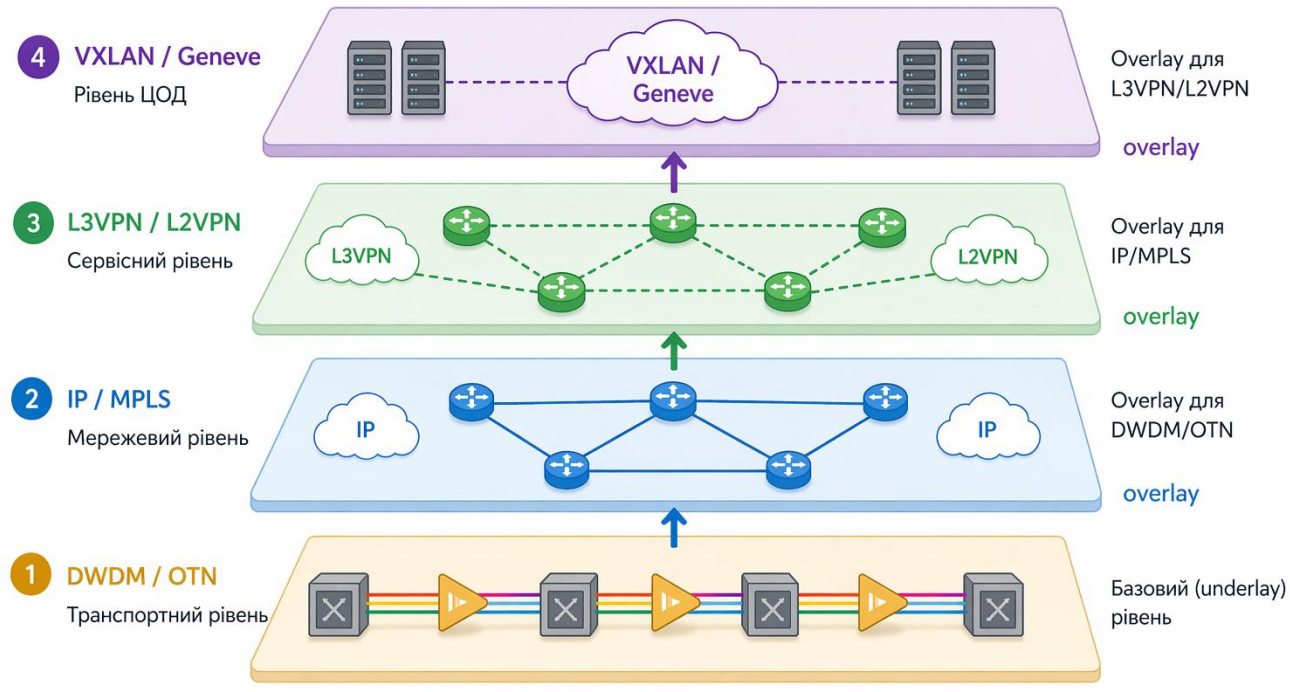

Рисунок 2.5 – Багаторівнева модель overlay/underlay мереж

Водночас overlay мережа є незалежною від underlay з точки зору адресації, маршрутизації та політик безпеки. Це означає, що зміни у конфігурації overlay мережі (додавання нових підмереж, зміна політик доступу, переміщення віртуальних машин) не вимагають змін у конфігурації underlay мережі. Ця незалежність забезпечує значну гнучкість та прискорює впровадження змін, що є особливо важливим у динамічних середовищах, таких як хмарні ЦОД.

У контексті первинних та накладених мереж можна виділити кілька рівнів абстракції. На найнижчому рівні знаходиться оптична інфраструктура DWDM/OTN, яка є underlay для всіх вищих рівнів. Поверх неї розгортається мережа IP/MPLS, яка є overlay відносно оптичної мережі та, одночасно, underlay для мереж наступного рівня. Мережі VPN (L3VPN, L2VPN) є overlay відносно мережі IP/MPLS. Нарешті, мережі VXLAN/Geneve у ЦОД є overlay відносно мережі IP. Кожен рівень абстракції додає нові функції (ізоляцію, безпеку, гнучкість), але також збільшує накладні витрати (overhead) на додаткові заголовки та обробку.

2.3. METRO ETHERNET

Metro Ethernet — це технологія надання послуг передачі даних на основі стандартів Ethernet у міських та регіональних мережах (Metropolitan Area Network, MAN). Metro Ethernet розширює знайому та широко розповсюджену технологію Ethernet за межі локальних мереж, забезпечуючи операторський клас обслуговування на міських та регіональних відстанях. Ця технологія стала домінуючою у сегменті мереж доступу та агрегації завдяки простоті, масштабованості, сумісності з існуючою інфраструктурою LAN та значно нижчій вартості порівняно з традиційними технологіями WAN, такими як SDH та ATM.

Стандартизацією послуг Metro Ethernet займається MEF (Metro Ethernet Forum, зараз офіційно відомий як MEF Forum) — галузева організація, що об’єднує операторів зв’язку, виробників обладнання та постачальників рішень. MEF визначає стандарти послуг, архітектуру мережі, параметри якості обслуговування та процедури сертифікації обладнання для забезпечення сумісності рішень різних виробників. Сертифікація MEF CE (Carrier Ethernet) підтверджує, що обладнання або послуга відповідає вимогам операторського класу.

2.3.1. Атрибути Carrier Ethernet

MEF визначає п’ять ключових атрибутів, які відрізняють Carrier Ethernet від звичайного LAN Ethernet та роблять його придатним для використання в мережах операторського класу.

Стандартизовані послуги — MEF визначає чітко специфіковані типи послуг (E-Line, E-LAN, E-Tree, E-Access), кожен з яких має стандартизований набір параметрів, що дозволяє клієнтам замовляти послуги у різних операторів із гарантованою сумісністю.

Масштабованість — Carrier Ethernet підтримує швидкості від 1 Мбіт/с до 100 Гбіт/с та забезпечує можливість зміни пропускної здатності без заміни обладнання.

Надійність — механізми захисту та відмовостійкості (spanning tree, ring protection, LAG) забезпечують доступність послуг на рівні, порівнянному з SDH.

Якість обслуговування — підтримка множинних класів обслуговування з гарантованими параметрами затримки, джитеру та втрат пакетів.

Управління та обслуговування — стандартизовані механізми OAM (Operations, Administration, and Maintenance) за стандартами IEEE 802.1ag та ITU-T Y.1731 забезпечують моніторинг якості, виявлення відмов та діагностику.

2.3.2. Типи послуг Metro Ethernet (MEF)

MEF визначає кілька стандартних типів послуг, які базуються на концепції Ethernet Virtual Connection (EVC) — логічного з'єднання між двома або більше інтерфейсами користувача (User Network Interface, UNI). EVC визначає, які UNI можуть обмінюватися кадрами, та може мати різні параметри QoS, пропускної здатності та CoS (Class of Service).

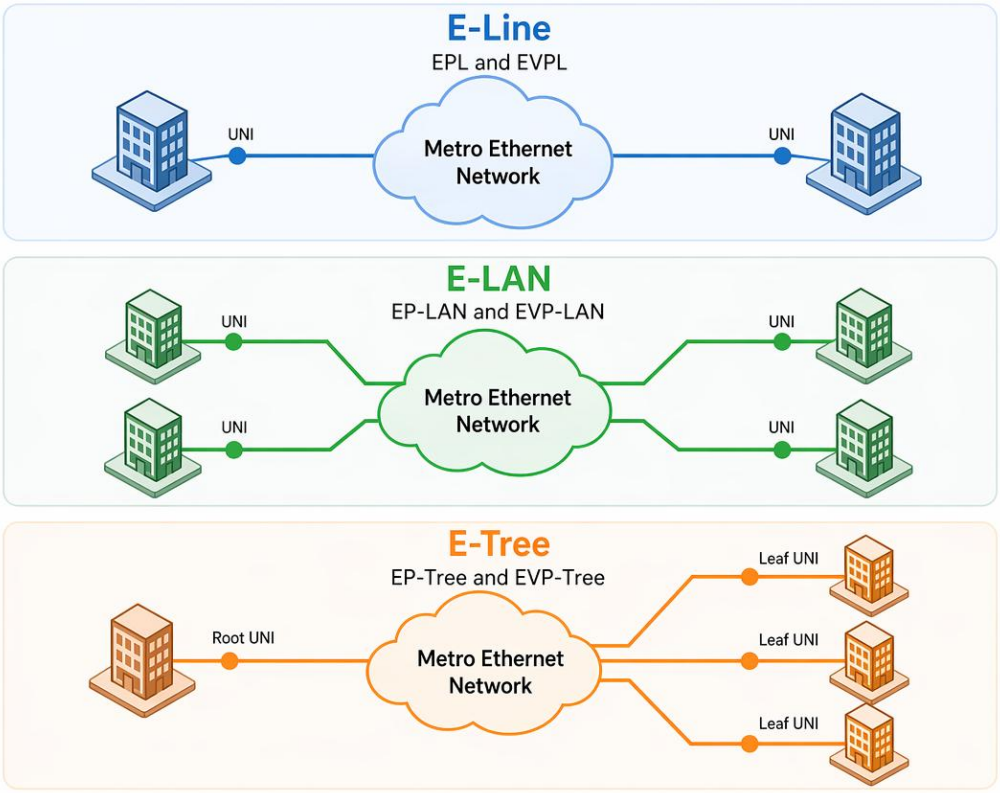

Рисунок 2.6 – Типи послуг Metro Ethernet (MEF)

E-Line (Ethernet Line Service) — це послуга з'єднання типу «точка-точка», що забезпечує двонаправлений обмін Ethernet-кадрами між двома UNI. E-Line є аналогом виділеного каналу (leased line), але на основі технології Ethernet. E-Line реалізується за допомогою EVC типу Point-to-Point. Ця послуга використовується для з'єднання двох офісів, підключення ЦОД до корпоративної мережі або організації резервного каналу зв'язку.

E-LAN (Ethernet LAN Service) — це послуга з'єднання типу «точка-багатоточок» (multipoint-to-multipoint), що забезпечує обмін кадрами між будь-якою парою UNI у межах однієї EVC. E-LAN є аналогом спільної локальної мережі, розтягнутої на відстані MAN. E-LAN зазвичай базується на технологіях VPLS (Virtual Private LAN Service) або EVPN (Ethernet VPN). Ця послуга використовується для об'єднання кількох офісів в єдину L2-мережу, де кожен офіс може безпосередньо обмінюватися даними з будь-яким іншим.

E-Tree (Ethernet Tree Service) — це послуга з'єднання типу «корінь-листок» (rooted multipoint), де один або кілька кореневих UNI (root) можуть обмінюватися кадрами з будь-яким UNI, тоді як листкові UNI (leaf) можуть обмінюватися кадрами лише з кореневими, але не між собою. E-Tree ідеально підходить для сценаріїв, де центральний вузол повинен мати доступ до всіх філій, але філії не повинні мати

прямого зв'язку між собою — наприклад, для IPTV, систем відеоспостереження або централізованих корпоративних застосунків.

2.3.3. Архітектура мережі Metro Ethernet

Архітектура мережі Metro Ethernet зазвичай складається з трьох рівнів: рівня доступу (access layer), рівня агрегації (aggregation layer) та рівня ядра (core layer). Ця ієрархічна архітектура забезпечує масштабованість, керованість та відмовостійкість мережі.

На рівні доступу розташовані комутатори доступу (access switches), які забезпечують підключення обладнання клієнтів (Customer Edge, CE) через інтерфейси UNI. Комутатори доступу виконують класифікацію трафіку, маркування QoS, обмеження пропускної здатності (rate limiting) та інкапсуляцію кадрів клієнтів у транспортні VLAN або MPLS-мітки. Підключення клієнтів зазвичай здійснюється через інтерфейси 100 Мбіт/с, 1 Гбіт/с або 10 Гбіт/с Ethernet.

Рівень агрегації об'єднує трафік від кількох комутаторів доступу та забезпечує його передачу до ядра мережі. Комутатори агрегації зазвичай з'єднані у кільцеву топологію з використанням протоколів захисту, таких як G.8032 (Ethernet Ring Protection Switching, ERPS). Протокол G.8032 забезпечує час перемикання менше 50 мілісекунд, що відповідає вимогам операторського класу та є порівнянним з механізмами захисту SDH. Між рівнем агрегації та ядром використовуються канали 10 Гбіт/с або 100 Гбіт/с.

Ядро мережі забезпечує високошвидкісну комутацію трафіку між вузлами агрегації та з'єднання з магістральними мережами. Ядро Metro Ethernet зазвичай побудоване на маршрутизаторах або комутаторах, що підтримують MPLS та забезпечують масштабовану маршрутизацію, Traffic Engineering та захист на рівні MPLS. Використання MPLS у ядрі дозволяє надавати послуги L2VPN (VPLS, EVPN) та L3VPN з гарантованою якістю обслуговування.

2.3.4. Технології транспорту в Metro Ethernet

Для передачі трафіку клієнтів через мережу Metro Ethernet використовуються кілька транспортних технологій. Стекування VLAN (QinQ або 802.1ad) є найпростішим підходом, при якому кадр клієнта з його VLAN-тегом (C-VLAN) інкапсулюється додатковим VLAN-тегом провайдера (S-VLAN). Це дозволяє ізолювати трафік різних клієнтів та зберегти VLAN-структуру клієнтської мережі прозоро. Однак QinQ має обмеження щодо масштабованості (4096 S-VLAN) та не підтримує механізмів Traffic Engineering.

MPLS (Multiprotocol Label Switching) є більш досконалим транспортним рішенням для Metro Ethernet. MPLS забезпечує масштабовану ізоляцію трафіку (через VPN-мітки), Traffic Engineering (через MPLS-TE), гарантовану якість обслуговування та швидке відновлення (через MPLS Fast Reroute). Для реалізації послуг E-Line використовується технологія pseudowire (PW), яка створює емуляцію з'єднання рівня 2 через мережу MPLS. Для реалізації послуг E-LAN використовуються технології VPLS (Virtual Private LAN Service, RFC 4761/4762) або EVPN (Ethernet VPN, RFC 7432). EVPN є сучаснішим рішенням, яке забезпечує більш ефективне вивчення MAC-адрес (через BGP замість flooding), мультихомінг (active-active) та інтеграцію з VXLAN.

PBB-TE (Provider Backbone Bridging with Traffic Engineering, IEEE 802.1Qay) використовує інкапсуляцію MAC-in-MAC для ізоляції трафіку та забезпечує Traffic Engineering без використання MPLS. PBB-TE **визначає явні шляхи для кадрів** (Ethernet Switched Paths, ESP) та підтримує механізми захисту, подібні до SDH. Однак PBB-TE не отримала широкого розповсюдження через домінування MPLS.

2.4. CARRIER GRADE NETWORKS

Carrier Grade Network (мережа операторського класу) — це мережева інфраструктура, що відповідає найвищим вимогам щодо надійності, доступності, масштабованості, безпеки та керованості, необхідним для надання телекомунікаційних послуг широкому колу клієнтів. Термін «carrier grade» (операторський клас) означає, що мережа здатна забезпечити рівень обслуговування, прийнятний для оператора зв'язку, який несе фінансову та юридичну відповідальність за якість послуг перед своїми клієнтами. Якщо мережі підприємств можуть допускати короткочасні простої для технічного обслуговування, то мережі операторського класу повинні функціонувати безперервно, забезпечуючи доступність на рівні «п'яти дев'яток» (99,999%), що відповідає не більше ніж 5 хвилинам 15 секундам незапланованого простою за рік.

2.4.1. Вимоги до мереж операторського класу

Побудова мережі операторського класу вимагає комплексного підходу, що охоплює всі аспекти мережевої інфраструктури — від вибору обладнання до проєктування архітектури та організації процесів експлуатації. Розглянемо ключові вимоги до таких мереж.

Висока доступність (High Availability, HA) є першочерговою вимогою до мережі операторського класу. Доступність визначається як частка часу, протягом якого послуга є працездатною, та вимірюється у відсотках. Рівень доступності 99,999% («п'ять дев'яток») означає максимальний час простою 5 хвилин 15 секунд на рік. Для досягнення такого рівня необхідне повне резервування всіх критичних компонентів: джерел живлення, процесорних модулів, інтерфейсних карт, вентиляторів охолодження та каналів зв'язку. Обладнання повинно підтримувати заміну компонентів у гарячому режимі (hot-swap) без переривання послуг. Програмне забезпечення повинно підтримувати оновлення без перезавантаження (In-Service Software Upgrade, ISSU).

Таблиця 2.4 — Рівні доступності та допустимий час простою

Рівень доступності	Кількість «дев'яток»	Макс. простій на рік
99%	Дві	3 доби 15 год 36 хв
99,9%	Три	8 год 45 хв 36 с
99,99%	Чотири	52 хв 34 с
99,999%	П'ять (carrier grade)	5 хв 15 с
99,9999%	Шість	31,5 с

Масштабованість (Scalability) визначає здатність мережі підтримувати зростаючу кількість клієнтів, сервісів та трафіку без деградації продуктивності та якості обслуговування. Масштабованість мережі операторського класу повинна забезпечуватися як горизонтально (додавання нових вузлів та каналів), так і вертикально (збільшення пропускної здатності існуючих каналів). Архітектура мережі повинна бути спроєктована з урахуванням прогнозованого зростання на 3–5 років, з можливістю подальшого розширення без суттєвої перебудови.

Якість обслуговування (Quality of Service, QoS) у мережах операторського класу повинна забезпечуватися на наскрізній основі (end-to-end) для кожного типу сервісу. Як було детально розглянуто у підрозділі 1.5, QoS включає управління пропускною здатністю, затримкою, джитером та втратами пакетів. У мережах операторського класу

механізми QoS повинні бути реалізовані на всіх рівнях мережі — від доступу до ядра — та забезпечувати виконання параметрів, визначених у SLA.

Безпека (Security) мережі операторського класу охоплює захист інфраструктури від зовнішніх та внутрішніх загроз, захист трафіку клієнтів від перехоплення та модифікації, а також забезпечення ізоляції між клієнтами. Ключовими елементами безпеки є: захист площини управління (Control Plane Protection) від DDoS-атак на протоколи маршрутизації, автентифікація пірів BGP та OSPF, шифрування управляючого трафіку (SSH, SNMPv3), фільтрація трафіку за допомогою Access Control Lists (ACL), захист від підміни адрес (spoofing) та впровадження механізмів RPKI для захисту BGP.

Керованість (Manageability) мережі операторського класу вимагає наявності розвинених систем мережевого управління (NMS), моніторингу (network monitoring) та автоматизації. Протоколи управління SNMP, NETCONF та gRPC забезпечують збір телеметрії та конфігурування обладнання. Сучасні мережі операторського класу все

2.4.2. Механізми забезпечення відмовостійкості

Відмовостійкість (fault tolerance) мережі операторського класу забезпечується на кількох рівнях: рівні обладнання, рівні каналів зв'язку та рівні сервісів. На рівні обладнання використовується апаратне резервування (hardware redundancy): дублювання процесорних модулів (Route Processor, RP) з механізмом Stateful Switchover (SSO), який забезпечує безперервність маршрутизації при переключенні на резервний процесор; дублювання комутаційної матриці (Switch Fabric); резервні джерела живлення з підключенням до різних електричних мереж та наявністю акумуляторних батарей та дизель-генераторів.

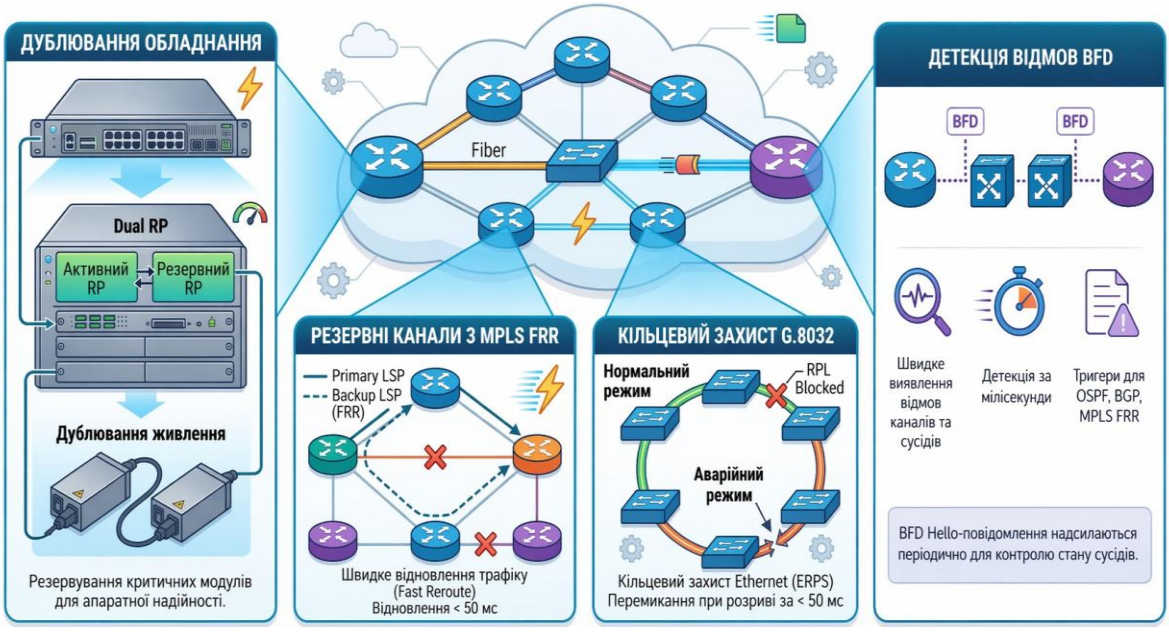

Рисунок 2.7 – Механізми відмовостійкості у мережі операторського класу

На рівні каналів зв'язку відмовостійкість забезпечується протоколами швидкого перемикання. У мережах MPLS використовується механізм Fast Reroute (FRR), визначений у RFC 4090, який забезпечує перемикання трафіку на резервний шлях протягом 50 мілісекунд. FRR попередньо обчислює резервний шлях (backup tunnel) для кожного захищеного з'єднання, що дозволяє миттєво перенаправити трафік у разі відмови, не очікуючи конвергенції протоколів маршрутизації. У мережах Ethernet використовується протокол G.8032 (ERPS), який забезпечує захисне перемикання у кільцевих топологіях за час менше 50 мс.

Протоколи маршрутизації забезпечують автоматичну конвергенцію мережі після відмови. OSPF та IS-IS з механізмами швидкої конвергенції (Sub-Second Fast IGP Convergence) забезпечують перерахунок маршрутів протягом секунд. BGP з механізмами Prefix Independent Convergence (PIC) та Add-Path забезпечує швидке перемикання між альтернативними шляхами у міждоменній маршрутизації. Механізм BFD (Bidirectional Forwarding Detection, RFC 5880) забезпечує швидке виявлення відмов каналів зв'язку (типово протягом 50–300 мс) та негайне сповіщення протоколів маршрутизації.

2.4.3. SLA та моніторинг у мережах операторського класу

Угода про рівень обслуговування (SLA) у мережах операторського класу визначає кількісні параметри якості, які оператор зобов'язується забезпечити, та фінансову відповідальність у разі їх порушення. Як було зазначено у підрозділі 1.4, SLA включає параметри доступності, затримки, джитеру, втрат пакетів та часу відновлення.

Для контролю виконання SLA використовуються активні та пасивні методи моніторингу. Активний моніторинг передбачає генерацію тестових пакетів та вимірювання параметрів їх доставки. Протокол ITU-T Y.1731 визначає стандартизовані механізми OAM для мереж Ethernet, включаючи Continuity Check Messages (CCM) для виявлення відмов, Loopback Messages (LBM/LBR) для перевірки зв'язності, Link Trace Messages (LTM/LTR) для визначення шляху кадрів та Frame Delay/Loss Measurement для вимірювання затримки та втрат. Протокол IP SLA (Service Level Agreement) від Cisco дозволяє вимірювати параметри QoS для IP-послуг шляхом генерації синтетичного трафіку.

Пасивний моніторинг базується на аналізі реального трафіку без генерації додаткових пакетів. Технології sFlow, NetFlow та IPFIX забезпечують збір статистики про потоки трафіку, що дозволяє аналізувати використання ресурсів, виявляти аномалії та планувати ємність мережі. Сучасні підходи до моніторингу все ширше використовують streaming telemetry на основі протоколів gRPC та gNMI, що забезпечує збір даних з обладнання у реальному часі з мінімальною затримкою та високою деталізацією.

2.4.4. Carrier Ethernet та перехід від SDH

Перехід від технології SDH до Carrier Ethernet є однією з ключових тенденцій у розвитку мереж операторського класу. Цей перехід зумовлений зростанням обсягів пакетного трафіку (IP, Ethernet), який витіснив традиційний трафік TDM (голос, виділені канали). SDH, розроблена для ефективної передачі TDM-трафіку, є неефективною для передачі пакетного трафіку через фіксований розподіл пропускної здатності та неможливість статистичного мультиплексування. Carrier Ethernet, навпаки, оптимізований для пакетного трафіку та забезпечує статистичне мультиплексування, яке дозволяє ефективно використовувати пропускну здатність при передачі пульсуючого трафіку.

Для забезпечення плавного переходу від SDH до Carrier Ethernet розроблено кілька технологій та підходів. Circuit Emulation Service (CES) дозволяє передавати трафік TDM (потоки E1, E3) через мережу Ethernet/MPLS, емулюючи виділений канал. Це дає змогу зберегти існуюче клієнтське обладнання TDM при переведенні транспортної мережі на Ethernet. Packet Transport Ethernet (PTE) та MPLS-TP (MPLS Transport Profile, RFC 5921) забезпечують транспортні функції, подібні до SDH (захист 50 мс, OAM, управління з'єднаннями), у пакетній мережі. MPLS-TP розроблено спільно ITU-T та IETF як міст між світом SDH та світом IP/MPLS.

◇ Контрольні питання

1. Дайте визначення первинної (транспортної) мережі. Назвіть основні етапи її історичної еволюції.
2. У чому полягає головний недолік ієрархії PDH і як його було подолано в SDH?
3. Опишіть структуру кадру STM-1 та призначення його основних полів (RSOH, MSOH, AU pointer).
4. Порівняйте функції елементів мережі SDH: TM, ADM, DXC, REG.
5. Що таке кільцева топологія SDH? Які типи захисту в ній використовуються (SNCP, MS-SPRing)?
6. Поясніть принцип роботи DWDM. Які діапазони C-band та L-band та який міжканальний інтервал є типовим?
7. Яку роль виконує EDFA у мережі DWDM? У чому його перевага над електричною регенерацією SDH?
8. Опишіть призначення ROADM та переваги, які він дає оператору зв’язку.
9. Що таке OTN та як вона співвідноситься з SDH і DWDM? Назвіть рівні OTU.
10. Дайте визначення overlay та underlay мереж. У чому їх взаємна залежність та незалежність?
11. Порівняйте протоколи тунелювання GRE, VXLAN та Geneve. Яке з них вибрати для віртуалізації ЦОД?
12. Що таке VNI та як він пов’язаний із масштабованістю VXLAN порівняно з VLAN?
13. Поясніть роль NFV та її зв’язок із концепцією overlay мереж.
14. Назвіть п’ять ключових атрибутів Carrier Ethernet за визначенням MEF.
15. Порівняйте типи послуг E-Line, E-LAN та E-Tree. Наведіть приклад застосування для кожної.
16. Опишіть трирівневу архітектуру Metro Ethernet: рівень доступу, агрегації та ядра.
17. Що означає рівень доступності 99,999% («п’ять дев’яток») у часі? Які заходи потрібні для його досягнення?
18. Поясніть механізми FRR та G.8032. Чим вони схожі та чим відрізняються?
19. Які параметри типово містить SLA операторського класу? Як здійснюється контроль їх виконання?
20. Які технології (CES, MPLS-TP) забезпечують перехід від SDH до Carrier Ethernet?

РОЗДІЛ 3

ПРОТОКОЛ IP У ГЛОБАЛЬНИХ МЕРЕЖАХ

Цей розділ присвячено ключовим аспектам функціонування IP у контексті WAN: адресації та маршрутизації в IPv4 та IPv6, ефективному використанню адресного простору через CIDR і VLSM, механізмам трансляції адрес NAT, керуванню трафіком та забезпеченню якості обслуговування на мережевому рівні.

Ключова ідея

Протокол IP виконує роль універсального «клею», що поєднує різнорідні канальні технології в єдину глобальну мережу. Розуміння IPv4, IPv6, CIDR, NAT та механізмів QoS на рівні IP є фундаментом для проєктування та експлуатації будь-якої сучасної WAN-інфраструктури.

3.1. IPv4 ТА IPv6 У ГЛОБАЛЬНИХ МЕРЕЖАХ

Протокол IP належить до мережевого рівня стеку TCP/IP та забезпечує адресацію вузлів і маршрутизацію пакетів у глобальних мережах. Сьогодні в Інтернеті паралельно функціонують дві версії — IPv4 та IPv6, — які істотно відрізняються за обсягом адресного простору, форматом заголовка, механізмами розширення функціональності та підходами до безпеки. Знання обох версій і принципів їхньої взаємодії є необхідною компетенцією фахівця з комп'ютерної інженерії та кібербезпеки.

3.1.1. Протокол IPv4: формат пакета та адресація

Протокол IPv4, визначений у RFC 791, залишається основою сучасного Інтернету попри обмеження його адресного простору. IPv4-адреса має довжину 32 біти (4 байти) і записується у десятковій нотації з крапками — наприклад, 192.168.1.100. Загальний обсяг адресного простору становить близько 4,3 мільярда адрес, чого виявилося недостатньо для сучасного Інтернету з мільярдами підключених пристроїв.

Рисунок 3.1 – Формат заголовка пакета IPv4

Заголовок пакета IPv4 має змінну довжину від 20 до 60 байтів. Серед його ключових полів варто виділити: Version (4 біти, значення 4 для IPv4), IHL (довжина заголовка у 32-бітових словах), DSCP/ECN (8 бітів, для класифікації трафіку та QoS), Total Length (загальна довжина пакета), поля фрагментації (Identification, Flags, Fragment Offset), TTL (максимальне число транзитних маршрутизаторів), Protocol (ідентифікатор протоколу верхнього рівня — 6 для TCP, 17 для UDP), Header Checksum, а також 32-бітові поля Source Address і Destination Address. Опціональні поля Options/Padding можуть розширити заголовок до 60 байтів.

IPv4 забезпечує негарантовану дейтаграмну доставку: кожен пакет маршрутизується незалежно, а послідовно надіслані пакети можуть проходити різними шляхами і прибувати у довільному порядку. Надійність доставки забезпечується протоколами транспортного рівня — насамперед TCP.

Історично адресний простір IPv4 поділявся на п’ять класів (A, B, C, D, E). Класова адресація виявилася неефективною через нерівномірний розподіл: мережа класу A (16 млн адрес) була надмірною для більшості організацій, а клас C (254 адреси) — недостатнім для середніх підприємств. Ці обмеження стимулювали розробку безкласової адресації CIDR, яку розглянемо в підрозділі 3.2.

Окрема важлива особливість IPv4 — механізм фрагментації. Оскільки різні канальні технології мають різні значення MTU (1500 байтів для Ethernet, 53 байти для ATM), маршрутизатори на межі мереж можуть розбивати великі пакети на фрагменти. Фрагментація збільшує навантаження на мережу, а втрата одного фрагмента вимагає повторної передачі всього пакета. Тому сучасна практика рекомендує використовувати Path MTU Discovery (RFC 1191) для визначення мінімального MTU на шляху та формування пакетів відповідного розміру без фрагментації.

3.1.2. Протокол IPv6: нове покоління IP

Протокол IPv6 (RFC 8200) розроблено для подолання обмежень IPv4 — насамперед вичерпання адресного простору. Робота над IPv6 (тоді IPng — IP next generation) розпочалася у першій половині 1990-х років, коли стало зрозумілим неминуче вичерпання адрес. Офіційне вичерпання вільних IPv4-адрес IANA сталося у лютому 2011 року, після чого регіональні інтернет-реєстри (RIR) почали поступово вичерпувати власні запаси.

Адреса IPv6 має довжину 128 бітів (16 байтів), забезпечуючи адресний простір приблизно $3{,}4 \cdot 10^{38}$ адрес — на 96 порядків більше за IPv4. Запис здійснюється у шістнадцятковій нотації, де кожні 16 бітів (4 шістнадцяткові цифри) розділяються двокрапкою, наприклад: 2001:0db8:0000:0000:0000:0000:0000:0001. Для скорочення дозволено опускати ведучі нулі та замінювати одну найдовшу послідовність нульових груп подвійною двокрапкою (::), тож наведену адресу можна записати як 2001:db8::1.

Адресний простір IPv6 використовує чотирирівневу ієрархію. Глобальна індивідуальна адреса (Global Unicast Address) складається з глобального префікса маршрутизації (зазвичай /48, виділяється провайдером), ідентифікатора підмережі (16 бітів, що дозволяє організації мати до 65 536 підмереж) та ідентифікатора інтерфейсу (64 біти). Ідентифікатор інтерфейсу може формуватися автоматично з MAC-адреси за алгоритмом EUI-64 або генеруватися випадково для приватності (Privacy Extensions, RFC 8981).

IPv6 визначає три типи адрес: індивідуальні (unicast), групові (multicast) та anycast. На відміну від IPv4, у IPv6 немає широкомовних (broadcast) адрес — їхню роль повністю виконують мультикастові. Зокрема, ff02::1 відповідає групі «всі вузли на локальному каналі», а ff02::2 — «всі маршрутизатори на локальному каналі». Anycast-

адреса виглядає як unicast, але призначена кільком інтерфейсам на різних вузлах; пакет доставляється до найближчого вузла за метрикою маршрутизації.

Серед спеціальних адрес IPv6 варто згадати: link-local (fe80::/10) — автоматично призначаються кожному інтерфейсу та дійсні лише в межах одного канального сегмента; unique local (fc00::/7, переважно fd00::/8) — аналог приватних адрес RFC 1918, призначений для внутрішніх мереж; адресу зворотної петлі ::1 (аналог 127.0.0.1) та невизначену адресу :: (аналог 0.0.0.0).

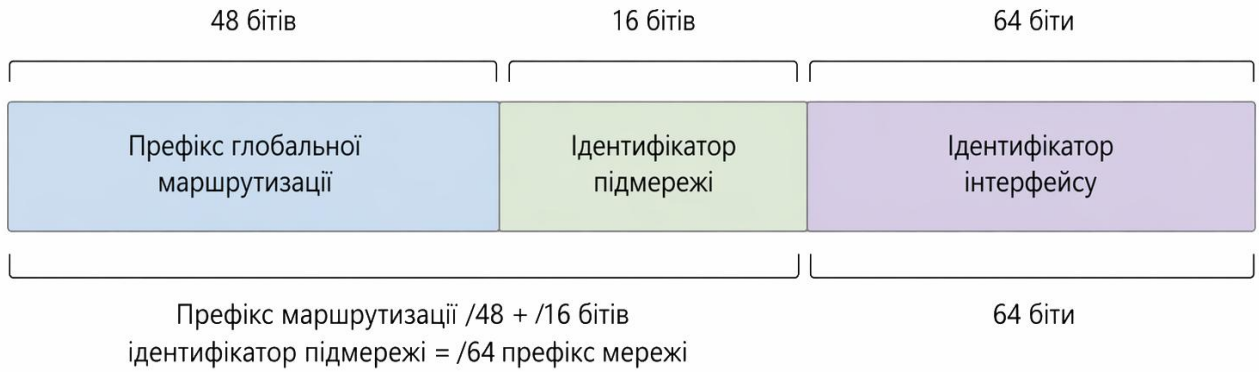

Рисунок 3.2 – Структура глобальної індивідуальної адреси IPv6

3.1.3. Заголовок IPv6 та розширення

Заголовок IPv6 має фіксовану довжину 40 байтів — істотна відмінність від IPv4 із його змінною довжиною. **Спрощення заголовка** — це усвідомлене архітектурне рішення: вилучено поля, які рідко використовувалися або сповільнювали обробку. Фіксована довжина прискорює апаратну обробку, оскільки позиція наступного заголовка завжди відома.

Заголовок IPv6 містить вісім полів: Version (4 біти, значення 6); Traffic Class (8 бітів, аналог DSCP/ECN для QoS); Flow Label (20 бітів, для ідентифікації потоку пакетів з однаковими вимогами до обробки); Payload Length (16 бітів, довжина корисного навантаження); Next Header (ідентифікатор наступного заголовка або протоколу верхнього рівня); Hop Limit (аналог TTL); Source Address і Destination Address (по 128 бітів). Порівняно з IPv4 вилучено поля IHL (зайве при фіксованому заголовку), Identification/Flags/Fragment Offset (фрагментація винесена в окремий заголовок розширення) та Header Checksum (контроль цілісності забезпечують канальний і транспортний рівні).

Особливістю IPv6 є механізм заголовків розширення (Extension Headers), що замінює поле Options протоколу IPv4. Заголовки розширення утворюють ланцюг: Next Header основного заголовка вказує на перший розширений, його Next Header — на наступний і так далі до останнього, який вказує на протокол верхнього рівня. Стандарт визначає такі заголовки розширення: Hop-by-Hop Options (обробляється кожним маршрутизатором на шляху), Routing (визначає шлях через задані проміжні вузли), Fragment, Authentication Header та Encapsulating Security Payload (для IPsec), Destination Options. Принципово важливо: фрагментацію в IPv6 виконує лише вузол-відправник, а не транзитні маршрутизатори, що спрощує обробку та підвищує продуктивність.

Таблиця 3.1 — Порівняння IPv4 та IPv6

Параметр	IPv4	IPv6
Довжина адреси	32 біти	128 бітів
Адресний простір	≈ 4,3 млрд	≈ $3{,}4 \cdot 10^{38}$
Заголовок	20–60 байтів (змінний)	40 байтів (фіксований)
Фрагментація	Маршрутизатори + хост	Лише хост
Контрольна сума	Так (Header Checksum)	Немає
Broadcast	Підтримується	Замінено multicast
IPsec	Опціонально	Вбудований (рекомендований)
Автоконфігурація	DHCP	SLAAC + DHCPv6
NAT	Широко використовується	Не потрібен (end-to-end)
QoS (Flow Label)	Відсутній	20-бітове поле

3.1.4. Механізми переходу від IPv4 до IPv6

Перехід від IPv4 до IPv6 — складний і тривалий процес, який не може відбутися одномоментно через масштаб глобальної інфраструктури. Для плавного переходу розроблено кілька механізмів співіснування та взаємодії двох протоколів.

Dual Stack (подвійний стек) — підхід, за якого мережеві пристрої одночасно підтримують обидва протоколи й можуть обмінюватися даними з вузлами кожної версії. Кожен інтерфейс має щонайменше одну IPv4- та одну IPv6-адресу. Вибір протоколу для з'єднання здійснюється за результатом DNS-запиту: запис AAAA → IPv6, запис A → IPv4. Механізм Happy Eyeballs (RFC 8305) оптимізує цей вибір, паралельно ініціюючи з'єднання обома протоколами та використовуючи те, яке встановлюється швидше, з пріоритетом IPv6. Dual stack — рекомендований підхід для переходу, бо забезпечує повну сумісність і дозволяє поступово переводити сервіси на IPv6.

Тунелювання дозволяє передавати IPv6-пакети через мережі, що підтримують лише IPv4. IPv6-пакет інкапсулюється в IPv4-пакет (протокол 41) і передається як звичайний IPv4-трафік; на вихідному кінці тунелю заголовок IPv4 знімається. Серед механізмів: 6to4 (RFC 3056) — автоматичні тунелі через IPv4-мережу з префіксом 2002::/16; 6in4 (RFC 4213) — ручні тунелі між визначеними кінцевими точками; ISATAP — зв'язність IPv6 у корпоративній мережі через IPv4-інфраструктуру; Teredo (RFC 4380) — тунелювання IPv6 через NAT з UDP/IPv4-інкапсуляцією.

Трансляція протоколів забезпечує обмін даними між вузлами лише з IPv4 та лише з IPv6. NAT64 (RFC 6146) перетворює пакети IPv6 на IPv4 і навпаки, дозволяючи IPv6-вузлам взаємодіяти з IPv4-серверами. DNS64 (RFC 6147) доповнює NAT64, синтезуючи записи AAAA для доменів, що мають лише A-записи, додаванням спеціального префікса (типово 64:ff9b::/96) до IPv4-адреси. Комбінація NAT64/DNS64 — ефективне рішення для мереж, що працюють виключно на IPv6, і забезпечує доступ до IPv4-ресурсів без необхідності dual stack на клієнтських пристроях.

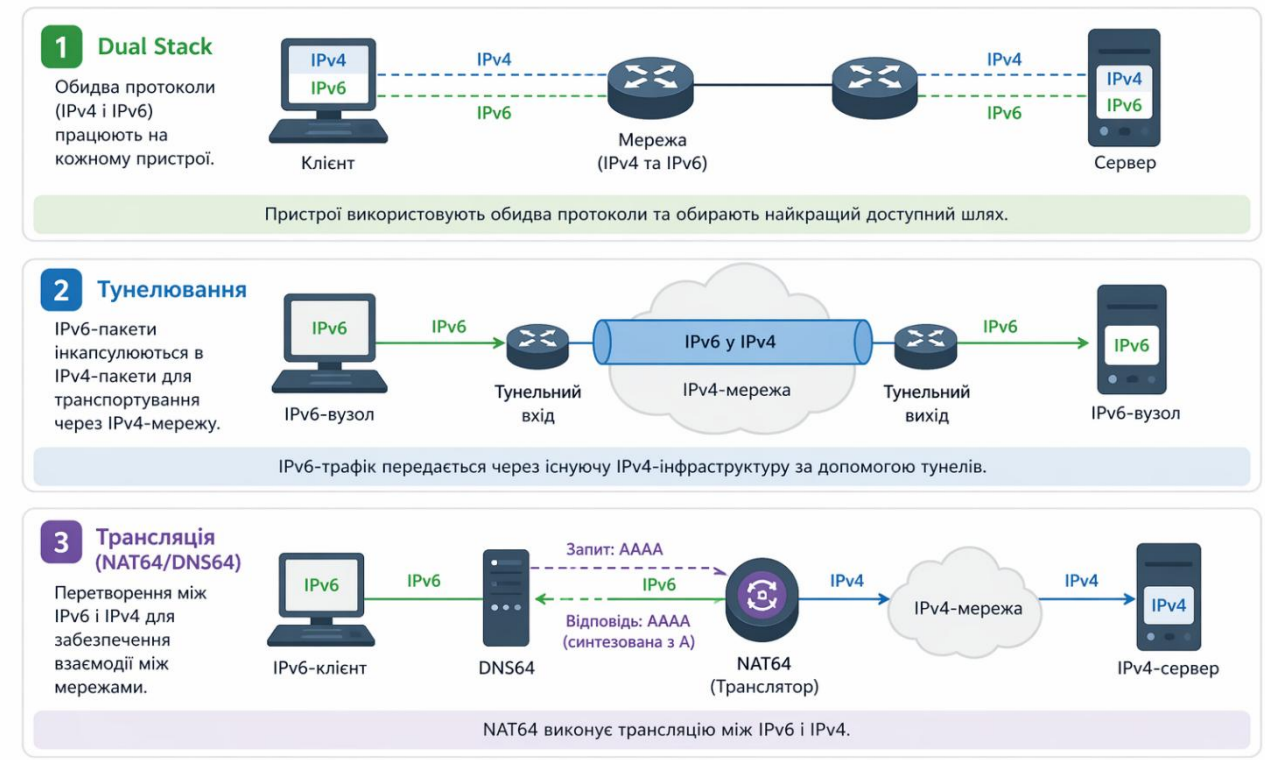

Рисунок 3.3 – Механізми переходу від IPv4 до IPv6

3.2. CIDR ТА VLSM

Класова адресація IPv4 створювала серйозні проблеми з ефективністю використання адресного простору. На початку 1990-х років стало очевидним, що темпи виділення мереж класу C призведуть до швидкого вичерпання адрес, а класи B виділяти стало економічно невиправдано через їхню надмірність. Рішенням стала безкласова адресація CIDR (Classless Inter-Domain Routing, RFC 4632) у поєднанні з VLSM (Variable Length Subnet Mask), які разом дозволили гнучко розподіляти адресний простір відповідно до реальних потреб.

3.2.1. Принципи CIDR

Основна ідея CIDR — відмова від жорсткого поділу простору на класи фіксованого розміру та перехід до гнучкого розподілу адрес на основі префіксів довільної довжини. Замість класів A, B, C з фіксованими межами між мережевою та хостовою частинами адреси (8, 16 чи 24 біти) CIDR дозволяє встановлювати межу в будь-якій позиції за допомогою маски підмережі або нотації з косою рискою. Наприклад, запис 192.168.10.0/22 означає мережу з 22-бітним префіксом, що включає 1024 адреси — кількість, недосяжну при класовій адресації.

Ключова перевага CIDR — можливість агрегації маршрутів (route aggregation, supernetting). Агрегація заміняє кілька окремих маршрутних записів одним узагальненим. Наприклад, чотири мережі 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 та 192.168.3.0/24 агрегуються в один маршрут 192.168.0.0/22. Це істотно зменшує розмір таблиць маршрутизації магістральних маршрутизаторів Інтернету. Без CIDR кількість маршрутів у глобальній таблиці BGP перевищила б можливості обладнання значно раніше — станом на 2024–2025 рр. глобальна BGP-таблиця містить понад 950 000 IPv4-префіксів, що стало можливим саме завдяки агрегації.

Для ефективної агрегації потрібна ієрархічність розподілу адресного простору: суміжні адресні блоки виділяються одному провайдеру або організації. IANA виділяє

великі блоки регіональним інтернет-реєстрам (RIR), ті — локальним інтернет-реєстрам (LIR)

3.2.2. VLSM та проєктування підмереж

VLSM дає змогу використовувати маски підмереж різної довжини в межах однієї мережі, забезпечуючи ефективний розподіл адресного простору відповідно до реальних потреб кожної підмережі. До впровадження VLSM протоколи маршрутизації на кшталт RIPv1 вимагали однакової маски для всіх підмереж однієї мережі, що призводило до значних втрат адрес.

Розгляньмо практичний приклад. Організація отримала мережу 10.1.0.0/16 (65 534 адреси) і має підрозділи з різною кількістю вузлів: головний офіс — 500 вузлів, два регіональні офіси — по 120 вузлів, п'ять філій — по 25 вузлів та десять з'єднань «точка-точка» між маршрутизаторами (по 2 адреси кожне). За фіксованої маски /24 (254 адреси) для з'єднань «точка-точка» витрачалося б 254 адреси замість потрібних двох, а для головного офісу довелося б виділити дві мережі /24. VLSM дозволяє виділити /23 для головного офісу (510 адрес), /25 для регіональних офісів (по 126 адрес), /27 для філій (по 30 адрес) та /30 для з'єднань «точка-точка» (по 2 адреси), забезпечуючи мінімальні втрати адресного простору.

Підтримка VLSM вимагає протоколів маршрутизації, що передають інформацію про маску підмережі разом із мережевою адресою: OSPFv2, IS-IS, EIGRP, RIPv2 та BGP-4. Застарілий RIPv1 не підтримує VLSM, тому не придатний для сучасних мереж.

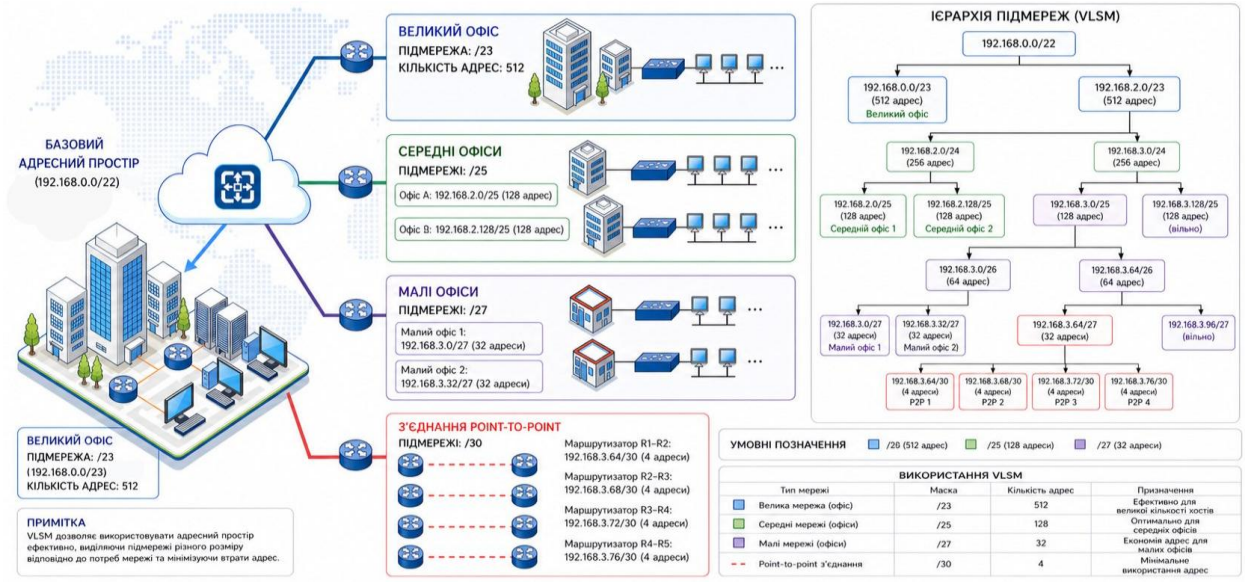

Рисунок 3.4 – Приклад використання VLSM для ефективного розподілу адресного простору

3.3. NAT У ГЛОБАЛЬНИХ МЕРЕЖАХ

Трансляція мережевих адрес (Network Address Translation, NAT) — механізм, що перетворює IP-адреси у заголовках пакетів під час їх проходження через маршрутизатор або міжмережевий екран. NAT розроблено як тимчасове рішення проблеми вичерпання адресного простору IPv4: він дозволяє великій кількості пристроїв з приватними IP-адресами (RFC 1918) використовувати спільну публічну IP-адресу для виходу в Інтернет. Попри те що IPv6 принципово вирішує проблему адресного простору, NAT залишається надзвичайно поширеним у сучасних мережах через інерцію впровадження IPv6 та додаткові функції безпеки, які він забезпечує.

3.3.1. Типи NAT

Статичний NAT (Static NAT) забезпечує постійне однозначне відображення між приватною та публічною IP-адресою. Кожній внутрішній адресі відповідає одна зовнішня, і це відображення не змінюється з часом. Статичний NAT використовується для серверів, які мають бути доступними з Інтернету за фіксованою адресою — веб-серверів, поштових серверів, VPN-шлюзів. Він не економить адреси, оскільки кожній внутрішній відповідає окрема зовнішня, але забезпечує двосторонню зв'язність та передбачуване відображення.

Динамічний NAT (Dynamic NAT) використовує пул публічних адрес, з якого внутрішнім адресам динамічно виділяються зовнішні при ініціації з'єднання. Після завершення з'єднання зовнішня адреса повертається до пулу. Динамічний NAT забезпечує певну економію адрес, якщо не всі внутрішні пристрої одночасно потребують доступу до Інтернету, але не є ефективним рішенням для мереж із великою кількістю активних пристроїв.

PAT (Port Address Translation), або NAT overloading чи NAPT (RFC 3022), — найпоширеніший тип NAT, що дозволяє множині внутрішніх пристроїв одночасно використовувати одну публічну IP-адресу. PAT транслює не лише IP-адресу, а й номер порту TCP/UDP. Кожне з'єднання отримує унікальну комбінацію (зовнішня IP-адреса, зовнішній порт), завдяки чому маршрутизатор однозначно ідентифікує з'єднання та спрямовує відповідні пакети до відповідного внутрішнього пристрою. Оскільки номер порту — 16-бітне поле, теоретично одна публічна адреса може обслуговувати до 65 535 одночасних з'єднань; на практиці кількість обмежена ресурсами маршрутизатора та зарезервованими портами і зазвичай становить 20 000–40 000.

Carrier Grade NAT (CGN, або LSN — Large Scale NAT, RFC 6888) — це NAT, що виконується на обладнанні інтернет-провайдера для спільного використання обмеженої кількості публічних IPv4-адрес великою кількістю абонентів. CGN створює додатковий рівень трансляції: абоненти використовують адреси з діапазону 100.64.0.0/10 (RFC 6598, спеціально виділеного для CGN), які транслюються в публічні адреси на обладнанні провайдера. CGN дозволяє провайдерам підключати нових абонентів навіть після вичерпання публічних IPv4-адрес, але створює проблеми для застосунків, що потребують вхідних з'єднань, та ускладнює ідентифікацію користувачів за IP-адресою.

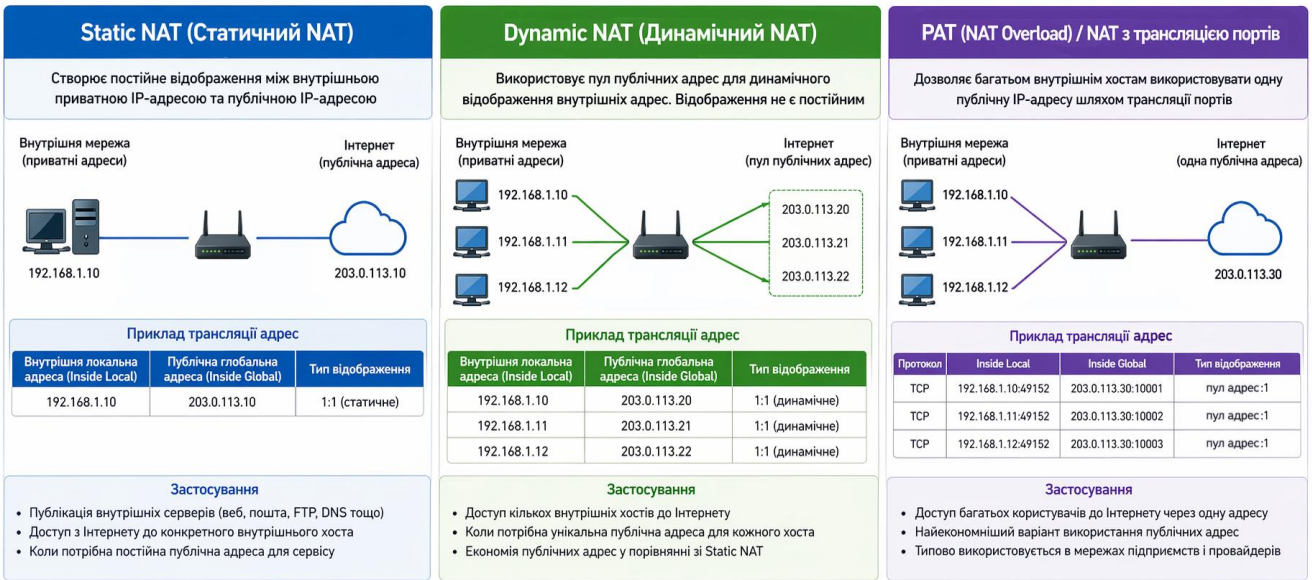

Рисунок 3.5 – Типи NAT та їх застосування

3.3.2. NAT та проблеми наскрізної зв’язності

Попри широке поширення, NAT порушує один із фундаментальних принципів архітектури Інтернету — наскрізну зв’язність (end-to-end connectivity). В оригінальній архітектурі IP кожен пристрій має унікальну глобальну адресу й може безпосередньо обмінюватися даними з будь-яким іншим. NAT руйнує цю модель: пристрої за NAT мають лише приватні адреси й недоступні з Інтернету напряму. Це створює проблеми для протоколів і застосунків, що потребують вхідних з’єднань або передають IP-адреси у корисному навантаженні.

До протоколів, що мають проблеми з NAT, належать: FTP (в активному режимі передає IP-адресу в команді PORT); SIP та H.323 (VoIP-протоколи, що передають адреси для встановлення медіапотоків); IPsec у транспортному режимі (перевіряє цілісність IP-заголовка, який змінює NAT). Для подолання цих проблем розроблено механізми NAT Traversal: UPnP та NAT-PMP дозволяють застосункам автоматично налаштовувати правила перенаправлення портів на домашніх маршрутизаторах; STUN (RFC 8489) дає змогу вузлу за NAT визначити свою зовнішню адресу та тип NAT; TURN (RFC 8656) забезпечує ретрансляцію трафіку через проміжний сервер, коли пряме з’єднання неможливе; ICE (RFC 8445) автоматично обирає найкращий метод обходу NAT для конкретної ситуації, поєднуючи STUN і TURN.

З погляду безпеки NAT часто помилково розглядається як механізм захисту, оскільки приховує внутрішню структуру мережі та запобігає прямому доступу до внутрішніх пристроїв з Інтернету. Проте NAT не замінює міжмережевий екран: він не виконує фільтрації за політиками безпеки, не аналізує вмісту пакетів і не захищає від вихідних загроз (наприклад, шкідливого ПЗ, що ініціює вихідні з’єднання). Крім того, CGN ускладнює розслідування інцидентів кібербезпеки, оскільки кілька абонентів провайдера ділять одну публічну IP-адресу, і встановити джерело атаки стає важче.

Таблиця 3.2 — Порівняння підходів: NAT (IPv4) vs нативний IPv6

Аспект	NAT (IPv4)	Нативний IPv6
Адресний простір	Обмежений, розширюється NAT	Практично необмежений
End-to-end зв’язність	Порушена	Повна
Продуктивність	Додаткова обробка	Без overhead на трансляцію
P2P-додатки	Ускладнені (NAT traversal)	Повна підтримка
Ідентифікація джерела	Ускладнена (CGN)	Однозначна (глобальна адреса)
Безпека	Приховує структуру (не firewall)	Firewall + IPsec end-to-end

3.4. УПРАВЛІННЯ ТРАФІКОМ

Управління трафіком (Traffic Engineering, TE) у глобальних мережах — це сукупність методів і механізмів для оптимізації використання мережевих ресурсів, забезпечення необхідної продуктивності застосунків та запобігання перевантаженням. Стандартна IP-маршрутизація обирає шлях за метрикою найкоротшого шляху, не враховуючи завантаження каналів та вимог окремих потоків трафіку. Це може призводити до ситуацій, коли одні канали перевантажені, тоді як інші недовантажені. Управління трафіком вирішує проблему свідомим розподілом потоків між доступними шляхами.

3.4.1. MPLS Traffic Engineering

MPLS Traffic Engineering (MPLS-TE) — один із найпотужніших і найпоширеніших механізмів управління трафіком у мережах операторського класу. MPLS забезпечує

комутацію пакетів на основі міток, що дозволяє визначати явні шляхи для потоків трафіку незалежно від метрики IGP (OSPF, IS-IS). MPLS-TE використовує протокол RSVP-TE (RFC 3209) для встановлення LSP (Label Switched Path) із заданими параметрами пропускної здатності та обмеженнями маршруту.

Процес встановлення LSP у MPLS-TE складається з кількох етапів. Спочатку головний маршрутизатор (head-end router) обчислює шлях для LSP алгоритмом CSPF (Constrained Shortest Path First), який враховує не лише метрику IGP, а й задані оператором обмеження: необхідну пропускну здатність, афінітні атрибути каналів, максимальну кількість транзитних вузлів тощо. Для цього CSPF використовує інформацію про доступну пропускну здатність каналів, що поширюється розширеннями OSPF-TE (RFC 3630) або IS-IS-TE (RFC 5305). Після обчислення шляху RSVP-TE встановлює LSP, резервуючи необхідну пропускну здатність на кожному транзитному вузлі: повідомлення RSVP PATH проходить від головного до кінцевого маршрутизатора, а RESV — у зворотному напрямку, виділяючи мітки та підтверджуючи резервування.

Серед важливих функцій MPLS-TE — автоматичне перенаправлення трафіку при змінах у мережі. Auto-Bandwidth динамічно змінює зарезервовану пропускну здатність LSP відповідно до фактичного навантаження. Fast Reroute (FRR) забезпечує перемикання трафіку на резервний шлях за час до 50 мс при відмові каналу або вузла шляхом попереднього встановлення резервних тунелів (backup tunnels) для кожного захищеного каналу (facility backup) або для кожного LSP окремо (one-to-one backup).

3.4.2. Segment Routing

Segment Routing (SR) — сучасна технологія управління трафіком, що спрощує архітектуру MPLS-TE завдяки усуненню необхідності у протоколі RSVP-TE та зберіганні стану LSP на кожному транзитному маршрутизаторі. У SR маршрут пакета кодується у вигляді впорядкованого списку сегментів (segments), вбудованого безпосередньо в заголовок пакета. Кожен сегмент може представляти вузол мережі (node segment), канал (adjacency segment) або сервіс. Маршрутизатори послідовно обробляють сегменти, спрямовуючи пакет відповідно до кожного з них.

SR має дві реалізації: SR-MPLS, де сегменти кодуються як мітки MPLS у стеку міток, та SRv6, де сегменти кодуються як IPv6-адреси у заголовку розширення SRH (Segment Routing Header). SR-MPLS забезпечує зворотну сумісність із наявною інфраструктурою MPLS, а SRv6 інтегрує Traffic Engineering безпосередньо в IPv6, усуваючи потребу в MPLS. SRv6 — перспективна технологія, що особливо активно впроваджується у мережах великих контент-провайдерів та хмарних операторів.

