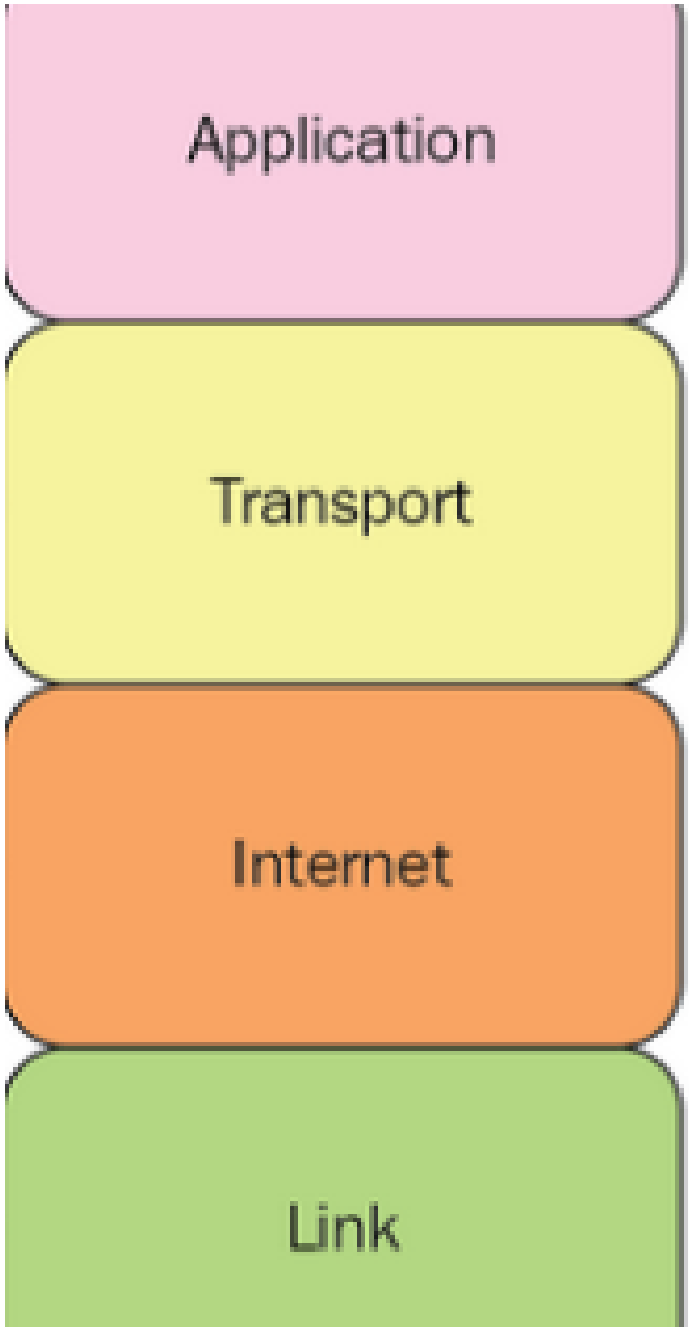
Транспортний рівень моделі OSI. Протоколи TCP та UDP

AGENDA

- Загальна інформація про транспортний рівень моделі OSI
- Послуги
- Протокол TCP
- Протокол TCP. Порти
- Протокол TCP. Сегменти і потоки
- Протокол TCP. З'єднання
- Заголовок TCP сегменту
- Протокол UDP
- Команда NETSTAT

Загальна інформація про транспортний рівень моделі OSI

- У комп'ютерних мережах транспортний рівень - це концептуальний набір мережевих функцій у чотирьохрівневій еталонній моделі DoD (та реалізованому на ній стеку протоколів TCP/IP) та семирівневій еталонній моделі OSI. Протоколи цього рівня забезпечують послуги зв'язку між хостами для додатків. Він надає такі послуги, як зв’язок, орієнтований на з'єднання, надійність, контроль потоку та мультиплексування.



Загальна інформація про транспортний рівень моделі OSI

- Найвідоміший транспортний протокол стеку протоколів TCP/IP - це протокол управління передачею (TCP). Він використовується для передачі, орієнтованої на з'єднання, тоді як протокол не орієнтований на з'єднання User Datagram (UDP) використовується для більш простої передачі повідомлень.
- TCP - це більш складний протокол, завдяки його продуманому дизайну, який включає надійні послуги передачі даних. Разом TCP і UDP складають, по суті, весь трафік в Інтернеті і є єдиними протоколами, реалізованими у всіх основних операційних системах.

