Служба доменних імен

Порядок денний

- Що таке DNS?
- Які послуги надає?
- Як це працює?
- Формат повідомлення
- Типи повідомлень

Що таке DNS?

- DNS — це служба перекладу імені хоста в IP-адресу
- DNS це
  - розподілена база даних, реалізована в ієрархії серверів імен
  - протокол прикладного рівня для обміну повідомленнями між клієнтами та серверами

Чому DNS?

- Легше запам'ятати ім'я хоста, ніж IP-адресу.
- Ім’я має для користувача більше значення, ніж 4-байтове число.
- Такі програми, як FTP, HTTP, електронна пошта тощо, вимагають від користувача введення адресата.
- Зазвичай користувач вводить ім'я хоста.
- Програма приймає ім’я хоста, надане користувачем, і пересилає його в DNS для перекладу на IP-адресу.

DNS Сервіси

Окрім служби перекладу адрес, DNS також надає такі послуги:

- Псевдонім хоста: хост зі складним іменем може мати один або кілька псевдонімів, які легше запам’ятати, наприклад, relay1.west-coast.media.com -> media.com. Чим довше ім’я є канонічним ім’ям хоста, тим коротшим є псевдонім хоста.

DNS Сервіси(продовження)

- Псевдоніми поштового сервера: як і вище, псевдоніми можуть існувати для довгих канонічних імен хостів.
- Балансування навантаження: набір серверів може мати одне ім’я, відображене на кількох машинах. DNS надає повний список імен додатку кінцевого користувача, який зазвичай займає перше в списку. DNS чергує імена в списку.

Як це працює?

- DNS працює шляхом обміну повідомленнями між клієнтською та серверною машинами.
- Клієнтська програма передасть ім’я цільового хоста процесу DNS (в Unix називається процедурою gethostbyname()), щоб отримати IP-адресу.
- Потім програма сидить і чекає на відповідь.

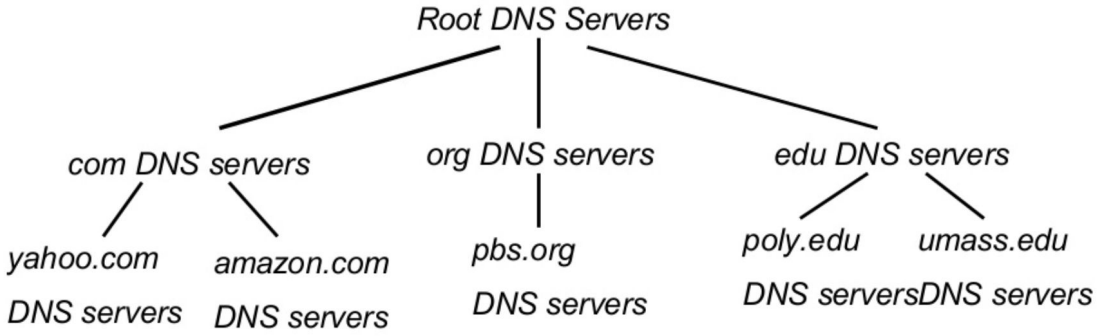
DNS

Чому б не централізувати DNS?

- єдина точка відмови
- обсяг трафіку
- віддалена централізована база даних
- обслуговування

не масштабується!

Розподілена ієрархічна база даних



Клієнт хоче IP для www.amazon.com; 1-е приблизно:

- клієнт запитує кореневий сервер, щоб знайти com DNS-сервер
- клієнт запитує DNS-сервер com, щоб отримати DNS-сервер amazon.com
- клієнт запитує DNS-сервер amazon.com, щоб отримати IP-адресу для www.amazon.com

DNS: Кореневі сервери імен

- зв’язується з локальним сервером імен, який не може розпізнати ім’я
- кореневий сервер імен:
  - зв’язується з авторитетним сервером імен, якщо відображення імен невідоме
  - отримує відображення
  - повертає відображення на локальний сервер імен

- 13 root name servers worldwide

TLD і авторитетні сервери

- Сервери доменів верхнього рівня (TLD).:
  - відповідальний за com, org, net, edu тощо та всі домени країн верхнього рівня uk, fr, ca, jp.
  - Network Solutions підтримує сервери для com TLD
  - Educause для edu TLD
- Авторитетні DNS-сервери:
  - DNS-сервери організації, надаючи офіційне зіставлення імені хоста з IP-адресою для серверів організації (наприклад, Інтернет, пошта).
  - може підтримуватися організацією або постачальником послуг

Локальний сервер імен

- не належить строго до ієрархії
- кожен Інтернет-провайдер (інтернет-провайдер, компанія, університет) має один.
  - також називається «сервер імен за замовчуванням»
- коли хост робить DNS-запит, запит надсилається на його локальний DNS-сервер
  - діє як проксі, пересилає запит в ієрархію

DNS Запити

Рекурсивний:

- Клієнтська машина надсилає запит на локальний сервер імен, який, якщо він не знаходить адресу у своїй базі даних, надсилає запит на кореневий сервер імен, який, у свою чергу, направляє запит на проміжний або авторитетний сервер імен. . Зауважте, що кореневий сервер імен може містити деяке зіставлення імені хоста з IP-адресою. Проміжний сервер імен завжди знає, хто є авторитетним сервером імен.

