

Сеть и сетевые протоколы: DHCP

Александр Нагернюк
Эксперт в области сетей и информационной безопасности



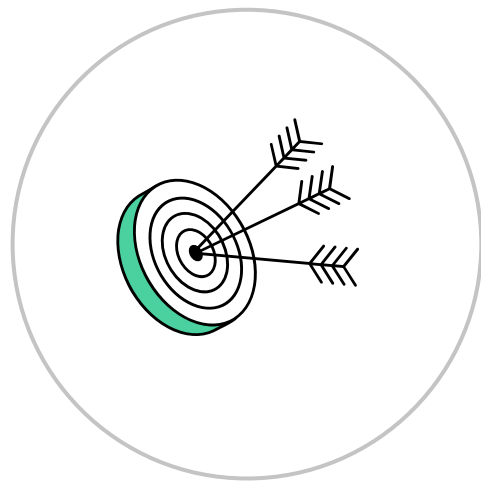
Александр Нагернюк

- О спикере:
- Сертифицированный специалист Cisco, PaloAlto, Huawei
- Более 10 лет опыта работы в Enterprise сетях и информационной безопасности
- Супервайзер сетевой команды Kert (ex. KPMG)



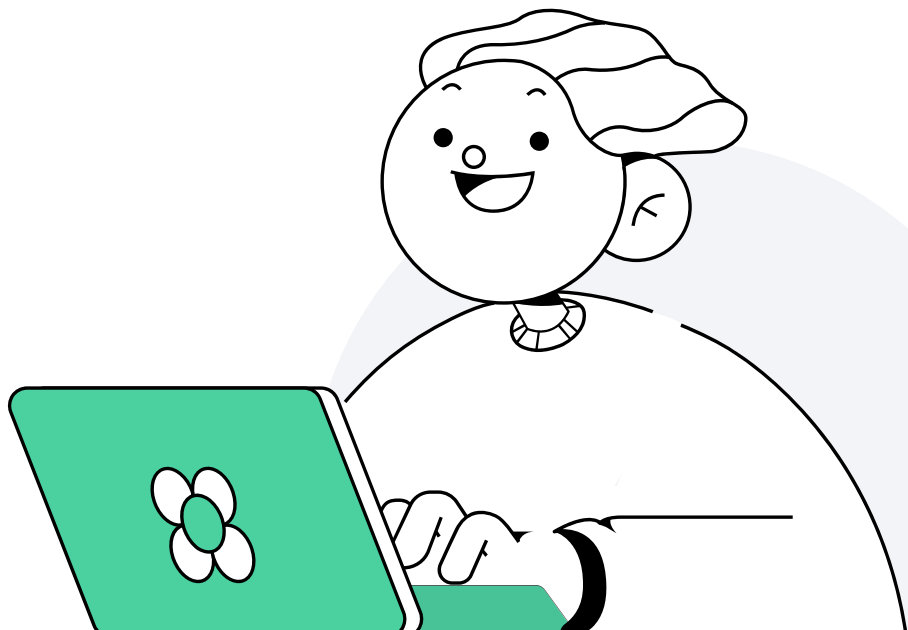
Цели занятия

- Понять устройство протокола DHCP
- Познакомиться с возможностями и особенностями настройки DHCP сервера. Закрепить это на практике
- Рассмотреть возможности окружения PXE, получить навыки создания среды PXE для работы бездисковых станций

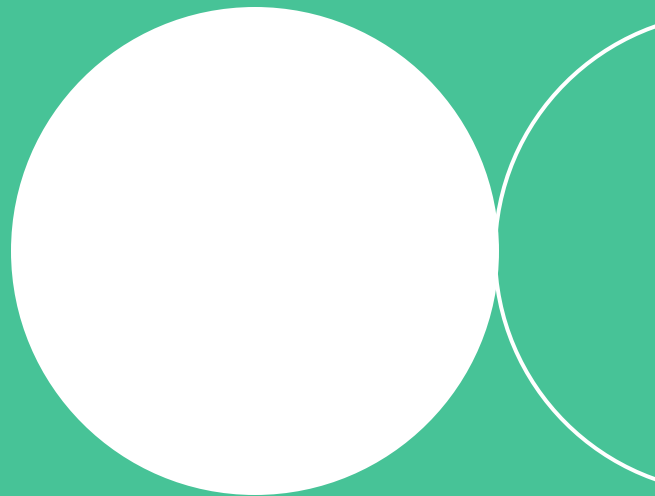


План занятия

- ① Основные понятия DHCP
- ② Механизм работы DHCP
- ③ Установка и конфигурация DHCP
- ④ PXE
- ⑤ Настройка и конфигурация PXE
- ⑥ Итоги занятия
- ⑦ Домашнее задание

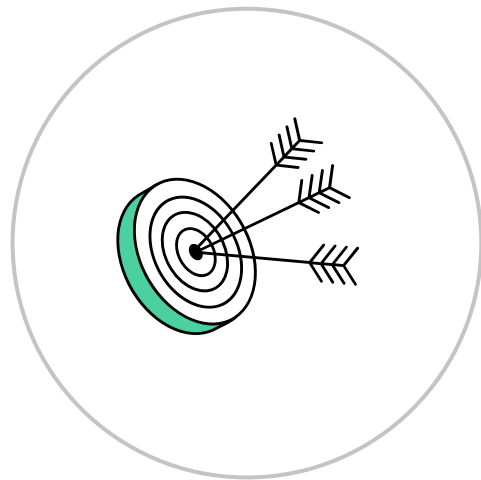


Основные понятия



Цели темы

- Познакомиться с протоколом DHCP и его предшественником BOOTP
- Узнать об особенностях архитектуры DHCP
- Разобраться с терминологией и механизмом работы



Дословный перевод DHCP

Dynamic Host
Configuration Protocol

Протокол динамической
конфигурации узла



DHCP

сетевой протокол прикладного уровня модели TCP/IP позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети




Протокол DHCP описан в



RFC2131

DHCP



Работает на
67/68 портах
поверх UDP

The background of the slide features three large, light gray circles that overlap each other. The central circle is the most prominent and contains the text.

DHCP

**является расширением
и дополнением протокола**

BOOTP

Дословный перевод BOOTP

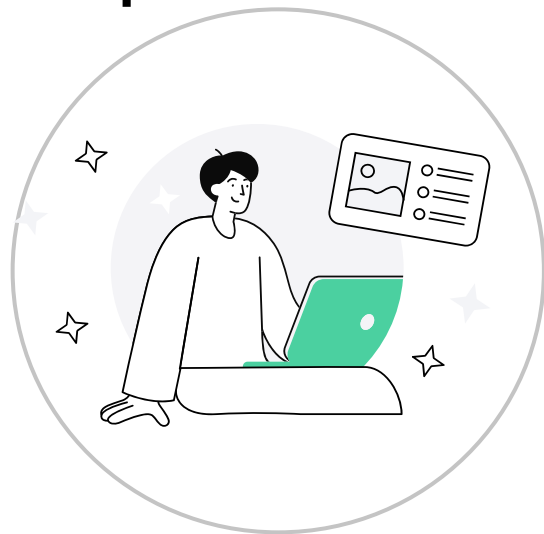
**BOOTSTRAP
PROTOCOL**

**Протокол начальной
загрузки**



BOOTP

сетевой протокол, используемый для автоматического получения клиентом IP-адреса (обычно во время загрузки компьютера)

