ЛАБОРАТОРНА РОБОТА №3. АНАЛІЗ РОБОТИ МЕРЕЖЕВИХ ПРОТОКОЛІВ ARP(RARP), DNS, DHCP

Тема роботи: Аналіз роботи мережевих протоколів ARP (RARP), DNS, DHCP.

Мета роботи: Вивчити принципи роботи та призначення протоколів ARP (RARP), DNS, DHCP .

Теоретичні відомості

Поняття мережевого протоколу.

Комунікація включає термінали, комунікаційні застосування і мережу, яка об'єднує їх. Вони взаємодіють для досягнення правильної комунікації (наприклад, встановлюють і припиняють сесію) та для оптимального використання мережевих транспортних послуг. Для здійснення цієї взаємодії необхідні комунікаційні протоколи як між кінцевими користувачами і мережею, так і всередині мережі між різними мережевими вузлами. Вони забезпечують встановлення наскрізних маршрутів відповідно до запитів користувачів, забезпечують надійне і захищене пересилання інформації, моніторингу та управління мережею.

Будь-який обмін даними між людьми або комп'ютерами підкоряється заздалегідь встановленим правилам, або протоколам. Ці протоколи залежать від характеристик джерела, каналу і адресата. Вони чітко визначають формати і розмір повідомлень, синхронізацію, характеристики інкапсуляції, кодування і метод розсилки стандартного повідомлення.

Ці правила особливо важливі для локальних мереж. Локальна провідна мережа - це область, в якій всі вузли повинні "говорити однією мовою" або, якщо говорити комп'ютерною мовою, "використовувати один і той же протокол".

Якщо люди, котрі знаходяться в одній кімнаті, говорять на різних мовах, вони не зможуть один одного зрозуміти. Аналогічно, якщо пристрої в локальній мережі використовують різні протоколи, вони не зможуть обмінюватися даними.

Найчастіше в локальних провідних мережах використовується протокол Ethernet.

Він визначає багато аспектів обміну даними в локальній мережі, наприклад: формат і розмір повідомлення, синхронізацію, кодування та методи розсилки повідомлень.

Мережеві протоколи – це стандарти, які дозволяють мережевим вузлам комунікувати між собою. Під поняттям протокол в комп'ютерній мережі звичайно розуміють систему правил, опрацьованих для здійснення комунікації між комп'ютерами. Протоколи керують форматом, синхронізацією, упорядкованістю даних, а також забезпечують контроль помилок. Без таких правил комп'ютер не може сприймати значення потоку бітів, які поступають до нього.

Існує велика кількість протоколів для передавання даних, запропонованих різними фірмами-розробниками. Однак, якщо передавач і приймач не користуються тим же протоколом, то вони не зрозуміють один одного. Тому запропоновані та впроваджені стандарти протоколів, пристосовані до еталонної моделі OSI. На жаль, в дійсності протоколи не повністю відповідають означенням моделі OSI. Окремі з них об'єднують суміжні рівні, інші розділяють їх або відкидають деякі з них. Звичайно, всі працездатні протоколи дозволяють осягнути однаковий результат – перенесення даних з одного місця до іншого, однак питання полягає у їх взаємній сумісності, у можливості взаємодії мереж з різними протоколами.

Спільні питання для протоколів на різних рівнях.

Основні проблеми, з якими будемо неодноразово зустрічатися при розгляді різних протоколів.

Симплексний, півдуплексний та дуплексний режими передавання. Важливо встановити принципи передавання даних. Якщо дані повинні пересилатися тільки від джерела до призначення (або багатьох призначень), то йдеться про симплексний режим передавання (simplex). Якщо дані між двома респондентами пересилаються у двох напрямках, але неодночасно, то це півдуплексний режим передавання (half-duplex); при одночасному перенесенні даних між респондентами в обидвох напрямках йдеться про дуплексний режим (full duplex).

Пріоритети. Протокол повинен визначити, скільки логічних каналів відповідає даному зв'язку, та визначити їх пріоритети. В багатьох мережах існує не менше двох логічних каналів

для кожного зв'язку: один - для звичайних даних, а другий – для даних з підвищеним пріоритетом.

Управління потоками даних. На кожному рівні може виникнути проблема узгодження швидкостей передавача і приймача даних. Існують декілька способів вирішення цієї проблеми, однак спільним для них є використання певного зворотнього зв'язку між приймачем та передавачем інформації. Зворотня інформація передається безпосередньо або посередньо в залежності від стану приймача в даний момент часу.

