ЛЕКЦІЯ 6

Моделі надання послуг

та якість обслуговування (QoS) у глобальних мережах

Навчальна дисципліна

«Глобальні мережі»

Державний університет «Житомирська політехніка»
Кафедра кібербезпеки та захисту інформації

Що було й що буде сьогодні

Пригадуємо ключове з лекції 5 та плануємо лекцію 6

← Лекція 5: що знаємо

- Виділені канали WAN: T1, E1, leased lines
- DTE / DCE / CSU-DSU — фізичне з'єднання
- HDLC — ISO/IEC 13239; Flag 0x7E; I/S/U
- Cisco HDLC vs ISO HDLC — поле Type
- PPP RFC 1661: LCP + NCP + автентифікація
- PAP (clear text) vs CHAP (MD5 challenge)

Лекція 6: що вивчимо →

1. Традиційні моделі: leased lines, MPLS VPN
2. Хмарні послуги: IaaS, PaaS, SaaS
3. Концепція XaaS: NaaS, SECaaS, UCaaS
4. SLA — угоди про рівень обслуговування
5. Метрики QoS: bandwidth, delay, jitter, loss
6. Модель IntServ (RFC 1633) + RSVP
7. Модель DiffServ (RFC 2474/2475) + DSCP
8. Механізми QoS: LLQ, WRED, shaping

Традиційні моделі мережевих послуг

Leased Lines · MPLS VPN · Managed Network Services — фундамент операторського бізнесу

Leased Lines

виділені канали

Постійно виділений канал фіксованої пропускної здатності між двома точками

✓ **Гарантії:**
гарантована смуга 24/7, мінімальна затримка

Реалізація:
T1 (1,544 Мбіт/с), E1 (2,048 Мбіт/с), T3, OC-3

Застосування:
критично важливі з'єднання; банки, дата-центри

MPLS VPN

тривалий час — основа корпоративних WAN

Ізоляція трафіку клієнтів на MPLS-інфраструктурі оператора

✓ **Гарантії:**
гарантована QoS, масштабування без зміни архітектури клієнта

Реалізація:
L3VPN (RFC 4364), L2VPN (VPWS, VPLS, EVPN)

Застосування:
з'єднання множини філій великих корпорацій

Managed Services

керовані мережеві послуги

Оператор бере на себе управління обладнанням, моніторинг, реагування на інциденти

✓ **Гарантії:**
рівень відповідальності визначається SLA

Реалізація:
аутсорсинг мережевої інфраструктури

Застосування:
клієнти без власного мережевого персоналу

Хмарні моделі надання послуг

Хто керує чим: On-Premise · IaaS · PaaS · SaaS



IaaS

віртуальні сервери, сховища, мережі

Приклади: Amazon EC2 · Azure · Google Compute Engine

Користувач: *IT-адміністратори*

PaaS

платформа для розробки й розгортання

Приклади: Google App Engine · Heroku · AWS Elastic Beanstalk

Користувач: *Розробники*

SaaS

готові програмні додатки через Інтернет

Приклади: Microsoft 365 · Google Workspace · Salesforce · Zoom

Користувач: *Бізнес-користувачі*

XaaS та угоди SLA

Everything as a Service — сучасна еволюція хмарних послуг + формалізація гарантій

Концепція XaaS · Everything as a Service

Тенденція надавати БУДЬ-ЯКІ IT-ресурси у формі хмарних сервісів

NaaS — **Network as a Service**
віртуальні мережеві ресурси без придбання обладнання

SECaaS — **Security as a Service**
кібербезпека через хмару: DDoS-захист, моніторинг

UCaaS — **Unified Communications as a Service**
інтегровані комунікації: VoIP, відео, месенджери

SASE — **Secure Access Service Edge**
об'єднання SD-WAN + SECaaS у єдиний хмарний сервіс

SLA · Service Level Agreement

Формальний документ, що визначає параметри якості послуг та відповідальність сторін

Типова SLA включає 4 групи параметрів:

1. **Доступність**
   наприклад, 99,95% — не більше 4 год 22 хв простою на рік
2. **Продуктивність**
   пропускна здатність, затримка, джитер, втрати пакетів
3. **Підтримка**
   час реагування, час відновлення (MTTR)
4. **Компенсація**
   service credits — від 5% до 100% місячної плати

Що таке QoS і навіщо він потрібен

Quality of Service — диференційоване обслуговування різних типів трафіку

Проблема «Best Effort»

Без механізмів QoS мережа обробляє всі пакети ***однаково*** за принципом «найкращих зусиль».