Переваги Segment Routing над класичним MPLS-TE: відсутність стану LSP на транзитних маршрутизаторах (stateless), що істотно підвищує масштабованість; відсутність протоколу RSVP-TE та супутніх повідомлень підтримки стану; інтеграція з контролерами SDN для програмного управління маршрутизацією; підтримка network programming у SRv6, що дозволяє кодувати не лише маршрут, а й операції обробки пакета (VPN, SFC — Service Function Chaining).

3.4.3. Балансування навантаження та контроль перевантажень

Балансування навантаження (load balancing) — важливий компонент управління трафіком, що забезпечує рівномірний розподіл трафіку між кількома доступними шляхами. У IP-мережах балансування реалізується на кількох рівнях. ECMP (Equal Cost Multi-Path) розподіляє трафік між шляхами з однаковою метрикою IGP, використовуючи хеш-функцію від параметрів пакета (IP-адреси джерела й призначення, номери портів, протокол) — це гарантує, що всі пакети одного потоку

Контроль перевантажень (congestion control) у глобальних мережах реалізується на кількох рівнях. На транспортному рівні TCP застосовує алгоритми керування перевантаженнями (Slow Start, Congestion Avoidance, Fast Retransmit, Fast Recovery), що динамічно регулюють швидкість передачі залежно від стану мережі. Сучасні алгоритми, як-от BBR (Bottleneck Bandwidth and Round-trip propagation time, розроблений Google), використовують вимірювання пропускної здатності та затримки для оптимальної адаптації швидкості — на відміну від класичних Reno та CUBIC, що реагують на втрати пакетів. На мережевому рівні механізм ECN (Explicit Congestion Notification, RFC 3168) дозволяє маршрутизаторам сигналізувати кінцевим вузлам про перевантаження маркуванням пакетів, без їх відкидання, що зменшує непотрібні повторні передачі та покращує загальну продуктивність.

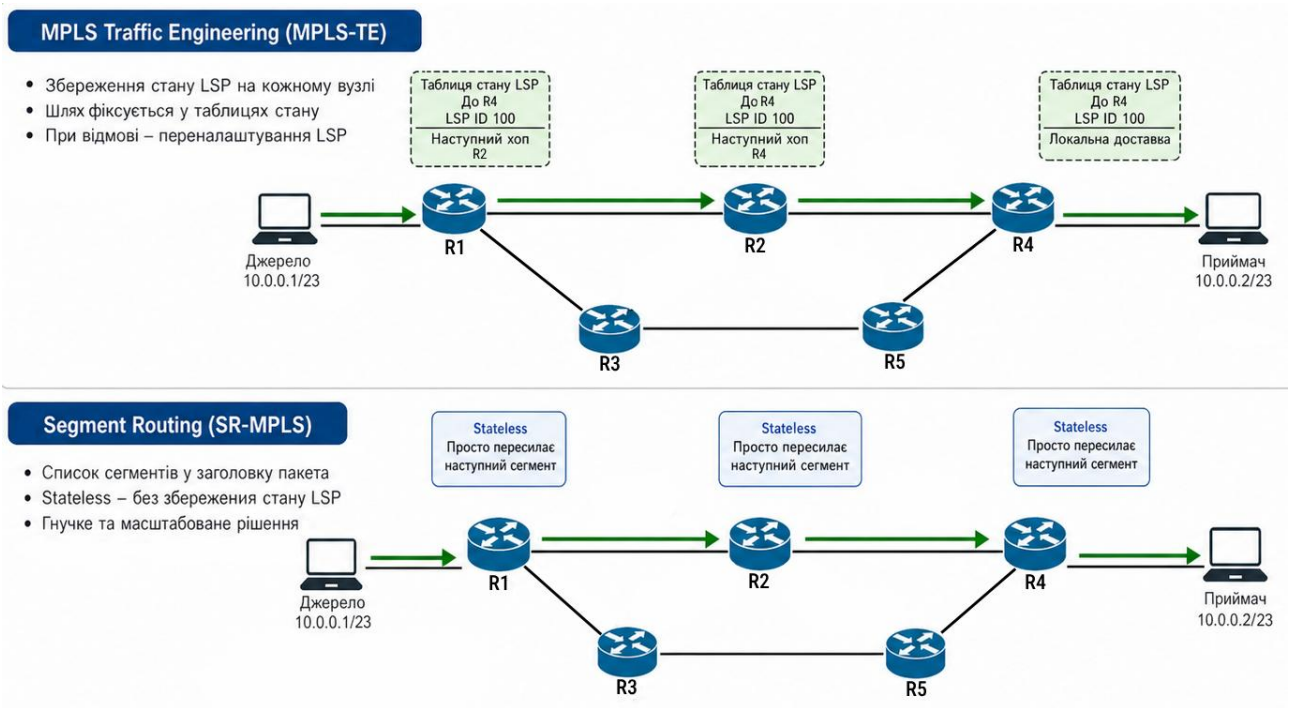

Рисунок 3.6 – MPLS Traffic Engineering та Segment Routing

3.5. QoS-МЕХАНІЗМИ

Якість обслуговування (Quality of Service, QoS) — критично важливий аспект функціонування протоколу IP у глобальних мережах. Як було детально розглянуто в підрозділі 1.5, сучасні мережі передають різнорідний трафік із принципово різними вимогами до параметрів передавання. Тут зосередимося на конкретних механізмах реалізації QoS на рівні IP та їхній інтеграції з технологіями глобальних мереж, що розглядалися в попередніх розділах.

3.5.1. Поле DSCP та класифікація трафіку на рівні IP

Основний інструмент забезпечення QoS на рівні IP — поле Differentiated Services Code Point (DSCP), яке займає 6 старших бітів 8-бітового поля DS у заголовку IPv4 та поле Traffic Class у заголовку IPv6. Два молодші біти поля DS використовуються для ECN (Explicit Congestion Notification). DSCP дозволяє визначити до 64 (2^6) різних класів обслуговування, кожен із яких отримує відповідну обробку (Per-Hop Behavior, PHB) на кожному маршрутизаторі мережі.

Стандарт визначає кілька груп PHB. Default Forwarding (DF, DSCP 000000) — стандартна обробка best-effort для трафіку без явної класифікації. Expedited Forwarding (EF, DSCP 101110 = 46) призначено для трафіку, що вимагає мінімальних

затримки, джитеру та втрат — насамперед голосу (VoIP). EF забезпечує пріоритетне обслуговування з гарантованою мінімальною пропускною здатністю та обмеженою максимальною. Assured Forwarding (AF) визначає чотири класи (AF1–AF4), кожен із трьома рівнями пріоритету відкидання (low, medium, high). Наприклад, AF41 (DSCP 34) має високий клас і низький пріоритет відкидання та зазвичай використовується для відеоконференцій. Class Selector (CS0–CS7) забезпечує зворотну сумісність зі старим полем IP Precedence.

Таблиця 3.3 — Типові значення DSCP для різних типів трафіку

Тип трафіку	DSCP (назва)	Значення	Поведінка
VoIP (голос)	EF	46	Мін. затримка та джитер
Відеоконференція	AF41	34	Гарантована смуга
Сигналізація VoIP	CS3	24	Середній пріоритет
Критичні бізнес-дані	AF31	26	Гарантована смуга
Звичайний трафік	AF21	18	Помірний пріоритет
Best-effort	DF (CS0)	0	Без гарантій
Scavenger (фоновий)	CS1	8	Найнижчий пріоритет

3.5.2. Поле Flow Label у IPv6 та його роль у QoS

Протокол IPv6 запровадив 20-бітове поле Flow Label у базовому заголовку, що дозволяє маршрутизаторам ідентифікувати потік пакетів, які потребують однакової обробки, без аналізу заголовків верхніх рівнів (TCP/UDP). Стандарт RFC 6437 встановлює, що Flow Label задається вузлом-відправником і залишається незмінним протягом усього шляху. Комбінація (Source Address, Destination Address, Flow Label) однозначно ідентифікує потік. Flow Label може використовуватися маршрутизаторами для швидкої класифікації трафіку без глибокого аналізу пакетів (Deep Packet Inspection), що особливо корисно для шифрованого трафіку, де заголовки TCP/UDP недоступні (наприклад, у IPsec ESP).

Окрім QoS, Flow Label ефективно застосовується для балансування навантаження в ECMP та LAG. Без Flow Label балансування шифрованого трафіку IPsec між кількома шляхами неможливе, оскільки всі пакети одного тунелю мають однакові IP-адреси, а заголовки TCP/UDP зашифровані. Flow Label забезпечує ентропію, потрібну для хеш-функції балансування, рівномірно розподіляючи трафік між шляхами.

3.5.3. Механізми обслуговування черг та формування трафіку

У підрозділі 1.5 розглянуто основні механізми керування чергами: FIFO, PQ, WFQ, CBWFQ та LLQ. У контексті IP у глобальних мережах ці механізми діють на кожному маршрутизаторі на шляху пакета, забезпечуючи наскрізну (end-to-end) якість обслуговування. Ефективна реалізація QoS вимагає узгодженої конфігурації на всіх маршрутизаторах мережі — це досягається QoS-політиками, що визначають правила класифікації, маркування, обслуговування черг та формування трафіку для кожного класу.

Формування трафіку (traffic shaping) на рівні IP реалізується алгоритмами Token Bucket і Leaky Bucket. Двошвидкісний триколірний маркувальник (Two-Rate Three-Color Marker, trTCM, RFC 2698) — найпоширеніша реалізація для Carrier Ethernet та MPLS-мереж. Він класифікує пакети як «зелені» (у межах узгодженої швидкості CIR), «жовті» (перевищують CIR, але в межах пікової швидкості PIR) або «червоні» (перевищують

PIR). Зелені пакети передаються без обмежень, жовті — з підвищеним пріоритетом відкидання, червоні — негайно відкидаються. Цей механізм є основою реалізації параметрів QoS, визначених у SLA між оператором і клієнтом.

Механізм WRED (Weighted Random Early Detection) запобігає перевантаженням раннім випадковим відкиданням пакетів із нижчим пріоритетом до настання повного переповнення черги. WRED ураховує DSCP (або IP Precedence) кожного пакета й визначає ймовірність відкидання залежно від рівня заповнення черги: пакети класу AF із високим пріоритетом відкидання (AF13, AF23) відкидаються раніше за пакети з низьким пріоритетом (AF11, AF21). Це дозволяє захищати високопріоритетний трафік під час перевантажень коштом обмеження низькопріоритетного.

3.5.4. Інтеграція QoS з MPLS та SD-WAN

У мережах MPLS QoS реалізується через поле TC (Traffic Class, раніше EXP) у заголовку MPLS, яке містить 3 біти і дозволяє визначити до 8 класів обслуговування. На вхідному маршрутизаторі PE (Provider Edge) значення DSCP з IP-заголовка відображається (mapped) у значення TC в MPLS-заголовку. Транзитні маршрутизатори P (Provider) обробляють трафік на основі TC, не аналізуючи IP-заголовок, що прискорює обробку. На вихідному PE значення TC може бути відображене назад у DSCP. Стандарт визначає два режими відображення DSCP↔TC: Uniform mode (значення DSCP та TC завжди синхронізовані) та Pipe mode (значення DSCP зберігається без змін, TC використовується незалежно в MPLS-мережі).

У рішеннях SD-WAN QoS реалізується на рівні застосунків (Application-Aware QoS). Контролер SD-WAN ідентифікує додатки за допомогою DPI або сигнатурного аналізу та автоматично застосовує відповідні політики QoS без потреби ручного маркування DSCP на кожному пристрої. SD-WAN також забезпечує динамічний вибір шляху (dynamic path selection): якщо якість одного WAN-каналу деградує (зростають затримки чи втрати), трафік чутливих до якості застосунків автоматично переключається на канал з кращими характеристиками. Цей підхід значно гнучкіший за статичну QoS-конфігурацію, але потребує постійного моніторингу стану каналів та значних обчислювальних ресурсів.

Контрольні питання

1. Порівняйте формат заголовка пакета IPv4 та IPv6. Які поля було вилучено в IPv6 та чому?
2. Поясніть механізм фрагментації в IPv4 та причини, чому в IPv6 фрагментація виконується лише вузлом-відправником.
3. Опишіть структуру глобальної індивідуальної адреси IPv6: глобальний префікс, ідентифікатор підмережі, ідентифікатор інтерфейсу.
4. Назвіть три типи адрес IPv6 (unicast, multicast, anycast). Поясніть, чим anycast відрізняється від unicast.
5. Що таке заголовки розширення IPv6? Наведіть приклади та порівняйте з полем Options у IPv4.
6. Порівняйте механізми переходу від IPv4 до IPv6: Dual Stack, тунелювання, NAT64/DNS64. Який підхід є рекомендованим?
7. Поясніть принципи безкласової адресації CIDR. У чому полягає перевага агрегації маршрутів?
8. Що таке VLSM? Наведіть приклад використання масок різної довжини для ефективного розподілу адресного простору.
9. Порівняйте Static NAT, Dynamic NAT та PAT. Який тип NAT забезпечує найбільшу економію адрес?
10. Що таке Carrier Grade NAT (CGN)? Які проблеми він створює для застосунків та для розслідування інцидентів безпеки?
11. Опишіть проблеми наскрізної зв'язності, спричинені NAT. Які протоколи мають проблеми з NAT?
12. Поясніть механізми NAT Traversal: STUN, TURN, ICE. Коли застосовується кожен з них?
13. Що таке MPLS Traffic Engineering? Опишіть процес встановлення LSP за допомогою CSPF та RSVP-TE.
14. Порівняйте Segment Routing (SR-MPLS, SRv6) з класичним MPLS-TE. Які переваги забезпечує SR?
15. Поясніть призначення поля DSCP у заголовку IPv4. Назвіть основні групи PHB: DF, EF, AF, CS.
16. Опишіть рекомендовані значення DSCP для VoIP, відеоконференції та критичних бізнес-даних.
17. Що таке поле Flow Label у IPv6? Як воно використовується для QoS та балансування навантаження?
18. Поясніть принцип роботи trTCM (Two-Rate Three-Color Marker) та його застосування для реалізації SLA.
19. Як працює механізм WRED? У чому його перевага над простим Tail Drop?
20. Опишіть інтеграцію QoS з MPLS (DSCP↔TC, Uniform vs Pipe mode) та SD-WAN (Application-Aware QoS).

РОЗДІЛ 4
ТЕХНОЛОГІЯ MPLS

У четвертому розділі детально розглядається технологія MPLS (Multiprotocol Label Switching) — одна з найважливіших інновацій у галузі телекомунікацій, що фундаментально змінила принципи побудови та функціонування магістральних мереж операторів зв'язку. MPLS поєднує переваги традиційної IP-маршрутизації третього рівня моделі OSI з високопродуктивною комутацією другого рівня, створюючи унікальний механізм пересилки пакетів, який часто характеризують як технологію рівня «2,5».

Розроблена наприкінці 1990-х років як відповідь на зростаючі вимоги до продуктивності та гнучкості мережевої інфраструктури, MPLS стала основою сучасних операторських мереж, забезпечуючи ефективну передачу трафіку, побудову віртуальних приватних мереж (VPN), управління трафіком (Traffic Engineering) та гарантування якості обслуговування (QoS).

Історично поява MPLS була зумовлена кількома технологічними та економічними чинниками. На початку 1990-х років швидке зростання обсягів інтернет-трафіку поставило перед операторами зв'язку серйозні виклики щодо масштабування мережевої інфраструктури. Традиційна IP-маршрутизація, що ґрунтувалася на аналізі заголовків пакетів на кожному проміжному вузлі, вимагала значних обчислювальних ресурсів і не забезпечувала достатньої продуктивності для магістральних каналів зв'язку. Водночас технологія ATM, хоча й забезпечувала високу швидкість комутації завдяки використанню комірок фіксованого розміру, мала значні обмеження у масштабованості та вартості реалізації. Архітектура «IP поверх ATM» призводила до неефективного використання мережевих ресурсів через необхідність підтримки повного зв'язку віртуальних каналів між маршрутизаторами.

Саме в цьому контексті з'явилися перші пропозиції щодо об'єднання механізмів маршрутизації та комутації. Компанія Ipsilon Networks запропонувала технологію IP Switching, Cisco Systems розробила Tag Switching, а IBM представила ARIS (Aggregate Route-based IP Switching). У 1997 році робоча група IETF розпочала стандартизацію єдиної технології під назвою MPLS, результатом чого стала публікація базового стандарту RFC 3031 «Multiprotocol Label Switching Architecture» у 2001 році. Цей стандарт визначив загальну архітектуру MPLS, принципи роботи з мітками, механізми їх розподілу та взаємодію з існуючими протоколами маршрутизації.

Ключова ідея

Технологія MPLS поєднує переваги маршрутизації на основі IP-протоколу та високопродуктивної комутації за мітками. Рішення про маршрутизацію приймається лише один раз — на вхідному маршрутизаторі домену, після чого пакет пересилається виключно за коротким значенням мітки, що відкриває можливості для побудови VPN, Traffic Engineering та забезпечення гарантованої якості обслуговування на єдиній інфраструктурі.

4.1. АРХІТЕКТУРА MPLS

Архітектура MPLS являє собою цілісну систему протоколів, механізмів та структур даних, що забезпечують комутацію пакетів на основі міток замість традиційного аналізу IP-заголовків. Ключова ідея MPLS полягає в тому, що рішення про маршрутизацію пакета приймається лише один раз — на вхідному маршрутизаторі мережі, після чого пакету присвоюється коротка мітка фіксованої довжини. Усі наступні маршрутизатори на шляху пакета виконують лише операції з мітками — заміну (swap), додавання (push) або видалення (pop) — без необхідності аналізу повного IP-заголовка. Це забезпечує значне підвищення продуктивності пересилки та відкриває можливості для реалізації складних сервісів, таких як VPN та Traffic Engineering.

Архітектуру MPLS можна розглядати з двох основних перспектив: площина управління (control plane) та площина даних (data plane). Площина управління відповідає за обмін маршрутною інформацією між маршрутизаторами, розподіл міток та побудову таблиць пересилки. Вона включає протоколи маршрутизації (OSPF, IS-IS, BGP), протоколи розподілу міток (LDP, RSVP-TE, MP-BGP) та відповідні бази даних. Площина даних відповідає за безпосередню пересилку пакетів на основі інформації, отриманої від площини управління. Чітке розділення на дві площини є однією з найважливіших архітектурних переваг MPLS, оскільки дозволяє незалежно оптимізувати процеси управління та пересилки.

4.1.1. Структура MPLS-мітки

Фундаментальним елементом технології MPLS є мітка (label) — 32-бітове поле з чітко визначеною структурою, яке додається до пакета між заголовками другого та третього рівнів моделі OSI. Саме тому MPLS-заголовок часто називають «shim header» — проміжний заголовок. Структура однієї MPLS-мітки включає чотири поля.

Перші 20 біт містять значення мітки (Label Value), яке може набувати значень від 0 до 1 048 575. Однак перші 16 значень (0–15) зарезервовані для спеціальних цілей і не використовуються для звичайної комутації. Зокрема, мітка 0 (IPv4 Explicit NULL) сигналізує маршрутизатору про необхідність видалити мітку та виконати пересилку на основі IPv4-заголовка. Мітка 3 (Implicit NULL) використовується в механізмі Penultimate Hop Popping (PHP), коли передостанній маршрутизатор на шляху видаляє мітку, дозволяючи останньому маршрутизатору виконати лише один пошук у таблиці маршрутизації замість двох. Мітка 1 (Router Alert) використовується для привернення уваги програмної частини маршрутизатора до певного пакета.

Біти 20–22 містять три біти, що історично називаються «експериментальними» (EXP bits), хоча їхнє призначення давно визначено — вони використовуються для підтримки механізмів якості обслуговування. У сучасній термінології RFC 5462 ці біти перейменовано на Traffic Class (TC). Три біти TC дозволяють визначити до восьми класів обслуговування, аналогічно полю IP Precedence у заголовку IPv4. Це забезпечує можливість диференційованого обслуговування трафіку в MPLS-мережі відповідно до моделі DiffServ.

Біт 23 — це біт Bottom of Stack (BoS, S-bit), який вказує, чи є поточна мітка останньою у стеку міток. Якщо значення BoS дорівнює 1, це означає, що під даною міткою знаходиться безпосередньо заголовок транспортованого протоколу (зазвичай IP). Якщо BoS дорівнює 0, під поточною міткою знаходиться ще одна MPLS-мітка. Цей механізм є критично важливим для реалізації стеку міток. Біти 24–31 містять 8-бітове поле Time To Live (TTL), яке функціонально аналогічне полю TTL в IP-заголовку: воно зменшується на одиницю на кожному проміжному маршрутизаторі, а при досягненні значення 0 пакет відкидається, що запобігає нескінченному циклу пакетів у разі виникнення маршрутних петель.

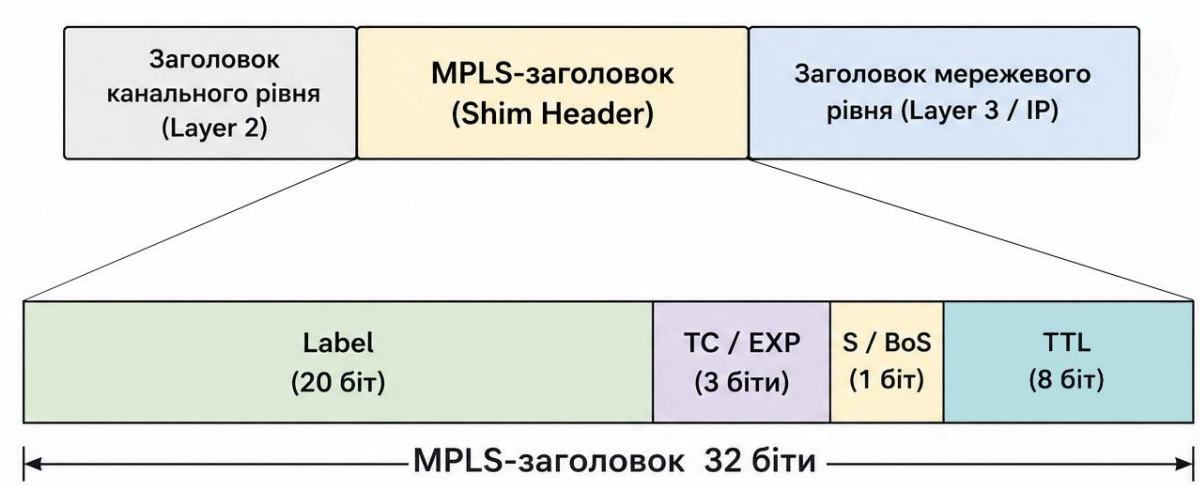

Рисунок 4.1 – Структура 32-бітового MPLS-заголовка (shim header)

4.1.2. Стек міток (Label Stack)

Механізм стеку міток (label stack) є одним із найважливіших архітектурних рішень MPLS. Стек складається з однієї або кількох MPLS-міток, розміщених одна над одною. Верхня мітка використовується для прийняття рішення про пересилку на поточному маршрутизаторі, тоді як нижні мітки можуть нести додаткову інформацію, необхідну для реалізації різних сервісів. Теоретично кількість міток у стеку необмежена, хоча на практиці рідко зустрічаються стеки глибиною більше чотирьох міток.

Найбільш поширеним є використання двох міток: зовнішня (транспортна) мітка забезпечує доставку пакета через MPLS-домен до потрібного вихідного маршрутизатора, а внутрішня (сервісна) мітка ідентифікує конкретний сервіс — наприклад, конкретну VPN-інстанцію або псевдопровід (pseudowire). Такий підхід дозволяє розділити функції транспортування та надання сервісів, забезпечуючи високу масштабованість архітектури.

Розміщення стеку міток у фреймі має важливе значення для розуміння взаємодії MPLS із канальними протоколами. Стек міток знаходиться після заголовка канального рівня (Ethernet, PPP, HDLC), але перед заголовком мережевого рівня. Для ідентифікації наявності MPLS-заголовка у фреймі використовуються спеціальні значення поля протоколу канального рівня: для Ethernet це значення EtherType 0x8847 (unicast) та 0x8848 (multicast), для PPP — значення 0x0281. MPLS не залежить від конкретного канального протоколу — мітки можуть бути додані до пакетів, що передаються через будь-який тип з'єднання.

4.1.3. Типи маршрутизаторів: LSR та LER

В архітектурі MPLS маршрутизатори, що підтримують комутацію за мітками, називаються LSR (Label Switch Router). Залежно від положення в мережі та виконуваних функцій, розрізняють три типи LSR.

Вхідний LSR (Ingress LSR або Ingress Edge LSR) розташований на межі MPLS-домену і виконує функцію класифікації вхідних IP-пакетів, визначення їх належності до відповідного класу еквівалентної пересилки (FEC) та додавання стеку MPLS-міток. Цей процес називається імпозицією міток (label imposition) або операцією push. Вхідний LSR є критично важливим елементом архітектури, оскільки саме він приймає рішення про маршрутизацію на основі повного аналізу IP-заголовка та присвоює пакету мітку, яка визначатиме його подальший шлях через MPLS-мережу.

Проміжний LSR (Transit LSR) розташований всередині MPLS-домену та виконує операцію заміни міток (label swap): при отриманні пакета з вхідною міткою він замінює її на відповідну вихідну мітку та передає пакет на наступний інтерфейс. Цей процес є набагато швидшим за повну IP-маршрутизацію, оскільки пошук у таблиці міток (LFIB — Label Forwarding Information Base) є операцією з фіксованим часом виконання. Проміжні LSR не аналізують IP-заголовок пакета, що забезпечує високу продуктивність пересилки.

Вихідний LSR (Egress LSR) розташований на протилежній межі MPLS-домену і виконує функцію видалення MPLS-міток (label disposition або операцію pop) та пересилки пакета на основі інформації з IP-заголовка. Вхідні та вихідні LSR разом називаються граничними LSR (Edge LSR) або LER (Label Edge Router). У контексті MPLS VPN граничні маршрутизатори називаються PE (Provider Edge), а проміжні — P (Provider). Ця термінологія стала настільки поширеною, що використовується навіть у мережах, де MPLS VPN не реалізовано.

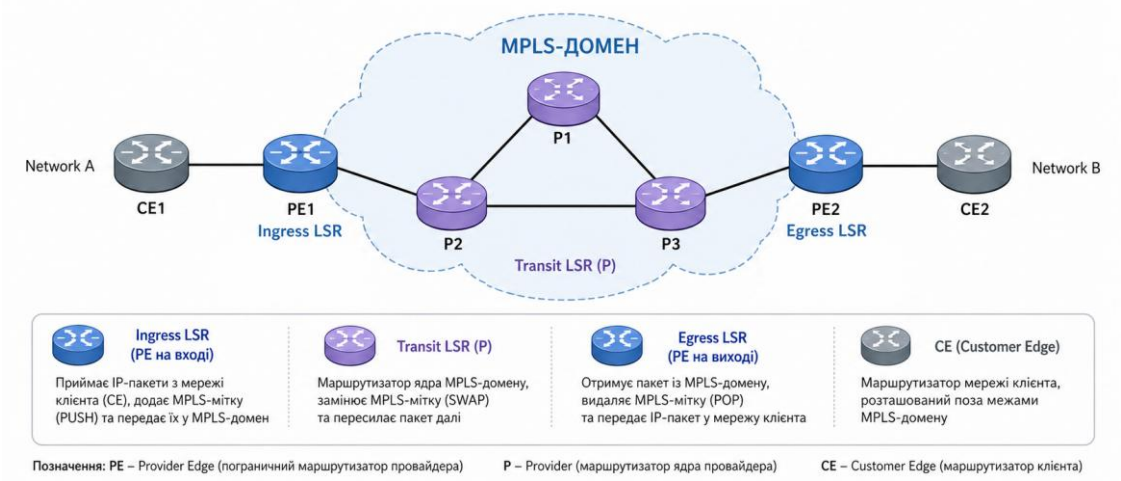

Рисунок 4.2 – Типи маршрутизаторів в MPLS-мережі: Ingress LSR, Transit LSR, Egress LSR

4.1.4. Клас еквівалентної пересилки (FEC) та шлях LSP

Клас еквівалентної пересилки (Forwarding Equivalence Class, FEC) є фундаментальною концепцією MPLS, яка визначає групу пакетів, що пересилаються однаковим шляхом через мережу та отримують однакове обслуговування. FEC може відповідати IP-префіксу в таблиці маршрутизації (наприклад, мережі 10.1.0.0/16), але може також визначатися на основі інших критеріїв: значення поля DSCP, порту призначення TCP/UDP, вхідного інтерфейсу або комбінації цих параметрів.

Принципово важливим є те, що в MPLS класифікація пакета та його призначення до конкретного FEC відбувається лише один раз — на вхідному LSR, після чого усі проміжні маршрутизатори пересилають пакет виключно на основі мітки, не повторюючи аналіз заголовка. Це відрізняє MPLS від традиційної IP-маршрутизації, де кожен маршрутизатор на шляху самостійно виконує пошук в таблиці маршрутів для визначення наступного кроку.

Концепція FEC дозволяє реалізувати гнучку політику маршрутизації. Наприклад, весь трафік до певної мережі може бути об’єднаний в один FEC і направлений по одному LSP, тоді як трафік з високим пріоритетом до тієї ж мережі може бути виділений в окремий FEC і направлений по альтернативному LSP з кращими характеристиками якості обслуговування. Така гнучкість є ключовою перевагою MPLS перед традиційною IP-маршрутизацією, де шлях пакета визначається виключно адресою призначення.

Шлях комутації за мітками (Label Switched Path, LSP) — це послідовність LSR, через які проходить мічений пакет від вхідного до вихідного маршрутизатора MPLS-

домену. LSP є однонаправленим: для двостороннього обміну даними між двома точками необхідно два окремих LSP — по одному в кожному напрямку. Кожен LSP

> **Важливо**
> *LDP створює LSP автоматично уздовж найкоротших шляхів IGP, тоді як RSVP-TE дозволяє явно задати шлях LSP через мережу, ігноруючи рішення IGP. Саме RSVP-TE є основою технології Traffic Engineering.*

4.1.5. Площина управління та площина даних

У площині управління MPLS використовуються дві ключові бази даних: LIB (Label Information Base) та LFIB (Label Forwarding Information Base). LIB містить усі прив'язки міток, отримані від усіх сусідніх LSR, включаючи ті, що наразі не використовуються для пересилки. LFIB, навпаки, містить лише ті прив'язки, що активно використовуються для пересилки пакетів, і є аналогом таблиці FIB у традиційній IP-маршрутизації.

Процес побудови LFIB включає кілька кроків: **спочатку протокол маршрутизації** (наприклад, OSPF) визначає найкращий шлях до кожного IP-префіксу та заповнює таблицю маршрутизації RIB; потім механізм CEF створює FIB на основі RIB; паралельно LDP обмінюється мітками з сусідніми LSR та заповнює LIB; нарешті, MPLS-процес об'єднує інформацію з FIB та LIB для створення LFIB, яка використовується для високошвидкісної пересилки мічених пакетів.

Площина даних MPLS оперує виключно з LFIB та виконує три базові операції з мітками: push, swap та pop. Ці операції виконуються на апаратному рівні в сучасних маршрутизаторах, що забезпечує пересилку пакетів зі швидкістю, близькою до швидкості каналу зв'язку (wire speed). Механізм Penultimate Hop Popping (PHP) — видалення верхньої мітки на передостанньому маршрутизаторі перед вихідним LSR — є важливою оптимізацією, що дозволяє вихідному LSR виконати лише один пошук замість двох.

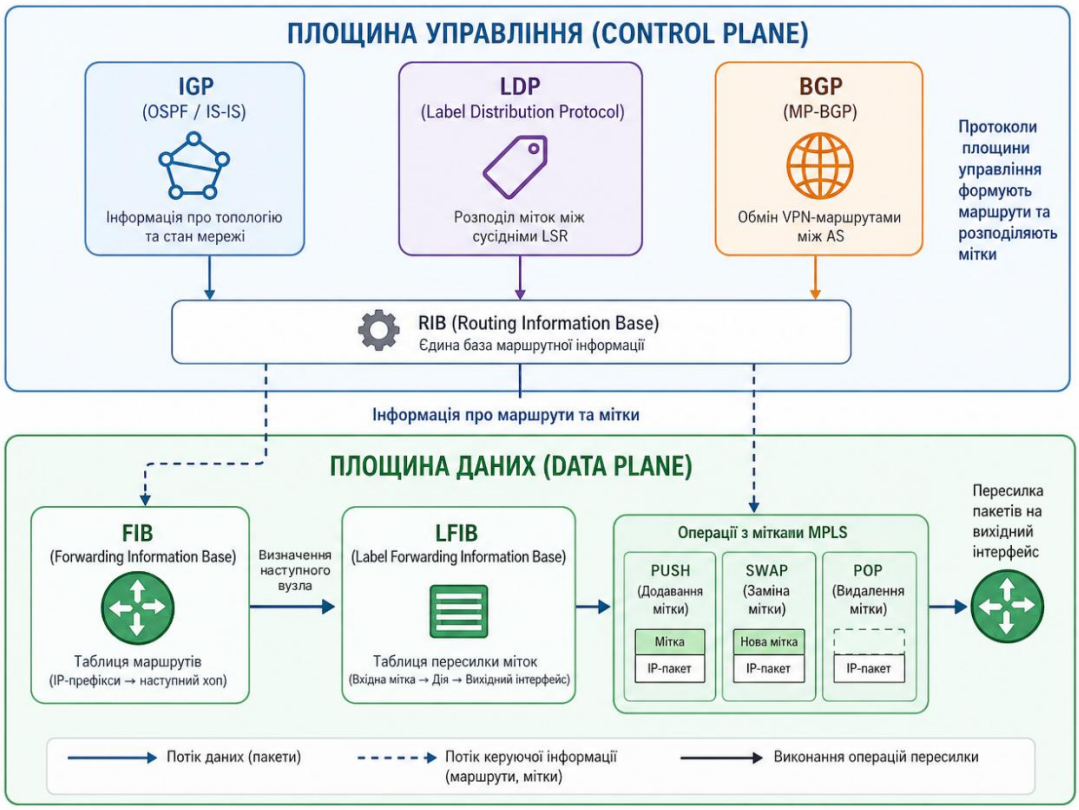

Рисунок 4.3 – Взаємодія площини управління та площини даних в MPLS

4.1.6. Порівняння MPLS з традиційною IP-маршрутизацією

Порівняння MPLS з традиційною IP-маршрутизацією дозволяє краще зрозуміти переваги та обмеження кожного підходу. У традиційній IP-маршрутизації кожен маршрутизатор на шляху пакета виконує повний аналіз заголовка: він визначає IP-адресу призначення, виконує пошук в таблиці маршрутизації за алгоритмом найдовшого збігу префікса (Longest Prefix Match, LPM) та визначає наступний крок. Цей процес повторюється на кожному вузлі незалежно, що, з одного боку, забезпечує високу стійкість мережі, але, з іншого боку, обмежує гнучкість маршрутизації.

MPLS змінює цю парадигму: рішення про маршрутизацію приймається один раз на вхідному LSR, після чого пакет пересилається за мітками. Це забезпечує кілька ключових переваг. По-перше, пошук у LFIB за точним значенням мітки є операцією з фіксованою складністю O(1), тоді як LPM у великих таблицях маршрутизації має складність O(log n) або навіть O(n) залежно від реалізації. По-друге, MPLS дозволяє реалізувати маршрутизацію на основі критеріїв, відмінних від адреси призначення, — це основа Traffic Engineering. По-третє, механізм стеку міток забезпечує ієрархічну інкапсуляцію, що є фундаментом для побудови VPN та інших сервісних моделей. По-четверте, MPLS є незалежною від протоколу мережевого рівня — одна й та сама MPLS-інфраструктура може транспортувати IPv4, IPv6, Ethernet-фрейми та інші протоколи.

Таблиця 4.1 — Порівняння MPLS та традиційної IP-маршрутизації

Критерій	Традиційна IP-маршрутизація	MPLS
Механізм пересилки	LPM за IP-адресою	Точний пошук за міткою
Рівень моделі OSI	Рівень 3	Рівень 2,5
Основа рішення	IP-адреса призначення	Мітка з вхідного LSR
Підтримка VPN	GRE, IPsec, VRF-Lite	Нативна (L2/L3VPN)
Traffic Engineering	Обмежена (метрики, PBR)	Повна (CSPF, RSVP-TE)
Швидкість відновлення	IGP convergence (с)	FRR: < 50 мс
Мультипротокольність	IPv4/IPv6	IPv4, IPv6, Ethernet, ATM

4.2. ПРОТОКОЛИ РОЗПОДІЛУ МІТОК: LDP, RSVP-TE

Протоколи розподілу міток є ключовим компонентом площини управління MPLS, оскільки саме вони забезпечують обмін інформацією про прив’язки міток між сусідніми LSR та формування таблиць пересилки LFIB. В архітектурі MPLS визначено кілька протоколів розподілу міток, кожен з яких призначений для конкретного застосування: LDP забезпечує розподіл міток для IGP-маршрутів, RSVP-TE використовується для побудови LSP з явно заданими шляхами та резервуванням ресурсів, а MP-BGP розподіляє мітки для BGP-маршрутів, що є критично важливим для реалізації MPLS VPN.

4.2.1. Label Distribution Protocol (LDP)

LDP (Label Distribution Protocol), стандартизований в RFC 5036, забезпечує розподіл міток для IP-префіксів, відомих протоколам внутрішньої маршрутизації. Основна ідея LDP полягає в тому, що замість модифікації існуючих протоколів маршрутизації для перенесення інформації про мітки, було створено окремий незалежний протокол, здатний працювати з будь-яким IGP. LDP виконує чотири основні функції: виявлення сусідніх LSR (discovery), встановлення та підтримка сесій

(session establishment and maintenance), розподіл прив'язок міток (label advertisement) та сповіщення про помилки та події (notification).

Процес виявлення сусідів у LDP ґрунтується на надсиланні повідомлень Hello на всіх інтерфейсах, де активовано MPLS. Ці повідомлення передаються як UDP-дейтаграми на мультикастну адресу 224.0.0.2 з використанням порту 646. Кожне повідомлення Hello містить ідентифікатор LDP (LDP ID), який зазвичай відповідає адресі Loopback-інтерфейсу маршрутизатора, та значення Hold Time. За замовчуванням повідомлення Hello надсилаються кожні 5 секунд, а значення Hold Time становить 15 секунд. Після виявлення сусіда два LSR встановлюють TCP-з'єднання (порт 646) для обміну повідомленнями LDP. Використання TCP гарантує надійну доставку повідомлень про прив'язки міток.

Після встановлення TCP-з'єднання LSR обмінюються повідомленнями ініціалізації, в яких узгоджують параметри сесії: версію протоколу, таймер keepalive, режим розподілу міток та інші параметри. Для підтримки сесії маршрутизатори періодично обмінюються повідомленнями Keepalive — за замовчуванням кожні 60 секунд. Якщо повідомлення Keepalive не отримано протягом періоду Hold Time (за замовчуванням 180 секунд), сесія LDP розривається.

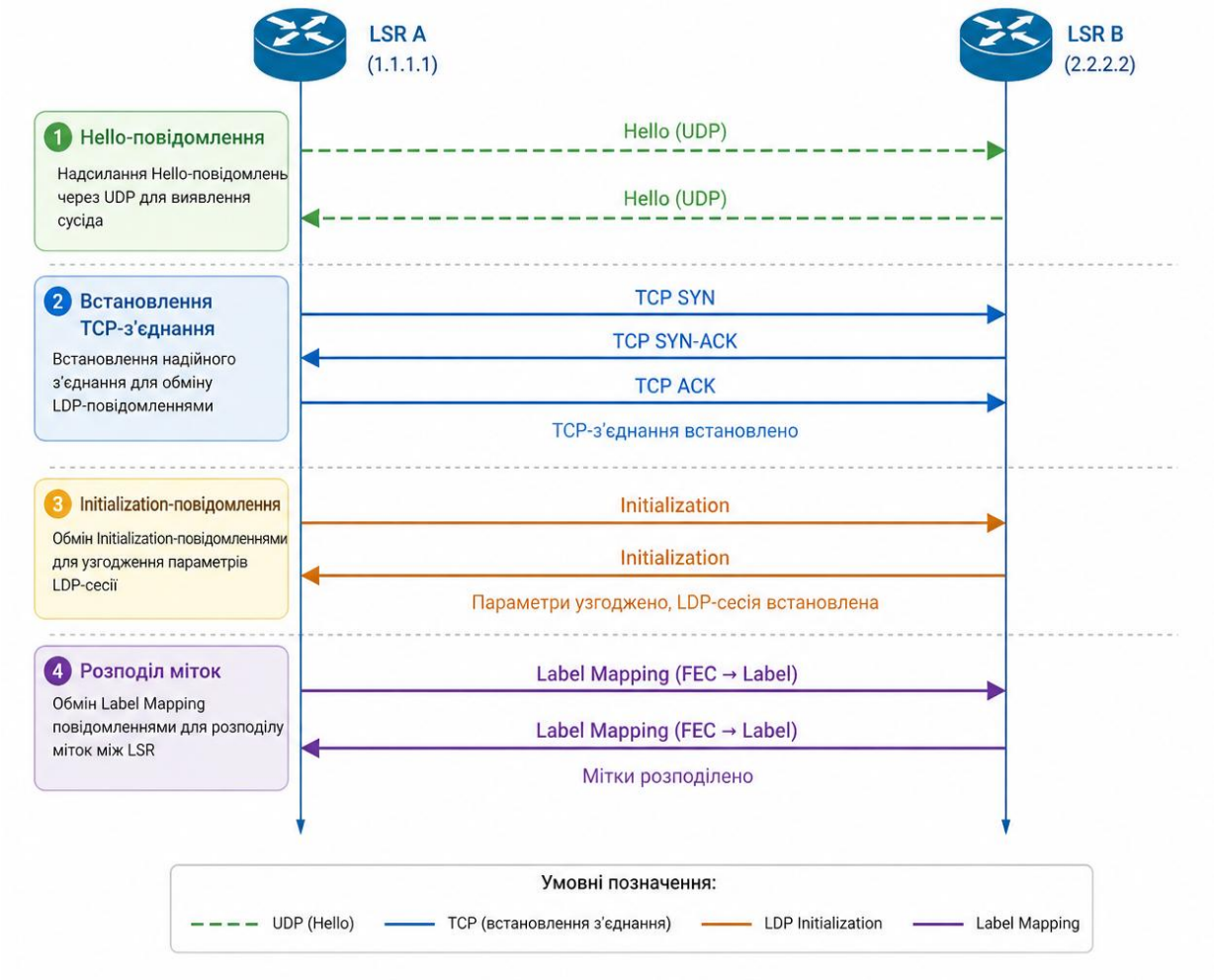

Рисунок 4.4 – Процес встановлення LDP-сесії та розподілу міток

Ключовим аспектом функціонування LDP є режими розподілу та збереження міток. В режимі Downstream Unsolicited (DU, за замовчуванням у Cisco IOS) кожен LSR автоматично розподіляє мітки для всіх відомих йому IGP-префіксів усім своїм LDP-сусідам, не чекаючи запиту. Альтернативний режим Downstream on Demand (DoD) передбачає, що мітки розподіляються лише за запитом від сусіднього LSR.

Щодо збереження міток, існують два режими: Liberal Label Retention Mode (за замовчуванням) — LSR зберігає всі отримані прив'язки міток від усіх сусідів, навіть якщо сусід не є наступним кроком для даного префікса; та Conservative Label Retention Mode — LSR зберігає лише ті прив'язки, що отримані від сусіда, який є наступним кроком. Liberal-режим забезпечує швидше відновлення після змін топології, тоді як Conservative-режим є більш ефективним з точки зору використання пам'яті.

Режим контролю LSP визначає, коли LSR розпочинає розподіл міток. В режимі Independent Control кожен LSR самостійно розпочинає розподіл міток, як тільки розпізнає FEC у своїй таблиці маршрутизації. В режимі Ordered Control LSR розподіляє мітку для FEC лише після того, як отримав прив'язку мітки від наступного кроку або сам є вихідним LSR для цього FEC.

4.2.2. RSVP-TE (Resource Reservation Protocol — Traffic Engineering)

RSVP-TE є розширенням протоколу RSVP (RFC 2205), спеціально адаптованим для потреб MPLS Traffic Engineering (RFC 3209). На відміну від LDP, який будує LSP автоматично уздовж найкоротших шляхів IGP, RSVP-TE дозволяє явно задавати шлях LSP через мережу та резервувати ресурси (зокрема, смугу пропускання) вздовж цього шляху. Це робить RSVP-TE незамінним інструментом для реалізації Traffic Engineering, де необхідно контролювати розподіл трафіку по мережі незалежно від рішень IGP.

Протокол RSVP-TE є протоколом «м'якого стану» (soft-state protocol), що означає необхідність періодичного оновлення резервацій ресурсів — без оновлення за визначений період сесія автоматично завершується. Цьому протистоять протоколи «жорсткого стану» (hard-state), у яких стан зберігається до явної команди на видалення (як, наприклад, у класичному LDP) у мережі. На відміну від протоколів «жорсткого стану», де резервація існує до явного видалення, в RSVP-TE резервація автоматично припиняється, якщо не отримано оновлення протягом визначеного часу. За замовчуванням повідомлення оновлення надсилаються кожні 30 секунд, а тайм-аут резервації настає після відсутності чотирьох послідовних оновлень (приблизно 120 секунд). Цей механізм забезпечує автоматичне вивільнення ресурсів у разі відмови вузла або каналу зв'язку.

Встановлення TE-тунелю за допомогою RSVP-TE відбувається в кілька етапів. Спочатку головний маршрутизатор тунелю (headend) виконує обчислення шляху за допомогою алгоритму CSPF (Constrained Shortest Path First), який є модифікацією алгоритму SPF з урахуванням обмежень — зокрема, доступної смуги пропускання та атрибутів каналів зв'язку. Результатом CSPF є явний маршрут (Explicit Route Object, ERO), що містить послідовність вузлів, через які повинен пройти тунель.

Після обчислення шляху headend надсилає повідомлення Path уздовж визначеного маршруту. Кожен проміжний маршрутизатор, отримавши повідомлення Path, перевіряє доступність запитуваних ресурсів (процедура Admission Control) і, у разі успіху, пересилає повідомлення Path далі. Коли повідомлення Path досягає кінцевого маршрутизатора тунелю (tail-end), той надсилає відповідне повідомлення Resv у зворотному напрямку. Повідомлення Resv містить мітку, яку кожен маршрутизатор повинен використовувати для пересилки пакетів цього тунелю, та підтвердження резервації ресурсів. Після отримання повідомлення Resv на headend тунель вважається встановленим.

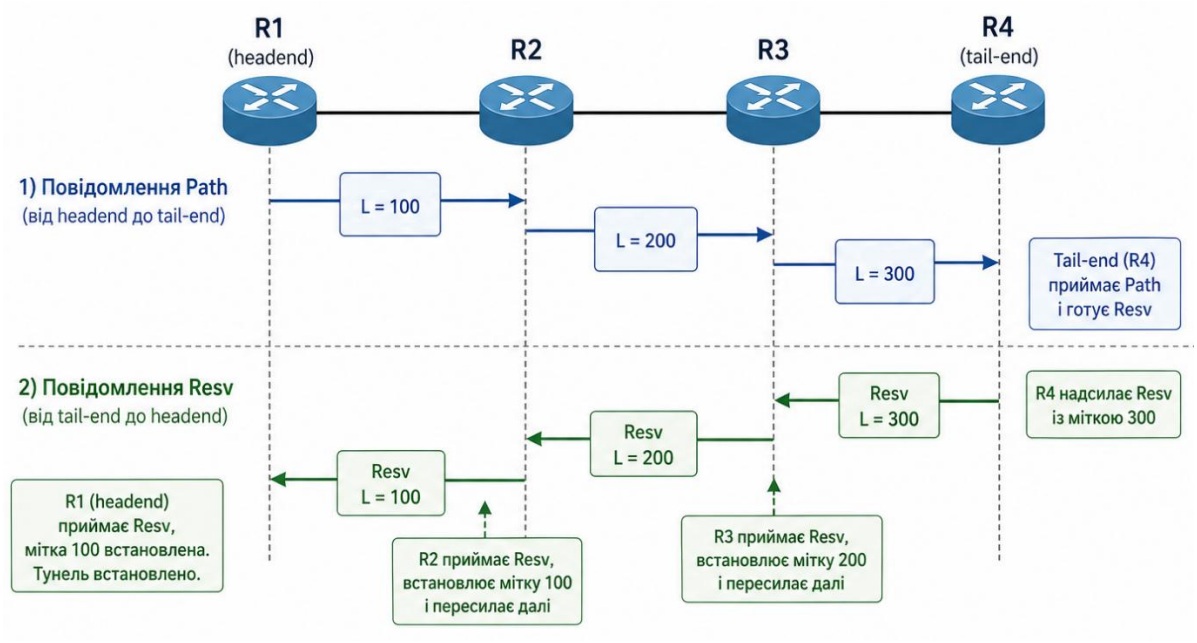

Рисунок 4.5 – Встановлення RSVP-TE тунелю: обмін повідомленнями

Важливою функцією RSVP-TE є підтримка механізму make-before-break (MBB), який дозволяє безперервно переключати трафік при зміні шляху тунелю. Коли виникає потреба в зміні шляху TE-тунелю, headend спочатку встановлює новий LSP за новим шляхом, а лише після його успішного встановлення переключає трафік зі старого LSP на новий та видаляє старий LSP. Цей механізм забезпечує мінімальні втрати пакетів при зміні шляху.

Протокол RSVP-TE також підтримує механізм Fast Reroute (FRR), стандартизований в RFC 4090, що забезпечує швидке перемикання трафіку (менше 50 мс) у разі відмови каналу або вузла. FRR працює шляхом попереднього обчислення та встановлення обхідних LSP на кожному маршрутизаторі вздовж основного TE-тунелю. При виявленні відмови маршрутизатор, що безпосередньо прилягає до місця відмови (Point of Local Repair, PLR), негайно переключає трафік на обхідний LSP, не чекаючи перерахунку основного шляху headend-маршрутизатором. Існують два режими FRR: Facility Backup, де один обхідний LSP може захищати кілька основних тунелів, та One-to-One Backup, де для кожного основного тунелю створюється окремий обхідний LSP.

Порівняння LDP та RSVP-TE дозволяє зрозуміти сфери їхнього оптимального застосування. LDP є простішим у конфігурації та обслуговуванні, автоматично будує LSP для всіх IGP-маршрутів і не вимагає явного визначення шляхів. Він ідеально підходить для базової MPLS-комутації та побудови транспортної основи для MPLS VPN. RSVP-TE, навпаки, є більш складним у конфігурації, але забезпечує повний контроль над шляхом LSP та резервування смуги пропускання. На практиці багато операторів зв’язку використовують обидва протоколи одночасно: LDP — для базової зв’язності та транспорту VPN, а RSVP-TE — для управління трафіком на критично важливих ділянках мережі.

4.3. ПЕРЕСИЛКА ПАКЕТІВ У MPLS (MPLS FORWARDING)

Механізми пересилки пакетів є серцевиною технології MPLS, оскільки саме вони визначають, як пакети переміщуються через мережу на основі інформації з міток. Площина даних MPLS реалізує три фундаментальні операції з мітками — push, swap та pop — які, в поєднанні з таблицями пересилки LFIB та FIB, забезпечують високопродуктивну комутацію трафіку.

4.3.1. Операції з мітками: push, swap, pop

Операція push (імпозиція міток) виконується на вхідному LSR, коли немічений IP-пакет надходить з-за меж MPLS-домену. Вхідний LSR аналізує IP-заголовок пакета, визначає FEC, до якого належить пакет, та додає до пакета стек із однієї або кількох MPLS-міток. У найпростішому випадку додається одна мітка, що відповідає шляху до IP-префікса призначення через MPLS-мережу. У складніших сценаріях, наприклад при MPLS VPN, вхідний PE-маршрутизатор додає стек із двох міток: внутрішня мітка ідентифікує VPN-інстанцію на вихідному PE-маршрутизаторі, а зовнішня мітка забезпечує транспортування пакета через P-мережу до вихідного PE.

Операція swap (заміна мітки) є основною операцією на проміжних LSR. При отриманні міченого пакета проміжний LSR виконує пошук у таблиці LFIB за значенням вхідної мітки, знаходить відповідний запис, замінює вхідну мітку на вихідну та передає пакет на зазначений вихідний інтерфейс. Важливо підкреслити, що при операції swap проміжний LSR не аналізує жоден заголовок під стеком міток — ні IP-заголовок, ні інші мітки в стеку. Це забезпечує постійний час обробки незалежно від глибини стеку міток або складності IP-заголовка.

Операція pop (диспозиція міток) виконується на вихідному LSR або, у разі використання механізму PHP, на передостанньому LSR. При операції pop верхня мітка видаляється зі стеку. Якщо під видаленою міткою знаходиться ще одна мітка (BoS = 0), маршрутизатор може виконати наступну операцію на основі нової верхньої мітки. Якщо ж видалена мітка була останньою в стеку (BoS = 1), під нею знаходиться заголовок транспортованого протоколу, і маршрутизатор виконує звичайну IP-маршрутизацію.

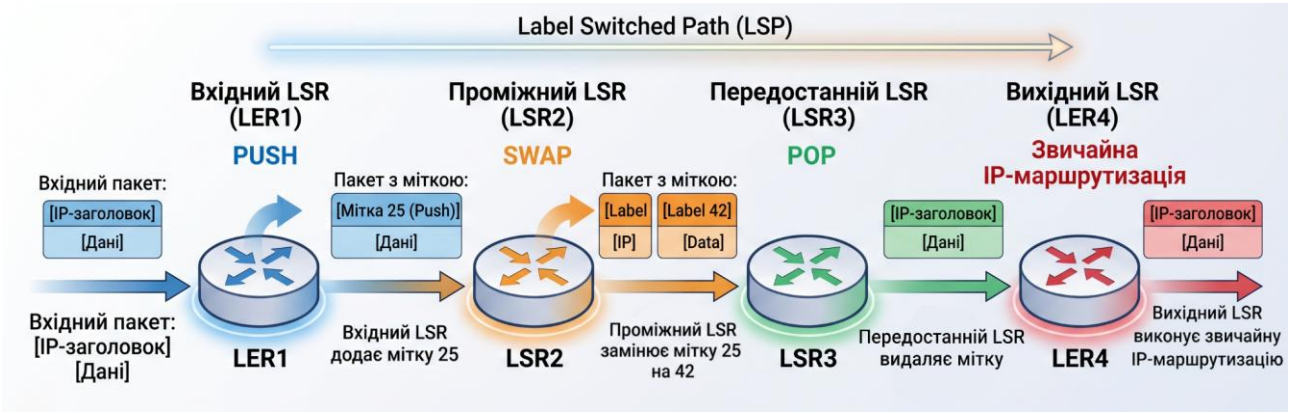

Рисунок 4.6 – Операції з мітками: push, swap, pop уздовж LSP

4.3.2. Penultimate Hop Popping (PHP)

Механізм Penultimate Hop Popping заслуговує окремої уваги, оскільки є ключовою оптимізацією продуктивності MPLS. Без PHP вихідний LSR повинен виконати дві операції: спочатку знайти запис у LFIB за вхідною міткою, а потім виконати пошук у FIB за IP-адресою призначення для визначення наступного кроку за межами MPLS-домену. PHP дозволяє уникнути першої операції: передостанній LSR видаляє верхню мітку, і вихідний LSR отримує вже немічений IP-пакет, для якого потрібен лише один пошук у FIB.

Для реалізації PHP вихідний LSR розподіляє через LDP мітку зі спеціальним значенням 3 (Implicit NULL) для префіксів, де він є вихідним маршрутизатором. Коли передостанній LSR бачить Implicit NULL як вихідну мітку, він виконує операцію pop замість swap. Існує також Explicit NULL (мітка 0 для IPv4 та мітка 2 для IPv6), яка

використовується замість Implicit NULL у випадках, коли необхідно зберегти інформацію QoS (поле TC) з MPLS-заголовка при переході до IP-домену.

4.3.3. Поведінка TTL у MPLS

Поведінка поля TTL у MPLS-пакетах регулюється RFC 3443 та має важливе значення для діагностики мережі та запобігання маршрутним петлям. При імпозиції мітки на вхідному LSR значення TTL з IP-заголовка копіюється в поле TTL MPLS-заголовка. При кожній операції swap на проміжних LSR значення TTL у MPLS-заголовку зменшується на одиницю. При диспозиції мітки на вихідному LSR значення TTL з MPLS-заголовка копіюється назад у TTL IP-заголовка. Такий механізм забезпечує коректну роботу утиліти traceroute через MPLS-домен: кожен проміжний LSR, де TTL досягає нуля, генерує повідомлення ICMP Time Exceeded.

У деяких сценаріях оператори можуть приховати внутрішню структуру MPLS-мережі від зовнішніх користувачів. Для цього використовується режим «no TTL propagation». У цьому режимі при імпозиції мітки поле TTL MPLS-заголовка встановлюється у максимальне значення 255, а при диспозиції мітки TTL IP-заголовка зменшується лише на одиницю незалежно від кількості проміжних LSR. Це ефективно приховує MPLS-вузли від traceroute.

4.3.4. Балансування навантаження та проблема MTU

Балансування навантаження в MPLS-мережах є важливим аспектом ефективного використання мережевих ресурсів. У MPLS-мережах балансування ускладнюється тим, що проміжні LSR не мають доступу до IP-заголовка — вони бачать лише стек міток. Для вирішення цієї проблеми використовуються два підходи. Перший — вхідний LSR виконує балансування при імпозиції, розподіляючи пакети різних потоків по різних LSP за допомогою хешування IP-заголовків. Другий — спеціальна мітка Entropy Label (RFC 6790), яка додається до стеку міток і містить хеш-значення, обчислене на основі полів IP-заголовка. Проміжні LSR можуть використовувати цю мітку для прийняття рішень про балансування без необхідності аналізу IP-заголовка.

Проблема MTU в MPLS-мережах виникає через те, що додавання стеку міток збільшує розмір фрейму. Кожна мітка в стеку додає 4 байти до загального розміру пакета. Для пакета з двома мітками це збільшення становить 8 байт. Якщо MTU каналу зв’язку становить стандартні 1500 байт для Ethernet, максимальний розмір IP-пакета, який може бути переданий через MPLS-мережу з двома мітками, зменшується до 1492 байт. Для запобігання фрагментації рекомендується збільшити MTU на всіх інтерфейсах MPLS-мережі. Типовою практикою є встановлення MTU 9000 байт (jumbo frames) або, як мінімум, 1518 байт (baby giant frames) на інтерфейсах MPLS-домену.

4.4. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ MPLS VPN (L2/L3)

Технологія MPLS VPN є одним із найважливіших та найбільш комерційно успішних застосувань MPLS. Вона дозволяє операторам зв’язку надавати послуги ізольованих віртуальних мереж множині клієнтів на базі єдиної фізичної інфраструктури. MPLS VPN забезпечує повну ізоляцію трафіку та адресних просторів різних клієнтів без використання шифрування або складних конфігурацій фільтрації, що значно спрощує управління мережею та зменшує операційні витрати.

4.4.1. L3VPN: архітектура та принципи роботи

L3VPN на основі MPLS, стандартизована в RFC 4364, є домінуючою моделлю надання VPN-послуг у сучасних операторських мережах. Архітектура L3VPN базується на моделі «рівний-до-рівного» (peer-to-peer model), де PE-маршрутизатори оператора беруть участь у маршрутизації клієнтського трафіку. Ця модель принципово відрізняється від традиційної «накладеної» моделі, де оператор надає лише канали зв'язку, а маршрутизація повністю залишається відповідальністю клієнта.

Ключовим архітектурним елементом L3VPN є VRF (Virtual Routing and Forwarding instance) — віртуальна таблиця маршрутизації та пересилки, що створюється на PE-маршрутизаторі для кожного клієнта. Кожна VRF є повністю ізольованою від інших VRF та від глобальної таблиці маршрутизації PE-маршрутизатора: маршрути, що належать одній VRF, невидимі для інших VRF, навіть якщо вони використовують однакові IP-адреси. Це дозволяє різним клієнтам використовувати адресні простори, що перетинаються, без конфліктів. PE-маршрутизатор може підтримувати сотні або навіть тисячі VRF одночасно.

Для розрізнення маршрутів різних VPN при їх передачі через MP-BGP між PE-маршрутизаторами використовується концепція Route Distinguisher (RD) — 8-байтовий ідентифікатор, що додається до 4-байтового IPv4-префікса, утворюючи 12-байтовий VPNv4-префікс. RD гарантує унікальність маршрутів у площині управління BGP навіть при використанні однакових IP-адрес різними клієнтами. Слід зазначити, що RD не визначає, до якої VPN належить маршрут — він лише забезпечує унікальність.

