Лекция 12. Символьная адресация в сетях

Как было уже сказано ранее, в стеке протоколов TCP/IP используются три типа адресов – физические, IP-адреса и символьные (например, доменные) имена. Физические адреса служат для адресации на канальном уровне. IP-адреса применяются на сетевом уровне, с их помощью можно построить большую составную сеть, например, Интернет. Доменные имена кажутся в этом ряду необязательными; действительно, сеть будет работать и без них. Однако человеку-пользователю сети неудобно запоминать числовые IP-адреса, ассоциируя их с конкретными сетевыми объектами. Мы привыкли к символьным именам, и именно поэтому в стек TCP/IP была введена система доменных имен DNS (Domain Name System). Она описывается в RFC 1034 и RFC 1035. Полное название доменных имен – FQDN (Fully Qualified Domain Name – полностью определенное имя домена). Кроме DNS-имен Windows Server 2003 поддерживает символьные имена NetBIOS (о них, а также о службе WINS, предназначенной для преобразования NetBIOS-имен в IP-адреса, рассказывается в конце этой лекции).

1. Система доменных имен

Пространство имен DNS

Система DNS основана на иерархической древовидной структуре, называемой пространством доменных имен. Доменом является каждый узел и лист этой структуры. На рис. 1 приведен фрагмент пространства доменных имен Интернета. Самый верхний домен называется корневым (root domain). Корневой домен как реальный узел не существует, он исполняет роль вершины дерева. Непосредственные его потомки (поддомены) – домены первого уровня TLD (Top-Level Domain – домены верхнего уровня). Их можно разделить на три группы (см. Приложение II):

- .arpa – особый домен, используемый для преобразования IP-адресов в доменные имена (обратное преобразование). Содержит единственный дочерний домен – in-addr;
- домены организаций – .com (коммерческие организации), .org (некоммерческие организации), .edu (образовательные учреждения) и т.д.;
- домены стран (географические домены) – .ru (Россия), .fr (Франция), .de (Германия) и т. д.