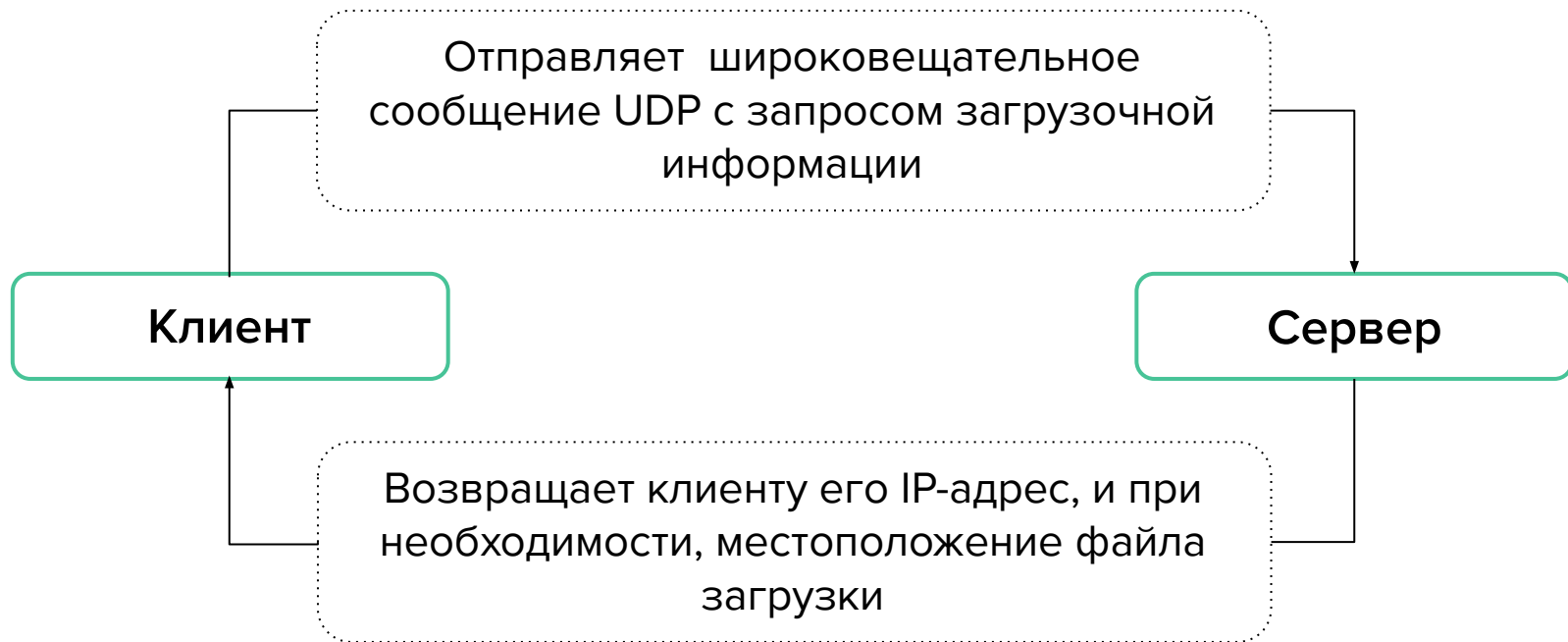


BOOTP определен в



RFC951

BOOTP



С помощью **TFTP** (протокол пересылки файлов) клиент загружает необходимое программное обеспечение и начинает работу

Дословный перевод TFTP

Trivial File Transfer
Protocol



Простой протокол
передачи файлов



TFTP

используется главным образом для первоначальной загрузки бездисковых рабочих станций



TFTP, в отличие от **FTP**,
не содержит возможностей
аутентификации (хотя возможна
фильтрация по IP-адресу)
и основан на транспортном
протоколе **UDP**



DHCPv6

**новая версия протокола для работы
с сетях на основе IPv6**




Протокола DHCPv6 описан в



RFC3315

DHCPv6

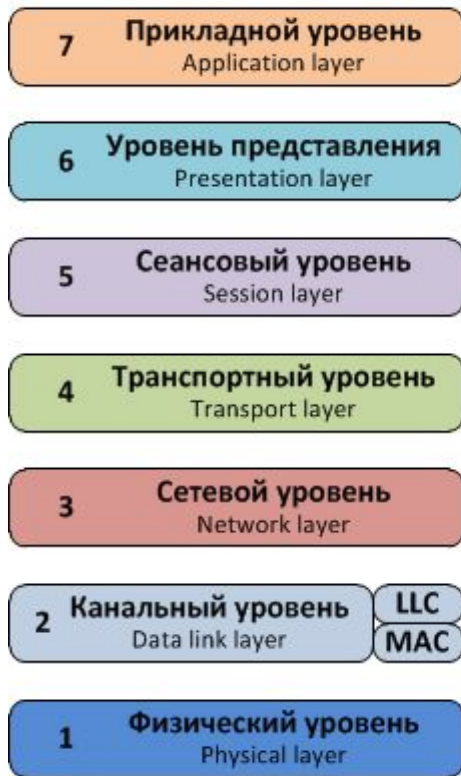


Работает на
546/547
портах
поверх UDP

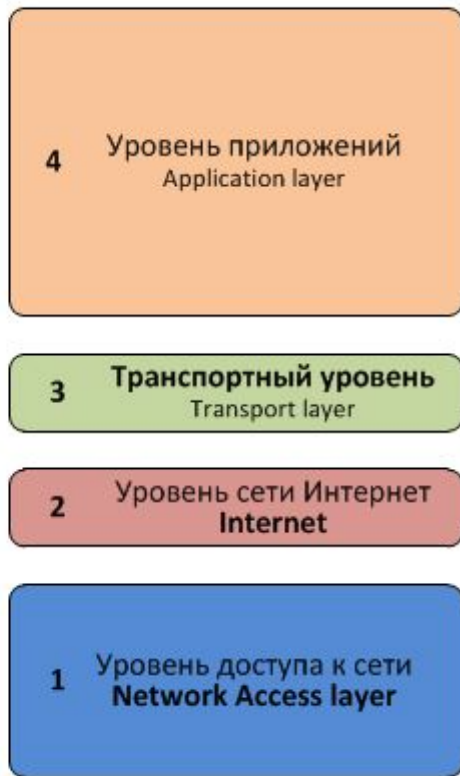
**DHCPv6 НЕ является
дополнением протокола BOOTP
и использует отличные от
DHCPv4 пакеты**

DHCP работает на прикладном уровне модели OSI

OSI



TCP/IP (DOD)



Протоколы уровней

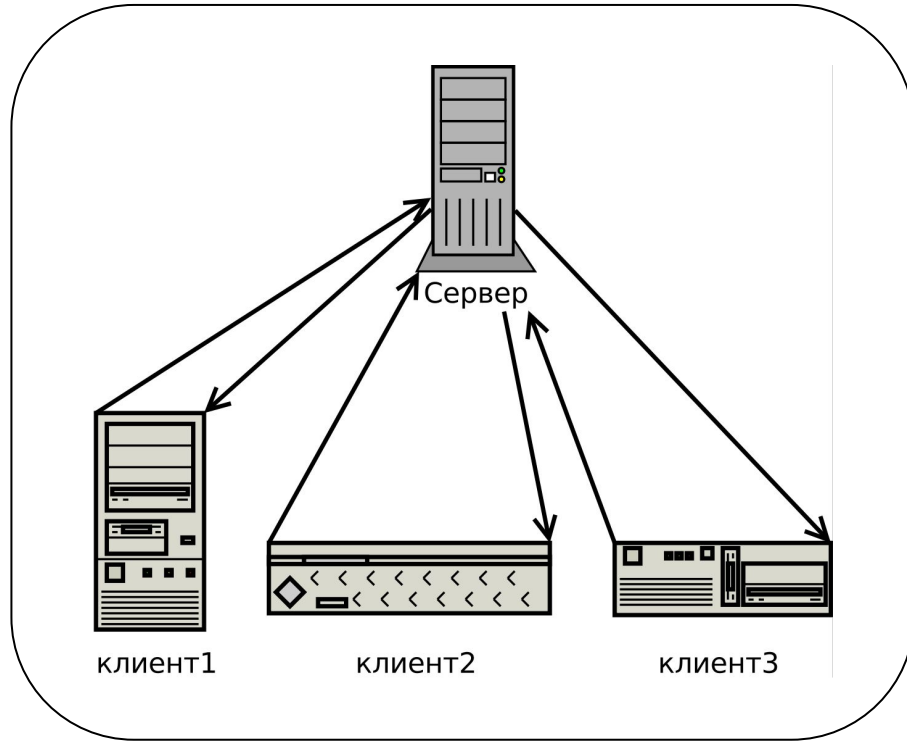
HTTP, SMTP, DHCP, DNS, Telnet, SSH, FTP, POP3, NTP, IMAP

TCP, UDP

IPv4, IPv6, Ipsec, RIP, OSPF, EIGRP, IS-IS, NAT

Ethernet, IEEE 802.11, PPP

Архитектура DHCP



Термины DHCP

1

Scope (область)

диапазон IP-адресов, из которого сервер будет предлагать адреса клиенту в аренду

2

Lease (аренда)

период, в течение которого клиент может использовать IP-адрес

3

Reservation (резервирование)

закрепление IP адреса за конкретным устройством

Термины DHCP

4

Exclusion range
(исключаемый диапазон)

диапазон IP-адресов,
которые не могут быть
назначены клиенту

5

Address pool
(пул адресов)

свободные IP-адреса,
готовые к выдаче клиентам

Механизмы выделения IP-адресов сервером DHCP

1

Динамическое присвоение

IP-

адрес выдается сервером по
общим правилам на
ограниченное время

2

Ручной режим работы DHCP-сервера

IP-адрес выдается вручную
системным администратором

Механизмы выделения IP-адресов сервером DHCP

3

Автоматическое назначение статистических адресов

IP-адрес выдается сервером на основании MAC-адреса клиента.

