Відображення доменних імен на IP-адреси. Система доменних імен DNS

AGENDA

- **Історія створення та основні поняття DNS**
- **Компоненти DNS**
- **Простір доменних імен**
- **Сервери імен (DNS-сервери)**
- **Основні схеми розв'язку DNS-імен**
- **Утиліта nslookup**
- **Кеш DNS**

Історія створення та основні поняття DNS

- Для ідентифікації вузлів в мережах TCP/IP апаратне і програмне забезпечення використовує IP-адреси. Користувачам незручно користуватись числовими IP-адресами, тому для них були введені так звані доменні імена, які є не числовими, а символьними.
- Так як для апаратури необхідні саме IP-адреси, постає питання розв'язку доменних імен, тобто як за доменним іменем знайти IP-адресу комп'ютера.
- На раньому етапі розвитку Інтернету на кожному вузлі вручну створювався текстовий файл hosts, в кожному рядку якого записувалась відповідність IP-адреси і доменного імені, наприклад:
- **102.54.94.97 rhino.acme.com # source server**

Історія створення та основні поняття DNS

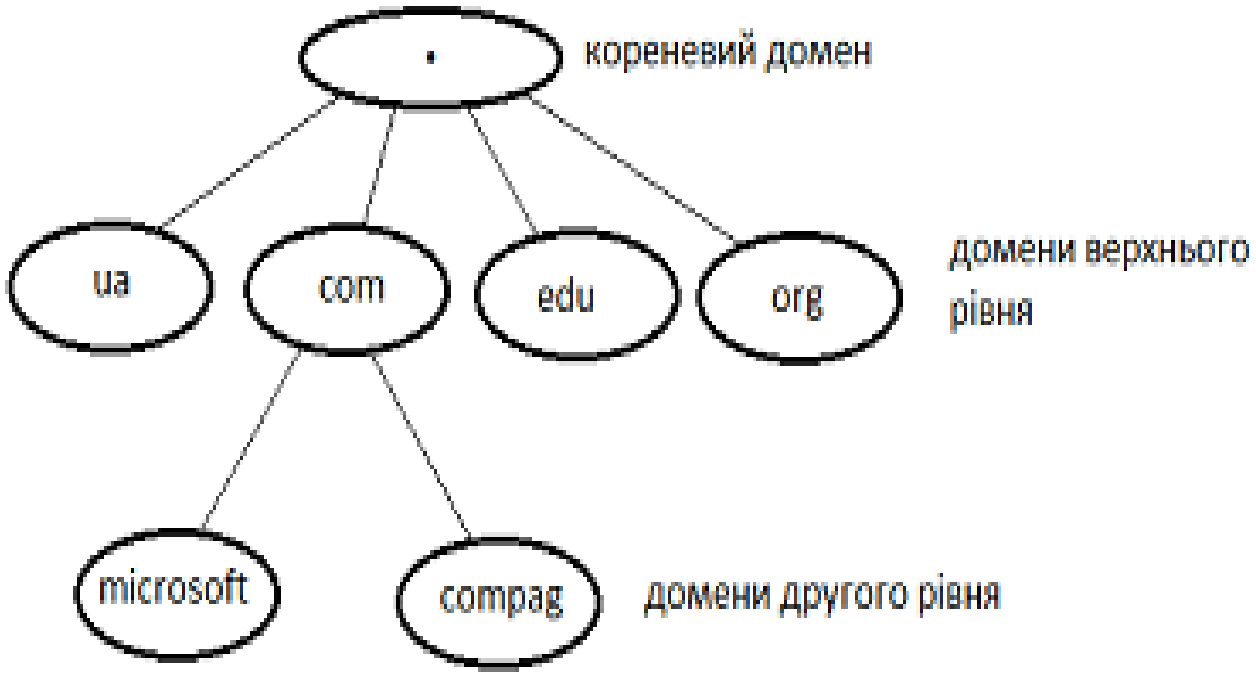
- Наприклад, у системі Windows 10 файл hosts розміщений у каталозі "\Windows\System32\drivers\etc"
- Аналогічно розміщувались і відповідності ідентифікаторів мереж і імен мереж у файлі networks.
- В ході розвитку Інтернету файли hosts зростали і виникла необхідність іншого вирішення завдання розв'язку імен. Так було створено спеціальну службу - систему доменних імен DNS (Domain Name System -1983 р.). DNS це розподілена база даних відображень "доменне ім'я - IP-адреса", яка має архітектуру "клієнт-сервер".