Встановлення та припинення зв'язку. На кожному рівні повинен діяти механізм для встановлення зв'язку між двома процесами, які повинні взаємодіяти між собою. Якщо на однаковому рівні існує багато процесів, то для організації взаємодії між двома визначеними процесами необхідна адресація. Із механізмом встановлення зв'язку тісно пов'язаний механізм припинення зв'язку, якщо він більше непотрібний. Це може виявитися достатньо складною процедурою.

Необхідно відзначити, що будь-який рівень може діяти у двох різних режимах.

У режимі комунікації із встановленням з'єднання (Connection-oriented Communication, CO) система працює як віртуальне коло і комунікація здійснюється подібно до звичайного телефонного виклику: набирання номера, очікування на встановлення з'єднання, обмін повідомленнями, завершення з'єднання, очікування на підтвердження, що з'єднання припинене. Режим комунікації із встановленням з'єднання гарантує, що жоден пакет не буде втрачений і всі пакети поступлять у тому ж порядку, в якому вони були відправлені.

На противагу цьому, *режим комунікації без встановлення з'єднання (Connectionless Communication, CL)* забезпечує тільки послуги передавання данограм (datagram) подібно до поштової системи передавання листів. У цьому режимі відсутні гарантії, що пакети будуть доставлені у тій же послідовності, у якій вони були надіслані. Будь-яка проміжна система допускає відкидання пакету, якщо вона має недостатньо ресурсів для його подальшого передавання (наприклад, внаслідок переповнення буферної пам'яті). У системах з режимом комунікації без встановлення з'єднання вищі рівні займаються відновленням потрібної послідовності пакетів, повторним передаванням втрачених пакетів і т.п., якщо потрібний надійний потік даних.

Фрагментація та дефрагментація повідомлень. Не всі процесори можуть приймати повідомлення довільної довжини. Тому необхідні механізми поділу довгих повідомлень на фрагменти, пересилання цих фрагментів за призначенням і відновлення повідомлень із фрагментів. Споріднена проблема виникає у зворотній ситуації, коли процесори генерують настільки короткі повідомлення, що пересилання кожного з них окремо стає неекономним. Розв'язання полягає у поєднанні декількох малих повідомлень до однієї і тієї ж станції-призначення в одне велике повідомлення, пересилання його і розділення на початкові менші повідомлення в станції-призначенні.

Впорядкованість частин повідомлення. Не всі комунікаційні канали зберігають початкову послідовність при пересиланні частин повідомлень. Тому протокол повинен містити засоби, для відновлення їх правильної послідовності після отримання. Звичайно частини повідомлень нумерують, але повинен існувати механізм дій з частинами, отриманими у невірній послідовності, а також дій щодо втрачених частин.

Мультиплексування і демультиплексування. Використання окремих каналів для кожної пари процесів, які комунікують між собою, може бути необгрунтоване або занадто дороге, тоді нижчий рівень може використати той же канал для комунікації багатьох незалежних процесів, тобто мультиплексування. Якщо процеси мультиплексування і демультиплексування прозорі, то такі процеси можна застосовувати на кожному рівні. Мультиплексування обов'язково застосовується на Фізичному рівні, оскільки всі дані повинні бути відправлені через одну або декілька фізичних ліній.

Маршрутизація (routing). Якщо для передавання даних між респондентами існує декілька можливих шляхів, то необхідно здійснити вибір конкретного шляху. Часом вирішення цього завдання здійснюється багатоступенево.

Фізична адресація.

У міру поширення мереж розроблялися стандартні правила роботи мережевого устаткування різних виробників. Стандартизація принесла мережам багато користі:

- спрощення конструкції мереж;
- спрощення розробки продуктів;
- поява нових можливостей для конкуренції;
- з'явилася можливість пов'язувати різні пристрої;
- спрощення навчання;
- розширення вибору постачальників.

Офіційно прийнятого протоколу локальних мереж не існує, але з плином часу особливо поширилася технологія, під назвою Ethernet. Вона стала стандартом де-факто.

Для будь-якого обміну даними необхідний спосіб ідентифікації джерела і адресата. При спілкуванні між людьми використовуються імена.

У мережах Ethernet використовується схожий метод ідентифікації вузлів-джерел і вузлів призначення. Кожному, підключеному до мережі Ethernet, вузлу привласнюється фізична адреса, яка служить його ідентифікатором в мережі. В процесі виготовлення, всім мережевим інтерфейсам Ethernet присвоюються фізичні адреси. Ця адреса називається адресою управління доступом до середовища, або MAC-адресою (Media Access Control). MAC-адреса ідентифікує кожен вузол джерела і кожен вузол призначення в мережі.

