Администрирование локальных сетей

Лекция 6.

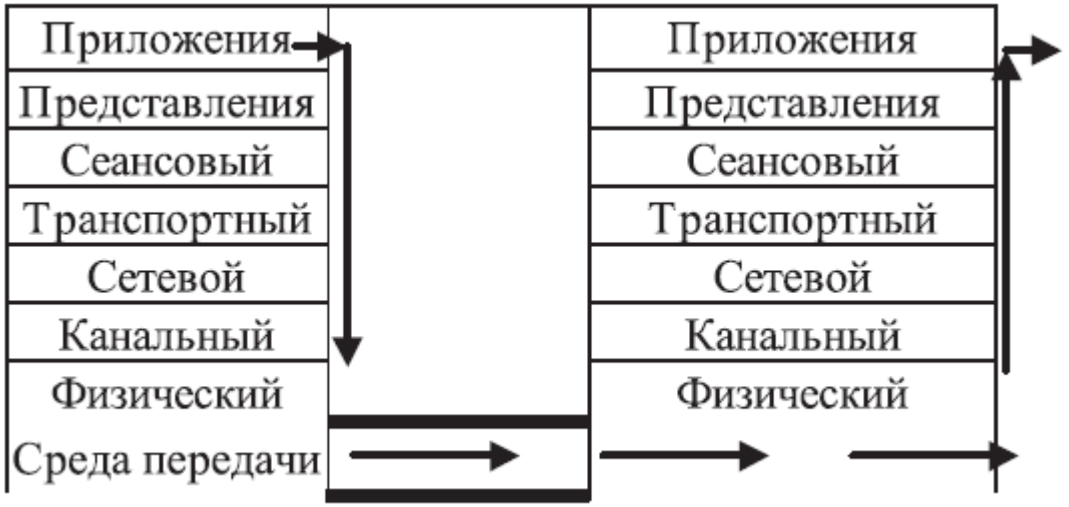
Управление доступом к сети

Основные вопросы лекции

- Сетевые подключения. Управление сетевыми подключениями.
- Динамическая адресация. Протокол DHCP. Сервисы DHCP.
- Службы имен. Система доменных имен (DNS), настройка сетевых узлов на ее использование.
- Система имен Windows. NetBIOS-имена сетевых узлов. Протокол NetBIOS, его особенности. Именование компьютеров в локальных сетях Windows.
- Обеспечение проверки подлинности в локальных сетях.
- Сервисы управления доступом.
- Ролевая модель управления доступом. Примеры реализации моделей управления доступом.

Сетевые подключения

- Для обеспечения передачи данных в сети необходимо подключение к телекоммуникационному каналу передачи данных.
- **Сетевым интерфейсом** называется физическое или виртуальное (программно эмулируемое) устройство, которое способно выполнять функции приема пакетов данных от других подобных устройств и передачи им пакетов данных. Характерным примером сетевого интерфейса являются сетевые адаптеры (сетевые карты) и модемы.
- В протоколах канального уровня, предполагающих связь нескольких сетевых интерфейсов, определяются адреса каждого из интерфейсов.
- Согласно протоколу Ethernet, каждый сетевой интерфейс должен иметь уникальный MAC-адрес, по которому можно отправить пакет.
- При использовании протокола IP каждый интерфейс идентифицируется уникальным IP-адресом.

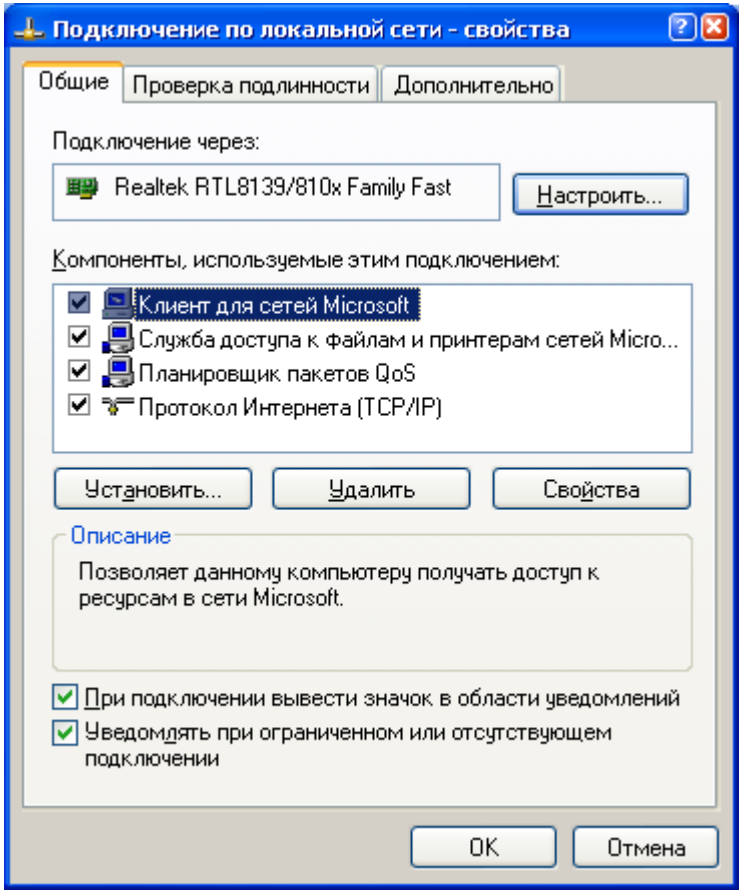


Управление сетевыми подключениями

- Каждый сетевой интерфейс, осуществляющий прием и передачу пакетов по протоколу IP, должен иметь уникальный сетевой адрес.
  - Под уникальным здесь понимается такой адрес, который в пределах данной IP-сети не принадлежит ни одному другому сетевому интерфейсу.
  - Один интерфейс может иметь несколько IP-адресов, но один и тот же IP-адрес не может принадлежать разным сетевым интерфейсам.
- IP-адреса объединены в блоки, которые называются сетями.
- Блоки адресов (сети) классифицированы по классам сетей, которые отличаются друг от друга особенностями маршрутизации.