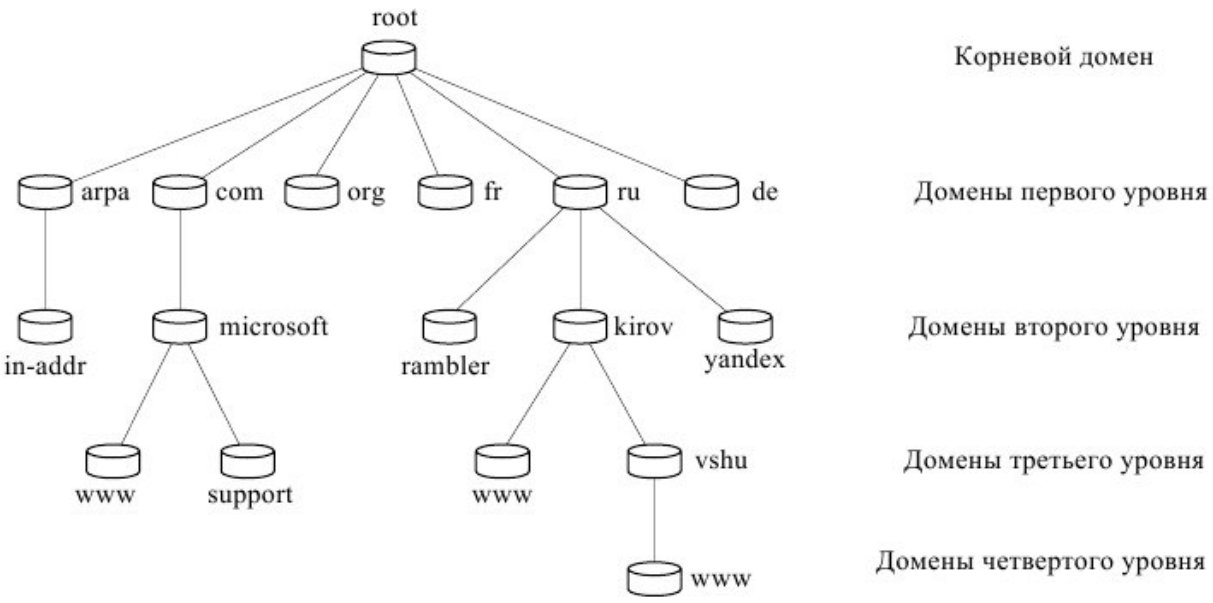

Рис. 1. Условный фрагмент пространства доменных имен Интернета

Домены первого уровня включают только домены второго уровня, записи об отдельных хостах могут содержаться в доменах, начиная со второго уровня. Созданием и управлением доменами первого уровня с 1998 года занимается международная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers – Корпорация Интернет по присвоению имен и адресов, www.icann.org). Домены второго уровня, находящиеся в географических доменах, распределяются специальными национальными организациями, которым ICANN передало полномочия в этом вопросе. Управлением доменами третьего и следующего уровней занимаются владельцы соответствующих доменов второго уровня. Полностью определенное доменное имя FQDN записывается следующим образом. Сначала идет имя хоста (лист в дереве пространства имен), затем через точку следует DNS-суффикс – последовательность доменных имен всех уровней до первого включительно. Запись оканчивается точкой, после которой подразумевается корневой домен. Пример FQDN для хоста www домена vshu:

www.vshu.kirov.ru.

В этой записи www – имя хоста, vshu.kirov.ru. – DNS-суффикс. Точку в конце FQDN обычно можно опускать.

Служба DNS

Пользователь работает с доменными именами, компьютеры пересылают пакеты, пользуясь IP-адресами. Для согласования двух систем адресаций необходима специальная служба, которая занимается

переводом доменного имени в IP-адрес и обратно. Такая служба в TCP/IP называется Domain Name Service – служба доменных имен (аббревиатура DNS совпадает с аббревиатурой системы доменных имен). Процесс преобразования доменного имени в IP-адрес называется разрешением доменного имени.

В те времена, когда в сети ARPANET было несколько десятков компьютеров, задача преобразования символьного имени в IP-адрес решалась просто – создавался текстовый файл hosts, в котором хранились соответствия IP-адреса символьному имени. Этот файл должен был присутствовать на всех узлах сети. По мере увеличения числа узлов объем файла стал слишком большим, кроме того, администраторы не успевали отслеживать все изменения, происходящие в сети. Потребовалась автоматизация процесса разрешения имен, которую взяла на себя служба DNS.

Служба доменных имен поддерживает распределенную базу данных, которая хранится на специальных компьютерах – DNS-серверах. Термин «распределенная» означает, что вся информация не хранится в одном месте, её части распределены по отдельным DNS-серверам. Например, за домены первого уровня отвечают 13 корневых серверов, имеющих имена от A.ROOT-SERVERS.NET до M.ROOT-SERVERS.NET, расположенных по всему миру (большинство в США). Такие части пространства имен называются зонами (zone).

Пространство имен делится на зоны исходя из удобства администрирования. Одна зона может содержать несколько доменов, так же как информация о домене может быть рассредоточена по нескольким зонам. На DNS-сервере могут храниться несколько зон. В целях повышения надежности и производительности зона может быть размещена одновременно на нескольких серверах, в этом случае один из серверов является главным и хранит основную копию зоны (primary zone), остальные серверы являются дополнительными, на них содержатся вспомогательные копии зоны (secondary zone).

Для преобразования IP-адресов в доменные имена существуют зоны обратного преобразования (reverse lookup zone). На верхнем уровне пространства имен Интернета этим зонам соответствует домен in-addr.arpa. Поддомены этого домена формируются из IP-адресов, как показано на рис. 2.

