Образовательный комплекс

Компьютерные сети

Лекция 15

Domain Name System

Microsoft®

Содержание

- Domain Name System

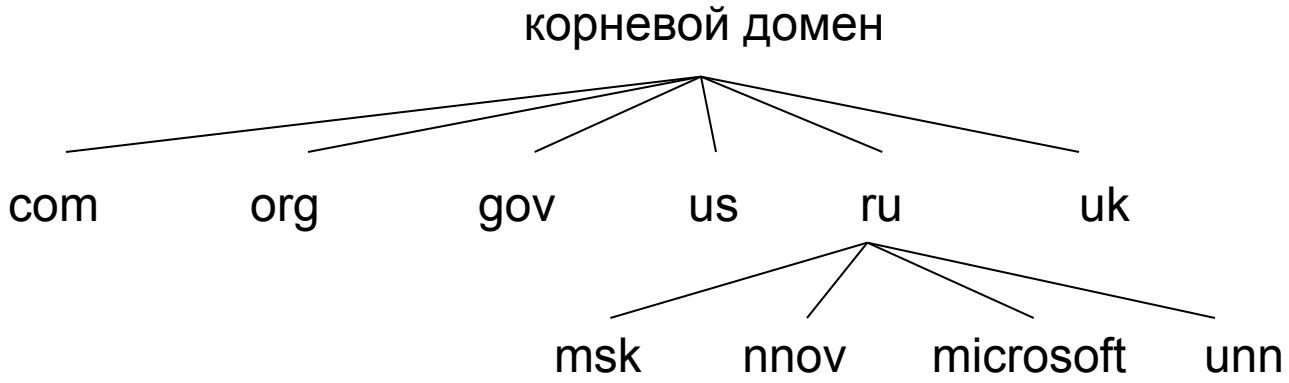
Domain Name System

- Система доменных имен (Domain Name System, DNS) позволяет использовать символьные имена узлов в IP-сетях
- DNS организован в виде распределенной базы данных и обеспечивает
  - Обновление базы данных
  - Распространение информации между серверами DNS
  - Обслуживание запросов на разрешение имен (определение IP-адреса по символьному имени и символьного имени по IP-адресу)

Domain Name System
Файл hosts

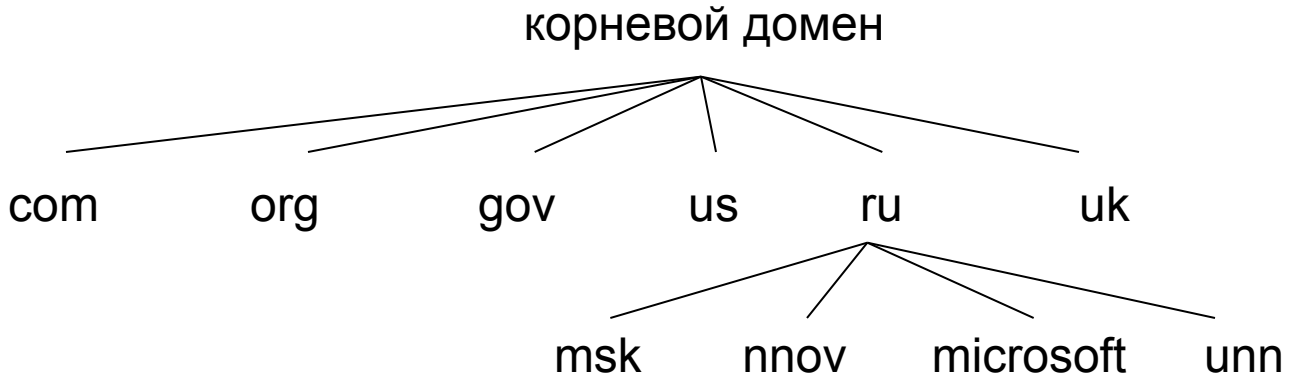
- До появления DNS соответствие между символьными именами и IP-адресами можно было установить в специальном файле. Этот способ можно использовать и сейчас.
  - Windows:
    WinDir\system32\drivers\etc\hosts
  - UNIX
    /etc/hosts
- Файл hosts содержит строки, Каждая из которых определяет одно соответствие между именем и IP-адресом
  - 127.0.0.1 localhost
  - 192.168.0.1 mygate

Domain Name System
Структура доменных имен…



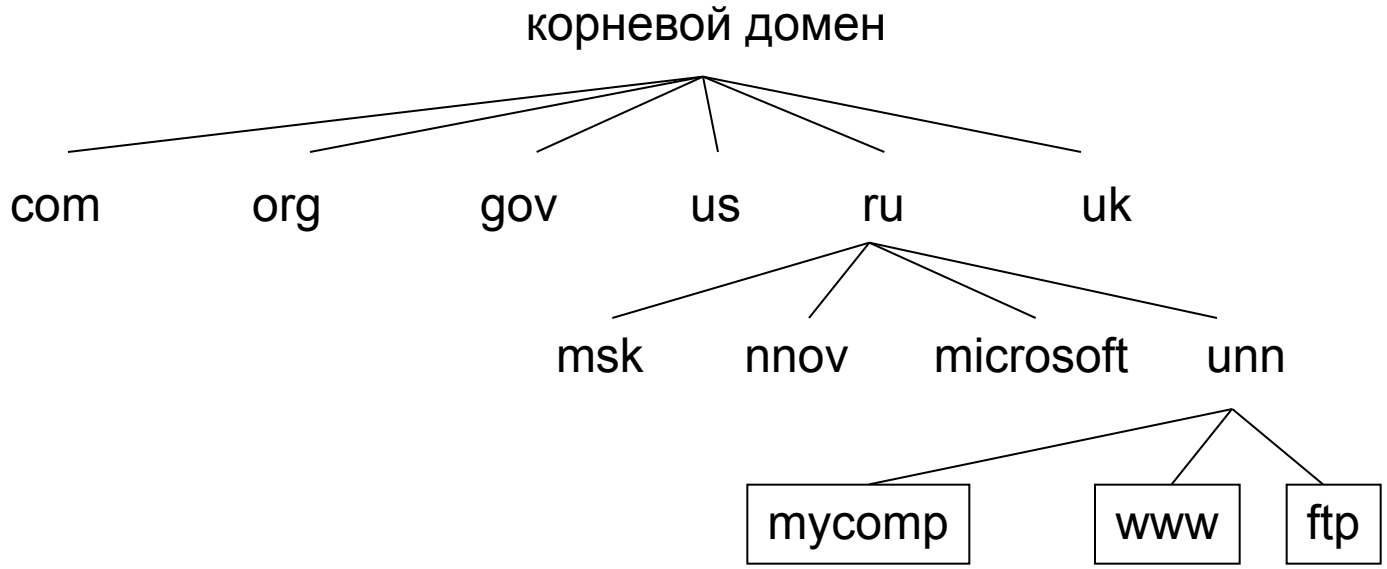
- Пространство доменных имен (Domain namespace) – иерархическая система именования
  - Верхний уровень называется корневым доменом (управляется IANA)
  - Ниже располагаются домены (поддеревья) первого уровня (также управляется IANA)
    - Домены организаций (com – коммерческие организации, org – некоммерческие организации, …)
    - Географические домены (us – United States, ru - Russia, …)
    - Домен обратного просмотра (in-addr.arpa.)