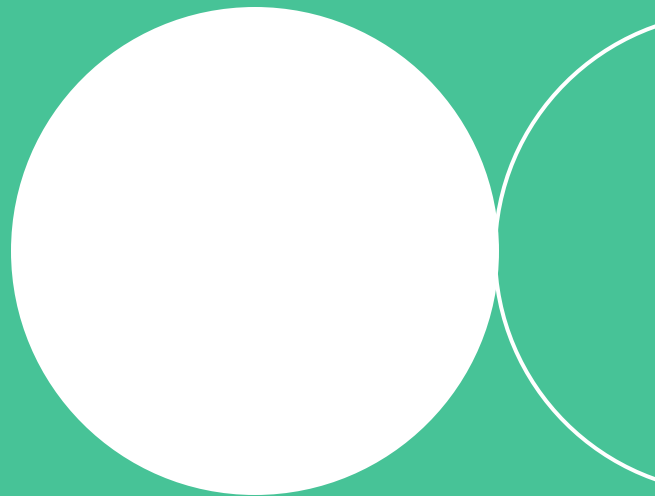
База соответствий ведется в конфигурационных файлах сервера системным администратором

Итоги темы

- 1 DHCP является дальнейшим развитием протокола BOOTP. DHCPv6 является отдельным протоколом, не совместимым с предыдущей версией
- 2 Протокол DHCP относится к Прикладному уровню модели OSI и работает по клиент-серверной модели
- 3 Сеть может устойчиво работать одновременно как с устройствами, являющимися клиентами DHCP, так и не поддерживающими протокол

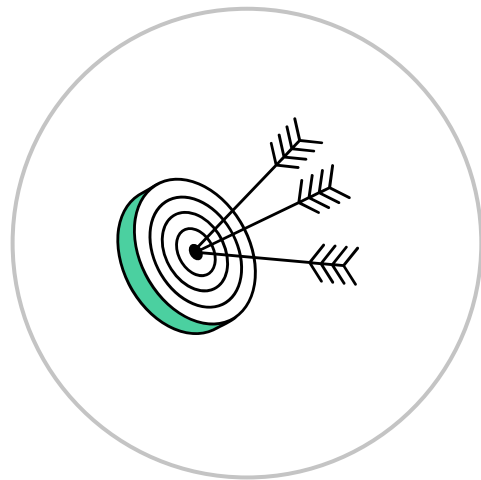



Механизм работы DHCP



Цели темы

- Понять особенности формата метаданных DHCP
- Усвоить порядок обмена между сервером и клиентом
- Выяснить какие настройки можно передавать с помощью DHCP





DHCP-сервер
служит для упрощения
добавления новых устройств
в сеть

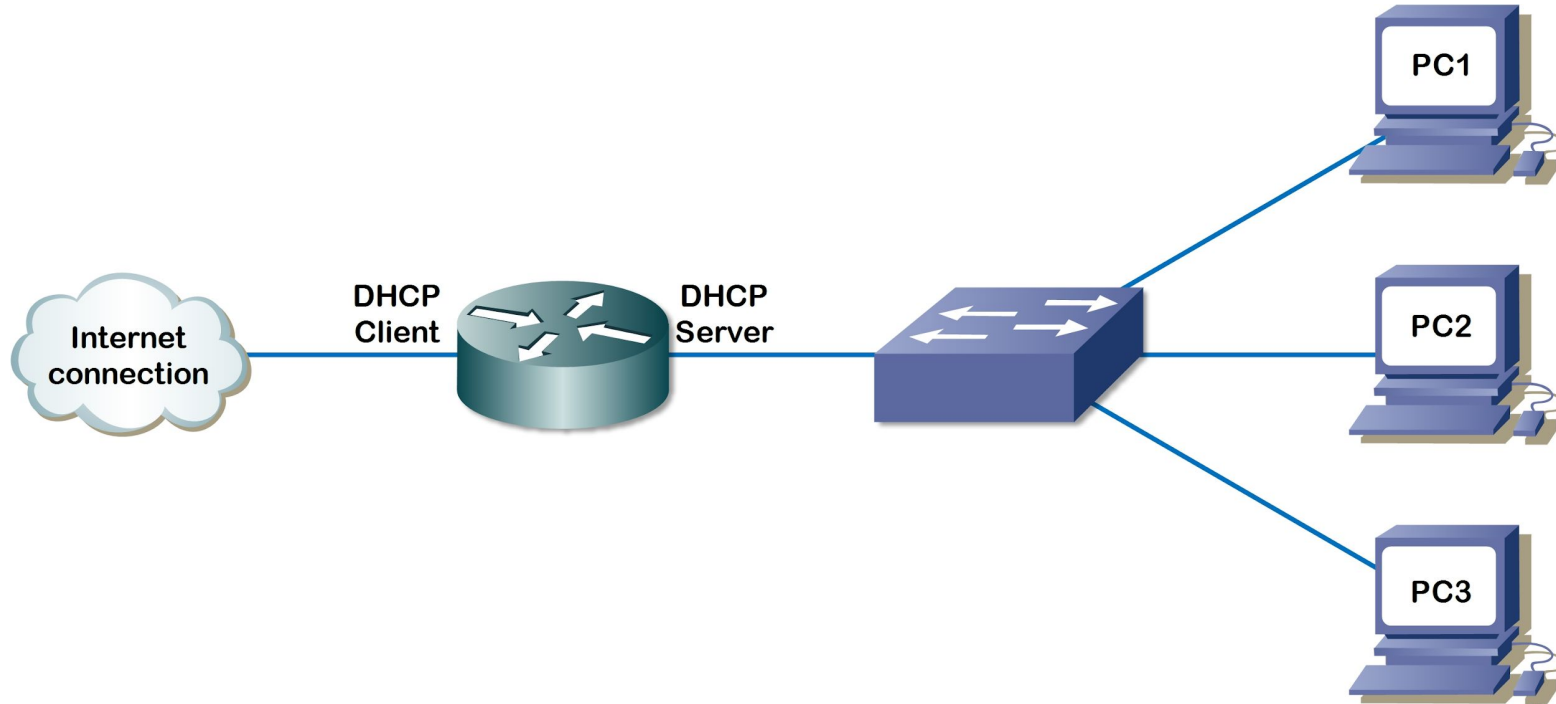
DHCP сервер

Домашний Wi-Fi роутер
имеет встроенный
DHCP сервер

Настройки производятся
автоматически

Для транспорта используются
порты UDP 67, 68 (клиент-
сервер, сервер-клиент)

DHCP сервер



Формат кадра DHCP

Dynamic Host Configuration Protocol				
Bit Offset	0-15		16-31	
0	OpCode	Hardware Type	Hardware Length	Hops
32	Transaction ID			
64	Seconds Elapsed		Flags	
96	Client IP Address			
128	Your IP Address			
160	Server IP Address			
196	Gateway IP Address			
228+	Client Hardware Address (16 bytes)			
	Server Host Name (64 bytes)			
	Boot File (128 bytes)			
	Options			

Формат кадра DHCP

- **Opcode** (op) – тип DHCP-сообщения
 - 0x01 запрос от клиента к серверу BOOTREQUEST
 - 0x02 ответ DHCP-сервера или BOOTREPLY
- **Hardware Type** (htype) – тип адреса на канальном уровне.
0x01 для протокола Ethernet и MAC-адресов.
Список допустимых значений в RFC 1700
- **Hardware Length** (hlen) – длина аппаратного адреса в байтах
Для Ethernet значение 0x06
- **Hops** – количество промежуточных маршрутизаторов, которые находятся на пути между клиентом и сервером.
DHCP-клиенты всегда ставят значение 0x00

Формат кадра DHCP

- **Transaction ID** (xid) – случайное значение для идентификации диалога
- **Seconds Elapsed** (secs) – время в секундах с момента начала процесса получения IP-адреса
- **Flags** – поле для флагов или специальных параметров DHCP
- **Client IP Address** (ciaddr) – IP-адрес клиента. Клиент заполняет его в случае, если клиент хочет продлить аренду IP-адреса
- **Your ID Address** (yiaddr) – IP-адрес, который DHCP-сервер предлагает клиенту.
- **Server IP Address** (siaddr) – IP-адрес сервера

Формат кадра DHCP

- **Gateway IP Address** (address) – IP-адрес промежуточного DHCP Relay Agent.
- **Client Hardware Address** (chaddr) – Если используется протокол Ethernet, то в это поле записывается MAC-адрес клиента
- **Server Host Name** (sname) – доменное имя сервера, поле не является обязательным.
- **Boot File** (file) – указатель файла для загрузки бездисковыми станциями, не является обязательным.
- **Options** - опции для динамической конфигурации хоста