Для контролю імпорту та експорту маршрутів між VRF використовується інший механізм — Route Target (RT). RT — це розширений атрибут BGP Community, який визначає, які маршрути повинні бути експортовані з VRF та імпортовані в інші VRF. Поєднання RD та RT забезпечує гнучку та масштабовану систему розповсюдження маршрутної інформації між VPN.

Процес пересилки пакетів у MPLS L3VPN використовує стек із двох міток. Коли CE-маршрутизатор клієнта надсилає IP-пакет до PE-маршрутизатора оператора, PE виконує пошук у відповідній VRF та визначає VPN-мітку (внутрішню мітку), яку було отримано від віддаленого PE через MP-BGP. Ця мітка ідентифікує конкретну VRF на віддаленому PE. Далі PE додає транспортну мітку (зовнішню мітку), яка забезпечує доставку пакета до віддаленого PE через P-мережу. Проміжні P-маршрутизатори виконують лише операцію swap для зовнішньої мітки, не маючи жодної інформації про VPN-мітку або IP-заголовок клієнтського пакета. На передостанньому P-маршрутизаторі зовнішня мітка видаляється (PHP), і пакет із VPN-міткою надходить до вихідного PE, який на основі VPN-мітки визначає VRF та передає пакет до відповідного CE-маршрутизатора.

Обмін маршрутною інформацією між CE та PE маршрутизаторами може здійснюватися за допомогою різних протоколів маршрутизації: статичної маршрутизації, RIPv2, OSPF, EIGRP або eBGP. eBGP є найбільш поширеним вибором для великих корпоративних клієнтів. Масштабованість MPLS L3VPN забезпечується кількома механізмами. Route Reflector (RR) централізує розповсюдження VPNv4-маршрутів між PE, усуваючи необхідність повного зв'язку iBGP-сесій. Без RR кожен PE повинен мати iBGP-сесію з усіма іншими PE, що дає $O(N^2)$ сесій. З RR кожен PE встановлює iBGP-сесію лише з RR, що зменшує кількість сесій до $O(N)$.

4.4.2. L2VPN: VPWS, VPLS, EVPN

L2VPN на основі MPLS забезпечує прозору передачу фреймів канального рівня (Ethernet, Frame Relay, ATM, PPP) між географічно розподіленими сайтами клієнта через MPLS-інфраструктуру оператора. На відміну від L3VPN, де оператор бере

участь у маршрутизації клієнтського трафіку, L2VPN забезпечує «прозорий» канал зв'язку, і клієнт самостійно здійснює маршрутизацію на третьому рівні. Існують два основних типи L2VPN-послуг: VPWS (Virtual Private Wire Service) — сервіс «точка-точка», що емулює виділений канал зв'язку, та VPLS (Virtual Private LAN Service) — сервіс «точка-багатоточка», що емулює Ethernet-комутатор.

VPWS реалізується за допомогою технології pseudowire (псевдопровід), стандартизованої в серії RFC 4447/4448. Псевдопровід — це двонаправлений тунель між двома PE-маршрутизаторами, що емулює канал зв'язку певного типу. Для встановлення псевдопроводу PE-маршрутизатори обмінюються мітками через LDP (targeted LDP session) або через MP-BGP. Як і в L3VPN, для пересилки фреймів через MPLS-мережу використовується стек із двох міток: зовнішня (транспортна) мітка забезпечує доставку до віддаленого PE, а внутрішня (pseudowire) мітка ідентифікує конкретний псевдопровід. Ця технологія також відома під назвою AToM (Any Transport over MPLS) у реалізації Cisco.

VPLS, стандартизована в RFC 4761 та RFC 4762, забезпечує емуляцію Ethernet-комутатора між множиною сайтів клієнта. Кожен PE-маршрутизатор, що обслуговує сайти VPLS, створює VSI (Virtual Switch Instance) — віртуальний комутатор, який виконує функції вивчення MAC-адрес, пересилки на основі MAC-адрес та широкомовної розсилки невідомих unicast-фреймів. VPLS вимагає повного зв'язку псевдопроводів між усіма PE-маршрутизаторами, що обслуговують дану VPLS-інстанцію. Для зменшення кількості псевдопроводів може використовуватися ієрархічна VPLS (H-VPLS).

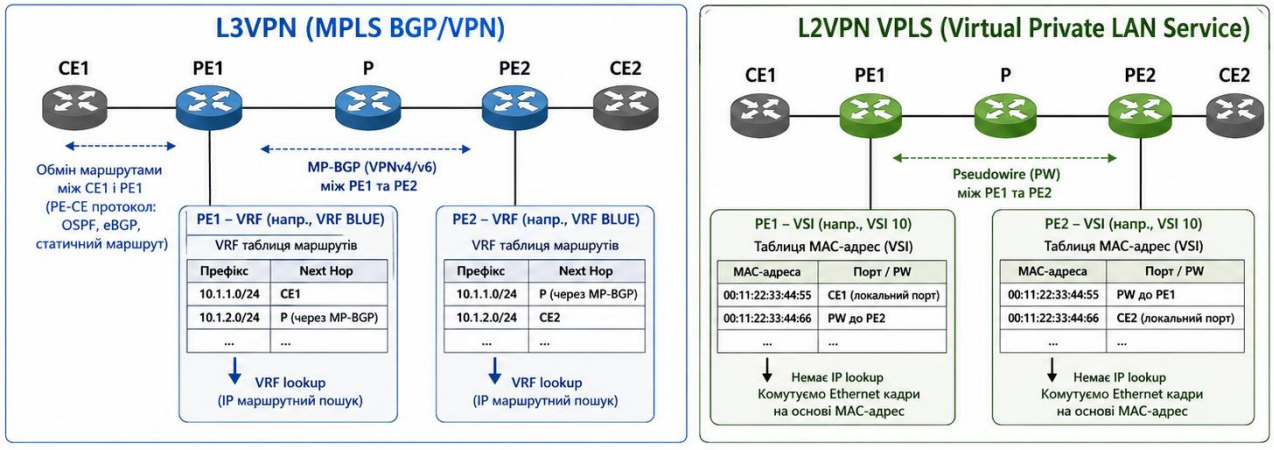

Рисунок 4.7 – Порівняння архітектур L3VPN та L2VPN (VPLS)

Сучасний розвиток L2VPN пов'язаний з технологією EVPN (Ethernet VPN), стандартизованою в RFC 7432. EVPN використовує MP-BGP для розповсюдження інформації про MAC-адреси та IP-адреси, що забезпечує контрольований процес вивчення MAC-адрес замість традиційного flooding. Це суттєво зменшує обсяг широкомовного трафіку та забезпечує оптимальну пересилку. EVPN також підтримує multihoming — підключення одного клієнтського сайту до кількох PE-маршрутизаторів для підвищення надійності. Завдяки використанню BGP для розповсюдження MAC-адрес, EVPN природно інтегрується з існуючою інфраструктурою Route Reflector. EVPN активно витісняє VPLS як основну технологію L2VPN в нових розгортаннях мереж.

Таблиця 4.2 — Порівняння типів MPLS VPN

Характеристика	L3VPN	VPWS	VPLS	EVPN
Рівень OSI	L3 (IP)	L2 (P2P)	L2 (MP)	L2/L3
Модель послуги	Peer-to-peer	Емуляція каналу	Емуляція LAN	Контрольований L2/L3
Ізоляція	VRF	Pseudowire	VSI + full mesh	EVI + BGP
Сигналізація	MP-BGP (VPNv4)	LDP / MP-BGP	LDP / MP-BGP	MP-BGP
Multihoming	Через PE-CE	Обмежена	Обмежена	Active-Active
Масштабованість	Висока (RR)	Висока	Середня	Висока (RR)
Сучасність	Зрілий стандарт	Зрілий стандарт	Замінюється EVPN	Активний розвиток

4.5. УПРАВЛІННЯ ТРАФІКОМ (TRAFFIC ENGINEERING)

Traffic Engineering (TE) — це комплекс технологій та методів, спрямованих на оптимальне використання мережевих ресурсів шляхом контролю розподілу потоків трафіку по мережі. Якщо традиційна IP-маршрутизація визначає шлях пакета виключно на основі метрики найкоротшого шляху, то Traffic Engineering дозволяє направляти трафік по альтернативних шляхах з урахуванням доступних ресурсів, вимог до якості обслуговування та бізнес-пріоритетів. MPLS TE поєднує гнучкість контролю шляхів, властиву технологіям з встановленням з'єднань, з простотою та масштабованістю IP-маршрутизації.

4.5.1. Мотивація та принципи Traffic Engineering

Необхідність Traffic Engineering найкраще ілюструється класичною проблемою, відомою як «fish problem» через характерну форму топології мережі. Розглянемо мережу, в якій між маршрутизаторами A та F існують два шляхи: прямий з високою пропускною здатністю та непрямий з нижчою пропускною здатністю. При використанні традиційної IP-маршрутизації весь трафік від A до F буде направлено по прямому шляху (як найкоротшому за метрикою IGP), тоді як непрямий шлях залишатиметься повністю незавантаженим. Навіть якщо прямий шлях стане перевантаженим, IGP не зможе перенаправити частину трафіку на альтернативний шлях. MPLS TE вирішує цю проблему, дозволяючи створити TE-тунелі по обох шляхах та розподілити трафік між ними відповідно до доступної пропускної здатності.

4.5.2. Алгоритм CSPF (Constrained SPF)

Обчислення шляху для TE-тунелю виконується алгоритмом CSPF (Constrained Shortest Path First). CSPF є модифікацією стандартного алгоритму Дейкстри (SPF), який використовується в OSPF та IS-IS, з додаванням урахування обмежень. Основним обмеженням є доступна смуга пропускання на кожному каналі зв'язку. Перед запуском алгоритму SPF, CSPF видаляє з графу мережі всі канали, які не задовольняють заданим обмеженням — наприклад, канали з недостатньою доступною пропускною здатністю або невідповідними атрибутами. Після цього запускається стандартний SPF на «очищеному» графі. Результатом CSPF є явний маршрут (ERO), що містить послідовність IP-адрес маршрутизаторів, через які повинен пройти TE-тунель.

Для роботи CSPF необхідна інформація про ресурси кожного каналу зв'язку в мережі. Ця інформація розповсюджується за допомогою розширень протоколів IGP: OSPF-TE (RFC 3630) та IS-IS-TE (RFC 5305). Ці розширення додають до стандартних

повідомлень IGP додаткові TLV (Type-Length-Value), що містять інформацію про максимальну та доступну пропускну здатність каналу, адміністративну групу каналу (affinity), TE-метрику та інші параметри. Ця інформація розповсюджується по всій IGP-зоні, що дозволяє кожному headend-маршрутизатору мати повну картину ресурсів мережі для обчислення оптимальних шляхів.

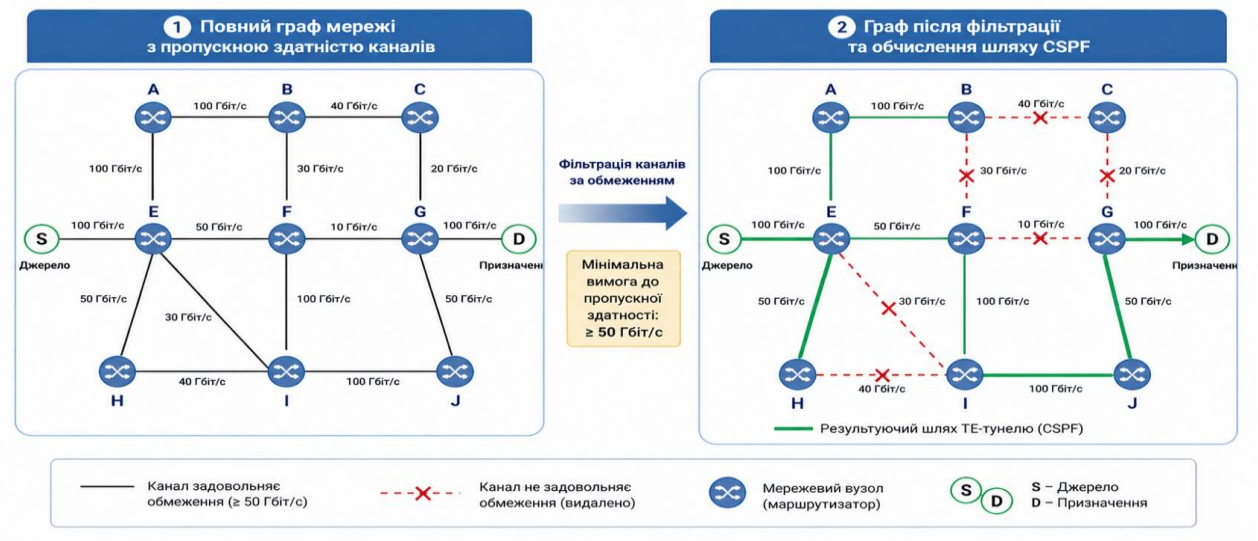

Рисунок 4.8 – Алгоритм CSPF: фільтрація каналів за обмеженнями та обчислення шляху

4.5.3. Резервування смуги пропускання та пріоритети

Резервування смуги пропускання є центральним механізмом MPLS TE. Кожен TE-тунель може мати налаштовану смугу пропускання, яка резервується на кожному каналі вздовж шляху тунелю. RSVP-TE підтримує вісім рівнів пріоритету (0–7, де 0 — найвищий пріоритет), які визначають порядок витіснення тунелів при нестачі ресурсів. Кожному TE-тунелю присвоюються два значення пріоритету: setup priority (пріоритет встановлення) та hold priority (пріоритет утримання). Тунель з вищим setup priority може витіснити (preempt) існуючий тунель з нижчим hold priority, якщо доступної смуги пропускання недостатньо. Цей механізм забезпечує гнучке управління ресурсами: критично важливі тунелі можуть мати вищий пріоритет і гарантовано отримувати необхідні ресурси.

Важливо розуміти, що резервування смуги пропускання в MPLS TE є «м'яким» (soft reservation): воно виконується лише на рівні площини управління RSVP-TE і не забезпечує автоматичного policing або shaping на рівні площини даних. Це означає, що трафік TE-тунелю може фактично перевищувати зарезервовану смугу пропускання, якщо не налаштовані відповідні механізми QoS. Проте адміністративне резервування є надзвичайно корисним для планування мережі: воно дозволяє CSPF правильно обчислювати шляхи з урахуванням фактичного завантаження мережі та запобігати надмірному використанню окремих каналів.

Механізм Auto-Bandwidth є розширенням MPLS TE, що дозволяє автоматично коригувати зарезервовану смугу пропускання TE-тунелю на основі реального обсягу трафіку. Маршрутизатор headend періодично вимірює обсяг трафіку, що проходить через TE-тунель (за замовчуванням кожні 5 хвилин), та зберігає максимальне значення за визначений інтервал (зазвичай одну годину). По закінченні інтервалу headend порівнює виміряне максимальне значення з поточною зарезервованою смугою пропускання і, якщо різниця перевищує заданий поріг, виконує перепризначення тунелю з новою смугою пропускання за механізмом make-before-break.

4.5.4. Інтеграція MPLS TE з QoS (DS-TE)

Інтеграція MPLS TE з механізмами QoS забезпечує комплексне рішення для гарантування якості обслуговування в операторських мережах. DiffServ-Aware Traffic Engineering (DS-TE), стандартизована в RFC 4124, розширює стандартний MPLS TE можливістю створювати TE-тунелі для різних класів трафіку з різними вимогами до смуги пропускання. DS-TE визначає концепцію «класових типів» (Class-Types, CT), кожен з яких має окремий пул пропускної здатності на кожному каналі зв'язку. Наприклад, голосовий трафік може мати гарантовану пропускну здатність 30% від ємності каналу, а трафік найкращих зусиль — решту 70%.

Дві моделі розподілу пропускної здатності визначені для DS-TE. Перша модель — **MAM** (Maximum Allocation Model) — встановлює жорсткі ліміти для кожного класового типу, забезпечуючи гарантоване розділення ресурсів. Друга модель — **RDM** (Russian Dolls Model) — дозволяє класам нижчого пріоритету використовувати невикористану пропускну здатність класів вищого пріоритету, забезпечуючи більш ефективне використання ресурсів при збереженні гарантій для пріоритетного трафіку. RDM є більш гнучкою та ефективною моделлю, хоча й складнішою у конфігурації.

Атрибути каналів (link attributes або affinity bits) є додатковим інструментом контролю шляхів TE-тунелів. Кожному каналу зв'язку може бути призначено 32-бітове значення атрибутів, де кожен біт може представляти певну характеристику каналу — наприклад, належність до певної географічної зони, тип середовища передачі, рівень надійності. TE-тунель може бути налаштований з маскою спорідненості, що визначає, які атрибути повинні бути присутні (include-any, include-all) або відсутні (exclude) на каналах, що входять до шляху тунелю. CSPF використовує цю інформацію для фільтрації каналів перед обчисленням шляху.

4.5.5. Fast Reroute (FRR) та реоптимізація

Механізм Fast Reroute, описаний в RFC 4090, є одним з найважливіших практичних застосувань MPLS TE, оскільки забезпечує швидке відновлення після відмов каналів або вузлів з часом перемикання менше 50 мілісекунд. Це робить MPLS-мережі конкурентоспроможними з SDH/SONET-мережами за показником часу відновлення, що є критично важливим для передачі голосового та відеотрафіку. FRR працює на основі локального відновлення: маршрутизатор, що безпосередньо виявив відмову (PLR), негайно переключає трафік на попередньо обчислений обхідний шлях, не чекаючи перерахунку основного шляху headend-маршрутизатором.

Існують два типи захисту FRR: захист каналу (link protection) та захист вузла (node protection). Захист каналу передбачає обчислення обхідного шляху навколо одного каналу зв'язку — при відмові каналу трафік переключається на обхідний шлях, що з'єднує ті самі два маршрутизатори, але через альтернативний шлях. Захист вузла є більш надійним: обхідний шлях обходить не лише канал, а й наступний маршрутизатор на шляху тунелю. Це забезпечує захист від відмови маршрутизатора, що є особливо важливим у мережах з обмеженою надлишковістю.

Для реалізації FRR на кожному PLR попередньо встановлюються обхідні тунелі (bypass tunnels) за допомогою RSVP-TE. При виявленні відмови PLR інкапсулює трафік захищеного тунелю в обхідний тунель, додаючи додаткову мітку (третю в стеку), і надсилає його по обхідному шляху. На точці злиття (Merge Point, MP) обхідний тунель з'єднується з основним шляхом, і пакет продовжує рух до призначення.

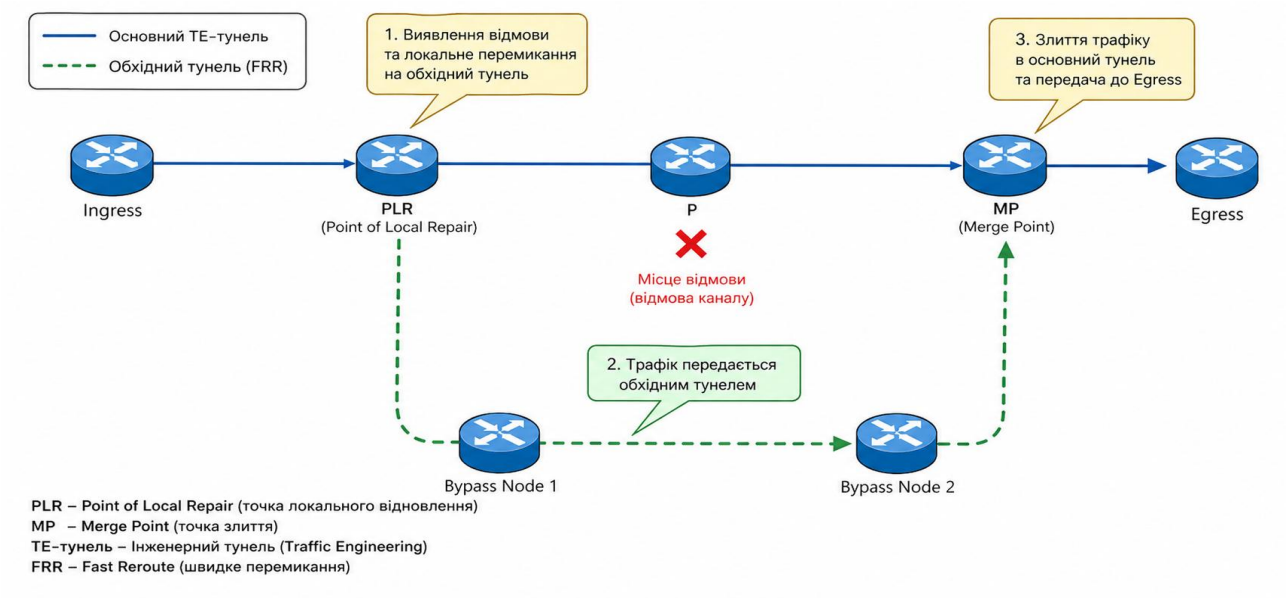

Рисунок 4.9 – Механізм Fast Reroute: захист каналу та вузла

Реоптимізація TE-тунелів — це процес перерахунку шляхів існуючих тунелів з метою знаходження більш оптимальних маршрутів. Реоптимізація може виконуватися періодично (за таймером, наприклад кожні 3600 секунд) або при зміні топології мережі (event-driven). При реоптимізації headend виконує CSPF з поточними даними про ресурси мережі і, якщо знаходить кращий шлях, переключає тунель за допомогою механізму make-before-break. Реоптимізація є важливим інструментом для підтримки оптимального розподілу трафіку в мережі, що постійно змінюється.

У сучасних мережах MPLS TE продовжує відігравати ключову роль, хоча його застосування еволюціонує. Технологія Segment Routing (SR), стандартизована в серії RFC 8402, пропонує альтернативний підхід до Traffic Engineering, що не вимагає протоколу RSVP-TE для сигналізації шляхів. У SR шлях визначається списком сегментів, що кодується безпосередньо у заголовку пакета, усуваючи необхідність підтримки стану на проміжних маршрутизаторах. SR може працювати як з MPLS data plane (SR-MPLS), так і з IPv6 data plane (SRv6). Незважаючи на активний розвиток SR, традиційний MPLS TE з RSVP-TE залишається широко використовуваним у існуючих мережах завдяки розвиненій екосистемі управління, підтримці FRR та глибокій інтеграції з механізмами QoS.

Контрольні питання

1. Поясніть структуру 32-бітового MPLS-заголовка та призначення кожного поля.
2. Що таке «shim header» та чому MPLS характеризують як технологію рівня «2,5»?
3. У чому полягає відмінність між Ingress LSR, Transit LSR та Egress LSR? Які операції з мітками виконує кожен з них?
4. Дайте визначення поняття FEC (Forwarding Equivalence Class). Як він визначається на вхідному LSR?
5. Що таке LSP (Label Switched Path)? Чим LSP, побудовані за допомогою LDP, відрізняються від LSP, побудованих за допомогою RSVP-TE?
6. Опишіть взаємодію площини управління (Control Plane) та площини даних (Data Plane) в MPLS. Які бази даних використовуються (LIB, LFIB, FIB)?
7. Порівняйте MPLS з традиційною IP-маршрутизацією за основними критеріями: механізм пересилки, продуктивність, гнучкість, підтримка VPN.
8. Опишіть процес встановлення LDP-сесії між двома маршрутизаторами. Які повідомлення використовуються (Hello, Initialization, Keepalive)?
9. Порівняйте режими розподілу міток Downstream Unsolicited та Downstream on Demand у LDP.
10. Поясніть різницю між Liberal та Conservative Label Retention Mode. Який режим забезпечує швидше відновлення після змін топології?
11. Опишіть процес встановлення TE-тунелю за допомогою RSVP-TE (повідомлення Path та Resv).
12. Чому RSVP-TE належить до протоколів «м'якого стану» (soft-state)? Як це впливає на масштабованість?
13. Поясніть призначення механізму make-before-break у RSVP-TE.
14. Опишіть три базові операції з мітками у MPLS: push, swap, pop. На яких маршрутизаторах вони виконуються?
15. Як працює механізм Penultimate Hop Popping (PHP) і яку проблему він вирішує? Чим відрізняються Implicit NULL та Explicit NULL?
16. Поясніть особливості поведінки поля TTL у MPLS. У чому полягає режим «no TTL propagation»?
17. Які проблеми створює балансування навантаження в MPLS-мережах та як вони вирішуються (Entropy Label)?
18. Поясніть проблему MTU в MPLS-мережах та способи її вирішення.
19. Що таке VRF і яку роль вона відіграє в архітектурі L3VPN?
20. Поясніть різницю між Route Distinguisher (RD) та Route Target (RT). Яку функцію виконує кожен з них?

РОЗДІЛ 5
ETHERNET В МЕРЕЖАХ ОПЕРАТОРІВ

У п’ятому розділі розглядаються технології Ethernet, що використовуються в мережах операторів зв’язку. Особлива увага приділяється концепції Carrier Ethernet, механізмам подвійного тегування VLAN (QinQ), технологіям VLAN stacking та Provider Backbone Bridging (PBB), агрегації каналів (EtherChannel), а також архітектурі сучасних міських мереж Metro Ethernet, що формують основу телекомунікаційної інфраструктури сучасних операторів зв’язку.

Технологія Ethernet, що зародилася у 1973 році в дослідницькому центрі Xerox PARC як рішення для локальних мереж, пройшла вражаючий еволюційний шлях від простого протоколу передачі даних зі швидкістю 10 Мбіт/с до основної технології побудови операторських мереж з пропускною здатністю 400 Гбіт/с і вище. Сьогодні Ethernet домінує не лише в корпоративних LAN, але й активно витісняє традиційні технології TDM (SONET/SDH, Frame Relay, ATM) у мережах операторів зв’язку, міських мережах (MAN) та навіть у магістральних мережах (WAN). Ця фундаментальна трансформація стала можливою завдяки розвитку концепції Carrier Ethernet — набору стандартів та специфікацій, що адаптують Ethernet для використання в операторських мережах із забезпеченням надійності, масштабованості та якості обслуговування (QoS) операторського класу.

Перехід операторів зв’язку до Ethernet-технологій обумовлений кількома ключовими чинниками. По-перше, Ethernet є найбільш поширеною технологією на рівні доступу — переважна більшість корпоративних та домашніх мереж використовують Ethernet як основний протокол канального рівня. Використання Ethernet у мережах операторів усуває необхідність перетворення протоколів на межі між клієнтською та операторською мережами, що спрощує архітектуру та зменшує затримки. По-друге, обладнання Ethernet значно дешевше за традиційне TDM-обладнання при порівнянній пропускній здатності, що суттєво знижує капітальні та операційні витрати оператора. По-третє, Ethernet забезпечує гнучке масштабування швидкості — від 10 Мбіт/с до 400 Гбіт/с — що дозволяє операторам надавати послуги різної ємності без заміни базового обладнання. По-четверте, широка екосистема виробників Ethernet-обладнання забезпечує конкуренцію та знижує ціни, тоді як традиційне TDM-обладнання пропонується обмеженим колом постачальників.

Еволюція Ethernet від локальної технології до операторської платформи відбувалася поступово. Перший стандарт Ethernet (IEEE 802.3) забезпечував швидкість 10 Мбіт/с у мережах із спільним середовищем передачі (shared media) на основі коаксіального кабелю. Fast Ethernet (IEEE 802.3u, 1995 рік) підвищив швидкість до 100 Мбіт/с та забезпечив перехід до повнодуплексного режиму на витій парі та волоконно-оптичному кабелі. Gigabit Ethernet (IEEE 802.3z/802.3ab, 1998–1999 роки) досяг швидкості 1 Гбіт/с і став домінуючою технологією для магістральних з’єднань у корпоративних мережах. 10 Gigabit Ethernet (IEEE 802.3ae, 2002 рік) вперше вийшов за межі LAN і став використовуватися в міських (MAN) та глобальних (WAN) мережах. Подальші стандарти — 25GbE, 40GbE, 50GbE, 100GbE (IEEE 802.3ba, 2010 рік) та 400GbE (IEEE 802.3bs, 2017 рік) — забезпечили пропускну здатність, достатню для магістральних мереж найбільших операторів зв’язку.

Ключова ідея

Carrier Ethernet перетворює традиційну локальну технологію на повноцінне рішення операторського класу, поєднуючи економічну ефективність Ethernet з надійністю, масштабованістю та якістю обслуговування, характерними для класичних TDM-мереж SDH/SONET.

5.1. CARRIER ETHERNET

Carrier Ethernet — це концепція розширення технології Ethernet для використання в мережах операторів зв'язку (carrier networks), що передбачає додавання до базового Ethernet-протоколу механізмів забезпечення надійності, масштабованості, управління якістю обслуговування та операційного управління, необхідних для надання телекомунікаційних послуг комерційного рівня. На відміну від традиційного LAN Ethernet, який працює за принципом «найкращих зусиль» (best effort) і не гарантує доставку даних, Carrier Ethernet забезпечує рівень обслуговування, порівнянний із традиційними TDM-технологіями, при значно нижчій вартості. Стандартизацію та просування Carrier Ethernet здійснює Metro Ethernet Forum (MEF) — міжнародна галузева організація, заснована у 2001 році, що об'єднує понад 200 операторів зв'язку, виробників обладнання та системних інтеграторів з усього світу.

5.1.1. Атрибути Carrier Ethernet за MEF

MEF визначає п'ять ключових атрибутів, яким повинна відповідати мережа для класифікації як Carrier Ethernet. Ці атрибути відрізняють Carrier Ethernet від традиційного LAN Ethernet і забезпечують відповідність вимогам операторів зв'язку до якості та надійності послуг. Першим атрибутом є стандартизовані сервіси (Standardized Services): мережа повинна підтримувати стандартні типи послуг, визначені MEF, з чітко описаними параметрами та інтерфейсами. Стандартизація сервісів забезпечує сумісність обладнання різних виробників та дозволяє операторам надавати уніфіковані послуги незалежно від використовуваної платформи. MEF визначає детальні специфікації для кожного типу сервісу, включаючи параметри продуктивності, інтерфейси та механізми управління.

Другий атрибут — масштабованість (Scalability): мережа повинна підтримувати мільйони Ethernet-сервісних інстанцій (EVC — Ethernet Virtual Connection) та мільйони MAC-адрес в одному домені. На відміну від корпоративних LAN, де кількість VLAN та MAC-адрес вимірюється сотнями або тисячами, операторська мережа повинна одночасно обслуговувати десятки тисяч клієнтів, кожен з яких може мати власну VLAN-структуру. Третій атрибут — надійність (Reliability): мережа повинна забезпечувати доступність на рівні 99,999% (не більше 5,26 хвилини простою на рік), що відповідає стандартам «п'яти дев'яток» традиційних телекомунікаційних мереж. Це вимагає впровадження механізмів захисту та швидкого відновлення після відмов з часом перемикання менше 50 мілісекунд.

Четвертий атрибут — якість обслуговування (Quality of Service, QoS): мережа повинна підтримувати диференційоване обслуговування трафіку з гарантіями затримки (latency), варіації затримки (jitter) та втрат (frame loss ratio) для різних класів сервісу. Операторська мережа повинна одночасно передавати голосовий, відеотрафік та дані з різними вимогами до якості: голосовий трафік потребує мінімальної затримки (менше 150 мс end-to-end) та джитеру (менше 30 мс), відеотрафік — високої пропускної здатності та мінімальних втрат, а трафік даних — гарантованої доставки. П'ятий атрибут — управління сервісами (Service Management): оператор повинен мати можливість комплексного моніторингу, діагностики та управління Ethernet-сервісами

через стандартні механізми OAM (Operations, Administration, and Maintenance). Це включає виявлення та локалізацію відмов, вимірювання параметрів продуктивності та автоматичне повідомлення про порушення SLA.

5.1.2. Архітектура та інтерфейси Carrier Ethernet

Архітектура Carrier Ethernet базується на кількох фундаментальних концепціях, що визначають взаємодію між мережею клієнта та мережею оператора. UNI (User-to-Network Interface) — це демаркаційна точка між мережею клієнта та мережею оператора, де визначаються параметри послуги, включаючи швидкість підключення (UNI bandwidth), кількість і тип EVC та параметри QoS. Фізично UNI зазвичай реалізується як Ethernet-порт на обладнанні оператора (PE — Provider Edge), до якого підключається обладнання клієнта (CE — Customer Edge). MEF визначає кілька типів UNI залежно від конфігурації: UNI з одним EVC (all-to-one bundling), UNI з кількома EVC (service multiplexing) та UNI без VLAN-тегування (bundling without C-VLAN tag preservation). NNI (Network-to-Network Interface) — це інтерфейс між мережами різних операторів (External NNI, E-NNI) або між різними доменами одного оператора (Internal NNI, I-NNI). E-NNI є критично важливим для надання мультиоператорських Ethernet-послуг, де клієнтський трафік повинен пройти через мережі кількох операторів для досягнення віддалених сайтів.

EVC (Ethernet Virtual Connection) — це логічне з’єднання між двома або більше UNI, що забезпечує передачу Ethernet-фреймів між клієнтськими сайтами. EVC є аналогом віртуального каналу (PVC) у технології Frame Relay та забезпечує ізоляцію трафіку різних клієнтів. Кожен EVC має набір атрибутів, що визначають його поведінку: тип (point-to-point або multipoint-to-multipoint), параметри QoS (bandwidth profile per EVC або per CoS), обробку CE-VLAN тегів (preservation або не-preservation) та параметри OAM. Важливим параметром EVC є CoS (Class of Service) — клас обслуговування, що визначає пріоритет обробки фреймів у мережі оператора. MEF визначає до восьми класів обслуговування, кожен з яких має власні гарантії щодо затримки, джитеру та втрат.

5.1.3. Типи Ethernet-сервісів MEF

MEF визначає три базових типи Ethernet-сервісів, кожен з яких може бути реалізований як порт-орієнтований або VLAN-орієнтований. **E-Line** (Ethernet Line) — це сервіс типу «точка-точка», що з’єднує два UNI через один EVC. E-Line є Ethernet-аналогом виділеної лінії або Frame Relay PVC і використовується для з’єднання двох офісів клієнта, підключення клієнта до дата-центру або для побудови WAN-з’єднань. Конкретними реалізаціями E-Line є EPL (Ethernet Private Line) — виділена лінія з повною ізоляцією трафіку, де кожен UNI використовується виключно для одного EVC, та EVPL (Ethernet Virtual Private Line) — з’єднання з мультиплексуванням кількох сервісів через один фізичний порт UNI, що дозволяє клієнту підключатися до кількох віддалених сайтів через один порт.

E-LAN (Ethernet LAN) — це сервіс типу «багатоточка-до-багатоточки» (multipoint-to-multipoint), що з’єднує множину UNI через multipoint-to-multipoint EVC. E-LAN емулює Ethernet-комутатор, забезпечуючи пряму зв’язність між усіма підключеними сайтами. Фрейм, надісланий від будь-якого UNI, може бути доставлений до будь-якого іншого UNI в тому ж EVC. Реалізаціями E-LAN є EP-LAN (Ethernet Private LAN) — з виділеними UNI для одного EVC, та EVP-LAN (Ethernet Virtual Private LAN) — з мультиплексуванням кількох EVC на одному UNI. E-LAN ідеально підходить для з’єднання множини офісів клієнта в єдину корпоративну мережу без необхідності побудови full-mesh з’єднань «точка-точка».

E-Tree (Ethernet Tree) — це сервіс типу «одна-коренева-точка-до-багатьох-листків» (rooted multipoint), де «кореневий» UNI може спілкуватися з усіма «листковими» UNI, а «листкові» UNI можуть спілкуватися лише з «кореневим», але не між собою. E-Tree ідеально підходить для сценаріїв «головний офіс — філії», розповсюдження контенту (content distribution) або доступу до Інтернету, де філії повинні мати доступ до центрального ресурсу, але не потребують прямої зв'язності між собою.

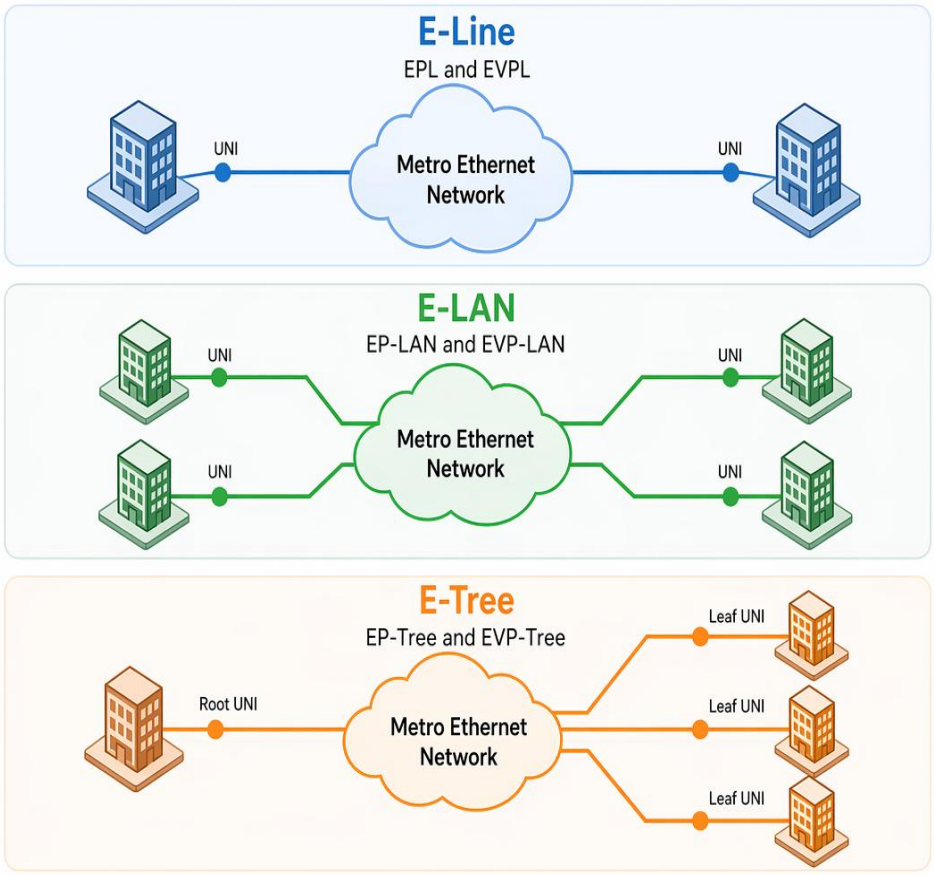

Рисунок 5.1 – Типи Ethernet-сервісів MEF: E-Line, E-LAN, E-Tree

5.1.4. Механізми OAM у Carrier Ethernet

Механізми OAM (Operations, Administration, and Maintenance) є критично важливим компонентом Carrier Ethernet, оскільки забезпечують можливість моніторингу, діагностики та управління Ethernet-сервісами на рівні, порівнянному з традиційними TDM-мережами, де механізми OAM вбудовані безпосередньо у структуру фрейму (overhead bytes у SONET/SDH). Стандарт IEEE 802.1ag (Connectivity Fault Management, CFM) визначає механізми виявлення та локалізації відмов у Ethernet-мережах. CFM використовує ієрархічну модель з трьома рівнями обслуговування (Maintenance Domain Levels, MD Levels), що дозволяє різним організаціям (оператору, замовнику, постачальнику) незалежно контролювати свої сегменти мережі. CFM визначає три типи функціональних точок: MEP (Maintenance End Point) — кінцева точка домену обслуговування, що генерує та приймає повідомлення OAM; MIP (Maintenance Intermediate Point) — проміжна точка, що може відповідати на запити, але не ініціює їх; та MD (Maintenance Domain) — область мережі, що контролюється однією організацією.

CFM використовує три типи повідомлень для виявлення та локалізації відмов. Continuity Check Messages (CCM) — це періодичні повідомлення, що надсилаються

між MEP для перевірки зв'язності. CCM надсилаються з конфігурованим інтервалом (від 3,3 мс до 10 хвилин) і дозволяють MEP виявити втрату зв'язності з віддаленим MEP, якщо протягом 3,5 інтервалів не отримано жодного CCM. Loopback Messages (LBM/LBR) — це повідомлення для перевірки досяжності конкретного MEP або MIP, аналогічні ICMP ping. Linktrace Messages (LTM/LTR) — це повідомлення для визначення шляху через мережу, аналогічні traceroute; вони проходять через всі MIP між двома MEP, формуючи карту шляху. Стандарт ITU-T Y.1731 розширює функціональність CFM додатковими механізмами вимірювання продуктивності: Frame Delay Measurement (вимірювання односторонньої та двосторонньої затримки), Frame Delay Variation (вимірювання джитеру) та Frame Loss Ratio (вимірювання коефіцієнта втрат фреймів). Ці механізми дозволяють оператору в реальному часі контролювати дотримання параметрів SLA для кожного EVC.

5.1.5. QoS та Bandwidth Profiles

Забезпечення якості обслуговування (QoS) у Carrier Ethernet реалізується через механізми класифікації, маркування, формування трафіку (shaping) та управління чергами (queuing). Класифікація трафіку може виконуватися на основі VLAN ID, значення поля CoS (Class of Service) у тегу 802.1Q (3 біти, що визначають до 8 класів обслуговування), значення поля DSCP у IP-заголовку або комбінації цих параметрів. На інтерфейсі UNI оператор застосовує bandwidth profile — набір параметрів, що визначають дозволену швидкість передачі для клієнта.

Bandwidth profile включає чотири ключових параметри: CIR (Committed Information Rate) — гарантовану швидкість передачі, CBS (Committed Burst Size) — допустимий обсяг пакетного навантаження понад CIR, EIR (Excess Information Rate) — додаткову швидкість передачі, та EBS (Excess Burst Size) — допустимий обсяг додаткового навантаження. Трафік, що відповідає CIR/CBS, маркується зеленим кольором і гарантовано доставляється. Трафік, що перевищує CIR, але відповідає EIR/EBS, маркується жовтим і доставляється за наявності вільних ресурсів. Трафік, що перевищує EIR/EBS, відкидається. Цей механізм відомий як алгоритм «trTCM» (two-rate Three Color Marker) і є основою policing трафіку в Carrier Ethernet.

5.1.6. Механізми захисту та надійності

Для забезпечення надійності Carrier Ethernet використовує кілька механізмів захисту та відновлення. Spanning Tree Protocol (STP, IEEE 802.1D) та його еволюції — Rapid STP (RSTP, IEEE 802.1w) та Multiple STP (MSTP, IEEE 802.1s) — забезпечують усунення петель та автоматичне відновлення зв'язності при відмові каналу, хоча час збіжності STP (до 50 секунд) є неприйнятним для операторських мереж. RSTP скорочує цей час до кількох секунд, а MSTP дозволяє створювати окремі інстанції STP для різних VLAN, оптимізуючи використання резервних шляхів. Ethernet Ring Protection Switching (ERPS, ITU-T G.8032) — це механізм захисту, спеціально розроблений для кільцевих Ethernet-топологій, що забезпечує час відновлення менше 50 мс, порівнянний із SONET/SDH APS. ERPS використовує протокол R-APS (Ring Automatic Protection Switching) для координації між вузлами кільця та блокує один канал у кільці (RPL — Ring Protection Link) для запобігання петлям. При виявленні відмови ERPS деблокує RPL та переключає трафік на резервний шлях протягом менше 50 мс. ERPS підтримує як одиночні, так і взаємопов'язані кільця (interconnected rings), що забезпечує побудову складних мережевих топологій з високою доступністю.

Агрегація каналів (Link Aggregation, IEEE 802.1AX) забезпечує об'єднання кількох фізичних каналів у один логічний, забезпечуючи як збільшення пропускної здатності, так і відмовостійкість — ця технологія детально розглядається у підрозділі

5.4. Додатково, для забезпечення надійності на рівні обладнання, операторські комутатори підтримують резервування контролерів (supervisor redundancy), джерел

Важливо

Час перемикання у разі аварії менше 50 мс, що забезпечується механізмом ERPS (G.8032), є де-факто стандартом «операторського класу» (carrier grade). Без виконання цієї вимоги Ethernet-мережа не може вважатися повноцінним замінником SDH/SONET у транспортних мережах операторів зв'язку.

5.2. QinQ

Технологія QinQ (також відома як 802.1ad Provider Bridging, VLAN stacking або Double Tagging) є одним із ключових механізмів, що забезпечує масштабованість Ethernet-мереж операторського класу. Основна ідея QinQ полягає у додаванні другого тегу 802.1Q (Service VLAN tag, S-tag) до Ethernet-фреймів клієнта, які вже містять власний тег 802.1Q (Customer VLAN tag, C-tag). Це подвійне тегування дозволяє оператору використовувати власний простір VLAN-ідентифікаторів для ізоляції та комутації трафіку різних клієнтів, повністю незалежно від VLAN-конфігурацій у клієнтських мережах. Термін «QinQ» буквально означає «802.1Q всередині 802.1Q», що точно описує принцип роботи технології.

5.2.1. Проблема масштабованості VLAN та рішення QinQ

Необхідність у QinQ зумовлена фундаментальним обмеженням стандарту IEEE 802.1Q: 12-бітове поле VLAN ID (VID) у тегу 802.1Q дозволяє визначити лише 4094 унікальних VLAN (значення 0 та 4095 зарезервовані). Для оператора зв'язку, що обслуговує тисячі клієнтів, кожен з яких може використовувати до 4094 власних VLAN, цього обсягу катастрофічно недостатньо. Навіть якщо кожному клієнту виділити лише один VLAN, оператор зможе обслуговувати не більше 4094 клієнтів в одному Ethernet-домені — це неприйнятно для великих операторських мереж.

QinQ вирішує цю проблему шляхом створення ієрархії VLAN: **зовнішній тег** (S-VLAN) використовується оператором для ідентифікації клієнта або сервісу, **а внутрішній тег** (C-VLAN) зберігає оригінальну VLAN-ідентифікацію клієнта. Таким чином, оператор може обслуговувати до 4094 клієнтів, кожен з яких може використовувати повний діапазон 4094 VLAN, що дає теоретичний максимум у 4094 × 4094 ≈ 16,8 мільйона унікальних комбінацій.

5.2.2. Структура фрейму з подвійним тегуванням

Структура фрейму з подвійним тегуванням QinQ відрізняється від стандартного тегованого фрейму наявністю двох тегів 802.1Q між MAC-адресами та полем EtherType/Length. Зовнішній тег (S-tag) використовує значення EtherType 0x88A8 (визначене стандартом IEEE 802.1ad), що відрізняється від стандартного EtherType 802.1Q (0x8100). Це розрізнення EtherType дозволяє мережевому обладнанню однозначно ідентифікувати фрейми з подвійним тегуванням та правильно обробляти їх. Внутрішній тег (C-tag) зберігає стандартний EtherType 0x8100 та оригінальний VLAN ID клієнта.

Кожен тег має однакову 4-байтову структуру: 16 біт TPID (Tag Protocol Identifier, EtherType), 3 біти PCP (Priority Code Point, пріоритет), 1 біт DEI (Drop Eligible Indicator, індикатор можливості відкидання) та 12 біт VID (VLAN Identifier). Слід зазначити, що подвійне тегування збільшує розмір Ethernet-фрейму на додаткові 4 байти (загалом 8 байт для двох тегів замість 4 для одного), що може впливати на ефективний MTU. Максимальний розмір стандартного Ethernet-фрейму становить 1518 байт (1522 з

одним тегом 802.1Q), тому фрейм з подвійним тегуванням може досягати 1526 байт, що перевищує стандартний MTU і потребує підтримки baby giant або jumbo frames на інтерфейсах операторської мережі.

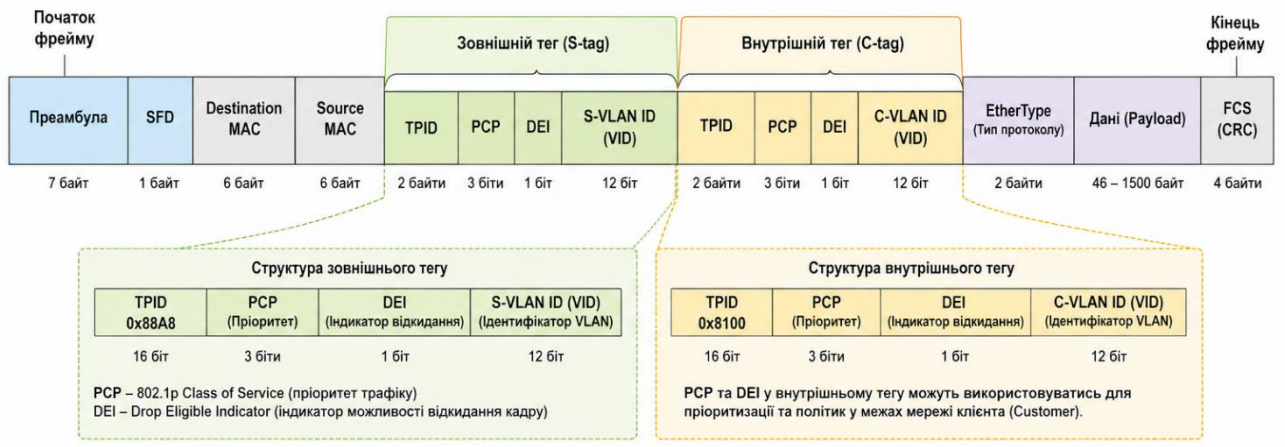

Рисунок 5.2 – Структура Ethernet-фрейму з подвійним тегуванням QinQ

5.2.3. Режими обробки фреймів QinQ

Процес обробки фреймів QinQ на межі між клієнтською та операторською мережами може виконуватися в двох основних режимах. Port-based QinQ (також відомий як basic QinQ) є простішим варіантом, де всі фрейми, що надходять на порт UNI, отримують однаковий S-VLAN ID незалежно від їх C-VLAN. Цей режим конфігурується шляхом призначення S-VLAN порту: будь-який фрейм, що входить через цей порт, автоматично отримує зовнішній S-tag з налаштованим S-VLAN ID. Port-based QinQ ідеально підходить для сценарію, де один фізичний порт UNI виділений для одного клієнта і всі його VLAN повинні транспортуватися через мережу оператора.

Selective QinQ (або VLAN-based QinQ) є гнучкішим варіантом, де S-VLAN ID призначається на основі значення C-VLAN ID вхідного фрейму. Це дозволяє на одному фізичному порту UNI розділити трафік клієнта на кілька сервісів: наприклад, C-VLAN 10-20 можуть бути відображені на S-VLAN 100 (корпоративний Інтернет), а C-VLAN 30-40 — на S-VLAN 200 (голосовий сервіс). Selective QinQ вимагає більш складної конфігурації, але забезпечує максимальну гнучкість у наданні мультисервісних послуг через один фізичний порт.

5.2.4. Прозорість QinQ та маніпуляція пріоритетами

Однією з важливих переваг QinQ є прозорість для клієнтської мережі: протоколи клієнта, що працюють на канальному рівні — STP, VTP, CDP, LLDP, BPDU — передаються через операторську мережу без змін, оскільки оператор оперує лише зовнішнім тегом і не аналізує вміст клієнтських фреймів. Це забезпечує повну ізоляцію доменів канального рівня різних клієнтів та дозволяє кожному клієнту незалежно управляти своєю мережевою інфраструктурою. Проте ця прозорість має і зворотний бік: оператор не може впливати на поведінку протоколів клієнтської мережі, що може спричинити проблеми, наприклад, якщо STP-BPDU клієнта впливатиме на топологію інших клієнтів. Для запобігання таким проблемам оператори зазвичай використовують BPDU-фільтрацію або BPDU-тунелювання на портах UNI.

QinQ також забезпечує можливість маніпуляції з мітками пріоритету (PCP). Оператор може встановлювати значення PCP у зовнішньому S-tag відповідно до класу обслуговування, узгодженого в SLA з клієнтом, при цьому значення PCP у внутрішньому C-tag залишається незмінним, що дозволяє клієнту зберігати власну схему QoS. Для забезпечення end-to-end QoS оператор може виконувати копіювання

(copying) або відображення (mapping) значень PCP між C-tag та S-tag. Наприклад, оператор може копіювати значення PCP з C-tag клієнта в S-tag, забезпечуючи збереження пріоритетів, встановлених клієнтом. Альтернативно, оператор може застосовувати власну політику класифікації, перевизначаючи пріоритети клієнта відповідно до умов SLA. Поле DEI (Drop Eligible Indicator) у S-tag може використовуватися для маркування фреймів, що підлягають відкиданню при перевантаженні мережі — зазвичай це фрейми з жовтим маркуванням (yellow traffic) відповідно до bandwidth profile.

Таблиця 5.1 — Порівняння звичайного VLAN (802.1Q) та QinQ (802.1ad)

Критерій	Звичайний VLAN (802.1Q)	QinQ (802.1ad)
Кількість тегів	Один (C-tag)	Два (S-tag + C-tag)
EtherType тегу	0x8100	Зовн.: 0x88A8, внутр.: 0x8100
Простір VLAN ID	4094	4094 × 4094 ≈ 16,8 млн
Призначення	Сегментація LAN	Ізоляція клієнтів оператора
Прозорість для клієнта	Клієнт бачить VLAN оператора	Клієнт повністю ізольований
Збільшення розміру фрейму	+4 байти	+8 байт (два теги)
Масштабованість	Обмежена (4094)	Висока (мільйони)
Сфера застосування	Корпоративні LAN	Операторські MAN/WAN

5.3. VLAN STACKING

VLAN stacking (накладання або стекування VLAN) є загальною концепцією багаторівневого тегування Ethernet-фреймів, яка включає QinQ як найбільш поширений варіант, але не обмежується ним. У ширшому розумінні VLAN stacking охоплює будь-які механізми додавання множинних VLAN-тегів до фрейму для забезпечення ієрархічної ізоляції трафіку, масштабування мережі та надання мультисервісних послуг. Ця концепція є природним розвитком ідеї VLAN (IEEE 802.1Q), що дозволяє розділяти трафік різних груп користувачів у одній фізичній мережі, з поширенням на мережі операторського класу, де необхідно підтримувати множину клієнтів із перекриваючимися VLAN-просторами. Стандарти IEEE 802.1ad та IEEE 802.1ah формалізують різні рівні VLAN stacking для різних масштабів мереж.

5.3.1. Модель Provider Bridge Network (IEEE 802.1ad)

У контексті операторських мереж VLAN stacking реалізує модель «мережа в мережі» (Provider Bridge Network), визначену стандартом IEEE 802.1ad. Ця модель передбачає чітке розмежування між клієнтським рівнем (C-component) та операторським рівнем (S-component). C-component оперує C-VLAN тегами (EtherType 0x8100) і відповідає за обробку трафіку відповідно до VLAN-конфігурації клієнта. S-component оперує S-VLAN тегами (EtherType 0x88A8) і забезпечує транспортування клієнтського трафіку через операторську мережу. Кожен клієнт або сервіс отримує унікальний S-VLAN ID, що забезпечує ізоляцію від інших клієнтів на рівні MAC-адрес та VLAN-тегів. Комутатори в мережі оператора виконують MAC-навчання та пересилку фреймів на основі комбінації S-VLAN ID та MAC-адрес призначення, не аналізуючи C-VLAN теги клієнта. Це означає, що MAC-таблиці комутаторів оператора містять MAC-адреси всіх клієнтських пристроїв, що є одним з обмежень масштабованості Provider Bridge Network.

5.3.2. Provider Backbone Bridging (IEEE 802.1ah)

Подальшим розвитком концепції VLAN stacking є технологія Provider Backbone Bridging (PBB), стандартизована в IEEE 802.1ah (також відома як MAC-in-MAC). PBB додає до ієрархії тегів ще один рівень інкапсуляції: замість простого додавання зовнішнього тегу, PBB інкапсулює весь клієнтський Ethernet-фрейм (включаючи MAC-адреси джерела та призначення) у новий фрейм із MAC-адресами магістральної мережі (Backbone MAC, B-MAC). Це вирішує одну з ключових проблем масштабованості QinQ: у великих мережах таблиці MAC-адрес на комутаторах магістральної мережі стають надзвичайно великими, оскільки вони повинні вивчати MAC-адреси всіх клієнтських пристроїв з усіх VLAN. PBB усуває цю проблему, оскільки магістральні комутатори бачать лише B-MAC адреси граничних пристроїв оператора (BEB — Backbone Edge Bridge), а не тисячі клієнтських MAC-адрес. Стандарт PBB визначає два нових ідентифікатори: B-VID (Backbone VLAN Identifier, 12 біт) для ідентифікації магістральних VLAN та I-SID (Service Instance Identifier, 24 біти), що дозволяє підтримувати до 16 мільйонів сервісних інстанцій — суттєво більше, ніж 4094 × 4094 комбінацій QinQ.

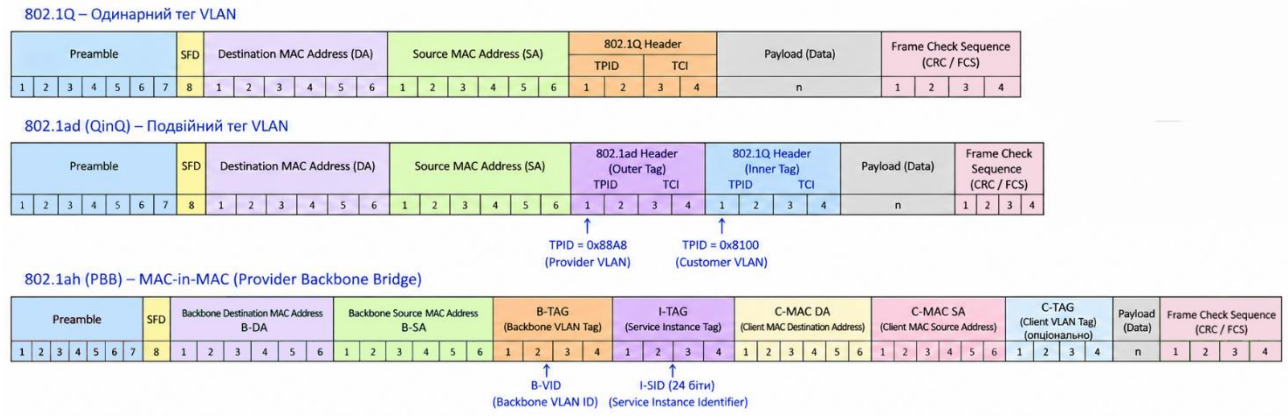

Рисунок 5.3 – Ієрархія технологій VLAN stacking: 802.1Q → 802.1ad (QinQ) → 802.1ah (PBB)

5.3.3. Трирівнева архітектура та VLAN stacking

Практичне застосування VLAN stacking в операторських мережах визначається трирівневою архітектурою: доступ (access), агрегація (aggregation) та ядро (core). На рівні доступу комутатори виконують класифікацію клієнтського трафіку та додавання S-VLAN тегів (QinQ). На рівні агрегації комутатори виконують об'єднання трафіку від множини пристроїв рівня доступу та можуть здійснювати додаткову обробку — наприклад, selective QinQ для поділу трафіку одного клієнта на різні сервіси. На рівні ядра трафік транспортується на основі S-VLAN тегів або B-VID (у випадку PBB) з мінімальною обробкою. Ця ієрархія забезпечує масштабованість мережі: зростання кількості клієнтів на рівні доступу не впливає на складність обробки на рівні ядра, оскільки ядро оперує лише обмеженою кількістю S-VLAN або B-VID. Крім того, ієрархічна архітектура дозволяє оптимізувати кожен рівень для його специфічних функцій: рівень доступу — для гнучкої класифікації та QoS, рівень агрегації — для ефективного об'єднання трафіку, рівень ядра — для високошвидкісного транспорту з мінімальною затримкою.

5.3.4. Взаємодія VLAN stacking із протоколами захисту

Важливим аспектом VLAN stacking є взаємодія з протоколами захисту від петель. У мережах із множинними VLAN-тегами традиційний STP не може ефективно працювати через неможливість розрізнення різних рівнів тегування. Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) вирішує цю проблему, дозволяючи створювати

незалежні інстанції STP для різних груп VLAN. У контексті QinQ це означає, що оператор може створити окремі MSTP-інстанції для різних S-VLAN, забезпечуючи незалежне управління топологією для кожного клієнта або групи клієнтів. Альтернативно, для кільцевих топологій рекомендується використовувати ERPS (ITU-T G.8032), який забезпечує значно швидше відновлення (менше 50 мс) порівняно з MSTP та є більш передбачуваним у поведінці. Технологія PBB-TE (Provider Backbone Bridge — Traffic Engineering), стандартизована в IEEE 802.1Qay, повністю відмовляється від STP та MAC-навчання, використовуючи замість них попередньо визначені шляхи (source-routed paths). Це забезпечує детерміновану пересилку фреймів, підтримку Traffic Engineering та швидке відновлення менше 50 мс, що робить PBB-TE конкурентом MPLS як технологію транспорту операторського класу.

5.4. ETHERCHANNEL

EtherChannel (також відомий як Link Aggregation, Port Channel або LAG — Link Aggregation Group) — це технологія об'єднання кількох фізичних Ethernet-каналів у один логічний канал для збільшення агрегованої пропускної здатності та забезпечення відмовостійкості. Стандартизована в IEEE 802.1AX (раніше IEEE 802.3ad), технологія агрегації каналів дозволяє об'єднати від двох до восьми фізичних портів в один логічний порт (Port Channel). Логічний канал EtherChannel сприймається усіма протоколами верхніх рівнів — STP, маршрутизацією, VLAN-тегуванням — як єдиний інтерфейс, що значно спрощує конфігурацію та управління мережею. Технологія підтримується як між комутаторами (switch-to-switch), так і між комутатором та сервером або маршрутизатором, що забезпечує гнучкість використання у різних сценаріях.