Domain Name System
Структура доменных имен…



- Именем домена является перечисление имен всех уровней на пути из домена к корню дерева
  - Fully Qualified Domain Name (FQDN) – полное имя домена, однозначно идентифицирующее положение домена в дереве (Именем корневого домена является пустая строка, завершающая точка означает, что далее идет имя корневого домена)
  - unn.ru – имя домена относительно другого домена
    - узел из домена nnov.ru проинтерпретирует данное имя как unn.ru.nnov.ru.
- Организация может создать локальное пространство имен, не имеющее ничего общего с пространством имен Интернета

Domain Name System
Структура доменных имен



- В любом домене кроме корневого могут быть определены имена узлов
- В доменных именах можно использовать символы a-z, A-Z, 0-9 и '-' (дефис); доменные имена нечувствительны к размеру букв
- Отдельные реализации позволяют использовать расширенное множество символов (например, реализация DNS в Windows)

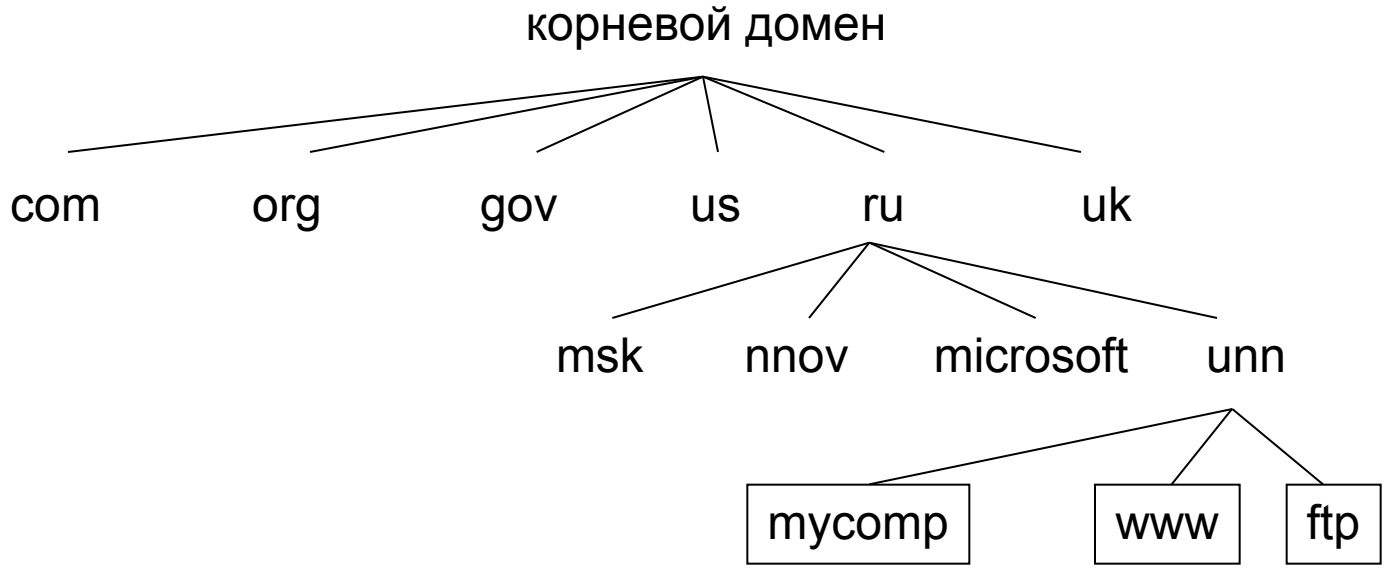
Domain Name System Термины…

- DNS-server (сервер DNS) – узел, содержащий информацию о структуре DNS-домена и обрабатывающий DNS-запросы клиентов
- DNS-resolver (ресолвер DNS) – программное обеспечение, обеспечивающее разрешение адресов посредством выполнения запросов к DNS-серверам
  - Обычно реализуется в виде библиотечных функций, но может выполняться в служебной программе
  - Может обращаться к локальному (выполняющемуся на том же узле, что и ресолвер) или удаленному серверу DNS