Виды DHCP сообщений

DHCPDISCOVER

обнаружение DHCP

DHCPOFFER

предложение DHCP

DHCPREQUEST

запрос DHCP

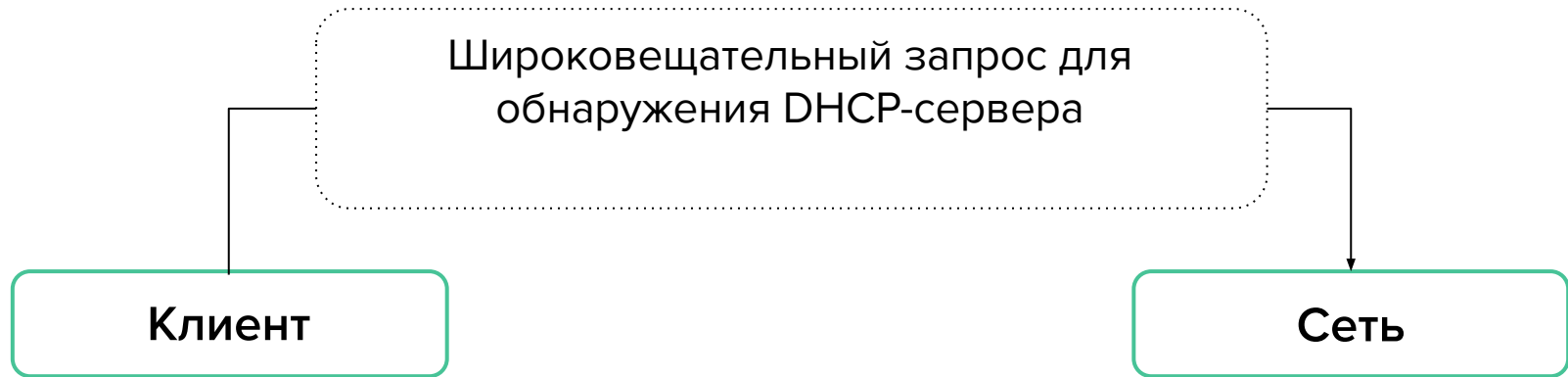
DHCPACK

подтверждение DHCP

Виды DHCP сообщений



DHCPDISCOVER сообщение



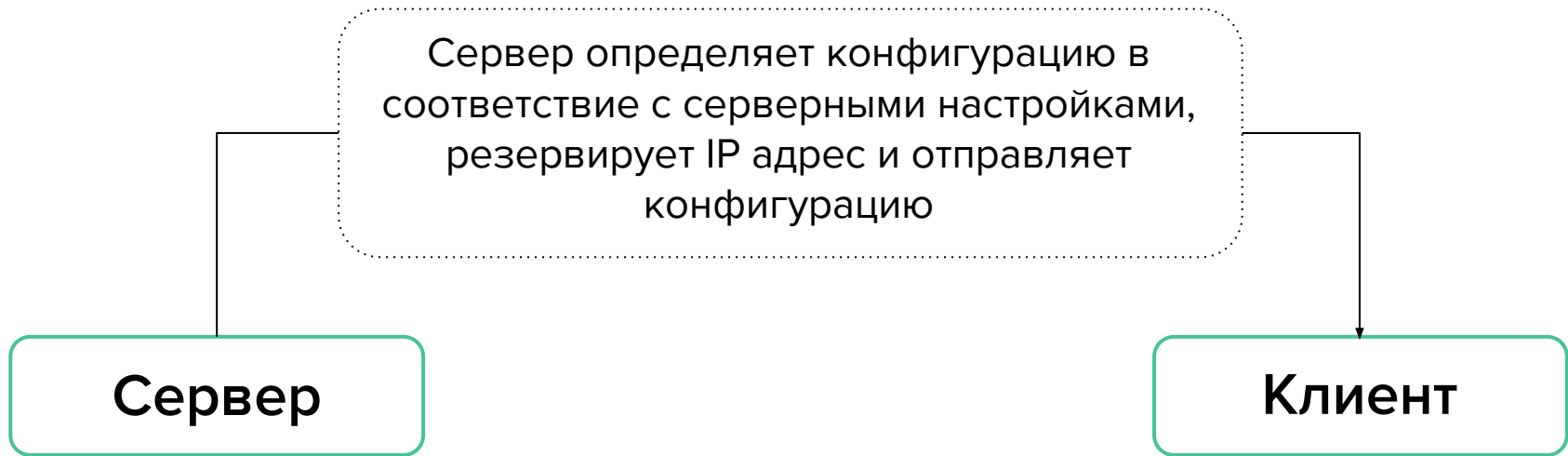
DHCPDISCOVER запросы

IP-адрес источника
0.0.0.0

IP-адрес назначения
255.255.255.255

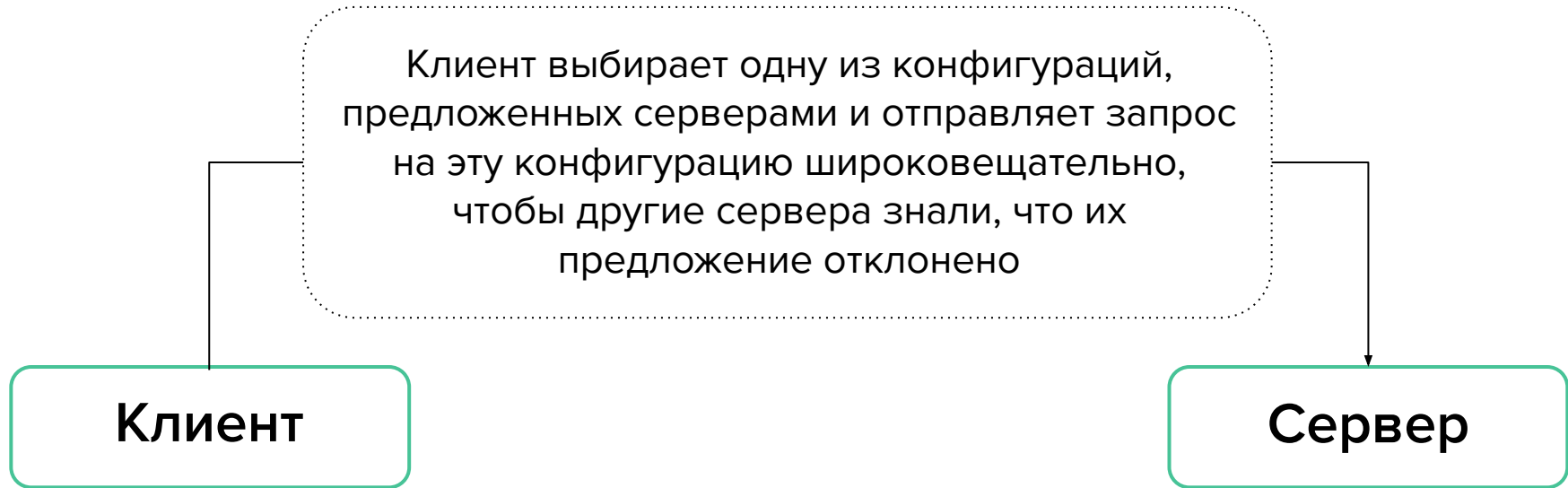
MAC-адрес
назначения
FF-FF-FF-FF-FF-FF

DHCP OFFER сообщение

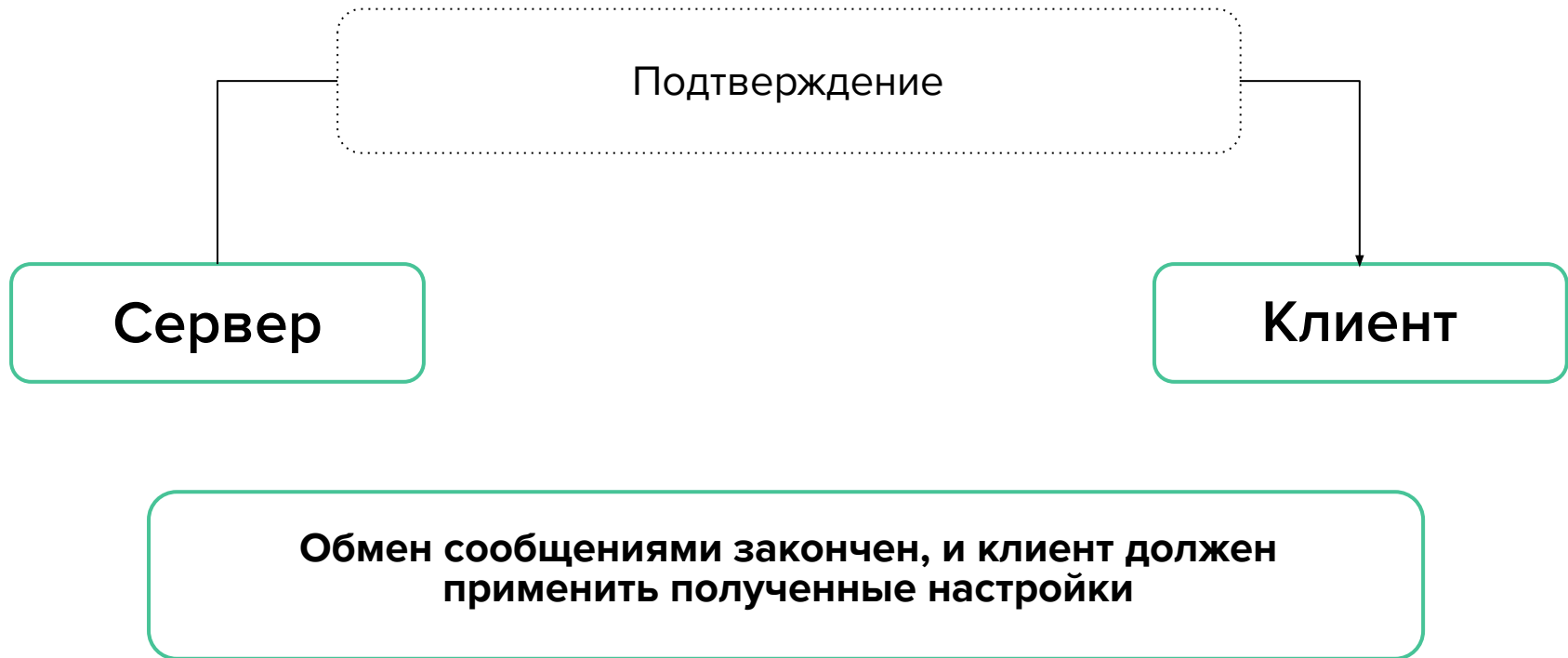


DHCPREQUEST сообщение

В сети может быть несколько DHCP-серверов



DHCPACK сообщение

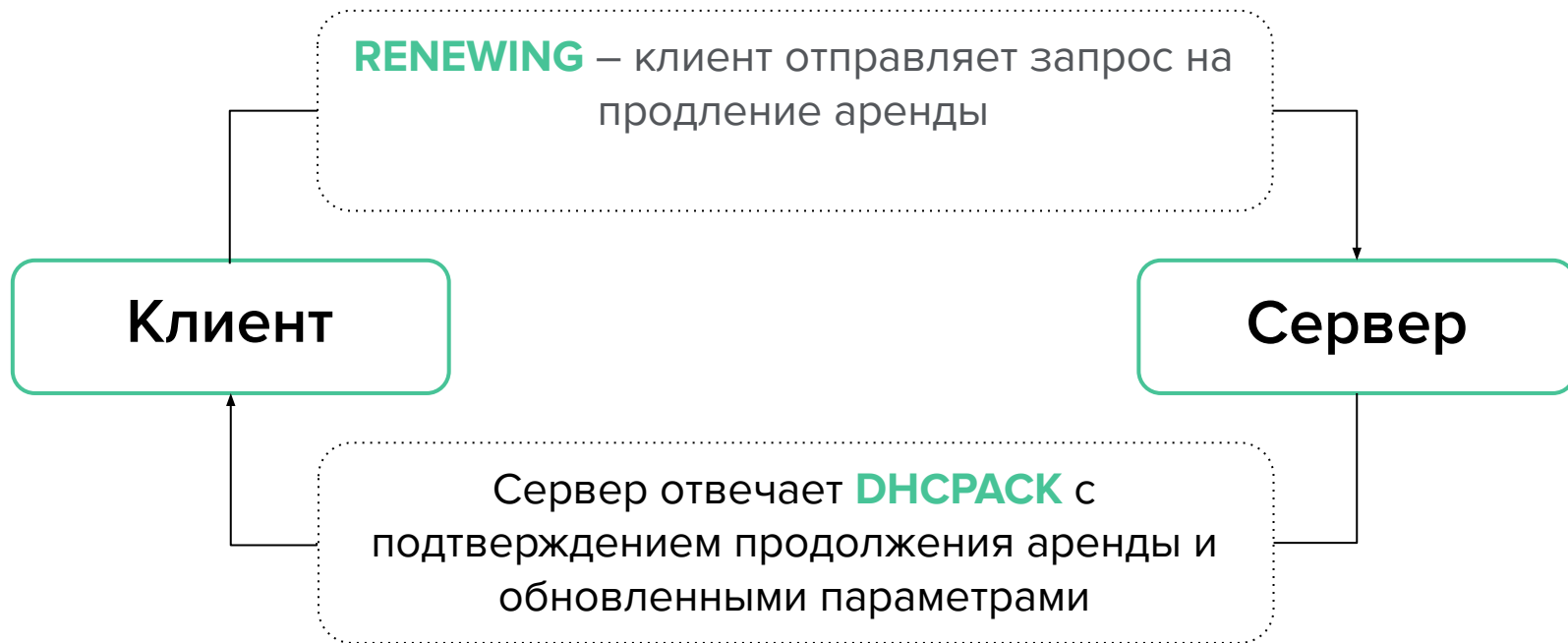


Другие сообщения DHCP

- **DHCPDECLINE** – отправляется клиентом, если он обнаруживает что адрес, предложенный сервером уже используется в сети
- **DHCPNAK** – отправляется сервером; после такого сообщения клиент должен повторить процедуру инициализации
- **DHCPRELEASE** – отправляется клиентом, если он по какой-то причине хочет прекратить аренду
- **DHCPINFORM** – отправляется клиентом, в случае если ему нужны только опции и не нужен IP адрес

**IP-адреса выдаются
сервером DHCP на время,
заданное в настройках сервера
(от минут до месяца). После
завершения половины времени
аренды, клиент пытается
обновить аренду**

Обновление аренды IP адреса



В случае отказа от продолжения аренды сервер отправляет **DHCPNACK** и клиент начинает инициализацию заново



REBINDING

при получении ответа, клиент пытается продлить аренду через широковещательные запросы

Если и это не выходит, клиент заново ищет DHCP-сервер

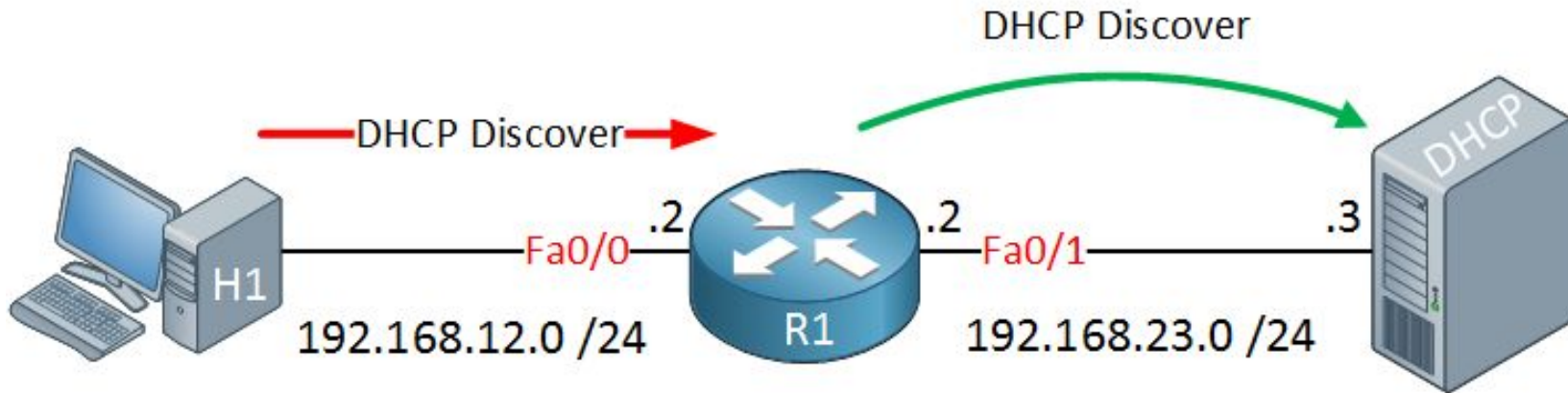
Запросы DHCP

**работают по умолчанию в
пределах широковещательного
диапазона, т.е. до ближайшего