Послуги

Послуги транспортного рівня передаються додатку через програмний інтерфейс до протоколів транспортного рівня. Послуги можуть включати такі функції:

- Зв'язок, орієнтований на з'єднання: програмі зазвичай простіше інтерпретувати з'єднання як потік даних, а не мати справу з моделями, що не мають з'єднання, такими як дейтаграмна модель протоколів UDP та IP.

- Доставка в однаковому порядку: мережевий рівень, як правило, не гарантує, що пакети даних будуть надходити в тому ж порядку, в якому вони були надіслані, але часто це бажана функція. Зазвичай це відбувається за допомогою нумерації сегментів, одержувач передає їх додатку в однаковому порядку.

Послуги

- Надійність: пакети можуть втрачатися під час транспортування через перевантаженість мережі та помилки. За допомогою коду виявлення помилок, такого як контрольна сума, транспортний протокол може перевірити, чи не є дані пошкоджені, і перевірити правильність отримання, надіславши відправнику повідомлення ACK або NACK.
- Контроль потоку: швидкість передачі даних між двома вузлами іноді повинна бути керована, щоб запобігти відправнику передавати більше даних, ніж може підтримуватися буфером прийому даних, викликаючи перевищення буфера.

Послуги

- Уникнення перевантажень: відстеження перевантажень може контролювати входження трафіку в телекомунікаційну мережу, щоб уникнути колапсу перевантаження, шляхом зниження швидкості відправки пакетів.
- Мультиплексування: порти можуть надавати кілька кінцевих точок входу (endpoints) на одному вузлі. Наприклад, ім'я на поштовій адресі є різновидом мультиплексування та відрізняє різних одержувачів одного і того ж поштового сервера. Комп'ютерні програми на вузлі будуть отримувати інформацію на своїх власних портах, що дає змогу використовувати більше ніж одну мережеву послугу одночасно. Мультиплексування є частиною транспортного рівня в моделі TCP / IP, але сеансового рівня в моделі OSI.

Протокол TCP

- TCP це орієнтований на з'єднання протокол, який забезпечує надійну, впорядковану та перевірену на предмет помилок доставку потоку октетів (байтів) між програмами, що працюють на хостах, що спілкуються через мережу IP. Основні Інтернет-служби, такі як всесвітня павутина (WWW), електронна пошта, віддалене адміністрування та передача файлів, покладаються на TCP.
- Протокол TCP описаний у RFC: 793.
- В контексті протоколу TCP використовуються такі поняття як порти, сегменти, потоки, з'єднання.

Протокол TCP. Порти

- TCP і UDP використовують номери портів для ідентифікації програмних кінцевих точок входу на хості, які відправляють та отримують дані. Такі програмні кінцеві точки входу часто називають Інтернет-сокетами.
- Кожна сторона TCP-з'єднання має пов'язаний 16-бітний номер (0-65535), зарезервований програмою, що надсилає або приймає дані. TCP-пакети, що надходять, ідентифікуються як такі, що належать певному TCP-з'єднанню комбінацією адреси хоста джерела, порту джерела, адреси хоста призначення та порту призначення. Наприклад, 192.168.0.4:51023 52.114.74.217:443

Протокол TCP. Порти

- Це означає, що серверний комп'ютер може надавати декільком клієнтам кілька сервісів одночасно. Наприклад, ми з одного комп'ютера можемо відкрити одночасно декілька різних веб-сторінок з одного веб-сервера.
- Номери портів класифікуються на три основні категорії:
- - відомі (well-known - (0 – 1023))
- - зареєстровані (registered - (1024 – 49151))
- - динамічні/приватні (dynamic or private - (49152 -65535)).
- Відомі порти присвоюються адміністрацією адресного простору Інтернет (IANA) і зазвичай використовуються на системному рівні або кореневими процесами.

