Лекція 3

Мережевий рівень

План лекції

- Завдання мережного рівня
- Функції протоколу IP
- Стандарти протоколу IP
- Адресація у протоколі IPv4
- Маски підмереж
- Формат заголовка пакета IPv4
- Контроль часу життя (TTL)
- Тип сервісу (QoS)
- Фрагментація

Завдання мережного рівня

- Доставка пакета від кінцевого вузла до кінцевого вузла в об’єднаній мережі
- Для цього використовується:
  - Універсальна адресація, яка забезпечує унікальні адреси у всій мережі
    - Адресація має бути ієрархічною, наприклад, за схемою адреса підмережі / адреса вузла
  - Просування (*forwarding*) пакета даних по об’єднаній мережі через послідовність підмереж до кінцевого вузла
  - Маршрутизація
    - Визначення шляху (послідовності транзитних вузлів), за яким пакет даних може досягти кінцевого вузла
- Протоколи мережного рівня
  - Мережні протоколи (IP, IPX)
  - Протоколи маршрутизації (RIP, OSPF, IS-IS, BGP)
  - Протоколи керування (ICMP)

Функції протоколу IP

- На рівні протоколу IP відпрацьовується передача пакета між мережами, і для цього передбачені ряд засобів:
  - Система глобальної адресації
  - Контроль часу життя пакета
  - Можливість динамічної фрагментації пакетів
  - Підтримка якості обслуговування
- Протокол IP відповідає лише за притаманні йому функції
  - Для передачі пакета всередині кожної з мереж, через які відбувається доставка, протокол IP звертається до засобів нижчого (канального) рівня
  - Питання гарантованої доставки пакета, його повторної передачі тощо — це справа засобів вищого (транспортного) рівня

Стандарти протоколу IP

- IP версії 4
  - IETF RFC-0791, Internet Protocol / J. Postel. – September 1981
- IP версії 6
  - IETF RFC-2460, Internet Protocol, Version 6 (IPv6) Specification / S. Deering, R. Hinden. – December 1998
  - IETF RFC-4291, IP Version 6 Addressing Architecture / R. Hinden, S. Deering. – February 2006

Адресація у протоколі IPv4

- Формат адреси: 32 біт
- Формат запису адреси: чотири числа, розмежовані крапками, що подають значення кожного октету в десятковій формі
- Класи адрес:

<table>
<tr><th></th><th colspan="5">Байт 1</th><th>Байт 2</th><th>Байт 3</th><th>Байт 4</th></tr>
<tr><td>Клас A</td><td>0</td><td colspan="4">№ мережі</td><td colspan="3">№ вузла</td></tr>
<tr><td>Клас B</td><td>1</td><td>0</td><td colspan="3">№ мережі</td><td colspan="2">№ вузла</td></tr>
<tr><td>Клас C</td><td>1</td><td>1</td><td>0</td><td colspan="3">№ мережі</td><td>№ вузла</td></tr>
<tr><td>Клас D</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="4">Адреса групи multicast</td></tr>
<tr><td>Клас E</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="3">Зарезервований</td></tr>
</table>

Діапазони адрес

Клас A 0.0.0.0 — 127.255.255.255

128 мереж по 16777216 адрес у кожній

Клас B 128.0.0.0 — 191.255.255.255

16384 мереж по 65536 адрес у кожній

Клас C 192.0.0.0 — 223.255.255.255

2097152 мереж по 256 адрес у кожній

Клас D 224.0.0.0 — 239.255.255.255

268435456 групових адрес

Клас E 240.0.0.0 — 247.255.255.255

Спеціальні адреси

0.0.0.0 – увесь простір IP адрес
127.0.0.0-127.255.255.255 – loopback (комп’ютерне “Я”)
255.255.255.255 – limited broadcast (не маршрутизується)
x.x.x.255 – broadcast (широкомовний для мережі x.x.x.0)

169.254.0.0-169.254.255.255 – автоматично самопризначається, якщо DHCP-сервер не відповідає

