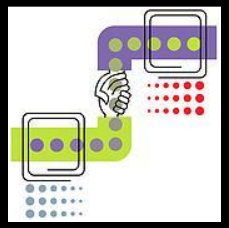
Служба DNS

Сетевое администрирование - Тема 3

«Человеческий фактор» DNS



Компьютеры и другие сетевые устройства, отправляя друг другу пакеты по сети, используют IP-адреса.

Но, человеку гораздо проще и удобнее запомнить некоторое символические имена сетевых узлов, чем четыре бессодержательных для него числа.

Должны существовать механизмы, сопоставляющие именам узлов их IP-адреса:

1. локальный для каждого компьютера файл hosts
2. централизованная иерархическая служба имен DNS

Система доменных имен DNS

DNS была описана Полом Мокапетрисом (Paul Mockapetris) в 1983.

- архитектура DNS остается неизменной с момента своего создания, но функции существенно изменились
- начиная с 90-х годов, DNS стали использовать в качестве инструмента балансировки нагрузки серверов информационных ресурсов - алгоритм Round Robin, который применяется серверами доменных имен при ответе на запросы клиентов

Роль имени (доменного имени) в процессе установки соединения - получение IP адреса.

Служба DNS

Система доменных имен — ключевая служба, на которую замыкаются адреса информационных ресурсов, а точнее их идентификаторы Uniform Resource Identifier

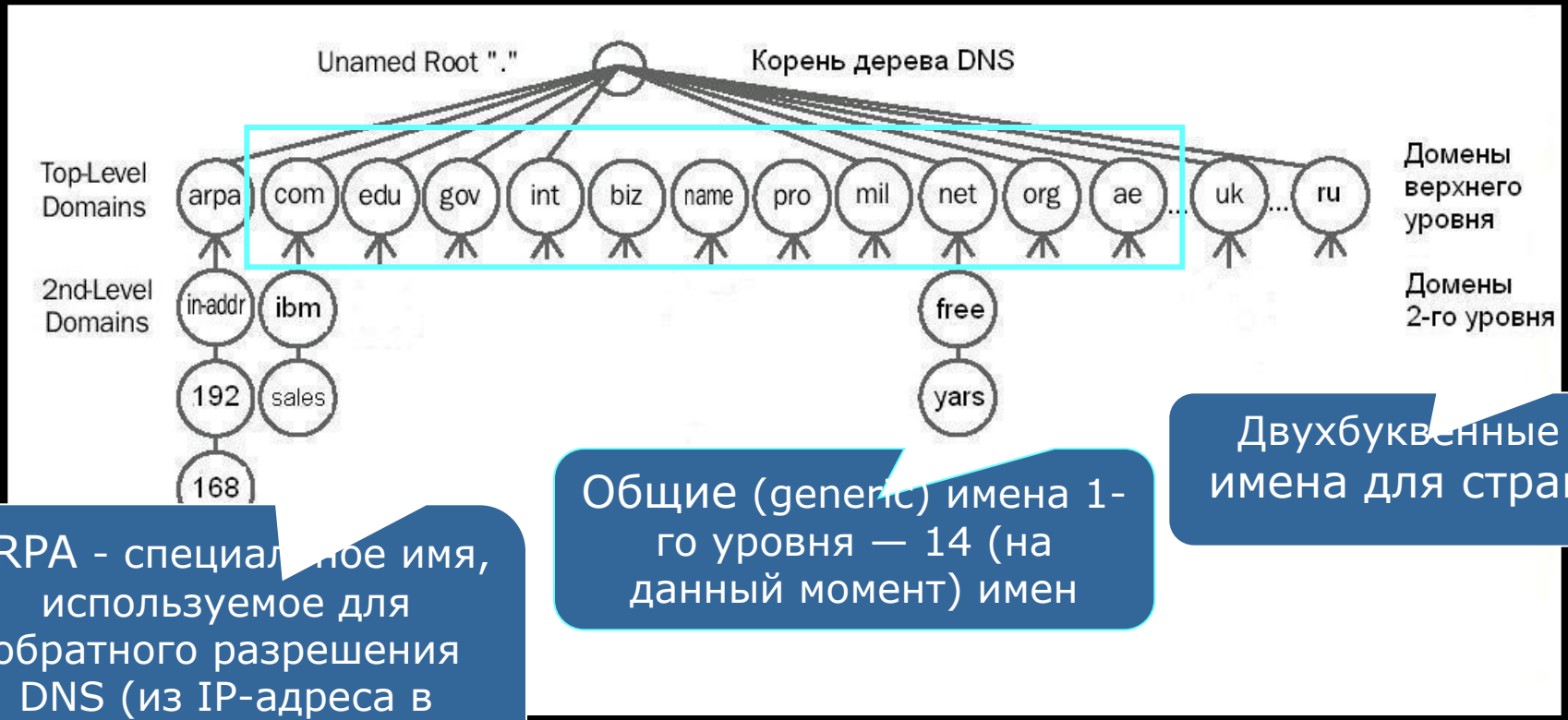
В системе доменных имен установлена жесткая иерархия:

