*Лекція № **6**.*
ТЕЗИ

DNS і BIND – Berkeley Internet Name Domain

Коротко про що йшлося в минулій лекції:
доменні імена введено щоб зробити роботу з мережевими сервісами простішою для людини.
В основі роботи механізму DNS лежить розприділена база даних про доменні імена.
Інформація про доменні імена поширюється тільки по мірі необхідності.
На запити про доменні імена відповідають DNS сервери.
Пошук інформації про доменне ім'я відбувається починаючи від кореневої зони.
Це - теоретично, а практично як правило використовується інформація з кешів DNS серверів різного рівня.
Відповіді DNS серверів можуть бути ***авторитетними*** або ***неавторитетними***.
Реєстрація доменного імені відбувається шляхом його ***делегування***.

З допомогою команди whois в процесі лаб. роботи ви вже бачили, яку інформацію про доменне ім'я зберігає реєстратор, коли делегує доменне ім'я.
Найважливіша, однак, інформація, яку зберігає (конфігурує) про ваше доменне ім'я реєстратор – це інформація (в описі вищої зони) про NS сервери, які будуть відповідати за вашу зону.

Технічна реалізація всіх цих деталей – як запитів, так і роботи самої бази даних DNS – якраз і здійснюється пакетом BIND.

Пакет BIND – найпоширеніша реалізація DNS для UNIX систем.
http://www.isc.org/
Актуальна на даний момент версія – 9.4.2

BIND поставляється з усіма UNIX системами по замовчуванню.

BIND – це пакет, побудований на основі моделі клієнт-сервер, тому
ділиться принципово на дві частини:
- ***пошуковий аналізтор*** – резолвер (***resolver***)
- ***сервер імен (named)***

resolver – це бібліотека підпрограм, яку використовує будь-яка інша програма, якій потрібна ретрансляція імен та адрес.
resolver – це клієнтська частина BIND.

DNS server – сервіс на сервері який відповідає на запити щодо доменних імен.
DNS server – серверна частина BIND, яка відповідє на запити клієнтської частини (не тільки, до речі BIND-резолвера, а і інших dns клієнтів).

База даних DNS зреалізована у вигляді звичайних текстових файлів – т.зв. ***файлів зон***. Цими файлами оперує DNS-сервер.
Зона – це сегмент простору доменних імен, який входить в компетенцію певного сервера дом. імен.
Термін “зона” також вживається як синонім до терміну “файл зони”.

Термін “домен” - дещо ширший. Під доменом розуміють частину ієрархії простору імен, що позначаються доменним іменем.

На BCIX вузлах працює resolver, але сервер dns – далеко не на всіх.

named – демон сервера dns. Працює на порті 53.
Використовує як tcp так і udp протоколи на транспортному рівні.

Сервер, по відношенню до його ролі (ролей) щодо забезпечення інформації про домен, може бути класифікований як:
- Основний (master)
- Підпорядкований (slave)
- Кешуючий (caching)

Master – компетентний (авторитетний) DNS щодо всієї інформації про зону. Файл зони створюється адміністратором вручну (чи з допомогою деякого програмного забезпечення).

Slave – це також авторитетний сервер для зони, ще називається ***вторинним.*** На відміну від основного файл зони не створюється на цьому сервері вручну, а ***реплікується*** з master- сервера з допомогою ***процедури передачі зони***.
Ззовні (для dns-клієнта) немає жодної різниці між цими двома серверами для конкретної зони: розрізнити, який сервер є основним, а який вторинним.

Кешуючий сервер також може відповідати на запити про зону, але його відповіді ніколи не є кометентними. Кешуючий зберігає актуальною інформацію на основі полів “refresh” та “serial”.

Настройка dns-кслієнта

dns-клієнт конфігурується по-суті одним файлом: ***/etc/resolv.conf***
Кожен процес, який потребує розв'язування доменних імен, вичитує цей файл і кешує його до завершення своєї роботи.

Директиви, допустимі в resolv.conf:

nameserver адреса	Адреси dns серверів, які опитуються клієнтом (в порядку слідування)
domain доменне ім'я	Ім'я по замовчуванню, яким доповнюється запит у випадку, якщо в запиті вказано неповністю класифіковане доменне ім'я (ме містить крапки).
search доменне ім'я доменне ім'я	Домени, в яких здійснювати пошук при запиті з не аовністю класифікованим іменем. Domain і search директиви разом як правило не використовують.
sortlist мережа[/маска] мережа[/маска]	Використовується разом з search, якщо повертається кілька результатів.
options параметр	Інші опції. Напр. debug, timeout:n (5 сек по замовчуванню), attempts:n (к-сть спроб, 2 по замовчуванню), rotate (для перебору серверів) etc

Якщо файлу resolv.conf немає, то клієнт повинен звертатися до локального dns-сервера, але деякі сторонні аплікації можуть мати в цьому випадку проблеми.