Коли підключений до Ethernet вузол включається в обмін даними, він розсилає кадри зі своєю MAC-адресою, в якості джерела, і MAC-адресою передбачуваного отримувача. Всі приймаючі вузли декодують кадр і прочитують MAC-адресу призначення. Якщо ця MAC-адреса відповідає налаштованій MAC-адресі мережевої інтерфейсної плати, вона обробляє і зберігає повідомлення. Якщо MAC-адреса призначення не відповідає MAC-адресі вузла, мережевий адаптер ігнорує повідомлення.

Логічна адресація.

Як правило, ім'я людини не змінюється. Адреса ж залежить від місця проживання і може змінитися. MAC-адреса вузла не змінюється. Фізично привласнена мережевому адаптеру і відома як фізична адреса, вона залишається незмінною, незалежно від розташування вузла в мережі.

IP-адреса схожа на адресу місця проживання людини. Вона називається логічною адресою, оскільки присвоюється логічно, в залежності від місцезнаходження вузла. IP-адреса, або мережева адреса, привласнюється вузлу мережевим адміністратором на основі характеристик локальної мережі.

IP-адреси складаються з двох частин. Одна з них є ідентифікатором локальної мережі. Мережева частина IP-адреси загальна у всіх вузлів в одній локальній мережі. Друга частина IP-адреси є ідентифікатором конкретного вузла.

Протокол визначення адрес ARP.

Фізична MAC-адреса і логічна IP-адреса необхідні комп'ютеру для обміну даними в ієрархічній мережі точно так, як для відправки листа необхідне ім'я та адреса людини.

В локальній мережі Ethernet мережева інтерфейсна плата приймає кадр тільки в тому випадку, якщо він відправлений на MAC-адресу широкомовного розсилання або MAC-адресу мережевого адаптера.

При цьому більшість мережевих додатків знаходять сервери і клієнти тільки по логічній IP-адресі.

Що робити, якщо у відправника є тільки логічна IP-адреса вузла призначення? Як вузол-відправник визначає MAC-адресу призначення, яку потрібно помістити в кадр?

За допомогою IP-протоколу, який називається протоколом визначення адрес (ARP), можна визначити MAC-адресу будь-якого вузла з тієї ж локальної мережі.

При наявності IP-адреси вузла ARP можна визначити і зберегти MAC-адресу в локальній мережі в три етапи.

1. Вузол-відправник створює і відправляє кадр за MAC-адресою широкомовного розсилання. У кадрі знаходиться повідомлення з IP-адресою вузла призначення.

2. Кожен мережевий вузол отримує цей кадр і порівнює IP-адресу з повідомлення зі своєю. Вузол з відповідною IP-адресою надсилає відправнику свою MAC-адресу.

3. Вузол-відправник отримує повідомлення і зберігає MAC-адресу і IP-адресу в таблиці ARP.

Коли MAC-адреса призначення виявляється в таблиці ARP відправника, з'являється можливість відправляти кадри прямо, оминаючи запит ARP.

ARP-таблиця для перетворення адрес

Перетворення адрес виконується шляхом пошуку по таблиці. Ця таблиця називається ARP-таблицею, зберігається у пам'яті і містить рядки для кожного вузла мережі. В двох стовпчиках містяться IP- та Ethernet-адреси. Якщо потрібно перетворити IP-адресу в Ethernet-адресу, то відбувається пошук запису з відповідною IP-адресою. Нижче наведений приклад спрощеної ARP-таблиці.

ARP-таблиця необхідна тому, що IP-адреси та Ethernet-адреси вибираються незалежно, і немає жодного алгоритму для перетворення однієї адреси в іншу. IP-адресу вибирає адміністратор мережі з урахуванням розташування машини у мережі Інтернет.

Якщо машину переміщують в іншу частину мережі Інтернет, то її IP-адреса повинна бути змінена. Ethernet-адресу вибирає виробник мережевого інтерфейсного обладнання з виділеного для нього, згідно з ліцензією, адресного простору. Якщо у пристрої змінюється мережевий адаптер, то змінюється і Ethernet-адреса.