Це означає: голосовий трафік, який не терпить затримки >150 мс, обробляється ***так само, як і Torrent,*** якому байдужі і затримка, і черговість пакетів.



Bandwidth

Пропускна здатність

макс. обсяг даних за одиницю часу (біт/с, кбіт/с, Мбіт/с)



Delay

Затримка

час передачі пакета від джерела до одержувача (мс)



Jitter

Джитер

варіація затримки між послідовними пакетами (мс)



Packet Loss

Втрати пакетів

відсоток пакетів, які не досягли одержувача (%)

Рекомендовані параметри QoS для різних типів трафіку

Джерело: ITU-T G.114, RFC 5127

Тип трафіку	Затримка	Джитер	Втрати	Пропускна здатність
VoIP (голос)	**< 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

Затримка — 4 складові

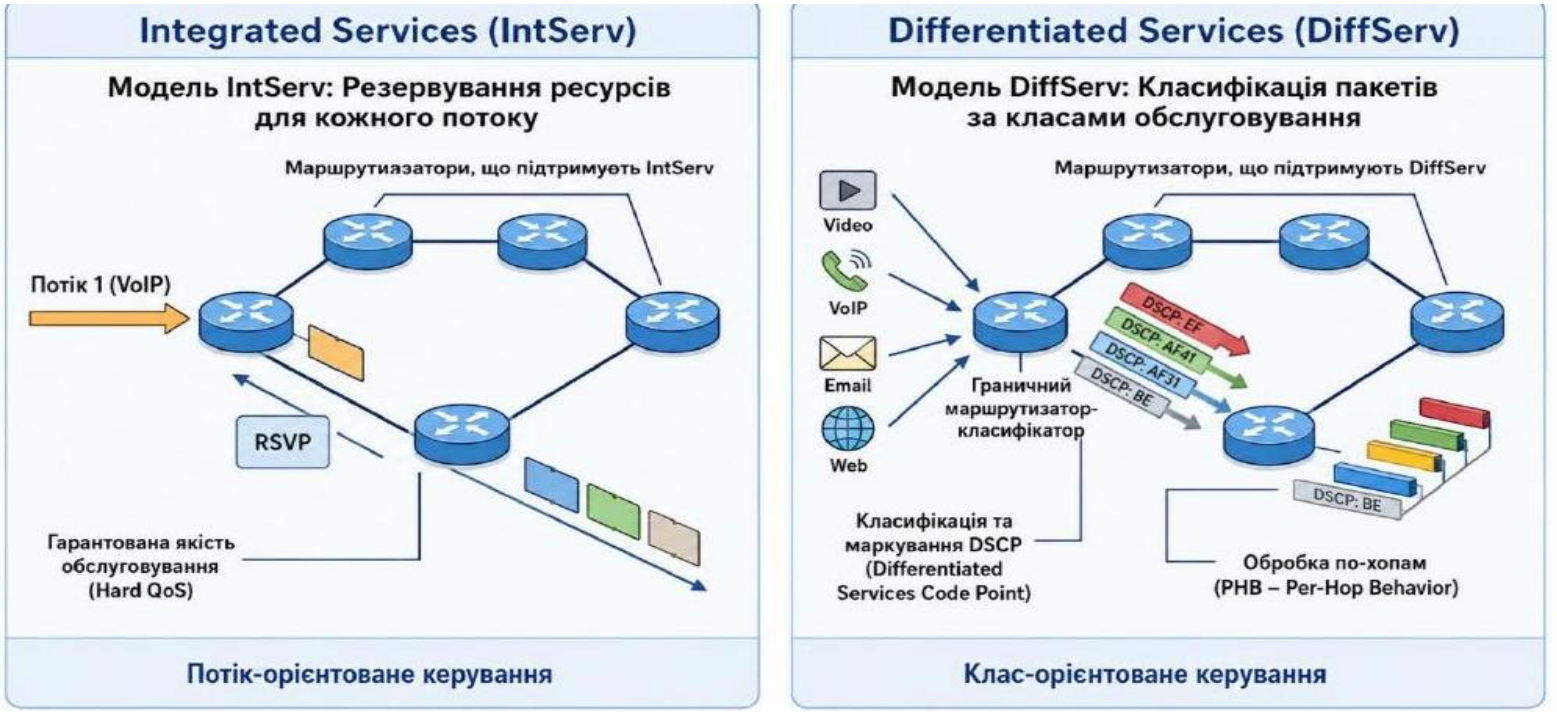
- **Серіалізація** — час на «виштовхування» біт в канал
- **Поширення** — швидкість світла у волокні (~5 мкс/км)
- **Обробка** — час на маршрутизацію в кожному вузлі
- **Черга** — очікування у чергах маршрутизатора *(← QoS тут!)*

