нетология

Сеть и сетевые протоколы: **DHCP, PXE**

Артем
Поневин

Артем Поневин

Инженер

Luxoft

Артем Поневин

Предисловие

На этом занятии мы поговорим:

- что такое и для чего нужен протокол DHCP / BOOTP;
- о возможностях протокола DHCP;
- о содержимом пакетов, которые отправляет/принимает DHCP сервер;
- о настройках сервера/клиента DHCP.

По итогу занятия вы получите представление о протоколе DHCP и как с ним начать работу в сетях Linux.

План занятия

1. Предисловие
2. Основные понятия
3. Конфигурация и работа с DHCP
4. PXE
5. DHCPv6
6. Диагностика ввода-вывода в Linux
7. Итоги
8. Домашнее задание

Основные понятия

Что такое DHCP

DHCP (Dynamic Host Configuration Protocol, протокол динамической настройки узла) – это сетевой протокол прикладного уровня модели TCP/IP, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети.

Протокол описан в RFC2131 в 1997 г.

Работает на 67/68 портах поверх UDP.

DHCP является расширением и дополнением протокола BOOTP.

BOOTP

BOOTP (BOOTSTRAP PROTOCOL) — сетевой протокол, используемый для автоматического получения клиентом IP-адреса (обычно во время загрузки компьютера). Разрабатывался для работы с бездисковыми станциями.

Клиент отправляет широковещательное сообщение UDP с запросом загрузочной информации. Сервер возвращает клиенту его IP-адрес и, при необходимости, местоположение файла загрузки. С помощью протокола пересылки файлов TFTP клиент загружает в собственную память необходимое программное обеспечение и начинает работу.

BOOTP определён в RFC951.

TFTP

TFTP (Trivial File Transfer Protocol, простой протокол передачи файлов) — 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.

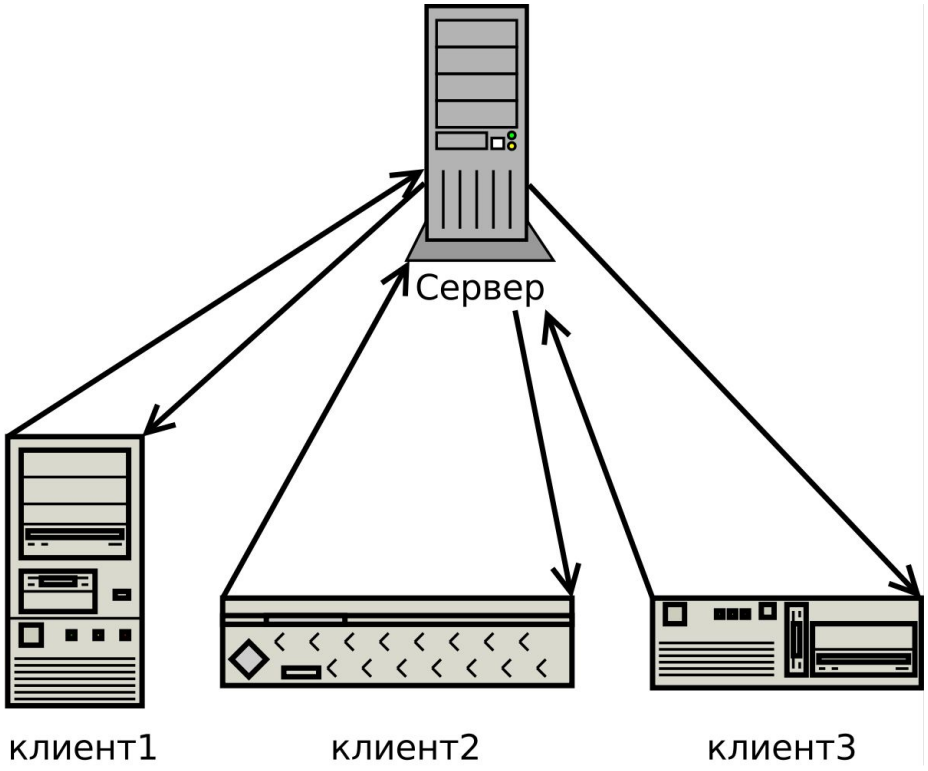
Уровень на модели OSI

DHCP работает на прикладном уровне.

OSI Model	TCP/IP Model	Protocols
Application layer	Application Layer	DNS, DHCP, FTP, HTTP, IMAP, LDAP, NTP, POP3
Presentation Layer		JPEG, MIDI, MPEG, TIFF
Session Layer		NrtBIOS, NFD, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP and UDP
Network Layer	Internet Layer	ICMP, IGMP, Ipsec, IPv6, IPX
Data Link Layer	Link Layer	ARP, ATM, CDP, FDDI, Frame-Relay, HDLC, PPP, STP, Token ring
Physical Layer		Ethernet, DSL, ISDN, Bluetooth

Архитектура DHCP

Работа DHCP организована по клиент-серверной модели, т.е. в работе протокола задействован DHCP-клиент и DHCP-сервер.