Протокол TCP. Порти

- Зазвичай використовують ці порти загальновідомі програми, що працюють як сервери та пасивно прослуховують з'єднання. Деякі приклади включають: FTP (20 та 21), SSH (22), TELNET (23), SMTP (25), HTTP через SSL / TLS (443) та HTTP (80).
- Зареєстрований порт - це мережевий порт призначений IANA для використання з певним протоколом або додатком, наприклад, 3306 : MySQL, 8008 : HTTP Alternate.
- Динамічні номери портів (також відомі як приватні номери портів) - номери портів, які доступні для використання будь-якою програмою для спілкування з будь-яким іншим додатком, використовуючи протокол управління передачею в Інтернеті (TCP) або протокол User Datagram (UDP)).

Протокол TCP. Сегменти і потоки

- Інформація, яка надходить протоколу TCP від прикладного рівня розглядається як неструктурований потік байтів. Для передачі на мережевий рівень із потоку вирізається деяка неперервна частина байтів, до неї додається заголовок і формується TCP сегмент (пакет).
- На відміну від інших протоколів, протокол TCP підтверджує отримування не пакетів, а байтів потоку.

Протокол TCP. З'єднання

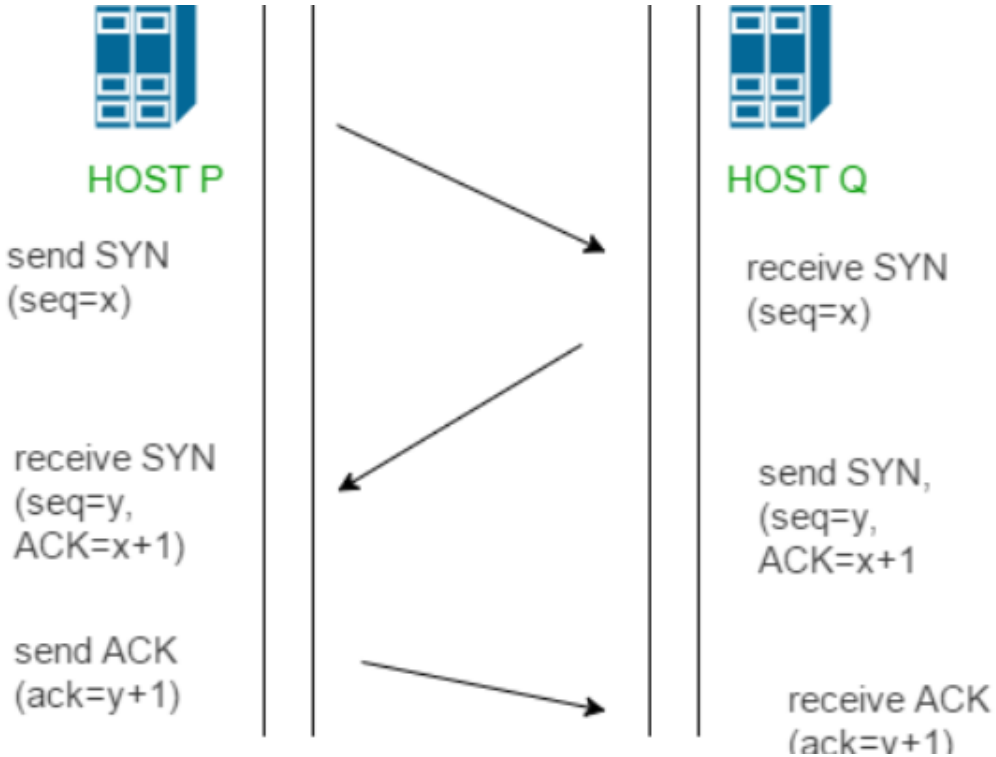
- Для організації надійної передачі даних передбачається встановлення логічного з'єднання між двома прикладними процесами. Для запобігання помилкової ініціалізації з'єднань використовується спеціальна процедура підтвердження зв'язку - так зване трикрокове рукостискання (three-way handshake).
- Процес складається із трьох кроків:
- 1. Клієнт посилає серверу сегмент з початковим номером послідовності (initial sequence number) и прапором SYN.
- Сервер намагається створити буфери та керуючі структури пам'яті сокету для обслуговування нового клієнта;
- У випадку успіху сервер посилає клієнту сегмент з номером послідовності і прапорами SYN и ACK, і переходить до стану SYN-RECEIVED;
- У випадку невдачі сервер посилає клієнту сегмент с прапором RST.