Для побудови локальних мереж (без маршрутизації в Інтернет) використовуються:
10.0.0.0-10.255.255.255 – 1 мережа класу A
172.16.0.0-172.31.255.255 – 16 мереж класу B
192.168.0.0-192.168.255.255 – 256 мереж класу C

Недоліки адресації IPv4

- Недостатній простір адрес
  - Лише 125 мереж класу A
- Недостатня структурованість:
  - Лише два рівня (номер мережі і номер вузла)
- Недостатня гнучкість:
  - Клас мережі визначає розрядність номера мережі і номера вузла
- Незручність використання “вручну”
  - Межа між номером мережі і номером вузла може знаходитись у різних місцях і визначається із самої адреси

Маски підмереж

- Фактично, це спроба додати гнучкості системі адресації IPv4
- Маска має вигляд неперервної послідовності одиниць, які відповідають розрядам IP-адреси, що віднесені до номеру мережі, за якою йде неперервна послідовність нулів, що відповідають розрядам IP-адреси, які віднесені до номеру вузла
- Маска може записуватись у такому самому вигляді, як і IP-адреса
  - Наприклад, для мережі класу C маску можна записати як 255.255.255.0.
- У масці кількість одиниць не обов'язково кратна 8
  - Наприклад, коректною є маска 255.255.240.0 (20 одиниць і 12 нулів)
  - Адреса 77.122.125.113 з маскою 255.255.240.0 означає:
    - номер мережі 77.122.112.0 і номер вузла 0.0.13.113
  - Адреса 77.122.125.113 без маски — адреса класу A:
    - номер мережі 77.0.0.0 і номер вузла 0.122.125.113
- Маски широко застосовуються у маршрутизації (так звана *безкласова маршрутизація*)
  - Для структурування мереж
  - Для виділення старшої частини адреси (так званого *префікса*), для зменшення об'ємів таблиць і підвищення продуктивності маршрутизаторів

Приклад з мережею класу С

	24 біта			**8 біт**	
Клас С	ідентифікатор мережі			ідент. вузла	
Маска підмережі:	11111111	11111111	11111111	00000000	=255.255.255.0
	255	255	255	0	

	26 біта				**6 біт**	
	ідентифікатор мережі				ідент. вузла	
Маска підмережі:	11111111	11111111	11111111	11	000000	=255.255.255.192
	255	255	255		192	

Формат заголовка пакета IPv4

<table>
<tr><td colspan="2">4 біта
Номер версії</td><td colspan="2">4 біта
Довжина заголовка</td><td colspan="5">8 біт
Тип сервісу
PR | D | T | R | </td><td colspan="4">16 біт
Загальна довжина</td></tr>
<tr><td colspan="6">16 біт
Ідентифікатор пакета</td><td colspan="2">3 біта
Прапорці
 | D | M</td><td colspan="5">13 біт
Зміщення фрагмента</td></tr>
<tr><td colspan="3">8 біт
Час життя (TTL)</td><td colspan="4">8 біт
Протокол верхнього рівня</td><td colspan="4">16 біт
Контрольна сума</td></tr>
<tr><td colspan="11">32 біта
IP-адреса відправника</td></tr>
<tr><td colspan="11">32 біта
IP-адреса призначення</td></tr>
<tr><td colspan="11">Опції та вирівнювання</td></tr>
</table>

Номер версії та довжина заголовку

Номер версії протоколу IP — 4 біти.

Для IPv4 має значення 4, для IPv6 — 6

Довжина заголовку — 4 біти.

Вказує на кількість рядків у заголовку. В одному рядку — 4 байти (32 біти). Найменше значення довжини — 5, тобто опції відсутні. Найбільше значення — F (1111 у бінарному вигляді або 15 у десятковому). Тобто максимальна довжина заголовку — 15 x 4 = 60 байт. Опції додаються рядком у 4 байти. Якщо опцій менше 4 байтів, то до рядка додаються байти вирівнювання — нульового значення.