Компоненти DNS

- DNS використовує три основних компоненти –
- • розпізнавачі (resolver, DNS-клієнти),
- • сервери імен (name server, DNS-сервери) і
- • простір доменних імен.
- DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитами про розв'язок доменного імені в IP-адресу, тобто про визначення IP-адреси вузла по його доменному імені. Простір доменних імен - це ієрархічне групування імен, яке має деревоподібну структуру.

Простір доменних імен

- Дерево імен починається із кореневого домену, який позначається крапкою. Потім ідуть домени першого рівня, другого рівня і т. д.



Простір доменних імен

- Запис доменного імені починається із наймолодшої складової, а закінчується найстаршою, наприклад, partnering.microsoft.com
- Сукупність імен, у яких декілька старших складових частин співпадають, складають домен імен. Наприклад, gorod.dp.ua і google.com.ua входять в домен ua.
- Розподіл імені на частини дозволяє розділити адміністративну відповідальність за призначення унікальних імен в межах свого рівня ієрархії. Наприклад, на першому рівні ієрархії одна організація відповідає за призначення імен в домені com, інша - в домені ua і т.д. Це дозволяє вирішити проблему утворення унікальних імен без взаємних консультацій між організаціями, які відповідають за імена одного рівня ієрархії.

Домени верхнього рівня — TLD-рівня (Top-Level Domains)

Первинні домени верхнього рівня		Нові домени верхнього рівня	
Назва	Опис	Назва	Опис
gov	Урядові заклади	firm	Ділові ресурси мережі
mil	Військові заклади	store	Торгівля
com	Комерційні організації	web	Організації, що регулюють діяльність у WWW
edu	Навчальні заклади	arts	Гуманітарна освіта
net	Мережні організації	rec	Ігри та розваги
org	Інші (некомерційні) організації	info	Інформаційні послуги
int	Міжнародні організації	nom	Індивідуальні ресурси

Домени верхнього рівня — домени країн (міжнародний стандарт)

Назва	Опис	Назва	Опис	Назва	Опис
au	Код Австралії	ch	Код Китаю	ua	Код України
uk	Код Великобританії	de	Код Німеччини	fr	Код Франції
it	Код Італії	ru	Код Росії	cz	Код Чехії
ca	Код Канади	us	Код США	jp	Код Японії

Примітка. Загальне число кодів країн — 300; комп'ютерні мережі існують приблизно в 170 з них

Простір доменних імен

Простір доменних імен

- За аналогією з файловою системою, в доменній системі імен розрізняють короткі імена, відносні імена і повні імена. Коротке ім'я це ім'я кінцевого вузла мережі. Відносне ім'я - це ім'я, яке починається з деякого рівня ієрархії, але не з верхнього. І повне доменне ім'я (Fully qualified domain name, FQDN) включає в себе всі рівні ієрархії, закінчуючи кореневою крапкою: milkyway.hmarka.net.
- Імена доменів нечутливі до зміни регістру символів. Так, наприклад, edu, Edu і EDU означають одне і те ж. Довжина імен компонентів може досягати 63 символів, а довжина повного шляху не повинна перевищувати 255 символів.

Простір доменних імен

- В інтернеті кореневий домен керується міжнародною некомерційною організацією ICANN (Internet Corporation for Assigned Names and Numbers).
- Зарезервувати домен другого рівня, такий як імя_компанії.com, просто. Домени вищого рівня управляються реєстраторами (registrars), призначеними ICANN. Для того щоб отримати ім'я, потрібно просто звернутися до відповідного реєстратора (в даному випадку com) і перевірити, чи доступне бажане ім'я і чи не є воно чиєїсь торговою маркою. Якщо все в порядку, замовник реєструється і за невелику щорічну абонентську плату отримує домен другого рівня

Простір доменних імен

- Структура доменів відображає не фізичну будова мережі, а логічний поділ між організаціями та їх внутрішніми підрозділами.
- Так, якщо факультети обчислювальної техніки і електротехніки розташовуються в одній будівлі і користуються однією спільною локальною мережею, вони тим не менше можуть мати різні домени. І навпаки, якщо, скажімо, факультет обчислювальної техніки розташовується в двох різних корпусах університету з різними локальними мережами, логічно все хости обох будівель зазвичай належать до одного і того ж домену.