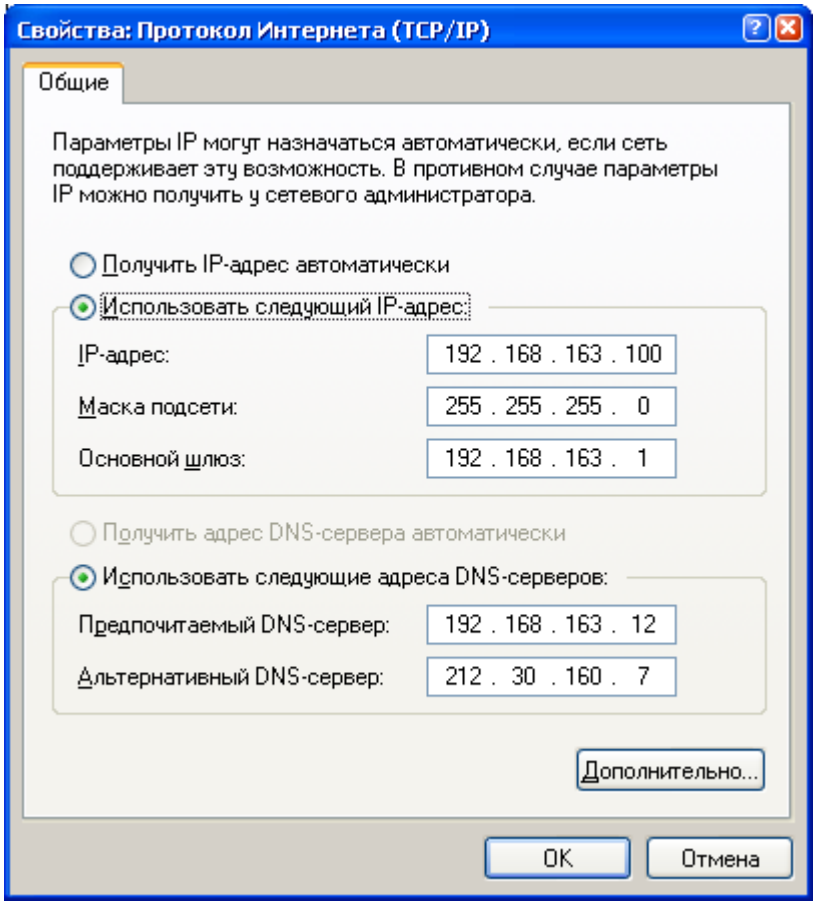
Настройка интерфейса

- Настройка подключения компьютера под управлением MS Windows включает в себя:
  - Конфигурирование сетевых компонентов



Установка статического IP адреса

- Настройку параметров протокола TCP/IP
- Назначение IP-адресов серверам DNS и WINS (для их задания используется окно, вызываемое с помощью кнопки **Дополнительно**.



Протокол DHCP

- **DHCP** (*Dynamic Host Configuration Protocol*) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.
- Протокол работает по модели «клиент-сервер».
- Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к *серверу DHCP*, и получает от него нужные параметры.
- Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров.

Распределение IP-адресов

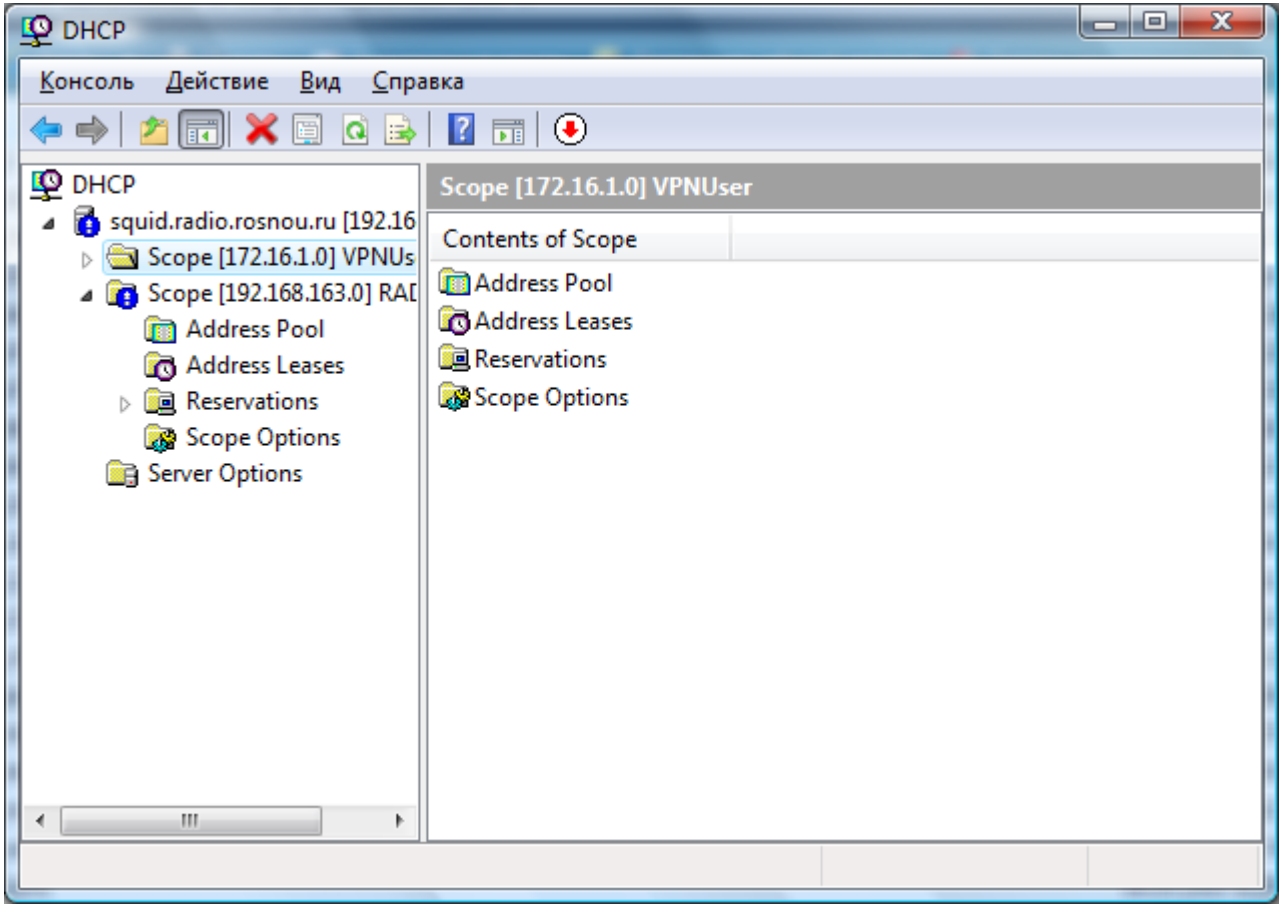
Протокол DHCP предоставляет три способа распределения IP-адресов:

- *Ручное распределение.* При этом способе сетевой администратор сопоставляет аппаратному адресу (обычно MAC-адресу) каждого клиентского компьютера определённый IP-адрес.
- *Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- *Динамическое распределение.* Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется *арендой адреса*. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый.