Настройка демона named

Для настройки named необхідними є наступні файли:

named.conf (named.boot в старших версіях)	Головний конфігураційний файл, з якого по замовчуванню стартує named, всі інші файли мають бути описані в цьому файлі.
named.root або named.ca, або інша назва	Файл кореневих вказівників – інформація про сервери для кореневих зон
master/localhost.rev – файл кільцевої зони	Використовується для локального розв'язування кільцевої IP адреси. (Розповісти про make-localhost !)
Файли прямого відображення зон	- не обов'язкові. Т.зв. Файли зон. Називають як правило ldi.lviv.ua.zone, ldi.lviv.ua.hosts, ldi.lviv.ua або ua.lviv.ldi
Файли зворотнього відображення зон	- не обов'язкові. т.зв. файли reverse-зон. Називають їх як правило 192.168.3.rev

Сучасний процес named по замовчуванню:
- стартує від користувача bind
- стартує в chroooted оточенні.
(після серйозних проблем з безпекою в версії 4)

Для управління named є утиліта ***rndc*** (версія named 9, а в 8 – ***ndc***).
З допомогою rndc можна отримати іформацію про статус сервера, перечитати конфігурацію, очистити кеш, отримати (retransfer) зону та ін.
rndc без параметрів виводить коротку інфо по команді.

named потрібно конфігурувати правильно з точки зору безпеки. Сервер повинен відповідати тільки на:
- запити про зони, для яких він є комперентним
- запити від ваших клієнтів (про будь-які зони)
- зона повинна віддаватися тільки тим серверам, яким ви довіряєте (trusted)

Коректність інформації, яку віддає сервер.
Тисячі серверів в мережі, що віддають інормацію навмисне чи ненавмисне некоректно.

Основні директиви, які викоритовуються в конф. файлі nmaed.conf:

options	directory “dir name”	Робоча директорія, відносно якої розташовано відносні файли.
	forwarders {IP address; ...}	IP сервери, які опитувати, якщо відповідь в локальному кеші відсутня
	forward only;	Використовувати тільки forwarders, не робити запитів до інших серверів самостійно.
	allow-query {}	Дозволити відповідати на запити адресам чи управляючим спискам.
	allow-transfer {}	Дозволити віддачу зон адресам чи спискам адрес.
	інші	
include	Включає інший файл як конфігураційний	
key	Ключі перевірки аутентичності	
logging	Настройка параметрів ведення логу	

acl	Визначає список управління доступом, наприклад
	acl trusted {
	127.0.0.1;
	194.44.44.197;
	};	

server	Визначає властивості вддаленого сервера	
zone	Визначає зону. Наприклад: ***zone "students.lviv.ua" { type master; allow-query { any; }; file "master/students.lviv.ua"; };*** або: ***zone "mr.lviv.ua" { type slave; allow-query { any; }; file "slave/mr.lviv.ua"; masters { 194.44.136.142; 62.64.65.114; }; };*** **ПОЯСНИТИ детально!**	

Файли зон

Створюються для зон, які описуємо в named.conf як master.
RFC 1033 описує синтаксис файлів зон.
Саме ці файли і складають базу даних dns.

Фацл зони містить т.зв. ***RR – записи (resource records)*** – записи ресурсів, в яких і міститься інфо про піддомени, саму зону, адреси, поштові сервери і т.п.

Приклад файлу зони:

```
;
$TTL   3600
@      IN SOA  ns.student.mr.lviv.ua.    hostmaster.mr.lviv.ua. (
            2008011100     ; serial
            3H             ; refresh
            1H             ; retry
            1W              ; expiry
            1D )           ; minimum

            IN     NS     zebra.mr.lviv.ua.
            IN     NS     big.litech.lviv.ua.

            IN     MX     30 mail

            IN     A      88.198.32.54
www         IN     CNAME  @
ftp         IN     CNAME  @
mail        IN     CNAME  @
```

Директиви з файлу зони:

$TTL	Задає час життя для ресурсів по замовчуванню
$ORIGIN	Встановлює зону по замовчувнню, якою доповнюються імена без крапки в кінці
$INCLUDE	Включає записи зовнішнього файлу
$GENERATE	Генерує діапазон записів за певними правилами (див. RFC)

RR – записи (resource records):

SOA	Start of Authority	Відмічає початок зони та містить дані про настройку зони: порядковий номер, час оновлення, час для повторення спроби, час, коли зона вважається застарілою, мінімальний час життя в кеші. SOA містить інфо про NS сервер, що поширює інформацію а також e-mail хостмастера.
NS	Name server	Сервери імен
A	Address	IP адрес
PTR	pointer	Вказівник. Забезпечує перетворення IP адреси в ім'я. Присутній в файлах реверс-зон.
MX	Mail excanger	Поштовий ретранслятор (сервер). Вказується з пріоритетом, бо може бути декілька. (Пояснити!)
CNAME	Canonical name	Канонічне ім'я. Використовується як певдонім. Пояснити!
TXT	Text	Довільна текстова інформація.

Спеціальний символ - @ - означає “ця зона”. Таким чином назва зони в явному вигляді не присутня в цьому файлі.