Таблиця 5.1
ARP-таблиця

IP-адреса	Ethernet-адреса
223.1.2.1	08:00:39:00:2F:C3
223.1.2.2	08:00:5A:21:A7:22
223.1.2.3	08:00:10:99:AC:54

У ході звичайної роботи мережева програма відправляє прикладне повідомлення, користуючись транспортними послугами TCP. Модуль TCP надсилає відповідне транспортне повідомлення через модуль IP. В результаті, складається IP-пакет, який має бути переданий драйверу Ethernet. IP-адреса місця призначення відома прикладній програмі, модулю TCP та модулю IP. Необхідно на її основі знайти Ethernet-адресу місця призначення. Для пошуку відповідної Ethernet-адреси використовується ARP-таблиця.

Запити та відповіді протоколу ARP

ARP-таблиця заповнюється автоматично модулем ARP по мірі необхідності. Коли за допомогою існуючої ARP-таблиці не вдається перетворити IP-адресу, то відбувається таке:

1) По мережі передається широкомовний ARP-запит.
2) Вихідний IP-пакет ставиться в чергу.

Кожний мережевий адаптер приймає широкомовні передачі. Усі драйвери Ethernet перевіряють поле типу в прийнятому Ethernet-кадрі й передають ARP-пакети модулю ARP. ARP-запит можна інтерпретувати так: «Якщо Ваша IP-адреса збігається із зазначеною, то повідомте мені Вашу Ethernet-адресу». Пакет ARP-запиту має вигляд:

Таблиця 5.2
Приклад ARP-запиту

IP-адреса відправника	223.1.2.1
Ethernet-адреса відправника	08:00:5A:21:A7:22
Шукана IP-адреса	223.1.2.3
Шукана Ethernet-адреса	<порожньо>

Кожний модуль ARP перевіряє поле потрібної IP-адреси в отриманому ARP-пакеті і, якщо адреса збігається з його власною IP-адресою, то надсилає відповідь прямо за Ethernet-адресою відправника запиту. Пакет з ARP-відповіддю виглядає приблизно так:

Таблиця 5.3
Приклад ARP-відповіді

IP-адреса відправника	223.1.2.3
Ethernet-адреса відправника	08:01:2A:2B:A7:21

IP-адреса автора запиту	223.1.2.1
Ethernet-адреса автора запиту	08:00:5A:21:A7:22

Цю відповідь отримує вузол, що зробив ARP-запит. Драйвер цього вузла перевіряє поле типу в Ethernet-кадрі й передає ARP-пакет модулю ARP. Модуль ARP аналізує ARP-пакет і додає запис у свою ARP-таблицю. Якщо в мережі немає вузла із потрібною IP-адресою, то ARP-відповіді не буде й не буде запису в ARP-таблиці. Протокол IP буде знищувати IP-пакети, що направляються за цією адресою. Протоколи верхнього рівня не можуть відрізнити випадок пошкодження мережі Ethernet від випадку відсутності вузла із потрібною IP-адресою.

Призначення протоколу RARP

Кожна система в мережі має унікальну апаратну адресу (MAC-адресу), яка призначається виробником мережевого інтерфейсу (мережевої плати). Принцип роботи RARP полягає в тому, що система може зчитати свою унікальну апаратну адресу з інтерфейсної плати і надіслати RARP запит (широкомовний кадр в мережу) з проханням відгукнутися кого-небудь і повідомити IP-адресу (за допомогою RARP відгуку).

Протокол RARP забезпечує визначення IP адреси по MAC-адресі (наприклад, при завантаженні пристрою, який не має можливості зберігати свою власну IP адресу), тобто виконує функції зворотні протоколу ARP. Унікальна MAC-адреса забезпечується виробником пристрою.

Клієнт RARP надсилає широкомовний кадр Ethernet із запитом, що містить MAC-адресу цільового вузла. У відповідь від сервера очікується RARP пакет (unicast), що містить відповідну йому IP-адресу. Відповідь може бути отримана безпосередньо від RARP сервера або від посередника (proxy). В якості посередника зазвичай виступає маршрутизатор. У сегменті мережі може бути кілька RARP серверів, так що можна очікувати кількох відповідей.

RARP використовується більшістю бездискових систем при завантаженні, для отримання своїх IP-адрес. Формат пакету RARP практично ідентичний пакету ARP. Запит RARP широкомовний, в ньому міститься апаратна адреса відправника, при цьому він запитує кого-небудь надіслати йому його IP адресу. Відгук зазвичай персональний.