Процесс получения IP-адреса

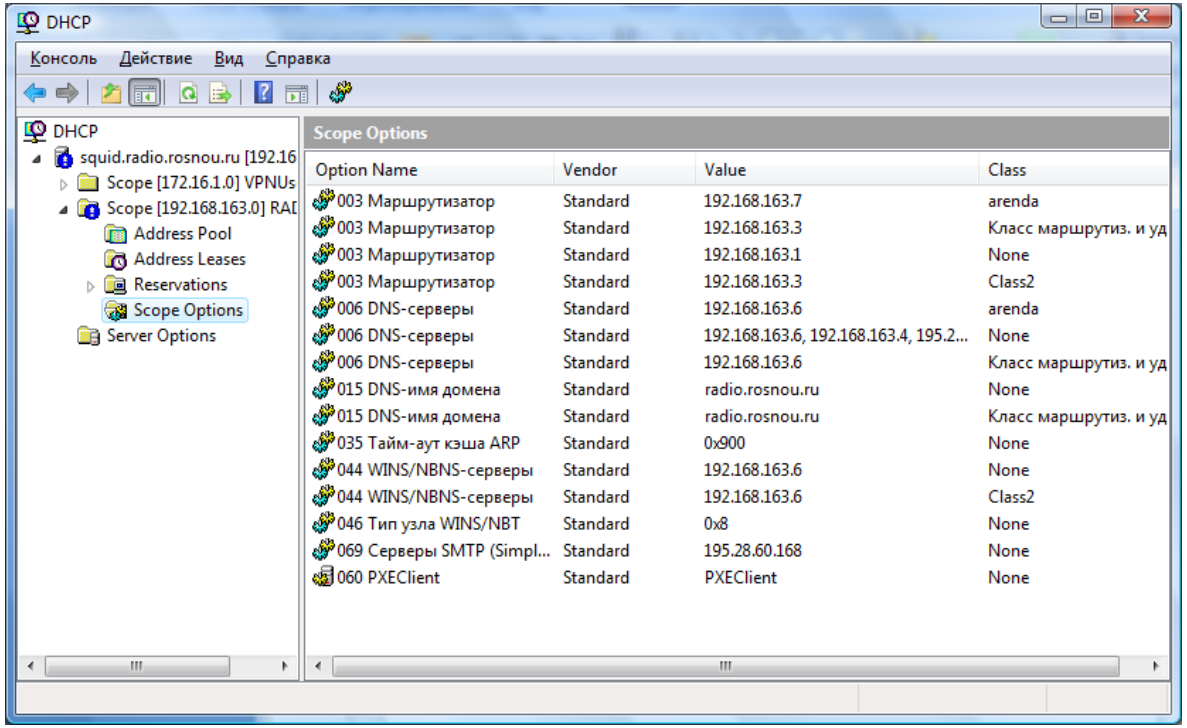
- Процесс получения сетевого адреса представляет собой обмен серией запросов и ответов между DHCP-клиентом и DHCP-сервером.

Управление DHCP сервером

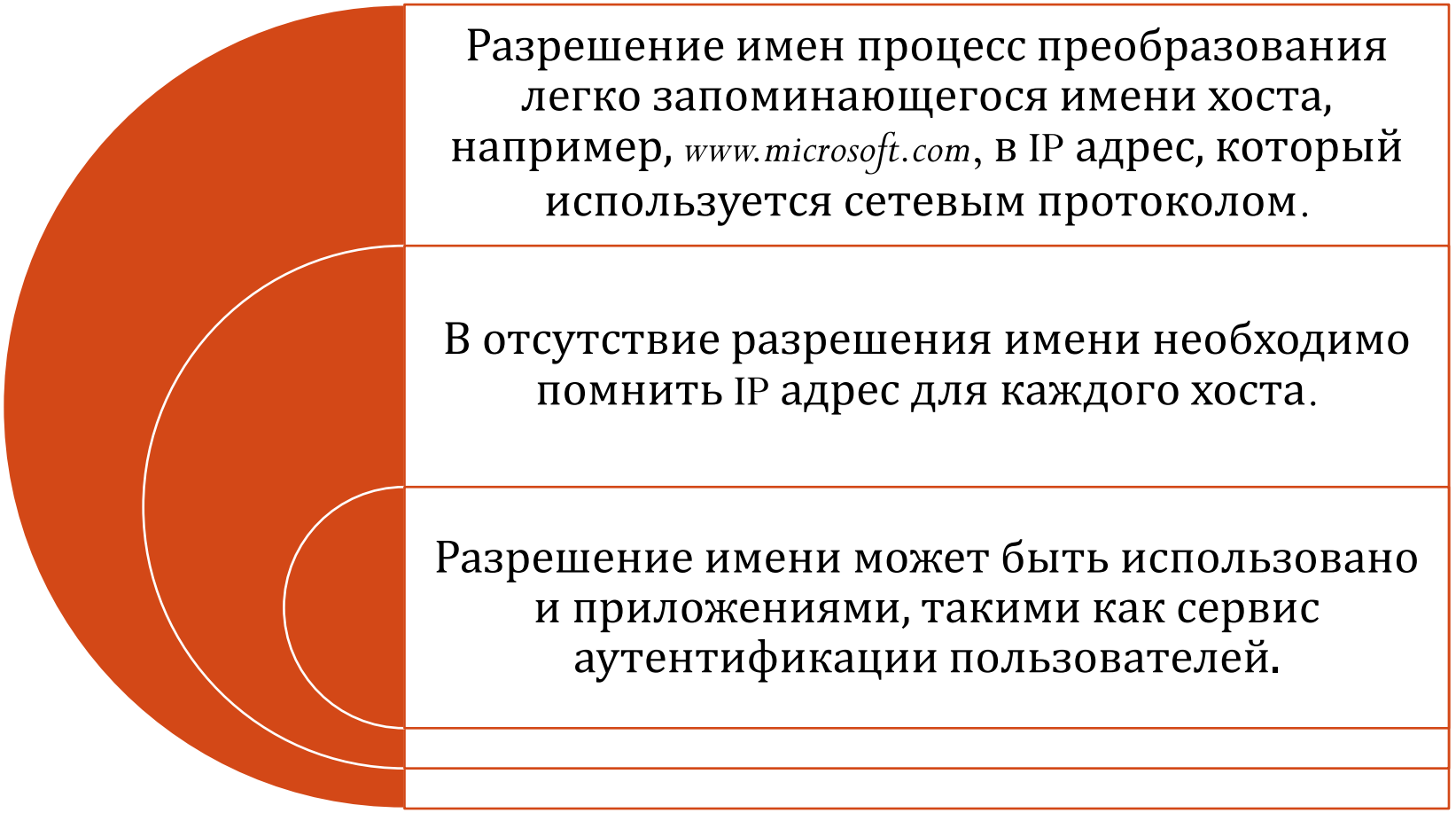


Параметры области

- При настройке сервера может быть задан ряд параметров настройки сетевого интерфейса
  - Маршрутизатор по умолчанию
  - Серверы DNS, WINS
  - Параметры таблицы ARP
  - Тип узда NBT и т.д.