Протокол TCP. З'єднання

- 2. Якщо клієнт отримує сегмент з прапором SYN, то він посилає сегмент з прапором ACK.
- Якщо він одночасно отримує і прапор ACK (що зазвичай і відбувається), то він переходить в стан ESTABLISHED;
- Якщо клієнт отримує сегмент з прапором RST, то він припиняє спроби з'єднатися;
- Якщо клієнт не отримує відповіді протягом 10 секунд, то він повторює процес з'єднання заново.

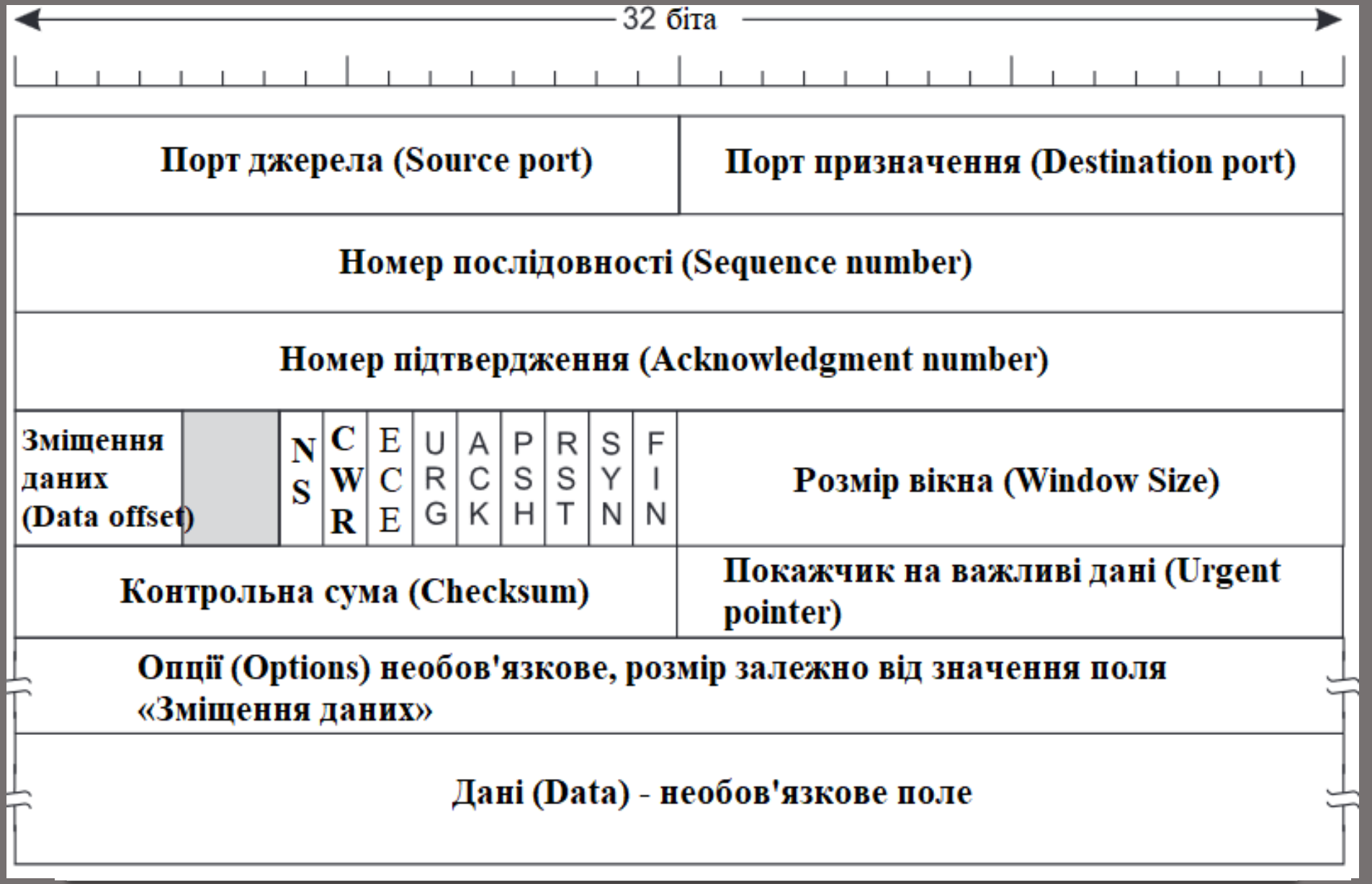
Протокол TCP. З'єднання

- 3. Якщо сервер в стані SYN-RECEIVED отримує сегмент з прапором ACK, то він переходить в стан ESTABLISHED.
- В іншому випадку після тайм-ауту він закриває сокет і переходить в стан CLOSED. Див. рис.