Сервери імен (DNS-сервери)

- На DNS-серверах зберігається база даних DNS-імен, причому дані про домени верхнього рівня містяться у кількох кореневих DNS-серверах, які позначаються латинськими літерами від A до M. Вони керуються різними організаціями, які діють за погодженням з ICANN.
- Інформація на DNS-сервері зберігається у текстових файлах із записами, які називаються записами ресурсів. Запис ресурсу має такий формат:
- **Domain_name Time_to_live Class Type Value**

Сервери імен (DNS-сервери)

- Поле Domain_name (ім'я домену) позначає домен, до якого належить поточний запис. Зазвичай для кожного домена існує кілька записів ресурсів.
- Поле імені домену є первинним ключем пошуку, використовуваним для виконання запитів. Порядок записів в базі даних значення не має. У відповідь на запит про домен повертаються всі записи необхідного класу, які задовольняють запиту
- Поле Time_to_live (час життя) вказує, наскільки довго розпізнавачу зберігати в кеші запит про розв’язок доменного імені. Рідко мінливим даним присвоюється високе значення цього поля, наприклад, 86 400 (число секунд в добі). Непостійна інформація позначається невеликим значенням, наприклад, 60 (1 хвилина).

Сервери імен (DNS-сервери)

- Третім полем кожного запису є поле Class (клас). Для інформації Інтернету значення цього поля завжди дорівнює IN. Для іншої інформації застосовуються інші коди, однак на практиці вони зустрічаються рідко.
- Поле Type (тип) означає тип DNS-запису
- Нарешті, останнє поле запису ресурса- це поле Value (значення) - може бути числом, ім'ям домену або текстовим ASCII-рядком. Сенс поля залежить від типу запису.

Сервери імен (DNS-сервери)

- Найпоширеніший тип запису (тип ресурсного запису) - тип A, в якому зберігається відповідність "доменне ім'я - IP-адреса" для свого домену і піддоменів. Приклад запису типу A:
- **www.microsoft.com. 59 IN A 65.55.57.27**
- Він містить повністю кваліфіковане доменне ім’я (FQDN), час життя (TTL) (це кількість часу, до якого дозволено кешувати запис розпізнавачем) та IP-адресу.

• Сервери імен (DNS-сервери)

- Крім типу A на DNS-сервері зберігаються записи таких типів:
- SOA (Start of Authority) - перший запис у файлі бази даних, визначає основні параметри зони DNS.
- NS - перечисляє додаткові DNS-сервери.
- PTR - запис який використовується для оберненого запиту, тобто визначення доменного імені вузла по його IP-адресі. Приклад: 51.200.55.157.in-addr.arpa. IN PTR mserver.microsoft.com.

