

# **Протокол DHCP**

# **Проблема автоматизации распределения IP-адресов**

Одной из основных задач системного администратора является настройка стека протоколов TCP/IP на всех компьютерах сети.

# Проблема автоматизации распределения IP-адресов

Есть несколько необходимых параметров, которые следует настроить на каждом компьютере:

- IP-адрес,
- Маска подсети
- Шлюз по умолчанию
- IP-адреса DNS-серверов

Назначенные IP-адреса должны быть уникальны

# Проблема автоматизации распределения IP-адресов

Если в сети менее десяти компьютеров, администратор может успешно справляться с задачей настройки стека TCP/IP вручную

- IP-адрес, назначенный таким образом, называется *статическим*

# Проблема автоматизации распределения IP-адресов

При числе узлов сети более десяти задача распределения параметров вручную становится трудной или вовсе не выполнимой.

- В стеке TCP/IP существует протокол, позволяющий автоматизировать процесс назначения IP-адресов и других сетевых параметров: DHCP – Dynamic Host Configuration Protocol;
- Описание протокола DHCP приводится в документе RFC 2131.

# Реализация DHCP в Windows

Протокол DHCP реализуется по модели «клиент-сервер», в сети должны присутствовать:

- DHCP-сервер
  - DHCP-клиент
- 
- На компьютере-сервере хранится база данных и работает служба DHCP сервера.
  - Компьютер-клиент (точнее, служба клиента DHCP) осуществляет запросы на автоматическую конфигурацию.

# Реализация DHCP в Windows

- Набор IP-адресов, выделяемых для компьютеров одной физической подсети, называется *областью действия (scope)*.
- При запросе клиента DHCP-сервер выделяет ему произвольный свободный IP-адрес из области действия.
- При необходимости некоторые адреса из области действия можно *зарезервировать (reserve)* за определенным MAC-адресом.

# Реализация DHCP в Windows

- Адреса выделяются клиентам на определенное время, поэтому предоставление адреса называется *арендой (lease)*.
- *Время аренды в Windows* может быть от 1 минуты до 999 дней (или неограниченно) и устанавливается администратором.



# Параметры DHCP

## Основные параметры DHCP

- Subnet mask – маска подсети;
- Router – список IP-адресов маршрутизаторов;
- Domain Name Servers – список адресов DNS-серверов;
- DNS Domain Name – DNS-суффикс клиента;
- WINS Server Names – список адресов WINS-серверов;
- Lease Time – срок аренды (в секундах);
- Renewal Time (T1) – период времени, через который клиент начинает продлевать аренду;
- Rebinding Time (T2) – период времени, через который клиент начинает осуществлять широковещательные запросы на продление аренды.

# Параметры DNSP

Параметры могут применяться на следующих уровнях:

- уровень сервера;
- уровень области действия;
- уровень класса;
- уровень клиента (для зарезервированных адресов).

# Адреса для динамической конфигурации

- При настройке областей действия перед администратором встает вопрос, какой диапазон адресов выбрать для сети своей организации?
- Если сеть имеет доступ в Интернет, диапазон адресов назначается ISP, чтобы обеспечить уникальность адресов в интернете.

# Адреса для динамической конфигурации

- Если хосты получают доступ к интернет-трафику через буферные узлы, то диапазон внутренних адресов организации должен выбираться из множества частных адресов.
- *Частные адреса (Private addresses), описанные в RFC 1918, специально выделены для применения во внутренних сетях и не могут быть присвоены хостам в Интернете.*

# Частные адреса

Существует три диапазона частных адресов:

- ID подсети – 10.0.0.0, маска подсети: 255.0.0.0;
- ID подсети – 172.16.0.0, маска подсети: 255.240.0.0;
- ID подсети – 192.168.0.0, маска подсети: 255.255.0.0.

Внутри этих диапазонов адресов можно организовывать любые возможные подсети.