- корень системы называется «root»;
- домены первого или верхнего уровня (top-level или TLD) – общего пользования и национальные .com, .org, .ru;
- более мелкие домены второго уровня, например, корпоративные – microsoft.com

DNS: основные концепции

1. Концепция использования DNS для разрешения имен узлов
   - нахождение соответствующего узлу IP-адреса
   - разрешения FQDN (Fully Qualified Domain Name – полностью определенное имя домена) в его IP-адрес
2. Концепция Зоны – область пространства имен DNS, функционирующая как административная единица
   - группа серверов ответственна (имеет полномочия) за записи, относящиеся к некоторому домену или поддомену

Пространство имен DNS



ARPA - специальное имя, используемое для обратного разрешения DNS (из IP-адреса в полное имя узла)

Общие (generic) имена 1-го уровня — 14 (на данный момент) имен

Двухбуквенные имена для стран

Владельцы ресурсов предпочитают использовать домены второго уровня в рамках национальных доменов или доменов общего назначения (например, microsoft.com), а не закапываться вглубь иерархии имен.

DNS: разрешение имен узлов

- Служба DNS хранит большое число записей ресурсов различного типа
  - A – представляет уникальный адрес узла в сети, сопоставляя его имя IP-адресу
  - NS – указывает на серверы DNS, ответственные за конкретный домен и его поддомены
  - MX – обозначает, что данный узел является почтовой службой для определенного домена
  - PTR – предоставляет возможность для обратного просмотра, сопоставляет IP-адресу узла его FQDN
  - SRV – сопоставляет отдельные службы одному или нескольким узлам и наоборот
  - SOA –запись ресурса начальной записи зоны
  - CNAME (alias) - отображает одно имя на другое