Кодеки VoIP — реальні цифри

- **G.711** — 64 кбіт/с *(еталонна якість, PSTN)*
- **G.729** — 8 кбіт/с *(економічний варіант)*
- **Opus** — 6–510 кбіт/с *(гнучкий, сучасний)*
- **HD-відеоконференція:** 4–8 Мбіт/с

Дві моделі QoS: IntServ та DiffServ

Потік-орієнтоване vs клас-орієнтоване керування якістю



IntServ (RFC 1633) · резервування ресурсів · протокол RSVP
два класи: **Guaranteed Service** (жорстка затримка) + **Controlled Load**
✗ **недолік:** *не масштабується — по стану для кожного потоку в кожному маршрутизаторі*

DiffServ (RFC 2474, 2475) · маркування DSCP · до 64 класів
поле **DSCP (6 біт)** у заголовку IP · ключова концепція: **PHB (Per-Hop Behavior)**
✓ **перевага:** *масштабується — стан тільки для класу, не для кожного потоку*

DiffServ у деталях: DSCP та PHB

6-бітове поле у заголовку IP + чотири стандартні класи поведінки

Поле DSCP у заголовку IP



Поле ToS/DS · 1 байт · до 64 класів (2^6)

→ **Маркування на кордоні** мережі (edge router). Далі кожен маршрутизатор в ядрі обробляє за DSCP-значенням — це і є PHB.

PHB — Per-Hop Behavior

Стандарт визначає, як пакет має бути оброблений на кожному вузлі

- **Default PHB** — best effort (за замовчуванням)
- **Expedited Forwarding (EF)** — DSCP 101110 · для голосу
- **Assured Forwarding (AF)** — AF1x…AF4x, 4 класи × 3 рівні відкидання = 12 значень
- **Class Selector (CS0–CS7)** — для зворотної сумісності зі старим IP Precedence

Типове відображення DSCP → застосунок у корпоративній мережі

DSCP	Ім'я	Клас трафіку	Пріоритет
101110 (46)	EF	VoIP (голос)	найвищий
100010 (34)	AF41	Відеоконференція	високий
011010 (26)	AF31	Multimedia streaming	середній +
010010 (18)	AF21	Транзакційні дані	середній
000000 (0)	Default (BE)	Web-трафік, файли	звичайний

Механізми управління перевантаженнями (Queuing)

Congestion Management — як маршрутизатор упорядковує пакети у чергах

FIFO — *First In, First Out*

Найпростіший — жодних пріоритетів. Хто перший, той і перший виходить.

✓ **простий, дешевий**

✗ *критичний трафік може «застрягти» за великими файлами*

PQ — *Priority Queuing*

Абсолютний пріоритет — черга вищого пріоритету обслуговується першою завжди.

✓ **гарантований пріоритет**

✗ *starvation — низькопріоритетний трафік може ніколи не пройти*

WFQ — *Weighted Fair Queuing*

Справедливий розподіл смуги між потоками з урахуванням ваг (пріоритетів).

✓ **справедливість, без starvation**

✗ *не гарантує жорсткої затримки для голосу*

CBWFQ — *Class-Based Weighted Fair Queuing*

Окрема черга для кожного налаштованого класу трафіку з мінімальною смугою.