маршрутизатора**

Как отправить DHCP пакеты в другие сети?



Как отправить DHCP пакеты в другие сети?



DHCP сервер

**может сообщать клиенту
дополнительные параметры
для работы в сети, количество
опций зависит от реализации
сервера**

Дополнительные опции DHCP



Список опций

или

man dhcp-options

Некоторые используемые опции DHCP

domain-name-servers

настраивает на
клиенте к какому
серверу dns-имен
обращаться

next-server

сервер, для загрузки
ПО на клиента

smtp-server

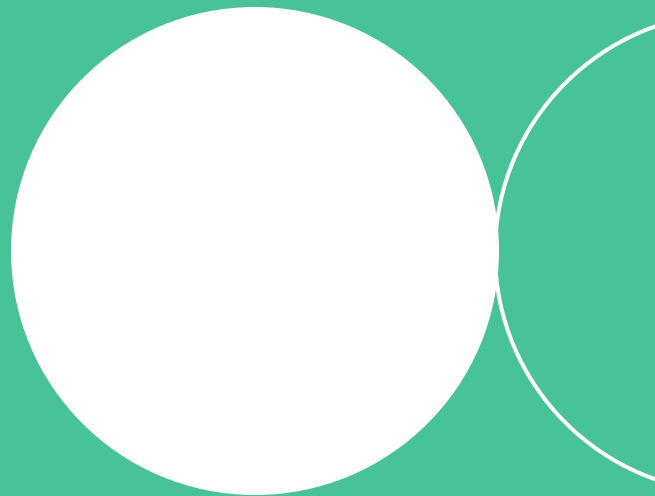
список доступных
клиенту почтовых
серверов

Итоги темы

- 1 Протокол DHCP работает поверх UDP. Для того чтобы не путать транзакции используется специальное поле XID
- 2 Для первоначальной аренды IP-адреса производится обмен 4 сообщениями: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK
- 3 Для работы в различных сегментах сети можно настроить агент DHCP-relay

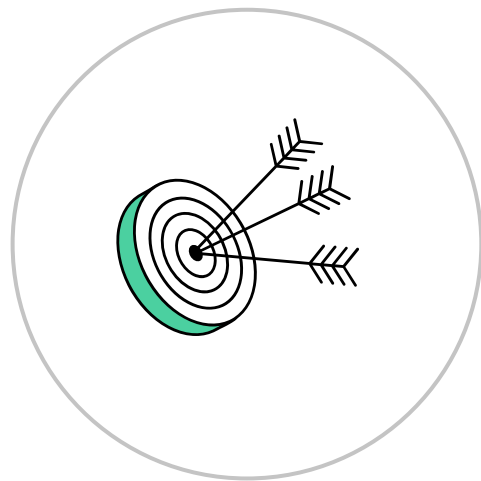


Установка и конфигурирование DHCP-сервера и DHCP-клиента



Цели темы

- Получить практический навык настройки DHCP-сервер
- Выяснить особенности настройки DHCP-клиента
- Обзорно познакомиться с угрозами безопасности у DHCP



Установка DHCP сервера Centos 7

- `yum install dhcp`
- `vim /etc/dhcp/dhcpd.conf`
- `systemctl enable-now dhcpd`
- `firewall-cmd --permanent --add-service=dhcp`
- `firewall-cmd --reload`
- `vim /etc/sysconfig/dhcpd`

Установка DHCP сервера Ubuntu 18 LTS

- `sudo apt-get install isc-dhcp-server -y`
- `sudo vim /etc/dhcp/dhcpd.conf`
- `systemctl enable-now dhcpd`
- `firewall-cmd --permanent --add-service=dhcp`
- `firewall-cmd --reload`
- `/etc/default/isc-dhcp-server`

Настройка DHCP клиента
производится редко.