DNS Запити (продовження)

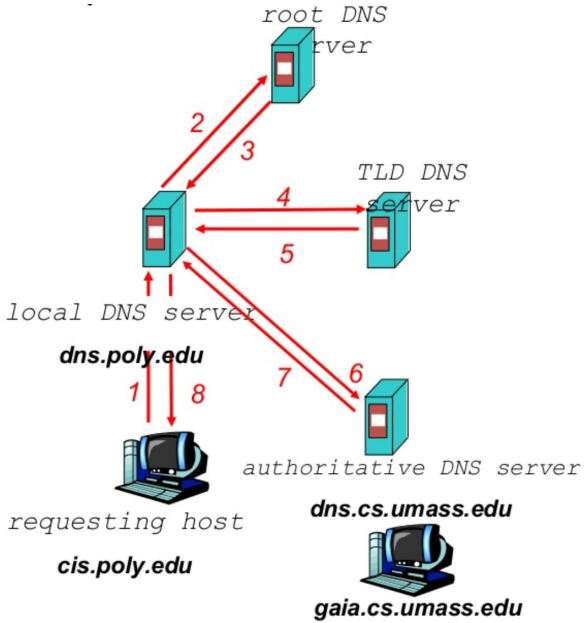
Ітеративний:

- Локальний сервер запитує кореневий сервер. Якщо адреси немає в базі даних, він матиме назву/адресу проміжного або авторитетного сервера імен і пересилатиме цю інформацію на локальний сервер імен, щоб він міг безпосередньо спілкуватися з проміжним або авторитетним сервером імен. Це робиться для запобігання перевантаженню кореневих серверів, які обробляють мільйони запитів. •24.10.15 •14

DNS приклад вирішення імені

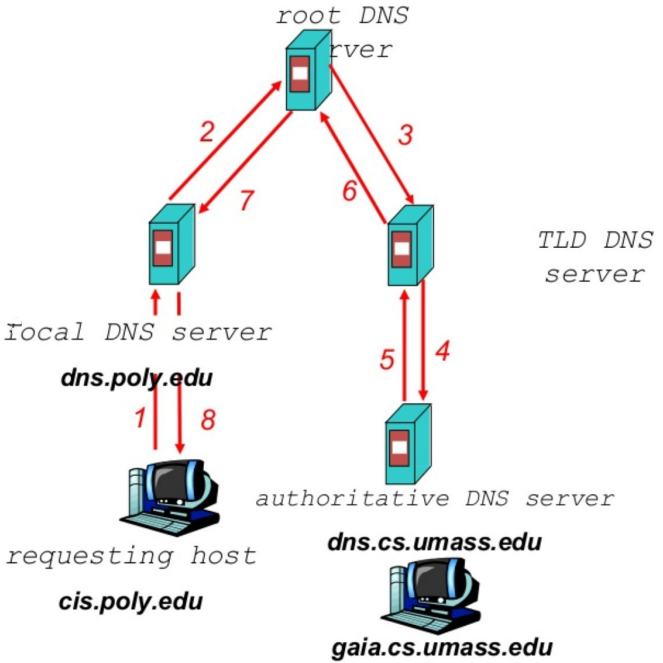
Хост на cis.poly.edu хоче IP-адресу для gaia.cs.umass.edu

- ітерований запит:
  - сервер, з яким зв’язалися, відповідає з іменем сервера, з яким потрібно зв’язатися
  - «Я не знаю цього імені, але запитайте на цьому сервері»



DNS приклад вирішення імені

- рекурсивний запит:
  - покладає тягар розпізнавання імен на сервер імен, з яким зв’язується
  - важкий вантаж?



DNS: кешування та оновлення записів

- як тільки (будь-який) сервер імен вивчає відображення, він кешує відображення
  - тайм-аут (зникнення) записів кешу через деякий час
  - Сервери TLD зазвичай кешуються на локальних серверах імен
    - Таким чином, кореневі сервери імен відвідуються не часто
- механізми оновлення/повідомлення, розроблені IETF
  - RFC 2136
  - http://www.ietf.org/html.charters/dnsind-charter.html

Робота DNS

- DNS використовує кешування, щоб збільшити швидкість перекладу.
- Дані DNS зберігаються в базі даних у формі ресурсних записів (RR). RR безпосередньо вставляють у повідомлення DNS.
- RR — це 4 кортежі, які складаються з: {ім’я, значення, тип, TTL}.

