*Лекція № **4**.*
ТЕЗИ

Протокол IP: адресація та маршрутизація. Організація підмереж. ПРОДОВЖЕННЯ

Пригадаємо НАЙВАЖЛИВІШІ речі з попердньої лекції:

IP адреса призначається НЕ комп'ютеру а інтерфейсу.
IP адреса містить інформацію про мережу: складається з ***розділу (поля) мережі та розділу (поля) вузла***.
Кількість байт, відведена під адресу мережі і під адресу вузла ***НЕОДИНАКОВА*** для всіх адрес.
Класи адрес: A (0- 127), B (128 – 191), C(192 – 223).
IP адреси можуть мати три можливі значення (***адреса мережі, адреса хоста, broadcast адреса***)
Маска підмережі.
Показує, ***скільки біт IP адреси відведено під розділ мережі***.
Маска – НЕ адреса.
Маска була введена з метою гнучкішого розбиття адресного простору на підмережі, на "адресні простори". З допомогою масок стає можливою ***CIDR*** – безкласова міждоменна маршрутизація.

В сьогоднішній лекції розглянемо приклад організації мережі з трьох підмереж а також розглянемо трохи детальніше питання маршрутизації та мультиплексінгу.

Два важливі RFC документи:
RFC 1878 описує всі можливі маски і адреси підмереж.
RFC 1918 – виділення адрес для приватного використання.

Звідки беруться IP адреси?
Виділення адрес знаходиться в компетенції 3-ох рівневої бюрократичної машини:

1.***IANA*** – The Internet Assigned Numbers Authority (http://www.iana.org/) - служба призначення числових Інет адрес. Виділяє крупні блоки адрес регіональним реєстраторам Інету
2.Регіональні реєстратори:
RIPE – в Європі та на Близькому Сході (http://www.ripe.net/).

3.Локальний реєстратор Інету. Можна подивитись список на http://www.ripe.net/ для України. В загальному випадку потрібно зв'язатися в першу чергу з найближчим провайдером.

Маршрутизація

IP доставляє дані з допомогою ***шлюзів.***
В початковій структурі мережі існувала ієрархія шлюзів. Існувала одна магістральна мережа, її шлюзи називалися ***магістральними шлюзами*** (core gateways). Ці шлюзи зберігали інформацію про маршрутизацію для всієї мережі. Вони обробляли і обмінювалися інформацією за допомогою GGP протоколу.
GGP – Gateway to Gateway Protocol – протокол взаємодії шлюзів. З його допомогою обмінюються інформацією шлюзи і тепер. + Інші протоколи.
З часом магістральна мережа втратила своє значення і зараз працює т.зв. ***доменна модель маршрутизації*** в Інеті.
Доменна модель працює на основі т.зв. ***автономних систем*** - системи шлюзів з спільним механізмом збору інформації про маршрутизацію та передачі її іншим незалежним системам.
Домени маршрутизації обмінюються інформацією з допомогою протоколу ***BGP*** – Border Gateway Protocol.
Існує також база даних (розприділена) ***PRDB – Policy Routing Database,*** за ведення якої відповідають регіональні реєстратори.

Маршрутизація на основі серверів (доменів) маршрутизації називається динамічною. На сервері працює демон routed який отримує інфо про маршрути.
Однак багато провайдерів не використовують динамічну маршрутизацію а будують власні правила маршрутизації на основі приватних договорів з іншими провайдерами. Таку маршрутизацію можна класифікувати як статичну: здійснюється на основі статичних таблиць маршрутизації.

Для того, щоб переглянути таблицю маршрутизації в Linux використовується команда **route**, а в BSD-системах – **netstat**.
Формат таблиці маршрутизації – дуже простий: важливими по-суті є тільки 2 перших поля:
Destination – ціль – адреса, з якою порівнюється IP того, кому пакет призначено;
Gateway – маршрутизатор, через який проходить шлях до вказаної в Destinaion адреси.

Іншими словами, для абсолютної більшості систем прийняття рішення про маршрутизацію базується на простому алгоритмі:

- якщо хост-адресат знаходиться в одній мережі зі мною, дані доставляються напряму адресату.
- якщо адресат знаходиться в зовнішній мережі – передаємо дані на шлюз по замовчуванню.

Зауважити, що тут власне стає зрозуміло навіщо використовують адресні маски:
для локальної доставки використовується адресна частина (розділ) IP адреси, а для передачі між мережами – мережева частина IP адреси.

Мультиплексія

Коли дані доставлені на локальну машину їх потрібно передати на вищий рівень і в кінці кінців відповідному користувачу чи процесу.
Система повинна вміти коректно передавати дані від багатьох різних процесів з допомого нечисленних протоколів транспортного та Інет рівнів.
На локальній машині може працювати багато аплікацій (браузер, клієнт ел. пошти, ftp клієнт), але ВСІ дані передаються за однією схемою на нижчих рівнях.

Об'єдання багатьох джерел даних в один потік називається мультиплексією (**multiplexing**)

Відповідно, доставлені дані потрібно ***демультиплексувати***.