Что такое разрешение имен?



Какие типы имен могут быть использованы для разрешения?

- Имена Системы доменных имен (DNS)
- Имена Network Basic Input/Output System (NetBIOS)

Что собой представляет имя хоста?

- Дружественное для пользователя имя для идентификации хоста в сетях TCP/IP
- Может быть присвоено серверу, принтеру, клиентскому компьютеру или другому устройству, которое присоединено к сети
- Должно быть уникально в пределах домена, но может повторяться в других доменах

Разрешение имени через файл hosts

Имена хостов могут быть разрешены через текстовый файл hosts.

В ОС Windows Server, файл hosts размещается в папке *%systemroot%*\system32\drivers\etc folder.

Изменения в файл могут быть внесены текстовыми редакторами, например Notepad, Edit, or WordPad.

Файл HOSTS

На начальном этапе развития Интернет для сопоставления имен компьютеров и их адресов использовался файл hosts, хранимый на одном из компьютеров в сети и при необходимости копируемый на пользовательские машины.

С ростом сети перед такой системой возникают проблемы:

- Файл становится слишком велик, чтобы им можно было эффективно управлять;
- Трафик разрешения имен загружает сервер и этот файл нельзя копировать достаточно часто, чтобы его содержимое было всегда актуально;
- Для файла hosts использовалась линейная структура данных, поэтому у каждого компьютера в сети должно быть уникальное имя.

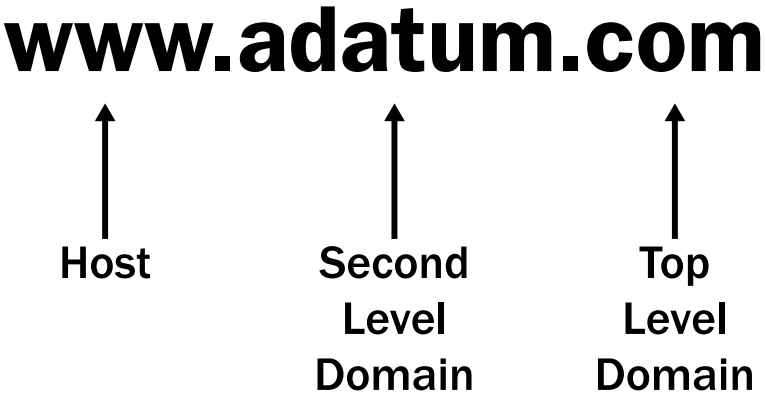
Службы имен

- Доменная система именования (Domain Name System) – способ сопоставления имен компьютеров с IP-адресами в распределенной БД.
- Компьютеры (хосты) в сетях TCP/IP идентифицируются уникальными IP-адресами.
- Кроме того, компьютеру в сети присваивается некоторое имя, например, mailserver.
- **Разрешение имен** – получение IP-адреса по его имени.
  - Когда пользователь или приложение ищет компьютер по имени хоста, выдается запрос к службе разрешения имен.

Службы доменных имен

- Используется несколько служб разрешения имен:
  - **Файлы hosts** – файлы статического сопоставления имен хостов и ip-адресов;
  - **Файлы lmhosts** – файлы статического сопоставления NetBIOS-имен и ip-адресов.
  - **DNS (Domain Name System)** – стандартная служба разрешения имен в Интернет, также используется в качестве службы разрешения имен в сетях Windows 2000, Windows Server 2003.
  - **WINS (Windows Internet Naming Service)** – служба, которая отслуживает NetBIOS-имена и ip-адреса, используя базу данных.

Структура DNS имени



Пространство доменных имен

- **Пространство имен** – определенная сфера, в которой имена схожих компонентов должны быть уникальны, но структурированы схожим образом.
- Пространство имен организовано в иерархию – начиная от корневого домена до имени хостов.
- Корневой домен – единственный домен, самый верхний в иерархии DNS, обозначается точкой (.)

Домены верхнего уровня

- Домены верхнего уровня контролируются Internet Activities Board, организации отвечающих за выдачу имен доменов. Наиболее часто используемые имена доменов верхнего уровня:
  - com – коммерческие организации
  - edu – образовательные учреждения
  - org – некоммерческие организации
  - net – провайдеры сетевых сервисов
  - xx – двухбуквенные коды стран (ru, fr, de, by и т.д.)
  - info – доступно для любых применений
  - name – используется для персональных сайтов
  - arpa – используется для обратного просмотра DNS

Домены второго уровня

- Сразу под доменами верхнего уровня располагается второй уровень доменов, регистрируемый индивидуальными организациями.
- После регистрации домена второго уровня, управление пространством имен в этом домене передается самой организации.
- Для удобства организация может разбить это пространство на домены третьего уровня (поддомены).
- Полное доменное имя (fully qualified domain name, FQDN) – исчерпывающее описание местоположения хоста в иерархии DNS.

Зона и серверы имен

- Пространство имен делится на зоны.
- **Зона –** файл, представляющий неразрывную часть пространства имен, за которую отвечает конкретный сервер.
  - Зоне соответствует набор записей ресурсов, хранящихся на DNS-сервере, которые сопоставляют IP-адреса с хостами и службами в данной зоне.
  - Зона охватывает минимум один домен, который считается корневым доменом зоны. Зона может включать поддомены этого корневого домена, но не обязательно охватывать их все.
  - В каждой зоне должен быть как минимум один сервер имен.
- Каждому серверу имен известен адрес хотя бы одного родительского сервера имен.
- Если сервер не может разрешить некоторое хост-имя, он отправляет запрос на другой сервер.