Domain Name System Термины

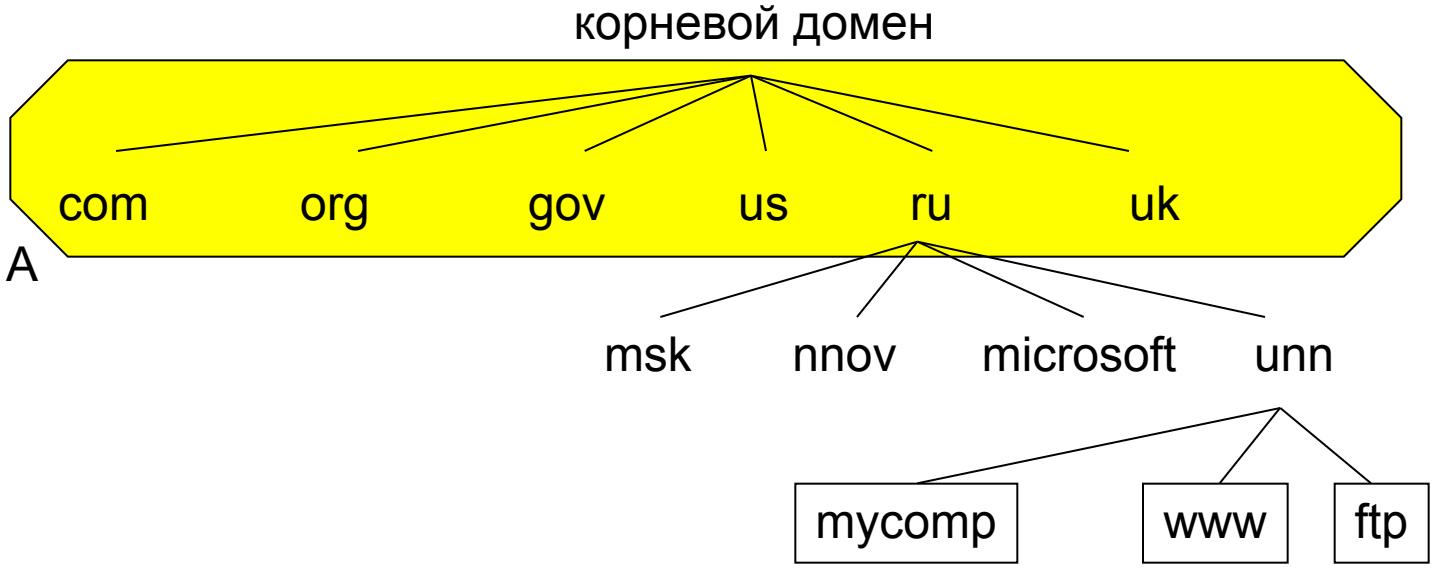
- Zone (зона) –непрерывное пространство имен (домен, возможно, за исключением некоторых или всех поддоменов)
- Resource records (записи ресурсов) – информация в базе DNS представлена в виде множества описаний зон. В каждой зоне посредством записей ресурсов определяется совокупность ресурсов, принадлежащих данной зоне
- Zone file (файл зоны) – файл, содержащий записи ресурсов для некоторой зоны

Domain Name System
Структура доменных имен…



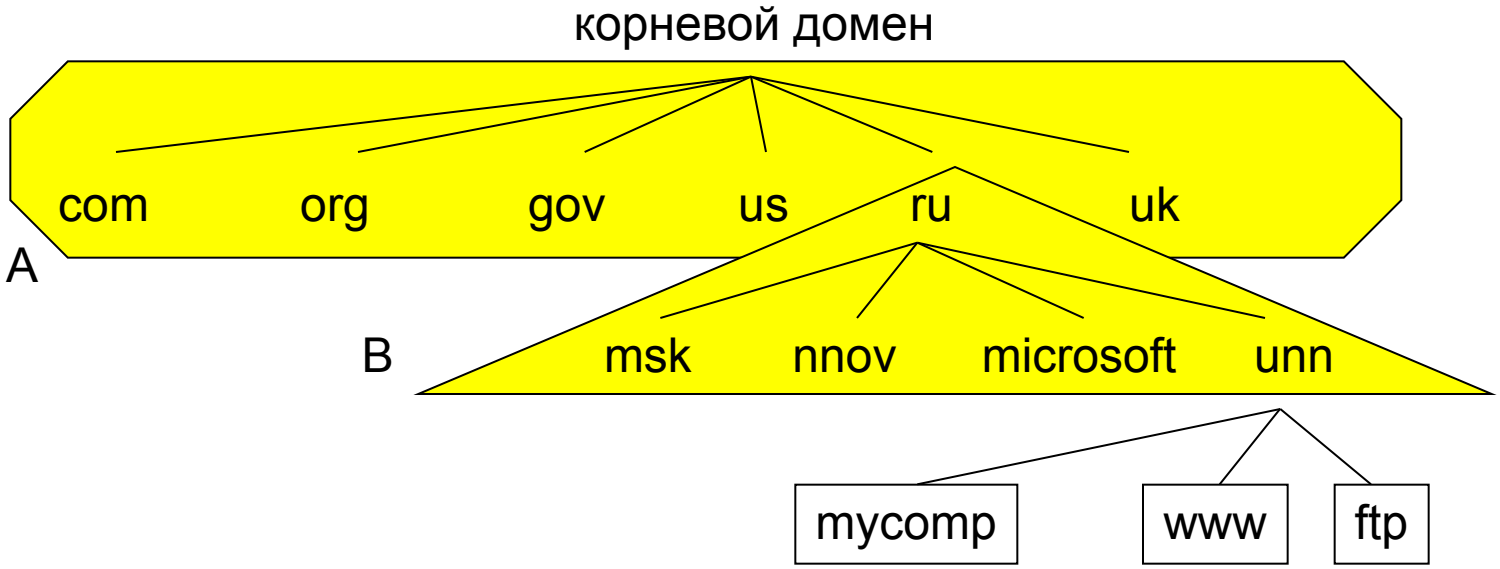
- Для каждого домена определен ответственный за него DNS-сервер
- На DNS-сервере может содержаться описание всего домена (поддерева), но часто управление поддоменами делегируется другим DNS-серверам
- Если DNS-сервер содержит описание некоторой зоны, он является **авторизованным** или **полномочным** сервером (authorized server) для данной зоны