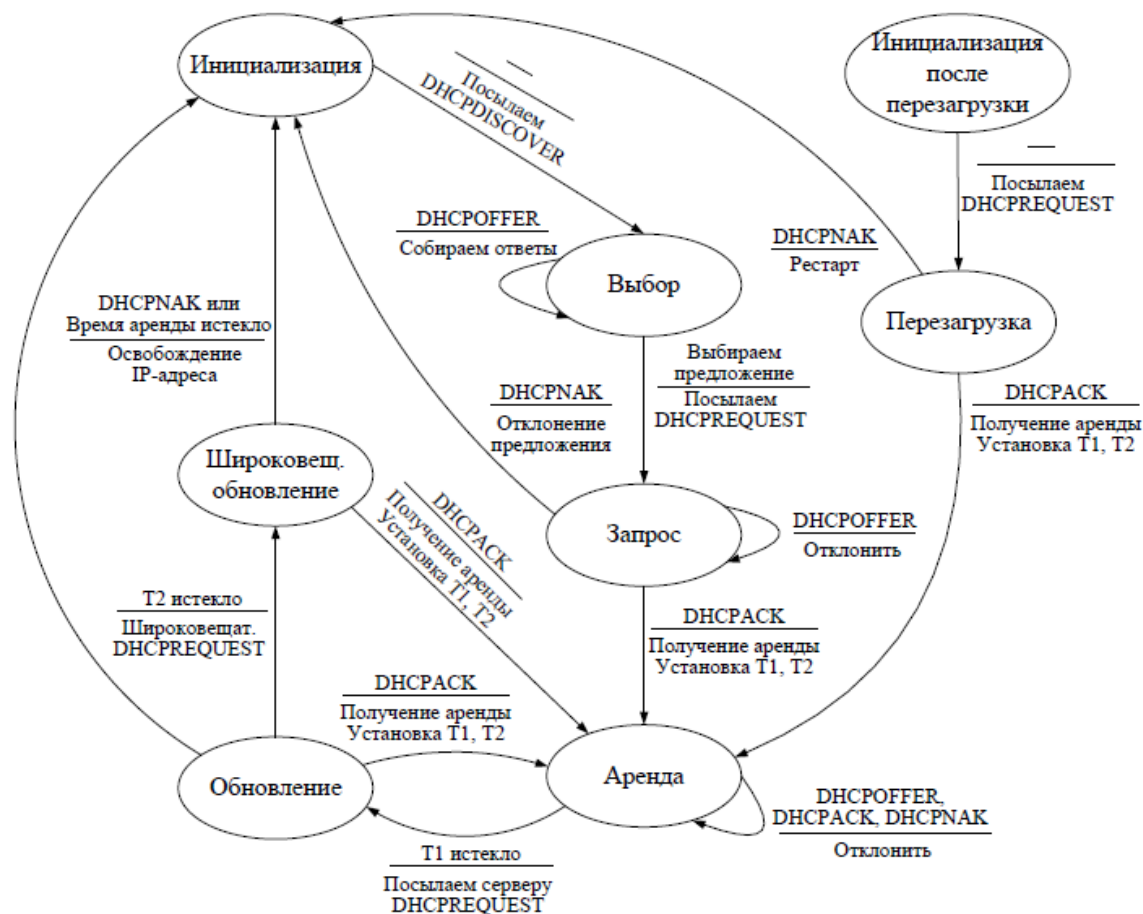
# DHCP-сообщения

- Процесс функционирования служб DHCP заключается в обмене сообщениями между сервером и клиентом. Типы DHCP сообщений приведены в таблице.

# DHCP сообщения

| Тип сообщения                      | Направление     | Значение   |
|------------------------------------|-----------------|--|
| DHCPDISCOVER<br>(DHCP-обнаружение) | Клиент → сервер | Широковещательный запрос для обнаружения DHCP-сервера          |
| DHCPOFFER<br>(DHCP-предложение)    | Сервер → клиент | Ответ на DHCPDISCOVER, содержит предлагаемые сетевые параметры |
| DHCPREQUEST<br>(DHCP-запрос)       | Клиент → сервер | Запрос предложенных параметров                                 |
| DHCPACK<br>(DHCP-подтверждение)    | Сервер → клиент | Подтверждение сетевых параметров                               |
| DHCPNAK<br>(DHCP-несогласие)       | Сервер → клиент | Отклонение запроса клиента                                     |
| DHCPDECLINE<br>(DHCP-отказ)        | Клиент → сервер | Отказ клиента от предложенных параметров                       |
| DHCPRELEASE<br>(DHCP-освобождение) | Клиент → сервер | Освобождение арендованного IP-адреса                           |
| DHCPINFORM<br>(DHCP-информация)    | Клиент → сервер | Запрос дополнительных параметров                               |

# Принцип работы DHCP





# Авторизация DHCP-сервера

Неправильное функционирование DHCP-сервера в любой сети может привести к нарушению работы всей сети.

Ошибки в настройке могут быть вызваны:

- Неправильным планированием, когда в одной подсети оказываются несколько DHCP-серверов,
- Действиями некомпетентного лица (возможно, злоумышленника).

# Авторизация DHCP-сервера

Для предотвращения последствий таких действий в Windows Server предусмотрен механизм *авторизации DHCP-серверов*. *Неавторизованный DHCP-сервер (unauthorized DHCP server)* не будет работать в этой операционной системе.

Процедуру авторизации может выполнить только администратор.

Адрес авторизованного DHCP-сервера регистрируется в каталоге Active Directory.

При запуске служба DHCP-сервера проверяет наличие IP-адреса своего компьютера в списке авторизованных DHCP-серверов Active Directory и только после этого может продолжать свою работу.