5.4.1. Принцип роботи та балансування навантаження

Принцип роботи EtherChannel базується на розподілі трафіку між фізичними каналами, що входять до групи агрегації, з використанням алгоритмів хешування. Комутатор обчислює хеш-значення на основі обраних полів Ethernet-фрейму або IP-пакета і використовує це значення для визначення, через який фізичний канал буде надіслано фрейм. Доступні режими балансування навантаження залежать від платформи і можуть включати: балансування за MAC-адресою джерела (src-mac), за MAC-адресою призначення (dst-mac), за обома MAC-адресами (src-dst-mac), за IP-адресою джерела (src-ip), за IP-адресою призначення (dst-ip), за обома IP-адресами (src-dst-ip), а також за номерами портів TCP/UDP або комбінацією IP-адрес та портів. Вибір оптимального алгоритму хешування залежить від характеру трафіку: у мережах із множиною клієнтів, що спілкуються з одним сервером, доцільно використовувати src-ip або src-mac; у мережах з одним клієнтом та множиною серверів — dst-ip або dst-mac; у загальному випадку — src-dst-ip для найбільш рівномірного розподілу.

Важливо розуміти, що EtherChannel не забезпечує рівномірного розподілу трафіку по каналах — розподіл залежить від характеру трафіку та обраного алгоритму хешування. Кожен потік (flow), визначений хеш-функцією, завжди передається через один і той самий фізичний канал, що гарантує збереження порядку фреймів у потоці. Однак це означає, що якщо один потік генерує значно більше трафіку, ніж інші, він може перевантажити один фізичний канал, тоді як інші залишаться незавантаженими. Для оцінки ефективності балансування оператор повинен контролювати утилізацію кожного фізичного каналу в групі агрегації та за потреби змінювати алгоритм хешування або перерозподіляти трафік.

5.4.2. Протоколи агрегації: LACP та PAgP

Для узгодження параметрів агрегації між двома комутаторами використовуються два протоколи: LACP (Link Aggregation Control Protocol, IEEE 802.1AX) та PAgP (Port Aggregation Protocol, пропрієтарний протокол Cisco). LACP є стандартним протоколом, підтримуваним обладнанням більшості виробників, і є рекомендованим для використання у мультивендорних середовищах та операторських мережах. PAgP працює лише між пристроями Cisco і зберігається переважно для сумісності з існуючими мережами. Обидва протоколи виконують подібні функції: виявлення сумісних портів на протилежному кінці з'єднання, перевірку параметрів агрегації (швидкість, дуплекс, VLAN, тип порту) та автоматичне додавання або видалення портів із групи агрегації при зміні стану. LACP підтримує два режими: active (активно ініціює LACPDU) та passive (відповідає на LACPDU). PAgP підтримує режими desirable (аналог active) та auto (аналог passive). Для встановлення агрегації хоча б один із двох комутаторів повинен бути в активному режимі. Існує також статичний режим (mode on), де агрегація конфігурується без протоколу узгодження — цей режим не рекомендується через відсутність автоматичної перевірки.

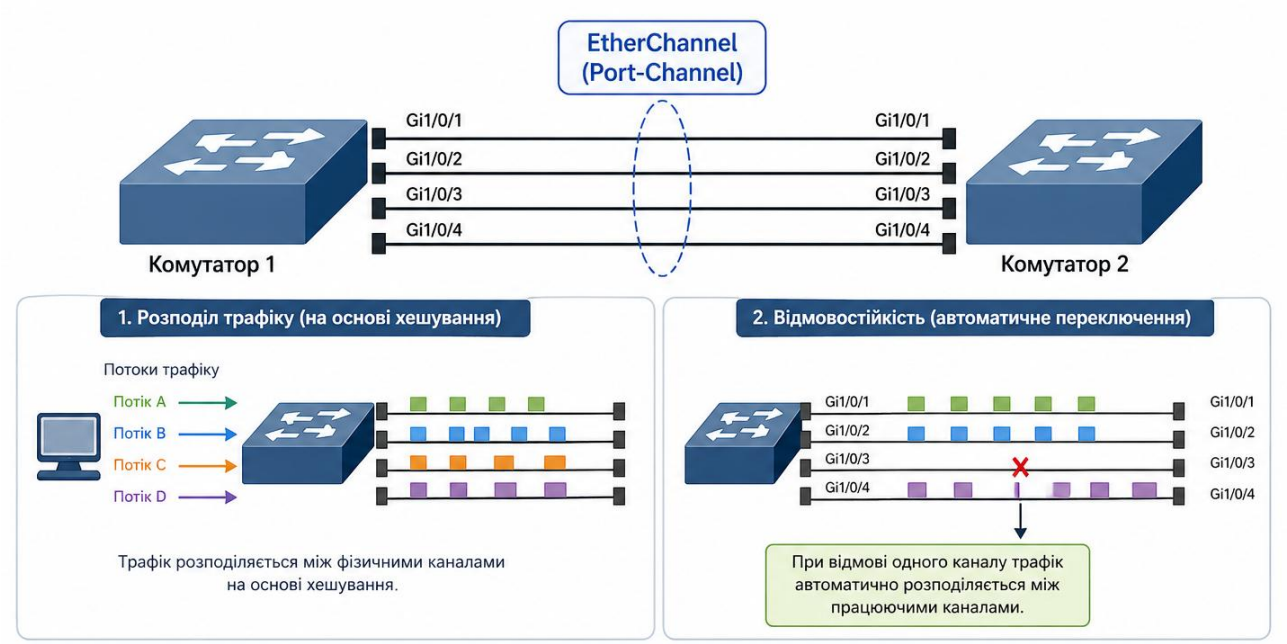

Рисунок 5.4 – EtherChannel: об'єднання фізичних каналів у логічний канал

5.4.3. Відмовостійкість та Multi-Chassis EtherChannel

Відмовостійкість є однією з ключових переваг EtherChannel. При виході з ладу одного або кількох фізичних каналів у групі агрегації трафік автоматично перерозподіляється між каналами, що залишилися працездатними, протягом кількох мілісекунд. Це відбувається значно швидше, ніж перерахунок STP, оскільки для STP логічний канал EtherChannel залишається активним, поки хоча б один фізичний канал працює. LACP додатково підтримує механізм «hot standby»: до групи агрегації можна додати до 16 портів, з яких лише 8 будуть активними, а решта — у стані очікування (standby). При виході з ладу активного порту один із standby-портів автоматично активується, забезпечуючи швидке відновлення повної пропускної здатності. Multi-Chassis EtherChannel (MCEC), реалізований у Cisco як Virtual Port Channel (vPC) або Virtual Switching System (VSS), розширює концепцію агрегації на кілька фізичних комутаторів. MCEC дозволяє підключеному пристрою (наприклад, серверу або комутатору доступу) встановити EtherChannel до двох фізичних комутаторів, які

виглядають як один логічний комутатор. Це забезпечує захист не лише від відмови каналу, а й від відмови комутатора.

Таблиця 5.2 — Порівняння EtherChannel та окремих каналів

Критерій	EtherChannel	Окремі канали
Пропускна здатність	Сума каналів (до 8×10G)	Один канал
Відмовостійкість	Автоматичне перемикання	STP (повільне)
STP	Один логічний порт	Кожен порт окремо
Балансування	Хеш (MAC/IP/Port)	Немає
Протоколи	LACP / PAgP	Не потрібні
Макс. портів	8 актив. + 8 standby	N/A

5.5. METRO ETHERNET

Metro Ethernet — це загальна назва для архітектури побудови міських (Metropolitan Area Network, MAN) та регіональних мереж на основі технології Ethernet. Концепція Metro Ethernet передбачає використання Ethernet як основного протоколу канального рівня на всіх сегментах мережі оператора — від рівня доступу клієнта до магістральних з'єднань між вузлами оператора. Історично міські мережі операторів будувалися на основі TDM-технологій (SONET/SDH) для транспортування голосового трафіку, а передавання даних здійснювалася через Frame Relay або ATM. міська мережа завжди була складним середовищем для надання послуг передачі даних, оскільки вона будувалася для задоволення жорстких вимог до надійності та доступності голосового зв'язку. Metro Ethernet фундаментально змінює цю парадигму, замінюючи складну багатошарову архітектуру єдиним Ethernet-рівнем, що суттєво спрощує управління мережею та знижує витрати. Базові концепції Carrier Ethernet, MEF-сервісів та bandwidth profile, які лежать в основі Metro Ethernet, детально розглянуто у підрозділах 2.3 та 5.1; у цьому підрозділі акцент зроблено на реалізаційних аспектах — трирівневій архітектурі, транспортних технологіях (Native Ethernet, EoS, EoMPLS) та операторських сценаріях розгортання.

5.5.1. Трирівнева архітектура Metro Ethernet

Архітектура Metro Ethernet побудована за трирівневою ієрархічною моделлю: рівень доступу (access), рівень агрегації (aggregation) та рівень ядра (core). Рівень **доступу** забезпечує підключення клієнтського обладнання (CE) до мережі оператора через інтерфейс UNI. Обладнання рівня доступу виконує класифікацію клієнтського трафіку, додавання S-VLAN тегів (QinQ), застосування bandwidth profiles та базову QoS-обробку. Типова пропускна здатність портів рівня доступу становить від 10 Мбіт/с до 10 Гбіт/с. Рівень агрегації об'єднує трафік від множини пристроїв рівня доступу та забезпечує його транспортування до рівня ядра. На цьому рівні виконуються функції агрегації EVC, міжвузлового OAM та більш складна QoS-обробка. Рівень ядра забезпечує високошвидкісний транспорт між вузлами агрегації, використовуючи

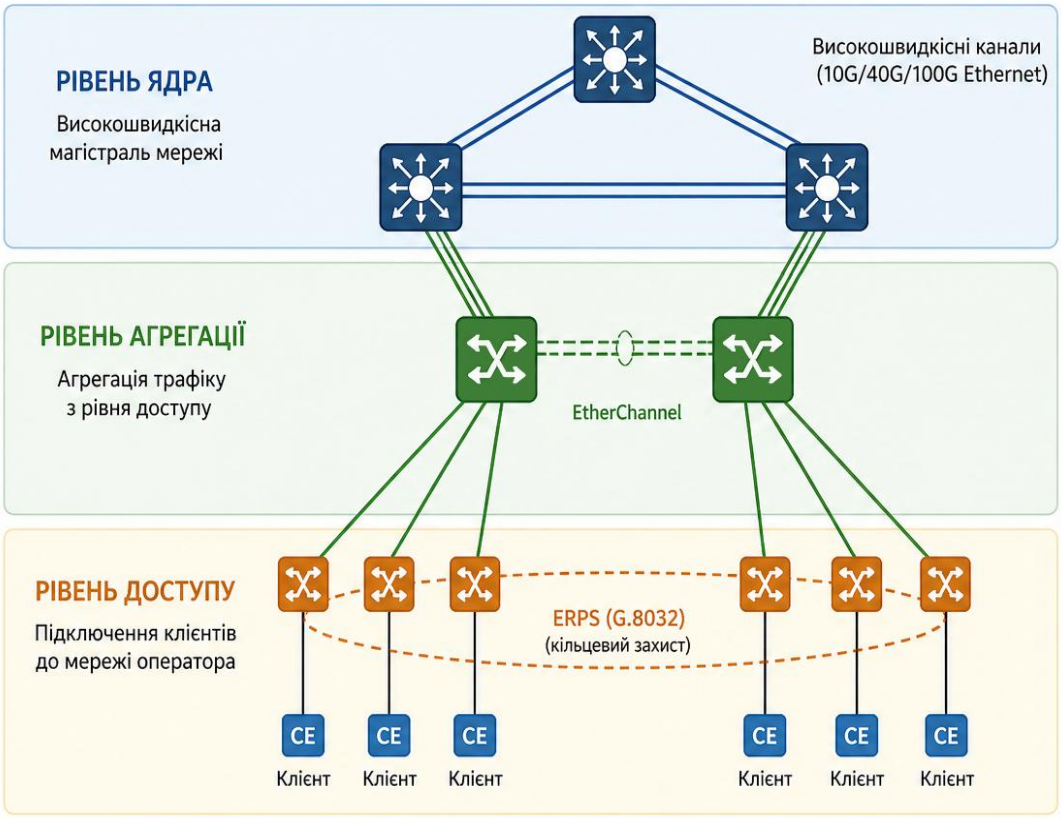

Рисунок 5.5 – Трирівнева архітектура Metro Ethernet: доступ, агрегація, ядро

5.5.2. Транспортні технології Metro Ethernet

Транспортні технології, що лежать в основі Metro Ethernet, еволюціонували від простого Ethernet-комутації до складних конвергентних рішень. Найпростішим варіантом є Native Ethernet — передавання Ethernet-фреймів безпосередньо через мережу комутаторів другого рівня з використанням VLAN для ізоляції трафіку та STP/RSTP/MSTP для захисту від петель. Ethernet over SONET/SDH (EoS) дозволяє транспортувати Ethernet-фрейми через існуючу SDH/SONET-інфраструктуру оператора. платформи MSPP, зокрема Cisco ONS 15454, інтегрують Ethernet-сервіси безпосередньо у SONET/SDH-мережу через E-Series, G-Series та ML-Series інтерфейсні карти, забезпечуючи поступовий перехід від TDM до Ethernet. G-Series карти забезпечують транспорт Ethernet «точка-точка» через SONET-канали з пропускною здатністю від STS-1 до повного Gigabit Ethernet, тоді як ML-Series карти підтримують RPR-топологію для побудови мультиточкових Ethernet-сервісів.

5.5.3. Ethernet over MPLS та інтеграція з VPN

Ethernet over MPLS (EoMPLS) є найбільш масштабованим варіантом транспорту для Metro Ethernet. MPLS забезпечує повну ізоляцію клієнтських мереж через VPN (L2VPN або L3VPN), гарантії QoS через Traffic Engineering та швидке відновлення через FRR. Технології VPWS, VPLS та EVPN на основі MPLS дозволяють реалізувати всі типи Ethernet-сервісів MEF: E-Line через VPWS (pseudowire між двома PE), E-LAN через VPLS або EVPN (multipoint-to-multipoint зв'язність), та E-Tree через відповідні розширення VPLS/EVPN. Поєднання MPLS у ядрі мережі з QinQ на рівні доступу є типовою архітектурою для великих операторських мереж, яка забезпечує масштабованість (MPLS елімінує проблему розміру MAC-таблиць), надійність (FRR менше 50 мс) та QoS (MPLS TE з DiffServ). EVPN, як найсучасніший варіант, додає

контрольоване вивчення MAC-адрес через BGP, підтримку active-active multihoming та інтеграцію L2/L3 сервісів.

5.5.4. Resilient Packet Ring (RPR) та кільцеві топології

Resilient Packet Ring (RPR, IEEE 802.17) є технологією, спеціально розробленою для кільцевих Metro Ethernet топологій, які є типовими для міських мереж завдяки існуючій топології волоконно-оптичних кабелів. RPR оптимізований для ефективного використання пропускної здатності через механізм spatial reuse: фрейми, адресовані вузлу в кільці, видаляються з кільця цим вузлом, вивільняючи пропускну здатність для інших вузлів на сегментах кільця за точкою призначення. Це є суттєвою перевагою перед SONET/SDH UPSR, де трафік проходить через все кільце навіть якщо призначення знаходиться на сусідньому вузлі. RPR також забезпечує швидке відновлення (менше 50 мс) через два механізми: wrapping (перенаправлення трафіку на зворотне кільце в точці відмови) та steering (вибір оптимального напрямку на вхідному вузлі). Як зазначається у «Building Multiservice Transport Networks», ML-Series карти Cisco ONS 15454 підтримують RPR-топологію для побудови стійких Ethernet-кілець поверх SONET-інфраструктури, використовуючи два віртуальних POS-порти на кожній ML-карті для з'єднання вузлів кільця через SONET-канали.

5.5.5. Сучасні тенденції та майбутнє Metro Ethernet

Сучасні тенденції розвитку Metro Ethernet пов'язані з кількома напрямками. Перший — стрімке зростання швидкостей: стандарти 25GbE, 50GbE, 100GbE та 400GbE забезпечують необхідну пропускну здатність для підтримки зростаючих обсягів трафіку, включаючи відеострімінг 4K/8K, хмарні обчислення та 5G-транспорт. Другий — конвергенція з програмно-визначеними мережами (SDN): контролери SDN, такі як OpenDaylight або Cisco NSO, дозволяють централізовано управляти конфігурацією Metro Ethernet, автоматизувати надання послуг через API та оптимізувати використання ресурсів мережі на основі аналітики в реальному часі. Третій — інтеграція з Segment Routing (SR): SR-MPLS та SRv6 спрощують сигналізацію та управління трафіком у Metro Ethernet мережах, замінюючи складні протоколи LDP та RSVP-TE на програмування шляхів безпосередньо у заголовках пакетів. Четвертий — перехід до Network Slicing для підтримки мереж 5G, де Metro Ethernet забезпечує транспортну інфраструктуру для fronthaul (з'єднання антени з базовою станцією), midhaul (між розподіленою та централізованою частинами базової станції) та backhaul (від базової станції до ядра мережі) сегментів.

Metro Ethernet є домінуючою архітектурою побудови міських мереж операторського класу, що базується на трирівневій ієрархічній моделі та інтегрує технології QinQ, EtherChannel, ERPS, MPLS та RPR. Еволюція від Native Ethernet через Ethernet over SONET/SDH до Ethernet over MPLS відображає зростаючі вимоги до масштабованості. Сучасні тенденції — зростання швидкостей до 400 Гбіт/с, SDN, Segment Routing та інтеграція з 5G — визначають Metro Ethernet як фундамент цифрової інфраструктури на найближчі десятиліття.

Контрольні питання

1. Назвіть п’ять ключових атрибутів Carrier Ethernet за визначенням MEF та поясніть, чому кожен з них є необхідним для мереж операторського класу.
2. Поясніть роль інтерфейсів UNI, NNI (E-NNI, I-NNI) та EVC в архітектурі Carrier Ethernet. У чому полягає різниця між Provider Edge та Customer Edge?
3. Порівняйте типи Ethernet-сервісів MEF — E-Line, E-LAN та E-Tree. Наведіть приклад типового сценарію застосування для кожного з них.
4. Опишіть відмінності між EPL та EVPL, а також між EP-LAN та EVP-LAN. У чому полягає принцип service multiplexing?
5. Як механізми OAM (IEEE 802.1ag, ITU-T Y.1731) забезпечують управління Ethernet-сервісами? Поясніть призначення MEP, MIP та повідомлень CCM, LBM/LBR, LTM/LTR.
6. Опишіть параметри bandwidth profile: CIR, CBS, EIR, EBS. Як працює алгоритм trTCM та що означають «зелений», «жовтий» і «червоний» трафік?
7. Поясніть принцип роботи механізму ERPS (G.8032). Що таке RPL (Ring Protection Link) та як забезпечується час відновлення менше 50 мс?
8. Чому використання QinQ є необхідним для масштабування мереж операторів? Скільки клієнтів та VLAN може теоретично підтримати оператор за допомогою подвійного тегування?
9. Опишіть структуру Ethernet-фрейму з подвійним тегуванням QinQ. Чому EtherType зовнішнього тегу відрізняється від внутрішнього (0x88A8 проти 0x8100)?
10. Порівняйте port-based QinQ та selective QinQ. Який варіант доцільніше використовувати для надання мультисервісних послуг через один UNI-порт?
11. У чому полягає прозорість QinQ для протоколів канального рівня клієнта? Які проблеми це може створювати та як вони вирішуються (BPDU-фільтрація, BPDU-тунелювання)?
12. Поясніть концепцію Provider Backbone Bridging (PBB, IEEE 802.1ah). Які переваги MAC-in-MAC інкапсуляції перед QinQ у великих операторських мережах?
13. Опишіть призначення ідентифікаторів B-VID та I-SID у PBB. Скільки сервісних інстанцій теоретично підтримує PBB?
14. Яким чином трирівнева архітектура (доступ, агрегація, ядро) забезпечує масштабованість мереж із VLAN stacking?
15. Поясніть принцип роботи EtherChannel та опишіть алгоритми балансування навантаження (src-mac, dst-mac, src-dst-ip тощо). Чому EtherChannel не забезпечує абсолютно рівномірного розподілу трафіку?
16. Порівняйте протоколи LACP та PAgP. У яких випадках доцільно використовувати кожен з них? Чому статичний режим (mode on) не рекомендується?
17. Що таке Multi-Chassis EtherChannel (MCEC, vPC, VSS)? Які переваги він надає порівняно зі звичайним EtherChannel між двома комутаторами?
18. Опишіть трирівневу архітектуру Metro Ethernet. Які функції виконує кожен рівень та які типові швидкості каналів використовуються?
19. Порівняйте Native Ethernet, Ethernet over SONET/SDH (EoS) та Ethernet over MPLS (EoMPLS) як транспортні технології Metro Ethernet. Які переваги забезпечує MPLS для великих операторських мереж?
20. Які технології Ethernet (тип сервісу MEF, механізм VLAN stacking, транспортна технологія) є оптимальними для трьох сценаріїв: корпоративний клієнт з трьома філіями, багатоквартирні будинки з triple-play, дата-центр з L2-розширенням між майданчиками?

РОЗДІЛ 6

ТЕХНОЛОГІЇ МЕРЕЖ ДОСТУПУ

У шостому розділі розглядаються п’ять ключових технологій мереж доступу: сімейство технологій xDSL на мідних лініях, пасивні оптичні мережі PON (з акцентом на GPON та XG-PON), мобільні мережі 4G/5G, бездротові локальні мережі стандартів Wi-Fi 6 та Wi-Fi 7, а також архітектура FTTH (Fiber to the Home). Для кожної технології детально аналізуються принципи роботи, архітектура, технічні характеристики, переваги та обмеження, а також практичні аспекти застосування у реальних мережах.

Мережі доступу є критичним компонентом сучасної телекомунікаційної інфраструктури, що формують так звану «останню милю» — ділянку між центральним вузлом оператора та кінцевим користувачем. Саме від якості та пропускної здатності цієї ділянки залежить реальна швидкість отримання послуг кожним абонентом незалежно від того, наскільки досконалою є магістральна мережа оператора. Еволюція мереж доступу від аналогових телефонних ліній до сучасних оптичних та бездротових систем відображає загальну тенденцію до зростання потреб у широкосмуговому доступі до Інтернету, хмарних сервісів, потокового відео та застосунків Індустрії 4.0.

Сучасна мережа доступу може бути реалізована на різноманітних фізичних середовищах: мідних телефонних парах, коаксіальних кабелях, волоконно-оптичних кабелях або через бездротові радіоканали. Кожне середовище передачі має свої характеристики за пропускною здатністю, дальністю дії, вартістю розгортання та обслуговування. Розуміння цих характеристик є необхідною умовою для прийняття обґрунтованих рішень при проєктуванні та експлуатації мереж доступу в контексті забезпечення кібербезпеки та захисту інформації.

6.1. ТЕХНОЛОГІЯ XDSL: ШИРОКОСМУГОВИЙ ДОСТУП ПО МІДНИХ ЛІНІЯХ

Технологія цифрової абонентської лінії (Digital Subscriber Line, DSL) є одним із найбільш поширених рішень для організації широкосмугового доступу до Інтернету в тих регіонах, де телефонна інфраструктура на мідних витих парах була розгорнута раніше, ніж відбулася масова прокладка оптичного волокна. Перевага DSL полягає у можливості використання існуючих мідних абонентських ліній — значних інвестицій, які були зроблені ще за часів аналогової телефонії — для передачі широкосмугових цифрових сигналів без необхідності прокладки нових кабелів до кожного абонента. Абревіатура xDSL позначає сімейство технологій, де буква «x» є змінною, яка замінюється відповідно до конкретного різновиду: ADSL, VDSL, HDSL, SHDSL тощо.

Фізична основа всіх технологій xDSL — той факт, що мідна витна пара, хоча й проєктувалась для передачі голосових сигналів у вузькому діапазоні від 300 до 3400 Гц, фактично здатна передавати сигнали на значно вищих частотах. Традиційна телефонна система штучно обмежувала смугу пропускання для потреб голосового зв’язку, залишаючи невикористаним весь частотний ресурс лінії вище 4 кГц. Технологія DSL використовує саме цей потенціал: сигнали DSL займають верхню частину частотного діапазону лінії, тоді як голосові сигнали ТфОП залишаються в нижній частині. Поділ між цими діапазонами здійснюється за допомогою спеціальних фільтрів — сплітерів (splitter), що встановлюються як у вузлі зв’язку, так і в приміщенні абонента.

6.1.1. ПРИНЦИП РОБОТИ DSL ТА МОДУЛЯЦІЯ DMT

Ключовим технічним рішенням, яке забезпечує високу пропускну здатність у технологіях xDSL, є метод модуляції DMT (Discrete MultiTone — дискретна багатотональна модуляція). DMT розбиває доступний частотний діапазон на велику кількість вузьких підканалів (bins), кожен з яких має ширину 4,3125 кГц. У стандарті ADSL передбачено 256 підканалів у діапазоні до 1,104 МГц. Підканали 0–7 (нижні ~32 кГц) зарезервовані для голосового сигналу та сигналізації; для передачі даних використовуються підканали 7–255, починаючи приблизно з 25,875 кГц. Кожен підканал діє як незалежна несуча, і обладнання DSL може незалежно налаштовувати кількість бітів, які передаються у кожному підканалі, залежно від якості сигналу на відповідній частоті. Якщо певні частоти зазнають сильного загасання або перешкод, відповідні підканали виключаються або використовують меншу кількість бітів на символ, тоді як підканали з гарними характеристиками можуть використовувати до 13-14 біт. Таким чином, система автоматично максимізує швидкість передачі при збереженні надійності з'єднання.

DSLAM (Digital Subscriber Line Access Multiplexer — мультиплексор доступу до цифрової абонентської лінії) є першим вузлом мережі оператора, до якого підключаються абоненти DSL. DSLAM концентрує з'єднання від множини абонентів та направляє агрегований трафік через магістральну мережу до серверів провайдера та мережі Інтернет. На відміну від кабельних модемів, які використовують спільне середовище передачі для групи абонентів, DSL є технологією типу «точка-точка»: кожен абонент має виділену лінію до DSLAM, що означає відсутність конкуренції за пропускну здатність з сусідами та забезпечує певні переваги з точки зору ізоляції трафіку.

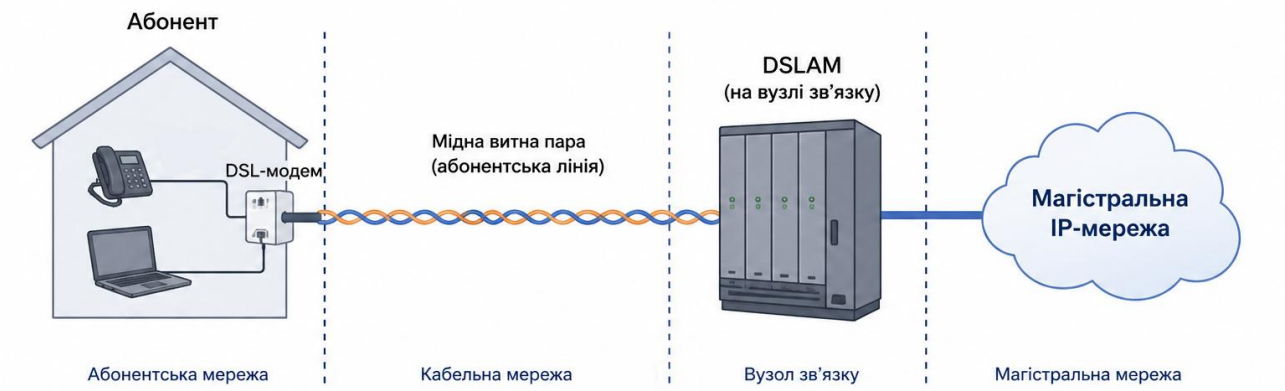

Рисунок 6.1 – Базова архітектура DSL

6.1.2. РІЗНОВИДИ ТЕХНОЛОГІЙ XDSL

Сімейство xDSL охоплює широкий спектр технологій, кожна з яких оптимізована для певного застосування. Найбільш поширеною є ADSL (Asymmetric DSL — асиметрична DSL), яка забезпечує різні швидкості передачі у прямому (від провайдера до абонента) та зворотному (від абонента до провайдера) напрямках. Асиметрія обумовлена тим, що більшість домашніх користувачів завантажують значно більше інформації, ніж відправляють. Стандарт ADSL (ITU-T G.992.1, G.DMT) забезпечує швидкість прямого потоку до 8 Мбіт/с та зворотного до 1 Мбіт/с на відстані до 5,5 км від вузла зв'язку. ADSL2+ (ITU-T G.992.5) подвоює використовувану смугу до 2,2 МГц та кількість підканалів до 512, досягаючи швидкості прямого потоку до 25 Мбіт/с.

VDSL2 (ITU-T G.993.2) є технологією наступного покоління, що досягає суттєво вищих швидкостей завдяки використанню більш широкого частотного діапазону до 30 МГц.

HDSL (High Data Rate DSL) є симетричною технологією для забезпечення сервісів T1/E1 (1,544/2,048 Мбіт/с) по двох мідних парах без регенераторів. Використовується переважно корпоративними клієнтами. SHDSL (ITU-T G.991.2) може працювати по одній парі зі швидкістю до 2,3 Мбіт/с або по двох парах до 4,72 Мбіт/с у симетричному режимі, використовуючи лінійне кодування TC-PAM для кращої спектральної сумісності.

6.1.3. ОБМЕЖЕННЯ ТА ЧИННИКИ ВПЛИВУ НА ЯКІСТЬ DSL

Найбільш суттєвим обмеженням технологій xDSL є залежність досяжної швидкості від відстані між абонентом та вузлом зв'язку. Ця залежність пояснюється фізичними властивостями мідної витої пари: загасання сигналу зростає зі збільшенням відстані та частоти. Крім відстані, на якість DSL-з'єднання впливають: діаметр провідника (менший AWG-номер означає більший діаметр і менше загасання), наявність катушок Пупіна (встановлених для покращення голосового зв'язку, але що повністю унеможливлюють роботу DSL), паралельні відгалуження (спричиняють відбиття сигналу та деградацію швидкості), перехресні завади від сусідніх пар у кабельному пучку, а також зовнішні електромагнітні перешкоди.

Перехресні завади поділяються на NEXT (Near-End Crosstalk — на ближньому кінці) та FEXT (Far-End Crosstalk — на дальньому кінці). NEXT є більш руйнівним, оскільки заважаючий сигнал не зазнає загасання вздовж лінії. Для мінімізації NEXT у стандартах DSL передбачені вимоги до спектрального маскування — обмеження потужності передачі на певних частотах. Важливим чинником є також несумісність технологій в одному кабелі: якщо у кабелі паралельно передаються сигнали T1 з кодуванням B8ZS або AMI і ADSL, ці технології можуть бути спектрально несумісними і взаємно погіршувати якість. Замість таких T1/E1-ліній рекомендується використовувати G.SHDSL, яка є спектрально-сумісною з ADSL.

Таблиця 6.1 – Порівняння технологій сімейства xDSL

Технологія	Стандарт	Макс. швидкість (прямий)	Макс. швидкість (зворот.)	Макс. відстань
ADSL	ITU-T G.992.1	8 Мбіт/с	1 Мбіт/с	~5,5 км
ADSL2+	ITU-T G.992.5	25 Мбіт/с	3,5 Мбіт/с	~5 км
VDSL2 (17a)	ITU-T G.993.2	100 Мбіт/с	100 Мбіт/с	~500 м
VDSL2 (30a)	ITU-T G.993.2	200 Мбіт/с	200 Мбіт/с	~300 м
G.fast (106 МГц)	ITU-T G.9700	До 1 Гбіт/с (дуплекс)	Динамічний	~100-250 м
HDSL	ETSI/ANSI	2,048 Мбіт/с	2,048 Мбіт/с	~3,6 км
SHDSL	ITU-T G.991.2	5,7 Мбіт/с (2 пари)	5,7 Мбіт/с	~3 км

6.1.4. ТЕХНОЛОГІЯ VECTORING (G.993.5)

Перехресні завади (crosstalk) між сусідніми витими парами в одному кабельному джгуті є основним фактором, що обмежує продуктивність VDSL2 на коротких лініях. На частотах вище 8 МГц рівень FEXT (Far-End Crosstalk) у щільному кабельному пучку може зменшувати корисну пропускну здатність на 50–70 %. Технологія Vectoring, стандартизована ITU-T у рекомендації G.993.5 (квітень 2010 р.), вирішує цю проблему шляхом активної компенсації перехресних завад на стороні DSLAM.

Принцип роботи Vectoring базується на матричних обчисленнях: DSLAM координовано опрацьовує сигнали всіх абонентських ліній одночасно, оцінює

коефіцієнти перехресних завад між парами і додає інверсний коригувальний сигнал, що нейтралізує FEXT у точці прийому. Така координація вимагає, щоб усі лінії в кабельному пучку обслуговувалися одним DSLAM з підтримкою Vectoring, тому ефект досягається лише за умови повної заміни обладнання вузла.

Застосування Vectoring на лініях VDSL2 з профілем 17a забезпечує реальне досягнення 100 Мбіт/с на відстанях до 400 м (без Vectoring — лише 50–60 Мбіт/с). Для профілю 30a Vectoring дозволяє утримувати 200 Мбіт/с до 200–250 м. Саме завдяки цій технології VDSL2 з Vectoring став основою масового розгортання FTTC (Fiber to the Cabinet), коли оптичне волокно прокладається до вуличного шафа, а останні сотні метрів до абонента використовують існуючу мідну інфраструктуру. Серед обмежень технології — необхідність повного контролю над усіма лініями в пучку (line unbundling зі сторонніми операторами ускладнює розгортання) та зростання обчислювального навантаження на DSLAM при великій кількості ліній.

6.2. ПАСИВНІ ОПТИЧНІ МЕРЕЖІ: PON, GPON ТА XG-PON

Пасивна оптична мережа (Passive Optical Network, PON) є однією з найбільш перспективних та широко розгортуваних технологій широкосмугового доступу на сьогодні. Концепція PON полягає у побудові мережі доступу на основі оптичного волокна, в якій між центральним вузлом оператора та абонентськими терміналами відсутні будь-які активні електронні елементи — всі проміжні вузлові пристрої є пасивними оптичними компонентами (спліттери, з'єднувачі, кабелі). Це кардинально спрощує обслуговування мережі та знижує витрати на її експлуатацію, оскільки пасивні елементи не потребують електроживлення, не виходять з ладу через перегрів і не вимагають активного моніторингу.

Архітектура PON складається з трьох основних елементів. Перший — OLT (Optical Line Terminal — оптичний лінійний термінал), що розміщується у центральному офісі або вузлі оператора і є серцем PON-мережі: він генерує оптичний сигнал для передачі абонентам та приймає сигнали від них, а також забезпечує підключення до магістральної мережі провайдера. Другий елемент — оптичні спліттери (optical splitters) — пасивні пристрої, що розподіляють один оптичний сигнал від OLT між кількома абонентськими волокнами. Типове значення коефіцієнта розгалуження — від 1:2 до 1:128, найчастіше 1:32 або 1:64. Третій елемент — ONT/ONU (Optical Network Terminal / Optical Network Unit), що встановлюється в приміщенні абонента та виконує перетворення оптичного сигналу в електричний.

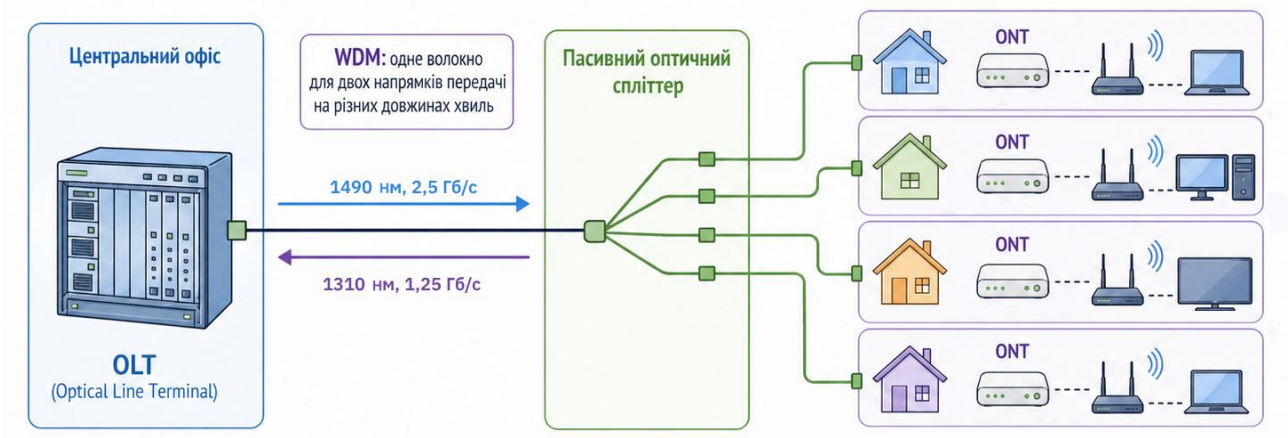

Рисунок 6.2 – Архітектура пасивної оптичної мережі PON

6.2.1. ПРИНЦИП РОБОТИ PON: МУЛЬТИПЛЕКСУВАННЯ ТА МНОЖИННИЙ ДОСТУП

Ключовою особливістю PON є те, що весь трафік між OLT та ONT передається через одне спільне волокно. Для розділення прямого (downstream) та зворотного (upstream) потоків використовується хвильове мультиплексування (WDM): прямий потік від OLT до ONT передається на довжині хвилі 1490 нм, а зворотний потік від ONT до OLT — на 1310 нм. Ці довжини хвиль поширюються по одному волокну у різних напрямках одночасно, забезпечуючи повний дуплекс при використанні єдиного волокна. Для послуг кабельного телебачення у GPON додатково зарезервована довжина хвилі 1550 нм для відеосигналу.

Оскільки від одного OLT-порту через каскад спліттерів обслуговується від кількох десятків до 128 абонентів, необхідний механізм розділення доступу до спільного середовища у зворотному напрямку. OLT призначає кожному ONT певний часовий інтервал (timeslot) для передачі — технологія TDMA (Time Division Multiple Access). Всі ONT суворо дотримуються цього розкладу, і їхні сигнали не накладаються у часі. OLT динамічно управляє розподілом пропускної здатності між ONT через механізм DBA (Dynamic Bandwidth Allocation), що дозволяє ефективно перерозподіляти ресурси залежно від поточного попиту.

Процес початкового підключення ONT включає: виявлення нових ONT (OLT надає вікна тиші для нових пристроїв), вимірювання дальності (ranging) — визначення часу затримки поширення для синхронізації часових інтервалів, та реєстрацію з призначенням логічного ідентифікатора (ONU-ID). Після реєстрації оператор може дистанційно конфігурувати ONT через протокол OMCI (ONT Management and Control Interface, G.988).

6.2.2. СТАНДАРТ GPON ТА ЕВОЛЮЦІЯ ДО XGS-PON

GPON (Gigabit Passive Optical Network, ITU-T G.984) є на сьогодні найбільш розповсюдженим стандартом PON у світі та забезпечує швидкість до 2,488 Гбіт/с у прямому напрямку та 1,244 Гбіт/с у зворотному. GPON підтримує коефіцієнт розгалуження до 1:128, а оптичний бюджет становить від 28 дБ (клас B+) до 32 дБ (клас C+), що дозволяє покривати відстані до 10-20 км залежно від конфігурації спліттерів. Протокол транспортування в GPON базується на GEM (GPON Encapsulation Method) — гнучкому контейнері для передачі трафіку різних типів: Ethernet-кадрів, TDM-потоків та інших протоколів.

XG-PON (10 Gigabit PON, ITU-T G.987) забезпечує асиметричну швидкість 10 Гбіт/с у прямому напрямку та 2,5 Гбіт/с у зворотному. XG-PON сумісний з існуючою оптичною інфраструктурою GPON: він використовує інші довжини хвиль (1577 нм для прямого та 1270 нм для зворотного потоку), тому обидва стандарти можуть співіснувати на одному волокні та в одному спліттері. Це дозволяє операторам плавно мігрувати з GPON на XG-PON без заміни кабелів і спліттерів, лише замінюючи активне обладнання. **XGS-PON** (ITU-T G.9807.1) є симетричним варіантом з 10 Гбіт/с в обох напрямках, що актуально для корпоративних застосувань. NG-PON2 (ITU-T G.989) застосовує TWDM-PON, мультиплексуючи кілька XGS-PON-каналів на різних довжинах хвиль та досягаючи загальної пропускної здатності 40-80 Гбіт/с.

6.2.3. БЕЗПЕКА В МЕРЕЖАХ PON

З точки зору кібербезпеки, архітектура PON має специфічні особливості. У прямому напрямку OLT транслює широкомовний сигнал, який фізично отримують усі ONT у дереві, тому кожен ONT може прийняти трафік, адресований іншому абоненту. Для запобігання несанкціонованому перехопленню стандарт GPON передбачає

шифрування прямого потоку (AES-128 у режимі CTR). Зворотний напрямок за своєю природою менш вразливий, оскільки кожний ONT передає лише у свій часовий слот.

Проте загрозою є «шахрайський ONT» (rogue ONT) — пристрій, що навмисно порушує протокол TDMA і передає поза своїм часовим вікном, блокуючи зв'язок для інших абонентів. Операторам рекомендується використовувати автентифікацію ONT за серійним номером та PLOAM-паролем, а також централізоване управління конфігурацією через OMCI для моніторингу всіх ONT у мережі.

Таблиця 6.2 – Порівняння стандартів PON

Стандарт	Орган	Швидкість (пряма)	Швидкість (зворотна)	Макс. ONT
BPON	ITU-T G.983	622 Мбіт/с	155 Мбіт/с	32
GPON	ITU-T G.984	2,5 Гбіт/с	1,25 Гбіт/с	128
EPON	IEEE 802.3ah	1 Гбіт/с	1 Гбіт/с	16-32
10G-EPON	IEEE 802.3av	10 Гбіт/с	10 Гбіт/с	16-32
XG-PON	ITU-T G.987	10 Гбіт/с	2,5 Гбіт/с	64
XGS-PON	ITU-T G.9807	10 Гбіт/с	10 Гбіт/с	64
NG-PON2	ITU-T G.989	40 Гбіт/с	40 Гбіт/с	256

6.3. МОБІЛЬНІ МЕРЕЖІ 4G/LTE ТА 5G NR

Мобільні мережі доступу пройшли значний еволюційний шлях від аналогових систем першого покоління (1G) до сучасних мереж 5G. Технологія 4G (LTE — Long Term Evolution та LTE-Advanced/Pro) запровадила повністю IP-орієнтовану архітектуру мобільного зв'язку та забезпечила пропускну здатність, достатню для потокового відео, мобільного Інтернету та відеоконференцій. Технологія 5G (New Radio, NR) виводить можливості мобільних мереж на принципово новий рівень, орієнтуючись не лише на мобільний широкосмуговий доступ, але й на підтримку масового Інтернету речей та критично важливих застосунків з ультра-низькою затримкою.

6.3.1. АРХІТЕКТУРА LTE: E-UTRAN ТА EPC

Мережа LTE складається з двох основних підсистем: радіодоступу (E-UTRAN) та ядра мережі (Evolved Packet Core, EPC). E-UTRAN складається виключно з базових станцій eNB (evolved NodeB), які на відміну від попередніх поколінь взаємодіють між собою через інтерфейс X2, що знижує затримку хендовера та спрощує архітектуру. Ядро мережі EPC включає: MME (Mobility Management Entity) — управління мобільністю та автентифікацією; SGW (Serving Gateway) — маршрутизація трафіку під час хендовера; PGW (Packet Data Network Gateway) — підключення до зовнішніх мереж та застосування QoS-політик; HSS (Home Subscriber Server) — сховище профілів абонентів.

На фізичному рівні LTE використовує OFDMA (Orthogonal Frequency Division Multiple Access) у прямому та SC-FDMA у зворотному напрямку. Доступна смуга частот розбивається на ресурсні блоки (Resource Blocks, RB) по 12 підносійних кожен, що динамічно призначаються різним користувачам у кожному підкадрі (1 мс). Смуга каналу в LTE може становити від 1,4 до 20 МГц, максимальна теоретична швидкість при 20 МГц та MIMO 4x4 досягає 300 Мбіт/с. LTE-Advanced (Release 10) підвищив можливості за рахунок carrier aggregation (до 5 несучих, ефективна смуга до 100 МГц) та масивного MIMO.

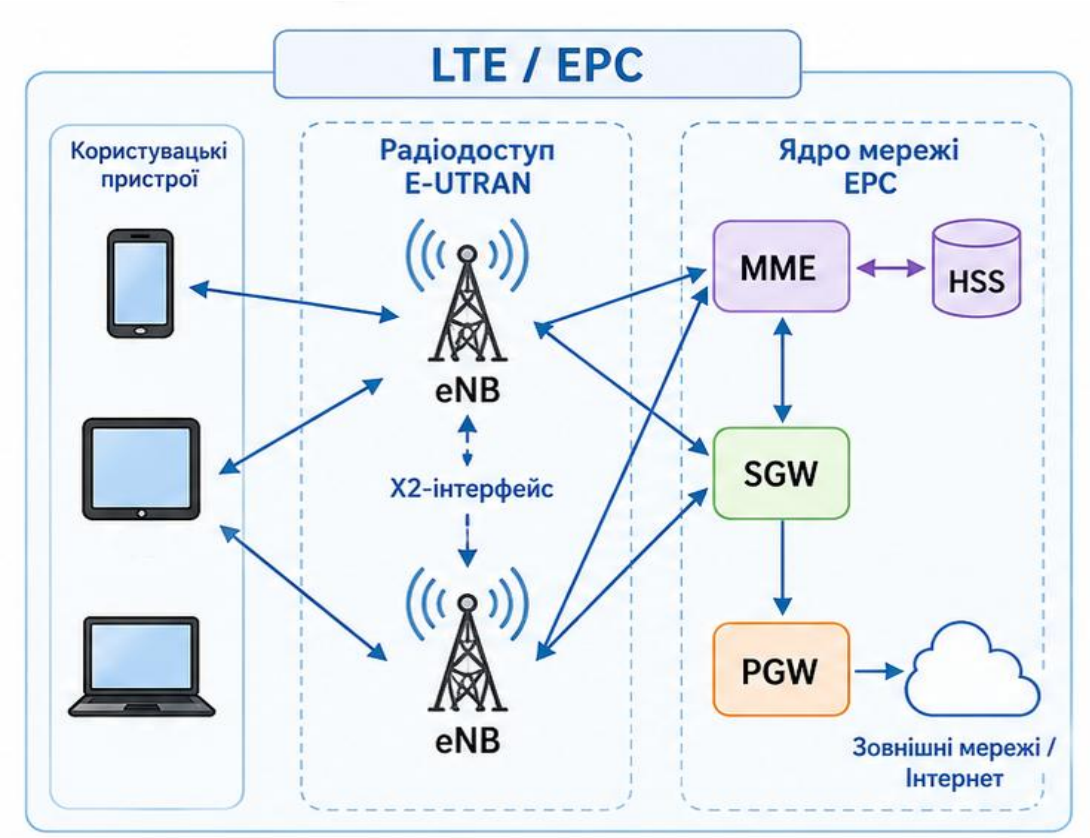

Рисунок 6.3 – Архітектура мережі LTE

6.3.2. ТЕХНОЛОГІЯ 5G NR: НОВА РАДІОІНТЕРФЕЙС ТА АРХІТЕКТУРА ЯДРА

5G NR (3GPP Release 15+) визначає два основних діапазони частот: FR1 (до 7,125 ГГц, Sub-6 GHz) та FR2 (24,25-52,6 ГГц, mmWave — міліметрові хвилі). Міліметрові хвилі забезпечують надзвичайно широкі смуги (до сотень МГц), але мають обмежену дальність та гіршу проникність, тоді як Sub-6 GHz забезпечує ширше покриття. На рівні радіоінтерфейсу 5G NR зберігає OFDM, але вводить гнучкий крок підносійних (SCS): 15, 30, 60, 120 або 240 кГц, що дозволяє знизити затримку (більший SCS — коротший символ — менша затримка). Смуга каналу може сягати 100 МГц у FR1 та 400 МГц у FR2.

Архітектура ядра мережі 5G (5GC, Service Based Architecture, SBA) базується на мікросервісному підході: кожна мережева функція (NF) реалізується як незалежний сервіс з відкритим API. Ключові NF: AMF (Access and Mobility Management Function — аналог MME), SMF (Session Management Function), UPF (User Plane Function — обробка трафіку), PCF (Policy Control Function), AUSF (Authentication Server Function), UDM (Unified Data Management). Протокол SEPP (Security Edge Protection Proxy) захищає міжоператорські з’єднання при роумінгу.

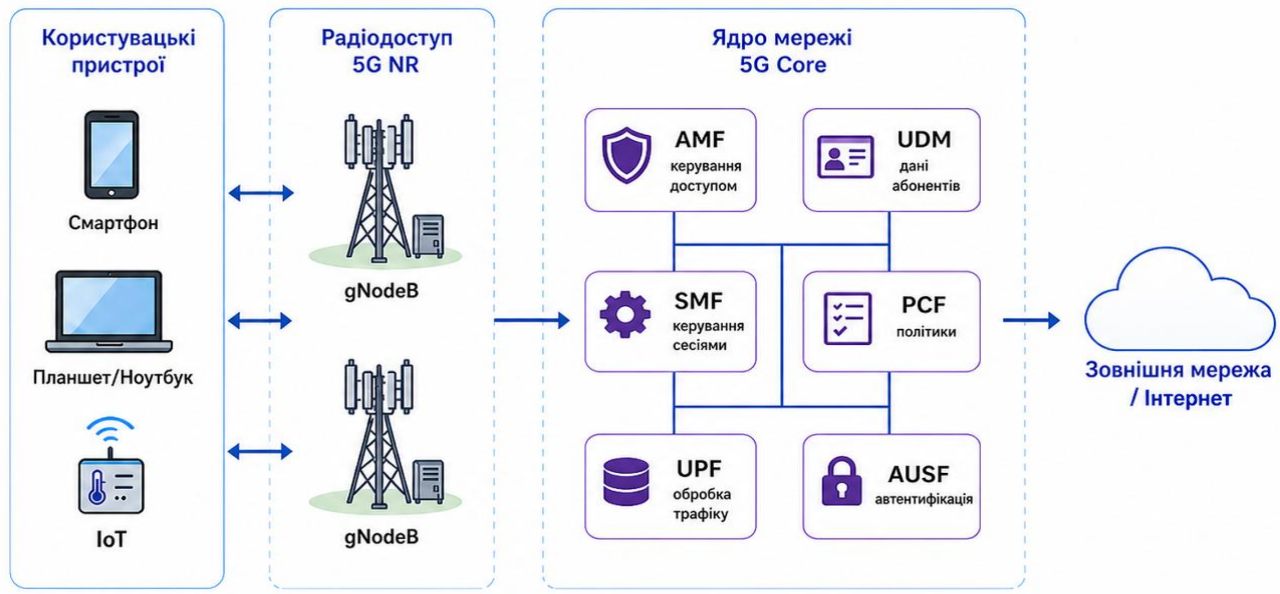

Рисунок 6.4 – Архітектура мережі 5G Core

6.3.3. КЛЮЧОВІ СЦЕНАРІЇ 5G ТА НАРІЗКА МЕРЕЖІ

Стандарт 5G визначає три основних класи застосувань. eMBB (enhanced Mobile Broadband) — максимальна пропускна здатність для споживачів: потокове відео 4K/8K, AR/VR. Максимальна теоретична швидкість до 20 Гбіт/с у прямому напрямку. **URLLC** (Ultra-Reliable Low Latency Communication) — для критично важливих застосунків: дистанційне медичне керування, автономне транспортування, промислова автоматизація. Вимоги: затримка менше 1 мс та надійність 99,9999%. mMTC (massive Machine Type Communication) — для IoT: підключення до 1 мільйона пристроїв на км2 з мінімальним енергоспоживанням.

Нарізка мережі (Network Slicing) — технологія, що дозволяє створювати кілька логічно ізольованих зрізів мережі поверх спільної фізичної інфраструктури, кожен з яких налаштований під конкретний клас послуг. З точки зору кібербезпеки, нарізка мережі є ефективним засобом ізоляції різних типів трафіку: зріз для URLLC-критичних застосувань відділено від зрізу для загального Інтернет-доступу, що мінімізує взаємний вплив та зменшує поверхню атаки. Управління зрізами здійснюється через NSSF (Network Slice Selection Function). Масивна MIMO (десятки-сотні антенних елементів) та 3D Beamforming дозволяють точно направляти радіосигнал до конкретного пристрою, підвищуючи спектральну ефективність.

6.3.4. БЕЗПЕКА МЕРЕЖ 4G ТА 5G

В LTE базовими механізмами безпеки є автентифікація за протоколом AKA (Authentication and Key Agreement) з використанням USIM-картки, **шифрування радіоінтерфейсу** (SNOW 3G, AES, ZUC) та захист цілісності сигнальних повідомлень. Відомою вразливістю LTE є можливість IMSI-catching (перехоплення ідентифікатора абонента у відкритому вигляді при початковому підключенні) за допомогою IMSI-catcher пристроїв. 5G усуває цю вразливість шляхом SUCI (Subscription Concealed Identifier) — зашифрованої версії ідентифікатора абонента, що передається замість відкритого IMSI. Шифрування виконується публічним ключем оператора, відомим лише SIM-картці та мережі.

Таблиця 6.3 – Порівняння характеристик LTE та 5G NR

Параметр	LTE (Release 8)	LTE-Advanced Pro	5G NR (Release 15+)
Макс. швидкість (DL)	150 Мбіт/с	1 Гбіт/с	20 Гбіт/с
Макс. швидкість (UL)	50 Мбіт/с	500 Мбіт/с	10 Гбіт/с
Затримка (повітр. інт.)	~10 мс	~5 мс	<1 мс (URLLC)
Смуга каналу	До 20 МГц	До 100 МГц	До 400 МГц (FR2)
Антенні системи	MIMO 4x4	MIMO 8x8	Масивна MIMO 64x64+
Нарізка мережі	Немає	Обмежена	Повноцінна (eMBB/URLLC/mMTC)
Архітектура ядра	EPC (монолітна)	EPC + NFV	5GC (SBA, мікросервіси)

6.4. БЕЗДРОТОВИЙ ДОСТУП WI-FI 6 ТА WI-FI 7: IEEE 802.11AX ТА IEEE 802.11BE

Технологія Wi-Fi є безперечним лідером серед бездротових технологій локального доступу. Стандарт Wi-Fi 6 (IEEE 802.11ax), прийнятий у 2019 році, ознаменував перехід від фокусу на максимальній пропускній здатності до ефективної роботи в середовищах з великою щільністю пристроїв. Wi-Fi 7 (IEEE 802.11be, активне розгортання з 2024-2025 рр.) піднімає продуктивність до рівня, що конкурує з провідними мережами Ethernet для кінцевих користувачів.

6.4.1. WI-FI 6 (IEEE 802.11AX): OFDMA, MU-MIMO ТА TWT

Wi-Fi 6 (IEEE 802.11ax) працює у діапазонах 2,4 та 5 ГГц (Wi-Fi 6E додає 6 ГГц). Максимальна теоретична пропускна здатність становить 9,6 Гбіт/с при 8 просторових потоках та 1024-QAM. Однак ключові інновації стосуються ефективності в щільних середовищах. Головною інновацією є OFDMA, що вперше з'явилась у стандартах Wi-Fi. OFDMA дозволяє точці доступу (AP) розподіляти доступні підносійні між кількома клієнтами одночасно через «ресурсні одиниці» (Resource Units, RU), замість того щоб кожен клієнт по черзі використовував весь канал. Це підвищує ефективність в сценаріях з багатьма клієнтами та невеликими пакетами даних (IoT, офіси).

MU-MIMO у Wi-Fi 6 розширено до 8 одночасних клієнтів у прямому напрямку та вперше введено MU-MIMO у зворотному (UL MU-MIMO, до 8 клієнтів). Механізм TWT (Target Wake Time) дозволяє AP та клієнту заздалегідь узгодити момент обміну даними, між якими пристрій перебуває у глибокому сні, продовжуючи час роботи IoT-пристроїв у десятки разів. BSS Coloring присвоює числовий ідентифікатор кожній зоні обслуговування (BSS), вбудований у заголовок кожного пакета, що дозволяє пристроям розрізняти власний та чужий трафік та підвищує просторове повторне використання частот.

6.4.2. WI-FI 7 (IEEE 802.11BE): MULTI-LINK OPERATION

Wi-Fi 7 (IEEE 802.11be, EHT — Extremely High Throughput) забезпечує теоретичну пропускну здатність до 46,1 Гбіт/с. Wi-Fi 7 охоплює всі три частотних діапазони та вводить ширину каналу 320 МГц у діапазоні 6 ГГц. Модуляція 4096-QAM (проти 1024-QAM у Wi-Fi 6) підвищує спектральну ефективність на 20%, кількість просторових потоків збільшена до 16.

Найбільш революційною функцією Wi-Fi 7 є MLO (Multi-Link Operation). MLO дозволяє пристрою одночасно використовувати кілька радіоканалів на різних частотних діапазонах (2,4 + 5 + 6 ГГц) як єдине агреговане з'єднання. Це кардинально

відрізняється від Wi-Fi попередніх поколінь, де пристрій використовував лише один діапазон одночасно. MLO дозволяє: підвищити пропускну здатність шляхом агрегації; знизити затримку та підвищити надійність (при завадах в одному каналі трафік перемикається на інший без перерви з'єднання); збалансувати навантаження між діапазонами. Preamble Puncturing дозволяє виключити зайняті частини широкого каналу та використовувати решту, замість відмови від усього каналу при будь-яких завадах.

6.4.3. БЕЗПЕКА WI-FI: WPA3 ТА ENTERPRISE

Протокол WPA2 з шифруванням AES-CCMP має відому вразливість KRACK (Key Reinstallation Attack, 2017). WPA3, введений у 2018 році, усуває її за допомогою протоколу SAE (Simultaneous Authentication of Equals, Dragonfly) замість PSK для особистих мереж. SAE забезпечує Forward Secrecy: компрометація пароля не дозволяє розшифрувати раніше перехоплений трафік. WPA3-Enterprise мандатує криптографічні алгоритми рівня 192 бітів для корпоративних мереж. Автентифікація через 802.1X та RADIUS з EAP-TLS/PEAP є рекомендованою практикою для корпоративних Wi-Fi. Для захисту від Rogue AP та MITM-атак застосовуються WIDS та Management Frame Protection (MFP, IEEE 802.11w).

Таблиця 6.4 – Порівняння стандартів Wi-Fi

Покоління	Стандарт	Діапазон	Макс. ширина каналу	Макс. швидкість	Ключові технології
Wi-Fi 4	802.11n	2,4 / 5 ГГц	40 МГц	600 Мбіт/с	MIMO, OFDM
Wi-Fi 5	802.11ac	5 ГГц	160 МГц	3,5 Гбіт/с	MU-MIMO DL
Wi-Fi 6	802.11ax	2,4 / 5 ГГц	160 МГц	9,6 Гбіт/с	OFDMA, MU-MIMO UL+DL, TWT
Wi-Fi 6E	802.11ax	2,4 / 5 / 6 ГГц	160 МГц	9,6 Гбіт/с	+Діапазон 6 ГГц
Wi-Fi 7	802.11be	2,4 / 5 / 6 ГГц	320 МГц	46,1 Гбіт/с	MLO, 4096-QAM, 16 потоків

6.5. АРХІТЕКТУРА FTTH: ОПТИЧНЕ ВОЛОКНО ДО БУДИНКУ

FTTH (Fiber to the Home) є вершиною еволюції технологій широкосмугового доступу. На відміну від технологій, що використовують оптичне волокно лише на магістральній ділянці, а для «останньої милі» покладаються на мідь або радіоканал, FTTH доводить оптоволокно безпосередньо до приміщення кожного абонента. Це забезпечує практично необмежену пропускну здатність, виняткову надійність та симетричні швидкості передачі. У сучасному розумінні FTTH реалізується переважно на основі PON, хоча можливі і топології «точка-точка» (P2P Ethernet over Fiber).

6.5.1. ВАРІАНТИ АРХІТЕКТУР FTTX

Абревіатура FTTx узагальнює всі варіанти оптичного доступу, де «x» вказує на точку закінчення волокна. FTTN (Fiber to the Node) доводить волокно до вуличного шафу в межах 1-2 км від абонента, а остання ділянка — мідна пара з VDSL2. FTTC (Fiber to the Curb) розміщує вузол ще ближче (300-500 м), дозволяючи використовувати вищошвидкісні профілі VDSL2 або G.fast. FTTB (Fiber to the Building) доводить волокно до підвального технічного приміщення, від якого розподіл відбувається мідною парою VDSL2/G.fast або внутрішньобудинковою Ethernet-мережею — економічне рішення для багатоквартирних будинків. FTTH та FTTP

доводять волокно безпосередньо до кожного приміщення, забезпечуючи максимальну пропускну здатність без жодних обмежень мідної ділянки.