Протокол динамічного конфігурування мережевих пристроїв (DHCP)

IP-адреси можна привласнювати статично або динамічно. Використовуючи статичну адресу, мережевий адміністратор може вручну налаштовувати мережеві дані вузла. Як мінімум, це буде IP-адреса, маска підмережі і основний шлюз.

Список користувачів локальної мережі часто змінюється. З'являються нові користувачі з ноутбуками, які потрібно підключити. Інші встановлюють нові робочі станції. Щоб кожній станції не доводилося вручну привласнювати IP-адресу, найпростіше це зробити автоматично. Для цього використовується протокол динамічного конфігурування мережевих пристроїв DHCP (Dynamic Host Configuration Protocol).

DHCP передбачає механізм автоматичного присвоєння інформації про адресу, наприклад, IP-адреси, маски підмережі, основного шлюзу та інших налаштувань. Це найбільш бажаний спосіб привласнення IP-адрес вузлам у великій мережі, оскільки він полегшує роботу фахівців служби підтримки та практично усуває можливість помилки.

Інша перевага DHCP полягає в тому, що адреси присвоюються вузлам тимчасово. Якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання. Це особливо корисно для мобільних користувачів, які то підключаються, то відключаються.

DHCP є розширенням протоколу BOOTP, що використовувався раніше для забезпечення бездискових робочих станцій IP-адресами при їхньому завантаженні. DHCP зберігає зворотну сумісність з BOOTP.

Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в RFC 2132. Деякими з опцій, що найчастіше використовуються, є:

- IP-адреса маршрутизатора за замовчуванням;
- маска підмережі;

- адреси серверів DNS;
- ім'я домену DNS.

Деякі постачальники програмного забезпечення можуть визначати власні додаткові опції DHCP.

Протокол DHCP працює у відповідності клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яке містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах, включаючи:

Динамічний розподіл – адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запитати IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". При закінченні терміну оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її іншим комп'ютерам.

Автоматичне виділення – сервер DHCP буде постійно призначати вільну IP-адресу з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих завдань IP і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережевих підключень.

Статичний розподіл – сервер DHCP робить призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначена мережева адреса.

Як працює DHCP

Протокол DHCP побудований так, що клієнт може звертатися із запитом відразу до декількох серверів.

Клієнт DHCP, що потребує адресу, надсилає широкомовний пакет DHCPDISCOVER в пошуках сервера. Пакет містить апаратну адресу запитувача клієнта. Потім один або кілька серверів DHCP розглядають запит і надсилають у відповідь пакет DHCPOFFER, що містить пропоновану IP-адресу і "час оренди".

Клієнт вибирає адресу з отриманих пакетів DHCPOFFER. Вибір клієнта залежить від його призначення - наприклад, він може вибрати адресу з найбільшим часом оренди. Слідом за тим клієнт надсилає пакет DHCPREQUEST з адресою вибраного сервера.

Обраний сервер надсилає підтвердження (DHCPACK), і процес узгодження завершується. Пакет DHCPACK містить обумовлені адресу та час оренди. Сервер позначає виділену адресу як зайняту - до закінчення терміну оренди ця адреса не може бути присвоєна іншому клієнту. Клієнту залишилося тільки сконфігурувати себе відповідно до призначення адреси і можна приступати до роботи в мережі.

Отже, на запит DHCPDISCOVER може відповісти кілька серверів. Клієнт повинен вибрати одну з пропозицій і надіслати у відповідь пакет DHCPREQUEST з ідентифікатором вибраного сервера. Інші сервери переглядають пакет DHCPREQUEST і укладають на основі ідентифікатора сервера, що їх пропозиція була відкинута. Таким чином, вони знають, що запропоновані ними IP-адреси вільні для призначення іншим клієнтам.

У разі якщо сервер не може прийняти конфігурацію, він надсилає пакет DHCPNAK (відмова в підтвердженні), що змушує клієнта почати процес узгодження заново.

Виходячи з цього, якщо в мережі два DHCP-сервера з різними конфігураціями, немає ніякої гарантії, що клієнт вибере саме Ваш сервер.

Служба доменних імен DNS

Щодня для отримання доступу до послуг, доступних по мережі Інтернет, ми звертаємося до тисячі серверів, розташованих в різних географічних точках. Кожному з цих серверів присвоюється унікальна IP-адреса, за якою він ідентифікується в мережі.

Було б неможливо запам'ятати всі IP-адреси всіх серверів, що надають різні послуги в мережі Інтернет. Замість цього пропонується більш простий спосіб пошуку серверів – співставити ім'я з деякою IP-адресою.