RRs

- TTL: час життя, використовується для вказівки, коли RR можна видалити з кешу DNS.
- Тип=
  - A - тоді NAME є ім'ям хоста та значенням його IP-адреси
  - NS – тоді NAME – доменне ім’я, а Value – IP-адреса авторитетного сервера імен
  - CNAME – тоді NAME є псевдонімом хоста, а Value – канонічним ім’ям хосту
  - MX – тоді NAME є псевдонімом хоста електронної пошти, а Value – канонічним ім’ям сервера електронної пошти

DNS записи

DNS: розподілена база даних, що зберігає записи ресурсів (RR)

RR format: (name, value, type, ttl)

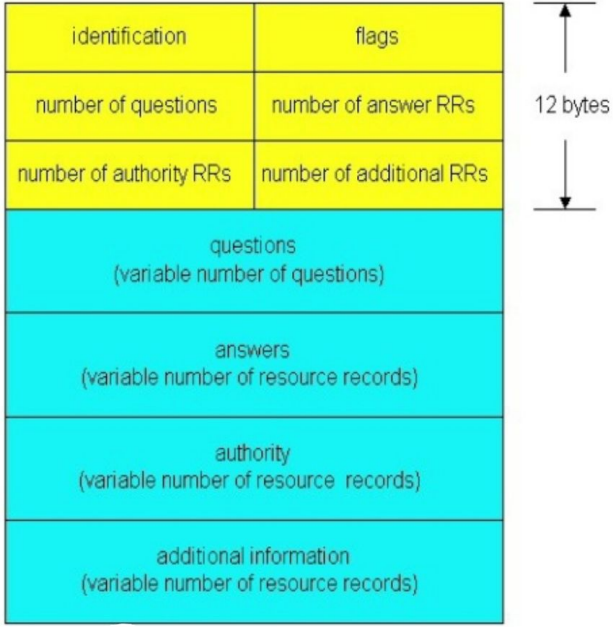
- *Type=A*
  - ***name*** *is hostname*
  - ***value*** *is IP address*
- *Type=NS*
  - ***name*** *is domain (eg., foo.com)*
  - ***value*** *is hostname of authoritative name server for this domain*
- *Type=CNAME*
  - ***name*** *is alias name for some "canonical" (the real) name, eg., www.ibm.com is really servereast.backup2.ibm.com*
  - ***value*** *is canonical name*
- *Type=MX*
  - ***value*** *is name of mailserver associated*

Протокол DNS, повідомлення

Протокол DNS: повідомлення запиту та відповіді, обидва з однаковим форматом повідомлення

заголовок повідомлення

- ідентифікація: 16 біт # для запиту, відповідь на запит використовує той самий #
- прапори:
  - запит або відповідь
  - бажана рекурсія
  - доступна рекурсія



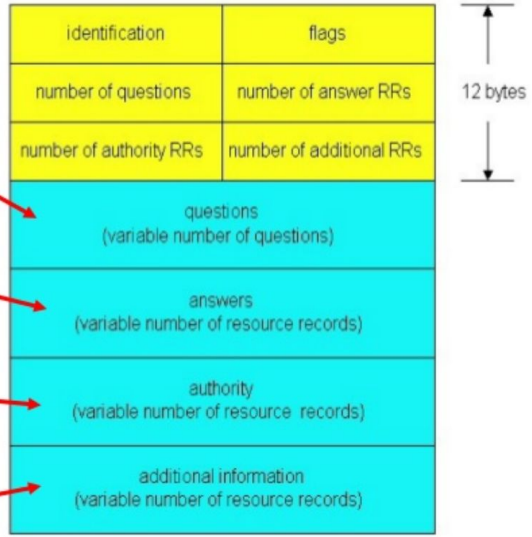
Протокол DNS, повідомлення

Name, type fields for a query

RRs in response to query

records for authoritative servers

additional "helpful" info that may be used



Поля повідомлень

- Ідентифікація – ідентифікує запит і копіюється у повідомлення відповіді, щоб зіставити його із запитом на стороні клієнта.
- Прапорці - однобітовий прапорець, який вказує, чи є повідомлення запитом чи відповіддю. Ще один біт, щоб визначити, чи відповідь надійшла від авторитетного відправника чи ні. Третій біт використовується, щоб вказати, що метод рекурсії бажаний.

Поля продовження

- Питання - містить ім'я, яке запитується, і тип, тобто тип A або MX.
- Відповіді - містить RR для запитуваних імен
- Authority - містить записи про авторитетні сервери
- Додаткова інформація – наприклад, якщо тип запиту – MX, то ця інформація може бути типом – A RR, що містить IP-адресу канонічного імені хоста

Вставлення записів в DNS

- приклад: новий стартап «Мережева утопія»
- зареєструйте назву networkuptopia.com у реєстратора DNS (наприклад, Network Solutions)
  - надати імена, IP-адреси офіційного сервера імен (основного та вторинного)
  - реєстратор вставляє два RR на сервер com TLD:

(networkutopia.com, dns1.networkutopia.com, NS) (dns1.networkutopia.com, 212.212.212.1, A)

- створити офіційний запис типу A на сервері для www.networkuptopia.com; Введіть запис MX для networkutopia.com

Підсумок

- DNS забезпечує механізм підтримки зручності Інтернету, приховуючи деякі робочі деталі.
- DNS-сервери потрібно створювати вручну. Нещодавно було представлено протокол оновлення, який дозволяє DNS обмінюватися даними для додавання та видалення.

Питання та відповіді