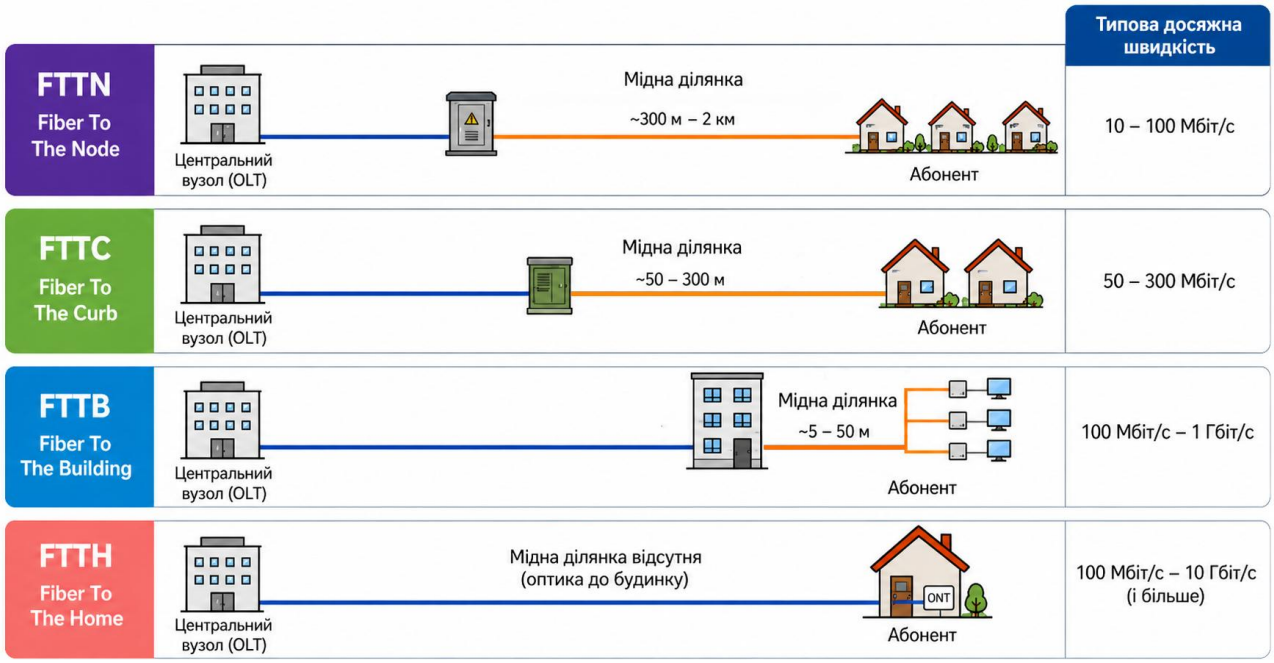

Рисунок 6.5 – Порівняння архітектур FTTx

6.5.2. КОМПОНЕНТИ FTTH-МЕРЕЖІ ТА ОПТИЧНА РОЗПОДІЛЬНА МЕРЕЖА (ODN)

Типова FTTH-мережа на основі GPON складається з кількох рівнів. Магістральний рівень (feeder level) — оптичний кабель від центрального офісу (CO) до первинних розподільних точок. Розподільний рівень (distribution level) — оптичний кабель та перші рівні спліттерів, що охоплюють певні квартали. Абонентський рівень (drop level) — індивідуальні дроп-кабелі від точок розподілу до кожного абонента. Термінальний рівень — ONT у приміщенні.

Оптична розподільна мережа (ODN, Optical Distribution Network) — сукупність всіх пасивних оптичних компонентів між OLT та ONT: кабелі, спліттери, з'єднувачі, зварні з'єднання, розподільні шафи. Проєктування ODN вимагає урахування оптичного бюджету (загальне загасання не має перевищувати допустиме значення), типу спліттерів (PLC-спліттери рекомендовані для великих коефіцієнтів розгалуження через рівномірність розподілу), типу роз'ємів (SC/APC рекомендований для FTTH через кращі характеристики зворотного відбиття). Загасання PLC-спліттера: ~4 дБ для 1:2, ~8 дБ для 1:4, ~11 дБ для 1:8, ~14 дБ для 1:16, ~17 дБ для 1:32, ~20 дБ для 1:64.

6.5.3. ONT ТА УПРАВЛІННЯ СЕРВІСАМИ ЧЕРЕЗ OMCI

ONT є пристроєм, що встановлюється в приміщенні абонента та виконує роль шлюзу між PON-мережею оператора та мережею кінцевого користувача. Сучасні ONT інтегрують: оптичний приймач/передавач для PON; Ethernet-порти (2-4 порти GE або 1-2 порти 2,5GE/10GE); Wi-Fi точку доступу (у багатьох моделях — Wi-Fi 6); телефонні FXS-порти для аналогових телефонів; CATV RF-порт для коаксіального підключення. Управління ONT здійснюється оператором через протокол OMCI (G.988), який дозволяє автоматично конфігурувати сервіси, оновлювати прошивку, моніторити

6.5.4. FTTH ТА БЕЗПЕКА ОПТИЧНОГО ДОСТУПУ

FTTH-мережі мають певні переваги з точки зору безпеки: оптичне волокно не випромінює електромагнітних сигналів, придатних для пасивного перехоплення без фізичного доступу до волокна. Проте це не знімає загроз на рівні протоколів: ONT та OLT є складними обчислювальними пристроями з потенційними вразливостями в програмному забезпеченні. Важливим аспектом є шифрування AES прямого потоку GPON, захист управляючого каналу OMCI від несанкціонованого доступу, а також автентифікація ONT для запобігання підключенню несанкціонованих пристроїв. Фізичний захист точок розгалуження (спліттерів) та дроп-кабелів також є важливою складовою безпеки FTTH-інфраструктури.

Таблиця 6.5 – Порівняння технологій широкосмугового доступу

Параметр	xDSL (VDSL2)	GPON / XGS-PON	5G NR (Sub-6)	Wi-Fi 6/7
Середовище	Мідна пара	Одномодове волокно	Радіо (ліцензоване)	Радіо (неліцензоване)
Макс. швидкість	200 Мбіт/с	2,5 / 10 Гбіт/с	До 3 Гбіт/с	9,6 / 46,1 Гбіт/с (теор.)
Симетричність	Переважно асимет.	Симет. / Асимет.	Асиметрична	Залежить від конфігурації
Макс. відстань	До 5 км (ADSL)	До 20-60 км	~0,1-1 км	До 300 м (у приміщенні)
Затримка	5-15 мс	1-5 мс	5-30 мс	1-10 мс
Мобільність	Немає	Немає	Повна	Обмежена (зона AP)
Вартість розгортання	Низька	Середня-висока	Середня	Низька (Enterprise — середня)
Залежність від відстані	Висока	Низька	Середня	Висока
Безпека перехоплення	Вразлива фізично	Стійка (без фіз. доступу)	Потребує шифрування	Вразлива (WPA2)/Стійка (WPA3)

Контрольні питання

1. Поясніть принцип роботи xDSL: як використовується частотний спектр мідної телефонної лінії?
2. Що таке модуляція DMT і яка її ключова перевага порівняно з традиційною модуляцією одного носія?
3. Порівняйте технології ADSL2+, VDSL2 та G.fast за швидкістю, дальністю та симетрією.
4. Що таке Vectoring у VDSL2 і чому ця технологія критично важлива для масового розгортання FTTC?
5. Поясніть архітектуру PON: яку роль виконують OLT, ONT та оптичний сплітер?
6. Як у PON реалізовано множинний доступ кількох ONT до одного волокна upstream?
7. Що таке процедура ranging у GPON і чому вона необхідна?
8. Порівняйте GPON, XG-PON та XGS-PON за швидкостями та довжинами хвиль. Чому XGS-PON важлива?
9. Опишіть механізми безпеки в мережах PON: шифрування, автентифікація ONT, оптичне підслуховування.
10. Поясніть архітектуру LTE: функції E-UTRAN та елементів EPC (MME, SGW, PGW, HSS, PCRF).
11. Що таке OFDMA та SC-FDMA у LTE? Чому використовуються різні схеми для downstream та upstream?
12. Опишіть нову архітектуру 5G Core (5GC). У чому відмінність сервіс-орієнтованої архітектури від EPC?
13. Назвіть три основні сценарії 5G (eMBB, URLLC, mMTC) та їх вимоги до мережі.
14. Що таке нарізка мережі (Network Slicing) у 5G? Які бізнес-можливості вона відкриває?
15. Як забезпечується безпека в LTE та 5G? Чим SUCI відрізняється від IMSI та яку проблему вирішує?
16. Поясніть принцип OFDMA у Wi-Fi 6 та його вплив на щільні мережі з багатьма клієнтами.
17. Що таке MU-MIMO у Wi-Fi 6 та яка різниця між downlink та uplink MU-MIMO?
18. Опишіть функцію Target Wake Time (TWT) та її роль в енергоефективності IoT-пристроїв.
19. Поясніть Multi-Link Operation (MLO) у Wi-Fi 7. Які переваги дає одночасне використання кількох діапазонів?
20. Що таке протокол SAE у WPA3 і чому він стійкіший за 4-етапний handshake WPA2?

РОЗДІЛ 7

BGP ТА VPN

У цьому розділі детально розглядаються архітектура BGP та принципи його роботи, відмінності між eBGP та iBGP, механізми масштабування через Route Reflectors, інструменти маршрутної політики, а також застосування BGP у побудові L2VPN, L3VPN та сучасної технології EVPN.

Протокол BGP (Border Gateway Protocol — протокол граничного шлюзу) є фундаментальним протоколом міждоменної маршрутизації, який забезпечує зв'язність між тисячами автономних систем глобальної мережі Інтернет. BGP є єдиним протоколом маршрутизації, що використовується між різними організаціями та операторами зв'язку, і відповідає за те, як інформація про IP-мережі досягає будь-якої точки планети. Без BGP сучасний Інтернет у своєму теперішньому вигляді був би неможливим.

Водночас BGP відіграє критичну роль не лише в міждоменній маршрутизації, але й у побудові віртуальних приватних мереж (VPN) операторського класу. Розширення MP-BGP (Multiprotocol BGP, RFC 4760) перетворило BGP на універсальний механізм обміну інформацією для MPLS L3VPN, L2VPN, EVPN та інших сервісів. Саме завдяки цим розширенням BGP став «клеєм», що з'єднує різні технології передачі даних в єдину операторську інфраструктуру.

Ключова ідея

BGP — це не просто протокол маршрутизації, а й потужний механізм реалізації бізнес-відносин між операторами. Кожне рішення BGP про вибір маршруту може відображати комерційну угоду між двома автономними системами.

7.1. АРХІТЕКТУРА BGP

BGP (Border Gateway Protocol) — це протокол маршрутизації типу path-vector, стандартизований в RFC 4271 (BGP-4), який забезпечує обмін інформацією про мережеву досяжність (Network Layer Reachability Information, NLRI) між автономними системами. Поточна версія BGP-4, що є єдиним стандартизованим протоколом зовнішньої маршрутизації (EGP — Exterior Gateway Protocol), використовується у всіх великих мережах операторського класу. BGP-сесії встановлюються поверх надійного транспорту TCP (порт 179), що звільняє протокол від необхідності самостійно вирішувати проблеми надійності передачі.

7.1.1. BGP як протокол path-vector

BGP належить до класу протоколів маршрутизації типу path-vector (вектор шляху), що є еволюцією протоколів типу distance-vector. На відміну від distance-vector (як RIP), де маршрутизатор знає лише відстань до мережі призначення та наступний вузол, BGP передає разом із маршрутом повний шлях у вигляді послідовності номерів автономних систем (AS-PATH). Це дозволяє кожному маршрутизатору перевіряти, чи не проходить маршрут через його власну AS, і таким чином виявляти та запобігати маршрутним петлям.

BGP суттєво відрізняється від протоколів внутрішньої маршрутизації (IGP — Interior Gateway Protocols), таких як OSPF та IS-IS, за кількома ключовими аспектами. По-перше, IGP оптимізовані для швидкої збіжності всередині однієї організації, тоді як

BGP оптимізований для стабільності та контрольованого розповсюдження маршрутів між тисячами організацій. По-друге, IGP використовують метрику (вартість) для вибору найкоротшого шляху, тоді як BGP використовує набір атрибутів та маршрутну політику для реалізації бізнес-рішень. По-третє, таблиця BGP в маршрутизаторах великих операторів містить понад 950 000 IPv4-префіксів і понад 180 000 IPv6-префіксів (за даними CIDR Report станом на 2024–2025 рр.).

Масштаб BGP

Станом на 2024 рік глобальна таблиця BGP містить понад 950 000 IPv4-маршрутів та понад 180 000 IPv6-маршрутів. Загальна кількість автономних систем у світі перевищує 100 000. Зростання таблиці BGP є постійним викликом для операторів мережевого обладнання.

7.1.2. Повідомлення та стани BGP

Протокол BGP визначає чотири типи повідомлень, що передаються через TCP-з'єднання між BGP-сусідами (peers). Кожне повідомлення має стандартний заголовок із маркером (19 байтів: 16 байтів маркера, 2 байти довжини, 1 байт типу).

OPEN — надсилається після встановлення TCP-з'єднання для ініціалізації BGP-сесії. Містить: версію BGP (4), номер AS відправника (ASN), Hold Time (час очікування Keepalive), BGP Router ID (32-бітний ідентифікатор), а також список опціональних параметрів (capabilities), серед яких — підтримка 4-байтових ASN (RFC 6793) та підтримка адресних сімейств MP-BGP.

UPDATE — несе основну інформацію про маршрути: список NLRI (префікси, що рекламуються), атрибути шляху для цих NLRI, а також список withdrawn routes (префікси, що більше не є досяжними). Одне повідомлення UPDATE може містити лише маршрути з однаковим набором атрибутів.

KEEPALIVE — надсилається кожні Hold Time / 3 секунди (зазвичай кожні 60 секунд) для підтвердження активності сесії. Якщо сусід не отримує Keepalive протягом Hold Time (зазвичай 180 секунд), сесія вважається відмовившою та скидається.

NOTIFICATION — надсилається при виявленні помилки (наприклад, некоректне значення атрибуту, невідповідний Hold Time, помилка FSM). Після відправки Notification TCP-з'єднання закривається. Містить код та підкод помилки для діагностики.

Процес встановлення BGP-сесії проходить через кілька станів кінцевого автомата (Finite State Machine, FSM): Idle (початковий стан, очікування адміністративного старту) → Connect (TCP-з'єднання ініційовано) → Active (TCP-з'єднання не вдалось, новий спроба) → OpenSent (OPEN надіслано, очікується OPEN від сусіда) → OpenConfirm (OPEN отримано, надіслано KEEPALIVE, очікується KEEPALIVE) → Established (сесія встановлена, обмін UPDATE можливий). Стан Established є робочим станом, в якому відбувається обмін маршрутною інформацією.

7.1.3. Атрибути BGP-маршрутів

Кожен BGP-маршрут, що рекламується в повідомленні UPDATE, супроводжується набором атрибутів (Path Attributes), які визначають характеристики маршруту та використовуються для вибору найкращого шляху. Атрибути класифікуються за двома осями: обов'язкові (Well-Known) або необов'язкові (Optional), транзитивні (Transitive, передаються далі) або нетранзитивні (Non-transitive, зупиняються на отримувачі).

Основні атрибути BGP та їх призначення:

- **ORIGIN** (Well-Known Mandatory) — вказує джерело маршруту: IGP (i, маршрут отримано через IGP), EGP (e, застарілий), Incomplete (?, маршрут отримано з перерозподілу). Маршрути з нижчим значенням ORIGIN мають перевагу при виборі найкращого шляху.
- **AS_PATH** (Well-Known Mandatory) — список номерів AS, через які пройшов маршрут. Є основним механізмом запобігання петлям (маршрутизатор відкидає маршрут, якщо бачить свій ASN в AS_PATH). Також використовується для Traffic Engineering через AS-PATH prepending.
- **NEXT_HOP** (Well-Known Mandatory) — IP-адреса наступного вузла, через який треба відправити пакет. Для eBGP NEXT_HOP встановлюється на IP-адресу відправника. Для iBGP NEXT_HOP не змінюється (передається "as-is" від eBGP-сусіда), тому всі iBGP-маршрутизатори повинні мати маршрут до NEXT_HOP через IGP.
- **LOCAL_PREFERENCE** (Well-Known Discretionary) — числове значення (за замовчуванням 100), що використовується всередині AS для визначення переважного виходу трафіку. Маршрут з вищим значенням LOCAL_PREF має пріоритет. Не передається через eBGP-кордон.
- **MED** (Multi-Exit Discriminator, Optional Non-transitive) — числовий атрибут, що дозволяє AS рекомендувати сусідній AS переважну точку входу при наявності кількох точок взаємодії. Менше значення MED — більший пріоритет. Передається тільки в межах сусідньої AS, не розповсюджується далі.
- **COMMUNITY** (Optional Transitive) — 32**-бітний тег** (або 64-бітний для Large Communities, RFC 8092), що дозволяє групувати маршрути та застосовувати до них спільну маршрутну політику. Стандартні communities: NO_ADVERTISE (не рекламувати жодному сусіду) та NO_EXPORT (не рекламувати за межі AS).
- **EXTENDED COMMUNITY** (Optional Transitive) — 64-бітне розширення атрибуту COMMUNITY, що використовується для Route Target та Route Distinguisher в архітектурі MPLS VPN.

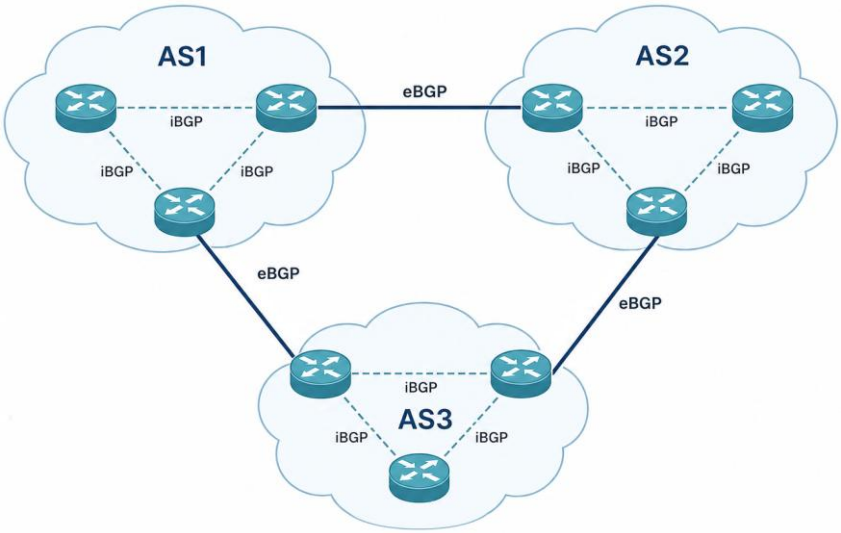

Рисунок 7.1 – Архітектура BGP: eBGP між AS та iBGP всередині AS

7.2. EBGP ТА IBGP

В архітектурі BGP розрізняють два типи BGP-сесій, кожен з яких виконує специфічну роль у процесі розповсюдження маршрутної інформації: eBGP (external BGP) — між маршрутизаторами різних AS, та iBGP (internal BGP) — між маршрутизаторами однієї AS. Незважаючи на однаковий протокол та однаковий

формат повідомлень, eBGP та iBGP суттєво відрізняються в поведінці атрибутів, правилах розповсюдження маршрутів та типових топологіях.

7.2.1. External BGP (eBGP)

eBGP-сесії встановлюються між маршрутизаторами (peers), що належать різним автономним системам. Зазвичай eBGP-сусіди є безпосередньо з'єднаними (directly connected), хоча в деяких сценаріях використовується eBGP multihop (параметр ebgp-multihop) для встановлення сесії через кілька проміжних вузлів, наприклад, між Loopback-інтерфейсами через IXP-фабрику.

Ключові особливості eBGP-сесій: при передачі маршруту через eBGP маршрутизатор додає свій ASN до атрибуту AS_PATH, змінює NEXT_HOP на власну IP-адресу (за замовчуванням) та скидає атрибут LOCAL_PREF (оскільки він є нетранзитивним і не розповсюджується між AS). Значення TTL для eBGP-пакетів за замовчуванням становить 1, що обмежує eBGP-сесії безпосередньо з'єднаними вузлами.

Типи eBGP-взаємодій визначають комерційні та технічні відносини між AS:

- **Transit peering** — відносини «клієнт–провайдер», де провайдер (upstream) надає клієнту (downstream) доступ до глобальної мережі Інтернет в обмін на оплату. Провайдер рекламує клієнту повну таблицю маршрутизації або маршрут за замовчуванням, а клієнт рекламує провайдеру свої власні префікси.
- **Peering** (Settlement-free peering) — безкоштовний обмін трафіком між AS приблизно рівного масштабу, де кожна AS рекламує іншій лише свої власні мережі та мережі своїх клієнтів (але не транзитних провайдерів). Здійснюється на IXP або через Private Peering Links.
- **Customer peering** — AS рекламує своїм клієнтам повну таблицю або маршрут за замовчуванням, приймає від них їх префікси та рекламує ці префікси своїм провайдерам та пірингам.

> **Принцип Gao-Rexford**
>
> *Модель Gao-Rexford описує комерційні відносини BGP: трафік завжди рухається від клієнта до провайдера або між пірингами, але ніколи від одного провайдера до іншого через клієнта. Цей принцип є основою стабільності глобального Інтернету.*

7.2.2. Internal BGP (iBGP)

iBGP-сесії встановлюються між маршрутизаторами всередині однієї автономної системи для розповсюдження зовнішніх (отриманих через eBGP) маршрутів. Ключова відмінність iBGP від eBGP полягає у правилі split-horizon: маршрутизатор не може рекламувати маршрут, отриманий через iBGP, іншому iBGP-сусіду. Це правило запобігає маршрутним петлям всередині AS, але призводить до вимоги повної зв'язності (full mesh): всі iBGP-маршрутизатори в AS повинні мати пряму iBGP-сесію між собою.

Ще одна важлива особливість iBGP: при передачі маршруту через iBGP атрибут AS_PATH не модифікується (ASN не додається), оскільки маршрут залишається всередині однієї AS. Атрибут NEXT_HOP також не змінюється: iBGP-маршрутизатор отримує маршрут з тим самим NEXT_HOP, що вказав eBGP-сусід (зазвичай IP-адреса на зовнішньому інтерфейсі граничного маршрутизатора). Для досяжності цього NEXT_HOP всі внутрішні маршрутизатори AS повинні мати маршрут до нього через IGP — це фундаментальна вимога архітектури BGP/IGP-взаємодії.

iBGP-сесії зазвичай встановлюються між Loopback-інтерфейсами маршрутизаторів, а не між фізичними. Це забезпечує стійкість iBGP-сесії до відмов окремих фізичних каналів: доки є будь-який IP-маршрут між Loopback-адресами через IGP, iBGP-сесія залишається активною. Проблема масштабованості full mesh: для AS із N iBGP-маршрутизаторами необхідно N×(N−1)/2 сесій. Для 100 маршрутизаторів — 4950 сесій. Саме для вирішення цієї проблеми були розроблені Route Reflectors та конфедерації BGP (BGP Confederations, RFC 5065).

Проблема масштабованості iBGP full mesh

При 50 iBGP-маршрутизаторах необхідно 1225 iBGP-сесій. При 100 — вже 4950. Кожна сесія споживає пам'ять та CPU для підтримки keepalive та оновлень. Без Route Reflectors або конфедерацій BGP великі AS є неуправляємими.

Таблиця 7.1 – Порівняння eBGP та iBGP

Характеристика	eBGP	iBGP
Де застосовується	Між різними AS	Всередині однієї AS
Модифікація AS_PATH	Додається ASN відправника	Не змінюється
Модифікація NEXT_HOP	Встановлюється на свою адресу	Не змінюється (зазвичай)
LOCAL_PREF	Скидається при виході з AS	Передається між iBGP-сусідами
TTL за замовчуванням	1 (безпосередні сусіди)	255 (через IGP)
Split-horizon	Маршрут не рекламується назад в ту ж AS	Маршрут не рекламується між iBGP-сусідами
Топологія	Point-to-point між AS	Full mesh або Route Reflector
Захист від петель	AS_PATH (відкидає свій ASN)	Split-horizon rule

7.3. ROUTE REFLECTORS

Вимога full mesh iBGP-сесій є основною проблемою масштабованості BGP у великих автономних системах. Для AS із N BGP-маршрутизаторами необхідно N×(N−1)/2 сесій. При зростанні мережі кількість сесій збільшується квадратично, що робить управління мережею надзвичайно складним. Стандарт RFC 4456 описує механізм Route Reflector як офіційне рішення цієї проблеми без зміни протоколу BGP.

7.3.1. Принцип роботи Route Reflector

Route Reflector (RR) — це спеціально виділений BGP-маршрутизатор, який виконує функцію «відбивача маршрутів»: він приймає маршрути від своїх iBGP-клієнтів і відображає (reflects) їх іншим клієнтам та non-client пірингам, порушуючи стандартне правило iBGP split-horizon. Маршрутизатори, що мають iBGP-сесію з RR і явно сконфігуровані як клієнти, називаються клієнтами RR (RR clients). Решта iBGP-маршрутизаторів, що мають сесію з RR, але не є клієнтами, називаються non-client peers.

Правила відображення маршрутів Route Reflector визначаються джерелом маршруту:

- Маршрут отримано від iBGP-клієнта: RR відображає його всім іншим клієнтам того ж кластеру, всім non-client iBGP-сусідам та всім eBGP-сусідам. Таким чином, клієнт може «спілкуватися» з іншими клієнтами та зовнішнім світом через RR без прямих iBGP-сесій між ними.

- Маршрут отримано від non-client iBGP-сусіда: RR відображає його лише своїм клієнтам (але не іншим non-clients, оскільки це порушило б split-horizon). Non-client peers повинні мати full mesh між собою.
- Маршрут отримано через eBGP: RR відображає його всім клієнтам та всім iBGP-сусідам (і клієнтам, і non-clients).

Для запобігання маршрутним петлям при використанні Route Reflectors вводяться два нові атрибути BGP. Атрибут ORIGINATOR_ID містить BGP Router-ID маршрутизатора, що вперше ввів маршрут в iBGP-домен. Якщо маршрутизатор отримує маршрут зі своїм власним ORIGINATOR_ID — він відкидає його. Атрибут CLUSTER_LIST містить список ідентифікаторів кластерів RR, через які пройшов маршрут. Якщо RR виявляє свій власний CLUSTER_ID у CLUSTER_LIST — він відкидає маршрут, запобігаючи петлям між кількома RR.

7.3.2. Ієрархічна структура Route Reflectors

Route Reflectors можуть бути організовані в ієрархічну структуру для подальшого масштабування. В базовій конфігурації один або кілька RR обслуговують усіх клієнтів у межах однієї AS. Кожен RR та його клієнти утворюють кластер (cluster), ідентифікований значенням CLUSTER_ID (зазвичай Loopback IP-адреса RR).

Для забезпечення надійності рекомендується використовувати резервні Route Reflectors: кожен клієнт повинен мати iBGP-сесії з принаймні двома RR. При виході з ладу одного RR клієнти продовжують отримувати маршрутну інформацію від резервного. Обидва RR мають однаковий CLUSTER_ID, що дозволяє виявляти маршрути від того ж кластеру.

В ієрархічній моделі введено поняття верхнього рівня RR (Super Route Reflectors або RR of RRs): звичайні RR є клієнтами Super-RR. Це дозволяє масштабувати BGP до мереж з тисячами маршрутизаторів. Наприклад, великий оператор може мати: 2–4 Super-RR на вершині ієрархії, 10–20 регіональних RR як клієнти Super-RR, сотні або тисячі PE-маршрутизаторів як клієнти регіональних RR.

У контексті MPLS VPN Route Reflectors відіграють критично важливу роль. PE-маршрутизатори обмінюються VPNv4/VPNv6-маршрутами через MP-BGP. Замість того щоб кожен PE мав iBGP-сесію з кожним іншим PE (що нереально при сотнях PE), всі PE підключаються до декількох RR. RR приймає VPNv4-маршрути від PE та відображає їх іншим PE, передаючи лише ті маршрути, RT яких відповідає RT клієнтів PE.

Таблиця 7.2 – Порівняння підходів до масштабування iBGP

Характеристика	Full Mesh iBGP	Route Reflector	BGP Confederation
Кількість сесій	N×(N−1)/2	N (клієнти → RR)	Зменшується до sub-AS
Зміна RFC	Не потрібна	RFC 4456	RFC 5065
Складність конфігурації	Висока (при великих N)	Низька–середня	Висока
Петлі запобігаються	Split-horizon	ORIGINATOR_ID, CLUSTER_LIST	AS_PATH (sub-AS номери)
Модифікація AS_PATH	Ні	Ні	Так (додаються sub-ASN)
Типове застосування	Малі AS (< 10 маршрутизаторів)	Більшість AS середнього та великого розміру	Деякі великі Tier-1 оператори

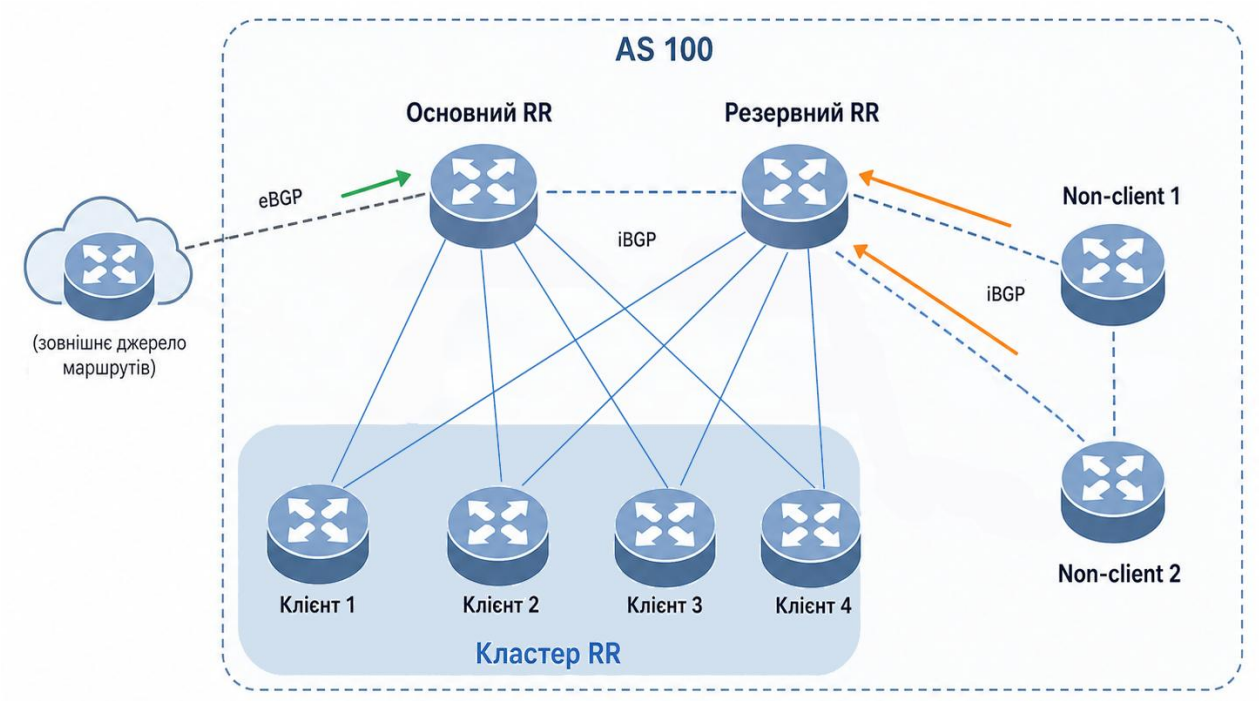

Рисунок 7.2 – Route Reflector: кластерна архітектура з клієнтами та non-client peers

7.4. BGP POLICY

Маршрутна політика (routing policy) є визначальною характеристикою BGP, що відрізняє його від протоколів внутрішньої маршрутизації. Якщо OSPF чи IS-IS вибирають маршрути виключно на основі метрики, то BGP надає адміністратору повний контроль над тим, які маршрути приймати, яким чином їх модифікувати та які рекламувати сусідам. Це дозволяє реалізувати складні бізнес-рішення: надавати транзит одним сусідам і відмовляти іншим, впливати на вибір шляхів трафіку, захищати власну мережу від небажаних маршрутів.

7.4.1. Алгоритм вибору найкращого маршруту BGP

Алгоритм вибору найкращого маршруту (BGP Best Path Selection) є послідовним процесом елімінації, де на кожному кроці відсіюються маршрути, що не задовольняють критерію, доки не залишиться один найкращий. Критерії розглядаються у строго визначеному порядку (перелічені від найвищого до найнижчого пріоритету):

Перевага маршруту з вищим значенням Weight (Cisco-специфічний атрибут, локальний для маршрутизатора, не передається сусідам; вищий — кращий).

Вищий LOCAL_PREFERENCE — надає перевагу маршруту при виборі виходу для трафіку з AS (вищий — кращий, за замовчуванням 100).

Маршрут, що походить від локального маршрутизатора (network або redistribute), — перевага перед маршрутами, отриманими від сусідів.

Коротший AS_PATH — менша кількість AS на шляху до призначення (менший — кращий). Механізм AS-PATH prepending штучно збільшує довжину AS_PATH для впливу на вибір шляху у сусідніх AS.

Нижчий Origin type — IGP (0) краще EGP (1), EGP краще Incomplete (2).

Нижчий MED (Multi-Exit Discriminator) — при рівних попередніх критеріях маршрут з меншим MED отримує перевагу (порівняння відбувається лише між маршрутами від однієї AS).

Перевага eBGP-маршруту над iBGP-маршрутом при рівних попередніх критеріях.

Нижча IGP-метрика до NEXT_HOP — серед рівноцінних маршрутів обирається той, чий NEXT_HOP досяжний через коротший IGP-шлях (Hot Potato Routing).

При рівності всіх попередніх критеріїв — маршрут від сусіда з нижчим BGP Router-ID (або нижчим ASN при рівних Router-ID).

7.4.2. Інструменти реалізації маршрутної політики

Для реалізації маршрутної політики в BGP використовуються кілька механізмів, які застосовуються як при отриманні маршрутів від сусідів (inbound policy), так і при рекламуванні маршрутів сусідам (outbound policy).

Route Maps — основний інструмент фільтрації та модифікації маршрутів в BGP. Route Map є послідовністю пронумерованих записів (clauses) зі своїм набором умов (match) та дій (set). Умови (match) можуть перевіряти: IP-префікс (через prefix-list або access-list), AS_PATH (через as-path access-list), атрибути Community чи Extended Community, значення MED, та інші параметри. Дії (set) можуть модифікувати: LOCAL_PREF, MED, AS_PATH (prepend), Community, NEXT_HOP, origin, weight.

Prefix Lists — забезпечують ефективну фільтрацію маршрутів за IP-префіксом та довжиною маски. На відміну від access-lists, prefix-lists дозволяють точно контролювати довжину маски за допомогою операторів ge (greater-or-equal) та le (less-or-equal). Наприклад: ip prefix-list FILTER permit 10.0.0.0/8 ge 24 le 28 — дозволяє лише префікси з простору 10.0.0.0/8 з маскою від /24 до /28.

AS-Path Access Lists (as-path access-list) — фільтрація маршрутів на основі регулярних виразів (regex) над атрибутом AS_PATH. Дозволяють реалізувати складні умови фільтрації: наприклад, прийняти лише маршрути, що походять безпосередньо від сусідньої AS (^65001$), або відфільтрувати маршрути транзитних AS.

BGP Communities — потужний механізм реалізації складних маршрутних політик. Оператор може визначати communities для групування маршрутів (наприклад, 65001:100 — «маршрути клієнтів», 65001:200 — «маршрути пірингів»). На основі community можна автоматично застосовувати різні LOCAL_PREF та рекламувати маршрути різним категоріям сусідів. Community також використовуються для реалізації послуги «BGP community-based traffic engineering», де клієнт може впливати на вибір шляху оператора.

7.4.3. Типові сценарії маршрутної політики

Розглянемо типовий практичний приклад маршрутної політики для оператора зв’язку з транзитними провайдерами та пірингами:

- Від транзитних провайдерів (upstream) отримуємо повну таблицю маршрутизації або default route. Встановлюємо LOCAL_PREF = 90 (нижче, ніж для пірингів та клієнтів), щоб трафік через провайдерів використовувався лише як резервний шлях. Рекламуємо провайдерам лише власні префікси та префікси клієнтів (але не префікси пірингів та інших транзитів).
- Від пірингів (peers) отримуємо лише їхні власні мережі та мережі їхніх клієнтів. Встановлюємо LOCAL_PREF = 110 (вище транзиту). Рекламуємо їм лише власні префікси та префікси клієнтів.
- Від клієнтів (customers) приймаємо лише їхні власні префікси (фільтрація через prefix-list з точними масками). Встановлюємо LOCAL_PREF = 150 (найвищий пріоритет). Рекламуємо клієнтам повну таблицю або default route.

AS-PATH prepending використовується для впливу на вибір шляху у сусідніх AS. Оператор може штучно збільшити довжину AS_PATH для маршруту, що рекламується через менш бажаний канал, додавши свій ASN кілька разів (наприклад, "65001 65001 65001"). Сусідня AS, отримавши два маршрути до тієї ж мережі — один з AS_PATH "65001" та інший з "65001 65001 65001" — обере перший як коротший. Це дозволяє керувати асиметрією трафіку: мінімізувати трафік через дорогий транзитний канал, спрямовуючи вхідний трафік через дешевший піринговий канал.

RPKI та безпека BGP

Resource Public Key Infrastructure (RPKI, RFC 6480) — система для криптографічної верифікації прав власності на IP-префікси та ASN. Route Origin Authorization (ROA) підписано власником IP-ресурсу та вказує, який ASN має право оголошувати певний префікс. RPKI Route Origin Validation (ROV) дозволяє відфільтровувати Invalid-маршрути, значно знижуючи ризики BGP hijacking.

7.5. L2VPN ТА L3VPN

Технології VPN (Virtual Private Network — віртуальна приватна мережа) на основі MPLS є одним із найважливіших застосувань BGP в операторських мережах. MP-BGP (Multiprotocol BGP, RFC 4760) розширює стандартний BGP шляхом введення нових адресних сімейств (Address Family Identifier, AFI) та підтипів (Subsequent AFI, SAFI), що дозволяє передавати інформацію про досяжність мереж різних типів поверх єдиної BGP-інфраструктури.

7.5.1. L3VPN: роль BGP в архітектурі

L3VPN на основі MPLS (RFC 4364) використовує MP-BGP для розповсюдження VPN-маршрутів між PE-маршрутизаторами. MP-BGP з адресним сімейством VPNv4 (AFI=1, SAFI=128) або VPNv6 (AFI=2, SAFI=128) передає префікси у форматі VPN-IPv4: 8-байтовий Route Distinguisher (RD) + 4-байтовий IPv4-префікс = 12-байтовий VPNv4-адрес. Це забезпечує глобальну унікальність адрес навіть при перекритті приватного адресного простору різних VPN-клієнтів.

Процес розповсюдження VPN-маршрутів через MP-BGP: PE-маршрутизатор отримує маршрути від CE через протокол PE-CE (статичний, OSPF, eBGP тощо), додає до кожного маршруту RD, прикріплює атрибути Route Target (RT) як Extended Community та рекламує через MP-BGP iBGP-сесію на Route Reflector або інші PE. Route Reflector поширює ці маршрути іншим PE. PE-отримувач перевіряє RT отриманих маршрутів та імпортує у відповідні VRF лише ті, RT яких збігається з його Import RT. MP-BGP також несе мітку VPN (Inner Label) для кожного маршруту, що дозволяє egress PE ідентифікувати вихідний інтерфейс або VRF.

Вибір протоколу для PE-CE взаємодії має практичне значення. eBGP є найбільш поширеним для великих клієнтів — дозволяє клієнту впливати на вибір шляхів через LOCAL_PREF та communities, підтримує multihoming. OSPF або IS-IS використовується для клієнтів, яким потрібна прозора маршрутизація всередині своєї VPN — PE виконує mutual redistribution між PE-CE OSPF та VPN-BGP. Статичні маршрути застосовуються для простих однозв'язних сайтів без вимог до динамічної маршрутизації.

7.5.2. L2VPN: роль BGP та типи послуг

L2VPN на основі MPLS забезпечує прозору передачу фреймів канального рівня між сайтами клієнта через MPLS-інфраструктуру оператора. BGP використовується двома способами: для автоматичного виявлення (auto-discovery) PE-

маршрутизаторів, що беруть участь у L2VPN, та для сигналізації — розподілу псевдодротових (PW) міток між PE.

VPWS (Virtual Private Wire Service, RFC 4448) — послуга «точка-точка» (point-to-point), що з'єднує два CE через псевдопровід. BGP може використовуватися для сигналізації псевдодроту (BGP-based VPWS, RFC 6624) замість LDP. Кожен псевдопровід ідентифікується унікальним Route Distinguisher та значенням VPWS Layer2 Info Extended Community, що несе інформацію про тип encapsulation та значення PW label.

VPLS (Virtual Private LAN Service, RFC 4761/4762) — забезпечує multipoint-to-multipoint зв'язність на L2, емулюючи Ethernet-комутатор. BGP-based VPLS (RFC 4761) використовує MP-BGP для авто-виявлення всіх PE в VPLS-домені та обміну PW-мітками. Перевага над LDP-based VPLS: не потрібно вручну конфігурувати full mesh псевдодротів — BGP автоматично встановлює необхідні з'єднання між PE при появі нового учасника VPLS.

Таблиця 7.3 – Порівняння L2VPN та L3VPN

Характеристика	L3VPN (RFC 4364)	L2VPN (VPWS/VPLS)
Рівень OSI	L3 (IP)	L2 (Ethernet, FR, ATM)
Участь оператора в маршрутизації	Так (peer-to-peer модель)	Ні (прозорий транспорт)
Роль BGP	Розповсюдження VPNv4/v6 маршрутів	Auto-discovery + label distribution
Адресне сімейство MP-BGP	VPNv4 (AFI=1, SAFI=128)	L2VPN (AFI=25, SAFI=65)
Ізоляція	VRF (окрема таблиця маршрутизації)	Pseudowire / VSI
Multihoming	Через PE-CE routing	Обмежена (у VPLS)
Масштабованість	Висока (через RR)	Середня (full mesh PW у VPLS)
Типове застосування	Корпоративні WAN	Розширення L2-мереж, DCI

7.6. EVPN

EVPN (Ethernet VPN, RFC 7432) є сучасною технологією побудови VPN на канальному рівні, яка використовує MP-BGP для розповсюдження інформації про MAC-адреси, IP-адреси та топологію мережі. EVPN об'єднує переваги L2VPN (прозора L2-зв'язність) та L3VPN (ефективна L3-маршрутизація) в єдиному рішенні та усуває ключові недоліки попередніх L2VPN технологій: відсутність підтримки active-active multihoming, неефективний flooding для вивчення MAC-адрес та відсутність інтегрованої L2/L3-маршрутизації.

7.6.1. Архітектура та типи маршрутів EVPN

В архітектурі EVPN PE-маршрутизатори (або VTEP — VXLAN Tunnel End Points у дата-центрах) використовують MP-BGP з адресним сімейством EVPN (AFI=25, SAFI=70) для обміну інформацією. Кожен EVPN-інстанс (EVI) є незалежним доменом комутації з власним набором RT для імпорту/експорту маршрутів. EVPN визначає п'ять основних типів маршрутів (Route Types), кожен з яких виконує специфічну функцію.

- Route Type 1 (Ethernet Auto-Discovery, AD) — використовується для виявлення учасників Ethernet Segment та забезпечення active-active multihoming.

Рекламується для кожного Ethernet Segment Identifier (ESI) та для кожного EVI. Дозволяє швидко сигналізувати про відмову або відновлення Ethernet Segment.

- Route Type 2 (MAC/IP Advertisement) — найпоширеніший тип. Несе прив'язку MAC-адреси до IP-адреси (аналог ARP/ND-запису), а також MPLS або VXLAN мітку для передачі трафіку. Дозволяє уникнути flooding ARP-запитів у великих мережах — PE отримує ARP-відповідь безпосередньо з таблиці BGP.
- Route Type 3 (Inclusive Multicast Ethernet Tag, IMET) — оголошує участь PE у розповсюдженні BUM-трафіку (Broadcast, Unknown unicast, Multicast) для конкретного EVI. Є аналогом механізму join-leave для multicast у VPLS, але реалізований через BGP.
- Route Type 4 (Ethernet Segment Route) — рекламується усіма PE, підключеними до одного Ethernet Segment (одного фізичного або LAG-з'єднання до CE). Використовується для Designated Forwarder (DF) Election — вибору одного PE, який відповідатиме за BUM-трафік в active-active режимі.
- Route Type 5 (IP Prefix Route) — несе IPv4/IPv6-префікси для L3-маршрутизації між EVPN-інстансами. Є розширенням RFC 9136, що дозволяє EVPN виконувати функції L3VPN без необхідності окремого VPNv4/v6.

7.6.2. Multihoming в EVPN

Active-Active multihoming є однією з ключових переваг EVPN перед VPLS. У VPLS клієнтський пристрій може бути підключений лише до одного PE (single-homed) або через спеціальні механізми до двох PE в режимі active-standby (де лише один PE активний). EVPN нативно підтримує active-active multihoming: клієнтський пристрій може підключатися до двох або більше PE одночасно, і всі вони активно передають трафік.

Механізм реалізації active-active multihoming: усі PE, підключені до одного CE, конфігурують однаковий Ethernet Segment Identifier (ESI) — унікальний 10-байтовий ідентифікатор сегменту. Через EVPN Route Type 4 відбувається виявлення всіх PE, що «бачать» цей ESI, та вибір Designated Forwarder для BUM-трафіку. Для unicast-трафіку всі PE-учасники активні — балансування навантаження між ними виконується на стороні CE (через LACP/LAG або ECMP). Для запобігання петлям EVPN використовує механізм Split Horizon: PE не пересилає трафік, отриманий від одного ESI, назад в той самий ESI.

7.6.3. EVPN з VXLAN Overlay

У сучасних дата-центрах EVPN найчастіше використовується у поєднанні з VXLAN (Virtual eXtensible LAN, RFC 7348) як overlay-технологією інкапсуляції. VXLAN забезпечує encapsulation Ethernet-кадрів у UDP/IP з 24-бітним VNI (VXLAN Network Identifier, до 16 мільйонів мережевих сегментів), подолання обмеження 4094 VLAN-ів та масштабування мереж дата-центрів. EVPN виступає як площина управління для VXLAN, вирішуючи проблему масштабованості традиційного VXLAN flood-and-learn підходу.

Архітектура EVPN-VXLAN у дата-центрі базується на топології Spine-Leaf (Clos fabric). Leaf-комутатори (VTEP) виконують функції PE: вони інкапсулюють трафік у VXLAN та розповсюджують MAC/IP-прив'язки через MP-BGP. Spine-комутатори виконують функції P-маршрутизаторів та Route Reflectors: вони пересилають VXLAN-трафік між Leaf та відображають EVPN-маршрути між VTEP. Усі Leaf-VTEP встановлюють iBGP-сесії (EVPN address family) зі Spine-маршрутизаторами, що виступають як Route Reflectors.

EVPN також підтримує інтегровану маршрутизацію та комутацію (Integrated Routing and Bridging, IRB), що дозволяє виконувати L3-маршрутизацію між різними VXLAN-мережами безпосередньо на Leaf-комутаторах. Для цього кожен Leaf конфігурує однакову anycast gateway IP та MAC-адресу для кожного SVI (Switched Virtual Interface). Ця концепція, відома як Distributed Anycast Gateway, дозволяє хосту в будь-якій точці фабрики використовувати однакову шлюзову IP-адресу незалежно від того, до якого Leaf він підключений, що усуває необхідність у централізованому шлюзі та забезпечує оптимальну локальну маршрутизацію.

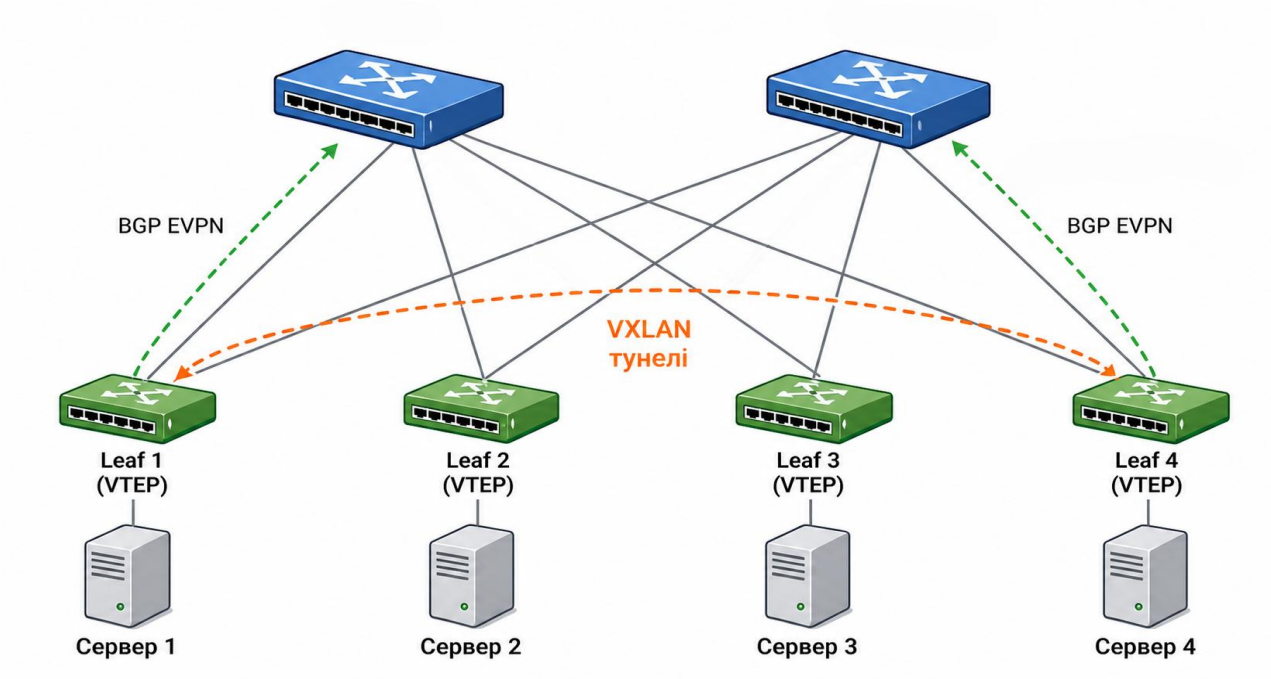

Рисунок 7.3 – EVPN-VXLAN у архітектурі Spine-Leaf дата-центру

Таблиця 7.4 – Порівняння L2VPN технологій: VPLS vs EVPN

Характеристика	VPLS (RFC 4762)	EVPN (RFC 7432)
Площина управління	LDP або MP-BGP	MP-BGP (EVPN NLRI)
Вивчення MAC	Data-plane flooding	Control-plane (BGP RT-2)
ARP/ND	Flood у мережу	Proxy ARP/ND (BGP RT-2)
Multihoming	Active-standby (обмежено)	Active-active (native ESI)
L3-маршрутизація	Через окремий L3VPN або IRB	Integrated (RT-5, IRB)
BUM-трафік	Ingress replication або PIM	Ingress replication, PIM або BIER
Масштабованість	Обмежена (full mesh PW)	Висока (RR-based)
Underlay	MPLS	MPLS або IP/VXLAN
Типове застосування	Legacy WAN L2VPN	Дата-центри, сучасні WAN L2VPN

Контрольні питання

1. Поясніть, чому BGP називають протоколом типу path-vector. Як атрибут AS-PATH використовується для прийняття рішень про маршрутизацію та запобігання петлям?
2. Назвіть чотири типи повідомлень BGP (OPEN, UPDATE, KEEPALIVE, NOTIFICATION) та опишіть їх призначення в життєвому циклі BGP-сесії.
3. Опишіть кінцевий автомат (FSM) BGP. Через які стани (Idle, Connect, Active, OpenSent, OpenConfirm, Established) проходить процес встановлення сесії?
4. Чим зарезервовані діапазони ASN (64512–65534 та 4200000000–4294967294) відрізняються від публічних? Коли використовуються 32-бітові ASN замість 16-бітових?
5. У чому полягає відмінність між eBGP та iBGP у поведінці атрибутів AS-PATH і NEXT-HOP? Чому ця різниця критична для коректної роботи BGP?
6. Поясніть правило iBGP split-horizon та його наслідки для масштабованості. Скільки iBGP-сесій потрібно для full mesh у AS зі 100 маршрутизаторами?
7. Як Route Reflector вирішує проблему масштабованості full mesh iBGP? Опишіть правила відображення маршрутів для клієнтських та non-client peers.
8. Поясніть призначення атрибутів ORIGINATOR_ID та CLUSTER_LIST. Як вони запобігають маршрутним петлям у топологіях з Route Reflectors?
9. Чим конфедерація BGP відрізняється від Route Reflectors як механізм масштабування iBGP? Які переваги та недоліки кожного підходу?
10. Опишіть алгоритм вибору найкращого маршруту BGP. Назвіть перші 5 критеріїв у порядку пріоритетності та поясніть їх призначення.
11. Поясніть атрибути LOCAL_PREFERENCE, MED та COMMUNITY. Як вони використовуються для реалізації політик маршрутизації?
12. Як AS-PATH prepending використовується для Traffic Engineering? Наведіть приклад застосування для впливу на вибір вхідного шляху трафіку в AS.
13. Опишіть архітектуру MPLS L3VPN. Поясніть роль PE-, P- та CE-маршрутизаторів, а також концепцію VRF (Virtual Routing and Forwarding).
14. Поясніть призначення Route Distinguisher (RD) та Route Target (RT) у MPLS L3VPN. Чому потрібні обидва атрибути?
15. Порівняйте L2VPN та L3VPN за рівнем абстракції, прозорістю для клієнта та сферами застосування.
16. Опишіть архітектуру VPLS (Virtual Private LAN Service). Порівняйте LDP-based та BGP-based сигналізацію у VPLS.
17. Назвіть п’ять типів маршрутів EVPN (Type 1–5) та коротко опишіть функцію кожного.
18. Як EVPN забезпечує active-active multihoming? Поясніть роль Ethernet Segment Identifier (ESI) та Designated Forwarder Election.
19. Опишіть архітектуру EVPN-VXLAN у топології Spine-Leaf дата-центру. Які функції виконують Spine- та Leaf-комутатори?
20. Поясніть концепцію Distributed Anycast Gateway у EVPN. Яку проблему вона вирішує порівняно з централізованим шлюзом?

РОЗДІЛ 8

БЕЗПЕКА ГЛОБАЛЬНИХ МЕРЕЖ

Восьмий розділ присвячено комплексному аналізу загроз, що існують у глобальних мережах, та технологій для протидії їм. Розглядаються класифікація кіберзагроз, механізми DDoS-атак та захисту від них, системи виявлення та запобігання вторгненням, технологія глибокого аналізу пакетів, міжмережеві екрани нового покоління, архітектура нульової довіри, а також специфічні механізми захисту протоколу BGP.

Глобальна мережа за своєю природою є відкритим і розподіленим середовищем, де пакети даних проходять через безліч вузлів під контролем різних організацій, а будь-який з цих вузлів може стати точкою атаки.

За даними численних звітів провідних компаній у галузі кібербезпеки, кількість та складність кібератак на глобальні мережі демонструє стійке зростання. DDoS-атаки досягають потужності в кілька терабітів на секунду, викрадення BGP-маршрутів призводить до масових порушень зв'язності, а витоки даних через незахищені мережеві канали завдають організаціям мільярдних збитків. Безпека WAN перестала бути суто технічним питанням і перетворилась на стратегічний пріоритет для будь-якої організації.

Ключова ідея

Безпека глобальних мереж — це не окремий продукт, а комплексна стратегія, що охоплює технічні засоби захисту, процеси управління інцидентами та усвідомлення ризиків на всіх рівнях організації. Жоден окремо взятий захід не забезпечує повного захисту — лише їх поєднання формує ефективну систему безпеки.

8.1. ЗАГРОЗИ ГЛОБАЛЬНИХ МЕРЕЖ

Глобальні мережі за своєю природою є відкритими системами, що забезпечують взаємодію мільйонів гетерогенних вузлів через спільну інфраструктуру. Ця відкритість, що є необхідною умовою функціональності мережі, одночасно є джерелом численних вразливостей. Аналіз загроз є необхідним першим кроком у побудові ефективної системи безпеки — без чіткого розуміння типів загроз, їхніх механізмів реалізації та потенційного впливу неможливо розробити адекватні та ефективні контрзаходи.

8.1.1. Класифікація кіберзагроз WAN

Загрози безпеці глобальних мереж класифікуються за кількома критеріями, кожен з яких висвітлює певний аспект загрози та допомагає у виборі відповідних засобів захисту.

За характером впливу на мережу загрози поділяються на пасивні та активні. Пасивні загрози не вносять змін у передану інформацію та не порушують функціонування мережі, натомість спрямовані на несанкціоноване отримання інформації: перехоплення трафіку (packet sniffing), аналіз трафіку для отримання метаданих комунікацій, прослуховування каналів зв'язку. Активні загрози передбачають втручання у нормальне функціонування мережі: DDoS-атаки, Man-in-the-Middle, підміна та модифікація пакетів, Spoofing.

За рівнем моделі OSI, на якому здійснюється атака: фізичний рівень (L1) — пошкодження ліній, несанкціоноване підключення; канальний (L2) — ARP spoofing,

MAC flooding, VLAN hopping; мережевий (L3) — IP spoofing, route hijacking, ICMP-атаки; транспортний (L4) — SYN flood, UDP flood, RST-атаки; сеансовий (L5) — захоплення сесії; представлення (L6) — TLS downgrade, підміна сертифіката; прикладний (L7) — Phishing, DNS spoofing, атаки на вебсервіси.

За джерелом загрози виділяють зовнішні атаки (хакери, конкуренти, державні актори, кіберзлочинні групи) та внутрішні (інсайдерські дії, зловживання привілеями, скомпрометований внутрішній вузол). Зловмисники-одинаки частіше використовують автоматизовані інструменти та відомі вразливості; державні актори (APT-групи) діють цілеспрямовано, із значними ресурсами та тривалими операціями — можуть роками зберігати доступ до критичної інфраструктури непоміченими.

За мотивацією: фінансово вмотивовані (ransomware, шахрайство, вимагання), ідеологічні (hacktivism, defacement, витік даних), державні (APT, кібершпигунство, саботаж критичної інфраструктури), деструктивні (wiper malware, виведення сервісів з ладу).

Рисунок 8.1 – Класифікація загроз глобальних мереж

8.1.2. Перехоплення трафіку та прослуховування

Перехоплення мережевого трафіку (eavesdropping, packet sniffing) є однією з найпоширеніших пасивних загроз у глобальних мережах. На фізичному рівні можливе підключення до оптичних кабелів за допомогою спеціальних оптичних розгалужувачів (optical splitters/taps), що дозволяє отримати копію оптичного сигналу без порушення основного з'єднання. Перехоплення за допомогою оптичних tap-пристроїв особливо небезпечне, оскільки не впливає на затримку або якість сигналу і практично не виявляється стандартними засобами моніторингу.

На канальному рівні використовуються методи ARP spoofing (ARP poisoning) для перенаправлення трафіку через контрольований зловмисником вузол. Зловмисник надсилає підроблені ARP-відповіді, що асоціюють його MAC-адресу з IP-адресою легітимного вузла (шлюзу або іншого хосту). Це призводить до того, що трафік,

призначений легітимному вузлу, спрямовується на зловмисника, де він може бути перехоплений і далі перенаправлений (MITM-атака).

На мережевому рівні маніпулювання таблицями маршрутизації через атаки на BGP дозволяє перенаправити потоки трафіку через вузли, контрольовані зловмисником, на глобальному рівні. Особливо небезпечними є BGP hijacking-атаки, коли зловмисник анонсує більш специфічний префікс і перехоплює трафік цілого регіону або організації. Аналіз трафіку (traffic analysis) навіть без розшифрування вмісту дозволяє визначити кількість та розмір повідомлень, часові патерни комунікації, ідентифікувати учасників та тривалість взаємодії.

Основним методом захисту є шифрування на різних рівнях: TLS на прикладному рівні (HTTPS, SMTPS, IMAPS), IPsec на мережевому рівні для захисту всього IP-трафіку між вузлами, MACsec (IEEE 802.1AE) на канальному рівні для захисту Ethernet-сегментів. Для захисту від аналізу трафіку використовуються: padding (доповнення пакетів до фіксованого розміру), traffic shaping (підтримка постійного рівня трафіку), а також Tor-подібні мережі для анонімізації.