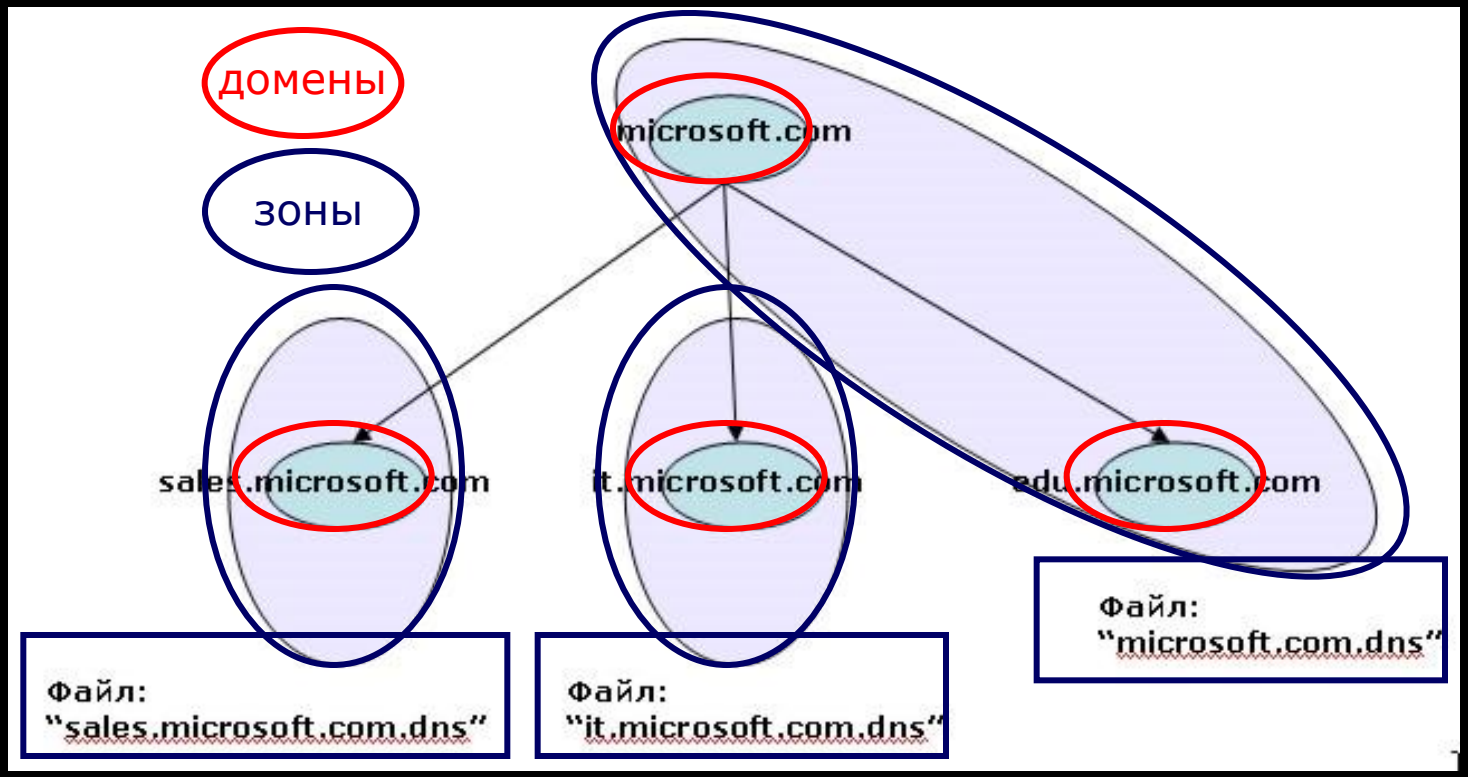
DNS: домены и зоны

Информация о доменах, хранящаяся в БД сервера DNS, организуется в зоны. Зона — основная единица репликации данных между серверами DNS.

Windows Server поддерживают следующие типы зон:

1. Стандартная основная (standard primary) — главная копия стандартной зоны
2. Стандартная дополнительная (standard secondary) — копия основной зоны
3. Интегрированная в Active Directory (Active Directory–integrated) - вся информация о зоне хранится в виде одной записи в базе данных AD
4. Зона-заглушка (stub, только в Windows 2003) — особый тип зоны

DNS: домены и зоны



Домен — понятие чисто логическое, относящееся только к распределению имен, и никак не связанное с технологией хранения информации о домене.

Зона — это способ представления информации в хранилище тех серверов DNS, которые отвечают за данный домен и поддомены.

DNS: домены и зоны

Зоны, рассмотренные на предыдущем слайде, являются зонами прямого просмотра (forward lookup zones):

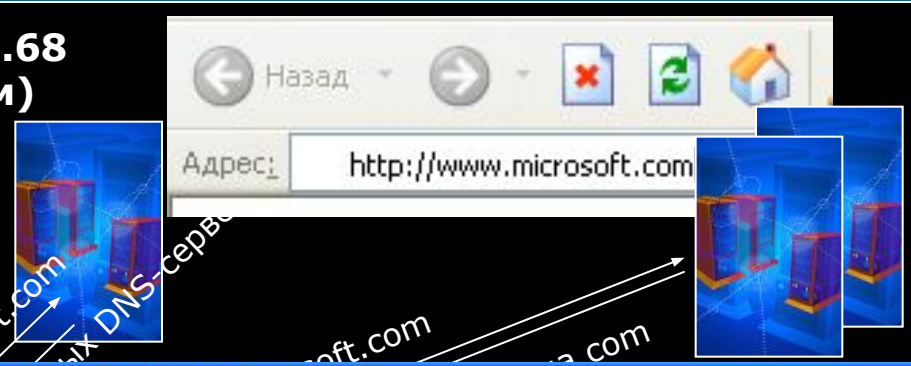
- Служат для разрешения имен узлов в IP-адреса
- Наиболее часто используемые для этого типы записи: A, CNAME, SRV

Для определения имени узла по его IP-адресу служат зоны обратного просмотра (reverse lookup zones)

- Основной тип записи в «обратных» зонах — PTR
- Для решения данной задачи создан специальный домен с именем «in-addr.arpa»