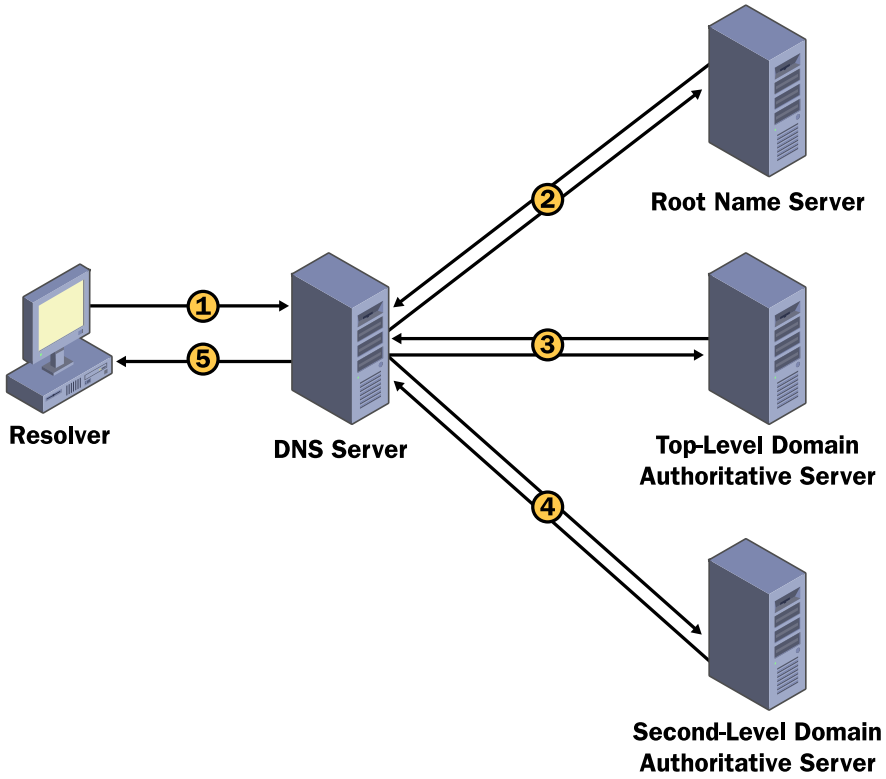
Типы зон в Windows

Windows Server поддерживает три типа зон:

- **Интегрированная зона Active Directory** – в зоне данного типа БД DNS хранится в Active Directory. Все DNS-серверы в зоне интегрированной в AD, считаются основными.
- **Основная зона** – мастер-копия БД DNS, размещаемая в стандартном текстовом ASCII файле. Напрямую можно изменять только информацию основной зоны.
- **Дополнительная зона** – информация представляет собой копию данных (только для чтения) существующей основой зоны. Эти сведения обновляются только на основном DNS-сервере, а затем передаются на все дополнительные серверы.

Процесс разрешения имен

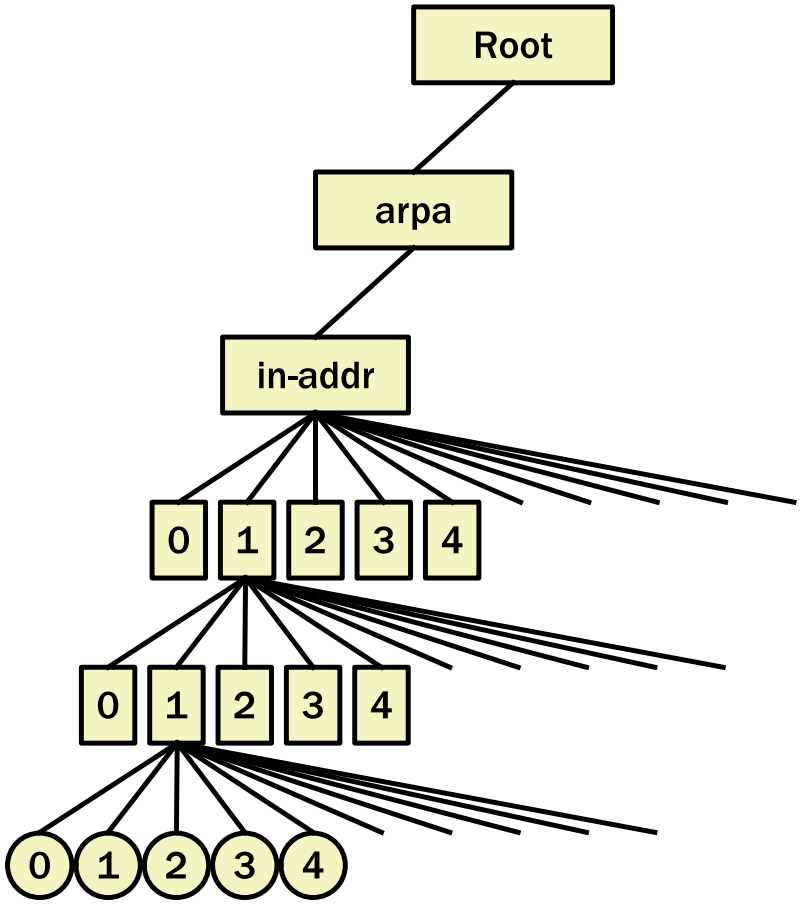
- **Разрешение имен –** определение ip-адреса, сопоставленного с этим именем.
- В DNS клиент, выполняющий разрешение имен, называется интерпретатором (resolver).
- Интерпретатор работает на прикладном уровне модели TCP/IP.



Запросы обратного просмотра

- При таком запросе ip-адрес разрешается в доменное или хост-имя.
- Поскольку база данных DNS индексируется по именам, а не ip-адресам, поиск на основе ip-адреса может оказаться длительным процессом.
- Для решения проблемы в корневом домене создается специальный домен in-addr.arpa, который использует ip-адреса в качестве индекса.
- Поскольку в ip-адресах детализация нарастает слева направо, а вдоменных именах – справа налево, порядок октетов ip-адреса при формировании соответствующего имени в домене in-addr.arpa меняется на обратный.
  - Например хост-имя для ip-адреса 192.168.160.115 , будет записью PTR для файла зоны 160.168.192.in-addr.arpa. Этот элемент будет выглядеть:
    - 115 IN PTR имя_хоста

Процесс обратного разрешения имени



Записи ресурсов

- Зонные файлы состоят из записей ресурсов. В таблице перечислены примеры записей ресурсов зоны.