✓ **керовані класи, гарантована смуга**

✗ *все ще не ідеально для голосу*

LLQ — *Low Latency Queuing*

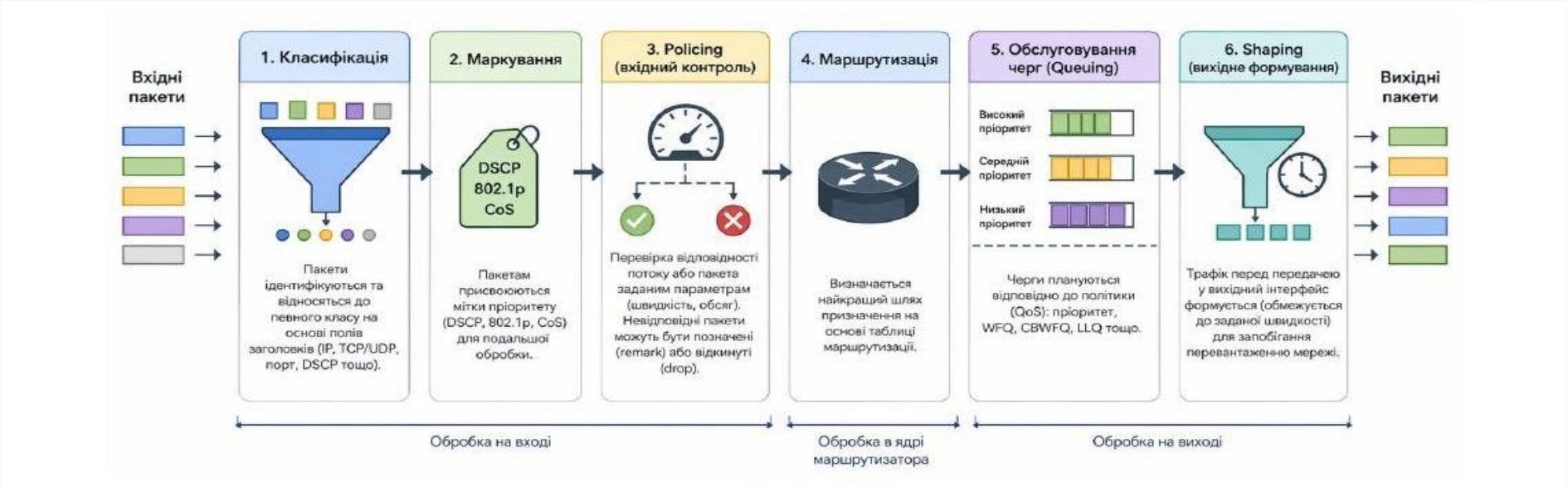
Поєднує PQ + CBWFQ: пріоритетна черга ДЛЯ ГОЛОСУ + обмежені класові черги для решти.

✓ **гарантована мінімальна затримка для голосу**

✗ *потрібне грамотне налаштування policing*

Інші механізми QoS: WRED, Shaping, Policing

Запобігання перевантаженням та формування трафіку



WRED

Weighted Random Early Detection

Запобігання перевантаженню: випадкове відкидання пакетів ще ДО повного заповнення черги, з урахуванням пріоритету.

★ ***альтернатива: Tail Drop (просто відкидає при переповненні)***

Shaping

Traffic Shaping (Token Bucket)

Формування трафіку: згладжує піки, буферизуючи надлишкові пакети до дозволеної швидкості. Пакети НЕ відкидаються.

★ ***виконується на ВИХІДНИХ інтерфейсах***

Policing

Traffic Policing

Обмеження трафіку: відкидає АБО перемарковує надлишкові пакети. Не буферизує — просто карає перевищення.

