

2. MAC-адреса

MAC-адреса (мак адреса) - це унікальний ідентифікатор мережевого інтерфейсу (зазвичай мережевої карти) для реалізації комунікації пристроїв в мережі на фізичному рівні.

Це унікальний номер, який зберігається у пам'яті, що доступна тільки для читання, призначена мережевій карті її виробником.

Довжина MAC-адреси дорівнює 48 бітам, що забезпечує 248 (або 281,474,976,710,656) загальне число всіх можливих адрес. Як правило, MAC-адреса записується як шість груп подвійних шестнадцятирічних чисел, розділених символами "-" або ":". Наприклад, MAC-адреса може виглядати так - "00:11:22:33:44:55", або так - "67-78-89-AB-CD-EF".

Щоб дізнатися MAC-адресу мережевих пристроїв на своєму комп'ютері, достатньо просто набрати "ifconfig" в командному рядку Linux, "ipconfig /all" в командному рядку Windows, або "networksetup -listallhardwareports" у Mac OS. Її буде відображено, як значення полів "HWaddr", "Physical address", або "Ethernet address" відповідно.

Загалом, MAC-адреса призначається на постійній основі пристрою і не може бути змінена. Але в деяких випадках існує можливість зміни MAC-адреси на програмному рівні. Це відомо, як MAC-спуфінг.

4. IP-адреси

Для зручнішого читання IP адресу представляють у вигляді чотирьох десяткових чисел², в діапазоні від 0 до 255, що розділені крапкою. Наприклад: 130.50.30.42. Її прийнято називати IP v. 4, або IPv4 (IP версії 4).

Перебравши всі можливі комбінації таких чисел можна підрахувати, що максимальна кількість IP-адрес — приблизно 4,2 мільярда штук.

В 70-х роках минулого століття, коли тільки виникла мережа Інтернет, ця кількість здавалася більш ніж достатньою. Сьогодні ж, коли з інтернетом працюють мільярди людей, коли навіть холодильники і лампочки можуть користуватися інтернетом, стало очевидно, що такої кількості IP-адрес не вистачає.

Світові організації що займаються розподілом адрес більше не видають їх провайдерам. Вільних IPv4-адрес, офіційно, більше немає.

Ipv6.

В 90-х роках минулого століття розробили вдосконалену версію правил обміну інформацією в мережі — протокол IPv6 (протокол IP версії 6). Для позначення IP-адреси в IPv6 використовуються не 4 байти (числа від до 256) а 16. Тому можлива кількість адрес IPv6 зростає до 340 трильйонів штук.

Проте, для використання IPv6 цей протокол мають використовувати всі учасники мережі: абонент, провайдер, інтернет-ресурс (сайт). Використання нового протоколу збільшується, але доволі повільно. І відмовитися від IPv4, на даний момент, неможливо.

Протоколи IPv4 та IPv6 можуть працювати одночасно, паралельно.

Реальні, та нереальні адреси (білі та сірі)

Як правило, навіть у звичайній квартирі, інтернет-пристроїв є декілька: комп'ютер, телефони, планшети. Але провайдер не видає по одній адресі для кожного пристрою, вона лише одна на одного абонента.

Для того щоб інтернетом могли користуватися усі домашні пристрої використовується спеціальне обладнання — роутери. Вони є посередником між інтернетом і Вашою домашньою мережею.

Уявіть собі що живете в ізольованій країні, з якої не випускають людей. І Ви не можете придбати будь-який товар за кордоном. Але є спеціальні люди, нехай дипломати, які мають таке право. Вони отримують замовлення від людей всередині країни, перетинають кордон, купують все необхідне, а після повернення роздають товар тому, хто його замовляв.

Ваш роутер отримує замовлення від усіх пристроїв домашньої мережі і завантажує інформацію з інтернету від свого імені, використовуючи одну IP-адресу що надана йому провайдером. Для світу виглядає що інтернетом користується лише один пристрій, хоча за ним насправді приховуються декілька різних.

В домашній мережі пристрої впізнають одне одного теж за допомогою IP-адрес. Існують спеціальні діапазони IP-адрес які рекомендовано використовувати в домашніх та локальних мережах підприємств. Наприклад 192.168.0.0-192.168.255.255.

Такі адреси називають приватними, або внутрішніми, або "сірими" чи "нереальними". Бо вони доступні лише в межах Вашої внутрішньої мережі. Від їх імені не можна надіслати інформацію в Інтернет чи отримати відповідь з Інтернету.

