

Система доменных имен DNS



Борисов Владимир Анатольевич
КАСК - филиал РАНХ и ГС
Красноармейск 2012 г.



DNS

- Domain Name Service — Система Доменных Имен.



DNS

- Является сетевой службой, которая в режиме реального времени сопоставляет символьную запись домена или доменного имени (URL) с его числовым значением (IP-адресом), и наоборот.

Доменная система наименования

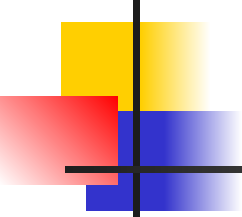


- Была придумана и введена для более комфортной и легкой работы пользователей.

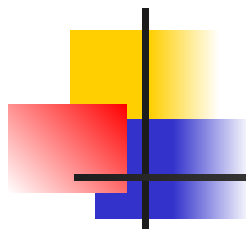
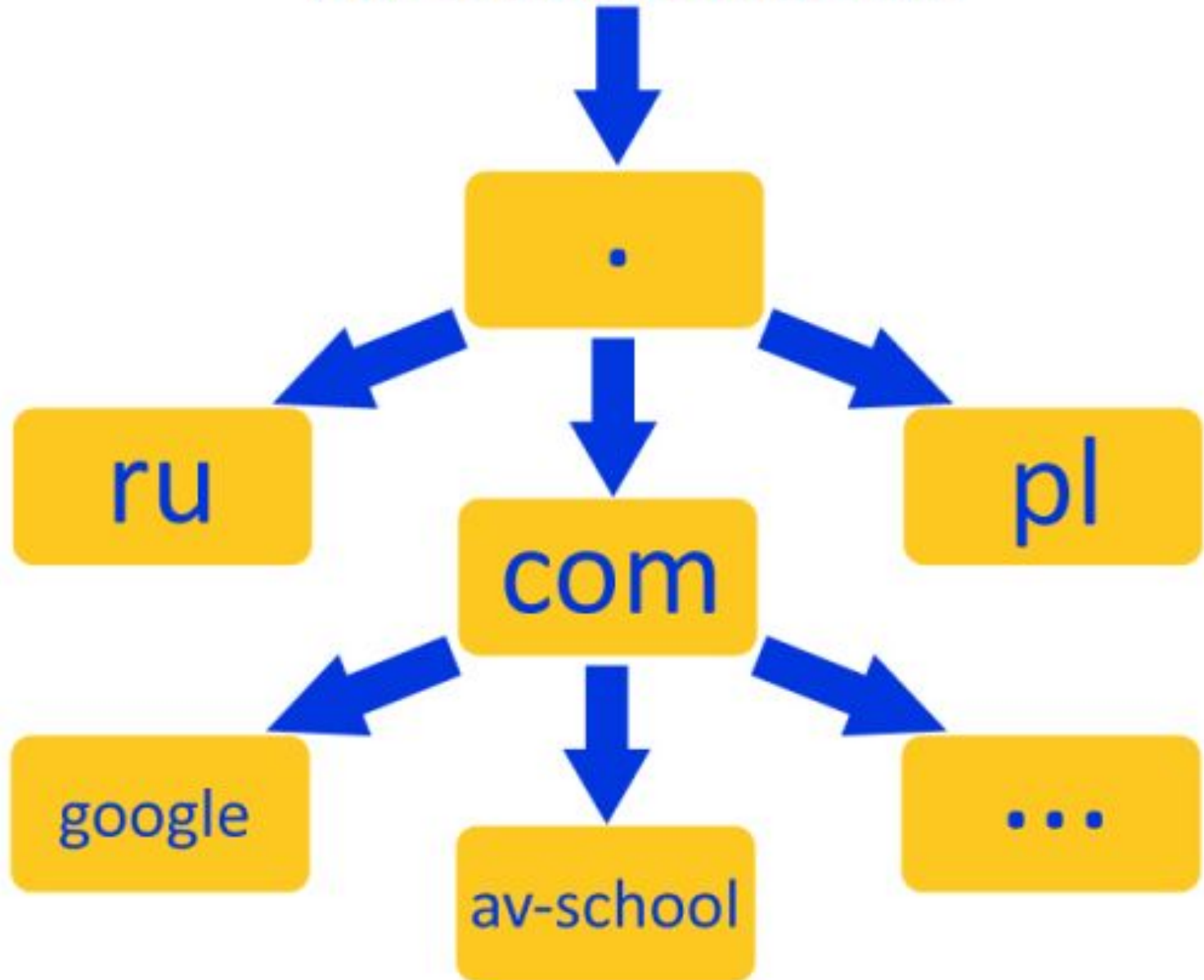