★ ***виконується на ВХІДНИХ інтерфейсах***

QoS у сучасних мережах: MPLS та SD-WAN

Як реалізовано QoS у двох основних операторських технологіях

QoS у MPLS

Поле TC у MPLS-заголовку

3 біти · до 8 класів обслуговування · аналогічне DSCP

MPLS Traffic Engineering (MPLS-TE)

явно визначає шляхи трафіку через мережу за допомогою протоколу **RSVP-TE**

DiffServ-Aware MPLS-TE

поєднує DiffServ + MPLS-TE:

- **голос** → пріоритетне обслуговування
- **бізнес-критичні дані** → гарантована смуга
- **best-effort** → ресурси, що залишилися

QoS у SD-WAN

Application-Aware Routing

ідентифікація конкретних застосунків через **Deep Packet Inspection**

Динамічний вибір каналу

Контролер моніторить кожен WAN-канал (затримка, джитер, втрати) та обирає найкращий для кожного застосунку.

Failover за якістю:

якщо Інтернет-канал деградує — голос **автоматично** переключається на MPLS

WAN-оптимізація:

- FEC (Forward Error Correction) — зменшення втрат
- Дуплікація пакетів для критичних застосунків
- Оптимізація TCP для каналів з високою затримкою

Практичний приклад: VoIP через WAN

Як забезпечити якість голосового виклику на всьому шляху від абонента до абонента

Вимоги для VoIP-виклику (кодек G.711)

Затримка	Джитер	Втрати пакетів	Пропускна здатність
< 150 мс	**< 30 мс**	**< 1 %**	**~ 87 кбіт/с***

* *G.711 payload 64 кбіт/с + IP/UDP/RTP overhead ≈ 87 кбіт/с з урахуванням заголовків*

Ланцюжок QoS-механізмів вздовж шляху пакета

1. **На IP-телефоні**
   маркування пакета → DSCP = EF (46)
2. **На комутаторі доступу**
   trust boundary — довірять чи перемаркувати; CoS 802.1p
3. **На маршрутизаторі CE**
   класифікація → LLQ: голос у пріоритетну чергу
4. **На вході в WAN**
   policing вхідного трафіку відповідно до SLA
5. **У ядрі оператора**
   MPLS TC = 5 · DiffServ-Aware MPLS-TE
6. **На виході**
   shaping відповідно до контракту клієнта

Порівняння традиційних моделей послуг

Leased Lines · Frame Relay · MPLS VPN · Internet VPN · SD-WAN

Критерій	Leased Line	MPLS VPN	Internet VPN	SD-WAN
Гарантія смуги	повна	SLA-контракт	немає (best effort)	адаптивно
Затримка	мінімальна	низька, стабільна	змінна	оптимізується
QoS	N/A (виділено)	DiffServ-Aware TE	обмежена	Application-aware
Вартість	найвища	висока	низька	середня
Швидкість розгортання	повільна (місяці)	середня (тижні)	миттєва	швидка
Типовий сценарій	критичні з'єднання	корпоративні WAN	філії з Інтернетом	гібридні мережі

Головні тренди сучасності

- → **MPLS** поступово поступається місцем **SD-WAN** (нижча вартість, вища гнучкість)
- → **Виділені канали** залишаються тільки для критично важливих з'єднань (банкінг, оборона, дата-центри)
- → **Гібридні мережі** (MPLS + Інтернет + LTE/5G) стають нормою — SD-WAN керує ними як одним ресурсом

Підсумок лекції

01 **Традиційні моделі послуг**

Leased Lines, MPLS VPN, Managed Services — основа операторського бізнесу

02 **Хмарні моделі: IaaS, PaaS, SaaS**

5 характеристик NIST; від максимального контролю до мінімальної складності

03 **XaaS та SLA**

NaaS, SECaaS, UCaaS, SASE; SLA формалізує доступність (99,9%…99,999%)

04 **4 метрики QoS**

bandwidth, delay (<150 мс для голосу), jitter (<30 мс), loss (<1%)

05 **IntServ vs DiffServ**

IntServ (RFC 1633, RSVP) — не масштабується; DiffServ (RFC 2474/2475, DSCP) — стандарт

06 **Механізми: LLQ, WRED, Shaping**

LLQ = PQ+CBWFQ для голосу; WRED — випадкове відкидання; shaping — на виході

→ **Наступна лекція:** *агрегування каналів WAN (MLPPP)*



Ваші запитання

Обговорення матеріалу лекції

Дякую за увагу!