8.1.3. Атаки підміни (Spoofing)

Атаки підміни (spoofing) полягають у фальсифікації ідентифікаційних даних для маскування справжнього джерела трафіку або видавання себе за довірений вузол.

IP spoofing — модифікація поля Source IP Address в заголовку IP-пакета, що дозволяє замаскувати справжнє джерело атаки та використовувати атаки з відбиттям (reflection attacks). Протидія: ingress filtering (BCP 38/RFC 2827) — оператори відфільтровують пакети з IP-адресами джерела, що не відповідають адресним блокам клієнта.

DNS spoofing (DNS cache poisoning) — підміна відповідей DNS-сервера для перенаправлення користувачів на фальшиві ресурси. Зловмисник відправляє підроблену DNS-відповідь раніше, ніж легітимний DNS-сервер. Захист: DNSSEC (DNS Security Extensions, RFC 4033–4035) забезпечує криптографічний підпис DNS-записів.

BGP route hijacking — анонсування чужих IP-префіксів через BGP. Зловмисник, що контролює BGP-маршрутизатор, анонсує більш специфічний префікс (наприклад, /24 замість /16), перехоплюючи трафік. Захист: RPKI (Resource Public Key Infrastructure) зі створенням ROA (Route Origin Authorization) — криптографічно підписаних записів, що вказують, які AS мають право анонсувати певні префікси.

Реальний приклад BGP hijacking

У квітні 2010 року China Telecom (AS23724) анонсувала близько 37 000 чужих IP-префіксів протягом 18 хвилин. Під час цього інциденту значна частина інтернет-трафіку, включаючи трафік американських військових та урядових сайтів, тимчасово маршрутизувалася через Китай. Інцидент продемонстрував критичну вразливість BGP та прискорив впровадження RPKI.

8.1.4. Атаки «людина посередині» (MITM)

Атака «людина посередині» (Man-in-the-Middle, MITM) є комбінацією перехоплення та підміни, при якій зловмисник розташовується на шляху передачі даних між двома сторонами, перехоплює та за потреби модифікує комунікацію, залишаючись непоміченим. MITM-атаки є особливо небезпечними, оскільки жертви продовжують вважати свій зв'язок захищеним, не підозрюючи про втручання третьої сторони.

Класичним прикладом MITM у протоколах TLS є атака зниження версії протоколу (downgrade attack): зловмисник втручається у процес TLS-рукостискання та змушує обидві сторони погодитися на використання застарілих та вразливих алгоритмів шифрування. Особливо небезпечний варіант MITM у контексті WAN — маніпулювання маршрутами BGP для перехоплення трафіку між двома організаціями.

Захист від MITM базується на механізмах взаємної автентифікації та шифрування. TLS з перевіркою сертифіката (Certificate Pinning) запобігає підміні сертифіката. HTTP Strict Transport Security (HSTS) примушує браузер завжди використовувати HTTPS. BGP-сесії захищаються MD5-автентифікацією (RFC 2385) або більш сучасним TCP-AO (RFC 5925). IPsec із взаємною автентифікацією через сертифікати забезпечує комплексний захист на мережевому рівні.

8.1.5. Сканування та розвідка

Сканування мережі та розвідка (reconnaissance) є підготовчими етапами більшості цілеспрямованих атак. Згідно з моделлю MITRE ATT&CK, розвідка є першою фазою («Reconnaissance») у ланцюжку кіберзагроз. Пасивна розвідка включає збір інформації з відкритих джерел (OSINT): аналіз DNS-записів (Whois, nslookup, dig), вивчення BGP-анонсів (через RouteViews, RIPE RIS), дослідження відкритих репозиторіїв та соціальних мереж.

Активна розвідка включає: трасування маршрутів (traceroute/tracert) для визначення топології мережі та IP-адрес прикордонних маршрутизаторів; сканування портів (Nmap) для визначення відкритих сервісів та їхніх версій; сканування вразливостей для виявлення незакритих CVE. Протидія: обмеження відповідей на ICMP-запити, фільтрація зондуючого трафіку на периметрі, розгортання honeypot-систем для виявлення та введення в оману зловмисників.

8.1.6. Експлуатація вразливостей мережевого обладнання

Мережеве обладнання — маршрутизатори, комутатори, міжмережеві екрани — являє собою складні комп'ютерні системи з власними операційними системами (Cisco IOS/IOS-XE/IOS-XR, Juniper Junos, Nokia SR OS), що також мають вразливості. Типові вразливості включають: використання стандартних або слабких паролів; незахищені протоколи управління (Telnet, SNMPv1/v2c без шифрування, HTTP-інтерфейс управління); невиправлені CVE у програмному забезпеченні; неналежно сконфігуровані права доступу.

Захист мережевого обладнання: регулярне оновлення ПЗ та прошивок; використання надійних паролів та багатофакторної автентифікації (MFA); обмеження доступу до управлінських інтерфейсів через окрему управлінську мережу (out-of-band management); шифрування управлінського трафіку (SSH замість Telnet, SNMPv3, HTTPS замість HTTP); інвентаризація та сканування вразливостей; принцип мінімальних привілеїв для облікових записів адміністраторів.

8.2. РОЗПОДІЛЕНІ АТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ (DDoS)

Розподілені атаки на відмову в обслуговуванні (Distributed Denial of Service, DDoS) є однією з найсерйозніших та руйнівних загроз для глобальних мереж. Сутність DDoS-атаки полягає у генерації надмірного обсягу трафіку або навантаження з багатьох джерел одночасно з метою вичерпання ресурсів цільової системи — пропускної здатності каналу, обчислювальних ресурсів серверів, або стану сесійних таблиць

Перші помітні DDoS-атаки відбулися на початку 2000-х років. Сучасні атаки досягають потужності в кілька терабітів на секунду: у жовтні 2017 року Google зафіксувала атаку потужністю 2,54 Тбіт/с, а у 2020 році AWS відбила атаку 2,3 Тбіт/с. Економічний вплив DDoS є значним: вартість простою для великих підприємств може вимірюватися сотнями тисяч доларів за годину.

8.2.1. Класифікація DDoS-атак

DDoS-атаки класифікуються за рівнем мережевої моделі та механізмом впливу на цільову систему.

Волюметричні атаки (L3–L4) — спрямовані на вичерпання пропускної здатності каналу між цільовою системою та Інтернетом. Типові вектори: UDP flood (надсилання великої кількості UDP-пакетів на випадкові порти), ICMP flood (Ping flood), DNS amplification (коефіцієнт ампліфікації до 179×), NTP amplification (коефіцієнт до 4096×), Memcached amplification (рекордний коефіцієнт до 51 000×). Механізм ампліфікації: зловмисник надсилає невеликий запит з підробленою IP-адресою жертви до рефлектора (DNS-сервера, NTP-сервера тощо), який відповідає значно більшим пакетом безпосередньо жертві.

Атаки на рівні протоколів (L3–L4) — експлуатують особливості реалізації мережевих протоколів для вичерпання ресурсів. SYN flood: зловмисник надсилає велику кількість TCP SYN-пакетів з підробленими IP-адресами, змушуючи сервер виділяти ресурси для незавершених з'єднань (half-open connections), поки таблиця сесій не переповниться. ACK flood і RST flood перевантажують stateful-обладнання необхідністю обробки пакетів з встановленого з'єднання. Fragmented Packet Attack: надсилання фрагментованих пакетів, що вимагають значних ресурсів для реасемблювання.

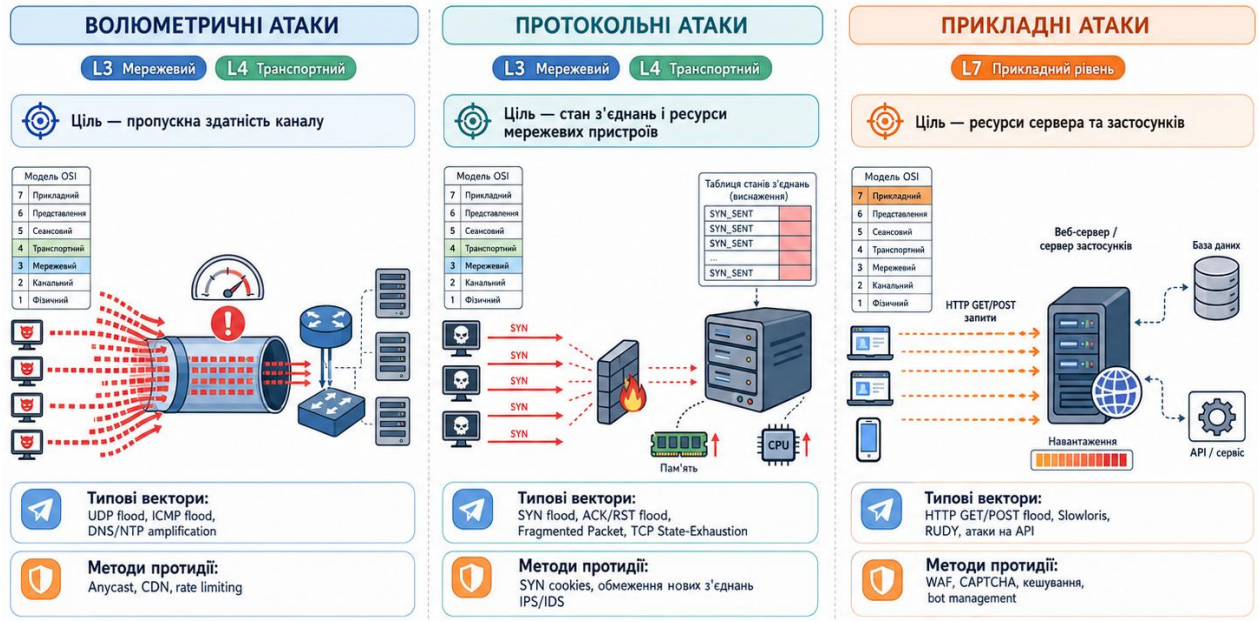

Рисунок 8.2 – Класифікація DDoS-атак за рівнями мережевої моделі

Атаки на рівні застосунків (L7) — найскладніші для виявлення, оскільки імітують легітимний трафік. HTTP GET/POST flood: масові HTTP-запити до ресурсомістких ендпоїнтів (пошукові запити, форми, API). Slowloris: відкриває велику кількість HTTP-з'єднань та підтримує їх, надсилаючи неповні заголовки з мінімальною швидкістю, виснажуючи пул потоків веб-сервера. RUDY (R-U-Dead-Yet): надсилає POST-запити з надзвичайно малою швидкістю передачі тіла запиту. DNS query flood: масові запити до DNS-сервера для його перевантаження.

Мультивекторні атаки — поєднують кілька типів атак одночасно, ускладнюючи протидію. Наприклад, одночасний UDP flood (для перевантаження каналу) + SYN flood (для виснаження stateful-обладнання) + HTTP flood (для перевантаження вебсервера).

8.2.2. Ботнети як інструмент DDoS-атак

Ботнет (botnet) — мережа скомпрометованих комп'ютерів та інших пристроїв, підключених до Інтернету, які централізовано керуються зловмисником (bot herder, botmaster) через сервери командного управління (Command and Control, C&C або C2). Ботнети є основним інструментом для організації масштабних DDoS-атак, розсилання спаму та здійснення фінансових шахрайств.

Еволюція архітектури ботнетів: перше покоління — централізована архітектура C&C (IRC-сервери або HTTP), де всі боти підключаються до одного сервера управління; друге покоління — P2P-архітектура, де боти утворюють децентралізовану мережу без єдиного сервера (Conficker, Zeus P2P) — значно складніша для нейтралізації; третє покоління — DGA (Domain Generation Algorithm), боти щодня генерують сотні псевдовипадкових доменних імен, одне з яких реєструється зловмисником як C&C-сервер — практично унеможливлює блокування.

Сучасні ботнети значною мірою складаються з пристроїв IoT — IP-камер, домашніх маршрутизаторів, NAS-сховищ, «розумних» побутових приладів, які мають слабкий захист (стандартні паролі, рідкісні оновлення) та завжди підключені до Інтернету. Ботнет Mirai (2016) заразив від кількох сотень тисяч до понад мільйона IoT-пристроїв та здійснив атаку потужністю близько 620 Гбіт/с (за різними джерелами — до 665 Гбіт/с) на сайт Krebs on Security та близько 1 Тбіт/с на провайдера OVH. Атака на DNS-провайдера Dyn у жовтні 2016 року спричинила масштабний збій сервісів Twitter, Netflix, Reddit, Airbnb та десятків інших платформ.

Загроза IoT-ботнетів

Мільярди слабко захищених IoT-пристроїв формують постійно зростаючий резервуар для ботнетів. Більшість виробників IoT-пристроїв досі не приділяють належної уваги безпеці, а користувачі рідко змінюють стандартні паролі та оновлюють прошивки. Після публікації вихідного коду Mirai у 2016 році з'явилися десятки його варіантів.

8.2.3. Методи протидії DDoS-атакам

Ефективна протидія DDoS вимагає багаторівневого підходу, що охоплює як превентивні заходи, так і механізми виявлення та реагування в реальному часі.

Надлишкова пропускна здатність (overprovisioning) — базовий превентивний захід: організація забезпечує пропускну здатність, що перевищує звичайний пік трафіку в кілька разів, що ускладнює волюметричні атаки.

Anycast routing — розподіл трафіку між багатьма центрами обробки в різних географічних точках шляхом анонсування одного IP-префіксу з різних місць. Трафік атаки розподіляється між усіма точками присутності, жодна з яких не отримує всього обсягу атаки. Саме цей механізм захищає кореневі DNS-сервери від DDoS.

Blackhole routing (RTBH) — перенаправлення трафіку, спрямованого на атаковану IP-адресу, у «чорну діру» (null route). Destination-based RTBH: blackhole для конкретної IP-адреси жертви (трафік до жертви блокується, але вона стає недоступною). Source-based RTBH: blackhole для IP-адрес джерел атаки (потребує знання адрес зловмисників). RTBH реалізується через BGP — маршрутизатор анонсує специфічний маршрут для атакованого префіксу з next-hop на Null0.

BGP Flowspec (RFC 5575/8955) — дозволяє динамічно розповсюджувати правила фільтрації трафіку через BGP на всі маршрутизатори оператора. Flowspec-правила можуть вказувати: IP-адресу джерела/призначення, порт, протокол, розмір пакета. Дії: rate-limit, redirect, discard. Дозволяє за секунди розгорнути фільтр на сотнях маршрутизаторів без ручного налаштування кожного.

Scrubbing centers (центри очищення трафіку) — найефективніший механізм для масштабних атак. Трафік до атакованого ресурсу перенаправляється (через BGP або DNS) до спеціалізованого центру очищення, де відокремлюється від атакуючого, і лише легітимний трафік пересилається далі. Хмарні DDoS-mitigation провайдери (Cloudflare, Akamai, AWS Shield Advanced) мають пропускну здатність в десятки Тбіт/с.

Захист від SYN flood — TCP SYN cookies (RFC 4987): сервер не зберігає стан з'єднання після SYN, а кодує параметри з'єднання у початковий номер послідовності (ISN) відповіді SYN-ACK. Якщо клієнт легітимний і надсилає ACK з правильним ISN, стан з'єднання створюється лише тоді. Апаратні SYN proxy реалізують цю логіку на рівні мережевого обладнання.

WAF (Web Application Firewall) — захист від L7 DDoS: виявлення та блокування аномальних HTTP-запитів через поведінковий аналіз, rate limiting на рівні сесії/IP/URL, CAPTCHA-виклики для підозрілих клієнтів, реп'ютаційні бази IP-адрес.

Таблиця 8.1 — Порівняльна характеристика типів DDoS-атак

Характеристика	Волюметричні	Протокольні	Прикладні (L7)	Ампліфікація
Рівень OSI	L3–L4	L3–L4	L7	L3–L4
Ціль атаки	Канал зв'язку	Таблиці стану, CPU	Ресурси сервера/застосунку	Канал через рефлектори
Типова потужність	10–100+ Гбіт/с	1–10 Гбіт/с	0,01–1 Гбіт/с	100+ Гбіт/с – Тбіт/с
Складність виявлення	Низька	Середня	Висока	Низька
Приклади	UDP flood, ICMP flood	SYN flood, ACK flood	HTTP flood, Slowloris	DNS, NTP, Memcached
Основний захист	Anycast, scrubbing	SYN cookies, proxy	WAF, CAPTCHA, аналіз	BCP38, інгрес фільтрація

8.3. СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ (IDS/IPS)

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) та системи запобігання вторгненням (Intrusion Prevention Systems, IPS) є критичними компонентами захисту глобальних мереж. Необхідність IDS/IPS обумовлена тим, що сучасні атаки часто використовують дозволені канали комунікації (наприклад, HTTP-з'єднання через порт 443), які міжмережеві екрани пропускають, тоді як IDS/IPS аналізують вміст трафіку для виявлення ознак зловмисної активності.

8.3.1. Архітектура та принципи роботи IDS

Система виявлення вторгнень здійснює пасивний моніторинг мережевого трафіку або системних подій з метою ідентифікації ознак несанкціонованої активності. На відміну від IPS, IDS не блокує трафік самостійно, а генерує сповіщення для адміністраторів або SIEM-системи.

Архітектура типової мережевої IDS (NIDS) включає: сенсор (sensor/probe) — компонент у стратегічних точках мережі (перед/після firewall, у DMZ, в ядрі мережі), що захоплює копію трафіку через SPAN-порт або мережевий TAP; препроцесор — нормалізує та реасемблює трафік; рушій виявлення — зіставляє трафік з базою правил або профілями нормальної активності; база правил та сигнатур — база знань про відомі атаки (наприклад, Snort rules, Suricata rules); модуль звітності та сповіщення — надсилає алерти в SIEM, SOC, на пошту.

За місцем розгортання: мережеві IDS (NIDS) — розгортаються у стратегічних вузлах мережі, аналізують увесь трафік у сегменті; хостові IDS (HIDS) — встановлюються на захищаємому хості, аналізують системні журнали, цілісність файлів (за допомогою контрольних сум), системні виклики та локальний мережевий трафік. HIDS є ефективнішими для виявлення атак на конкретний хост, але не надають загальної картини мережі.

8.3.2. Методи виявлення вторгнень

Сигнатурний метод (signature-based, misuse detection) — базується на порівнянні трафіку з базою відомих сигнатур атак. **Сигнатура** — це характерний патерн (послідовність байтів, заголовок пакета, поведінковий шаблон), що відповідає конкретному типу шкідливої активності. Перевага: висока точність виявлення відомих атак (низький рівень false positives), відносно низька обчислювальна вартість. Недолік: не виявляє нові (zero-day) атаки, потребує регулярного оновлення бази сигнатур. Приклади: Snort, Suricata, Cisco Firepower.

Аномальний метод (anomaly-based) — базується на побудові профілю нормальної мережевої активності (baseline) під час навчального періоду та ідентифікації статистичних відхилень. Характеристики, що профілюються: обсяги трафіку, розподіл протоколів, часові патерни активності, типові пари хостів та порти. Перевага: виявляє нові, невідомі атаки, у тому числі zero-day. Недолік: вищий рівень false positives (хибних тривог), складніша налаштовка, вимагає тривалого навчального періоду.

Сучасні IDS/IPS поєднують обидва підходи, доповнюючи їх машинним навчанням та поведінковим аналізом. Supervised learning-моделі навчаються на labeled-датасетах атак та нормального трафіку. Unsupervised learning (кластеризація) виявляє аномалії без попереднього навчання. Deep learning-моделі (LSTM, автоенкодери) ефективні для аналізу часових послідовностей мережевих подій.

8.3.3. Системи запобігання вторгненням (IPS)

IPS є еволюцією IDS, що додає до функцій виявлення здатність автоматично блокувати або модифікувати шкідливий трафік у реальному часі. Принципова відмінність: IDS розгортається out-of-band (копія трафіку через SPAN/TAP), тоді як IPS розгортається inline — на шляху трафіку, подібно до міжмережевого екрана.

Дії IPS при виявленні загрози: drop packet — пакет видаляється без сповіщення відправника; reset connection — TCP RST надсилається обом сторонам для примусового завершення з'єднання; quarantine — ізоляція підозрілого хосту через зміну VLAN або ACL; rate limit — обмеження швидкості трафіку від підозрілого джерела; alert only — без блокування (режим IDS, корисний для налаштування).

Ризики IPS: хибнопозитивне спрацювання (false positive) може заблокувати легітимний трафік та спричинити відмову в обслуговуванні для корпоративних користувачів. IPS є потенційною точкою відмови (single point of failure) — вихід з ладу без bypass-режиму може повністю зупинити трафік. Для критичних мережевих

сегментів IPS розгортається з fail-open режимом (при відмові IPS пропускає трафік) або резервується у high-availability кластер.

8.3.4. Розгортання IDS/IPS у глобальних мережах

Стратегічні точки розгортання: на Internet edge (між ISP та внутрішньою мережею) — для виявлення зовнішніх загроз і сканування; між DMZ та внутрішньою мережею — для захисту від компрометованих серверів; між підрозділами (east-west трафік) — для виявлення lateral movement при атаках; на WAN-каналах та VPN-концентраторах — для аналізу трафіку від віддалених офісів та мобільних користувачів.

Інтеграція IDS/IPS з іншими системами: SIEM (Security Information and Event Management) — кореляція алертів від IDS/IPS з подіями від firewall, EDR, DNS-логів для виявлення складних атак; SOAR (Security Orchestration, Automation and Response) — автоматизоване реагування на типові інциденти без участі людини; Threat Intelligence Platforms — збагачення алертів контекстом (репутація IP, пов'язані IOC).

Таблиця 8.2 — Порівняльна характеристика IDS та IPS

Характеристика	IDS	IPS
Режим роботи	Пасивний (копія трафіку через SPAN/TAP)	Активний (inline, на шляху трафіку)
Реакція на загрозу	Генерація сповіщення, логування	Автоматичне блокування/модифікація пакетів
Вплив на затримку трафіку	Відсутній (out-of-band)	Мінімальний (мікросекунди–мілісекунди)
Ризик блокування легітимного трафіку	Відсутній	Наявний (false positive → відмова в обслуговуванні)
Вплив виходу з ладу	Втрата моніторингу, трафік не порушується	Потенційне порушення зв'язку (потребує bypass)
Час реагування на загрозу	Хвилини–години (залежить від адміністратора)	Мілісекунди (автоматично)
Типове застосування	Моніторинг, аудит, аналіз інцидентів	Активний захист критичних сегментів мережі

8.4. ГЛИБОКИЙ АНАЛІЗ ПАКЕТІВ (DPI)

Глибокий аналіз пакетів (Deep Packet Inspection, DPI) — це технологія мережевого аналізу, яка дозволяє інспектувати не лише заголовки мережевих пакетів (як це робить традиційна пакетна фільтрація), але й їхній вміст (payload), реасемблювати потоки для аналізу прикладних протоколів та виявляти складні загрози, приховані у легітимному трафіку. DPI є технологічною основою сучасних NGFW, IPS, систем класифікації трафіку та мережевого моніторингу.

8.4.1. Архітектура та технічна реалізація DPI

Технічна реалізація DPI включає кілька послідовних модулів:

- Модуль захоплення пакетів (packet capture) — отримує пакети з мережевого інтерфейсу за допомогою kernel bypass технологій (DPDK, PF_RING, XDP) для забезпечення мінімальних втрат та максимальної продуктивності на швидкостях 10–100 Гбіт/с.

- Модуль реасемблювання (reassembly engine) — збирає фрагментовані IP-пакети, відновлює TCP-потоки з окремих сегментів (TCP stream reassembly), обробляє out-of-order пакети. Це необхідно, оскільки шкідливий вміст може бути розподілений між кількома пакетами для ухилення від виявлення.
- Модуль ідентифікації протоколів (protocol/application identification) — визначає прикладний протокол без прив'язки до номера порту. Сучасні додатки часто використовують нестандартні порти або шифрування для маскування, тому ідентифікація базується на поведінкових патернах та сигнатурах на рівні payload (наприклад, визначення BitTorrent, YouTube, Skype незалежно від порту).
- Модуль аналізу вмісту (content analysis engine) — пошук сигнатур загроз (використовуючи алгоритми Aho-Corasick або PCRE для ефективного пошуку множини патернів), виявлення аномалій, класифікація URL та контенту. Ключовим є використання FPGA (Field-Programmable Gate Arrays) та Network Processing Units (NPU) для апаратного прискорення.
- Модуль прийняття рішень та виконання (policy enforcement) — застосовує правила безпеки: дозволити, заблокувати, перенаправити, обмежити швидкість, записати у лог. Відправляє телеметрію та алерти до SIEM та Threat Intelligence платформ.

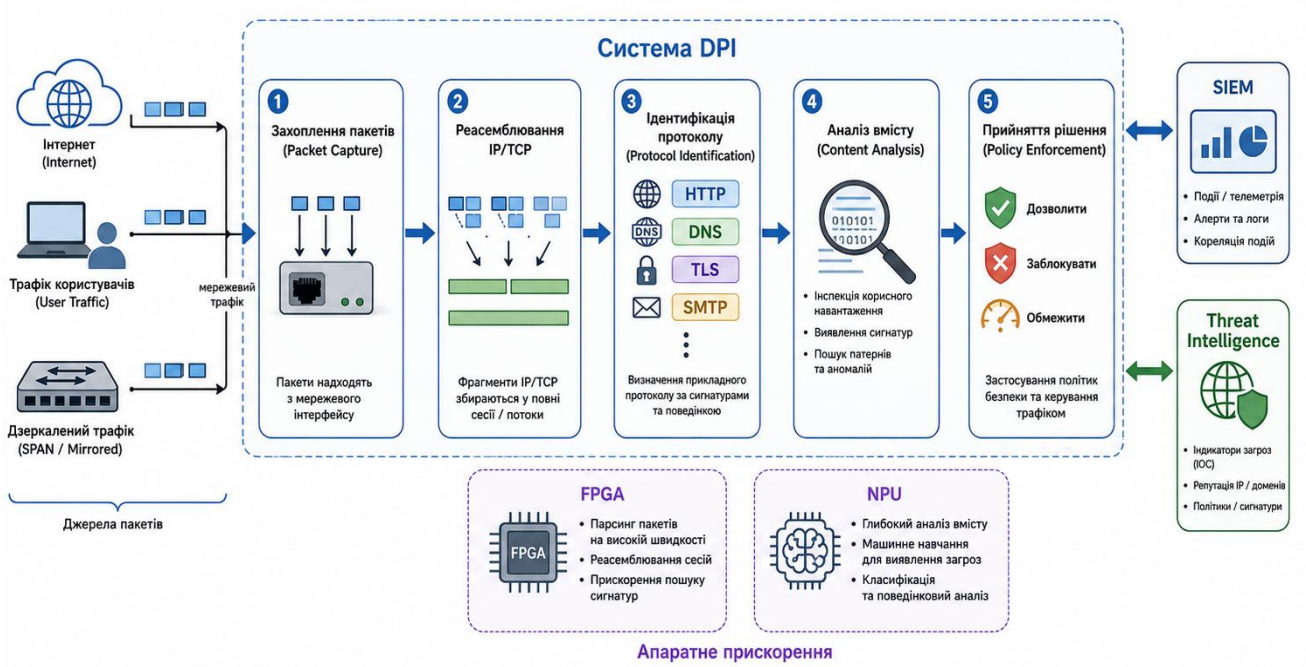

Рисунок 8.3 – Архітектура системи глибокого аналізу пакетів

8.4.2. Обмеження DPI та сучасні виклики

Суттєвим обмеженням DPI є зростаюче використання шифрування трафіку. Понад 90% веб-трафіку у 2020-х роках передається через HTTPS. Протокол TLS 1.3 (RFC 8446) додатково посилив захист приватності, приховавши SNI (Server Name Indication) через ECH (Encrypted Client Hello). Це робить традиційний DPI практично неефективним для зашифрованого трафіку.

TLS-інспекція (SSL inspection, MITM proxy) — DPI-система виступає як man-in-the-middle: встановлює TLS-сесію з клієнтом від імені сервера (підписуючи сертифікат власним CA-сертифікатом, встановленим як довірений) та окрему TLS-сесію з

сервером. Це дозволяє аналізувати розшифрований трафік, але викликає серйозні питання щодо приватності та сумісності з certificate pinning.

Аналіз зашифрованого трафіку (ETA, Encrypted Traffic Analysis) — виявлення загроз без розшифрування на основі метаданих TLS-сесії (розподіл довжин пакетів, міжпакетні інтервали, розмір ClientHello, підтримувані cipher suites, характеристики сертифіката). Cisco ETA та академічні дослідження демонструють можливість ідентифікації шкідливого ПЗ у зашифрованому трафіку з точністю 90%+.

DPI та приватність

Технологія DPI викликає серйозні питання щодо приватності та може порушувати права людини при використанні в авторитарних режимах для цензури та слідкування (DPI-based Great Firewall of China). У демократичних країнах використання DPI операторами регулюється законодавством про net neutrality та захист персональних даних (GDPR у ЄС).

8.5. МІЖМЕРЕЖЕВІ ЕКРАНИ (FIREWALL)

Міжмережевий екран (firewall) є одним із найбільш фундаментальних та найширше використовуваних інструментів мережевої безпеки. Firewall контролює вхідний та вихідний мережевий трафік між мережевими сегментами на основі заздалегідь визначеного набору правил безпеки, забезпечуючи розмежування між зонами з різними рівнями довіри (Інтернет, DMZ, внутрішня мережа).

8.5.1. Еволюція технологій міжмережевих екранів

Перше покоління — пакетні фільтри (кінець 1980-х) — аналізують кожен пакет незалежно від контексту за полями заголовка: IP-адреси джерела та призначення, номери портів, протокол (TCP/UDP/ICMP). Перевага: висока продуктивність, проста конфігурація. Недолік: не враховують стан з'єднання — неможливо відрізнити відповідь на легітимний запит від несанкціонованого вхідного пакета; вразливі до IP spoofing та атак фрагментованими пакетами.

Друге покоління — stateful inspection firewalls (початок 1990-х) — підтримують таблицю стану активних з'єднань (connection state table) та аналізують пакети в контексті з'єднання. Firewall дозволяє відповіді на встановлені з'єднання і блокує несанкціоновані вхідні пакети, навіть якщо вони відповідають базовим правилам пакетного фільтра. Перевага: ефективніший захист, менше правил. Cisco ASA та Juniper SRX є класичними представниками цього покоління.

Третє покоління — проксі-сервери прикладного рівня (ALG) — виконують повний аналіз на рівні прикладних протоколів, включаючи синтаксичний розбір команд. Захищають від атак, прихованих у легітимних протоколах. Недолік: суттєво вища затримка, менша продуктивність.

8.5.2. Міжмережеві екрани нового покоління (NGFW)

Next-Generation Firewalls (NGFW) поєднують функціональність stateful inspection з можливостями DPI, ідентифікацією застосунків та користувачів, вбудованими IPS та інтеграцією з Threat Intelligence. Концепцію NGFW вперше описав Gartner у 2009 році.

Ідентифікація застосунків (App-ID) — визначає конкретний додаток або сервіс незалежно від порту та протоколу. Наприклад, NGFW може відрізнити YouTube від Facebook, дозволивши один і заблокувавши інший, навіть якщо обидва використовують HTTPS/443. Це дозволяє реалізувати policy «allow WebEx, block Zoom» або «allow business apps, block gaming».

Identity Awareness (User-ID) — прив'язка правил безпеки до конкретних користувачів або груп (через інтеграцію з Active Directory, LDAP, SAML, RADIUS). Замість «дозволити IP 10.1.1.5 доступ до 192.168.10.0/24» — «дозволити групі Finance доступ до SAP-сервера».

Вбудована IPS — NGFW виконує функції IPS inline, використовуючи ту ж DPI-інфраструктуру для ідентифікації застосунків і виявлення загроз без додаткової затримки.

TLS-інспекція — дозволяє аналізувати зашифрований трафік, виступаючи як SSL forward proxy. Критично важлива функція, оскільки без неї NGFW «сліпий» до більшості сучасного трафіку.

Інтеграція з Threat Intelligence — автоматичне оновлення правил на основі хмарних баз загроз: репутаційні списки IP та URL, хеші шкідливих файлів, поведінкові патерни зловмисного ПЗ. Palo Alto Networks, Fortinet, Check Point, Cisco Firepower є провідними NGFW-платформами.

Таблиця 8.3 — Порівняння поколінь міжмережевих екранів

Характеристика	Пакетний фільтр	Stateful Inspection	NGFW
Рівень аналізу	L3–L4	L3–L4 + стан з'єднання	L3–L7 (додатки, користувачі)
Ідентифікація застосунків	Ні	Ні (лише за портами)	Так (DPI, App-ID)
Вбудована IPS	Ні	Ні	Так
Identity Awareness	Ні	Ні	Так (AD, LDAP, SAML)
TLS-інспекція	Ні	Обмежена	Так (SSL forward proxy)
Threat Intelligence	Ні	Обмежена	Так (хмарна інтеграція)
Продуктивність	Дуже висока	Висока	Залежить від функцій

8.6. АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ (ZERO TRUST) ДЛЯ WAN

Архітектура нульової довіри (Zero Trust Architecture, ZTA) є фундаментальним переосмисленням підходу до мережевої безпеки, що відмовляється від традиційної периметрової моделі «довіряй всьому всередині мережі, не довіряй нічому зовні». ZTA базується на принципі «never trust, always verify» — кожен запит на доступ до будь-якого ресурсу повинен бути автентифікований, авторизований та постійно перевірений, незалежно від того, чи надходить він з корпоративної мережі, домашнього офісу або публічного Інтернету.

Традиційна периметрова модель («замкова» або castle-and-moat) вважала все, що знаходиться всередині корпоративної мережі, довіреним — після проходження через firewall та VPN. Ця модель виявилася недостатньою в умовах: масового переходу на хмарні сервіси (дані більше не знаходяться «всередині» мережі); широкого розповсюдження BYOD та мобільних пристроїв; збільшення кількості внутрішніх загроз (insider threats); та цільових атак (APT), при яких зловмисник, потрапивши «всередину», може безперешкодно переміщатися lateral movement.

8.6.1. Принципи та архітектура Zero Trust

Модель Zero Trust базується на кількох фундаментальних принципах:

«Ніколи не довіряй, завжди перевіряй» (Never Trust, Always Verify) — кожен запит на доступ повинен проходити автентифікацію та авторизацію незалежно від мережевого розташування суб'єкта.

Принцип мінімальних привілеїв (Least Privilege Access) — суб'єкту надається лише той доступ, що необхідний для виконання конкретного завдання, на мінімально можливий час.

Мікросегментація — мережа поділяється на дрібні ізольовані сегменти з контролем трафіку між ними, що обмежує lateral movement зловмисника у разі компрометації одного вузла.

Постійна верифікація (Continuous Validation) — автентифікація не є одноразовим актом при вході, а постійним процесом. Сесія може бути припинена при виявленні аномальної поведінки.

Припущення про компрометацію (Assume Breach) — система проєктується виходячи з припущення, що зловмисник вже може знаходитися всередині. Це мотивує до сегментації, шифрування всього трафіку (навіть internal east-west) та розгортання систем виявлення аномалій.

Архітектурно Zero Trust складається з двох площин: площина управління (Control Plane) відповідає за автентифікацію, авторизацію та видачу токенів доступу (Policy Decision Point, PDP); площина даних (Data Plane) виконує рішення PDP та пропускає або блокує трафік (Policy Enforcement Point, PEP). Критичні компоненти ZTA: IdP (Identity Provider) для централізованої автентифікації, PKI для управління сертифікатами, MFA (Multi-Factor Authentication), EDR (Endpoint Detection and Response).

8.6.2. Мікросегментація

Мікросегментація є ключовим технічним механізмом реалізації Zero Trust. На відміну від традиційної макросегментації (VLAN, DMZ), що поділяє мережу на великі зони, мікросегментація створює ізольовані сегменти навколо окремих застосунків, сервісів або навіть окремих хостів. Навіть якщо зловмисник скомпрометував один вузол, він не зможе безперешкодно переміщатися до інших ресурсів.

Технічна реалізація: розподілені хостові firewall з централізованим управлінням (VMware NSX, Illumio, Guardicore) — кожен хост має власний набір правил, що контролюється централізовано; програмно-визначені мережі (SDN/NFV) для динамічного сегментування; Identity-based segmentation — сегменти визначаються не IP-адресами, а ідентичністю хосту/процесу/користувача.

8.6.3. Реалізація Zero Trust у WAN: ZTNA та SASE

ZTNA (Zero Trust Network Access) — замінює традиційний VPN для доступу до корпоративних ресурсів. Традиційний VPN надає широкий мережевий доступ після автентифікації (будь-хто в мережі може досягти будь-якого ресурсу). ZTNA, натомість, надає доступ лише до конкретного застосунку на основі ідентичності користувача та стану пристрою. Ресурс не видимий з Інтернету — з'єднання ініціюється з боку клієнта до хмарного брокера (reverse connection), що унеможливлює сканування та DDoS. Приклади: Zscaler Private Access (ZPA), Cloudflare Access, Cisco Duo.

SASE (Secure Access Service Edge) — концепція, запропонована Gartner у 2019 році, що об'єднує функції мережі та безпеки у єдиній хмарній платформі. SASE поєднує: SD-WAN (оптимізація WAN-з'єднань), ZTNA (безпечний доступ до

застосунків), SWG (Secure Web Gateway — захист веб-трафіку), CASB (Cloud Access Security Broker — контроль хмарних сервісів), FWaaS (Firewall as a Service — NGFW у хмарі). Замість традиційної архітектури «backhauling» трафіку від філій до центрального ЦОД через MPLS для інспекції firewall, SASE забезпечує інспекцію безпосередньо у найближчій точці PoP хмарного провайдера. Провідні SASE-платформи: Zscaler, Palo Alto Prisma Access, Cato Networks, Cisco+.

SSE (Security Service Edge)

SSE є підмножиною SASE, що включає лише компоненти безпеки (ZTNA, SWG, CASB, FWaaS) без SD-WAN. Організації, що вже мають розгорнуту SD-WAN-інфраструктуру, можуть доповнити її SSE-рішенням замість повного переходу на SASE.

8.7. ЗАХИСТ ПРОТОКОЛУ BGP

Протокол BGP є критичним компонентом інфраструктури Інтернету — він забезпечує маршрутизацію між тисячами автономних систем, але за своєю початковою конструкцією є надзвичайно довірливим: маршрутизатор приймає анонси BGP-сусіда без будь-якої верифікації права на анонсування конкретних префіксів. Ця архітектурна особливість, що виникла в епоху, коли Інтернет об'єднував лише кількох довірених партнерів, сьогодні є серйозною проблемою безпеки глобального масштабу.

8.7.1. Загрози безпеці BGP

Підміна BGP-партнера (peer spoofing) та TCP Reset атаки — оскільки BGP працює поверх TCP (порт 179) та традиційно не вимагає автентифікації, зловмисник може надіслати підроблений TCP RST-пакет до BGP-сесії, примусово розірвавши її, що призведе до тимчасової втрати маршрутів та перебоїв у з'язності.

BGP hijacking (викрадення маршрутів) — зловмисник анонсує чужі IP-префікси, спрямовуючи трафік через свою інфраструктуру. Анонсування більш специфічного маршруту (наприклад, /24 замість /16) є достатньо, щоб у більшості AS трафік пішов через зловмисника. Метою може бути: перехоплення трафіку для шпигунства, відмова в обслуговуванні (трафік спрямовується в null route), фішинг (підробка DNS відповідей для перехопленого трафіку).

Route leaks (витоки маршрутів) — помилкове (часто ненавмисне) розповсюдження маршрутів, отриманих від одного провайдера, іншому провайдеру. Класичний приклад: клієнт AS отримує повну таблицю від провайдера A і помилково рекламує її провайдеру B, ставши «транзитом» між двома великими операторами — і перевантажуючись трафіком, для якого не має достатньо ресурсів.

Route flapping — повторювана зміна стану маршруту (нестабільний BGP-сусід, що постійно підключається та відключається) може перевантажити CPU маршрутизаторів та перешкодити конвергенції. Механізм Route Flap Damping (RFC 2439) пригнічує нестабільні маршрути, хоча його агресивне застосування може затримувати відновлення після реальних відмов.

8.7.2. Механізми захисту BGP-сесій

MD5-автентифікація (RFC 2385) — додає криптографічний HMAC-MD5 до кожного TCP-сегмента BGP-сесії. Захищає від підміни та модифікації повідомлень, але MD5 вважається криптографічно слабким. Рекомендується використовувати TCP-AO (TCP Authentication Option, RFC 5925), що підтримує сильніші алгоритми (HMAC-SHA1, HMAC-SHA256) та захищає від атак повтором.

GTSM (Generalized TTL Security Mechanism, RFC 3682) — встановлює TTL=255 у вихідних BGP-пакетах. Оскільки BGP-партнери зазвичай є безпосередніми сусідами (або знаходяться на відстані 1–2 стрибки), пакет від легітимного партнера дійде з TTL≥254. Пакети з нижчим TTL відкидаються як потенційно підроблені. Простий та ефективний захист від атак з відстані більше одного хопа.

Обмеження кількості маршрутів (maximum-prefix) — обмеження максимальної кількості префіксів, що приймаються від BGP-сусіда. При перевищенні ліміту сесія скидається або переходить в режим тільки-сповіщення. Захищає від випадкового або навмисного заповнення таблиці маршрутизації.

8.7.3. RPKI та валідація маршрутів

Інфраструктура відкритих ключів ресурсів (Resource Public Key Infrastructure, RPKI, RFC 6480) створює криптографічно верифіковану прив'язку між IP-префіксами та автономними системами через Route Origin Authorization (ROA). **ROA** — це підписаний запис, що містить: IP-префікс, ASN, якому дозволено анонсувати цей префікс, та максимальну довжину префіксу (max-length).

RPKI Route Origin Validation (ROV) — процес перевірки BGP-анонсів відповідно до опублікованих ROA. Маршрут може мати статус Valid (є ROA, ASN та довжина префіксу збігаються), Invalid (є ROA, але ASN або довжина не збігаються — ймовірний hijack), NotFound (немає ROA для цього префіксу). Більшість операторів налаштовані на відхилення Invalid-маршрутів та прийняття Valid і NotFound. За даними RIPE NCC, станом на 2024 рік близько 40% IPv4-маршрутів мають відповідний ROA, і частка зростає.

BGPsec (RFC 8205) є перспективним розширенням, що забезпечує криптографічну верифікацію не лише походження маршруту, а й всього AS-шляху. Кожна AS підписує своє оголошення маршруту, і отримувач може верифікувати, що маршрут дійсно пройшов через зазначені AS у зазначеному порядку. BGPsec є значно складнішим у впровадженні, ніж RPKI (потребує оновлення BGP-стека на кожному маршрутизаторі в шляху), тому його широке розгортання очікується не раніше кінця 2020-х років.

8.7.4. Фільтрація префіксів та найкращі практики

Фільтрація префіксів є базовим механізмом захисту BGP. Стратегія відповідно до NIST SP 800-54 включає: блокування спеціальних адрес (RFC 1918 — 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16; loopback 127.0.0.0/8; link-local 169.254.0.0/16; multicast 224.0.0.0/4; документальні 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24); фільтрація надмірно специфічних префіксів (довший за /24 для IPv4 або /48 для IPv6); прийняття від клієнтів лише їхніх власних префіксів (через IRR-фільтри або RPKI).

Механізми стійкості BGP: Graceful Restart (RFC 4724) — дозволяє маршрутизатору відновлюватися після перезавантаження без повної втрати маршрутів; BFD (Bidirectional Forwarding Detection, RFC 5880) — швидке виявлення відмов між BGP-сусідами (10–100 мс замість типового Hold Timer 90–180 с); ECMP та multipath для балансування навантаження між кількома BGP-шляхами; моніторинг BGP-оголошень через Route Views, RIPE RIS, BGPmon для своєчасного виявлення hijacking.

Контрольні питання

1. Класифікуйте загрози глобальних мереж за характером впливу, рівнем OSI та джерелом. Наведіть приклади для кожної категорії.
2. У чому полягає відмінність між пасивними та активними атаками? Чому пасивні атаки часто важче виявити?
3. Опишіть механізм атаки BGP hijacking. Наведіть реальний приклад та поясніть, як RPKI/ROA захищає від неї.
4. Опишіть механізм атаки з ампліфікацією (reflection/amplification). Які протоколи найчастіше використовуються як рефлектори та які коефіцієнти ампліфікації вони забезпечують?
5. Що таке ботнет і яку роль він відіграє у DDoS-атаках? Порівняйте централізовану C&C архітектуру з P2P та DGA.
6. Порівняйте три категорії DDoS-атак (волюметричні, протокольні, прикладні) за рівнем OSI, потужністю та складністю виявлення.
7. Поясніть принцип роботи blackhole routing (RTBH) та BGP Flowspec. В яких сценаріях кожен із цих механізмів є переважним?
8. Поясніть принцип роботи scrubbing center для захисту від DDoS. Як трафік перенаправляється до центру очищення і назад?
9. У чому полягає різниця між IDS та IPS? Опишіть ризики хибнопозитивних спрацювань для кожного типу системи.
10. Порівняйте сигнатурний та аномальний методи виявлення вторгнень за точністю, обчислювальними витратами та здатністю виявляти zero-day атаки.
11. Опишіть архітектуру DPI-системи. Яку роль відіграють модулі реасемблювання, ідентифікації протоколів та аналізу вмісту?
12. Як впливає шифрування трафіку (TLS 1.3, ECH) на ефективність DPI? Опишіть підхід TLS-інспекції та пов'язані ризики для приватності.
13. Опишіть еволюцію міжмережевих екранів від пакетних фільтрів до NGFW. Які ключові можливості з'явилися на кожному поколінні?
14. Сформулюйте п'ять основних принципів архітектури Zero Trust. Чому традиційна периметрова модель безпеки є недостатньою?
15. Поясніть відмінність між ZTNA та традиційним VPN. Чому ZTNA вважається безпечнішим підходом для сучасних гібридних середовищ?
16. Що таке SASE? Які компоненти воно об'єднує та яку архітектурну проблему вирішує для організацій із розподіленими філіями?
17. Назвіть основні загрози безпеці BGP. Чому протокол BGP є таким вразливим за своєю природою?
18. Як працює RPKI та яку роль відіграє ROA у валідації маршрутів? Що означають статуси Valid, Invalid та NotFound?
19. Опишіть механізм GTSM (TTL security hack) для захисту BGP-сесій. Від яких атак він захищає і в чому його обмеження?
20. Поясніть концепцію ZTNA (Zero Trust Network Access) та її переваги над традиційним VPN. Як ZTNA реалізує принцип найменших привілеїв для віддаленого доступу?

РОЗДІЛ 9

МОНІТОРИНГ ТА ОПТИМІЗАЦІЯ МЕРЕЖ

У цьому розділі розглядаються основні технології та підходи, що використовуються для моніторингу й оптимізації глобальних мереж: SNMP для збору параметрів роботи обладнання, NetFlow та IPFIX для аналізу мережевих потоків, Syslog для централізованого збирання журналів подій, системи управління мережею, засоби аналізу трафіку, механізми балансування навантаження та архітектури високої доступності.

Сучасні глобальні мережі є складними багаторівневими системами, у яких одночасно функціонують маршрутизатори, комутатори, міжмережеві екрани, балансувальники навантаження, сервери, хмарні сервіси та засоби захисту інформації. Для забезпечення стабільної роботи такої інфраструктури недостатньо лише правильно спроєктувати мережу. Необхідно постійно контролювати її стан, своєчасно виявляти відмови, аналізувати трафік, оцінювати продуктивність каналів і прогнозувати можливі перевантаження.

Моніторинг мережі — це процес безперервного спостереження за станом мережевих пристроїв, каналів зв'язку, сервісів і прикладних систем. Його основним завданням є своєчасне виявлення несправностей, зниження тривалості простоїв, підвищення надійності інфраструктури та забезпечення відповідності фактичних параметрів роботи мережі встановленим вимогам.

Оптимізація мережі передбачає аналіз зібраних даних і внесення змін до конфігурації, топології або політик обслуговування трафіку з метою підвищення продуктивності, відмовостійкості та безпеки. До таких змін можуть належати перерозподіл трафіку між каналами, налаштування пріоритетів QoS, впровадження балансування навантаження, резервування критичних компонентів, оновлення правил фільтрації та коригування маршрутної політики.

Ключова ідея

Моніторинг і оптимізація мережі забезпечують перехід від реактивного адміністрування, коли проблема усувається лише після її появи, до проактивного управління, коли потенційні збої виявляються заздалегідь на основі аналізу показників, журналів подій і мережевих потоків.

9.1. SNMP — ПРОТОКОЛ УПРАВЛІННЯ МЕРЕЖАМИ

SNMP (Simple Network Management Protocol) — це один із найпоширеніших протоколів для моніторингу та управління мережевим обладнанням. Він використовується для отримання інформації про стан маршрутизаторів, комутаторів, серверів, міжмережевих екранів, безперебійних джерел живлення, точок доступу та інших пристроїв, що підтримують мережеве адміністрування.

Основне призначення SNMP полягає у збиранні параметрів роботи обладнання та передаванні їх до системи моніторингу. За допомогою цього протоколу адміністратор може отримувати відомості про завантаження процесора, використання оперативної пам'яті, стан інтерфейсів, кількість переданих і прийнятих пакетів, помилки на портах, температуру обладнання, стан блоків живлення та інші важливі показники.

SNMP застосовується як у невеликих локальних мережах, так і в масштабних операторських і корпоративних інфраструктурах. Його перевагою є широка підтримка виробниками обладнання, відносна простота впровадження та можливість інтеграції з більшістю систем управління мережею.

9.1.1. Архітектура SNMP

Архітектура SNMP базується на взаємодії трьох основних компонентів:

- керуючої системи;
- агента SNMP;
- бази керуючої інформації MIB.

Керуюча система — це програмний комплекс, який здійснює моніторинг мережі. Вона надсилає запити до пристроїв, отримує відповіді, зберігає зібрані дані, формує графіки, сповіщення та звіти. Прикладами таких систем є Zabbix, PRTG, LibreNMS, Nagios, SolarWinds та інші платформи моніторингу.

Агент SNMP — це програмний компонент, що працює на мережевому пристрої. Він збирає локальну інформацію про стан обладнання та надає її керуючій системі у відповідь на запити. Агент може також самостійно надсилати повідомлення про важливі події, наприклад про відмову інтерфейсу, перевищення температури або перезавантаження пристрою.

MIB (Management Information Base) — це структурована база керуючої інформації, у якій описано параметри, доступні для моніторингу. Кожен параметр має унікальний ідентифікатор OID (Object Identifier). За допомогою OID система моніторингу звертається до конкретного показника, наприклад до лічильника трафіку на інтерфейсі або до значення завантаження процесора.

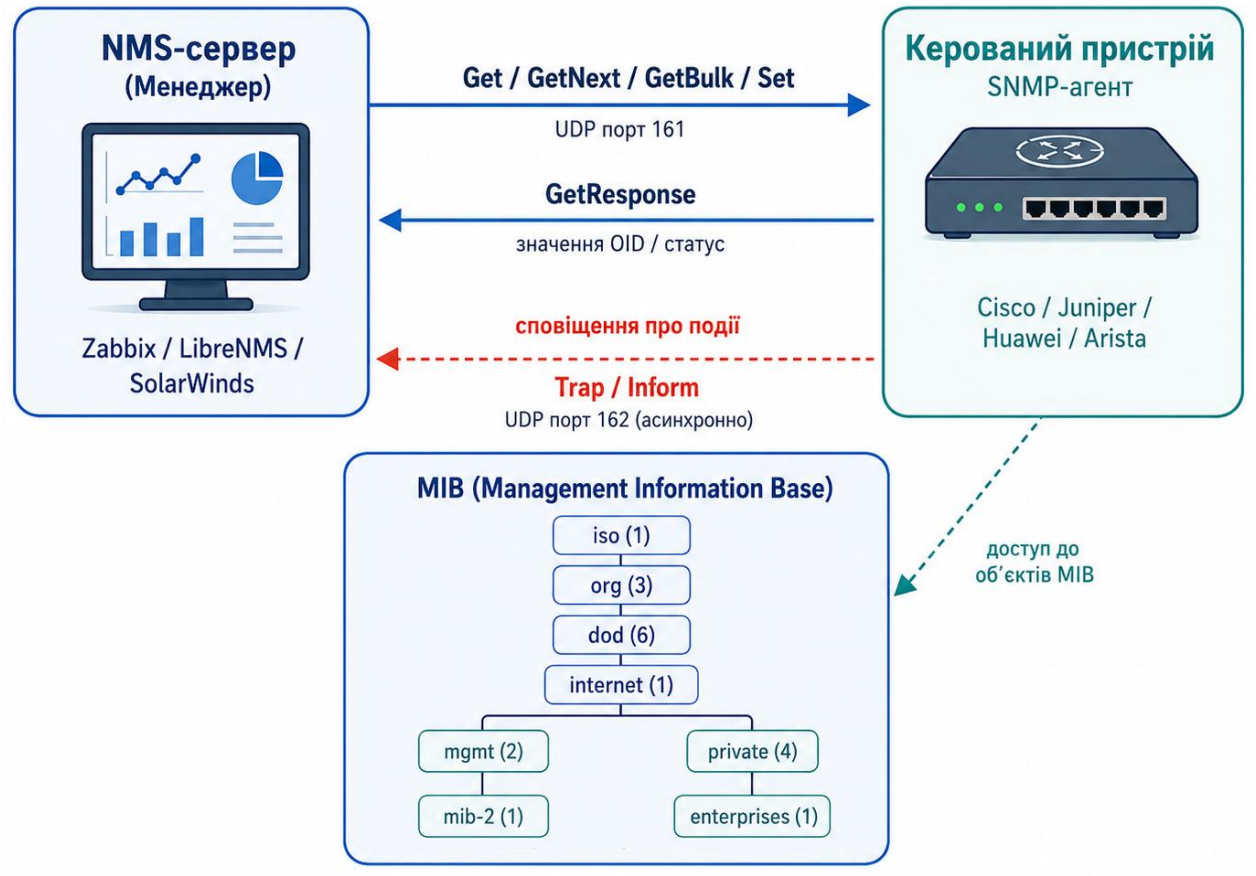

Рисунок 9.1 – Архітектура SNMP: взаємодія Менеджера, Агента та MIB

9.1.2. Основні операції SNMP

У SNMP використовуються кілька базових типів операцій, за допомогою яких керуюча система отримує або змінює дані на пристрої.

Операція **Get** використовується для отримання значення конкретного параметра. Наприклад, система моніторингу може запитати поточний стан інтерфейсу або кількість байтів, переданих через порт.

Операція **GetNext** дозволяє послідовно переглядати об’єкти в дереві MIB. Вона корисна тоді, коли потрібно отримати набір пов’язаних параметрів, наприклад інформацію про всі інтерфейси пристрою.

Операція **GetBulk** з’явилася у SNMPv2 і використовується для ефективного отримання великої кількості даних за один запит. Це зменшує навантаження на мережу та прискорює збір інформації з пристроїв, які мають багато інтерфейсів або параметрів.

Операція **Set** використовується для зміни значення певного параметра на пристрої. У практиці адміністрування ця операція застосовується обережно, оскільки неправильна зміна параметрів може порушити роботу обладнання. У багатьох мережах SNMP використовується лише для читання, а зміни конфігурації виконуються іншими засобами.

Окрему роль відіграють повідомлення **Trap** та **Inform**. Повідомлення Trap надсилається агентом до керуючої системи у разі виникнення події. Наприклад, пристрій може повідомити про відмову інтерфейсу, втрату живлення або перевищення критичного порогу температури. Повідомлення Inform також передає інформацію про подію, але передбачає підтвердження отримання з боку керуючої системи, що робить його надійнішим.

9.1.3. Версії SNMP

Існує кілька основних версій SNMP: SNMPv1, SNMPv2c та SNMPv3.

SNMPv1 є першою версією протоколу. Вона має просту структуру та підтримується багатьма пристроями, однак не забезпечує належного рівня безпеки. Для доступу використовується рядок спільноти, який фактично виконує роль простого пароля. Оскільки цей рядок передається мережею без захисту, SNMPv1 не рекомендується використовувати в сучасних захищених мережах.

SNMPv2c розширює можливості першої версії, зокрема додає операцію GetBulk, що підвищує ефективність отримання великих обсягів даних. Проте механізм безпеки у SNMPv2c залишається таким самим, як у SNMPv1: використовується рядок спільноти без шифрування. Тому SNMPv2c можна застосовувати лише в ізольованих або додатково захищених сегментах мережі.

SNMPv3 є сучасною та найбільш безпечною версією протоколу. Вона підтримує автентифікацію користувачів, контроль цілісності повідомлень і шифрування. Завдяки цьому SNMPv3 є рекомендованим варіантом для використання в корпоративних і операторських мережах, особливо тоді, коли моніторинг здійснюється через незахищені або спільні канали зв’язку.

9.1.4. MIB та OID

База керуючої інформації MIB має ієрархічну структуру у вигляді дерева. У цьому дереві кожен об’єкт має власний унікальний ідентифікатор OID. Такий підхід дозволяє однозначно визначати параметри різних пристроїв і виробників.

Наприклад, один OID може відповідати назві пристрою, інший — часу його роботи після останнього перезавантаження, ще інший — кількості помилок на певному інтерфейсі. Система моніторингу не обов'язково повинна знати внутрішню логіку роботи пристрою. Їй достатньо звернутися до потрібного OID і отримати значення відповідного параметра.

Для стандартних параметрів використовуються загальновідомі MIB-модулі, які підтримуються більшістю виробників. Водночас виробники мережевого обладнання можуть створювати власні MIB-модулі для специфічних функцій. Наприклад, окремі OID можуть описувати стан вентиляторів, блоків живлення, оптичних модулів, температурних датчиків або ліцензійних функцій пристрою.

У практичній роботі адміністратор часто використовує MIB-браузер або засоби системи моніторингу для перегляду доступних OID і вибору параметрів, які потрібно контролювати.

9.1.5. Використання SNMP у моніторингу мережі

SNMP найчастіше використовується для регулярного опитування пристроїв. Система моніторингу з певним інтервалом надсилає запити до агентів SNMP і отримує поточні значення параметрів. На основі цих даних будуються графіки, визначаються порогові значення, формуються попередження та звіти.

Типовими показниками, які збираються за допомогою SNMP, є:

- стан мережевих інтерфейсів;
- завантаження процесора;
- використання оперативної пам'яті;
- обсяг переданого й прийнятого трафіку;
- кількість помилок і відкинутих пакетів;
- температура обладнання;
- стан блоків живлення та вентиляторів;
- час безперервної роботи пристрою;
- стан оптичних модулів і рівні оптичного сигналу.

На основі цих показників адміністратор може виявити перевантаження каналу, деградацію фізичного з'єднання, нестачу ресурсів пристрою, нестабільну роботу інтерфейсу або інші проблеми, що впливають на якість роботи мережі.

Наприклад, якщо кількість помилок на інтерфейсі постійно зростає, це може свідчити про несправний кабель, пошкоджений оптичний модуль, неправильне узгодження швидкості або фізичну деградацію лінії. Якщо завантаження процесора маршрутизатора тривалий час перебуває на високому рівні, це може вказувати на надмірне навантаження, некоректну конфігурацію або аномальний трафік.

9.1.6. Переваги та обмеження SNMP

До основних переваг SNMP належать простота впровадження, широка підтримка обладнанням різних виробників, можливість централізованого моніторингу та придатність для тривалого збору статистики. Протокол дозволяє швидко отримати базову інформацію про стан мережі без встановлення додаткового програмного забезпечення на більшість мережевих пристроїв.

Водночас SNMP має певні обмеження. По-перше, він не призначений для глибокого аналізу вмісту трафіку. SNMP показує значення лічильників і станів, але не

пояснює, які саме застосунки або користувачі створюють навантаження. Для цього використовуються технології аналізу потоків, зокрема NetFlow та IPFIX.

По-друге, часте опитування великої кількості пристроїв може створювати додаткове навантаження на систему моніторингу й самі пристрої. Тому інтервали опитування потрібно налаштовувати з урахуванням важливості параметрів і масштабу мережі.

По-третє, використання SNMPv1 і SNMPv2c пов'язане з ризиками безпеки, оскільки ці версії не забезпечують повноцінного захисту переданих даних. У сучасних мережах доцільно застосовувати SNMPv3, обмежувати доступ до SNMP лише з адрес систем моніторингу та використовувати фільтрацію на міжмережевих екранах або списках контролю доступу.

9.1.7. Рекомендації щодо безпечного використання SNMP

Для безпечного використання SNMP у корпоративних і операторських мережах доцільно дотримуватися таких рекомендацій.

Насамперед варто використовувати SNMPv3, оскільки ця версія підтримує автентифікацію та шифрування. Якщо з технічних причин доводиться застосовувати SNMPv2c, потрібно обмежити доступ до протоколу лише з визначених адрес систем моніторингу.