Итеративный запрос DNS

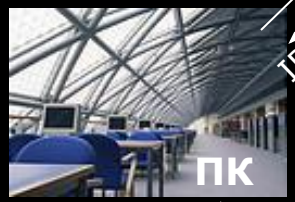
217.15.135.68 (Ятелеком)

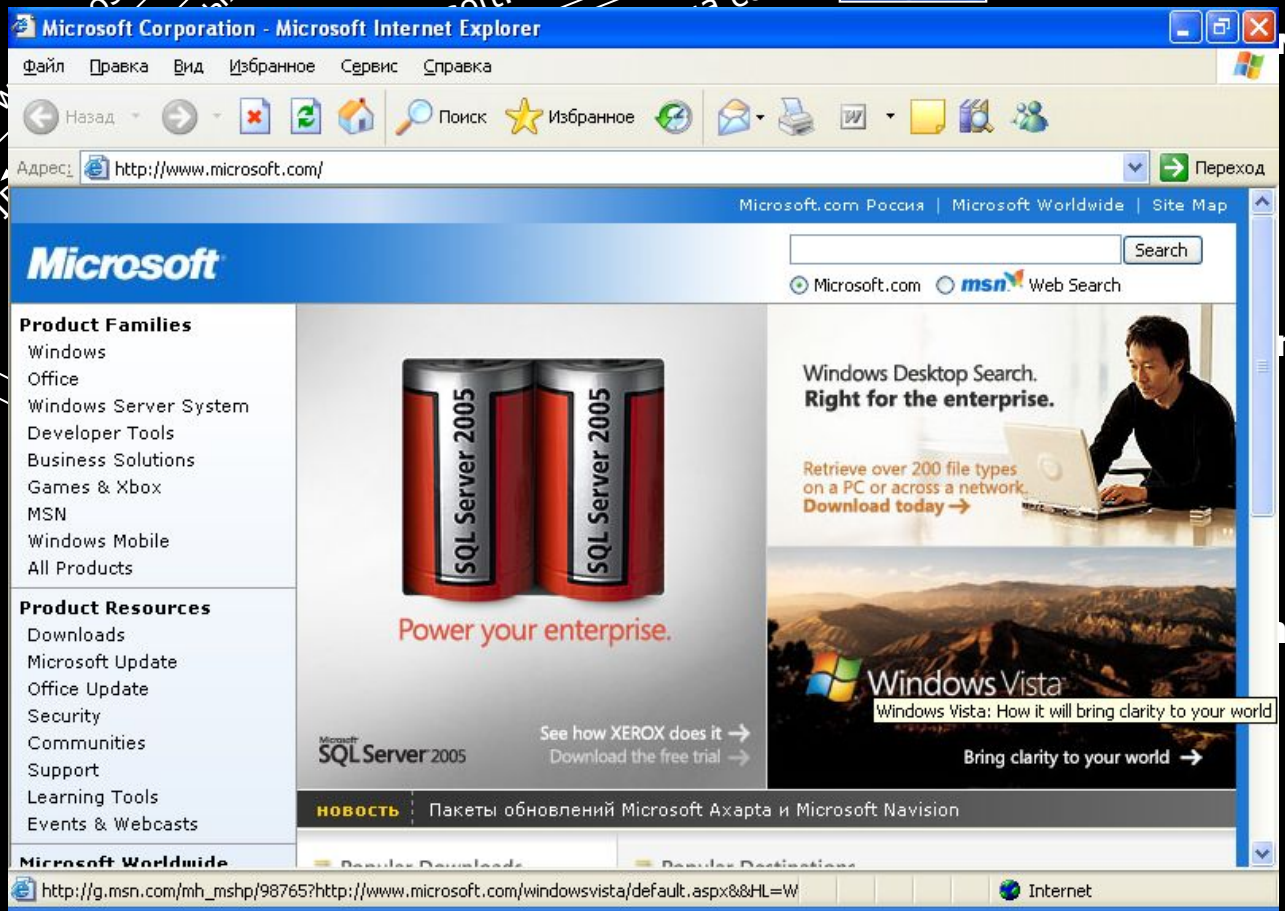


Корневые серверы DNS

мена com

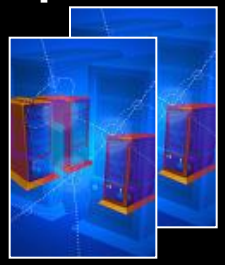
microsoft.com