Тип сервісу (QoS)

- Класичний варіант
  - PR (3 біта) – пріоритет
  - Прапорці
    - D – мінімізація затримки
    - T – максимізація перепускної спроможності
    - R – максимізація надійності доставки
  - 2 біта не використовують
- “Differentiated Services” – DiffServ
  - 3 старших біта – пріоритет
  - DP (2 біта) – Drop Precedence
  - 3 біта не використовують

Загальна довжина пакету

Поле загальної довжини пакету становить 2 байта (16 біт).

До загальної довжини пакету входить довжина заголовку пакету та його поля даних. Тому найменша довжина пакету не може бути меншою за довжину заголовку + 1 байт даних. Максимальна довжина пакету визначається максимальним значенням цього поля і становить FFFF у шістнадцятковій системи числення, або 65535 у десятковій. Інколи кажуть, що максимальна довжина IP пакету становить 64К-1 байт. У 1 кбайті — 1024 байти.

Фрагментація

- Кожна мережа має своє значення MTU
  - MTU – Maximum Transfer Unit
- Під час відправлення розмір пакета узгоджений з MTU тієї мережі, до якої підключений кінцевий вузол
  - Це завдання виконує протокол транспортного рівня
- На транзитному вузлі може виникнути ситуація, коли пакет неможливо передати за маршрутом через те, що MTU наступної мережі менший за розмір пакета. Тоді можна:
  - Або знищити пакет і надіслати відправнику ICMP повідомлення про знищення пакета і про необхідне значення MTU – тоді відправник зможе сам формувати пакети необхідного розміру
  - Або розділити пакет на частини (фрагменти) безпосередньо на транзитному вузлі

Підтримка фрагментації в IP

- Ідентифікатор пакета дозволяє розпізнавати фрагментовані пакети – усі фрагменти одного пакета мають однаковий ідентифікатор
- Прапорці:
  - D – не фрагментувати
  - M – не останній фрагмент
- Зміщення – 13 розрядів
  - Вимірюється не в байтах, а в блоках по 8 байт

Процедура збирання пакета з фрагментів

- Коли надходить пакет – перевіряють поля
  - Ідентифікатор пакета
  - Протокол
  - Адреса джерела
  - Адреса призначення
- Якщо такого набору значень полів раніше не було – вважають, що це фрагмент нової дейтаграми, і розпочинають її збирання
  - Виділяють буфер у 64кБ
  - Виділяють поле для бітової маски надходження блоків (кожний блок – 8 байт, отже маска 8 кб)
  - Якщо зміщення фрагменту, що надійшов, =0 (перший фрагмент) і прапорець M=0 (останній фрагмент), то збирання вважають завершеним
  - Інакше фрагмент, що надійшов, копіюють у буфер на місце, що визначене його зміщенням, і встановлюють відповідні біти у бітовій масці
  - Після цього процедуру збирання вважають завершеною лише тоді, коли бітова маска буде заповнена від початку і до кінця (кінець визначають за фрагментом, в якому M=0)
  - Послідовність надходження фрагментів значення не має
  - Якщо фрагмент, що надійшов, повинен бути вставленим у місце в буфері, яке вже зайняте, то згідно RFC його треба вставляти, замінюючи ті дані, що надійшли раніше

Контроль часу життя

- Спочатку встановлюється певне значення часу життя (максимум 255)
- Під час проходження кожного транзитного вузла час життя зменшується на 1
- Якщо час життя зменшується до 0, транзитний вузол повинен знищити пакет і повідомити про це відправника
- Дозволяє уникнути нескінченної циркуляції пакета внаслідок помилок у маршрутизації
- Дозволяє обмежити розповсюдження пакета
  - наприклад, встановлення часу життя у 1 забезпечує доставку пакета лише найближчим сусідам
- Дозволяє проводити дослідження (трасування) маршруту
  - Відправляють послідовність пакетів з часом життя 1, 2, 3 і т.д.
  - Отримують відповіді про знищення пакета через вичерпання часу життя від усіх транзитних вузлів послідовно