Служба доменних імен (DNS) дозволяє використовувати ім'я вузла для запиту IP-адреси окремого сервера. Реєстрація та організація імен у цій системі виконується за

спеціальними високорівневими групами, що називаються доменами. До числа найбільш популярних високорівневих доменів мережі Інтернет відносяться .com, .edu і.net.

В DNS-сервері записана спеціальна таблиця, в котрій асоціюються імена вузлів домену з відповідним IP-адресами. Якщо клієнт знає ім'я сервера, наприклад, веб-сервера, але потрібно знайти IP-адресу, він направляє запит на цей DNS-сервер через порт 53.

При отриманні запиту DNS-сервер з'ясовує по своїй таблиці, чи є відповідність між запитуваною IP-адресою і веб-сервером. Якщо на DNS-сервері відсутній запис по запитуваному імені, він опитує інший DNS-сервер в межах свого домену. Після розпізнавання IP-адреси DNS-сервер відправляє результат назад до клієнта. Якщо DNS-серверу не вдалося визначити IP-адресу, клієнт не зможе встановити зв'язок з цим веб-сервером і отримає повідомлення про закінчення часу очікування.

Процес визначення IP-адреси по DNS-протоколу з клієнтського програмного забезпечення досить простий і прозорий для користувача.

DNS має ієрархічну структуру. Розподілена база даних прив'язок імен вузлів до IP-адрес поширюється по безлічі DNS-серверів у всьому світі. У цьому полягає відмінність від файлу HOSTS, всі прив'язки в якому редагувалися централізовано на одному сервері.

Ієрархічна структура DNS будується по іменах доменів і поділяється на невеликі керовані зони. У кожного DNS-сервера є окремий файл з базою даних. Сервер управляє прив'язкою імен до IP-адрес тільки в невеликій частині загальної структури DNS. Отримавши запит на перетворення імені, що не входить до власної зоні DNS, DNS-сервер передає цей запит на обробку іншому DNS-серверу у відповідній зоні.

Ієрархія DNS

Система DNS складається з трьох компонентів: записи ресурсів, простір доменних імен та DNS-сервери.

Запис ресурсу – це запис у файлі бази даних зони DNS. Вона ідентифікує тип вузла, IP-адресу вузла і параметри бази даних DNS.

Простір доменних імен – ієрархічна структура іменування, що використовується при організації записів ресурсів. Простір доменних імен складається з різних доменів (груп) та записів ресурсів у кожній групі.

DNS-сервери – ці сервери відповідають за ведення баз даних, в яких зберігаються записи ресурсів та відомості про структуру простору доменних імен. DNS-сервери починають обробку запитів клієнтів з пошуку в просторі доменних імен і записах ресурсів, що зберігаються в файлах бази даних зони. Якщо DNS-сервер не знаходить необхідної інформації в базі даних зони DNS, сервер звертається до додаткових DNS-серверів для обробки запиту перетворення імені на IP-адресу.

Перетворювачі

Перетворювач (resolver) – це додаток або функція операційної системи, що виконується на DNS-клієнтах і DNS-серверах. Якщо в запиті використовується доменне ім'я, перетворювач звертається до DNS-серверу і перетворює це ім'я в IP-адресу. Перетворювач реалізується на стороні DNS-клієнта і служить для створення запиту імені DNS, надсилається на DNS-сервер. Перетворювачі також розміщуються на DNS-серверах. Якщо DNS-сервер не має даних, він, за допомогою перетворювача, передає запит до інших DNS-серверів.

В системі DNS використовується ієрархічна структура перетворення імен. Ця ієрархія виглядає як перевернуте дерево з коренем вгорі і гілками, що ростуть вниз.

На чолі ієрархії знаходяться кореневі сервери, які містять записи, що дозволяють звернутися до серверів доменів верхнього рівня, які в свою чергу містять записи, які вказують на сервери доменів другого рівня.

Різні домени верхнього рівня представляють або певний вид організації, або країну походження. Приклади доменів верхнього рівня:

- .au – Австралія;
- .co – Колумбія;
- .com – комерційні або промислові підприємства;
- .ua – Україна;
- .org – некомерційні організації.

Під доменами верхнього рівня знаходяться домени другого рівня, а під ними розташовані домени нижчих рівнів.