Такі, однакові, адреси можуть бути у і Вашого домашнього комп'ютера і в сусідського і на роботі. Вони використовуються для обміну інформацією лише в межах внутрішньої мережі, грубо кажучи — лише в межах Вашого приміщення (квартири, офісу).

IP-адреси що є унікальними в світі, які використовують провайдери, через які можна обмінюватися інформацією в Інтернеті називають зовнішніми, або "білими" чи "реальними".

Абоненту може видаватися "реальна" адреса. Від імені якої можна виходити в інтернет. На "реальну" адресу також можна приймати інформацію (коли хтось першим підключається до Вас, а не навпаки).

Якщо абоненту видається "нереальна" адреса, то з нею теж можна виходити в інтернет. Але це не прямий зв'язок з інтернетом — отримувати інформацію на "нереальну" адресу можна лише через посередника (сервер провайдера).

Для звичайного користування достатньо і "нереальної" IP-адреси. В більшості випадків користувач не відчуває жодних незручностей. Але коли користувач бажає отримати доступ до своєї адреси ззовні, з Інтернету (наприклад на внутрішній ігровий сервер, на систему відеоспостереження тощо) — потрібна "реальна", зовнішня IP-адреса.

Статична та динамічна IP-адреса

Тут все просто. Якщо адреса, що видається провайдером, незмінна, кожного разу однакова — то вона статична.

Якщо IP-адреса час від часу змінюється (наприклад після кожного підключення до провайдера) — то вона динамічна.

Коли абоненту потрібна зовнішня IP-адреса то, як правило, провайдер закріплює її за абонентом. Тому часто під словом "статична" мають на увазі "реальна" зовнішня IP-адреса.

Але насправді може бути як статична зовнішня адреса, так і динамічна зовнішня. Статичність і "реальність" це дві різні характеристики IP-адреси.

Як перевірити свою IP-адресу. Перш за все потрібно зрозуміти, що IP-адреса це характеристика мережевого підключення. Навіть на одному комп'ютері може бути декілька мережевих підключень і кожна з них може мати свою IP-адресу.

Наприклад роутер має щонайменше 2 IP-адреси. Одна — видана провайдером для роботи з Інтернетом, інша — локальна адреса для роботи з домашніми пристроями. IP-адреси можна переглянути на сторінці "Статус" роутера, або, якщо до провайдера підключається лише один комп'ютер, напряду, то переглянувши стан мережевого підключення.

В роутерах мережеве підключення до провайдера, як правило називають WAN (Wide Area Network), а підключення в локальну мережу LAN (Local Area Network). IP-адреса інтерфейсу WAN і буде адресою, яку видав провайдер.

Якщо ця IP адреса з діапазону:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

то це приватна ("сіра") IP адреса і Ви виходите в інтернет від імені IP-адреси посередника-провайдера. Інакше — у Вас зовнішня ("реальна") IP адреса.

Існують спеціальні сайти, які показують "Вашу IP-адресу" (наприклад ipinfo.io). Але треба пам'ятати, що вони показують не особисто Вашу адресу, а адресу з якої Вас видно в Інтернеті, а це насправді може бути адреса посередника (сервера-роутера в провайдера).

5. Мережеві реквізити (статичні та динамічні)

Мережеві реквізити можуть призначатися статично (вручну адміністратором) або динамічно за протоколом DHCP. До мережевих реквізитів належать:

- mac-адреса
- ip-адреса
- мережева маска
- шлюз за замовчанням (default gateway)
- dns-сервер

DHCP (аббревіатура від Dynamic Host Configuration Protocol – в перекладі «Протокол Динамічної Налаштування Вузла») – це технологія, призначена для автоматичного присвоєння IP-адрес мережних пристроїв. Безліч системних адміністраторів воліють використовувати DHCP замість ручного призначення IP-адрес мережевих комп'ютерів, при цьому DHCP також використовується для конфігурації маски підмережі, шлюзу і DNS-серверів.

Оточення DHCP вимагає двох складових елементів – це DHCP-сервера і клієнта DHCP.

Перший елемент (DHCP) встановлює потрібні параметри конфігурації мережі, присвоює і оновлює адреси для приєднуються або залишають мережу пристроїв.

Інший (DHCP-клієнт) підключається до мережі, отримує від сервера налаштування, і починає працювати. Набір DHCP-параметрів включає діапазон доступних IP-адрес, відповідну маску підмережі, шлюз мережі і ім'я для серверних адрес.