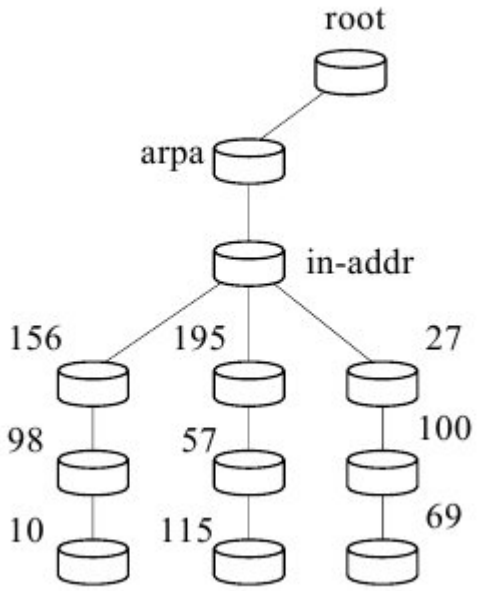

Рис. 2. Формирование поддоменов домена arpa

Следуя правилам формирования DNS-имен, зона обратного преобразования, соответствующая подсети 156.98.10.0, будет называться 10.98.156.in-addr.arpa.

Процесс разрешения имен

Служба DNS построена по модели «клиент-сервер», т. е. в процессе разрешения имен участвуют DNS-клиент и DNS-серверы. Системный компонент DNS-клиента, называемый DNS-распознавателем, отправляет запросы на DNS-серверы. Запросы бывают двух видов:

– итеративные – DNS-клиент обращается к DNS-серверу с просьбой разрешить имя без обращения к другим DNS-серверам;

– рекурсивные – DNS-клиент перекладывает всю работу по разрешению имени на DNS-сервер. Если запрашиваемое имя отсутствует в базе данных и в кэше сервера, он отправляет итеративные запросы на другие DNS-серверы.

В основном DNS-клиентами используются рекурсивные запросы. На рис. 3 проиллюстрирован процесс разрешения доменного имени с помощью рекурсивного запроса.