Рекурсивный запрос DNS

Корневые серверы DNS

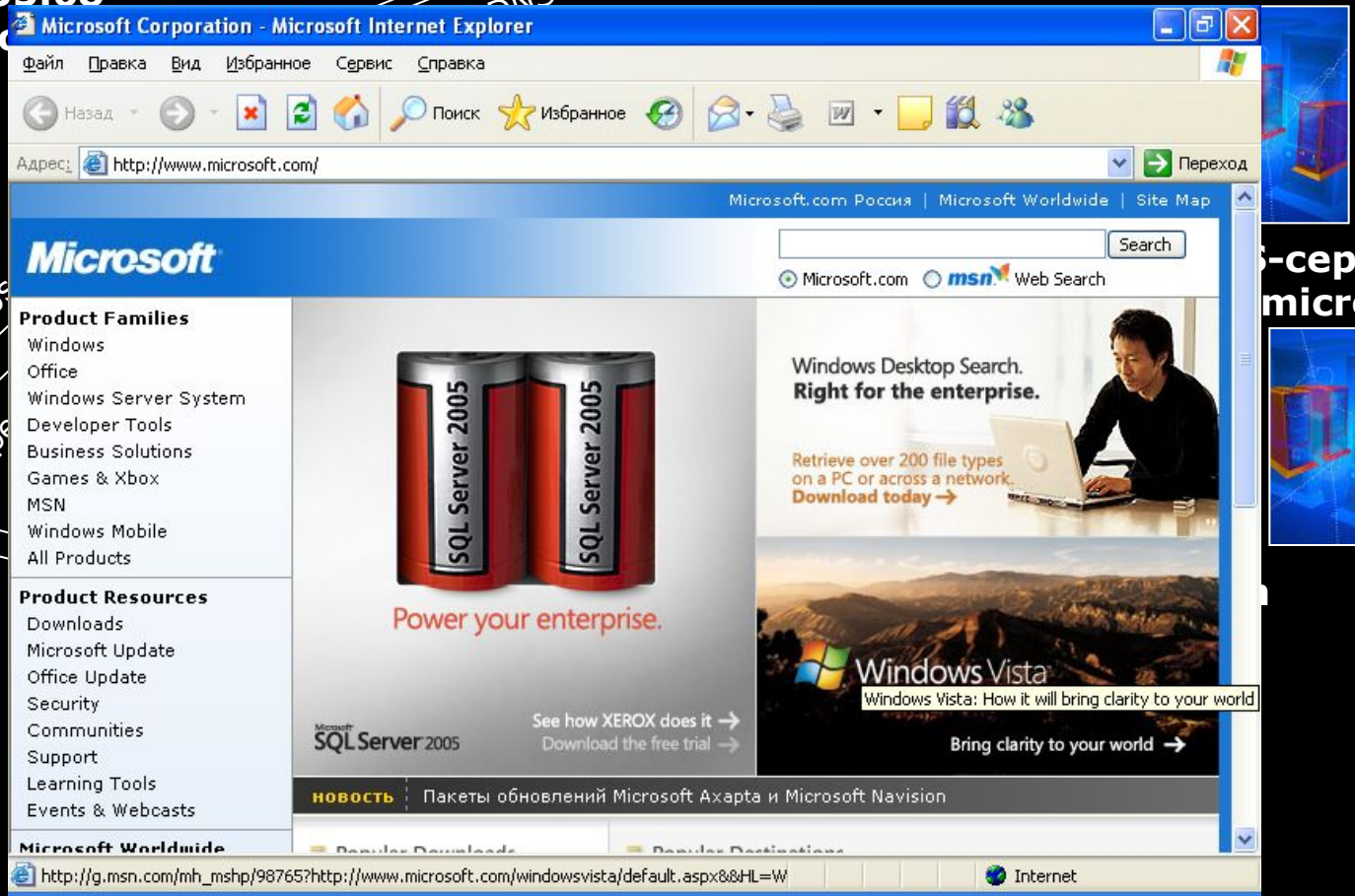


www.microsoft.com

DNS-серверов домена com

DNS-серверы домена com

217.15.135.68
(Ятелеко



-серверы
microsoft.com

www.micros

IP-адре