Протокол TCP. З'єднання

- Формально з'єднання можна визначити як набір параметрів, які характеризують процедуру обміну даними між процесами. Це такі параметри як повні адреси процесів (тобто IP-адреса + номер порту), узгоджені розміри сегментів, які може відсилати кожна із сторін, розмір вікна, початкові номери даних, які передаються.
- В протоколі TCP для забезпечення поєднання надійності з продуктивністю передачі даних використовується алгоритм ковзного вікна (Sliding window algorithm) - див лекцію "Методи передачі даних на канальному рівні".



Формат TCP сегменту

Заголовок TCP сегменту

- Кожен сегмент починається з заголовка фіксованого формату, який має розмір мінімум 20-байтів. За ним можуть слідувати додаткові поля (параметри).
- Порт джерела (Source port) ідентифікує номер TCP-порту, з якого відправляється сегмент.
- Порт призначення (Destination port) ідентифікує номер TCP-порту, на який відправляється сегмент.
- Номер послідовності (Sequence number) є числом, що відображає номер першого байту в поточному сегменті надісланих даних від хоста-відправника до хоста-отримувача. Якщо встановлений прапор SYN (йде встановлення сесії), то поле містить початковий порядковий номер - ISN (Initial Sequence Number). З метою безпеки це значення генерується випадковим чином і може дорівнювати від 0 до 2^{32}-1. Використовується для відстежування кількості та правильної послідовності отриманих сегментів даних.

Заголовок TCP сегменту

- Номер підтвердження (Acknowledgment number) відображає кількість уже отриманих хостом байт плюс ISN протилежної сторони.
- Зміщення даних (Data offset) 4-бітний номер, який визначає розмір TCP-заголовка в 32-бітових словах. Мінімальний розмір становить 5 (0101) слів, а максимальний — 15 (1111), що є відповідно 20 і 60 байт. Фактично визначає розмір поля Опції (Options) від 0 до 40 байт.
- 100—102 біти, зарезервовані для майбутнього використання і повинні містити нулі *(000)*.

Заголовок TCP сегменту

- Поле прапорці (керуючі біти) - прапорці вважається встановленими, якщо їх бітове значення є *1*.
- - NS — Одноразова сума (Nonce Sum), використовується з метою покращення роботи механізму явного повідомлення про перевантаження (Explicit Congestion Notification, ECN).
- - CWR — Вікно перевантаження зменшено (Congestion Window Reduced), прапорець встановлюється, щоб показати що TCP-сегмент був отриманий зі встановленим полем ECE, іншими словами це є підтвердженням отримання сегменту даних з прапорцем ECE від хоста партнера.

Заголовок TCP сегменту

- - ECE — ECN-Exo (ECN-Echo), поле показує, що відправник підтримує ECN.
- - URG — Важливість (Urgent), вказує, що TCP-сегмент містить важливі дані. Важливі дані відправляються до відповідного протоколу верхнього рівня минаючи чергу і без перевірки успішності надходження попередніх сегментів.
- - ACK — Підтвердження (Acknowledge) успішності отримання TCP-сегменту
- - PSH — Просування (Push), також як і прапорець URG, вказує, на пріоритетність TCP-сегменту. Хост-відправник позачергово надсилає цей сегмент даних через IP-мережу. За аналогією з прапорцем URG, PSH інструктує хост-отримувач, що сегмент даних має бути негайно переданий до прикладного рівня (кінцевого споживача даних).