Запись ресурса	Применение
A	Запись адреса, сопоставляющая хост-имя с ip-адресом
AAAA	Запись адреса для протокола IPv6
CNAME	Запись канонического имени для создания псевдонима
MX	Запись почтового сервера, идентифицирует почтовый сервер для домена
NS	Запись сервера имен, идентифицирует сервер имен для конкретного DNS-домена
PTR	Запись указателя сопоставляет ip-адрес с хостом в зоне обратного именования
SOA	Начальная запись зоны (Start of Authority), указывает домен, за который отвечает DNS-сервер
SRV	Запись службы позволяет указывать, какие службы предоставляет домен
WINS	Запись WINS идентифицирует WINS-сервер
WINS_R	Запись обратного просмотра WINS заставляет DNS использовать команду nbtstat для выполнения клиентских запросов на обратный просмотр
WKS	Запись общеизвестных сервисов

DNS и Active Directory

- DNS – служба локатора, используемая Active Directory.
  - AD делает свои службы доступными в сети, публикуя их в DNS.
- При установке контроллера домена он использует динамические обновления для регистрации своих служб в DNS как записей SRV.
  - После этого клиенты могут находить службы через простые DNS – запросы.

Анализ существующей реализации DNS

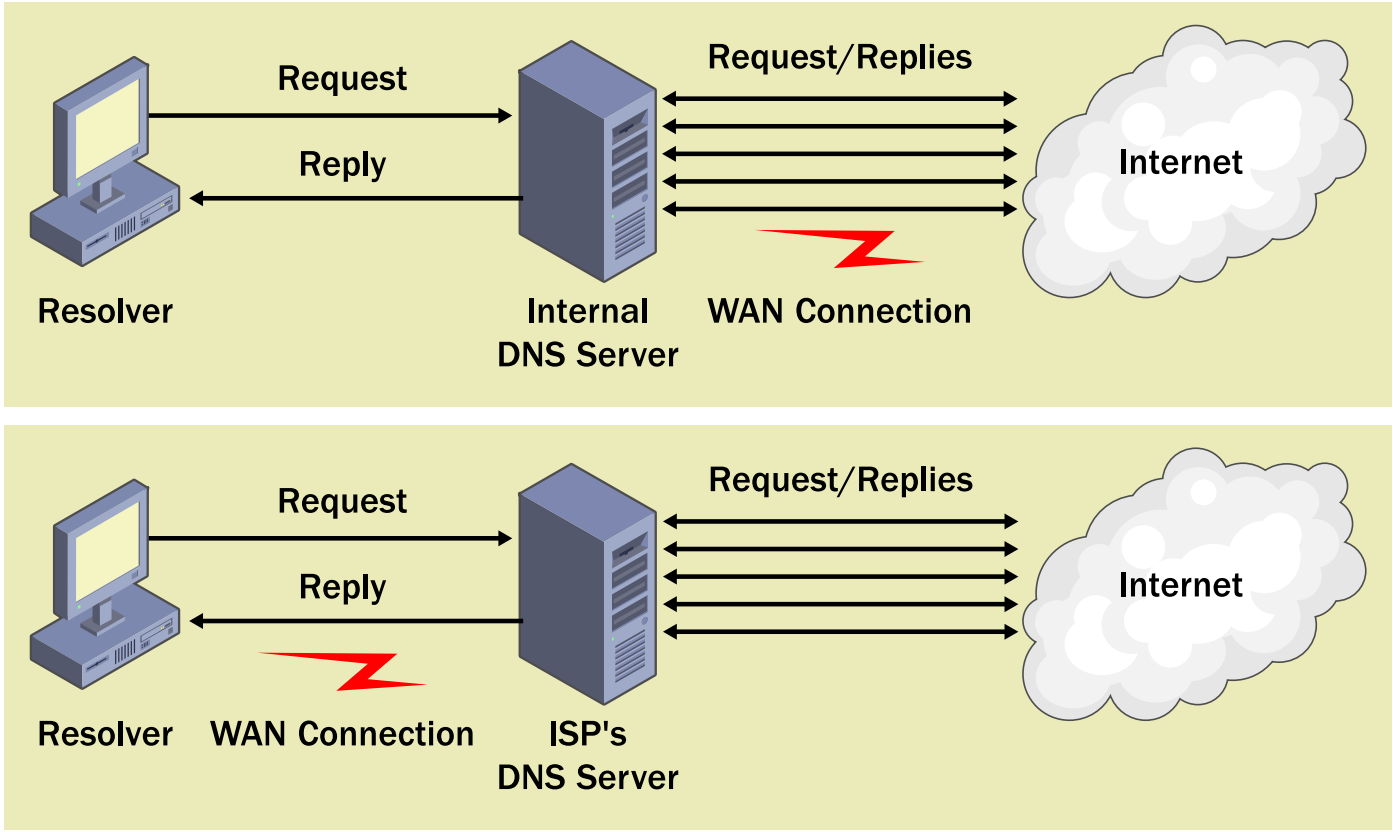
- Для анализа существующей структуры необходимо определить:
  - Существующие зоны DNS, обслуживающие их сервера и типы зон на серверах (основные, дополнительные, зоны-заглушки);
  - Зонные передачи:
    - Добавочная передача зоны – серверы отслеживают и передают только измененные записи ресурсов зоны;
    - Полная передача зоны – передается зона на дополнительный сервер целиком;
    - Быстрая передача зоны – передача в одном сообщении несколько записей ресурсов.

Ход анализа

При первоначальном анализе существующей инфраструктуры необходимо ответить на следующие вопросы:

- Использует ли организация одно и тоже пространство имен в Active Directory и в качестве внешнего пространства имен DNS?
- Какие зоны используются: интегрированные или обычные?
- Какие способы передачи или репликации применяются?
- Сколько DNS-серверов имеется в компании и какова их роль?
- Защищены ли DNS серверы?
- Сколько пользователей в каждом сегменте сети?