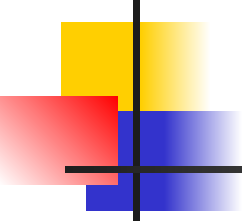
DNS

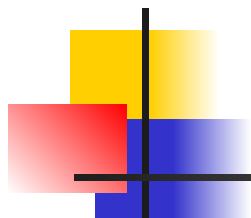
- Это целая сеть особых серверов, оборудованных специализированным программным обеспечением, которые либо работают с определенными доменными зонами и именами, либо выполняют некоторые служебные функции.

- 
-
- В основе функционирования DNS лежит принцип иерархического деления доменных зон и имен, за которые отвечают отдельно взятые серверы, управляемые частными лицами или организациями.

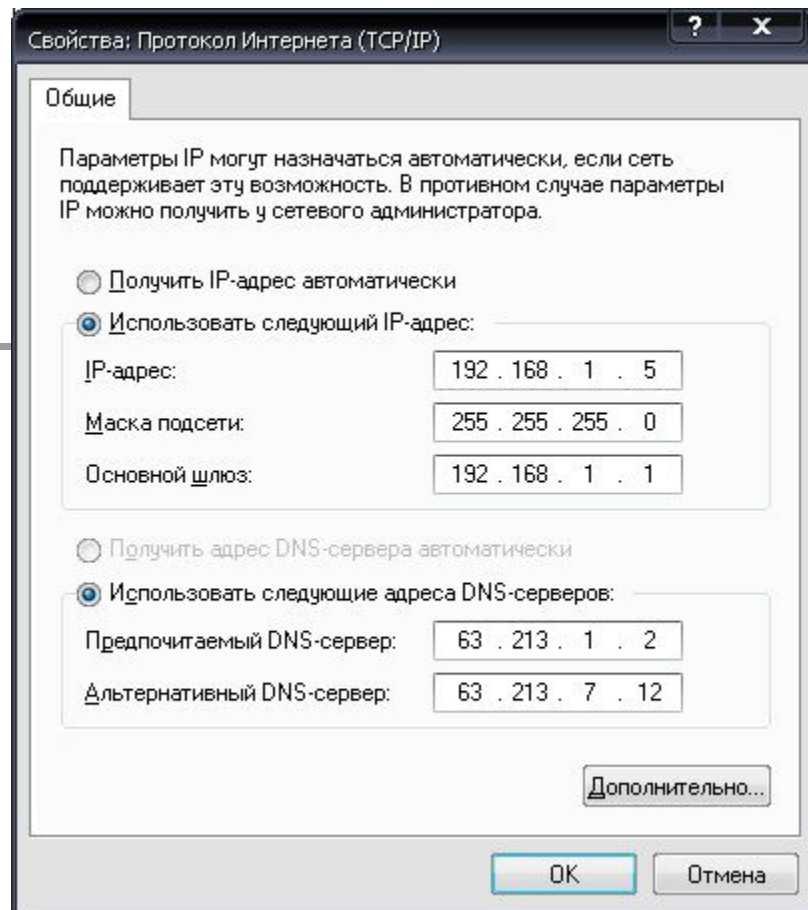
AV-school.com.



- 
-
- Для надежности и устойчивости службы DNS в целом и отдельных ее уровней создаются еще несколько серверов с идентичной информацией, чтобы в случае проблем с одним DNS-сервером его нагрузку без всякой потери информации можно было перенести на другой сервер раздачи адресов.



- С помощью специального ПО и некоторых аппаратных средств дополнительно поддерживается синхронность информации, размещенной на разных серверах.





Терминология



Корневой домен (root)

- Своеобразный корень в древе обозначений доменов, неименованный уровень.
- Задается в виде точки в конце имени.
- Например точка, стоящая в конце имени: `subdomain.domain.com.`



Домен верхнего уровня

- Имя (чаще аббревиатура или сокращение), состоящее из двух или трех символов, обычно указывающее на страну или тип организации, владеющей сайтом.