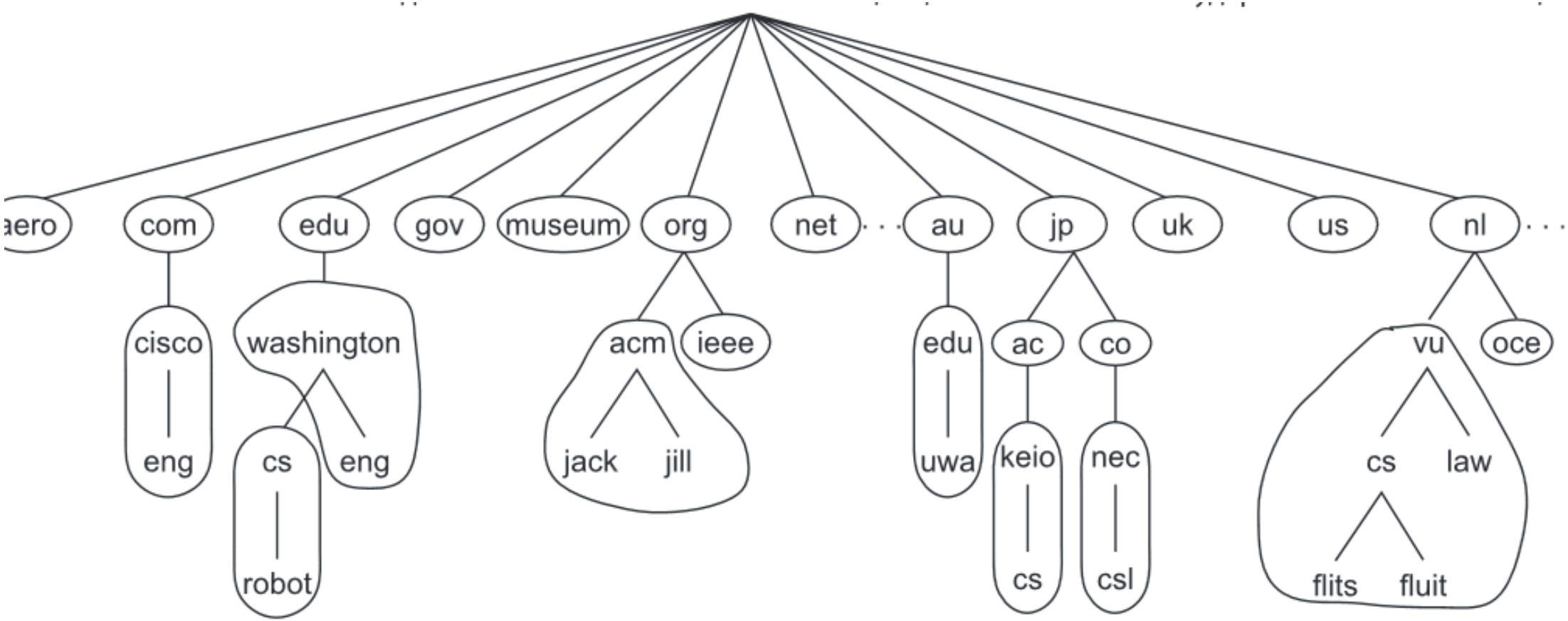
Сервери імен (DNS-сервери)

- CNAME (Canonical NAME) - дозволяє хосту присвоювати псевдонім (alias). Наприклад:
- bar.example.com. CNAME foo.example.com.
- bar.example.com. - канонічне (справжнє) ім'я, foo.example.com. - псевдонім.
- MX (mail exchanger) - вказує на сервер для прийому електронної пошти, яка приходить на адреси вказаного домену і пріоритет поштового серверу. Формат запису:
- owner-name ttl class rr pref name
- example.com. 193 IN MX 10 mail.example.com.
- де, owner-name - ім'я локального домену, ttl - час, протягом якого запис можна тримати у кеші, class - тип мережі, де діє служба, за замовчуванням приймають IN (Internet), rr (resource record) - тип ресурсного запису, pref - пріоритет (від 0 до 65535), менші значення мають вищий пріоритет.

Сервери імен (DNS-сервери)

- Теоретично один сервер міг би містити всю базу даних DNS і відповідати на всі запити до неї. На практиці цей сервер виявився б занадто перевантаженим. Більш того, якби з ним коли-небудь що-небудь трапилося, то весь Інтернет не працював би.Чтоби уникнути проблем, пов'язаних зі зберіганням всієї інформації в одному місці, простір імен DNS розділене на непересічні зони (zones). Один можливий спосіб поділу простору імен на зони зображений на рис . Кожна окреслена зона містить частину загального дерева доменів

Сервери імен (DNS-сервери)



Сервери імен (DNS-сервери)

- Кожна зона також асоціюється з одним або більше сервером імен. Це хости, на яких знаходиться база даних для зони. Зазвичай у зони є один основний сервер імен, який отримує інформацію з файлу на своєму диску, і один або більше другорядних серверів імен, які отримують інформацію з основного сервера імен.

Основні схеми розв'язку DNS-імен

- Існують дві основні схеми розв'язку DNS-імен - ітеративна і рекурсивна. В разі ітеративної схеми роботу з пошуку IP-адреси координує сам DNS-клієнт:
- - DNS-клієнт звертається до кореневого DNS-сервера із інформацією про повне доменне ім'я;
- - DNS-сервер відповідає, вказуючи на адресу наступного DNS-сервера, який обслуговує домен верхнього рівня;
- - DNS-клієнт робить запит до наступного DNS-сервера, який відсилає його до DNS-сервера потрібного під-домену і т. д., поки не буде знайдено DNS-сервер, який зберігає відповідність доменне ім'я - IP-адреса.