Domain Name System
Структура доменных имен…



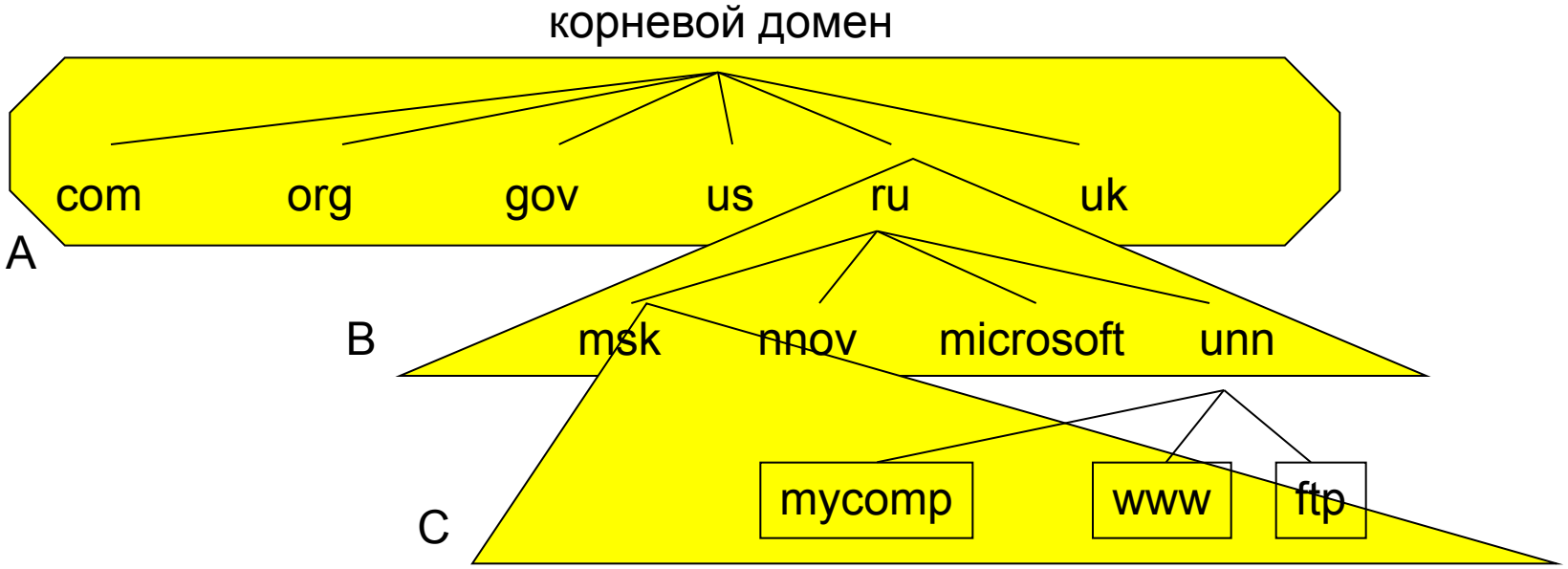
- A – зона, авторитетными серверами для которой являются DNS-сервера корневого домена
  - Корневые серверы обслуживают множество запросов, поэтому управление поддоменами делегируется другим DNS-серверам
  - Корневые серверы являются авторизованными для зоны, содержащей только корневой домен без его поддоменов
- В настоящий момент существует 13 корневых серверов (управляются IANA)

Domain Name System
Структура доменных имен…



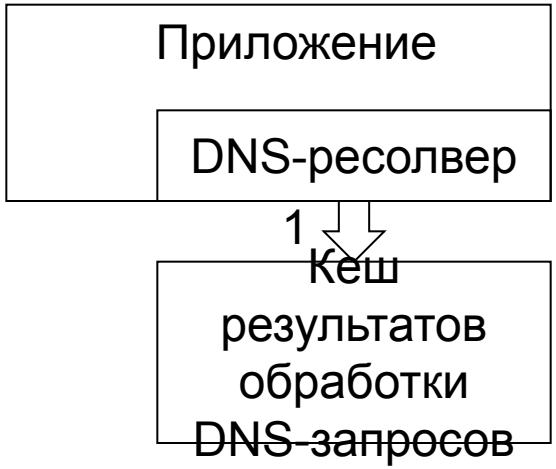
- B – существует DNS-сервер, которому делегировано управление зоной ru.
  - В зонах первого уровня определено большое количество поддоменов, поэтому DNS-сервера, ответственные за зоны первого уровня, в свою очередь, делегирует управление большинством своих поддоменов другим DNS-серверам
  - DNS-сервер, которому делегировано управление зоной ru., является авторитетным для зоны, включающей домен ru. и некоторые его поддомены

Domain Name System
Структура доменных имен



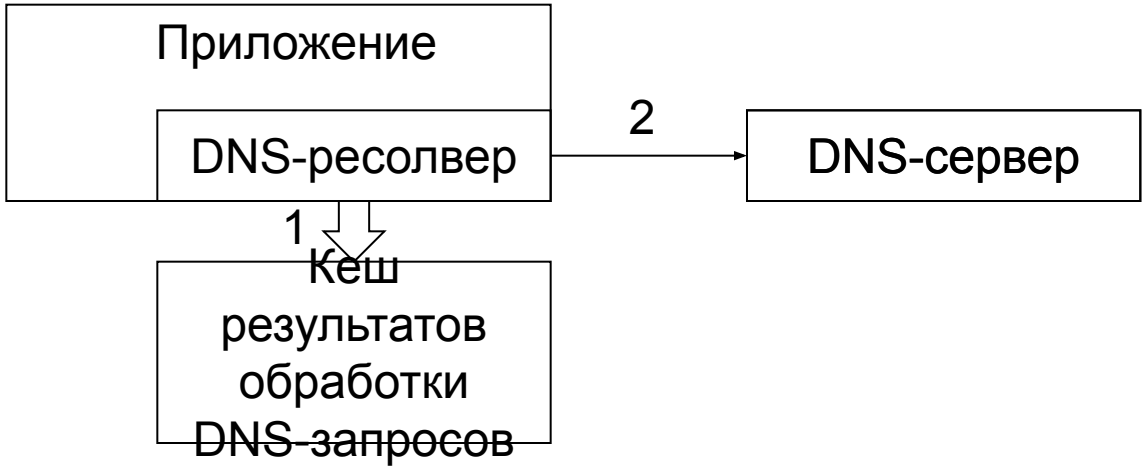
- C – поддомен второго уровня
  - DNS-сервер, которому делегировано управление доменом unn.ru., может содержать описание всего домена (то есть быть авторитетным для зоны, включающей весь домен unn.ru.) или делегировать управление поддоменами другим серверам