Пример

- **ru** – Россия
- **ua** – Украина
- **fr** – Франция
- **de** – Германия
- **uk** – Англия
- **us** – США
- **com** – коммерческая организация
- **edu** – образовательная организация
- **gov** – правительственная организация
- **mil** – военная организация
- **net** – провайдер
- **org** – прочие



Домен второго уровня

- Имя произвольной длины, зарегистрированное частным лицом или организацией для использования в Интернете (обычно основано на домене верхнего уровня).
- Например: domain.org



Субдомен

- Дополнительное имя, которое может создать организация в пределах домена второго уровня.
- Например: `subdomain.domain.org`



Имя хоста или ресурса

- Последняя часть древа DNS.
- Задает определенный хост или ресурс.
- Например: `host.subdomain.domain.org`



Принцип работы



Узлы DNS

- Именные серверы, они же серверы DNS, каждый из которых хранит информацию о нескольких доменах.
- Эта информация находится в файлах, которые называются зонами.



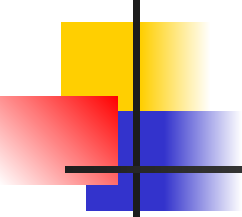
Зона

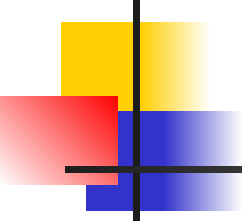
- Состоит из записей, в которых прописан главный сервер имен доменной зоны, адрес электронной почты администратора и другая информация, нужная для синхронизации информации, расположенной на разных серверах.



Записи доменных зон

- **A** - хранит соответствие имени домена и его IP.
- **MX** - указывает имя почтового сервера, на который надо пересылать всю почту, предназначенную адресам в этом домене.
- **NS** - обозначает и указывает именные сервера.

- 
-
- DNS берет свое начало с 13 так называемых корневых серверов, которые расположены в США и хранят зоны для корневого домена (".").
 - Эти серверы хранят информацию об именных серверах для всех доменов первого уровня.

- 
-
- Из-за ограничения на размеры DNS-пакета (512 байт) в DNS в ответ трассировки может быть включено не более 13 серверов, хотя на самом деле за 13 виртуальными серверами (зачастую зеркалами корневых) стоят 190 (с разным численным разбросом на каждый).
 - Ближайший к пользователю адрес зеркала корневого сервера выбирается с помощью системы IP AnyCast.

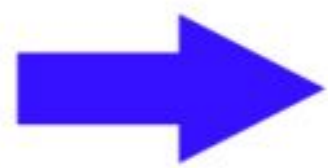
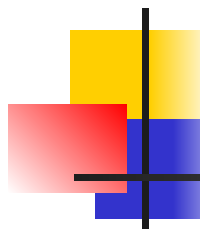
DNS – reverse DNS (обратная DNS)

- В качестве доменного имени используется особым образом записанный IP-адрес, преобразованный в домене in-addr.arpa.
- В зонах, соответствующих доменам обратной DNS, для каждого IP-адреса (или имени в in-addr.arpa) хранится запись, сопоставляющая его с доменным именем.



Сходимость

- Если сконвертировать с помощью обратной DNS IP-адрес в доменное имя, а потом это имя с помощью обычной DNS обратно в IP, то должен получиться тот же самый адрес.



DNS



IP
198.230.xxx.yyy.



**reverse
DNS**



convergence...?





Фишинг

- Независимо от введенного пользователем URL, он перенаправляется на лжестраничку, где ему по стандартной схеме предлагают ввести персональные данные или просто вешают зловреда.
- В последнем случае хакеру удастся установить на компьютер пользователя небольшую утилиту, прописывающуюся в реестре ОС, после чего все обращения идут через тот DNS, который укажет злоумышленник.



Вывод

- С приходом DNS пользователи получили выгоду, связанную с легкостью запоминания адресов интернет-ресурсов, а также еще одну головную боль из-за новых видов мошеннических актов и хакерских атак, довольно быстро набирающих обороты в таком необходимом всем сервисе.



Ресурсы

- <http://av-school.ru/article/a-175.html>
- <http://ru.wikipedia.org/wiki/DNS>
- <http://school-collection.edu.ru/catalog/rubr/13899a9b-11fc-4a07-861c-1cf294b8f895/113185/>
- <http://site.nic.ru/content/view/225/29>
- <http://www.cctld.ru/ru/docs/legals/domainsite.php>
- <http://a-nomalia.narod.ru/rInform/155.htm>
- <http://citforum.ru/internet/dns/khramtsov/>
- http://mdesign.ru/faq/faq_list/4070cbadcae59?start
- <http://it.sander.su/DNS.php>