Комбинирование сервисов DNS



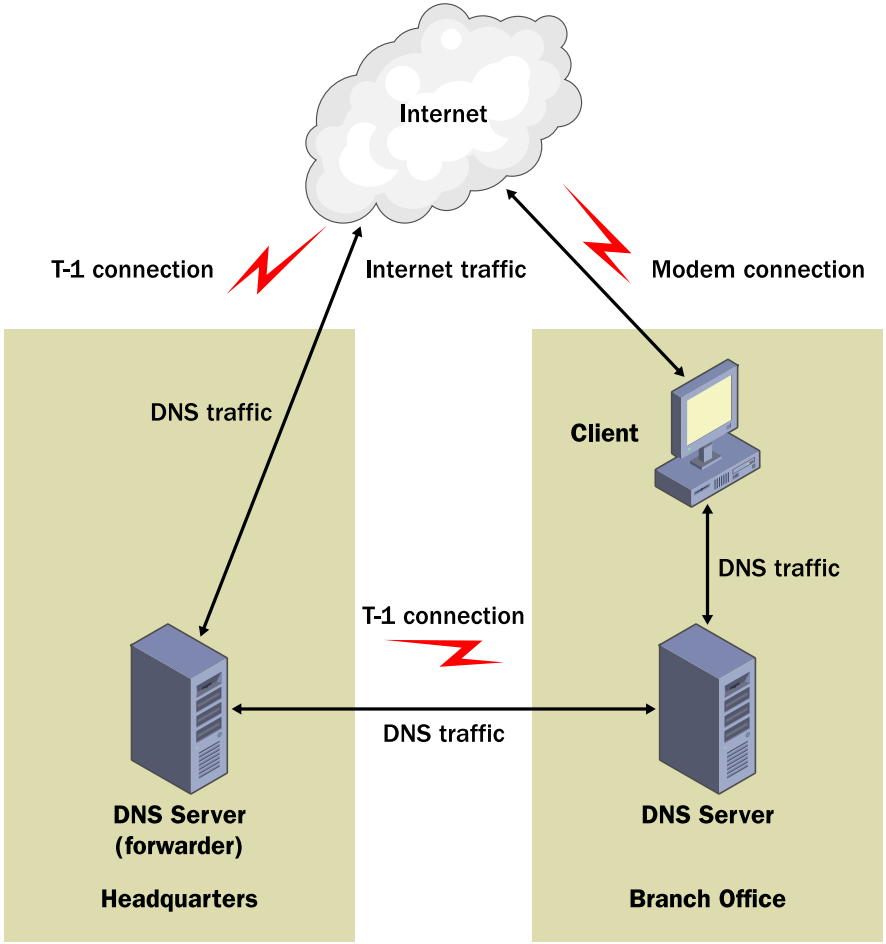
Дополнительные типы DNS серверов

- В дополнение к стандартным типам DNS серверов, также существуют:
  - Кэширующий сервер (Caching-only servers)
  - Сервер пересылки (Forwarders)

Использование кэширующего сервера

- Кэширующий сервер не содержит записей зон и записей узлов доменов.
- Сервер пересылает поступающие запросы к другим DNS серверам.
- Сервер кэшируют результаты полученных запросов для ускорения обработки повторных запросов.

Использование пересылки



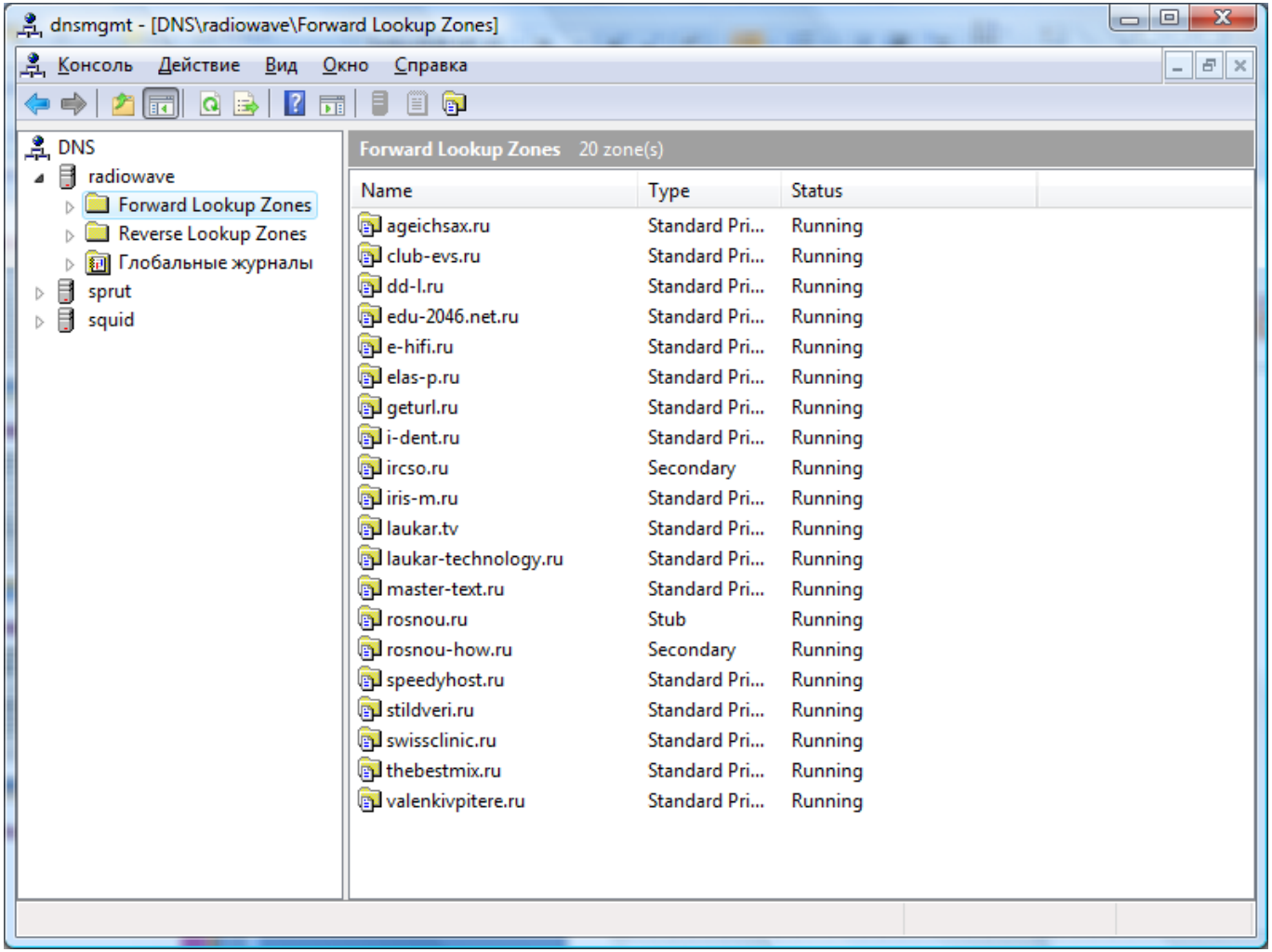
Угрозы безопасности DNS

- **Получение отпечатка** (Footprinting) — это процесс получения злоумышленником данных зоны DNS, позволяющий ему узнать доменные имена DNS, имена и IP-адреса компьютеров с важными сетевыми ресурсами.
  - Как правило, злоумышленник начинает атаку с применения этих данных DNS для составления, или получения отпечатка, схемы сети. Имена доменов DNS и компьютеров обычно отражают функции или местоположение домена или компьютера, что должно облегчить пользователям запоминание и распознавание доменов и компьютеров. Злоумышленник пользуется этим принципом DNS для изучения функций и местоположения доменов и компьютеров в сети.
- **Атака типа «отказ в обслуживании»** состоит в том, что злоумышленник пытается нарушить работу сетевых служб, «завалив» один или несколько DNS-серверов сети рекурсивными запросами.
  - Поскольку DNS-сервер занят исключительно обработкой этих запросов, загрузка его центрального процессора в конечном счете достигает максимума, и служба «DNS-сервер» становится недоступной. В сети нет работоспособного DNS-сервера, сетевые службы, использующие DNS, становятся недоступными для пользователей сети.