**В общем случае настройки по
умолчанию должны работать
лучше всего**

Базовые проверки для RHEL-based ОС:

`/etc/sysconfig/network`

NETWORKING=yes

`/etc/sysconfig/network-scripts/ifcfg-*`

**DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes**

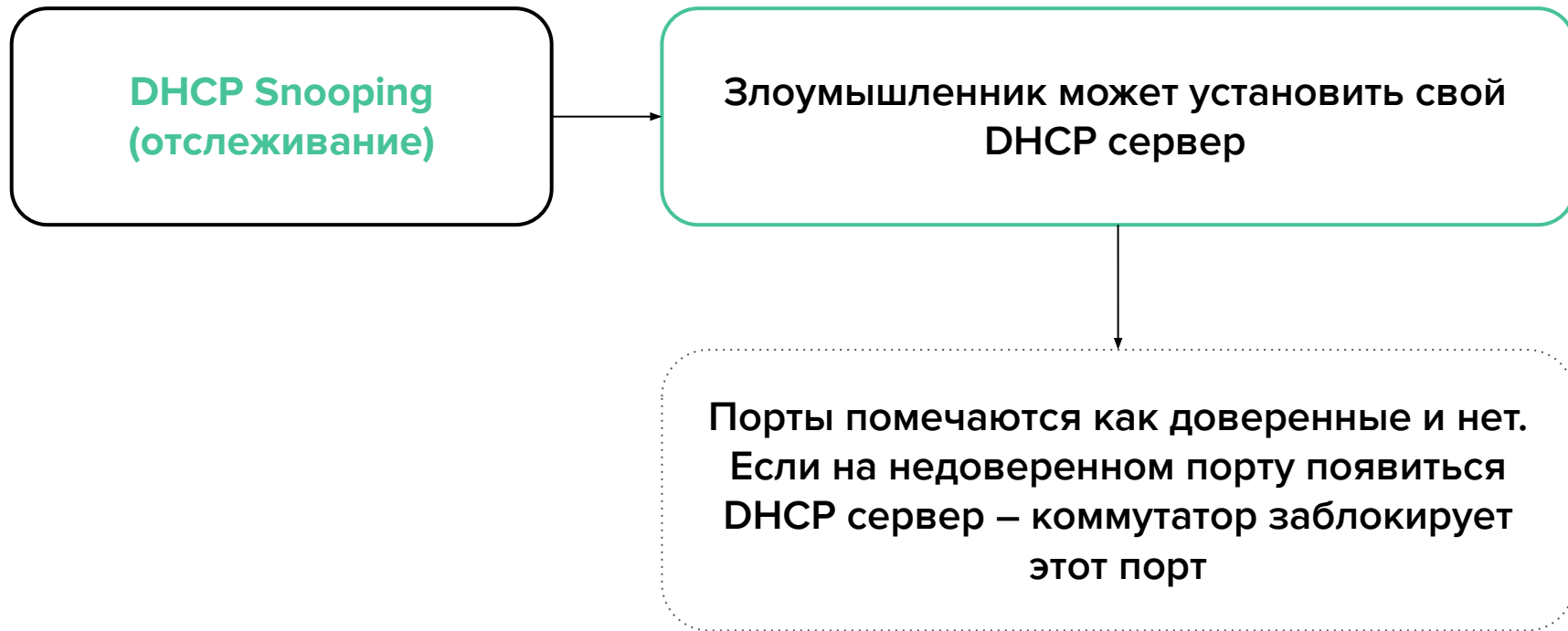
Безопасность DHCP

DHCP Starvation
(истощение ресурсов)

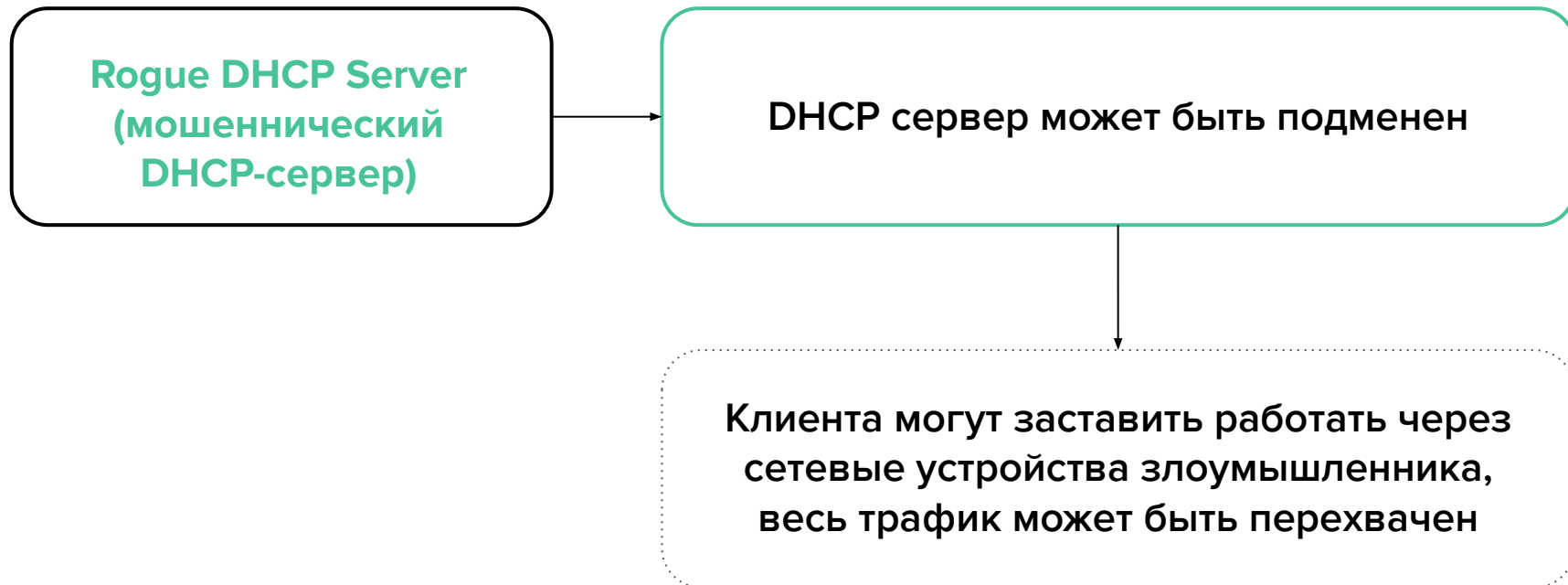
Адреса могут быть исчерпаны
злонамеренно при достаточном
количестве запросов