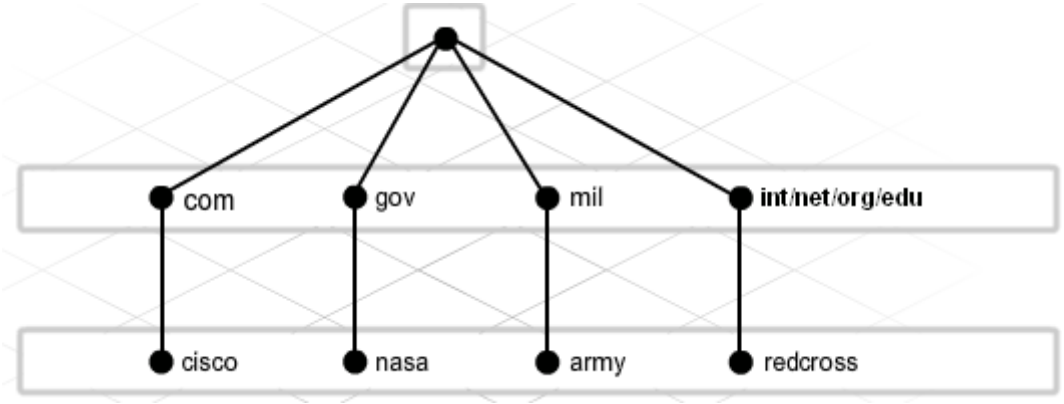


Рис.5.1 Ієрархія DNS доменів.

Перетворення імен в DNS

Якщо вузлу потрібно перетворити ім'я DNS, він за допомогою перетворювача звертається до DNS-серверу у власному домені. Перетворювачу відомо IP-адресу DNS-сервера, до якого потрібно звернутися - ця адреса була попередньо налаштована в складі конфігурації IP вузла.

Отримавши запит від клієнтського перетворювача, DNS-сервер спочатку перевіряє локальні записи DNS, що зберігаються в його кеші. Якщо серверу не вдається перетворити ім'я в IP-адресу локально, сервер за допомогою власного перетворювача пересилає запит іншому DNS-серверу, адреса якого була попередньо налаштована. Цей процес продовжується до тих пір, поки не буде отримана IP-адреса. Результат перетворення імені повертається до вихідного DNS-сервера, який використовує його для відповіді на відправлений запит.

У процесі перетворення імені DNS кожен DNS-сервер кешує, або запам'ятовує відповіді на запити, які він отримує. Кешування інформації дозволяє DNS-серверу швидше відповідати на наступні запити перетворювача, перевіряючи наявність записів в кеші перед відправкою запитів на інші DNS-сервери.

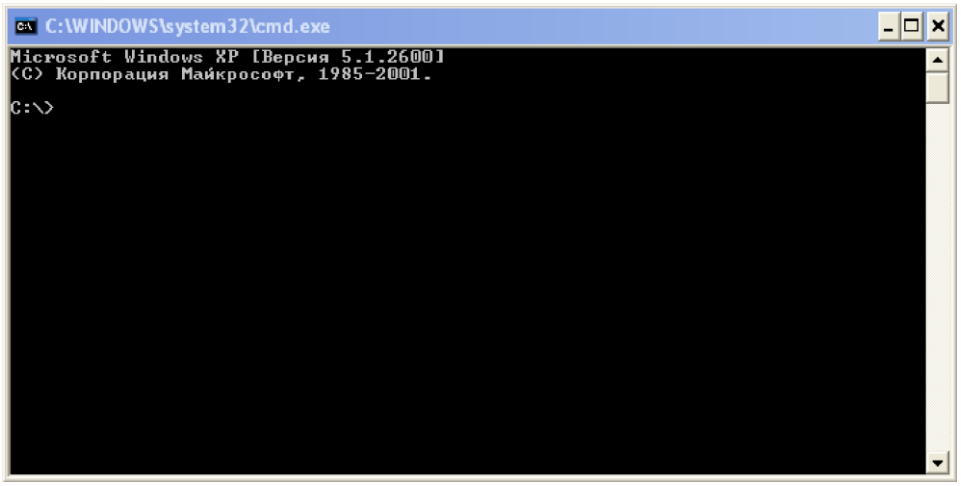
DNS-сервер кешує інформацію протягом обмеженого часу. Термін знаходження записів в кеші DNS-сервера повинен бути обмежений, оскільки записи імен вузлів можуть час від часу змінюватися. Наявність застарілої інформації в кеші DNS-сервера може привести до того, що клієнтам будуть повідомлятися невірні IP-адреси комп'ютерів.