Необхідно змінювати стандартні рядки спільноти, зокрема public і private, оскільки вони є типовими й добре відомими. Такі значення не повинні використовуватися у робочих мережах.

Доступ на запис через SNMP бажано вимикати, якщо він не є необхідним. У більшості випадків для моніторингу достатньо доступу лише на читання. Це зменшує ризик несанкціонованої зміни параметрів пристрою.

Також доцільно використовувати окрему мережу управління або окремий захищений сегмент для систем моніторингу. Це дозволяє ізолювати службовий трафік від користувацького та зменшити ризик перехоплення або підміни даних.

Крім того, потрібно регулярно перевіряти, які саме пристрої доступні за SNMP, які версії протоколу вони використовують і чи не залишилися на них небезпечні стандартні налаштування.

9.1.8. Місце SNMP у сучасній системі моніторингу

Попри появу нових підходів до спостереження за інфраструктурою, SNMP залишається важливою складовою моніторингу мереж. Його часто використовують разом з іншими джерелами даних: журналами подій Syslog, потоковою статистикою NetFlow/IPFIX, даними телеметрії та показниками прикладних сервісів.

У сучасній інфраструктурі SNMP доцільно розглядати як базовий механізм збору технічних параметрів обладнання. Він добре підходить для контролю стану інтерфейсів, ресурсів пристрою, апаратних компонентів і загальних показників доступності. Однак для повного розуміння роботи мережі SNMP потрібно доповнювати іншими інструментами, які дозволяють аналізувати характер трафіку, події безпеки, продуктивність сервісів і поведінку користувачів.

Таким чином, SNMP є не самостійним універсальним рішенням, а важливим елементом комплексної системи моніторингу, яка поєднує збір параметрів обладнання, аналіз мережевих потоків, централізоване зберігання журналів подій і візуалізацію стану інфраструктури.

9.2. NETFLOW — ТЕХНОЛОГІЯ АНАЛІЗУ МЕРЕЖЕВИХ ПОТОКІВ

NetFlow — це технологія аналізу мережевого трафіку, розроблена компанією Cisco для збирання статистики про IP-потоки, що проходять через мережеве обладнання. На відміну від SNMP, який переважно працює з агрегованими лічильниками інтерфейсів, NetFlow дозволяє отримати значно детальнішу інформацію: хто з ким обмінювався даними, через які порти, яким протоколом, у якому обсязі та протягом якого часу.

Мережевий потік у NetFlow — це сукупність пакетів, які мають спільні ознаки та розглядаються обладнанням як один логічний обмін даними. Наприклад, потік може відповідати з'єднанню між клієнтом і сервером, передаванню даних між двома вузлами або окремому типу трафіку в межах корпоративної чи операторської мережі.

Основна цінність NetFlow полягає в тому, що ця технологія дозволяє перейти від загального спостереження за завантаженням інтерфейсів до розуміння реальної структури трафіку. Якщо SNMP показує, що на певному інтерфейсі зросло навантаження, то NetFlow дозволяє з'ясувати, які саме вузли, протоколи або сервіси спричинили це зростання.

NetFlow широко використовується для моніторингу глобальних мереж, планування пропускної здатності, виявлення аномалій, аналізу інцидентів безпеки, оптимізації маршрутизації та контролю якості обслуговування. Подібні технології реалізовані також в обладнанні інших виробників: J-Flow у Juniper, NetStream у Huawei, Cflowd у Nokia, а також у стандартизованому підході IPFIX.

9.2.1. Принцип роботи NetFlow

Робота NetFlow базується на аналізі пакетів, що проходять через мережевий пристрій. Маршрутизатор або комутатор перевіряє заголовки пакетів, визначає належність пакета до певного потоку та створює запис про цей потік у спеціальній таблиці.

У класичному варіанті NetFlow потік визначається за сімома ключовими полями:

- IP-адреса джерела;
- IP-адреса призначення;
- порт джерела;
- порт призначення;
- номер протоколу транспортного рівня;
- тип сервісу або значення поля ToS/DSCP;
- вхідний інтерфейс.

Якщо новий пакет має ті самі значення ключових полів, що й уже наявний запис, він зараховується до відповідного потоку. Якщо хоча б одне ключове поле відрізняється, створюється новий запис потоку.

Для кожного потоку обладнання накопичує статистику: кількість пакетів, кількість байтів, час початку та завершення потоку, вхідний і вихідний інтерфейси, TCP-прапорці, інформацію про автономні системи, маски мереж та інші параметри залежно від версії NetFlow і налаштувань пристрою.

Типовий процес роботи NetFlow складається з таких етапів:

- пакет надходить на інтерфейс мережевого пристрою;
- пристрій аналізує заголовки пакета;

- визначається, чи належить пакет до вже відомого потоку;
- якщо потік існує, оновлюються його лічильники;
- якщо потоку ще немає, створюється новий запис;
- після завершення або неактивності потоку запис експортується до колектора;
- колектор зберігає, обробляє та візуалізує отримані дані.

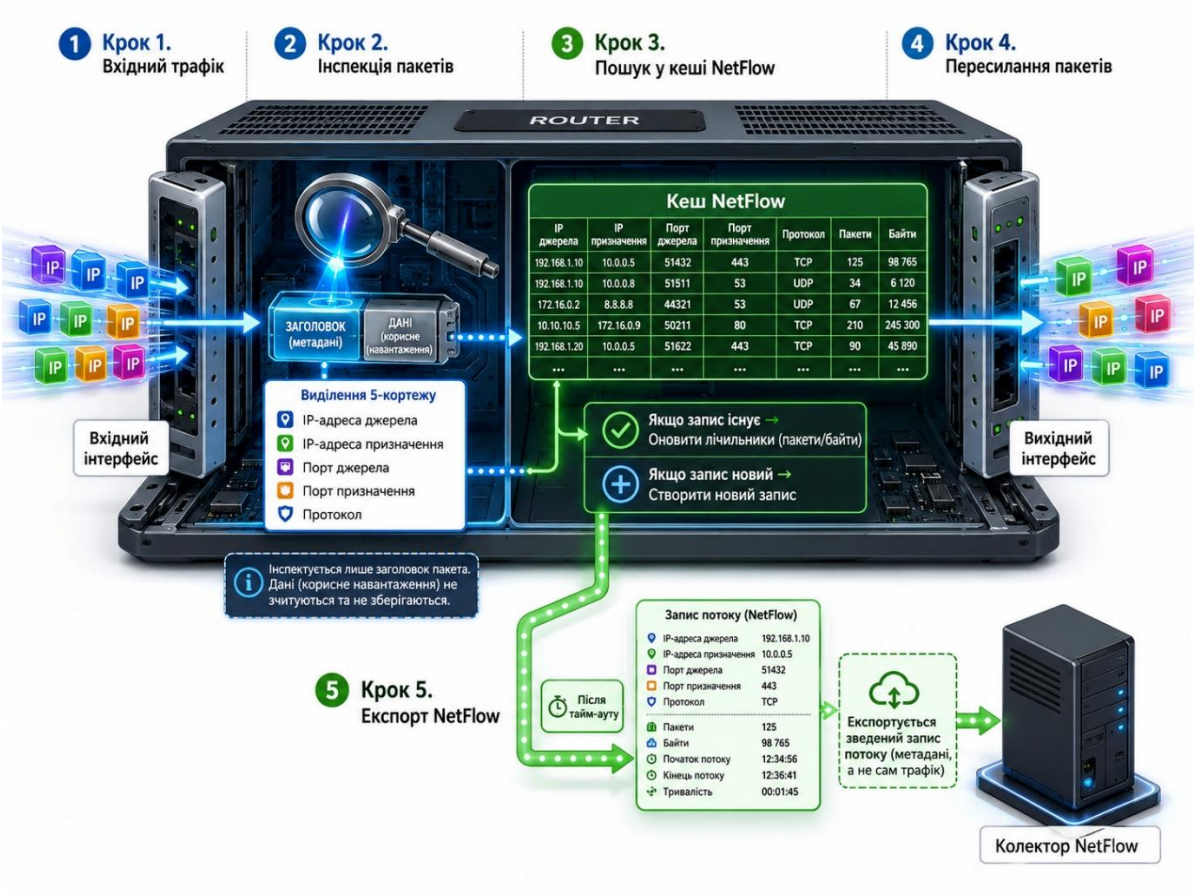

Рисунок 9.2 – Інспекція пакетів та створення NetFlow-записів

9.2.2. Кеш NetFlow та завершення потоків

Кеш NetFlow — це тимчасова таблиця, у якій мережевий пристрій зберігає активні записи потоків. Кожен запис існує доти, доки потік залишається активним або поки не спрацює одна з умов завершення.

Потік може бути завершений у кількох випадках. Найпоширенішою умовою є неактивність: якщо протягом певного часу для потоку не надходять нові пакети, пристрій вважає його завершеним і експортує відповідний запис. Іншою умовою є досягнення максимального часу існування активного потоку. Це потрібно для того, щоб довгі з'єднання, наприклад передавання великих файлів або тривалі сеанси, періодично експортувалися до колектора й були видимими в системі аналізу.

Також потік може завершуватися після виявлення TCP-прапорців FIN або RST, які свідчать про завершення або примусове розірвання TCP-з'єднання. У деяких випадках записи експортуються також у разі переповнення кешу або зміни конфігурації NetFlow.

Правильне налаштування часу активності та неактивності потоків має важливе значення. Якщо інтервали надто короткі, колектор отримуватиме велику кількість дрібних записів, що збільшить навантаження на систему аналізу. Якщо інтервали

надто довгі, інформація про потоки надходитиме із затримкою, що ускладнить оперативне виявлення проблем.

9.2.3. Основні компоненти NetFlow

Типова архітектура NetFlow складається з трьох основних компонентів:

- експортера;
- колектора;
- системи аналізу.

Експортер — це мережевий пристрій, який аналізує трафік, створює записи потоків і надсилає їх до колектора. Зазвичай експортерами є маршрутизатори, комутатори рівня L3, міжмережеві екрани або інші пристрої, через які проходить значний обсяг трафіку.

Колектор — це сервер або програмний компонент, який приймає записи NetFlow від одного чи кількох експортерів. Його завдання полягає у прийманні даних, перевірці їхньої цілісності, збереженні в базі даних і підготовці до подальшої обробки.

Система аналізу забезпечує інтерпретацію зібраної інформації. Вона будує графіки, формує звіти, визначає найбільших споживачів трафіку, виявляє аномальні потоки, допомагає аналізувати інциденти та оцінювати завантаження мережі.

У великих мережах колектори можуть обробляти дані від десятків або сотень експортерів. Тому важливо правильно планувати обсяг збереження даних, продуктивність серверів, період зберігання історії та механізми фільтрації або вибіркового збору трафіку.

9.2.4. Flexible NetFlow

Flexible NetFlow — це розвиток класичної технології NetFlow, який забезпечує гнучкіше визначення потоків і розширені можливості аналізу трафіку. На відміну від ранніх версій NetFlow, де набір полів був фіксованим, Flexible NetFlow дозволяє адміністратору самостійно визначати, які параметри пакета будуть використовуватися для ідентифікації потоку, а які — для збирання додаткової статистики.

У Flexible NetFlow використовуються три основні логічні компоненти:

- запис потоку;
- експортер;
- монітор потоку.

Запис потоку визначає, які поля будуть ключовими, а які — інформаційними. Ключові поля використовуються для визначення належності пакетів до одного потоку. Інформаційні поля зберігають додаткові дані, наприклад кількість байтів, кількість пакетів, час початку і завершення потоку, значення DSCP або інформацію про інтерфейси.

Експортер визначає, куди і як потрібно надсилати зібрані записи. У його налаштуваннях зазначається адреса колектора, транспортний протокол, номер порту, версія експорту та інші параметри передавання даних.

Монітор потоку об’єднує запис потоку та експортер, а потім застосовується до певного інтерфейсу у вхідному або вихідному напрямку. Саме монітор визначає, який трафік буде аналізуватися та які записи будуть створюватися.

Гнучкість Flexible NetFlow особливо корисна в сучасних мережах, де потрібно аналізувати не лише класичні IP-потоки, а й трафік із позначками QoS, VLAN, MPLS, IPv6 або специфічними полями, важливими для безпеки й оптимізації маршрутизації.

Наприклад, адміністратор може налаштувати аналіз трафіку за IP-адресами джерела й призначення, значенням DSCP та вхідним інтерфейсом. Це дозволить оцінити, як у мережі передається трафік різних класів обслуговування. В іншому випадку можна додати поля, пов'язані з BGP, щоб аналізувати трафік між автономними системами.

9.2.5. Версії NetFlow та IPFIX

Існує кілька основних версій NetFlow, серед яких найбільш відомими є NetFlow v5 і NetFlow v9.

NetFlow v5 є однією з найпоширеніших класичних версій. Вона використовує фіксований формат запису та добре підходить для базового аналізу IPv4-трафіку. До запису можуть входити адреси джерела й призначення, порти, протокол, кількість пакетів і байтів, час початку та завершення потоку, інтерфейси, TCP-прапорці та інші параметри.

Недоліком NetFlow v5 є обмежена гнучкість. Через фіксований формат ця версія не підтримує повноцінний опис IPv6, MPLS-міток, розширених BGP-полів та інших сучасних параметрів. Тому для складних операторських і корпоративних мереж NetFlow v5 часто є недостатнім.

NetFlow v9 став важливим кроком уперед завдяки використанню шаблонного підходу. Замість фіксованого набору полів пристрій може надсилати колектору шаблон, який описує структуру майбутніх записів. Після цього колектор використовує отриманий шаблон для правильного тлумачення даних.

Шаблонний підхід дає змогу одному колектору приймати записи з різними наборами полів від різних пристроїв. Завдяки цьому NetFlow v9 підтримує IPv6, MPLS, VLAN, BGP, багатоадресний трафік та інші розширені параметри. Саме NetFlow v9 став основою для Flexible NetFlow.

IPFIX (IP Flow Information Export) — це стандартизований підхід до експорту інформації про IP-потоки, розроблений IETF на основі ідей NetFlow v9. Його можна розглядати як відкритий стандарт для передавання даних про мережеві потоки між експортерами та колекторами. IPFIX зберігає шаблонну логіку, але формалізує її у вигляді стандарту, придатного для обладнання різних виробників.

9.2.6. Структура пакета NetFlow v9

NetFlow v9 використовує шаблонну структуру передавання даних. Це означає, що колектор спочатку отримує опис формату запису, а вже потім — самі дані, які відповідають цьому опису.

Пакет NetFlow v9 складається із загального заголовка та одного або кількох наборів даних. Заголовок містить службову інформацію, необхідну для обробки пакета: номер версії, кількість наборів, час роботи пристрою, часову мітку, номер послідовності та ідентифікатор джерела.

Після заголовка передаються набори даних. Вони можуть містити:

- шаблон запису;
- записи потоків за відповідним шаблоном;
- шаблон параметрів;
- службові або додаткові дані.

Шаблон запису описує, які поля будуть міститися в подальших записах потоків. Наприклад, шаблон може вказувати, що запис містить IP-адресу джерела, IP-адресу призначення, кількість пакетів, кількість байтів, вхідний інтерфейс і значення DSCP.

Записи потоків містять фактичні значення відповідно до раніше переданого шаблону. Якщо колектор не отримав або втратив шаблон, він не зможе правильно інтерпретувати відповідні записи. Саме тому шаблони періодично надсилаються повторно.

Шаблони параметрів використовуються для передавання додаткової службової інформації, наприклад параметрів вибіркового збору трафіку або опису інтерфейсів.

9.2.7. Вибірковий збір трафіку

У великих мережах повний аналіз кожного пакета може створювати значне навантаження на мережеве обладнання та систему збору статистики. Тому в операторських і магістральних мережах часто застосовується вибірковий збір трафіку.

Вибірковий збір означає, що пристрій аналізує не всі пакети, а лише певну їх частину. Наприклад, може оброблятися кожен сотий або кожен тисячний пакет. На основі такого зразка система оцінює загальну структуру трафіку.

Перевагою цього підходу є зниження навантаження на обладнання, зменшення обсягу записів і можливість застосування NetFlow у мережах з дуже високою пропускною здатністю. Недоліком є нижча точність, особливо для малих або короткочасних потоків.

Вибірковий збір доцільно використовувати для аналізу загальних тенденцій, планування пропускної здатності та оцінювання структури трафіку. Якщо ж потрібно детально розслідувати інцидент безпеки або дослідити короткочасну аномалію, бажано використовувати повніший збір даних або додаткові інструменти аналізу.

9.2.8. Використання NetFlow у моніторингу та безпеці

NetFlow має широкий спектр практичного застосування. Одним із головних напрямів є аналіз використання пропускної здатності. За допомогою NetFlow можна визначити, які вузли, сервіси або підмережі створюють найбільше навантаження на канали зв’язку. Це допомагає планувати розширення каналів, оптимізувати маршрутизацію та обґрунтовувати модернізацію інфраструктури.

Іншим важливим напрямом є виявлення аномалій. Нетипове зростання кількості потоків, велика кількість з’єднань до одного вузла, незвичні порти або раптова зміна структури трафіку можуть свідчити про атаку, зараження шкідливим програмним забезпеченням, сканування мережі або помилку в налаштуваннях.

NetFlow також використовується для виявлення DDoS-атак. Під час таких атак часто спостерігається різке збільшення кількості потоків, пакетів або байтів у напрямку певної цілі. Аналіз потоків дозволяє швидко визначити атакований вузол, джерела трафіку, тип протоколу й характер навантаження.

У сфері інформаційної безпеки NetFlow корисний для розслідування інцидентів. Навіть якщо вміст пакетів не зберігається, записи потоків дозволяють відновити загальну картину подій: які вузли взаємодіяли між собою, коли почався обмін, скільки даних було передано та які порти використовувалися.

Для операторських мереж NetFlow важливий також у задачах оптимізації маршрутизації. На основі потокової статистики можна побудувати матрицю трафіку між граничними вузлами мережі. Така матриця показує, між якими напрямками передається найбільший обсяг даних, і допомагає планувати пропускну здатність магістральних з’єднань.

9.2.9. Порівняння SNMP і NetFlow

SNMP і NetFlow вирішують різні, але взаємодоповнювальні завдання. SNMP добре підходить для контролю стану обладнання та інтерфейсів, тоді як NetFlow використовується для аналізу структури трафіку.

SNMP показує, скільки трафіку пройшло через інтерфейс, який стан має порт, наскільки завантажений процесор або скільки помилок виникло на лінії. NetFlow, своєю чергою, пояснює, які саме потоки сформували це навантаження.

Наприклад, якщо SNMP показує, що інтерфейс завантажений на 90 %, адміністратор бачить лише сам факт перевантаження. Дані NetFlow дозволяють уточнити причину: чи це резервне копіювання, відеотрафік, атака, робота хмарного сервісу, передавання файлів або помилка в маршрутизації.

Тому в сучасних системах моніторингу доцільно використовувати обидва підходи. SNMP забезпечує загальний контроль стану мережі, а NetFlow дає деталізацію мережевої активності.

9.2.10. Обмеження NetFlow

Попри значні переваги, NetFlow має певні обмеження. Насамперед ця технологія не аналізує вміст пакетів. Вона працює переважно з метаданими: адресами, портами, протоколами, кількістю байтів, кількістю пакетів і часовими мітками. Тому NetFlow не замінює системи глибокого аналізу пакетів, міжмережеві екрани або системи виявлення вторгнень.

Другим обмеженням є обсяг даних. У великих мережах кількість потоків може бути дуже значною, тому колектори повинні мати достатню продуктивність і дисковий простір. Якщо систему збирання даних спроєктовано неправильно, вона може втрачати записи або обробляти їх із затримкою.

Третім обмеженням є залежність від місця збору. NetFlow показує лише той трафік, який проходить через пристрій, де ввімкнено аналіз потоків. Якщо трафік проходить іншим шляхом або не потрапляє на відповідний інтерфейс, він не буде відображений у статистиці.

Також потрібно враховувати вплив на продуктивність обладнання. У сучасних пристроях NetFlow часто реалізується апаратно або з оптимізацією, але неправильні налаштування, надмірна деталізація або занадто частий експорт можуть створювати додаткове навантаження.

9.2.11. Рекомендації щодо впровадження NetFlow

Під час впровадження NetFlow важливо визначити, які саме завдання має вирішувати система аналізу потоків. Для базового моніторингу достатньо збирати інформацію про адреси, порти, протоколи, кількість пакетів і байтів. Для задач безпеки можуть знадобитися додаткові поля, наприклад TCP-прапорці, значення DSCP, інформація про автономні системи або VLAN.

Необхідно правильно вибрати точки збору. У корпоративній мережі NetFlow доцільно вмикати на граничних маршрутизаторах, міжмережевих екранах, вузлах підключення до центрів обробки даних і магістральних інтерфейсах. В операторській мережі важливими точками є граничні маршрутизатори, вузли агрегації та магістральні з’єднання.

Також потрібно враховувати продуктивність колектора. Він має обробляти очікувану кількість записів, зберігати історію за потрібний період і забезпечувати швидкий пошук під час аналізу інцидентів.

Доцільно налаштовувати період зберігання даних залежно від потреб організації. Для оперативного моніторингу може бути достатньо кількох днів або тижнів детальної історії, тоді як для розслідування інцидентів безпеки може знадобитися збереження агрегованих даних протягом кількох місяців.

У великих мережах варто використовувати вибірковий збір трафіку або попередню агрегацію даних. Це дозволяє зменшити навантаження на мережеві пристрої та систему зберігання, зберігаючи при цьому достатню точність для аналізу загальних тенденцій.

9.2.12. Значення NetFlow для оптимізації глобальних мереж

NetFlow є одним із найважливіших інструментів для розуміння реальної поведінки трафіку в глобальних мережах. Він дозволяє не лише побачити факт перевантаження, а й встановити його причину. Завдяки цьому адміністратор може приймати обґрунтовані рішення щодо розширення каналів, зміни маршрутної політики, налаштування QoS або посилення захисту.

У глобальних мережах NetFlow особливо корисний для аналізу трафіку між філіями, центрами обробки даних, хмарними сервісами та зовнішніми мережами. На основі зібраної статистики можна визначати критичні напрямки передавання даних, виявляти неефективні маршрути, оцінювати вплив окремих застосунків на канал і планувати розвиток інфраструктури.

Таким чином, NetFlow доповнює SNMP і Syslog, формуючи важливу частину комплексної системи моніторингу. SNMP показує технічний стан обладнання, Syslog фіксує події, а NetFlow пояснює, як саме використовується мережа і які потоки формують її навантаження.

9.3. SYSLOG — ЦЕНТРАЛІЗОВАНИЙ ЗБІР ЖУРНАЛІВ ПОДІЙ

Syslog — це стандартний механізм передавання журналів подій від мережевих пристроїв, серверів, міжмережевих екранів, систем безпеки та прикладних сервісів до централізованого сервера збору повідомлень. Він використовується для фіксації подій, пов’язаних із роботою обладнання, зміною конфігурації, помилками, спробами автентифікації, відмовами інтерфейсів, порушеннями безпеки та іншими важливими станами інфраструктури.

На відміну від SNMP, який переважно збирає числові показники стану пристроїв, і NetFlow, який описує мережеві потоки, Syslog фіксує саме події. Це дозволяє адміністратору бачити, що відбулося в мережі, коли саме це сталося, на якому пристрої та з яким рівнем важливості.

Централізований збір журналів подій є обов’язковою складовою сучасного мережевого адміністрування. Якщо журнали зберігаються лише локально на пристроях, вони можуть бути втрачені після перезавантаження, переповнення буфера або навмисного видалення зловмисником. Передавання подій на окремий захищений сервер дозволяє зберегти історію роботи інфраструктури, спростити пошук причин збоїв і підвищити рівень безпеки.

Syslog широко застосовується в корпоративних і операторських мережах, центрах обробки даних, хмарних середовищах, системах моніторингу та платформах SIEM. Його основна перевага полягає у простоті, універсальності та підтримці більшістю мережевого й серверного обладнання.

9.3.1. Архітектура та принципи роботи Syslog

Архітектура Syslog базується на передаванні повідомлень від джерел подій до сервера збору журналів. Джерелами подій можуть бути маршрутизатори, комутатори,

міжмережеві екрани, сервери, системи віртуалізації, операційні системи, прикладні сервіси та засоби захисту інформації.

У найпростішому випадку мережевий пристрій генерує повідомлення про подію та надсилає його безпосередньо на центральний Syslog-сервер. Сервер приймає повідомлення, зберігає його, індексує та надає адміністратору можливість пошуку, фільтрації, аналізу й побудови звітів.

У більших мережах може використовуватися багаторівнева архітектура. Наприклад, пристрої окремої філії надсилають повідомлення на локальний проміжний сервер, а той передає їх до центральної системи зберігання. Такий підхід зменшує навантаження на канали зв'язку, спрощує фільтрацію подій і підвищує стійкість системи збору журналів.

Передавання повідомлень Syslog традиційно здійснюється через UDP-порт 514. Цей спосіб простий і має невеликі накладні витрати, однак UDP не гарантує доставки повідомлень. У разі перевантаження мережі, втрати пакетів або недоступності сервера частина повідомлень може бути втрачена.

Для критичних систем доцільно використовувати передавання через TCP або захищене передавання через TLS. TCP забезпечує надійнішу доставку повідомлень, а TLS додатково захищає їх від перехоплення та підміни. Це особливо важливо тоді, коли журнали передаються через незахищені сегменти мережі або між віддаленими майданчиками.

9.3.2. Формат повідомлення Syslog

Повідомлення Syslog містить службову та змістову частини. Службова частина допомагає системі збору правильно обробити повідомлення, а змістова частина містить опис самої події.

У сучасному форматі Syslog, визначеному RFC 5424, повідомлення може містити такі основні елементи:

- пріоритет повідомлення;
- версію формату;
- часову мітку;
- ім'я або адресу вузла;
- назву застосунку чи процесу;
- ідентифікатор процесу;
- ідентифікатор типу повідомлення;
- структуровані дані;
- текст повідомлення.

Часова мітка показує, коли саме відбулася подія. Ім'я вузла або IP-адреса дозволяє визначити пристрій, який створив повідомлення. Назва застосунку або процесу допомагає зрозуміти, який компонент системи згенерував подію. Текст повідомлення містить основний опис: наприклад, інформацію про зміну стану інтерфейсу, невдалу спробу входу, помилку маршрутизації або зміну конфігурації.

Для ефективного аналізу журналів важливо, щоб усі пристрої мали правильно налаштований час. Якщо часові мітки на різних пристроях відрізняються, кореляція подій стає складною або неможливою. Наприклад, невдала спроба входу на VPN-шлюзі, зміна стану порту на комутаторі та спрацювання правила міжмережевого екрана можуть бути частинами одного інциденту, але без синхронізованого часу їх важко пов'язати між собою.

9.3.3. Рівні важливості повідомлень

Кожне повідомлення Syslog має рівень важливості, який показує критичність події. Рівні нумеруються від 0 до 7: чим менше число, тим критичнішою є подія.

Таблиця 9.1 — Рівні важливості повідомлень Syslog

Рівень	Назва	Зміст
0	Emergency	система непридатна до роботи
1	Alert	потрібне негайне втручання
2	Critical	критична помилка
3	Error	помилка в роботі системи або сервісу
4	Warning	попередження про можливу проблему
5	Notice	важлива, але некритична подія
6	Informational	інформаційне повідомлення
7	Debug	діагностичне повідомлення для налагодження

У практичній роботі не всі рівні повідомлень однаково важливі. Наприклад, повідомлення рівнів 0–3 зазвичай потребують оперативної реакції, оскільки можуть свідчити про відмову сервісу, критичну помилку або порушення роботи обладнання. Повідомлення рівнів 4–5 корисні для попередження про потенційні проблеми. Повідомлення рівня 6 використовуються для загального інформування, а рівень 7 переважно застосовується під час діагностики та налагодження.

У робочих мережах потрібно обережно використовувати рівень Debug, оскільки він може створювати дуже велику кількість повідомлень. Якщо залишити такий рівень увімкненим на тривалий час, це може перевантажити сервер збору журналів або ускладнити пошук справді важливих подій.

9.3.4. Джерела та категорії повідомлень

Окрім рівня важливості, у Syslog використовується поняття джерела або категорії повідомлення. Воно показує, яким типом системи або процесу було створено подію. Наприклад, окремі категорії можуть використовуватися для ядра операційної системи, системи автентифікації, поштових сервісів, мережевих процесів або локальних застосунків.

У мережевому обладнанні категорії повідомлень допомагають відокремити події маршрутизації, зміни конфігурації, події безпеки, повідомлення про інтерфейси та службові повідомлення системи. Це спрощує фільтрацію й маршрутизацію журналів.

Наприклад, повідомлення про невдалу спробу входу адміністратора до маршрутизатора має інше значення, ніж повідомлення про зміну стану порту. Перше може бути ознакою атаки або помилки автентифікації, а друге — наслідком фізичного від’єднання кабелю, перезавантаження пристрою або несправності каналу.

Правильне розділення повідомлень за категоріями дозволяє будувати ефективні правила сповіщення. Критичні повідомлення про безпеку можуть одразу передаватися до SIEM або групи реагування, тоді як інформаційні повідомлення можуть лише зберігатися для історичного аналізу.

9.3.5. Налаштування Syslog у мережевій інфраструктурі

Під час налаштування Syslog адміністратор має визначити кілька основних параметрів:

- адресу сервера збору журналів;
- транспортний протокол;
- рівень важливості повідомлень, які потрібно надсилати;
- джерельний інтерфейс для передавання повідомлень;
- формат часових міток;
- правила фільтрації та зберігання подій.

У мережевому обладнанні часто вказують окремий інтерфейс, з якого надсилатимуться повідомлення. Зазвичай для цього використовують стабільну адресу керування або loopback-інтерфейс. Це важливо, тому що фізичні інтерфейси можуть змінювати стан, тоді як loopback-адреса залишається сталою і зручною для ідентифікації пристрою в журналах.

Також важливо налаштувати часові мітки з точністю до секунд або мілісекунд, залежно від вимог організації. Для розслідування інцидентів безпеки або короткочасних відмов точність часу має велике значення.

У Linux-системах для роботи із Syslog часто використовуються служби rsyslog або syslog-ng. Вони дозволяють приймати, фільтрувати, пересилати й зберігати журнали подій. У великих інфраструктурах ці служби можуть працювати як проміжні вузли, що приймають журнали від локальних систем і передають їх до центрального сховища або SIEM.

9.3.6. Синхронізація часу

Синхронізація часу є однією з найважливіших умов ефективної роботи з журналами подій. Якщо пристрої мають різний час, адміністратору важко встановити реальну послідовність подій.

Наприклад, маршрутизатор може зафіксувати втрату зв’язку о 14:32:15, сервер автентифікації — невдалу спробу входу о 14:35:42, а міжмережевий екран — блокування підозрілого з’єднання о 14:31:58. Якщо час на цих пристроях не синхронізований, незрозуміло, яка подія була першою і чи пов’язані вони між собою.

Для синхронізації часу найчастіше використовується NTP. Він дозволяє пристроям отримувати точний час від визначених серверів часу. У корпоративній мережі доцільно використовувати внутрішні NTP-сервери, які синхронізуються із зовнішніми надійними джерелами часу. Це зменшує залежність від зовнішніх ресурсів і підвищує контроль над інфраструктурою.

У спеціалізованих середовищах, де потрібна дуже висока точність, може використовуватися PTP. Такий підхід застосовується у телекомунікаційних мережах, фінансових системах, промислових середовищах і мережах мобільного зв’язку нового покоління.

Правильно налаштована синхронізація часу є основою для кореляції подій, аналізу інцидентів, аудиту дій адміністраторів і побудови достовірної часової картини роботи мережі.

9.3.7. Централізована інфраструктура збору журналів

Централізація журналів подій є не лише зручністю, а й важливою вимогою безпеки. Локальні журнали на пристроях можуть бути видалені або змінені

зловмисником після отримання несанкціонованого доступу. Централізований сервер збору журналів ускладнює приховування слідів атаки, оскільки копії повідомлень зберігаються поза межами скомпрометованого пристрою.

У MITRE ATT&CK видалення або очищення журналів подій розглядається як спосіб приховування слідів активності зловмисника. Саме тому журнали важливо передавати на захищений сервер одразу після їх створення. Це дозволяє зберегти докази навіть у разі компрометації окремого вузла.

Централізований збір журналів також вирішує проблему обмеженої пам'яті мережевих пристроїв. Багато комутаторів, маршрутизаторів і міжмережевих екранів можуть зберігати лише обмежену кількість локальних повідомлень. Після переповнення буфера старі записи видаляються. Центральний сервер, навпаки, може зберігати журнали протягом місяців або років відповідно до політики організації.

Ще однією перевагою централізації є можливість кореляції подій. Події з VPN-шлюзу, міжмережевого екрана, комутатора доступу, сервера автентифікації та системи виявлення вторгнень можуть бути частинами одного інциденту. Якщо всі вони зберігаються в одному місці та мають синхронізовані часові мітки, адміністратор або аналітик безпеки може швидше встановити причину проблеми.

9.3.8. Syslog і SIEM

SIEM — це система управління інформацією та подіями безпеки, яка збирає, зберігає, аналізує та корелює події з різних джерел. Syslog є одним із найважливіших джерел даних для таких систем.

До SIEM можуть надходити журнали з маршрутизаторів, комутаторів, міжмережевих екранів, VPN-шлюзів, серверів, засобів антивірусного захисту, систем виявлення вторгнень, хмарних сервісів і прикладних систем. На основі цих даних SIEM може виявляти підозрілу активність, формувати сповіщення, будувати звіти й допомагати у розслідуванні інцидентів.

Кореляція подій дозволяє знаходити зв'язки між окремими повідомленнями. Наприклад, одна невдала спроба входу може не бути критичною. Але якщо протягом короткого часу зафіксовано багато невдалих спроб входу з однієї адреси, потім успішний вхід і зміну конфігурації мережевого пристрою, така послідовність може свідчити про компрометацію облікового запису.

Сучасні SIEM-платформи можуть доповнювати події інформацією про відомі загрози, аналізувати поведінку користувачів і систем, а також автоматизувати реагування на інциденти. Проте ефективність SIEM значною мірою залежить від якості вхідних даних. Якщо журнали неповні, час на пристроях не синхронізований або важливі джерела не підключені, система не зможе коректно виявляти складні інциденти.

9.3.9. Зберігання та захист журналів подій

Журнали подій можуть містити чутливу інформацію: IP-адреси, імена користувачів, результати автентифікації, відомості про зміну конфігурації, адреси внутрішніх сервісів і дані про спрацювання засобів захисту. Тому сервери збору журналів потрібно захищати так само ретельно, як і інші критичні елементи інфраструктури.

Доступ до журналів має бути обмежений лише для уповноважених адміністраторів і фахівців з безпеки. Необхідно використовувати розмежування прав доступу, автентифікацію, журналювання дій користувачів і регулярний перегляд прав.

Важливо забезпечити цілісність журналів. Для цього можуть застосовуватися незмінні сховища, цифрові підписи, контрольні суми, резервне копіювання та передавання копій журналів до окремого сховища. У критичних системах доцільно використовувати підхід, за якого після запису журнал не може бути змінений без залишення сліду.

Період зберігання журналів визначається політикою організації, нормативними вимогами та потребами розслідування інцидентів. Для оперативного аналізу можуть зберігатися детальні журнали за останні тижні або місяці, а для аудиту — агреговані або архівні дані за триваліший період.

Також потрібно регулярно перевіряти, чи всі важливі пристрої справді надсилають журнали до центральної системи. Втрата журналів з одного критичного пристрою може суттєво ускладнити розслідування інциденту.

9.3.10. Використання Syslog для діагностики несправностей

Syslog є важливим інструментом діагностики мережевих проблем. Журнали подій дозволяють встановити, коли виникла несправність, який пристрій її зафіксував і які супутні події відбувалися в той самий час.

Наприклад, якщо користувачі скаржаться на втрату доступу до сервісу, адміністратор може перевірити журнали маршрутизаторів, комутаторів, міжмережевих екранів і серверів. Повідомлення про зміну стану інтерфейсу, перезапуск протоколу маршрутизації, помилку автентифікації або блокування трафіку можуть допомогти швидко визначити джерело проблеми.

Syslog також корисний для аналізу нестабільних з’єднань. Якщо інтерфейс багаторазово переходить зі стану “працює” у стан “не працює”, це може свідчити про несправний кабель, модуль, порт, неправильне налаштування швидкості або проблеми на стороні провайдера.

У поєднанні з SNMP і NetFlow журнали подій дають повнішу картину роботи мережі. SNMP показує зміну числових показників, NetFlow пояснює структуру трафіку, а Syslog фіксує події, які могли спричинити ці зміни.

9.3.11. Рекомендації щодо впровадження Syslog

Для ефективного використання Syslog у мережевій інфраструктурі доцільно дотримуватися кількох рекомендацій.

Насамперед потрібно централізувати збирання журналів з усіх критичних пристроїв: маршрутизаторів, комутаторів, міжмережевих екранів, VPN-шлюзів, серверів автентифікації, систем виявлення вторгнень і ключових серверів.

Для важливих систем бажано використовувати надійне або захищене передавання повідомлень через TCP або TLS. UDP можна залишати для менш критичних повідомлень або ізольованих сегментів, де ризик втрати повідомлень є прийнятним.

Потрібно налаштувати синхронізацію часу через NTP або PTP. Без узгодженого часу журнали втрачають значну частину своєї цінності для розслідування інцидентів і аналізу причин відмов.

Необхідно визначити, які рівні важливості повідомлень надсилати до центральної системи. Надмірна кількість інформаційних і діагностичних повідомлень може ускладнити аналіз, тоді як надто жорстка фільтрація може призвести до втрати важливих подій.

Сервер збору журналів потрібно захищати від несанкціонованого доступу, регулярно резервувати та контролювати його працездатність. Також бажано налаштувати сповіщення про припинення надходження журналів від критичних пристроїв.

Окрему увагу слід приділяти перевірці правил кореляції та сповіщення. Вони мають виявляти не лише окремі критичні події, а й послідовності дій, що можуть свідчити про атаку або помилку конфігурації.

9.3.12. Значення Syslog у комплексному моніторингу

Syslog є одним із базових джерел інформації для моніторингу, діагностики та безпеки мережі. Він дозволяє зберігати історію подій, аналізувати причини несправностей, виявляти підозрілу активність і підтверджувати факти зміни конфігурації.

У комплексній системі моніторингу Syslog доповнює SNMP і NetFlow. SNMP відповідає на питання “який стан має пристрій або інтерфейс?”, NetFlow — “який трафік проходить через мережу?”, а Syslog — “які події відбулися і коли саме?”. Разом ці джерела даних формують цілісне уявлення про стан мережевої інфраструктури.

Для глобальних мереж, де взаємодіє велика кількість віддалених вузлів, централізований збір журналів подій є критично важливим. Він скорочує час пошуку причин відмов, підвищує якість реагування на інциденти, допомагає виконувати аудит і забезпечує доказову базу під час розслідування порушень безпеки.

9.4. СИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ (NMS)

Система управління мережею (Network Management System, NMS) — це програмна платформа, яка об’єднує засоби збору даних, моніторингу стану обладнання, аналізу подій, сповіщення адміністраторів, побудови звітів і контролю мережевої інфраструктури. Якщо SNMP, NetFlow та Syslog є окремими механізмами отримання інформації, то NMS виконує роль центральної системи, у якій ці дані збираються, обробляються та подаються у зручному для адміністратора вигляді.

Основне призначення NMS полягає у забезпеченні цілісного бачення стану мережі. Адміністратор має отримувати не розрізнені повідомлення з окремих пристроїв, а узагальнену картину: які вузли доступні, які інтерфейси перевантажені, де виникли помилки, які сервіси недоступні, які події потребують негайної реакції.

У глобальних мережах NMS має особливе значення, оскільки така інфраструктура складається з великої кількості віддалених вузлів, магістральних каналів, граничних маршрутизаторів, операторських сервісів, міжмережевих екранів, балансувальників навантаження та систем безпеки. Без централізованої системи управління своєчасне виявлення несправностей і контроль якості роботи мережі стають практично неможливими.

NMS дозволяє перейти від ручного перегляду стану окремих пристроїв до системного управління всією мережею. Такий підхід скорочує час пошуку несправностей, зменшує тривалість простоїв, підвищує прозорість роботи інфраструктури та допомагає планувати її розвиток.

9.4.1. Призначення та основні функції NMS

Система управління мережею виконує кілька ключових функцій.

По-перше, вона здійснює моніторинг доступності пристроїв і сервісів. NMS регулярно перевіряє, чи відповідають маршрутизатори, комутатори, сервери,

міжмережеві екрани, точки доступу та інші елементи інфраструктури. Якщо пристрій перестає відповідати, система створює подію та надсилає сповіщення адміністратору.

По-друге, NMS збирає технічні показники роботи обладнання. До таких показників належать завантаження процесора, використання оперативної пам'яті, стан інтерфейсів, обсяг переданого й прийнятого трафіку, кількість помилок, температура обладнання, стан блоків живлення та вентиляторів.

По-третє, система управління мережею забезпечує візуалізацію стану інфраструктури. Це можуть бути графіки навантаження, карти мережі, інформаційні панелі, таблиці стану пристроїв, діаграми доступності та звіти за певний період.

По-четверте, NMS формує сповіщення про несправності або перевищення порогових значень. Наприклад, адміністратор може отримати повідомлення, якщо канал завантажений понад 90 %, процесор маршрутизатора тривалий час працює з високим навантаженням, інтерфейс перейшов у стан відмови або сервер перестав відповідати.

По-п'яте, NMS допомагає у плануванні розвитку мережі. На основі історичних даних можна оцінити, які канали поступово наближаються до межі пропускної здатності, які пристрої потребують модернізації, які сегменти мережі мають нестабільну роботу та де необхідно посилити резервування.

9.4.2. Типова архітектура NMS

Типова система управління мережею складається з кількох взаємопов'язаних компонентів:

- модулів збору даних;
- бази даних або сховища показників;
- механізму обробки подій;
- системи сповіщень;
- засобів візуалізації;
- модуля звітності;
- засобів інтеграції з іншими системами.

Модулі збору даних отримують інформацію з мережевих пристроїв і сервісів. Для цього можуть використовуватися SNMP, NetFlow, IPFIX, Syslog, SSH, програмні інтерфейси, агенти операційних систем та інші механізми. У великих мережах збір даних може виконуватися через проміжні вузли, які розміщуються у філіях або окремих сегментах мережі. Це зменшує навантаження на центральний сервер і підвищує стійкість системи.

Сховище даних зберігає поточні та історичні показники. Саме завдяки історії адміністратор може порівнювати стан мережі за різні періоди, виявляти тенденції, аналізувати повторювані проблеми та будувати прогнози щодо розвитку інфраструктури.

Механізм обробки подій відповідає за аналіз отриманих даних. Він визначає, чи є певна зміна нормальною, попереджувальною або критичною. Наприклад, короткочасне зростання навантаження на канал може не потребувати реакції, але тривале перевищення порогу має створити сповіщення.

Система сповіщень передає повідомлення адміністраторам або черговій зміні. Сповіщення можуть надсилатися електронною поштою, через месенджери, систему заявок, SMS або спеціалізовані платформи реагування. Для критичних подій важливо

налаштовувати ескалацію: якщо перший відповідальний фахівець не відреагував, повідомлення має бути передане іншому рівню підтримки.

Засоби візуалізації дозволяють швидко оцінити стан мережі. Добре побудована інформаційна панель має показувати доступність ключових вузлів, завантаження каналів, кількість активних інцидентів, стан сервісів і динаміку основних показників.

Модуль звітності використовується для аналізу якості роботи мережі, підготовки звітів щодо доступності, перевірки виконання угод про рівень обслуговування та планування модернізації.

9.4.3. Функціональна модель FCAPS

Для опису завдань управління мережею часто використовується модель FCAPS. Вона охоплює п’ять основних напрямів:

- управління відмовами;
- управління конфігурацією;
- облік і аналіз використання ресурсів;
- управління продуктивністю;
- управління безпекою.

Управління відмовами передбачає виявлення, реєстрацію, аналіз і усунення несправностей. Система має визначити, який пристрій або сервіс недоступний, коли виникла проблема, які події передували відмові та які елементи інфраструктури були зачеплені.

Таблиця 9.2 — Функціональні напрями моделі FCAPS

Напрям	Зміст	Приклади реалізації в NMS
Управління відмовами	Виявлення та усунення несправностей	сповіщення про відмову вузла, падіння інтерфейсу, втрату доступності сервісу
Управління конфігурацією	Контроль і збереження налаштувань	резервне копіювання конфігурацій, фіксація змін, порівняння версій
Облік ресурсів	Аналіз використання ресурсів мережі	звіти щодо трафіку, використання каналів, активності клієнтів або підрозділів
Управління продуктивністю	Контроль якості та швидкодії	графіки навантаження, затримки, втрат пакетів, використання ресурсів
Управління безпекою	Контроль доступу та подій безпеки	аудит дій адміністраторів, інтеграція з SIEM, контроль підозрілих змін

Управління конфігурацією пов’язане з обліком налаштувань мережевого обладнання, контролем змін, резервним копіюванням конфігурацій і відстеженням відхилень від затверджених параметрів. Для великих мереж це особливо важливо, оскільки несанкціонована або помилкова зміна конфігурації може спричинити масштабну відмову.

Облік і аналіз використання ресурсів дає змогу визначати, хто і як використовує мережеві ресурси. У корпоративних мережах це може застосовуватися для внутрішньої звітності, а в операторських мережах — для обліку послуг, контролю використання каналів і планування тарифних моделей.

Управління продуктивністю передбачає контроль завантаження каналів, затримки, втрат пакетів, помилок на інтерфейсах, використання процесора, пам’яті та інших параметрів. Метою є не лише фіксація проблеми, а й виявлення тенденцій, які можуть призвести до погіршення якості роботи мережі.

Управління безпекою охоплює контроль доступу до системи управління, фіксацію дій адміністраторів, моніторинг подій безпеки, перевірку несанкціонованих змін і взаємодію з SIEM або іншими засобами захисту.

Модель FCAPS не обмежується конкретним програмним продуктом. Вона є зручною основою для оцінювання того, наскільки повно система управління мережею охоплює основні адміністративні завдання.

9.4.4. Популярні системи управління мережею

На практиці використовуються як комерційні системи управління мережею, так і рішення з відкритим кодом. Вибір конкретної платформи залежить від масштабу мережі, бюджету, типу обладнання, вимог до звітності, потреб безпеки та кваліфікації адміністративної команди.

Zabbix — одна з найпоширеніших систем моніторингу з відкритим кодом. Вона підтримує SNMP, агенти для операційних систем, перевірки сервісів, збирання показників, сповіщення, шаблони пристроїв і побудову графіків. Zabbix добре підходить для корпоративних мереж, центрів обробки даних і розподілених інфраструктур. Для великих середовищ можуть використовуватися проміжні вузли збору даних, які передають інформацію на центральний сервер.

Nagios — відома система моніторингу, яка історично стала основою для багатьох інших рішень. Її перевагою є велика кількість додаткових модулів і гнучкість налаштування перевірок. Nagios часто використовується для контролю доступності сервісів, серверів і мережевих пристроїв. Водночас для побудови сучасних інформаційних панелей або масштабного збору метрик можуть знадобитися додаткові компоненти.

PRTG Network Monitor — комерційна система моніторингу, орієнтована на швидке впровадження та зручний інтерфейс. Вона підтримує SNMP, перевірки доступності, моніторинг каналів, серверів, віртуальних середовищ і сервісів. PRTG часто використовують у малих і середніх організаціях, де важливими є простота налаштування та зрозуміле подання інформації.

LibreNMS — система моніторингу з відкритим кодом, орієнтована насамперед на мережеве обладнання. Вона добре працює з SNMP, автоматично виявляє пристрої, будує графіки інтерфейсів, підтримує багато виробників обладнання та зручна для моніторингу маршрутизаторів, комутаторів і серверів.

Prometheus і **Grafana** часто використовуються в сучасних інфраструктурах для збирання, зберігання та візуалізації показників. Prometheus відповідає за збирання числових показників, а Grafana — за побудову інформаційних панелей. Такий підхід особливо поширений у середовищах із контейнеризацією, мікросервісами та хмарними сервісами. У мережевому моніторингу ці інструменти можуть доповнювати класичні NMS.

9.4.5. Порівняння популярних NMS-платформ

Під час вибору NMS важливо враховувати не лише функціональні можливості, а й зручність обслуговування. Система моніторингу сама стає критичним елементом інфраструктури, тому її потрібно резервувати, захищати, оновлювати й регулярно перевіряти.

Таблиця 9.3 — Порівняння популярних систем управління мережею

Система	Тип рішення	Основне призначення	Переваги
Zabbix	рішення з відкритим кодом	комплексний моніторинг мережі, серверів і сервісів	гнучкі шаблони, масштабованість, підтримка SNMP та агентів
Nagios	рішення з відкритим кодом / комерційні варіанти	контроль доступності сервісів і пристроїв	велика кількість модулів, гнучкість перевірок
PRTG	комерційне рішення	швидке впровадження моніторингу в організації	зручний інтерфейс, просте налаштування, готові датчики
LibreNMS	рішення з відкритим кодом	моніторинг мережевого обладнання	автоматичне виявлення пристроїв, зручні графіки, підтримка багатьох виробників
Prometheus + Grafana	рішення з відкритим кодом	збір показників і візуалізація	гнучкі інформаційні панелі, зручність для сучасних сервісів

9.4.6. Інформаційні панелі та звітність

Одним із найважливіших елементів NMS є інформаційна панель. Вона має швидко показувати поточний стан мережі та допомагати адміністратору визначати пріоритети реагування.

Якісна інформаційна панель повинна містити:

- загальний стан мережі;
- кількість активних критичних подій;
- доступність ключових вузлів;
- завантаження основних каналів;
- стан магістральних інтерфейсів;
- інформацію про відмови обладнання;
- динаміку основних показників за останній період.

Не варто перевантажувати інформаційну панель великою кількістю другорядних даних. Основне завдання такої панелі — швидко відповісти на питання: чи працює мережа, де є проблема, наскільки вона критична і хто має на неї реагувати.

Звітність у NMS використовується для оцінювання роботи мережі за певний період. Звіти можуть містити дані про доступність сервісів, завантаження каналів, кількість інцидентів, середній час реагування, повторювані несправності та динаміку використання ресурсів. Такі звіти корисні для технічних фахівців, керівництва, служби підтримки та підрозділів, що відповідають за планування розвитку інфраструктури.

9.4.7. Сповіщення та правила реагування

Сповіщення є одним із головних механізмів практичного використання NMS. Якщо система лише збирає дані, але не повідомляє про критичні події, її користь значно зменшується.

Під час налаштування сповіщень потрібно визначити порогові значення, рівні критичності, канали доставки повідомлень і правила ескалації. Наприклад, короткочасне завантаження каналу на 95 % може бути лише попередженням, а тривале перевищення цього рівня протягом 15 хвилин — критичною подією.

Важливо уникати надмірної кількості сповіщень. Якщо адміністратори отримують сотні повідомлень на день, вони можуть перестати реагувати на них належним чином. Тому потрібно групувати пов'язані події, придушувати повторювані повідомлення та налаштовувати залежності між об'єктами.

Наприклад, якщо недоступний маршрутизатор філії, не потрібно окремо створювати критичні сповіщення для кожного комутатора й сервера за ним. Достатньо вказати першопричину — втрату зв'язку з маршрутизатором або каналом до філії.

Правильно налаштована система сповіщень скорочує час виявлення проблеми та допомагає швидше перейти до її усунення.

9.4.8. Інтеграція NMS з іншими системами

У сучасній інфраструктурі NMS рідко працює ізольовано. Вона може взаємодіяти з системами управління заявками, засобами безпеки, платформами автоматизації, системами резервного копіювання та хмарними сервісами.

Інтеграція з ITSM дозволяє автоматично створювати заявки на основі критичних подій. Наприклад, якщо NMS виявляє відмову магістрального каналу, у системі заявок може автоматично створитися інцидент із зазначенням пристрою, часу події, рівня критичності та відповідальної групи.

Інтеграція з SIEM дає змогу поєднати технічні події мережі з подіями безпеки. Наприклад, зміна конфігурації маршрутизатора, невдала спроба входу та раптове зростання трафіку можуть бути розглянуті як частини одного інциденту.

Інтеграція з платформами автоматизації дозволяє виконувати частину реакцій без ручного втручання. Наприклад, система може автоматично перевірити доступність сусідніх вузлів, зібрати діагностичну інформацію, створити резервну копію конфігурації або запустити заздалегідь підготовлений сценарій перевірки.

Проте автоматизацію потрібно впроваджувати обережно. Дії, які можуть змінити стан мережі, повинні бути добре протестовані, задокументовані та обмежені відповідними правами доступу.

9.4.9. Сучасні підходи до моніторингу

Класичний моніторинг часто ґрунтується на періодичному опитуванні пристроїв. Наприклад, NMS кожні кілька хвилин надсилає SNMP-запит і отримує значення певного параметра. Такий підхід є простим і надійним, але має обмеження: між двома опитуваннями короткочасна проблема може залишитися непоміченою.

У сучасних мережах дедалі частіше застосовується потокова телеметрія. У цьому підході пристрої не чекають періодичного запиту, а самостійно передають показники до системи збору з визначеною частотою або у разі зміни стану. Це зменшує затримку отримання даних і дає змогу швидше виявляти короткочасні події.

Іншим напрямом розвитку є автоматизація на основі намірів адміністратора. Її ідея полягає в тому, що адміністратор описує бажаний стан мережі, а система перевіряє, чи відповідає реальна конфігурація цьому стану. Якщо виявлено відхилення, система може повідомити адміністратора або виконати коригувальні дії.

Такі підходи не скасовують класичні NMS, а доповнюють їх. У багатьох організаціях одночасно використовуються SNMP, Syslog, NetFlow, потокова телеметрія, системи візуалізації та засоби автоматизації.

9.4.10. Вибір NMS для організації

Вибір системи управління мережею має ґрунтуватися на реальних потребах організації, а не лише на популярності певного продукту.

Для невеликої мережі достатньо простої системи, яка контролює доступність пристроїв, стан інтерфейсів і базові показники ресурсів. У такому середовищі важливими є простота встановлення, зрозумілий інтерфейс і мінімальні витрати на підтримку.

Для середньої корпоративної мережі потрібні ширші можливості: шаблони пристроїв, автоматичне виявлення вузлів, гнучкі сповіщення, резервне копіювання конфігурацій, звітність і підтримка різних виробників обладнання.

Для операторської мережі або великого центру обробки даних важливими стають масштабованість, розподілений збір даних, висока продуктивність, підтримка великої кількості пристроїв, інтеграція з іншими системами та можливість автоматизації типових операцій.

Під час вибору NMS доцільно оцінювати такі критерії:

- кількість пристроїв і сервісів, які потрібно контролювати;
- підтримку обладнання різних виробників;
- можливості збору даних через SNMP, Syslog, NetFlow та інші механізми;
- зручність побудови інформаційних панелей;
- гнучкість сповіщень;
- можливості звітності;
- вимоги до ліцензування;
- складність адміністрування;
- можливості інтеграції з SIEM, ITSM та засобами автоматизації;
- наявність резервування самої системи моніторингу.

Правильно обрана NMS має відповідати не лише поточному масштабу мережі, а й можливому зростанню інфраструктури в майбутньому.

9.4.11. Обмеження та типові помилки впровадження NMS

Попри значну користь, система управління мережею не усуває проблеми автоматично. Вона лише надає дані, які потрібно правильно інтерпретувати та використовувати.

Однією з типових помилок є моніторинг лише доступності пристроїв без аналізу продуктивності. Пристрій може відповідати на запити, але при цьому мати перевантажений процесор, заповнену пам’ять, помилки на інтерфейсах або втрати пакетів.

Друга помилка — відсутність правильно налаштованих порогових значень. Якщо пороги занадто низькі, система створюватиме надмірну кількість сповіщень. Якщо вони занадто високі, адміністратор дізнається про проблему занадто пізно.

Третя помилка — відсутність актуальної карти мережі. Якщо NMS не відображає реальну топологію, адміністратору складніше визначити, яка подія є причиною, а яка лише наслідком.

Четверта помилка — відсутність резервування самої системи моніторингу. Якщо центральний сервер NMS виходить з ладу, організація втрачає можливість оперативно контролювати стан мережі.

П’ята помилка — відсутність регулярного перегляду правил сповіщення. Мережа змінюється, додаються нові сервіси, змінюються маршрути й навантаження, тому правила моніторингу потрібно періодично переглядати.

9.4.12. Значення NMS у глобальних мережах

У глобальних мережах NMS є ключовим інструментом оперативного управління. Вона об’єднує дані з різних джерел, дозволяє контролювати стан віддалених вузлів, швидко виявляти несправності, аналізувати тенденції та підвищувати надійність інфраструктури.

SNMP дає NMS числові показники стану обладнання, Syslog передає події, NetFlow та IPFIX пояснюють структуру трафіку, а засоби візуалізації допомагають подати цю інформацію у зрозумілій формі. У результаті адміністратор отримує не окремі фрагменти даних, а цілісну картину роботи мережі.

Ефективна NMS скорочує час виявлення несправностей, допомагає швидше встановлювати першопричину проблем, підтримує виконання угод про рівень обслуговування, спрощує аудит і створює основу для подальшої автоматизації мережевого управління.

9.5. АНАЛІЗ ТРАФІКУ

Аналіз мережевого трафіку є одним із ключових інструментів моніторингу, оптимізації та захисту глобальних мереж. Він дозволяє визначати, які вузли обмінюються даними, які протоколи використовуються, які сервіси створюють найбільше навантаження, де виникають затримки, втрати пакетів або аномальна активність.

На відміну від загального моніторингу доступності пристроїв, аналіз трафіку дає змогу зрозуміти реальну поведінку мережі. Наприклад, адміністратор може бачити не лише те, що канал перевантажений, а й причину цього перевантаження: резервне копіювання, відеоконференції, оновлення програмного забезпечення, атака, помилка маршрутизації або некоректна робота певного застосунку.

Аналіз трафіку використовується для кількох основних завдань:

- виявлення перевантажених каналів;
- пошуку причин затримок і втрат пакетів;
- аналізу роботи прикладних сервісів;
- контролю використання пропускної здатності;
- виявлення шкідливої або підозрілої активності;
- перевірки ефективності політик QoS;
- планування розвитку мережевої інфраструктури;
- розслідування інцидентів безпеки.

У сучасних мережах рідко використовується лише один метод аналізу. Зазвичай застосовується багаторівневий підхід: SNMP показує загальні показники пристроїв та інтерфейсів, NetFlow і IPFIX описують мережеві потоки, Syslog фіксує події, а засоби захоплення пакетів дозволяють детально дослідити окремі з’єднання.

9.5.1. Рівні деталізації аналізу трафіку

Методи аналізу трафіку відрізняються рівнем деталізації. Одні інструменти показують лише загальне завантаження інтерфейсу, інші дозволяють бачити структуру потоків, а найдетальніші — аналізувати вміст окремих пакетів.

Перший рівень — аналіз агрегованих показників. На цьому рівні адміністратор отримує інформацію про завантаження інтерфейсів, кількість переданих і прийнятих байтів, кількість помилок, втрат або відкинутих пакетів. Такі дані зазвичай збираються за допомогою SNMP. Вони добре підходять для загального моніторингу, але не пояснюють, які саме вузли або сервіси створили навантаження.

Другий рівень — аналіз мережевих потоків. Він дає змогу визначити, між якими адресами відбувався обмін, які порти й протоколи використовувалися, скільки байтів і пакетів було передано. Для цього застосовуються NetFlow, Flexible NetFlow, IPFIX та подібні технології.

Третій рівень — захоплення й аналіз пакетів. На цьому рівні досліджуються окремі пакети, їхні заголовки, послідовність обміну, прапорці TCP, затримки між пакетами, повторні передавання та помилки протоколів. Такий підхід використовується для глибокої діагностики складних проблем.

Четвертий рівень — глибокий аналіз пакетів. Він дозволяє класифікувати трафік не лише за адресами й портами, а й за ознаками прикладних протоколів. Це корисно для виявлення застосунків, контролю політик безпеки, обмеження небажаного трафіку та виявлення складних загроз.

П’ятий рівень — поведінковий аналіз. Він ґрунтується на виявленні відхилень від нормальної поведінки мережі. Наприклад, система може виявити незвично велику кількість з’єднань, нетипові напрями передавання даних, підозрілу активність вузла або різке збільшення трафіку в неробочий час.

9.5.2. Захоплення та аналіз пакетів

Захоплення пакетів — це метод детального дослідження мережевого обміну, за якого окремі пакети зберігаються для подальшого аналізу. Такий підхід використовується тоді, коли потрібно точно визначити, що відбувається під час обміну між вузлами.

Найвідомішими інструментами для аналізу пакетів є Wireshark і tcpdump. Wireshark має графічний інтерфейс і зручний для детального перегляду пакетів, фільтрації, пошуку помилок протоколів і навчальних цілей. tcpdump працює у командному рядку й часто використовується на серверах, маршрутизаторах, міжмережевих екранах або віддалених вузлах, де немає графічного середовища.