Для вирішення задачі передачі на транспортний рівень в IP використовується ***нумерація протоколів***.
Файл ***/etc/protocols***

```
ip     0      IP            # internet protocol, pseudo protocol number
tcp    6      TCP           # transmission control protocol
udp    17     UDP           # user datagram protocol
```

Номер протоколу передається в одному з байтів 3-ого слова заголовку пакету IP.

Для передачі на прикладний рівень протокли (TCP, UDP) використовують ***номери портів.***
Файл ***/etc/services***

```
http          80/tcp    www www-http #World Wide Web HTTP
http          80/udp    www www-http #World Wide Web HTTP
```

Номери портів до 1024 – т.зв. ***зарезервовані***
від 1024 до 49151 – ***зареєстровані***
вище 49151 - ***приватні***

Номерами протоколів та портів займається IANA (див. вище). Ведеться реєстр і потійно додаються нові як протоколи так і порти.

Важливим є також поняття ***динамічного виділення порта***
Динамічні номери портів призначаються процесам при потребі.
Гаратнується, що двом різним процесам не буде призначено однаковий динамічний порт і що призначений номер порта буде в приватному діапазоні.

Обмін портами здійснюється при встановленні зв'язку TCP.
Динамічно порт призначається як правило на сторні клієнта а на сторні сервера працює аплікація на стандартному порті.
Таким чином клієнт може відкрити декілька з'єднань з одни і тим же сервісом на сервері.

Пара, що складається з IP адреси та номера порта називається сокетом.
Сокет однозначно ідентифікує будь-який мережевий процес в Інет.

На лаб роботах ми побачимо, як працює зв'язка IP адрес – номер порта.

Приклад

Допустимо, що ми хочемо організувати мережу для невеликої організації, яка має три підрозділи, що територіально знаходяться в одному будинку. Окрім того допустимо, що нам потрібно забезпечити доступом до Інет всіх працівників організації

Незв'язані та зв'язані з Інет мережі.

Вирішити скільки *реальних* (*зовнішніх*) IP адрес нам потрібно.
Допустимо, що 1 зовнішньї адреси вистачить.
Провайдер дає нам

- або IP, IP зовнішнього дня нас шлюзу (gateway), netmask, dns сервери

- або дає змогу отримувати цю інформацію динамічно (IP при цьому може бути стала) по протоколу ***DHCP – Dynamic Host Configuration Protocol***.

В будь якому з цих випадків нам потрібно

- побудувати локальну мережу
- настроїти свій шлюз так, щоб з його допомогою могли користуватись Інетом всі клієнти внутрішньої мережі.

  Це робиться з допомогою технології (і демона) NAT – Network Address Translation або/і proxy-сервісів.
- подбати про безпеку.

Виберемо для внутрішньої мережі мережу класу С 192.168.3.0.
Адресний простір – 256 адрес 192.168.3.0 – 192.168.3.255
Оскільки підмереж нам потрібно три (три незалежні підрозділи), то можемо розбити наш адресний прстір на чотири підмережі по 64 адреси в кожній а далі 2 з них об'єднати в одну:

<table>
<tr><td rowspan="4">Маска:
63 = 111111
отже тільки 6 останніх бітів для адреси хоста,

11000000=192

255.255.255.192

/26</td><td>адреса мережі: 192.168.3.0
діапазон хост адрес: 192.168.3.1-192.168.3.62
broadcast адреса: 192.168.3.63</td><td></td></tr>
<tr><td>адреса мережі: 192.168.3.64
діапазон хост адрес: 192.168.3.65-192.168.3.126
broadcast адреса: 192.168.3.127</td><td></td></tr>
<tr><td>адреса мережі: 192.168.3.128
діапазон хост адрес: 192.168.3.129-192.168.3.190
broadcast адреса: 192.168.3.191</td><td rowspan="2">об'єднаємо в одну підмережу:
адреса мережі: 192.168.3.128
діапазон хост адрес: 192.168.3.129-192.168.3.254
broadcast адреса: 192.168.3.255
маска буде: 255.255.255.128 або /25</td></tr>
<tr><td>адреса мережі: 192.168.3.192
діапазон хост адрес: 192.168.3.193-192.168.3.254
broadcast адреса: 192.168.3.255</td></tr>
</table>

Можна як завгодно об'єднувати підмережі, *але ПРИДАТНІ до використання IP адреси визначаються найменшою мережею*! Приклад. адреси 192.168.3.191 і 192.168.3.192 НЕ будуть видимі з двох інших, менших підмереж. В деяких моментах це може бути зовсім не принципово, але восновному на це слід звертати увагу.

НАМАЛЮВАТИ МАЛЮНОК:

сервер GW з 1 інтерфейсом зовнішнім і трьома внутрішніми (перші адреси в відповідному діапазоні), NAT. Пояснити конфігурацію інтерфейсфв.

три hubs і три підмережі.

Пояснити машрути, трансляцію адрес (NAT).

Плюси використання NAT і proxy-сервісів.
Недоліки NAT, недоліки proxy-сервісів.