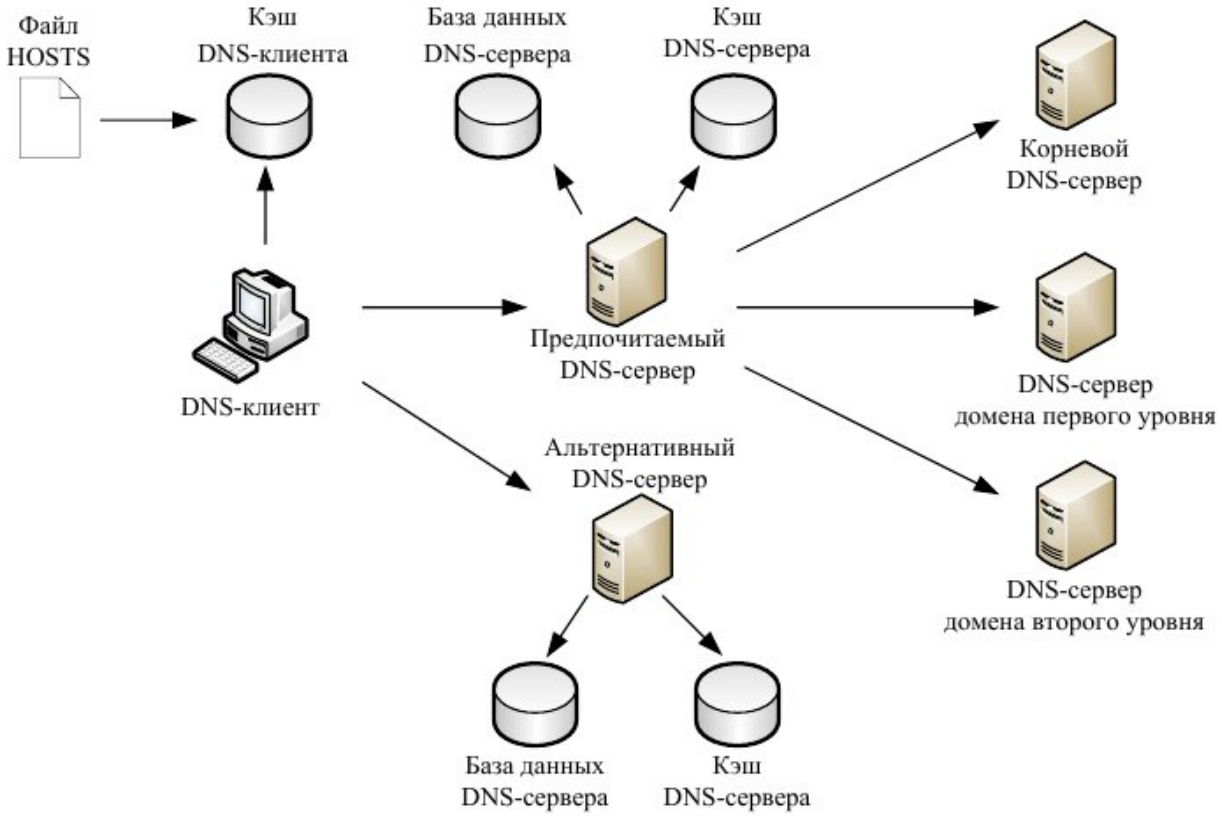

Рис. 3. Процесс обработки рекурсивного DNS-запроса

Сначала DNS-клиент осуществляет поиск в собственном локальном кэше DNS-имен. Это память для временного хранения ранее разрешенных запросов. В эту же память переносится содержимое файла HOSTS (каталог windows/system32/drivers/etc). Утилита IPconfig с ключом /displaydns отображает содержимое DNS-кэша. Если кэш не содержит требуемой информации, DNS-клиент обращается с рекурсивным запросом к предпочитаемому DNS-серверу (Preferred DNS server), адрес которого указывается при настройке стека TCP/IP. DNS-сервер просматривает собственную базу данных, а также кэш-память, в которой хранятся ответы на предыдущие запросы, отсутствующие в базе данных. В том случае, если запрашиваемое доменное имя не найдено, DNS-сервер осуществляет итеративные запросы к DNS-серверам верхних уровней, начиная с корневого DNS-сервера.

Рассмотрим процесс разрешения доменного имени на примере. Пусть, требуется разрешить имя www.microsoft.com. Корневой домен содержит информацию о DNS-сервере, содержащем зону .com. Следующий запрос происходит к этому серверу, на котором хранятся данные о всех поддоменах зоны .com, в том числе о домене microsoft и его DNS-сервере. Сервер зоны microsoft.com может непосредственно разрешить имя www.microsoft.com в IP-адрес.

Иногда оказывается, что предпочитаемый DNS-сервер недоступен. Тогда происходит запрос по той же схеме к альтернативному DNS-серверу, если, конечно, при настройке стека TCP/IP был указан его адрес.

Записи о ресурсах

База данных DNS-сервера содержит записи о ресурсах (resource record), в которых содержится информация, необходимая для разрешения доменных имен и правильного функционирования службы DNS. Существует более 20 типов записей о ресурсах, приведем самые важные:

- A (Host Address – адрес хоста) – основная запись, используемая для непосредственного преобразования доменного имени в IP-адрес;
- CNAME (Canonical Name – псевдоним) – запись определяет псевдоним хоста и позволяет обращаться по разным именам (псевдонимам) к одному и тому же IP-адресу;
- MX (Mail Exchanger – почтовый обменник) – запись для установления соответствия имени почтового сервера IP-адресу;
- NS (Name Server – сервер имен) – запись для установления соответствия имени DNS-сервера IP-адресу;
- PTR (Pointer – указатель) – запись для обратного преобразования IP-адреса в доменное имя;
- SOA (Start Of Authority – начало авторизации) – запись для определения DNS-сервера, который хранит основную копию зоны;
- SRV (Service Locator – определитель служб) – запись для определения серверов некоторых служб (например, POP3, SMTP, LDAP).