Угрозы безопасности DNS

- **Изменение данных** — это попытка злоумышленника (получившего отпечаток сети с помощью DNS) использовать действительные IP-адреса в созданных им IP-пакетах, тем самым придавая этим пакетам такой вид, словно они посланы с действительных IP-адресов в сети.
  - Такие действия называются подменой IP-адреса (IP spoofing). Имея действительный IP-адрес (IP-адрес, лежащий в пределах диапазона IP-адресов подсети), злоумышленник может получить доступ к сети и разрушить данные или провести атаки какого-либо другого типа.
- **Перенаправление** имеет место, когда злоумышленнику удалось перенаправить запросы имен DNS на серверы, находящиеся под его контролем. Один из способов перенаправления включает в себя попытку засорить кэш DNS-сервера ошибочными данными DNS, которые могут привести к перенаправлению запросов на серверы, находящиеся под контролем злоумышленника.
  - Если первоначально был сделан запрос на example.microsoft.com, а в ссылочном ответе имеется запись для имени, находящегося вне домена microsoft.com, например malicious-user.com, то DNS-сервер будет использовать кэшированные данные malicious-user.com для разрешения запроса этого имени.

Управление DNS сервером



Имена NetBIOS

- **NetBIOS –** это программный интерфейс, который использовался на протяжении многих лет для предоставления возможностей сетевого обмена приложениям.
  - Некоторые возможности исходной архитектуры Windows NT, встроенные в Windows Server 2003, полностью основывались на системе именования NetBIOS для именования других компьютеров в сети.
- **Имя NetBIOS** содержит до 16 символов, последний из которых регистрируется в Windows для идентификации конкретных функций определенных компьютеров, например, контроллеров домена или браузеров.
  - Если включена служба NetBIOS, то каждому компьютеру операционной системой присваивается имя NetBIOS.
  - Это имя может совпадать или не совпадать с именем входа пользователя или хост-именем компьютера.

Стандарт NetBT

- Поскольку NetBIOS запускается поверх интерфейса Transport Device Interface (TDI), она может теоретически использовать любые совместимые протоколы для своих нужд низкоуровневого взаимодействия.
  - Первоначально операционные системы, предшествовавшие Windows 2000, использовали для трафика NetBIOS интерфейс NetBEUI (NetBIOS Extended Use Interface). Однако NetBEUI не является маршрутизируемым и при использовании TCP/IP определен способ, посредством которого можно было бы предоставлять услуги NetBIOS.
  - Этот стандарт получил название NetBIOS over TCP/IP, или **NetBT**.
- Стандарт NetBT определяет два вида служб – службы **сеансов** и **дейтаграмм**.
  - Службы сеансов используют TCP для обеспечения полностью надежной ориентированной на соединения службы передачи сообщений
  - Службы дейтаграмм используют протокол UDP, который требует небольшого объема служебной информации и имеет не очень высокую надежность.

Типы узлов NetBT

- В стандарте NetBT определены несколько типов узлов, которые указывают, какие методы и в каком порядке должен использовать компьютер.
- Типы узлов присваиваются клиентам сервером DHCP или определяются параметрами TCP/IP, заданными в конфигурации клиента.
- В стандарте NetBT определяются следующие типы узлов:
  - **B-узел**. Клиент использует широковещательные сообщения в сети как для регистрации, так и для разрешения имен.
  - **P-узел**. Клиент направляет отдельное сообщение для регистрации или разрешения имени серверу имен NetBIOS.
  - **M-узел**. Клиент использует широковещательные сообщения для регистрации имен; для разрешения имен клиент использует сначала широковещательные сообщения, и если это не дает результата, то он направляет запросы серверу имен NetBIOS.
  - **H-узел**. Клиент направляет отдельное сообщение регистрации или разрешения имени серверу имен NetBIOS (NBNS); если NBNS недоступен, то клиент использует широковещательные сообщения, пока не будет восстановлено соединение с NBNS.

Служба WINS

- **WINS** (*Windows Internet Name Service*) — служба сопоставления NetBIOS-имен компьютеров с ip-адресами узлов.
- Сервер **WINS** осуществляет регистрацию имен, выполнение запросов и освобождение имен.
- При использовании NetBIOS поверх TCP/IP необходим WINS сервер для определения корректных IP адресов.
  - Использует 137 порт по TCP и UDP.

Разрешение имен NetBIOS

- Если включена система NetBIOS, то на всех компьютерах Windows поддерживается кэш имен NetBIOS, разрешение которых они уже выполняли.
  - Когда компьютеру требуется разрешение NetBIOS-имени, то сначала происходит обращение к кэшу.
  - Если это имя не найдено в кэше, то далее используется метод, определяемый типом узла данного компьютера.
- Клиент, не использующий WINS, отправляет широковещательные сообщения для разрешения имени, и в случае неудачного результата обращается к локальному файлу LMHOSTS.
- Клиент WINS может использовать для разрешения имен NetBIOS любой из имеющихся методов.
  - Сначала он использует кэш имен NetBIOS, затем обращается к серверу WINS.
  - Если сервер WINS не дает результата, то происходит рассылка широковещательных сообщений, и в случае неудачного результата происходит обращение к файлу LMHOSTS.

Кэш имен NetBIOS

- Во время каждого сетевого сеанса клиентский компьютер сохраняет в кэше памяти все имена NetBIOS, для которых было успешно выполнено разрешение, чтобы их можно было использовать повторно.
- Кэш хранится в памяти, его использование является самым быстрым и эффективным способом разрешения имен.
- Это первый ресурс, к которому обращаются узлы всех типов, когда им требуется разрешение какого-либо имени.
- Текущее содержимое кэша имен NetBIOS компьютера можно просмотреть с помощью команды:
  - **nbtstat –c**

Управление WINS сервером