Domain Name System
Разрешение имен…



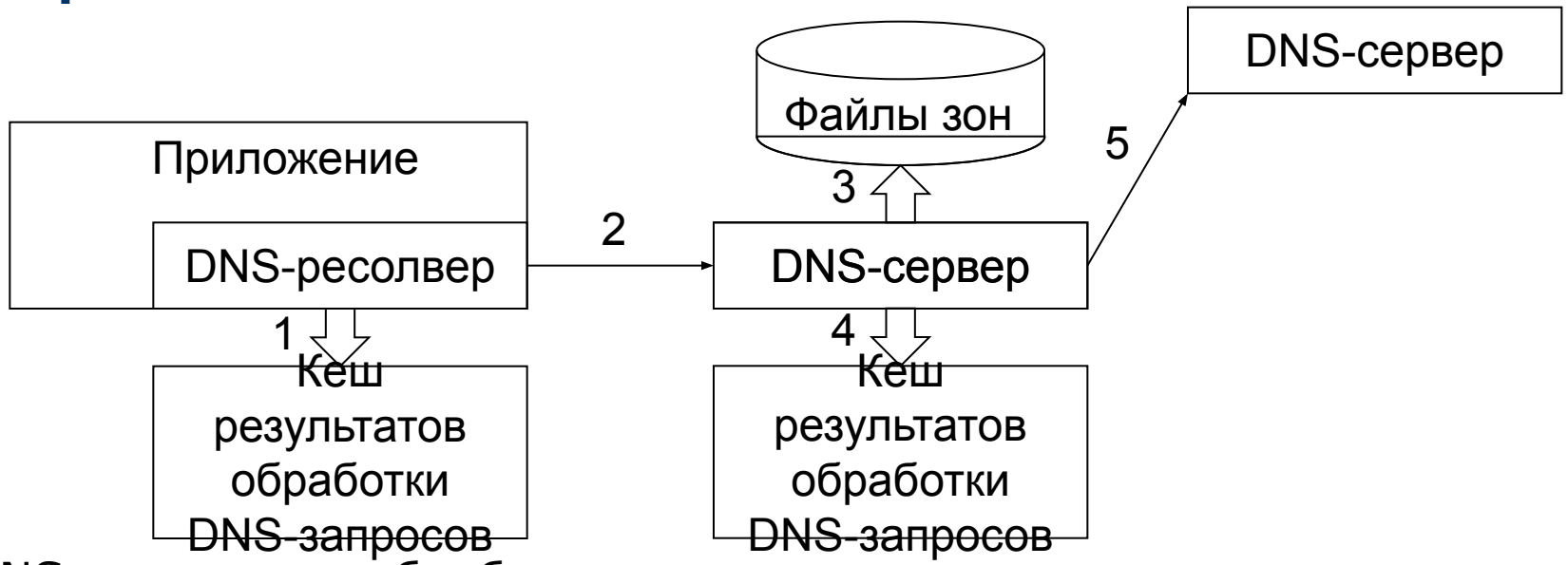
- Приложение может запросить у ресолвера разрешение имени (например, вызвав библиотечную функцию gethostbyname())
- Ресолвер имеет локальный кеш, содержащий результаты обработки предыдущих запросов
  - Результаты могут быть положительные и отрицательные
  - Время жизни результатов в кеше ограничено
  - Если кеш ресолвера содержит ответ на выполненный запрос, то данный ответ возвращается приложению

Domain Name System
Разрешение имен…



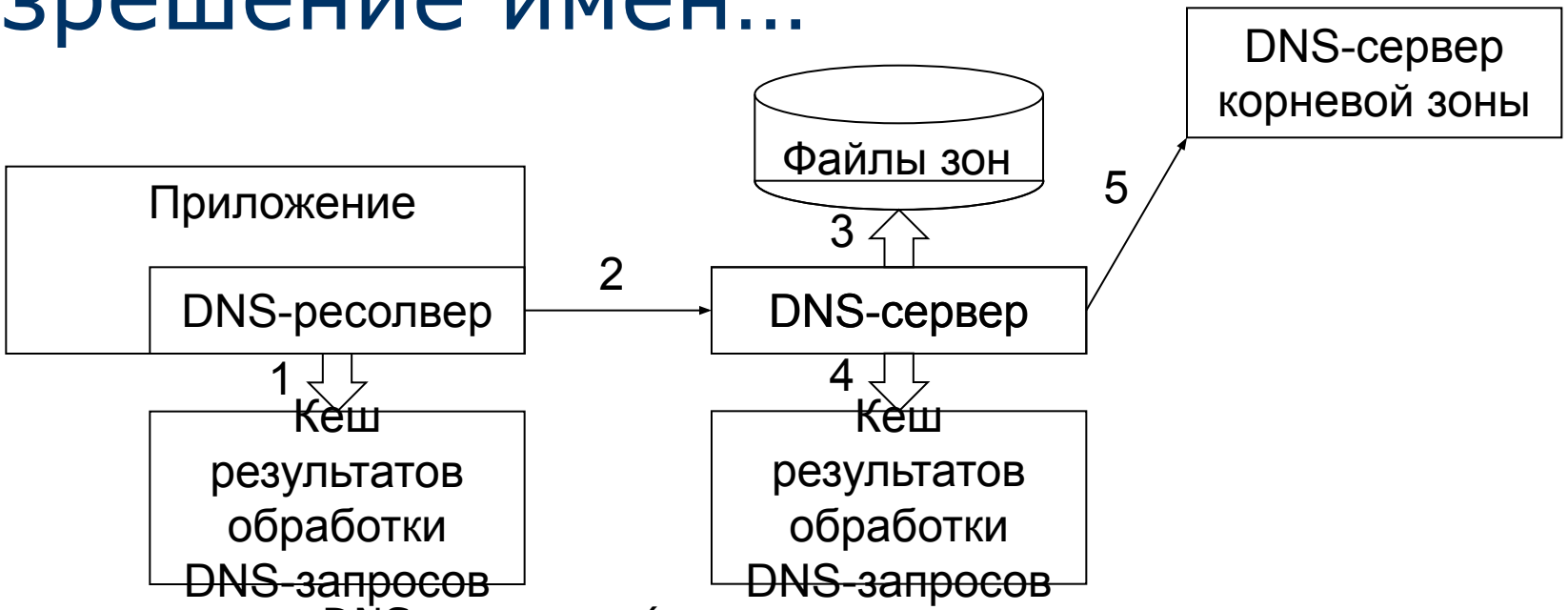
- Если кеш ресолвера не содержит ответа, ресолвер посылает запрос DNS-серверу
  - Одним из параметров настройки узла TCP/IP является IP-адрес DNS-сервера, обеспечивающего разрешение имен
  - Если настройки узла содержат IP-адреса нескольких DNS-серверов, ресолвер обращается к ним в том порядке, в котором они перечислены в настройках, до получения положительного или отрицательного ответа о разрешении имени
  - Если параметры настройки узла не содержат адресов DNS-серверов, ресолвер возвращает приложению ошибку разрешения адреса