Легитимные клиенты не могут получить
настройки и подключиться к сети

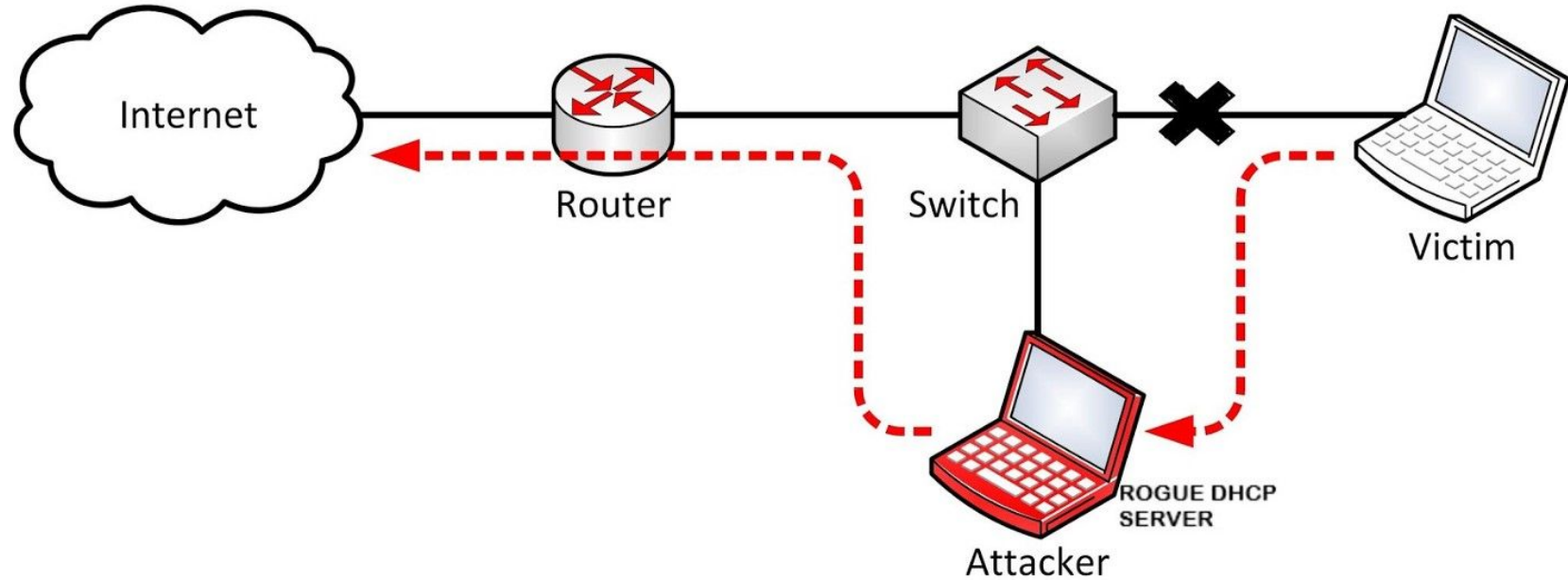
Безопасность DHCP



Безопасность DHCP



Безопасность DHCP



Анализаторы трафика (снифферы)

tcpdump

классическая утилита для
сбора трафика



```
tcpdump -i eth0 udp port 67 or port 68 -vvv -e -n
```

Wireshark

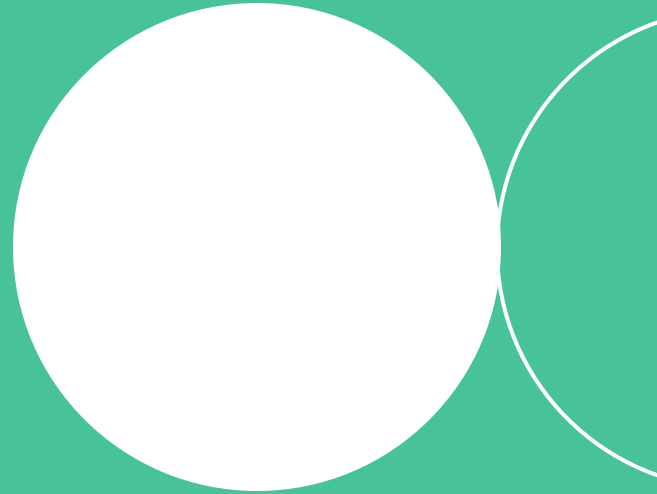
кроссплатформенная
программа, имеет
графический интерфейс

Итоги темы

- 1 При настройке DHCP-сервера необходимо убедиться в том, что в файрволе будет добавлено соответствующее правило для портов 67, 68 UDP
- 2 Настройка DHCP-клиента производится очень редко, так как механизм работы DHCP обеспечивает работу клиента с настройками по умолчанию
- 3 Основная угроза безопасности DHCP исходит из внутренней сети. Следовательно борьба с угрозами заключается в правильном контроле LAN

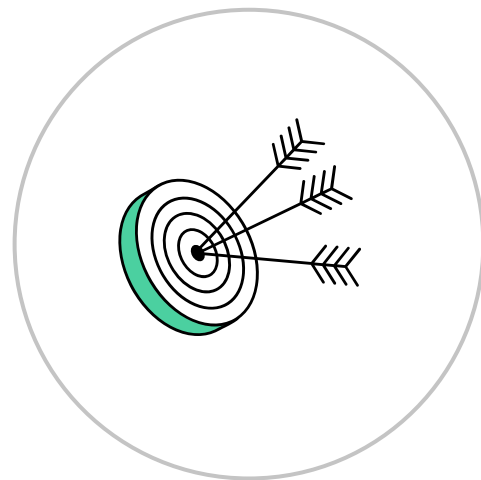


PXE



Цели темы

- Познакомиться с технологией PXE
- Разобраться в различиях толстого и тонкого клиента, их преимуществах и недостатках
- Понять возможности внедрения и использования технологии PXE в локальной сети



Дословный перевод PXE

Preboot eXecution
Environment

Среда предварительного
исполнения

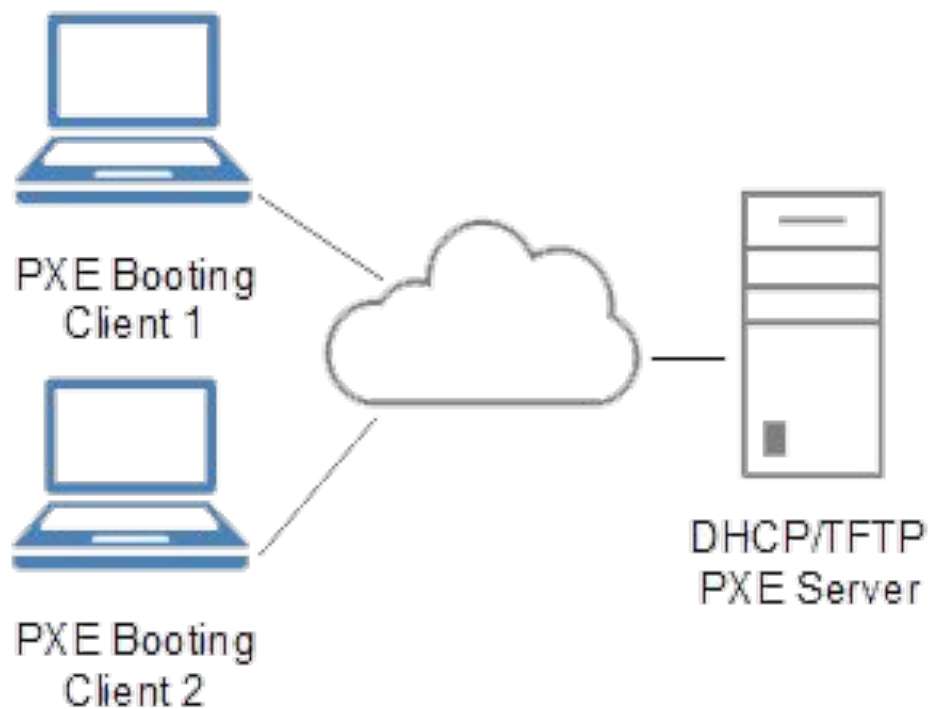


PXE

**технология, которая позволяет компьютеру
загружаться и работать используя
сетевую карту**



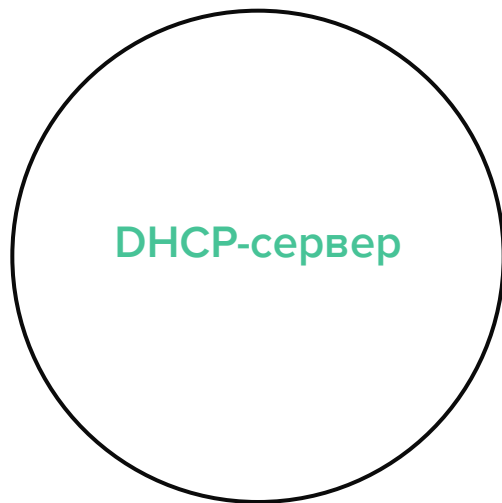
Технология PXE



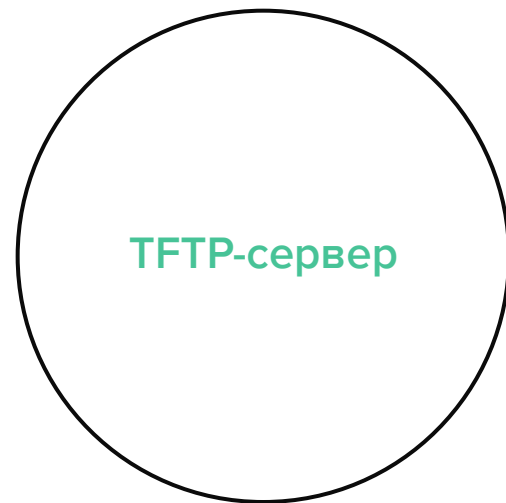
Для запуска компьютера достаточно иметь:



Большинство современных компьютеров поддерживает PXE



Экземпляр сервера, который поддерживает необходимые опции и сконфигурированный для отправки ответов



Сервер, на котором размещены файлы загрузки

Виды клиентов в клиент-серверной архитектуре

Тонкий (thin client)