Разрешенные символы

Изначально имена узлов Интернета ограничивались использованием набора символов, указанного в документах RFC 952 и 1123 (unicode). Эти ограничения позволяли использовать в именах:

- прописные и строчные буквы латинского алфавита (A-Z, a-z),
- цифры (0-9),
- дефисы (-).

Кроме того, первым символом в имени DNS могла быть цифра, а имена должны были кодироваться и представляться с помощью набора символов ASCII США.

Эти требования поддерживались, когда система DNS была введена как часть документа RFC 1035, содержащего одну из основных спецификаций стандартов DNS. Для использования DNS в международных параметрах настройки эти требования накладывали существенные ограничения в тех случаях, когда в местных стандартах именования разрешалось использовать расширенные наборы символов.

Для снятия таких ограничений корпорация Майкрософт расширила поддержку символов в DNS за рамки спецификации RFC 1035. Служба DNS теперь по умолчанию обеспечивает поддержку расширенного набора символов формата UTF-8 (Unicode transformation format).

2. Имена NetBIOS и служба WINS

Протокол NetBIOS (Network Basic Input Output System – сетевая базовая система ввода-вывода) был разработан в 1984 году для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. В операционных системах Microsoft Windows NT, а также в Windows 98, протокол и имена NetBIOS являлись основными сетевыми компонентами. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в связи с чем фундаментом сетевых решений стали протоколы TCP/IP и доменные имена.

Пространство имен NetBIOS

Имена NetBIOS не образуют никакой иерархии в своем пространстве, это простой линейный список имен компьютеров, точнее работающих на компьютере служб. Имена компьютеров состоят из 15 видимых символов плюс 16-й служебный символ. Если видимых символов меньше 15, то оставшиеся символы заполняются нулями (не символ нуля, а байт, состоящий из двоичных нулей). 16-й символ соответствует службе, работающей на компьютере с данным именем.

Просмотреть список имен пространства NetBIOS, которые имеются на данном компьютере, можно с помощью команды «*nbtstat –n*».

На рисунке 4 изображен вывод команды «*nbtstat –n*» на сервере *dc1.world.ru*, являющийся списком NetBIOS-имен, сгенерированных данным сервером.

```
C:\nbtstat -n

Подключение по локальной сети:
Адрес IP узла: [192.168.0.1] Код области: []

                Локальная таблица NetBIOS-имен

      Имя                 Тип          Состояние
    ---------------------------------------------------
    DC1            <00>  Уникальный  Зарегистрирован
    WORLD          <00>  Группа      Зарегистрирован
    WORLD          <1C>  Группа      Зарегистрирован
    DC1            <20>  Уникальный  Зарегистрирован
    WORLD          <1B>  Уникальный  Зарегистрирован
    WORLD          <1E>  Группа      Зарегистрирован
    WORLD          <1D>  Уникальный  Зарегистрирован
    ..__MSBROWSE__.<01>  Группа      Зарегистрирован
```

Рис. 4. Пример списка имен NetBios

В угловых скобках указан шестнадцатиричный код 16-го служебного символа какого-либо имени. Например, имя *DC1* и 16-й символ «*00*»

соответствуют службе «*Рабочая станция*», которая выполняет роль *клиента* при подключении к ресурсам файлов и печати, предоставляемых *другими компьютерами* сети. А то же имя *DC1* и символ с кодом «*20*» соответствуют службе «*Сервер*», которая предоставляет *ресурсы файлов и печати данного сервера* для других компьютеров сети. Имя *WORLD* соответствует либо NetBIOS-имени домена *world.ru* (вспомните установку *первого* контроллера домена), либо имени т.н. сетевой *рабочей группы*, отображаемой в *Сетевом окружении* любого Windows-компьютера.