Domain Name System Разрешение имен…



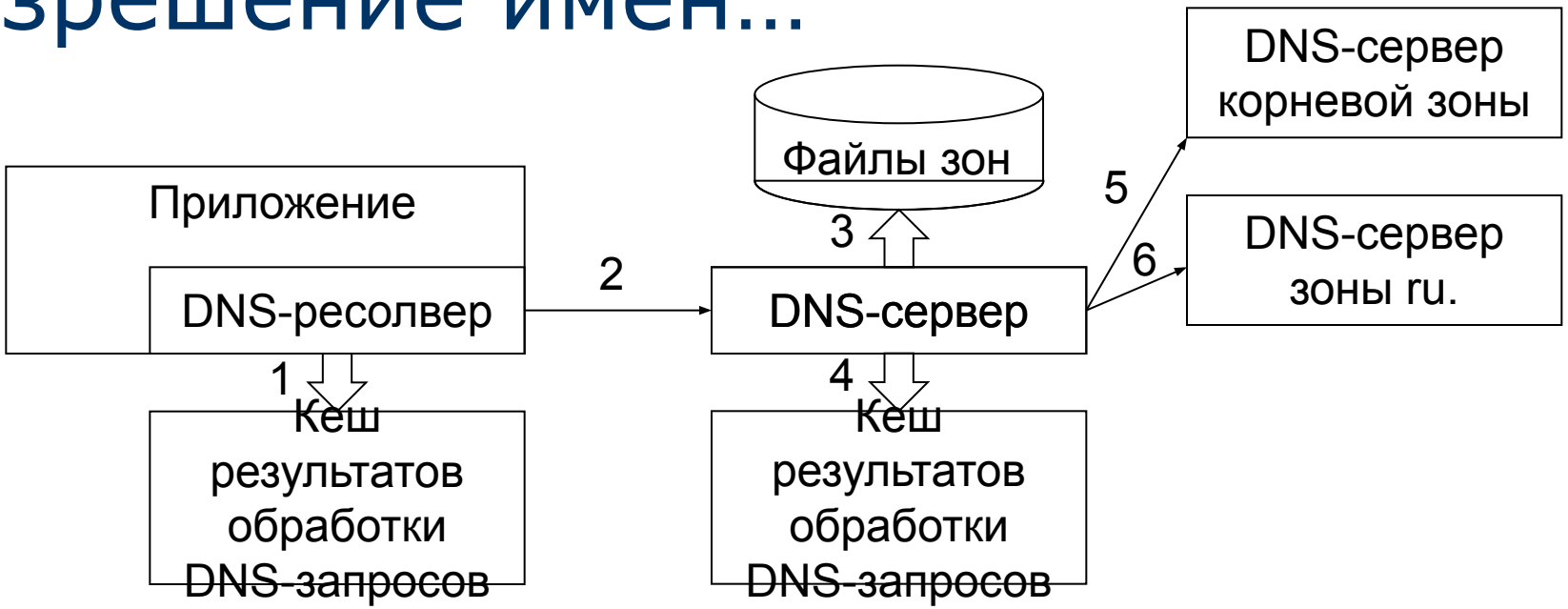
- DNS-сервер при обработке запроса
  - Если запрос относится к зоне, для которой он является авторизованным DNS-сервером – формирует ответ на основании содержимого файла соответствующей зоны
  - В противном случае, если кеш обработанных запросов содержит ответ, возвращается результат из кеша
  - В противном случае выполняется запрос (или последовательность запросов) к другим DNS-серверам

Domain Name System Разрешение имен…



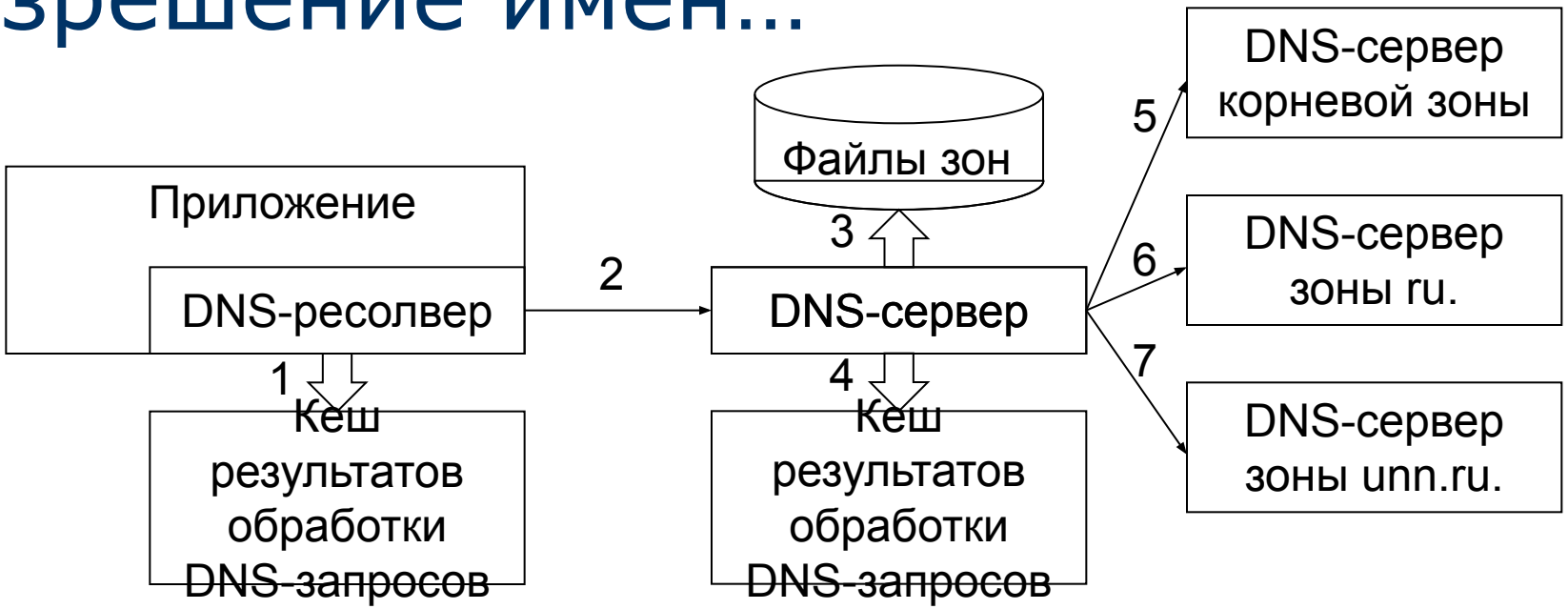
- Запросы к другим DNS-серверам (предположим, мы выполняем запрос на разрешении имени www.unn.ru.)
  - Сначала выполняется запрос одному из DNS-серверов, отвечающих за корневой домен
    - Корневые сервера, скорее всего не являются авторизованными для зоны unn.ru., соответственно, запись с данным именем не хранится в их базах данных
    - Если корневой сервер содержит ответ в своем кеше разрешенных запросов – отправляется ответ из кеша
    - В противном случае, если адрес в запросе принадлежит одному из поддоменов корневого домена – возвращается IP-адрес DNS-сервера, отвечающего за данный домен. Если такого поддомена нет – возвращается ответ об отсутствии запрошенного имени