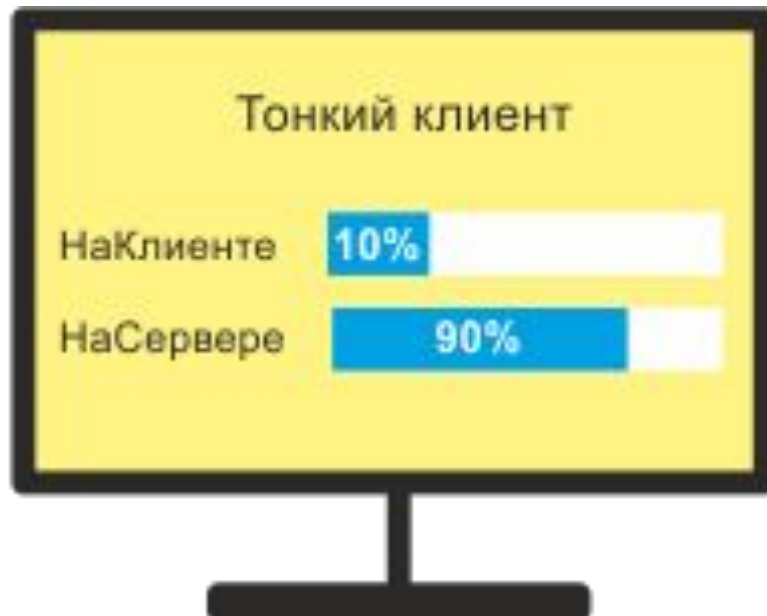
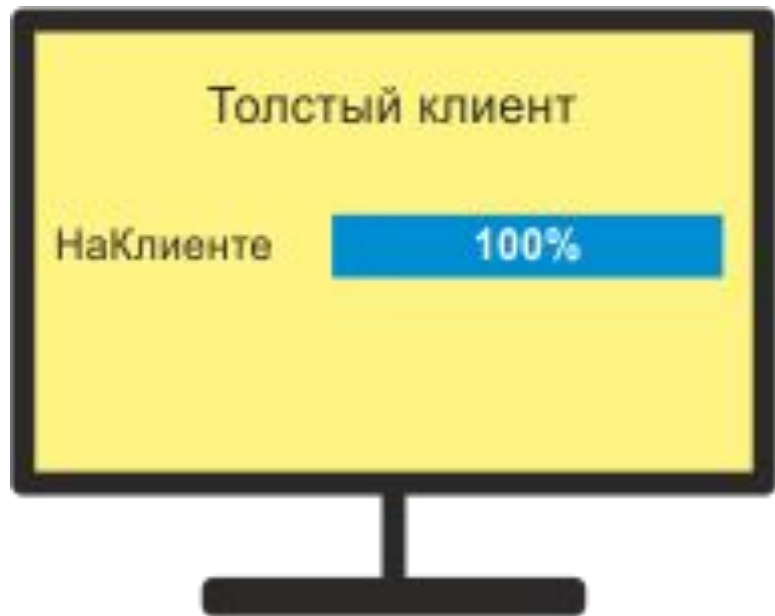
Не может работать без сервера.
Ограниченная
функциональность

Толстый (rich client)



Может работать и при обрыве
связи с сервером.
Многопользовательская работа

Виды клиентов в клиент-серверной архитектуре



Варианты использования PXE



Установка

Можно использовать для
установки операционной
системы на компьютеры
через сеть

Загрузка

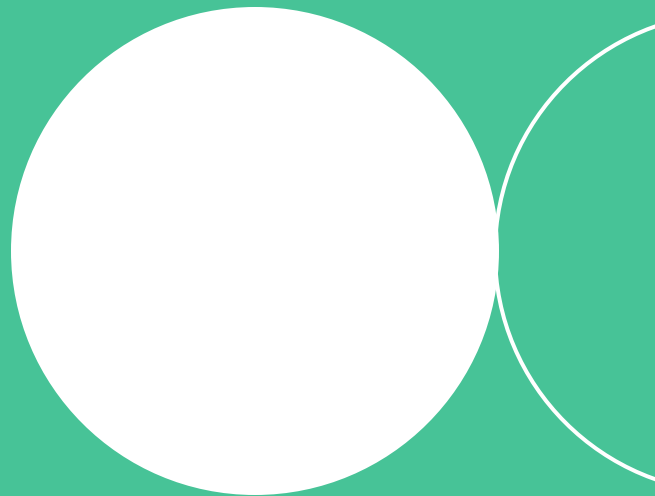
Для работы с
операционной системой
или с программным
обеспечением через сеть

Итоги темы

- 1 Для функционирования PXE в локальной сети обязательно должен быть TFTP сервер. Он не обязательно должен совпадать с DHCP сервером
- 2 Преимуществом тонкого клиента является низкие требования к аппаратному обеспечению
- 3 Толстый клиент позволяет устройству работать в автономном режиме, когда недоступен сервер

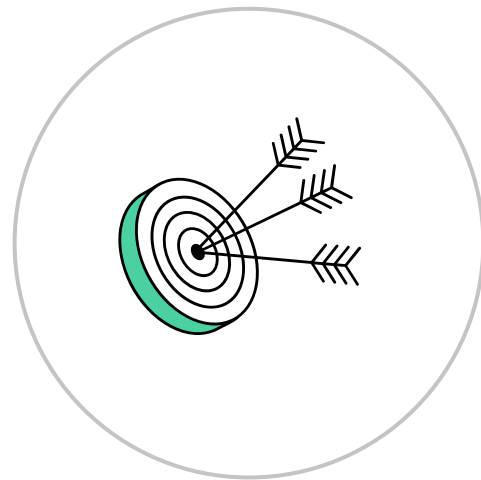


Настройка и конфигурация PXE



Цели темы

- Приобрести практический навык настройки PXE сервера
- Выяснить возможные проблемы и варианты их решения



Установка PXE на Centos 7

- `yum install tftp tftp-server syslinux wget`
- `vim /etc/xinetd.d/tftp`
- `vim /usr/lib/systemd/system/tftp.service`
- `vim /etc/dhcp/dhcpd.conf`
- `mkdir /tftpboot; mkdir /tftpboot/pxelinux.cfg; chmod 777 /tftpboot`
- `cp -v /usr/share/syslinux/pxelinux.0 /tftpboot`
`cp -v /usr/share/syslinux/menu.c32 /tftpboot`
`cp -v /usr/share/syslinux/memdisk /tftpboot`
`cp -v /usr/share/syslinux/mboot.c32 /tftpboot`
`cp -v /usr/share/syslinux/chain.c32 /tftpboot`
- `vim /tftpboot/pxelinux.cfg/default`
- `systemctl restart dhcpd`
- `systemctl restart tftp`

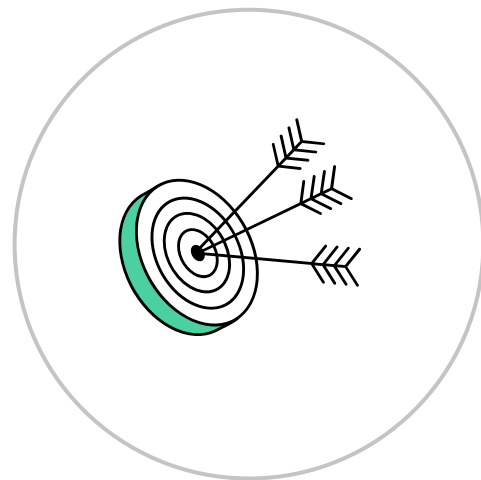
Итоги темы

- 1 Настройка PXE обязательно включает в себя настройку TFTP и DHCP серверов.
- 2 Дополнительно, для загрузки больших образов, можно использовать настройку FTP сервера, как например **vsftpd server**



Итоги занятия

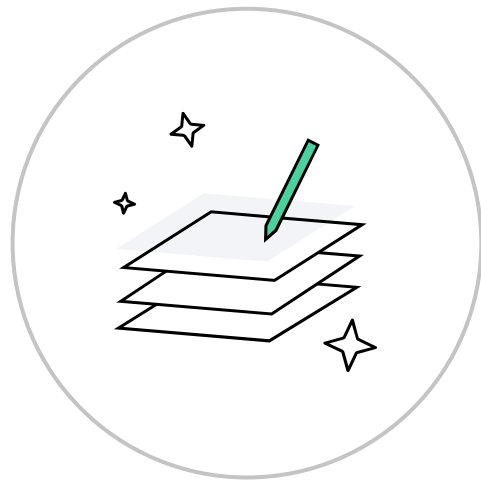
- Изучили устройство протокола DHCP
- Познакомились с возможностями и особенностями настройки DHCP сервера. Закрепили это на практике
- Рассмотрели возможности окружения PXE, получили навыки создания среды PXE для работы бездисковых станций



Домашнее задание

Давайте посмотрим вашу практику после лекции

- 1 Практика: домашнее задание (обязательное) с проверкой от преподавателя
- 2 Вопросы по домашнему заданию задавайте в чате учебной группы
- 3 Задачи можно сдавать по частям.
Зачёт по домашней работе ставят после того, как приняты все задачи



Задавайте вопросы Оставляйте обратную связь о занятии

Александр Нагернюк
Эксперт в области сетей и информационной безопасности