Основні схеми розв'язку DNS-імен

- В разі рекурсивної схеми роботу з пошуку IP-адреси координує DNS-сервер. Рекурсивна схема:
- - DNS-клієнт робить запит до локального DNS-сервера, тобто сервера, який обслуговує під-домен, до якого належить DNS-ім'я клієнта;
- - якщо локальний DNS-сервер знає відповідь, то повертає ii DNS-клієнту;
- - в іншому випадку, локальний DNS-сервер виконує ітеративні запити до кореневого DNS-сервера і отримавши відповідь, повертає її клієнту.
- Найчастіше використовується рекурсивна схема, тому що DNS-клієнт, як правило, звертається із запитом, що має прапор "потрібна рекурсія" і більшість DNS-серверів її підтримують.

Утиліта nslookup

- Для перевірки роботи серверів DNS часто використовується утиліта **nslookup**
- Утиліта **nslookup** може працювати у двох режимах - інтерактивному і автономному.
- При запуску **nslookup** відображає ім'я і адресу сервера DNS, до якого підключена утиліта, і переходить до інтерактивного режиму. У цьому режимі список доступних команд видається за командою ?, а вихід - командою exit.
- Щоб отримати IP-адресу вузла треба набрати його ім'я натиснути Enter.

Утиліта nslookup

- Щоб переключитися з основного сервера DNS на інший, треба виконати команду :
- **server ім'я**
- **,** де ім'я - це ім'я або IP-адреса сервера DNS, наприклад:
- **server 8.8.8.8**
- Для роботи у автономному режимі треба в командному рядку ввести команду :
- **nslookup [-параметр] комп'ютер [-сервер]**
- , якщо сервер не вказаний, буде використано поточний сервер, наприклад, знайти IP-адресу хосту:
- **nslookup ukr.net**
- Знайти DNS ім'я за IP-адресою:
- **nslookup 8.8.8.8**

Утиліта nslookup

- знайти IP-адресу хосту, використовуючи конкретний DNS сервер:
- **nslookup ukr.net ns1.cloudns.net**
- Параметр складається із дефіса, команди, яка іде за ним без пробілів і можливо знака **= значення**.
- **Приклади параметрів:**
- -type=тип_запису - перегляд запису певного типу для домену
- Де тип_запису може бути: soa, ns, mx, any
- Наприклад, знайти записи типу ns для домену:
- **nslookup -type=ns cloudns.net**
- Запросити запис типу soa для домену:
- **nslookup -type=soa cloudns.net**

Утиліта nslookup

- -**timeout=число** , встановлення часу очікування відповіді в секундах:
- **nslookup –timeout=20 ukr.net**
- **-retry=число** , встановлення повторних спроб запиту до сервера DNS:
- **nslookup -retry=20 ukr.net**

Кеш DNS

- Кеш DNS (іноді його називають кешем DNS-розпізнавача) - це тимчасова база даних, що підтримується операційною системою комп'ютера, що містить записи всіх останніх відвідувань та спроб відвідування веб-сайтів та інших доменів Інтернету.
- Кеш DNS намагається пришвидшити процес, обробляючи вирішення імен нещодавно відвіданих адрес, перш ніж запит буде відправлений в Інтернет.
- Перш ніж браузер відправить свої запити зовнішній мережі, комп'ютер перехоплює кожен із них і шукає доменне ім'я в базі даних кешу DNS.

Кеш DNS

- Вміст локального кешу DNS можна переглянути в Windows за допомогою команди ipconfig /displaydns [показати]
- Кеш DNS може бути пошкодженим внаслідок технічних збоїв або отруєним (poisoned), коли в нього вставляються несанкціоновані доменні імена або IP-адреси.
- Отруєння кешу DNS зазвичай асоціюється з комп'ютерними вірусами або іншими мережевими атаками, які вставляють невірні записи DNS в кеш (або в файл hosts).
- Якщо зловмисник перенаправить ваш запит на gmail.com, наприклад, на веб-сайт, схожий на Gmail, ви можете в кінцевому підсумку постраждати від фішингової атаки.

Кеш DNS

- Під час усунення проблем із отруєнням кешу або іншими проблемами з підключенням до Інтернету адміністратор комп’ютера може захотіти очистити (тобто скинути чи стерти) кеш DNS.
- У Microsoft Windows ви можете очистити локальний кеш DNS, використовуючи команду ipconfig /flushdns у командному рядку [показати].
- Маршрутизатор може також мати кеш DNS, тому крім очищення кешу DNS на комп’ютері бажано перезавантажити маршрутизатор.