Domain Name System
Разрешение имен…



- Далее выполняется запрос к DNS-серверу, отвечающему за домен ru.
  - Если данный DNS-сервер является авторизованным для зоны unn.ru., он сформирует ответ в соответствии с содержимым своей базы данных
    - Ответ от сервера, авторизованного для зоны, содержащей запрашиваемое имя, называется авторизованным. Ответ от любого другого DNS-сервера является неавторизованным
  - Если сервер не является авторизованным, может быть возвращен ответ из кеша
  - В противном случае возвращается IP-адрес DNS-сервера, отвечающего за поддомен unn.ru.

Domain Name System
Разрешение имен…

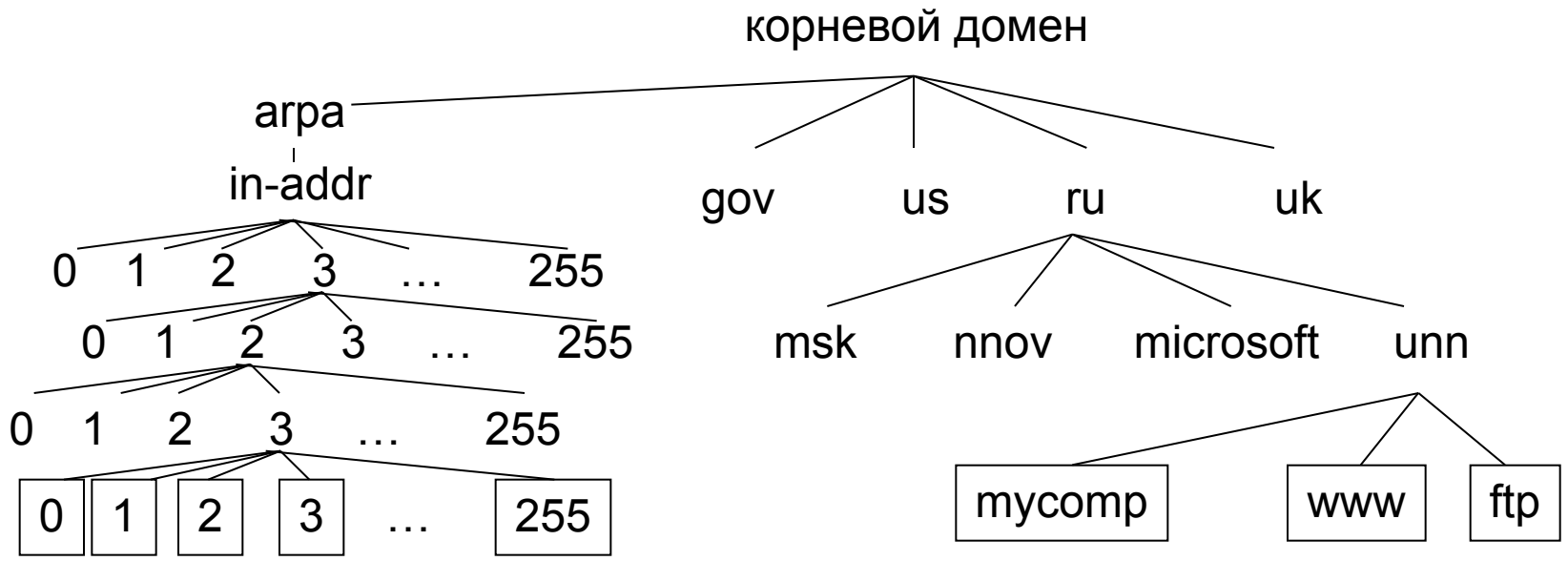


- Далее выполняется запрос к DNS-серверу, отвечающему за домен unn.ru.
  - Данный DNS-сервер обязательно является авторизованным для зоны unn.ru., поэтому он формирует авторизованный ответ о данном имени
- После получения ответа DNS-сервер, обслуживавший запрос, возвращает результат ресолверу

Domain Name System
Разрешение имен

- При разрешении имени могут использоваться два типа запросов
  - Рекурсивный – клиент требует, чтобы ему вернули запрашиваемую запись ресурса, либо установили, что такой записи не существует
    - Такой запрос направляет ресолвер DNS-серверу
  - Нерекурсивный (итеративный) – клиент просит вернуть ему либо запрашиваемую запись, либо IP-адрес DNS-сервера, от которого можно получить более конкретную информацию
    - В нашем примере – запросы от обслуживающего DNS-сервера к DNS-серверам, авторизованным для корневой зоны и зон ru. и unn.ru.

Domain Name System
Зоны обратного просмотра



- Reverse lookup zones – зоны обратного просмотра, предназначены для определения доменных имен по IP-адресам
  - Домен in-addr.arpa. содержит 256 поддоменов с именами 0, 1, 2, …, 255
  - Домены d.in-addr.arpa. содержат по 256 поддоменов с именами 0, 1, 2, …, 255
  - Домены c.d.in-addr.arpa. содержат по 256 поддоменов с именами 0, 1, 2, …, 255
  - Домены b.c.d.in-addr.arpa. содержат по 256 записей с именами 0, 1, 2, …, 255
  - Записи a.b.c.d.in-addr.arpa. содержат канонические имена узлов

Domain Name System
Записи ресурсов…

- Описания ресурсов последовательно размещаются в файлах зон и имеют следующий синтаксис
  [Owner] [TTL] [Class] Type Data
  - запись [поле] означает, что данное поле необязательно
  - Owner (владелец) – имя узла или имя домена, которому принадлежит запись ресурса
    - если имя не указано, используется имя из предыдущей записи
  - TTL (time to live) – время жизни записи в кеше ресолвера DNS или DNS-сервера (в секундах)
    - если TTL не указан, используется минимальное значение TTL из записи SOA