Пристрої, які мають активний DHCP-протокол, автоматично отримують потрібні налаштування від DHCP-сервера. Всі найбільш використовувані мережні пристрої (телефони, комп'ютери, ігрові приставки і ін) підтримують DHCP, мають DHCP і всі популярні нині операційні системи.

6. Маршрутизація за умовчанням — default gateway

Шлюз за умовчанням (англ. Default gateway), шлюз останньої надії (англ. Last hope gateway) — в маршрутизованих протоколах — адреса маршрутизатора, на який відправляється трафік, для якого неможливо визначити маршрут виходячи з таблиць маршрутизації. Застосовується в мережах з добре вираженими центральними маршрутизаторами, в малих мережах, в клієнтських сегментах мереж. Шлюз за умовчанням задається відповідним записом у таблиці маршрутизації виду «мережа 0.0.0.0 з маскою мережі 0.0.0.0».

Якщо мережа містить маршрутизатори, потрібно сконфігурувати шлюз за замовчуванням. Маршрутизатором називається пристрій, що з'єднує два чи більше сегменти мережі. В моделі взаємодії відкритих систем маршрутизатори функціонують на мережному рівні.

Для того щоб сконфігурувати сервер Windows Server 2003 як маршрутизатор, необхідно встановити дві чи більше мережних карт, зв'язати кожен з них із своїм мережним сегментом і сконфігурувати необхідним чином. Можна також використовувати маршрутизатори, що поставляються сторонніми організаціями; як правило, вони забезпечують більше можливостей, ніж сервери Windows Server 2003, сконфігуровані як маршрутизатори.

Припустимо, що мережа сконфігурована, як показано на Рис. 6.4. Мережна IP-адреса мережі А — 10.0.9.0, а мережі Б — 10.0.56.0. В цьому випадку потрібно налаштувати кожен мережну карту в маршрутизаторі на IP-адресу сегменту із яким вона з'єднана.

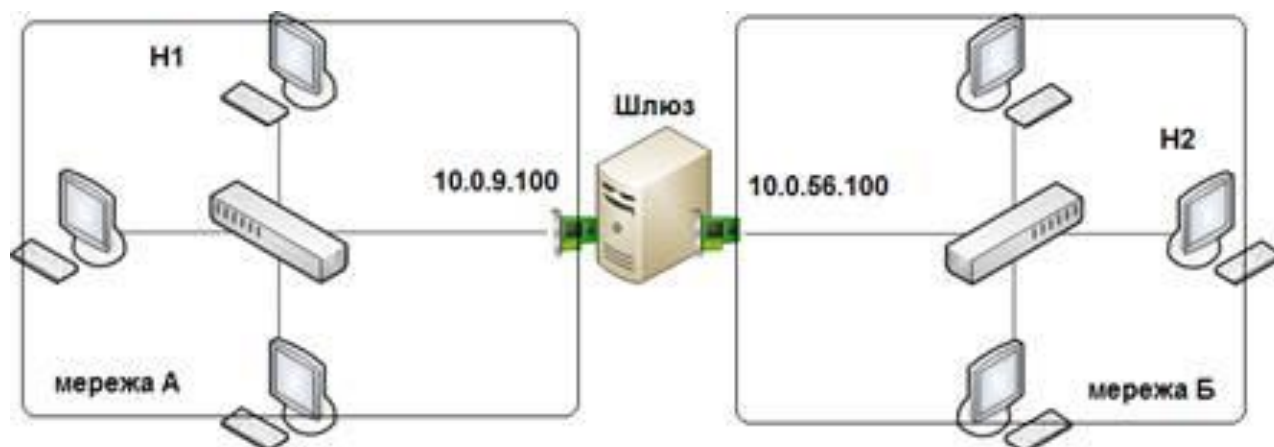


Рисунок – Конфігурування шлюзу за замовчуванням

Комп'ютери кожного сегменту конфігуруються так, щоб вказувати на IP-адресу мережної карти в маршрутизаторі, яка з'єднана з цим сегментом. Наприклад, комп'ютер Н1 на Рис. 6.2 з'єднаний з мережею А. Для нього конфігурується шлюз за замовчуванням з адресою 10.0.9.100. Комп'ютер Н2 зв'язаний з мережею Б, відповідний шлюз за замовчуванням має адреси 10.0.56.100.