Имя «..__*MSBROWSE*__.» говорит о том, что данный компьютер является *Обозревателем сетевого окружения* по протоколу TCP/IP. Т.е. если на каком-либо компьютере с системой Windows открыть «*Сетевое окружение*», то данный компьютер будет запрашивать *список компьютеров*, сгруппированных в сетевой рабочей группе WORLD, именно с сервера DC1.

Все эти имена, перечисленные в данной табдице, будут автоматически регистрироваться в базе данных сервера WINS после того, как данный сервер будет установлен в сети и данный компьютер станет клиентом сервера WINS.

Процесс разрешения имен в пространстве NetBIOS

Когда один компьютер пытается использовать ресурсы, предоставляемые другим компьютером через интерфейс NetBIOS поверх протокола TCP/IP, то первый компьютер, называемый клиентом, вначале должен определить IP-адрес второго компьютера, называемого сервером, по имени этого компьютера. Это может быть сделано одним из трех способов:

- широковещательный запрос;
- обращение к локальной базе данных NetBIOS-имен, хранящейся в файле *LMHOSTS* (этот файл хранится в той же папке, что и файл *hosts*, отображающий FQDN-имена);
- обращение к централизованной БД имен NetBIOS, хранящейся на сервере WINS (Windows Internet Naming Service (служба имен в Интернете для Windows)).

В зависимости от *типа* узла NetBIOS, разрешение имен осуществляется с помощью различных комбинаций перечисленных способов:

- **b-узел** (*broadcast node*, *широковещательный узел*) — разрешает имена в IP-адреса посредством широковещательных сообщений (компьютер, которому нужно разрешить имя, рассылает по локальной сети широковещательное сообщение с запросом IP-адреса по имени компьютера);
- **p-узел** (*peer node*, *узел «точка — точка»*) — разрешает имена в IP-адреса с помощью WINS-сервера (когда клиенту нужно разрешить имя компьютера в IP-адрес, клиент отправляет серверу имя, а тот в ответ посылает адрес);
- **m-узел** (*mixed node*, *смешанный узел*) — комбинирует запросы b- и p-узла (WINS-клиент смешанного типа сначала пытается применить широковещательный запрос, а в случае неудачи обращается к WlNS-серверу;

поскольку разрешение имени начинается с широковещательного запроса, m-узел загружает сеть широковещательным трафиком в той же степени, что и b-узел);

h-узел (*hybrid node*, *гибридный узел*) — также комбинирует запросы b-узла и p-узла, но при этом сначала используется запрос к WINS-серверу и лишь в случае неудачи начинается рассылка широковещательного сообщения, поэтому в большинстве сетей h-узлы работают быстрее и меньше засоряют сеть широковещательными пакетами.

С точки зрения производительности, объема сетевого трафика и надежности процесса разрешения NetBIOS-имен самым эффективным является *h-узел*.

Если в свойствах протокола TCP/IP Windows-компьютера нет ссылки на WINS-сервер, то данный компьютер является b-узлом. Если в свойствах протокола TCP/IP имеется ссылка хотя бы на один WINS-сервер, то данный компьютер является h-узлом. Другие типы узлов настраиваются через реестр системы Windows.

Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

Репликация WINS-серверов

В больших сетях для распределения нагрузки по регистрации и разрешению NetBIOS-имен необходимо использовать несколько серверов WINS (рекомендации Microsoft — один WINS-сервер на каждые 10000 сетевых узлов). При этом одна часть клиентов будет настроена на регистрацию и обращение для разрешения имен на один WINS-сервер, другая часть — на второй сервер и т.д. Для того, чтобы все серверы WINS имели полную информацию *обо всех* имеющихся в корпоративной сети NetBIOS-узлах, необходимо настроить репликацию баз данных серверов WINS между собой. После завершения репликации каждый сервер WINS будет иметь полный список NetBIOS-узлов всей сети. И любой клиент, регистрируясь на «ближайшем» к нему WINS-сервере, при этом может послать запрос «своему» серверу на разрешение имен NetBIOS-узлов, зарегистрированных не только на данном WINS-сервере, но и на всех остальных серверах WINS.