Заголовок TCP сегменту

- - RST — Обривання (Reset) вказує, хосту-отримувачу негайно скинути з'єднання без подальшої взаємодії. Така ситуація наступає у разі, якщо сервер (хост-відправник) не надає послуги визначеного сервісу.
- - SYN — Синхронізація (Synchronize) використовується для встановлення з'єднання між хостами при так званому трикроковому рукостисканні
- - FIN — Фініш (Finish) вказує на завершення з'єднання

Заголовок TCP сегменту

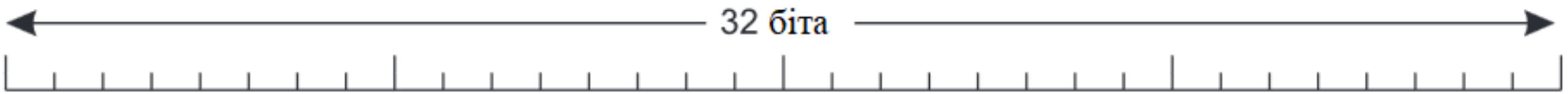
- Розмір вікна (англ. Window Size) визначає кількість байтів даних, які відправник може надіслати до того, як отримає підтвердження (запит на новий сегмент) від хоста-отримувача
- Контрольна сума (Checksum) розраховується на основі усього TCP-сегменту включно із заголовком та важливих полів IP-пакету: IP-адрес хостів відправника та отримувача, номеру протоколу (TCP має номер 6) та загального розміру IP-пакету. Контрольна сума забезпечує можливість перевірки цілісності надісланих даних.

Заголовок TCP сегменту

- Покажчик важливості (Urgent pointer). Поле береться до уваги тільки в разі встановленого прапорця URG, та містить значення зміщення відносно номеру послідовності сегменту. Фактично це число вказує на позицію в TCP-сегменті де закінчуються важливі дані. Тобто важливі дані знаходяться одразу після TCP-заголовка і закінчуються перед місцем на яке вказує покажчик важливості.

Протокол UDP

- Серед набору протоколів стеку TCP/IP є транспортний протокол без встановлення з'єднання, UDP (User Datagram Protocol - протокол передачі дейтаграм користувача). UDP дозволяє додаткам відправляти мережеві пакети без встановлення з'єднань.
- За допомогою протоколу UDP передаються сегменти, що складаються з 8-байтного заголовка, за яким іде поле корисного навантаження. Див. рис .



Порт джерела (Source port)	Порт отримувача (Destination port)
Довжина UDP (Length)	Контрольна сума UDP (Checksum)

Протокол UDP

- Два номери портів служать для ідентифікації сокетів всередині відправляючої та приймаючої машини, аналогічно TCP.
- Поле Довжина UDP показує довжину заголовка і даних.
- Необов'язкове поле Контрольна сума служить для підвищення надійності. Воно містить контрольну суму заголовка, даних і псевдозаголовка (IP-адрес хостів відправника та отримувача, номеру протоколу (UDP має номер 17) та загального розміру IP-пакету).

Протокол UDP

- Протокол UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів і для яких неважлива надійність передалі даних.
- Наприклад, цей протокол може використовуватися для різноманітних мережевих ігор реального часу, потокового відео та аудіо.
- Також, UDP використовують такі протоколи прикладного рівня як:
- TFTP (англ. Trivial File Transfer Protocol, найпростіший протокол передачі файлів),
- SNMP (англ. Simple Network Management Protocol, простий протокол управління мережею),
- DHCP (англ. Dynamic Host Configuration Protocol, протокол динамічної конфігурації вузла),
- DNS (англ. Domain Name System, служба доменних імен).

Команда NETSTAT

- Команда NETSTAT призначена для отримання відомостей про стан мережних з'єднань і портах TCP і UDP, які прослуховуються на даному комп'ютері , а також, для відображення статистичних даних по мережних інтерфейсах і протоколах.
- Формат команди:
- NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
- Основні параметри:
- -a - Відображення всіх підключень і прослуховуючих портів
- -e - Відображення статистики Ethernet

Команда NETSTAT

- -p proto - Відображення підключень для протоколу, що задаються цим параметром. Можна вибрати зі значень TCP, UDP, TCPv6 або UDPv6. Використовується разом з параметром -s для відображення статистики по протоколам.
- -s - Відображення статистики протоколу. За замовчуванням статистика відображається для протоколів IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP і UDPv6.
- Interval - Повторне виведення статистичних даних через вказаний інтервал в секундах. Для припинення виведення даних натисніть клавіші CTRL + C. Якщо параметр не заданий, відомості про поточну конфігурацію виводяться один раз.

QUESTIONS

THANKS FOR YOUR ATTENTION