Варто пам’ятати, що інформація про NS-сервери доменів оновлюється не миттєво, а з затримкою (інколи, в декілька годин). Протягом цього часу кореневі DNS-сервери видають застарілі відомості про домен. Тому, якщо після реєстрації або перенесення домену (зміни NS-серверів), сайт відразу не став працювати, потрібно зачекайти деякий час, щоб обновились дані.

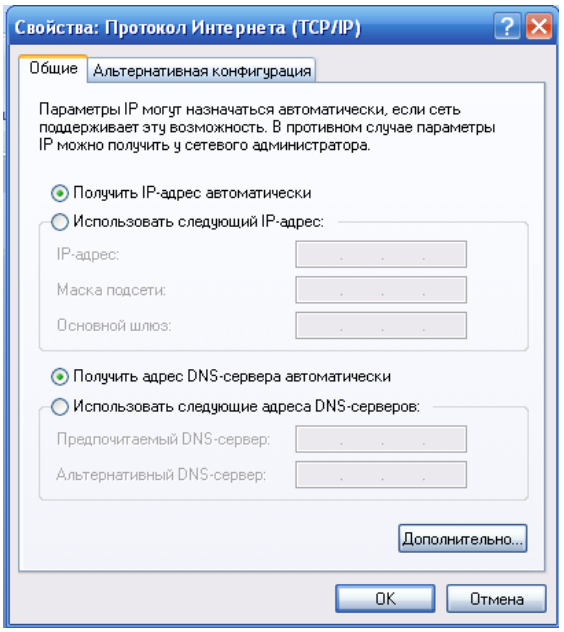
Порядок виконання роботи

1. Ознайомтеся із теоретичними відомостями до роботи.
2. Визначте MAC-адресу Вашого ПК. Для цього виконайте такі пункти:

a) На робочому столі виберіть кнопку **Пуск** -> **Выполнить.**
b) У вікні, що з'явилось введіть команду **cmd** і натистність ОК.
c) Відкриється вікно командної стрічки Windows



d) В командній стрічці введіть команду **ipconfig /all**. Запишіть у звіт результати виконання даної команди.
3. В командній стрічці введіть команду **arp –a.** Запишіть у звіт результати виконання даної команди.
4. Налаштуйте динамічне присвоєння IP-адреси на Вашому ПК. Для цього виберіть кнопку **Пуск->Подключение->Отобразить все подключения**. Клікніть по кнопці **Подключение по локальной сети** правою кнопкою маніпулятора і виберіть пункт **Свойства.**
5. У вікні, що зявилось виберіть **Свойства Протокол TCP/IP.** Відкриється вікно налаштувань



6. Виберіть “Получить IP-адрес автоматически”.
7. Перевірте адресу Вашого комп’ютера. Для цього виконайте пункт 2.
8. В командній стрічці введіть команду **ipconfig /release.** Перевірте адресу Вашого комп’ютера.
9. В командній стрічці введіть команду **ipconfig /renew.** Перевірте адресу Вашого комп’ютера.
10. У вікні командної стрічки Windows виконайте команду **ping ww.cisco.com**.
11. Запишіть IP –адресу, що відображається у звіт.
12. В командній стрічці введіть команду **nslookup.** Який DNS-сервер використовується за замовчуванням?
13. В командній стрічці введіть команду **?**, шоб побачити перелік всіх доступних команд в режимі **NSLOOKUP**.
14. В командній стрічці введіть команду **set type=mx,** щоб мати змогу визначити поштові сервери.

15. В командній стрічці введіть команду **www.cisco.com.** Які у даного сервера основне ім'я, поштова адреса та час життя (TTL) за замовчуванням?
16. У командному рядку ведіть команду **exit**, щоб повернутися до звичайного командного рядка.
17. Тут же введіть команду **ipconfig /all.** Запишіть IP-адреси всіх DNS-серверів, що використовуються в локальній мережі.
18. У командному рядку ведіть команду **exit**, щоб вийти із командного рядка та завершити виконання роботи.
19. Оформіть звіт про виконання даної роботи.

Контрольні питання

1) Що таке мережевий протокол та яке його призначення?
2) Що таке фізична адреса? Скільки MAC-адрес може бути в комп’ютера та чому?
3) Як ще називають MAC-адресу?
4) Яке основне призначення протоколів ARP та RARP?
5) В чому відмінність механізмів статичного та динамічного присвоєння IP-адрес?
6) Який порт використовує протокол DHCP?
7) Які Вам відомі ієрархії DNS доменів?

Для чого використовується команда **nslookup**?