Domain Name System
Записи ресурсов

- [Owner] [TTL] [Class] Type Data
  - Class – используемый стек протоколов, для Интернета используется значение IN; другие возможные значение – CH (Chaos), HS (Hesoid)
    - по умолчанию используется значение IN
  - Type – тип записи (SOA, NS, MX, A, и т.д.)
  - Data – данные записи ресурса, содержимое зависит от типа записи (доменное имя, IP-адрес, произвольная строка и пр.)
- Комментарии начинаются с символа ";" и заканчиваются в конце строки

Domain Name System
Типы записей ресурсов…

- SOA (Start Of Authority) – содержится в начале файла зоны и определяет следующие ее параметры
  - Owner, TTL, Class, Type
  - Authoritative server – основной авторизованный сервер для данной зоны
  - Responsible person – почтовый адрес администратора, ответственного за данную зону
  - Serial number – порядковый номер версии зоны (дополнительные DNS-сервера, обслуживающие зону, при обновлении сравнивают номер версии в своей копии с номером версии зоны на основном сервере и выполняют обновление только в том случае, если номер их локальной копии меньше)

Domain Name System
Типы записей ресурсов…

- SOA (Start Of Authority)
  - Refresh (в секундах) – интервал, с которым дополнительные сервера зоны проверяют наличие в ней изменений
  - Retry (в секундах) – интервал, через который дополнительный сервер в случае неудачного завершения обслуживания запроса на передачу предпринимает следующую попытку
  - Expire (в секундах) – время после последнего успешного приема зоны, в течение которого дополнительный сервер обслуживает запросы к ней
  - Minimum TTL (в секундах) – TTL по умолчанию для всех записей ресурсов зоны, также используется как TTL для отрицательных ответов для зоны

Domain Name System
Типы записей ресурсов…

- SOA (Start Of Authority)

```
unn.ru. IN SOA ns.unn.ru. admin.unn.ru. (
  2008083101; Serial number
  3600;   Refresh (1 час)
  300;    Retry (10 мин)
  86400; Expire (1 сутки)
  3600;   Minimum TTL (1 час)
)
```

Domain Name System
Типы записей ресурсов…

- NS – определяет авторизованный DNS-сервер данной зоны
  - для зоны Интернет должно быть определено не менее двух авторизованных серверов, имеющих IP-адреса в разных сетях класса C
  - для определения локальных зон можно использовать один DSN-сервер

```
unn.ru  IN  NS  ns.unn.ru.
unn.ru  IN  NS  ns2.unn.ru.
unn.ru  IN  NS  ns3.unn.ru.
```

Domain Name System
Типы записей ресурсов…

- A – сопоставляет доменному имени IP-адрес (IPv4)
- AAAA или A6 – сопоставляет доменному имени IP-адрес (IPv6)
- PTR – сопоставляет IP-адресу доменное имя узла
- CNAME – определение псевдонима DNS-имени

```
mail.unn.ru.    IN  CNAME    ns.unn.ru.
ns.unn.ru.          IN  A   1.2.3.4
ns2             IN  A6 1.2.3.4.5.6.7.8
4.3.2.1.in-addr.arpa.  IN  PTR    ns.unn.ru.
```

Domain Name System
Типы записей ресурсов…

- MX – определяет имя почтового сервера для указанного доменного имени (почта, отправленная на адрес user@unn.ru будет отправляться именно на этот сервер)
  - можно указать несколько почтовых серверов и их относительные приоритеты после поля "тип записи" (чем меньше численное значение, тем выше приоритет)

```
unn.ru.      IN MX   0  mail.unn.ru.
*.unn.ru.    IN MX   0  mail.unn.ru.
unn.ru.      IN MX   10 mail2.unn.ru.
```

Domain Name System
Типы записей ресурсов

- SRV – позволяет определять адреса сервисов в домене, содержит поля
  - _Service – имя сервиса
  - _Protocol – имя протокола
  - Name – имя доменной записи
  - TTL, Class, SRV
  - Priority – приоритет записи (чем меньше значение, тем выше приоритет)
  - Weight – вес записи (используется для балансировки нагрузки)
  - Port – номер порта сервиса
  - Data – доменное имя хоста, на котором запущен сервис

```
_http._tcp.unn.ru. IN SRV 0 0 80  www.unn.ru.
_ftp._tcp.unn.ru.   IN SRV 0 0 80  ftp.unn.ru.
```

Domain Name System
Делегирование управления

- Делегирование управления поддоменом осуществляется посредством указания в зоне родительского домена авторизованного DNS-сервера для дочернего домена
- Обычно используется следующая пара записей
  - имя_поддомена IN NS имя_DNS_сервера
  - имя_DNS_сервера IN A IP_адрес_DNS_сервера

```
vmk.unn.ru.    IN  NS ns.vmk.unn.ru.
ns.vmk.unn.ru.     IN  A   5.6.7.8
vmk.unn.ru.    IN  NS ns2.vmk.unn.ru.
ns2.vmk.unn.ru.    IN  A   9.10.11.12
```

Domain Name System
Berkley Internet Name Domain

- Berkley Internet Name Domain (bind) – сервер DNS, реализованный Кевином Дунлапом (Kevin Dunlap) в 1985 г. и включенный в BSD UNIX
- В настоящий момент – самая распространенная реализация (текущая версия – 9)
- Конфигурация описывается в
  - основном конфигурационном файле (в UNIX - /etc/named.conf)
  - файлах зон (имена файлов зон задаются в основном конфигурационном файле)

Domain Name System
DNS в Windows

- Реализация DNS-сервера для Windows поддерживает дополнительную функциональность
  - Интеграция с Active Directory
  - Поддержка динамических обновлений и удаление устаревших записей
  - Безопасное динамическое обновление в зонах, интегрированных в Active Directory
  - Интеграция с другими сетевыми сервисами

Заключение

- Сервис доменных имен (DNS) обеспечивает установление соответствия между доменными именами и IP-адресами
  - Одинаково важны как прямое, так и обратное разрешение адресов
- DNS поддерживает иерархическую структуру именования ресурсов, и соответствующую схему делегирования ответственности за домены

Тема следующей лекции

- Dynamic Host Configuration Protocol
- Доставка почты

Вопросы для обсуждения

Литература

- Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server. – М.: Русская редакция, 2001.
- В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2001.