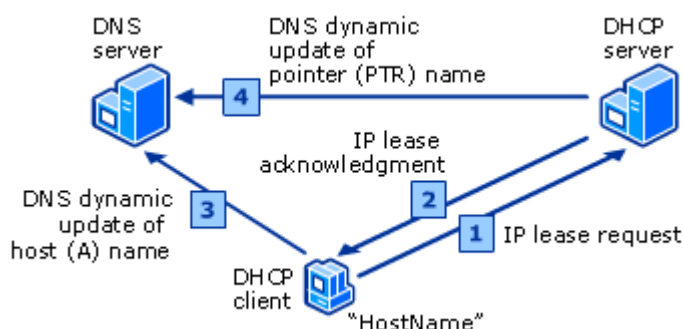


Тема занятия: Сетевые сервисы DNS и DHCP

По данной теме, вы можете посмотреть видео, перейдя по ссылке <https://www.youtube.com/watch?v=FQN8S1jHF0c>

Теоретическая часть

Сетевые сервисы относятся к ядру вашей сети, той основе, на которой все строится. По убеждениям автора это достаточно простые, однако, от этого не менее важные сервисы.



DHCP

DHCP – сервис, который позволяет устройству в сети динамически получать IP адрес и некоторые настройки сети от центрального сервера. Если Ваш компьютер настроен на динамическое получения IP адреса, то при загрузке он будет отправлять широковещательные запросы, в надежде, что ему ответит DHCP сервер. DHCP сервер даст ответ, тогда компьютер даст запрос на получение IP от этого сервера, предоставив ему свой мак-адрес. В ответ сервер выдаст IP или сообщит, что это невозможно.

DNS

DNS – сервис, разрешающий доменные имена в IP адреса. Например, при обращении к ресурсам Интернет в поле URL мы вбиваем читабельное имя google.com, а работа с ресурсом осуществляется с помощью IP. Перед тем, как обратиться к ресурсу компьютер-клиент обращается к DNS серверу, запрашивая IP адрес для определенного имени. Если в базе DNS сервера такое имя есть, он возвращает клиенту искомый IP адрес. Если имя не найдено, в большинстве случаев DNS сервер обратится к вышестоящему DNS серверу. И так до самой верхушки: 13 корневых DNS серверов, которые обеспечивают работу корневой зоны DNS в сети Интернет. Получение ответа происходит по цепочке в обратном направлении.

Службы DNS и DHCP могут быть установлены на различных серверах и сетевых устройствах. Начиная от домашних роутеров, и заканчивая

отдельными серверами, специально выделенными под эти задачи. При планировании сети важно правильно выбрать месторасположение и количество серверов, обеспечивающих надежную работу этих сервисов.

Например, для отказоустойчивости DHCP можно настроить несколько серверов, а для DNS помимо избыточности устанавливают внутренние и внешние DNS-сервера.

[Настройка DNS и DHCP серверов](#) может быть выполнена как ОС Windows так и Linux. В зависимости от выбранной платформы могут быть различные преимущества и особенности настройки. Например, в Windows 2012 появилась возможность поднять службу DHCP в отказоустойчивом режиме и использовать безопасные подключения для DNS. Для того, чтобы установить сетевые службы DNS и DHCP на серверах Windows необходимо поднять соответствующие роли. Дальнейшая настройка зависит от параметров вашей сети.

Работа [ActiveDirectory](#) тесно связана с сервисом DNS. Установить службы DNS можно в процессе поднятия роли ADDS, таким образом, установка DNS сервера будет произведена на контроллере домена. DHCP, кстати также имеет интеграцию с доменом: доменная машина не получит IP от DHCP сервера, если он не активирован в AD.

Для установки DNS и DHCP сервера требуется, чтобы сам сервер имел статический IP. Также на момент установки серверов крайне рекомендуется уже иметь разработанный план подсетей, областей и исключений. Также не стоит забывать о правильной конфигурации сетевого оборудования. Например, получение ip адреса от DHCP сервера будет работать в рамках одного широковещательного домена. Если вы используете оборудование Cisco и несколько vLan, для каждого из них нужно прописать ip-helper с указанием ip адреса DHCP сервера. В случае использования другого сетевого оборудования нужно найти механизмы для настройки этого функционала. После установки роли, подключиться к службам для дальнейшего управления можно с помощью консоли, которая находится в меню инструментов для администрирования.

Дальнейшая настройка DHCP сервера требует конфигурирования хотя бы одной области, в рамках которой будет указан пул выдаваемых IP адресов, адреса, которые нужно исключить из выдачи, а также резервирования. Резервировать IP адрес нужно для того, чтобы этот адрес выдавался автоматически, но только одному единственному устройству. В качестве уникального идентификатора используется МАК адрес сетевого

интерфейса устройства, которому требуется выдать IP. Кроме этих настроек также можно указать ряд сетевых параметров (options), которые будут получены вместе с IP адресом. Например, шлюз и DNS сервера сети, прокси-сервера для выхода в Интернет, параметры PXE для загрузки устройства по сети, а также многое другое.

Для дальнейшей настройки DNS сервера потребуется создание хотя бы одной прямой и, при необходимости, обратной зоны, указать необходимость динамических обновлений и настроить пересылку запросов. Для настройки можно использовать готовый мастер, вызвать который можно из меню консоли управления DNS.

При создании зоны нужно указать ее тип. Существует 3 типа зон:

Основная. Используется непосредственно для управления записями Зоны.

Дополнительная. Является копией основной и может выдавать информацию о записях зоны, однако не позволяет редактирование.

Зона-заглушка. Хранит в себе только информацию о NS-серверах зоны, упрощая процесс разрешения имен и администрирования DNS.

После того как зона создана. Ее нужно наполнить требуемыми записями.

Наиболее используемые из них

A (AAAA для IPv6)– ставит имя в соответствие IP адресу.

CNAME – псевдоним для записи A

MX – адрес почтового шлюза для доменной зоны.

NS – адреса серверов, обслуживающих зону.

TXT – запись произвольных двоичных данных.

PTR – ставит IP адрес в соответствие имени.

Есть еще другие, такие как SOA, SRV и пр.

Нужно отметить, что другие DNS сервера обновляют информацию о вашей зоне с некоторой задержкой, соответственно, нужно помнить, что, несмотря на то, что изменения DNS зоны применяются незамедлительно, говорить об однозначном отсутствии ошибок в разрешении имен можно только через 48 часов после применения изменений.

Одной из частых задач, возникающих при установке собственного DNS сервера, является перенос зоны от провайдера. Для этого необходимо:

Создать дополнительную зону.

Стянуть все данные с основной зоны при помощи синхронизации.

Сделать зону основной

Изменить для нее NS сервера.

Говоря о создании резервной копии важно понимать, что сам сервис разворачивается за несколько минут и основными данными, которые подлежат защите, является:

Для DHCP: дамп настроек сервера и областей.

Для DNS: дамп настроек и зон.

Методов защиты этой информации существует великое множество. Какой из способов выбрать – решать Вам.

Данный текст был призван пролить свет на необходимость и принципы работы сетевых сервисов DNS и DHCP в инфраструктуре Вашего предприятия.

Закрепление материала:

1. Сервис DHCP, основные функции.
2. Сервис DNS, основные функции.
3. Где могут быть установлены службы DNS и DHCP?
4. Что необходимо для установки DNS и DHCP сервера?
5. Какие действия необходимо выполнить при переносе зоны провайдера?

Задания выполнить в Word и направить на почту: ignat-880@mail.ru не позднее 13.04.2020г.