Захоплення пакетів дозволяє дослідити:

- процес встановлення TCP-з’єднання;
- повторні передавання пакетів;
- втрати або затримки;
- помилки в роботі DNS, DHCP, HTTP, TLS та інших протоколів;
- неправильну фрагментацію;
- невідповідність портів або адрес;
- аномальні або підозрілі пакети.

Наприклад, якщо користувач скаржиться на повільну роботу вебсервісу, захоплення пакетів може показати, чи проблема пов’язана із затримкою встановлення TCP-з’єднання, повільною відповіддю сервера, повторними передаваннями, втратою пакетів або помилками DNS.

Водночас захоплення пакетів має певні обмеження. По-перше, у великих мережах повне збереження всіх пакетів швидко створює дуже великий обсяг даних. По-друге, пакети можуть містити чутливу інформацію, тому доступ до таких даних має

бути суворо обмежений. По-третє, у сучасних мережах значна частина трафіку шифрується, тому вміст прикладних даних часто недоступний для перегляду без спеціальних умов.

9.5.3. Аналіз мережевих потоків

Аналіз мережевих потоків є проміжним підходом між загальним моніторингом інтерфейсів і повним захопленням пакетів. Він не зберігає вміст пакетів, але фіксує важливі відомості про обмін між вузлами: адреси, порти, протоколи, кількість байтів, кількість пакетів, час початку й завершення потоку.

Для такого аналізу використовуються NetFlow, IPFIX та подібні технології. Вони особливо корисні у глобальних мережах, де повне захоплення трафіку є надто ресурсомістким, а загальні лічильники SNMP не дають достатньої деталізації.

Аналіз потоків дозволяє відповісти на такі питання:

- які вузли створюють найбільше навантаження;
- які сервіси найактивніше використовують канал;
- які напрями трафіку є найважливішими;
- чи є підозріле зростання кількості з’єднань;
- чи спостерігаються ознаки DDoS-атаки;
- чи відповідає реальний трафік очікуваній політиці використання мережі.

Інструменти на зразок ntopng і nfdump можуть використовуватися для збирання, перегляду та аналізу потокової статистики. Вони допомагають знаходити найбільших споживачів трафіку, аналізувати активність за адресами, портами, протоколами та часовими інтервалами.

У порівнянні із захопленням пакетів аналіз потоків є менш деталізованим, але значно краще масштабується. Саме тому він часто використовується в операторських мережах, корпоративних WAN і центрах обробки даних.

9.5.4. Глибокий аналіз пакетів

Глибокий аналіз пакетів (DPI) — це метод дослідження трафіку, за якого система аналізує не лише базові заголовки пакетів, а й додаткові ознаки протоколів прикладного рівня. Це дає змогу точніше визначати тип трафіку, навіть якщо він використовує нестандартні порти або намагається маскуватися під інший сервіс.

DPI може застосовуватися для:

- класифікації застосунків;
- виявлення небажаного або забороненого трафіку;
- реалізації політик безпеки;
- контролю якості обслуговування;
- виявлення шкідливої активності;
- обмеження або пріоритизації окремих типів трафіку.

Наприклад, звичайна фільтрація за портом може вважати, що трафік через порт 443 є вебтрафіком HTTPS. Однак DPI може додатково аналізувати ознаки сеансу та визначити, що через цей порт працює інший застосунок або тунель. Це особливо важливо для безпеки, оскільки багато сучасних сервісів і шкідливих програм використовують поширені порти для обходу простих правил фільтрації.

Водночас DPI має обмеження. Через поширення шифрування системи не завжди можуть бачити вміст переданих даних. У таких випадках вони аналізують метадані,

особливості встановлення з'єднання, сертифікати, розміри пакетів, часові інтервали та інші непрямі ознаки.

Застосування DPI також потребує врахування правових і етичних аспектів, оскільки надмірний аналіз вмісту трафіку може порушувати приватність користувачів. У навчальному та корпоративному контексті DPI слід розглядати як інструмент безпеки й управління мережею, а не як засіб необмеженого спостереження.

9.5.5. Поведінковий аналіз трафіку

Поведінковий аналіз трафіку ґрунтується на порівнянні поточної активності мережі з типовою або очікуваною поведінкою. Якщо система виявляє суттєве відхилення, вона може створити попередження або передати подію до системи безпеки.

Для такого аналізу важливо мати базову модель нормальної роботи мережі. Наприклад, у звичайний робочий день філія може передавати певний обсяг даних до центру обробки даних, використовувати типові сервіси й підтримувати стабільну кількість з'єднань. Якщо раптом уночі з'являється великий обсяг вихідного трафіку до невідомих зовнішніх адрес, це може бути ознакою витоку даних або компрометації вузла.

Поведінковий аналіз допомагає виявляти:

- сканування мережі;
- нетипові спроби з'єднання;
- різке збільшення кількості потоків;
- підозрілий вихідний трафік;
- аномальне використання DNS;
- активність шкідливого програмного забезпечення;
- ознаки витоку даних;
- нетипову поведінку користувачів або серверів.

Системи класу NDR використовують аналіз мережевої активності для виявлення загроз, які можуть залишатися непоміченими для традиційних засобів захисту. Такі системи не замінюють міжмережеві екрани, IDS/IPS або SIEM, але доповнюють їх, надаючи глибше розуміння поведінки мережі.

9.5.6. Інструменти аналізу трафіку

Для аналізу трафіку використовуються різні інструменти, які відрізняються призначенням, рівнем деталізації та складністю впровадження.

Wireshark застосовується для детального аналізу пакетів. Він зручний для навчання, діагностики протоколів, аналізу помилок і розслідування окремих проблем. Його доцільно використовувати тоді, коли потрібно розглянути конкретний обмін між вузлами.

tcpdump використовується для захоплення пакетів у командному рядку. Його перевагою є простота, швидкість і можливість роботи на серверах або мережевих пристроях без графічного інтерфейсу.

ntopng використовується для огляду мережевої активності, аналізу вузлів, протоколів, потоків і загального навантаження. Він зручний для оперативного перегляду структури трафіку.

nfdump орієнтований на роботу з даними NetFlow та IPFIX. Він дозволяє зберігати, фільтрувати й аналізувати записи потоків, що корисно для мереж із великим обсягом трафіку.

Zeek може використовуватися для глибшого аналізу мережевої активності та формування журналів про роботу протоколів. Він корисний у задачах безпеки, оскільки створює структуровані записи про мережеві взаємодії.

NDR-платформи застосовуються для виявлення загроз на основі аналізу мережевої поведінки. Вони допомагають знаходити аномалії, підозрілі з'єднання, нетипову активність і можливі ознаки компрометації.

Жоден інструмент не є універсальним. Для повноцінного аналізу доцільно поєднувати кілька підходів: SNMP для контролю стану пристроїв, NetFlow або IPFIX для аналізу потоків, Syslog для подій, Wireshark або tcpdump для детального дослідження пакетів, а NDR або SIEM — для аналізу загроз.

9.5.7. Аналіз трафіку для оптимізації продуктивності

Одним із головних практичних завдань аналізу трафіку є оптимізація продуктивності мережі. Адміністратор має визначити, чи достатньо пропускної здатності каналів, чи правильно працює маршрутизація, чи не створюють окремі сервіси надмірне навантаження та чи відповідає мережа потребам користувачів.

Аналіз трафіку дозволяє виявити:

- перевантажені канали;
- нерівномірний розподіл навантаження між маршрутами;
- неефективне використання резервних каналів;
- зайвий або дубльований трафік;
- надмірне використання каналу окремими вузлами;
- проблеми з маршрутизацією;
- сервіси, які потребують пріоритизації.

Наприклад, у корпоративній WAN-мережі може виявитися, що значна частина трафіку між філіями проходить через центральний офіс, хоча технічно можливий пряміший шлях. Така ситуація збільшує затримку, перевантажує центральний вузол і погіршує якість роботи сервісів. Аналіз потоків допомагає побачити цю проблему та обґрунтувати зміну маршрутизації або архітектури.

Також аналіз трафіку використовується для перевірки політик QoS. Якщо голосовий або відеотрафік має високий пріоритет, система аналізу повинна підтвердити, що відповідні пакети правильно маркуються, проходять потрібними чергами й не втрачаються під час перевантаження.

9.5.8. Аналіз трафіку для забезпечення безпеки

У сфері безпеки аналіз трафіку дозволяє виявляти активність, яка не завжди помітна за журналами подій або традиційними засобами контролю доступу. Навіть якщо вміст трафіку зашифрований, метадані можуть містити багато корисної інформації: напрями обміну, тривалість з'єднань, обсяг переданих даних, частоту звернень і типи протоколів.

Аналіз трафіку допомагає виявляти:

- DDoS-атаки;
- сканування портів;

- спроби підбору доступу;
- зв’язок із підозрілими зовнішніми адресами;
- аномально великий вихідний трафік;
- нетипову активність серверів;
- ознаки поширення шкідливого програмного забезпечення;
- спроби прихованого передавання даних.

Наприклад, якщо робоча станція, яка зазвичай звертається лише до внутрішніх сервісів, починає встановлювати сотні з’єднань із зовнішніми адресами, це може свідчити про зараження або участь у ботнеті. Якщо сервер баз даних раптом починає передавати великий обсяг інформації за межі організації, це може бути ознакою витоку даних.

Особливо важливо поєднувати аналіз трафіку з іншими джерелами даних. Події Syslog можуть показати невдалу спробу входу, NetFlow — подальший обмін із підозрілою адресою, а SIEM — зв’язати ці події в один інцидент.

9.5.9. Планування пропускної здатності

Аналіз трафіку є основою для планування пропускної здатності мережі. Замість того щоб розширювати канали лише після появи скарг користувачів, адміністратор може заздалегідь оцінити тенденції й підготувати модернізацію.

Для цього аналізують:

- середнє та пікове завантаження каналів;
- добові, тижневі та сезонні коливання трафіку;
- зростання кількості користувачів;
- появу нових сервісів;
- збільшення використання хмарних платформ;
- обсяг резервного копіювання;
- зміну структури трафіку між філіями.

Якщо канал регулярно досягає високого рівня завантаження, потрібно планувати його розширення або оптимізацію використання. Важливо враховувати, що замовлення нового каналу, оновлення обладнання або зміна операторської послуги може потребувати значного часу. Тому планування має виконуватися заздалегідь.

У глобальних мережах також важливо враховувати пікові періоди. Для університетської мережі це може бути початок навчального року або період дистанційного навчання, для електронної комерції — періоди великих розпродажів, для медіа — періоди важливих суспільних подій. Аналіз історичних даних допомагає підготувати інфраструктуру до таких навантажень.

9.5.10. Обмеження аналізу трафіку

Попри значну користь, аналіз трафіку має низку обмежень.

По-перше, не всі методи дають однакову деталізацію. SNMP показує лише загальні показники, NetFlow і IPFIX описують потоки, але не зберігають вміст пакетів, а захоплення пакетів дає детальну інформацію, проте погано масштабується для великих мереж.

По-друге, шифрування ускладнює аналіз прикладного вмісту. Це позитивно з погляду безпеки та приватності, але обмежує можливості деяких засобів глибокого

аналізу. У таких умовах важливішими стають метадані, поведінкові ознаки та кореляція з іншими джерелами.

По-третє, аналіз трафіку може створювати додаткове навантаження на обладнання та системи зберігання. Повне захоплення пакетів або надмірна деталізація потоків потребують значних ресурсів. Тому необхідно правильно вибирати точки збору, періоди зберігання та рівень деталізації.

По-четверте, трафік потрібно аналізувати з урахуванням контексту. Один і той самий обсяг переданих даних може бути нормальним для сервера резервного копіювання, але підозрілим для робочої станції користувача. Саме тому важливо знати призначення вузлів, топологію мережі та типові сценарії роботи.

9.5.11. Рекомендації щодо організації аналізу трафіку

Для ефективного аналізу трафіку доцільно дотримуватися кількох практичних рекомендацій.

Насамперед потрібно визначити цілі аналізу. Якщо основне завдання — контроль завантаження каналів, достатньо SNMP і NetFlow. Якщо потрібно розслідувати складні інциденти, знадобляться захоплення пакетів, журнали подій, SIEM і засоби поведінкового аналізу.

Важливо правильно обрати точки збору. У глобальній мережі доцільно аналізувати трафік на граничних маршрутизаторах, міжмережевих екранах, вузлах підключення філій, магістральних інтерфейсах і каналах до центрів обробки даних.

Необхідно налаштовувати збереження історії. Для оперативного аналізу можуть бути потрібні детальні дані за останні дні або тижні, а для планування розвитку — агрегована статистика за місяці або роки.

Також потрібно забезпечити захист зібраних даних. Дані про трафік можуть розкривати структуру мережі, поведінку користувачів, внутрішні сервіси та потенційно чутливу інформацію. Тому доступ до них має бути обмежений, а передавання й зберігання — захищені.

Окрему увагу варто приділити регулярному перегляду правил аналізу. Мережа змінюється, з’являються нові сервіси, змінюються маршрути й профілі навантаження. Тому правила фільтрації, пороги сповіщень і моделі нормальної поведінки потрібно періодично оновлювати.

9.5.12. Значення аналізу трафіку для глобальних мереж

Аналіз трафіку є наскрізною функцією мережевого управління. Він поєднує завдання продуктивності, безпеки, діагностики та планування розвитку інфраструктури. Без аналізу трафіку адміністратор бачить лише окремі симптоми: перевантажений канал, недоступний сервіс або повідомлення про помилку. З аналізом трафіку стає можливим встановити причину цих симптомів.

У глобальних мережах аналіз трафіку особливо важливий через розподілену структуру, велику кількість віддалених вузлів, різні типи каналів і залежність від операторських послуг. Він дозволяє контролювати якість роботи WAN, виявляти неефективні маршрути, обґрунтовувати розширення каналів, перевіряти політики QoS і своєчасно реагувати на загрози.

Таким чином, аналіз трафіку доповнює SNMP, NetFlow, Syslog і NMS, формуючи комплексний підхід до управління мережею. Його результати використовуються як для щоденної діагностики, так і для стратегічного планування розвитку глобальної мережевої інфраструктури.

9.6. БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Балансування навантаження — це технологія розподілу мережевого трафіку або обчислювальних запитів між кількома ресурсами: серверами, каналами зв'язку, вузлами обробки, центрами обробки даних або хмарними майданчиками. Основна мета балансування полягає в тому, щоб уникнути перевантаження одного ресурсу, підвищити продуктивність сервісу, забезпечити кращу відмовостійкість і скоротити час відповіді для користувачів.

У глобальних мережах балансування навантаження має особливе значення, оскільки користувачі можуть звертатися до сервісів із різних регіонів, через різних провайдерів і з різними показниками затримки. Якщо всі запити спрямовувати до одного сервера або одного центру обробки даних, це створює ризик перевантаження, збільшує затримку та знижує доступність сервісу.

Балансувальник навантаження — це апаратний або програмний компонент, який приймає запити від клієнтів і розподіляє їх між кількома серверами або вузлами обробки відповідно до заданого алгоритму. Для клієнта вся група серверів зазвичай виглядає як один логічний сервіс з однією віртуальною IP-адресою. Саме балансувальник визначає, який сервер має обробити конкретний запит.

Балансування навантаження використовується для вебсервісів, прикладних програмних інтерфейсів (API), баз даних, поштових систем, систем автентифікації, хмарних платформ, корпоративних порталів і сервісів дистанційного доступу. У сучасних мережах воно є не лише засобом підвищення продуктивності, а й важливою складовою високої доступності.

9.6.1. Принцип роботи балансувальника навантаження

Типова схема балансування навантаження передбачає наявність клієнтів, балансувальника та групи серверів, які обробляють запити. Клієнт звертається не безпосередньо до конкретного сервера, а до віртуальної адреси сервісу. Балансувальник приймає цей запит, аналізує його параметри та переспрямовує до одного з доступних серверів.

Після обробки запиту відповідь може повертатися клієнту через балансувальник або безпосередньо від сервера, залежно від обраної архітектури. У більшості корпоративних і хмарних середовищ відповідь проходить через балансувальник, оскільки це спрощує контроль сеансів, фільтрацію, шифрування та облік трафіку.

Балансувальник виконує кілька важливих функцій:

- приймає клієнтські запити;
- визначає доступні сервери;
- перевіряє працездатність вузлів;
- обирає сервер для обробки запиту;
- підтримує прив'язку сеансу, якщо вона потрібна;
- може завершувати або переспрямовувати захищені з'єднання;
- фіксує статистику звернень;
- допомагає приховати внутрішню структуру серверної інфраструктури.

Завдяки балансувальнику адміністратор може додавати нові сервери до пулу, виводити вузли на технічне обслуговування, оновлювати програмне забезпечення й розподіляти навантаження без повної зупинки сервісу.

9.6.2. Алгоритми балансування навантаження

Алгоритм балансування визначає, за яким правилом новий запит буде передано на певний сервер. Вибір алгоритму залежить від характеру сервісу, потужності серверів, тривалості запитів, кількості активних з'єднань і вимог до стабільності сеансів.

Найпростішим є циклічний алгоритм (Round Robin). Він послідовно розподіляє запити між серверами по колу: перший запит — на перший сервер, другий — на другий, третій — на третій, після чого цикл повторюється. Такий підхід простий, але не враховує реальне навантаження і потужність окремих серверів.

Зважений циклічний алгоритм (Weighted Round Robin) враховує різну продуктивність серверів. Кожному серверу задається вага. Потужніший сервер отримує більшу кількість запитів, а менш продуктивний — меншу. Це зручно, коли сервери мають різні ресурси або працюють у різних умовах.

Алгоритм найменшої кількості з'єднань (Least Connections) передає новий запит на сервер, який має найменше активних з'єднань. Він корисний тоді, коли тривалість обробки запитів суттєво відрізняється. Наприклад, один користувач може швидко отримати невелику сторінку, а інший — завантажувати великий файл або виконувати складний запит.

Алгоритм найменшого часу відповіді враховує не лише кількість активних з'єднань, а й швидкість реакції серверів. Запити спрямовуються до вузла, який відповідає швидше або має кращі поточні показники продуктивності. Такий підхід ефективний у динамічних середовищах, але потребує постійного контролю стану серверів.

Алгоритм за IP-адресою клієнта використовує адресу джерела для вибору сервера. Завдяки цьому запити від одного клієнта можуть потрапляти на той самий сервер. Це корисно для сервісів, де важливо зберігати прив'язку сеансу до конкретного вузла.

Алгоритм випадкового вибору з двох варіантів полягає в тому, що балансувальник випадково обирає два сервери, порівнює їхній поточний стан і спрямовує запит на менш завантажений. Такий підхід поєднує простоту з достатньо ефективним розподілом навантаження у великих системах.

9.6.3. Балансування на транспортному та прикладному рівнях

Балансувальники навантаження можуть працювати на різних рівнях мережевої моделі. Найчастіше розрізняють балансування на транспортному рівні та балансування на прикладному рівні.

Балансування на транспортному рівні працює з IP-адресами та портами. Балансувальник приймає рішення на основі мережевої та транспортної інформації: адреси клієнта, адреси сервісу, протоколу TCP або UDP, номера порту та стану з'єднання. Такий підхід має високу продуктивність, оскільки не потребує глибокого аналізу вмісту запиту.

Балансування на прикладному рівні аналізує зміст запиту прикладного протоколу. Наприклад, для HTTP або HTTPS балансувальник може враховувати адресу вебресурсу, шлях запиту, заголовки, тип вмісту або інші параметри. Це дозволяє гнучкіше розподіляти трафік: одні запити спрямовувати на сервери вебсторінок, інші — на сервери зображень, треті — на сервери прикладного програмного інтерфейсу.

Перевагою балансування на транспортному рівні є швидкість і простота. Воно добре підходить для сервісів, де достатньо розподіляти з'єднання за адресами та

портами. Перевагою балансування на прикладному рівні є гнучкість, оскільки воно дозволяє враховувати логіку роботи сервісу.

Водночас балансування на прикладному рівні потребує більше ресурсів, оскільки балансувальник аналізує значно більше даних. Крім того, для захищених з'єднань може знадобитися завершення TLS-сеансу на балансувальнику, щоб він міг бачити параметри прикладного запиту.

9.6.4. Перевірка працездатності серверів

Однією з найважливіших функцій балансувальника є перевірка працездатності серверів. Якщо сервер перестав відповідати або працює некоректно, балансувальник має автоматично припинити надсилати йому нові запити.

Перевірка може бути простою або розширеною. Проста перевірка встановлює, чи доступний сервер на певному порту. Наприклад, балансувальник може перевірити, чи відповідає сервер на TCP-порт 443. Якщо порт відкритий, сервер вважається доступним.

Розширена перевірка аналізує не лише доступність порту, а й правильність відповіді сервісу. Наприклад, балансувальник може звернутися до спеціальної сторінки перевірки стану й очікувати відповідь про готовність сервісу. Це дозволяє виявити ситуації, коли сервер формально доступний, але прикладна система на ньому працює неправильно.

Перевірки працездатності мають бути налаштовані обережно. Якщо перевірки виконуються занадто часто, вони можуть створювати додаткове навантаження на сервери. Якщо надто рідко — балансувальник може із запізненням виявити відмову. Також важливо правильно визначити кількість невдалих перевірок, після яких сервер виводиться з обслуговування.

Для критичних сервісів доцільно використовувати кілька рівнів перевірки: доступність мережевого порту, відповідь прикладного сервісу та перевірку залежностей, наприклад доступності бази даних або внутрішнього сховища.

9.6.5. Прив'язка сеансу до сервера

У деяких сервісах важливо, щоб усі запити одного користувача протягом певного часу потрапляли на той самий сервер. Це називається прив'язкою сеансу до сервера.

Така прив'язка потрібна тоді, коли стан користувацького сеансу зберігається локально на конкретному сервері. Наприклад, сервер може зберігати інформацію про авторизацію, кошик покупок, тимчасові дані або проміжні результати роботи користувача. Якщо наступний запит потрапить на інший сервер, сервіс може працювати некоректно.

Прив'язка сеансу може реалізовуватися за IP-адресою клієнта, спеціальним файлом cookie, ідентифікатором сеансу або іншою ознакою. Найгнучкішим підходом для вебсервісів є використання cookie, оскільки IP-адреса клієнта може змінюватися або бути спільною для багатьох користувачів через NAT.

Водночас прив'язка сеансу має недоліки. Вона може призвести до нерівномірного розподілу навантаження, якщо частина користувачів створює значно більше запитів, ніж інші. Крім того, у разі відмови сервера сеанс користувача може бути втрачений.

Сучасні прикладні системи часто намагаються уникати жорсткої прив'язки до одного сервера. Для цього стан сеансу зберігається у спільному сховищі, базі даних або розподіленому кеші. У такому випадку будь-який сервер із пулу може обробити запит користувача, що значно підвищує масштабованість і відмовостійкість.

9.6.6. Завершення TLS-з’єднань на балансувальнику

Для захищених вебсервісів часто використовується завершення TLS-з’єднань на балансувальнику. У такій архітектурі клієнт встановлює захищене з’єднання з балансувальником, а балансувальник уже передає запит до внутрішнього сервера.

Цей підхід має кілька переваг. По-перше, балансувальник централізовано керує сертифікатами, що спрощує їх оновлення та контроль. По-друге, сервери прикладного рівня звільняються від частини криптографічного навантаження. По-третє, балансувальник може аналізувати параметри прикладного запиту й застосовувати правила маршрутизації на основі URL, заголовків або інших ознак.

Проте така архітектура потребує обережного проєктування. Якщо трафік між балансувальником і внутрішніми серверами передається незашифрованим, потрібно гарантувати захищеність внутрішньої мережі. У критичних середовищах доцільно використовувати повторне шифрування між балансувальником і серверами.

Також потрібно захищати сам балансувальник, оскільки він обробляє велику кількість клієнтських з’єднань і може мати доступ до розшифрованого трафіку. Для цього застосовують обмеження адміністративного доступу, регулярне оновлення програмного забезпечення, контроль журналів подій і резервування балансувальників.

9.6.7. Глобальне балансування навантаження

У глобальних мережах часто використовують не лише локальне балансування між серверами в одному центрі обробки даних, а й глобальне балансування між різними майданчиками. Такий підхід дає змогу спрямовувати користувачів до найближчого, найменш завантаженого або найбільш доступного центру обробки даних.

Глобальне балансування може враховувати:

- географічне розташування користувача;
- затримку до різних майданчиків;
- доступність сервісу;
- завантаження центрів обробки даних;
- стан каналів зв’язку;
- політики резервування;
- вимоги до обробки даних у певному регіоні.

Одним із поширених підходів є використання DNS-балансування. У цьому випадку система доменних імен повертає клієнту адресу того майданчика, який відповідає обраній політиці. Наприклад, користувач із Європи може бути спрямований до європейського центру обробки даних, а користувач з Азії — до азійського.

Іншим підходом є використання Anycast, коли одна й та сама IP-адреса оголошується з кількох географічно розподілених вузлів. Мережа спрямовує користувача до найближчого або найкращого з погляду маршрутизації вузла. Такий підхід часто використовується для служб DNS, мереж доставки вмісту та глобальних сервісів із високими вимогами до доступності.

Глобальне балансування особливо важливе для сервісів, які мають працювати безперервно навіть у разі відмови окремого центру обробки даних або регіону.

9.6.8. Балансування навантаження і відмовостійкість

Балансування навантаження тісно пов’язане з відмовостійкістю. Якщо один сервер виходить із ладу, балансувальник має автоматично вилучити його з пулу й

спрямовувати нові запити до інших працездатних серверів. Це дозволяє зберегти доступність сервісу навіть у разі відмови окремого вузла.

Проте балансування саме по собі не гарантує повної високої доступності. Якщо балансувальник є єдиним вузлом входу до сервісу, він сам стає одиничною точкою відмови. Тому для критичних систем балансувальники також резервують.

Найпоширенішими є дві схеми резервування:

- активний/резервний режим;
- активний/активний режим.

В активному/резервному режимі один балансувальник обробляє трафік, а другий перебуває в очікуванні. Якщо основний вузол відмовляє, резервний бере на себе його функції. Така схема простіша в реалізації, але частина ресурсів використовується лише під час аварії.

В активному/активному режимі кілька балансувальників одночасно обробляють трафік. Це дозволяє краще використовувати ресурси та підвищити продуктивність, але вимагає складнішого узгодження стану, маршрутів і політик.

Для коректної роботи відмовостійкої схеми важливо також резервувати мережеві з'єднання, комутатори, канали до провайдерів, сервери прикладного рівня, бази даних і системи зберігання. Інакше відмова одного залежного компонента може зупинити весь сервіс, навіть якщо балансувальник працює правильно.

9.6.9. Балансування навантаження в WAN та SD-WAN

У глобальних мережах балансування може застосовуватися не лише для серверів, а й для каналів зв'язку. Організація може мати кілька підключень до Інтернету, кілька операторських каналів, MPLS-з'єднання, VPN-тунелі або мобільні резервні канали. Завдання полягає в тому, щоб ефективно використовувати ці ресурси та забезпечити безперервність зв'язку.

У традиційних WAN балансування між каналами може виконуватися за допомогою маршрутизації, політик вибору шляху, резервування шлюзів або протоколів динамічної маршрутизації. Однак такі підходи не завжди враховують якість каналу в реальному часі.

У SD-WAN балансування реалізується гнучкіше. Система може оцінювати затримку, втрати пакетів, джитер, завантаження каналу та доступність сервісів. На основі цих показників трафік різних застосунків спрямовується різними шляхами. Наприклад, голосовий трафік може передаватися через канал із мінімальною затримкою, резервне копіювання — через дешевший широкосмуговий канал, а критичні бізнес-застосунки — через найбільш стабільний маршрут.

Такий підхід дозволяє не лише розподіляти навантаження, а й підвищувати якість роботи сервісів. Якщо один канал погіршується або відмовляє, трафік автоматично перемикається на інший шлях відповідно до політики організації.

9.6.10. Типові помилки під час впровадження балансування

Під час впровадження балансування навантаження часто виникають помилки, які знижують ефективність або надійність рішення.

Першою помилкою є використання одного балансувальника без резервування. У такій схемі сервери можуть бути відмовостійкими, але сам балансувальник залишається критичною точкою відмови.

Друга помилка — неправильні перевірки працездатності. Якщо балансувальник перевіряє лише доступність порту, він може вважати сервер справним, навіть якщо

прикладний сервіс працює некоректно. Краще перевіряти не лише порт, а й фактичну відповідь сервісу.

Третя помилка — надмірна прив'язка сеансів до конкретного сервера. Це може погіршити розподіл навантаження та ускладнити відновлення після відмови. Якщо можливо, стан сеансу варто зберігати не на окремому сервері, а у спільному сховищі.

Четверта помилка — ігнорування продуктивності самого балансувальника. Він має обробляти достатню кількість з'єднань, запитів і зашифрованих сеансів. Якщо його ресурси недостатні, він стане вузьким місцем усієї системи.

П'ята помилка — відсутність моніторингу. Потрібно контролювати не лише сервери, а й сам балансувальник: кількість активних з'єднань, час відповіді, кількість помилок, стан перевірок працездатності, завантаження процесора, пам'яті та мережевих інтерфейсів.

Шоста помилка — відсутність тестування аварійних сценаріїв. Схему балансування потрібно перевіряти не лише в нормальному режимі, а й під час відмови сервера, каналу, балансувальника або цілого майданчика.

9.6.11. Рекомендації щодо проєктування балансування навантаження

Під час проєктування балансування навантаження потрібно насамперед визначити мету: підвищення продуктивності, забезпечення відмовостійкості, зменшення затримки, розподіл користувачів між регіонами або оптимізація використання каналів.

Для критичних сервісів необхідно використовувати щонайменше два балансувальники в резервованій схемі. Також потрібно резервувати сервери, канали зв'язку, комутатори, шлюзи та залежні системи, зокрема бази даних і сховища.

Алгоритм балансування має відповідати характеру сервісу. Для однотипних коротких запитів може бути достатньо циклічного розподілу. Для сервісів із різною тривалістю запитів краще використовувати алгоритм найменшої кількості з'єднань або найменшого часу відповіді. Для сервісів із локальним збереженням стану може знадобитися прив'язка сеансу.

Перевірки працездатності потрібно налаштовувати так, щоб вони відображали реальний стан сервісу. Найкраще перевіряти не лише мережеву доступність, а й готовність прикладної системи обробляти запити.

Для захищених вебсервісів потрібно продумати, де завершується TLS-з'єднання: на балансувальнику, на сервері або з повторним шифруванням між ними. Це рішення впливає на продуктивність, безпеку, можливість аналізу запитів і складність адміністрування.

Також необхідно налаштувати моніторинг і журналювання. Балансувальник має передавати події до Syslog або SIEM, а його показники мають контролюватися через NMS або іншу систему моніторингу.

9.6.12. Значення балансування навантаження для глобальних мереж

Балансування навантаження є важливим механізмом забезпечення продуктивності, масштабованості та відмовостійкості глобальних мереж. Воно дозволяє ефективно використовувати серверні ресурси, розподіляти користувачів між майданчиками, зменшувати затримку та підтримувати доступність сервісів у разі відмови окремих компонентів.

У глобальних мережах балансування навантаження працює разом з іншими технологіями: моніторингом SNMP, аналізом потоків NetFlow/IPFIX, журналами Syslog,

системами управління мережею, SD-WAN, DNS, Anycast і механізмами високої доступності. Саме поєднання цих засобів дозволяє створювати стійкі сервіси, здатні працювати під великим навантаженням і витримувати відмови окремих вузлів.

Отже, балансування навантаження не слід розглядати лише як спосіб розподілу запитів між серверами. Це комплексний інструмент управління продуктивністю та доступністю, який відіграє ключову роль у побудові сучасної глобальної мережевої інфраструктури.

9.7. ВИСОКА ДОСТУПНІСТЬ — ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ РОБОТИ

Висока доступність (High Availability, HA) — це властивість системи або сервісу підтримувати працездатність протягом заданого часу з мінімальними перервами в роботі. Основна мета високої доступності полягає не в тому, щоб повністю усунути всі можливі відмови, а в тому, щоб зробити їхній вплив на користувачів мінімальним.

Жодна реальна система не може гарантувати абсолютну доступність. Відмови обладнання, помилки програмного забезпечення, помилкові дії персоналу, збої електроживлення, аварії каналів зв'язку та зовнішні події є об'єктивними ризиками для будь-якої інфраструктури. Тому під час проєктування мережі важливо не лише намагатися зменшити ймовірність відмов, а й забезпечити швидке виявлення проблеми, автоматичне перемикання на резервні ресурси та відновлення сервісу.

У глобальних мережах висока доступність має особливе значення, оскільки відмова одного вузла або каналу може вплинути на роботу віддалених філій, центрів обробки даних, хмарних сервісів, систем автентифікації, корпоративних застосунків і клієнтських сервісів. Саме тому HA розглядається як одна з ключових вимог до сучасної мережевої інфраструктури.

Висока доступність досягається поєднанням кількох підходів: резервуванням обладнання, дублюванням каналів зв'язку, використанням протоколів автоматичного перемикання, балансуванням навантаження, моніторингом стану компонентів, синхронізацією даних і регулярним тестуванням аварійних сценаріїв.

9.7.1. Поняття доступності та основні метрики

Доступність системи визначається як частка часу, протягом якого сервіс залишається працездатним і доступним для користувачів. Зазвичай вона вимірюється у відсотках за певний період, наприклад за рік або місяць.

Для оцінювання високої доступності використовують кілька ключових метрик.

Час простою — це період, протягом якого сервіс або система недоступні для користувачів. Простій може бути плановим, наприклад під час технічного обслуговування, або позаплановим, якщо він спричинений аварією чи відмовою.

MTBF — середній час між відмовами. Ця метрика показує, як довго система в середньому працює до виникнення наступної відмови. Чим більший MTBF, тим надійнішою є система.

MTTR — середній час відновлення після відмови. Він охоплює час виявлення проблеми, діагностики, усунення несправності та повернення сервісу до нормальної роботи. Зменшення MTTR є одним із найефективніших шляхів підвищення доступності.

RTO — цільовий час відновлення. Це максимально допустимий час, протягом якого сервіс може бути недоступним після аварії.

RPO — допустима втрата даних у часі. Ця метрика показує, який обсяг даних організація може втратити без критичних наслідків. Наприклад, RPO у 15 хвилин означає, що система має бути здатна відновитися з втратою даних не більше ніж за останні 15 хвилин.

Доступність системи можна подати так:

$$\text{ДОСТУПНІСТЬ} = \frac{MTBF}{MTBF + MTTR}$$

З цієї формули випливає важливий практичний висновок: для підвищення доступності можна або збільшувати надійність компонентів, або скорочувати час відновлення. На практиці часто ефективніше інвестувати не лише в дороге обладнання, а й у моніторинг, автоматизацію, резервування та підготовлені процедури відновлення.

Таблиця 9.4 — Рівні доступності та допустимий час простою

Рівень доступності	Час простою / рік	Час простою / місяць	Типова сфера застосування
99% (дві дев'ятки)	3,65 дня	7,2 год	некритичні внутрішні системи
99,9% (три дев'ятки)	8,76 год	43,8 хв	стандартні бізнес-застосунки
99,99% (чотири дев'ятки)	52,6 хв	4,38 хв	критичні корпоративні сервіси, електронна комерція
99,999% (п'ять дев'яток)	5,26 хв	26 сек	телекомунікаційні сервіси, фінансові системи
99,9999% (шість дев'яток)	31,5 сек	2,6 сек	критичні системи, системи життєзабезпечення

Не кожна система потребує максимальної доступності. Чим вищий рівень доступності, тим складнішою та дорожчою стає архітектура. Тому рівень НА має визначатися не бажанням досягти "найкращого" показника, а реальними бізнес-вимогами, вартістю простою та критичністю сервісу.

9.7.2. Висока доступність і резервування

Висока доступність і резервування пов'язані між собою, але не є тотожними поняттями. Резервування означає наявність додаткових компонентів: запасних каналів, блоків живлення, маршрутизаторів, серверів, дисків або інших ресурсів. Проте саме по собі резервування не гарантує автоматичного відновлення сервісу.

Наприклад, сервер із двома блоками живлення має резервування живлення. Якщо один блок вийде з ладу, сервер продовжить працювати. Проте якщо в мережі є два маршрутизатори, але немає механізму автоматичного перемикання шлюзу, користувачі можуть втратити зв'язок до моменту ручного втручання адміністратора.

Висока доступність передбачає, що відмова виявляється автоматично, після чого трафік або сервіс перемикається на резервний компонент із мінімальним простоєм. Для цього потрібні не лише резервні ресурси, а й механізми контролю стану, виявлення відмов, автоматичного перемикання, синхронізації стану та запобігання конфліктам між вузлами.

Отже, резервування є основою високої доступності, але не замінює її. Щоб резервний компонент справді забезпечував НА, система має вміти швидко виявити відмову, правильно обрати активний вузол і продовжити роботу без значного впливу на користувачів.

Таблиця 9.5 — Порівняння High Availability та Redundancy

Параметр	Висока доступність	Резервування
Основна мета	мінімізація простою сервісу	наявність запасних компонентів
Перемикання при відмові	автоматичне або напівавтоматичне	може бути ручним
Основний фокус	безперервність роботи сервісу	дублювання ресурсів
Типові метрики	RTO, RPO, доступність у відсотках	N+1, 2N, кількість резервних компонентів
Складність	вища, потребує моніторингу та логіки перемикання	нижча, якщо резерв лише фізично присутній
Приклади	VRRP, HSRP, GLBP, кластеризація, балансування навантаження	резервні канали, RAID, UPS, запасні блоки живлення
Робота зі станом сервісу	потребує синхронізації стану	не вирішує проблему стану автоматично

9.7.3. Протоколи резервування першого шлюзу: HSRP, VRRP, GLBP

Однією з типових проблем у локальних і корпоративних мережах є відмова шлюзу за замовчуванням. Робочі станції, сервери та інші вузли зазвичай мають одну адресу шлюзу, через яку передають трафік за межі локальної мережі. Якщо цей маршрутизатор або комутатор рівня L3 відмовляє, вузли втрачають зв’язок із зовнішніми мережами.

Для вирішення цієї проблеми використовують протоколи резервування першого шлюзу. Вони дозволяють кільком маршрутизаторам або комутаторам рівня L3 спільно обслуговувати одну віртуальну IP-адресу шлюзу. Для кінцевих пристроїв ця адреса виглядає як звичайний шлюз за замовчуванням, але фактично за нею працює група пристроїв.

До найпоширеніших протоколів цього класу належать:

- HSRP;
- VRRP;
- GLBP.

HSRP — протокол резервування шлюзу, розроблений Cisco. У групі HSRP один пристрій виконує роль активного шлюзу, а інший перебуває в резерві. Якщо активний пристрій відмовляє, резервний бере на себе його функції та починає відповідати за віртуальну IP-адресу.

VRRP — відкритий стандарт резервування шлюзу. Його принцип подібний до HSRP: один маршрутизатор є основним, інші — резервними. Перевагою VRRP є підтримка обладнанням різних виробників, що робить його зручним для змішаних мереж.

GLBP також належить до рішень Cisco, але, на відміну від HSRP і VRRP, дозволяє не лише резервувати шлюз, а й розподіляти навантаження між кількома маршрутизаторами. У GLBP кілька пристроїв можуть одночасно обслуговувати трафік від різних клієнтів.

Протоколи резервування першого шлюзу особливо корисні у мережах кампусів, дата-центрів, корпоративних філій і операторських вузлів доступу. Вони дозволяють зменшити залежність від одного маршрутизатора та забезпечити автоматичне відновлення зв’язності у разі його відмови.

9.7.4. Резервування каналів і маршрутів

Висока доступність глобальної мережі неможлива без резервування каналів зв'язку. Навіть якщо всі мережеві пристрої працюють справно, пошкодження оптичної лінії, аварія у провайдера або збій на проміжному вузлі може призвести до втрати зв'язку між майданчиками.

Для підвищення стійкості WAN-інфраструктури використовують кілька підходів:

- підключення до двох або більше провайдерів;
- фізично незалежні траси прокладання каналів;
- резервні VPN-тунелі;
- динамічну маршрутизацію;
- автоматичне перемикання на резервний канал;
- використання SD-WAN для вибору найкращого шляху.

Якщо два канали проходять однією фізичною трасою, вони не забезпечують повноцінної відмовостійкості. Наприклад, один будівельний інцидент або пошкодження кабельної каналізації може одночасно вивести з ладу обидва з'єднання. Тому для критичних мереж важливо перевіряти не лише наявність двох договорів із провайдерами, а й реальну незалежність фізичних маршрутів.

Динамічна маршрутизація дозволяє мережі автоматично перебудовувати шляхи після відмови. У корпоративних і операторських мережах для цього можуть використовуватися OSPF, IS-IS, BGP та інші протоколи. Час збіжності маршрутизації має відповідати вимогам сервісу: для критичних систем повільне перемикання може бути неприйнятним.

У SD-WAN резервування каналів поєднується з оцінюванням їхньої якості. Система може враховувати затримку, втрати пакетів, джитер і завантаження каналу. Якщо якість одного з'єднання погіршується, трафік критичних застосунків може бути автоматично переведений на кращий шлях.

9.7.5. Кластеризація та резервування серверних сервісів

Для високої доступності прикладних сервісів недостатньо резервувати лише мережу. Якщо вебсервер, база даних або система автентифікації працює на одному вузлі, саме цей вузол стає одиничною точкою відмови. Тому критичні сервіси розгортають у кластерній або розподіленій архітектурі.

Кластер — це група серверів або вузлів, які спільно забезпечують роботу одного сервісу. Залежно від архітектури один вузол може бути активним, а інший резервним, або кілька вузлів можуть одночасно обробляти запити.

В активному/резервному режимі один вузол обслуговує користувачів, а другий очікує відмови основного. Такий підхід простіший, але частина ресурсів використовується лише під час аварії.

В активному/активному режимі кілька вузлів одночасно обробляють трафік. Це підвищує продуктивність і дозволяє краще використовувати ресурси, але потребує складнішої синхронізації, балансування навантаження й контролю стану.

Особливо складним є забезпечення високої доступності сервісів, які зберігають стан. До них належать бази даних, системи авторизації, платіжні сервіси, системи обліку та прикладні платформи, де важлива послідовність операцій. Для таких систем потрібно забезпечити реплікацію даних, узгодженість стану та контроль втрат під час аварії.

Якщо сервіс не зберігає стан локально на одному вузлі, його значно легше масштабувати й резервувати. Саме тому сучасні архітектури часто прагнуть відокремити прикладну логіку від сховища стану та використовувати спільні бази даних, розподілені кеші або зовнішні сховища сеансів.

9.7.6. Одиничні точки відмови

Одинична точка відмови — це компонент, відмова якого може призвести до недоступності всього сервісу або значної частини інфраструктури. Виявлення та усунення таких точок є одним із головних завдань проєктування високодоступних систем.

Одиничними точками відмови можуть бути:

- один маршрутизатор на виході до провайдера;
- один комутатор агрегації;
- один балансувальник навантаження;
- один сервер бази даних;
- один канал зв’язку між майданчиками;
- одне джерело живлення;
- одна система зберігання даних;
- один сервер автентифікації;
- одна система моніторингу.

Не всі одиничні точки відмови мають однакову критичність. Наприклад, відмова одного тестового сервера може бути прийнятною, тоді як відмова шлюзу до Інтернету або сервера автентифікації може зупинити роботу великої кількості користувачів.

Для усунення одиничних точок відмови застосовують дублювання компонентів, резервування каналів, кластеризацію, балансування навантаження, реплікацію даних, резервне живлення та географічне рознесення майданчиків.

Важливо враховувати не лише технічні компоненти, а й організаційні процеси. Якщо лише один адміністратор знає, як відновити критичний сервіс, це також створює ризик. Тому для високої доступності потрібні документація, регламенти, підготовлені сценарії відновлення та навчання персоналу.

9.7.7. Виявлення відмов і автоматичне перемикання

Для реалізації високої доступності система повинна швидко виявляти відмови. Якщо відмова не виявлена, резервні компоненти не будуть задіяні, навіть якщо вони фізично присутні.

Виявлення відмов може здійснюватися за допомогою:

- періодичних службових повідомлень між вузлами;
- перевірок доступності сервісу;
- моніторингу інтерфейсів;
- аналізу стану процесів;
- контролю відповідей прикладної системи;
- даних від NMS або SIEM.

Періодичні службові повідомлення дозволяють вузлам перевіряти, чи працюють їхні сусіди. Якщо протягом заданого часу відповідь не надходить, вузол може вважатися недоступним. Проте інтервал таких перевірок потрібно обирати обережно.

Надто довгий інтервал збільшує час реакції, а надто короткий може спричинити помилкові спрацювання під час короткочасних затримок.

Автоматичне перемикання має бути спроєктоване так, щоб уникати ситуації, коли два вузли одночасно вважають себе активними. Така проблема може призвести до конфліктів, дублювання адрес, пошкодження даних або нестабільної роботи сервісу. Для її запобігання використовують механізми кворуму, контроль доступності спільних ресурсів, додаткові канали зв'язку між вузлами та чітко визначені правила вибору активного вузла.

Після перемикання система має або автоматично повернутися до початкового стану після відновлення основного вузла, або залишитися на резервному до ручного втручання адміністратора. Вибір залежить від політики організації та характеру сервісу. Автоматичне повернення може бути зручним, але іноді воно створює ризик повторних перемикань, якщо основний вузол працює нестабільно.

9.7.8. Географічне резервування та аварійне відновлення

Для критичних сервісів резервування в межах одного майданчика може бути недостатнім. Пожежа, затоплення, тривале відключення електроживлення, аварія у провайдера або інша масштабна подія може зробити недоступним увесь центр обробки даних. У таких випадках потрібне географічне резервування.

Географічне резервування передбачає розміщення компонентів сервісу на кількох фізично віддалених майданчиках. Це можуть бути два центри обробки даних, основний майданчик і хмарне середовище або кілька регіонів хмарного провайдера.

Існує кілька моделей географічного резервування.

У моделі "активний/резервний майданчик" основний центр обробки даних обробляє трафік, а резервний використовується лише під час аварії. Такий підхід простіший, але резервні ресурси можуть простоювати більшу частину часу.

У моделі "активний/активний майданчик" кілька майданчиків одночасно обслуговують користувачів. Це дозволяє краще використовувати ресурси, зменшити затримку для користувачів із різних регіонів і підвищити стійкість сервісу. Водночас така модель складніша, оскільки потребує синхронізації даних, глобального балансування та узгоджених процедур перемикання.

Аварійне відновлення — це сукупність процедур, які дозволяють відновити роботу сервісу після масштабної відмови. Воно включає резервне копіювання, реплікацію даних, підготовлені плани відновлення, перевірку працездатності резервних майданчиків і регулярні навчання персоналу.

План аварійного відновлення має відповідати показникам RTO і RPO. Якщо організація вимагає відновлення сервісу за 15 хвилин, недостатньо мати лише резервну копію, яку можна вручну відновлювати кілька годин. Архітектура має бути спроєктована відповідно до реальних часових вимог.

9.7.9. Висока доступність у WAN та SD-WAN

У WAN-мережах висока доступність залежить від стійкості каналів зв'язку, граничних маршрутизаторів, протоколів маршрутизації, VPN-тунелів, систем безпеки та сервісів, які використовують ці канали. Відмова одного елемента може призвести до недоступності філії або погіршення якості роботи застосунків.

Традиційний підхід до HA у WAN передбачає дублювання каналів і маршрутизаторів, використання кількох провайдерів, протоколів динамічної маршрутизації та резервування шлюзів. Така схема працює ефективно, але потребує уважного налаштування пріоритетів маршрутів, часу збіжності та політик перемикання.

SD-WAN розширює можливості високої доступності, оскільки дозволяє одночасно використовувати кілька типів каналів: MPLS, широкосмуговий Інтернет, LTE/5G, супутникові або інші з'єднання. Система може постійно оцінювати якість кожного каналу та спрямовувати трафік відповідно до вимог конкретного застосунку.

Наприклад, голосовий трафік може передаватися через канал із найменшою затримкою та джитером, а резервне копіювання — через менш дорогий канал із більшою затримкою. Якщо основний канал втрачає якість або повністю відмовляє, SD-WAN може автоматично перемкнути трафік на інший доступний шлях.

Для критичних сервісів важливо не лише мати резервний канал, а й перевіряти, чи здатний він реально забезпечити необхідну якість. Якщо резервний канал має надто малу пропускну здатність або високу затримку, сервіс формально залишиться доступним, але працюватиме незадовільно.

9.7.10. Моніторинг високої доступності

Висока доступність неможлива без якісного моніторингу. Система має постійно контролювати стан обладнання, каналів, сервісів, кластерів, балансувальників, джерел живлення, систем зберігання та резервних майданчиків.

Для моніторингу HA використовуються:

- SNMP для контролю стану пристроїв та інтерфейсів;
- Syslog для фіксації подій і перемикань;
- NetFlow/IPFIX для аналізу трафіку;
- NMS для централізованого відображення стану мережі;
- перевірки доступності сервісів;
- журнали кластерів і балансувальників;
- засоби моніторингу баз даних і прикладних систем.

Особливо важливо контролювати не лише основні компоненти, а й резервні. Поширеною помилкою є ситуація, коли резервний канал або вузол існує формально, але давно не перевірявся і в момент аварії виявляється непрацездатним.

Система моніторингу має повідомляти не лише про повну відмову, а й про деградацію. Наприклад, збільшення затримки, зростання втрат пакетів, нестабільність каналу або часті перемикання між вузлами можуть бути ознаками майбутньої серйозної проблеми.

Також важливо відстежувати фактичний рівень доступності за певний період і порівнювати його з вимогами SLA. Якщо сервіс має забезпечувати 99,99% доступності, організація повинна мати достовірні дані, які підтверджують або спростовують виконання цієї вимоги.

9.7.11. Тестування аварійних сценаріїв

Наявність резервних компонентів не гарантує, що вони спрацюють під час реальної аварії. Тому високодоступні архітектури потрібно регулярно тестувати.

Тестування аварійних сценаріїв може включати:

- вимкнення одного з резервованих маршрутизаторів;
- від'єднання основного каналу зв'язку;
- перевірку перемикання шлюзу;
- перевірку роботи балансувальника при відмові сервера;
- тестування відновлення бази даних;

- перевірку резервного майданчика;
- відпрацювання процедур аварійного відновлення.

Такі перевірки бажано проводити планово, у погоджені часові вікна, з попередньою підготовкою та фіксацією результатів. Після тесту потрібно аналізувати, чи спрацювало перемикання, скільки часу тривало відновлення, чи були втрати даних, чи отримали адміністратори потрібні сповіщення та чи відповідає результат вимогам RTO і RPO.

Навчання з аварійного відновлення допомагають команді відпрацювати дії під час реальної відмови. Під час таких навчань моделюється аварійна ситуація, перевіряються інструкції, ролі відповідальних осіб, канали комунікації та технічні процедури.

У деяких сучасних інфраструктурах застосовується контрольоване тестування стійкості, коли окремі компоненти навмисно виводяться з роботи для перевірки реакції системи. Такий підхід може бути корисним, але його потрібно застосовувати дуже обережно, лише після підготовки та з чіткими межами впливу.

9.7.12. Типові помилки під час проєктування НА

Під час проєктування високої доступності часто виникають типові помилки.

Перша помилка — ототожнення резервування з високою доступністю. Наявність другого маршрутизатора або каналу не гарантує безперервності роботи, якщо немає автоматичного перемикання, моніторингу та перевірених процедур відновлення.

Друга помилка — залишення одиничних точок відмови. Наприклад, мережа може мати два маршрутизатори, але один комутатор агрегації, через який проходить увесь трафік. У такому разі саме комутатор залишається критичною точкою відмови.

Третя помилка — відсутність тестування. Схема може виглядати правильно на документації, але під час реальної аварії не спрацювати через помилку конфігурації, застарілу резервну копію або недоступний резервний канал.

Четверта помилка — ігнорування залежностей між сервісами. Наприклад, вебсервіс може бути зарезервований, але залежати від єдиного сервера бази даних або єдиного сервера автентифікації.

П’ята помилка — занадто складна архітектура без належної документації. Складні рішення можуть підвищувати доступність, але якщо адміністратори не розуміють логіку їхньої роботи, відновлення після аварії може затягнутися.

Шоста помилка — відсутність моніторингу резервних компонентів. Резервний вузол, який не перевірявся місяцями, може виявитися непрацездатним саме тоді, коли він потрібен.

Сьома помилка — невідповідність рівня НА реальним потребам. Надмірне прагнення до “п’яти дев’яток” для некритичного сервісу може призвести до невиправданих витрат, тоді як недостатній рівень доступності для критичного сервісу створює ризики для всієї організації.

9.7.13. Рекомендації щодо побудови високодоступної архітектури

Під час побудови високодоступної архітектури насамперед потрібно визначити критичність сервісів. Не всі системи потребують однакового рівня доступності. Для кожного сервісу варто встановити вимоги до RTO, RPO, допустимого простою та вартості перерви в роботі.

Далі необхідно виявити всі одиничні точки відмови. Для цього аналізують фізичну топологію, логічні залежності, джерела живлення, канали зв'язку, сервери, системи зберігання, бази даних, балансувальники, системи автентифікації та моніторингу.

Після цього потрібно обрати механізми резервування й автоматичного перемикання. Для шлюзів можуть використовуватися HSRP, VRRP або GLBP. Для каналів — динамічна маршрутизація, SD-WAN або резервні VPN-тунелі. Для серверів — кластеризація, балансування навантаження та реплікація даних.

Важливо передбачити моніторинг усіх компонентів, включно з резервними. Система має виявляти не лише повну відмову, а й деградацію якості роботи.

Необхідно створити документацію: схеми мережі, опис залежностей, інструкції перемикання, контакти відповідальних осіб, порядок дій у разі аварії та правила повернення до штатного режиму.

Також потрібно регулярно тестувати аварійні сценарії. Перевірка має підтверджувати, що фактичний час відновлення відповідає встановленим вимогам, а персонал знає порядок дій.

Окрему увагу слід приділяти оновленням. Високодоступна система має дозволяти виконувати обслуговування з мінімальним простоєм: почергово оновлювати вузли, переводити трафік на резервні компоненти й повертати їх у роботу після перевірки.

9.7.14. Значення високої доступності для глобальних мереж

Висока доступність є однією з базових вимог до сучасних глобальних мереж. Вона забезпечує безперервність роботи сервісів, зменшує вплив відмов, підвищує довіру користувачів і дозволяє виконувати вимоги угод про рівень обслуговування.

У глобальних мережах HA охоплює не один окремий компонент, а всю інфраструктуру: маршрутизатори, комутатори, канали зв'язку, провайдерські підключення, VPN, балансувальники, сервери, бази даних, системи моніторингу, живлення та аварійного відновлення.

Ефективна висока доступність ґрунтується на поєднанні технічних і організаційних заходів. Потрібні не лише резервні пристрої, а й моніторинг, автоматизація, документація, перевірені сценарії відновлення та підготовлена команда.

Таким чином, висока доступність є підсумковим елементом моніторингу та оптимізації мережі. SNMP дозволяє контролювати стан обладнання, NetFlow та IPFIX — аналізувати трафік, Syslog — фіксувати події, NMS — об'єднувати дані в єдину систему управління, балансування навантаження — розподіляти запити, а HA забезпечує безперервність роботи всієї інфраструктури навіть за наявності відмов.

Контрольні питання

1. Що таке моніторинг мережі та яку роль він відіграє в забезпеченні стабільної роботи глобальної мережевої інфраструктури?
2. Чим відрізняється моніторинг мережі від її оптимізації?
3. Яке призначення протоколу SNMP у системах моніторингу мережі?
4. Які основні компоненти входять до архітектури SNMP та яку функцію виконує кожен із них?
5. Чим відрізняються версії SNMPv1, SNMPv2c та SNMPv3 з погляду безпеки?
6. Що таке MIB та OID у контексті SNMP і для чого вони використовуються?
7. У чому полягає основна відмінність між SNMP і NetFlow?
8. Що таке мережевий потік у технології NetFlow?
9. За якими сімома ключовими полями класичний NetFlow визначає належність пакета до потоку?
10. Яке призначення кешу NetFlow і за яких умов запис потоку експортується до колектора?
11. Чим Flexible NetFlow відрізняється від класичних версій NetFlow?
12. Яке значення має шаблонна структура NetFlow v9 і чому вона є гнучкішою за фіксований формат NetFlow v5?
13. Для яких завдань у мережевому адмініструванні та безпеці використовується Syslog?
14. Чому централізований збір журналів подій є важливим для безпеки мережевої інфраструктури?
15. Яку роль відіграє синхронізація часу під час аналізу журналів подій Syslog?
16. Що таке система управління мережею NMS і які основні функції вона виконує?
17. Які напрями охоплює модель FCAPS і як вони пов’язані з управлінням мережею?
18. Які рівні деталізації аналізу трафіку використовуються в сучасних мережах?
19. Яке призначення балансування навантаження та які основні алгоритми розподілу запитів між серверами використовуються?
20. Що таке висока доступність мережі та чим вона відрізняється від простого резервування компонентів?
21. Які переваги та обмеження має вибірковий збір трафіку в NetFlow/IPFIX?
22. Чому для критичних систем доцільно використовувати передавання Syslog-повідомлень через TCP або TLS, а не лише через UDP?
23. Які типові помилки можуть виникати під час впровадження системи управління мережею NMS?
24. Як аналіз трафіку допомагає виявляти DDoS-атаки, сканування мережі або ознаки витоку даних?
25. Які метрики використовуються для оцінювання високої доступності системи: MTBF, MTTR, RTO та RPO?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bejtlich R. The Practice of Network Security Monitoring. 2013. 376 с.
2. Building multiservice transport networks (networking technology) / R. Harris та ін. Cisco Press, 2006. 576 с.
3. Cheswick W. R., Bellovin S. M., Rubin A. D. Firewalls and Internet security. 2-ге вид. Boston : Addison-Wesley, 2003. 433 с.
4. Cisco firewalls. Indianapolis, IN : Cisco Press, 2011. 889 с.
5. Fiber optic data communication: technological trends and advances / ред. D. C. M. San Diego : Academic Press, 2002. 568 с.
6. Ghein L. D. MPLS fundamentals. Cisco Press, 2006. 672 с.
7. Gilman E., Barth D. Zero Trust Networks. O'Reilly Media, 2017. 315 с.
8. Halabi S. Metro ethernet. Pearson Education, Limited, 2003. 240 с.
9. Hassan M. Wireless and Mobile Networking. CRC Press LLC, 2022. 282 с.
10. Hucaby D. Cisco CCNP certification library (CCNP self-study). 4-те вид. Cisco Press, 2007. 665 с.
11. Kuhn R., Sriram K., Montgomery D. Border Gateway Protocol Security. National Institute of Standards and Technology, 2007. 61 с.
12. Kurose J. F., Ross K. W. Computer networking: a top-down approach. 8-ме вид. Pearson Education, Limited, 2021. 797 с.
13. Lam C. F. Passive Optical Networks. Elsevier, 2007. 369 с.
14. Lammle T. CCNA routing and switching complete study guide: exam 100-105, exam 200-105, exam 200-125. Wiley & Sons, Incorporated, John, 2016. 1136 с.
15. Lee B. G. Broadband wireless access and local networks: Mobile WiMax and WiFi. Boston, Mass : Artech House, 2008. 618 с.
16. Mauro D., Schmidt K. Essential SNMP. O'Reilly Media, Incorporated, 2001. 291 с.
17. Northcutt S., Novak J. Network intrusion detection. 3-тє вид. New Riders Pub., 2002. 512 с.
18. Osborne E., Simha A. Traffic Engineering with MPLS. Brand: Cisco Press, 2002. 608 с.
19. Pepelnjak I., Guichard J. MPLS and VPN architectures, volume I. Cisco Press, 2002. 512 с.
20. Pepelnjak I., Guichard J., Apcar J. MPLS and VPN architectures, volume II. Cisco Press, 2003. 504 с.
21. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. 5-те вид. Prentice Hall, 2015. 944 с.
22. Stallings W. Data and computer communications. 8-ме вид. Pearson Education, Limited, 2007. 901 с.
23. Subramanian M., Gonsalves T. A., Rani N. U. Network management: principles and practice. Pearson Education India, 2010. 726 с.
24. Varghese G. Network algorithmics. 2005. С. 491.
25. William S. Network security essentials: applications and standards. 4-те вид. Upper Saddle River, N.J : Pearson Prentice Hall, 2011. 432 с.
26. Zhou X. Wi-Fi 6. 2021. 69 с.

ПРИМІТКИ

Навчальне видання

Марія КОЛОЩУК
Ольга ДЯЧУК

ГЛОБАЛЬНІ МЕРЕЖІ

Навчальний посібник

Електронне видання

Редактори
Комп’ютерна верстка: Колощук М.С.

Гарнітура Arial
Ум. друк. арк. 21,12 (60×84/8)

Державний університет «Житомирська політехніка»
м. Житомир, вул. Чуднівська, 103