Источник изображения

Механизмы выделения IP-адресов сервером DHCP

- динамическое присвоение – IP-адрес выдается сервером по общим правилам на ограниченное время;
- автоматическое назначение статических адресов – IP-адрес выдается сервером на основании MAC-адреса клиента. База соответствий ведется в конфигурационных файлах сервера системным администратором;
- ручной режим работы DHCP-сервера – IP-адрес выдается вручную системным администратором.

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

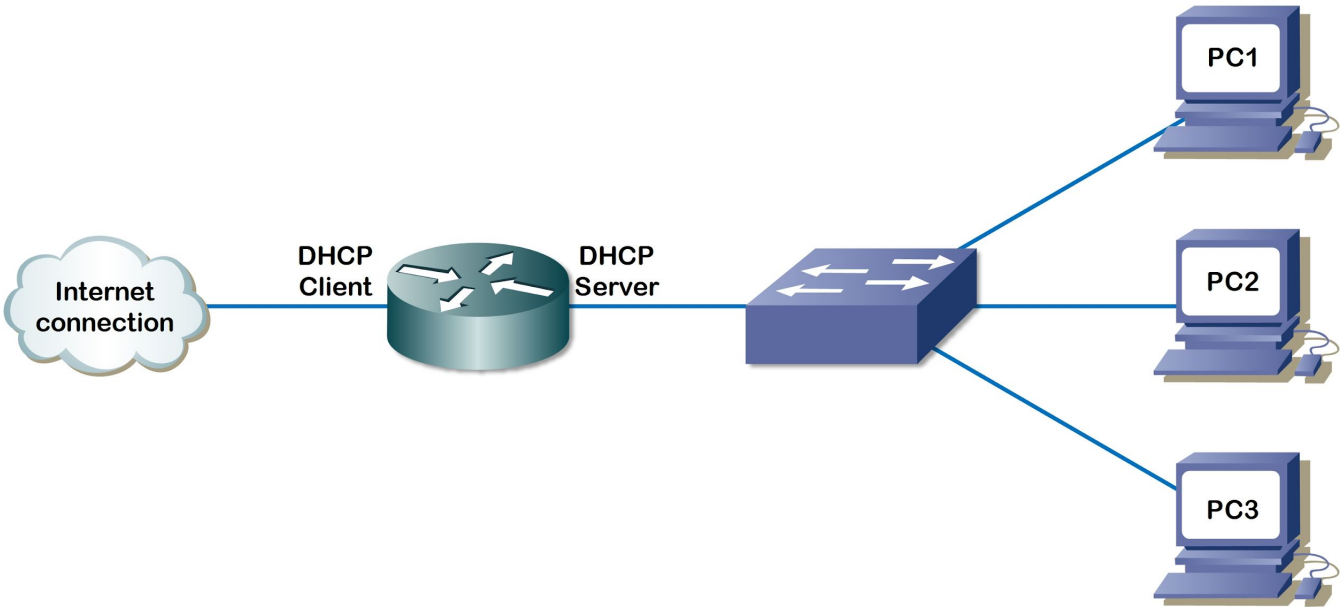
Установка DHCP сервера Ubuntu 18 LTS

- 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

Конфигурирование и работа с DHCP

Настройка DHCP-сервера

DHCP-сервер служит для упрощения добавления новых устройств в сеть. Каждый домашний Wi-Fi роутер имеет встроенный DHCP сервер и производит все настройки автоматически.



Источник изображения

Термины DHCP

- Scope (область) – диапазон IP-адресов, из которого сервер будет предлагать адреса клиенту в аренду;
- Exclusion range (исключаемый диапазон)– диапазон IP-адресов, которые не могут быть назначены клиенту;
- Lease (аренда) – период, в течение которого клиент может использовать IP-адрес;
- Reservation (резервирование) – закрепление IP адреса за конкретным устройством;
- Address pool (пул адресов) – свободные (незадействованные) IP-адреса, готовые к выдачи клиентам.

Виды DHCP сообщений

Источник изображения

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			

DHCPDISCOVER

DHCPDISCOVER – клиент отправляет в сеть широковещательный запрос для обнаружения DHCP-сервера;

- IP-адрес источника — 0.0.0.0;
- IP-адрес назначения — 255.255.255.255;
- MAC-адрес назначения — FF-FF-FF-FF-FF-FF.

DHCPOFFER

Получив запрос от клиента, сервер определяет конфигурацию в соответствии с серверными настройками, резервирует IP адрес и отправляет конфигурацию клиенту.

DHCPREQUEST

В сети может быть несколько DHCP-серверов, поэтому клиент выбирает одну из конфигураций, предложенных серверами, и отправляет запрос на эту конфигурацию широковещательно, чтобы другие сервера знали что их предложение отклонено.

DHCPACK

Получив запрос на конфигурацию, сервер отправляет клиенту подтверждение.

После этого обмен сообщениями закончен, и клиент должен применить полученные настройки.

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.

Обновление аренды IP адреса

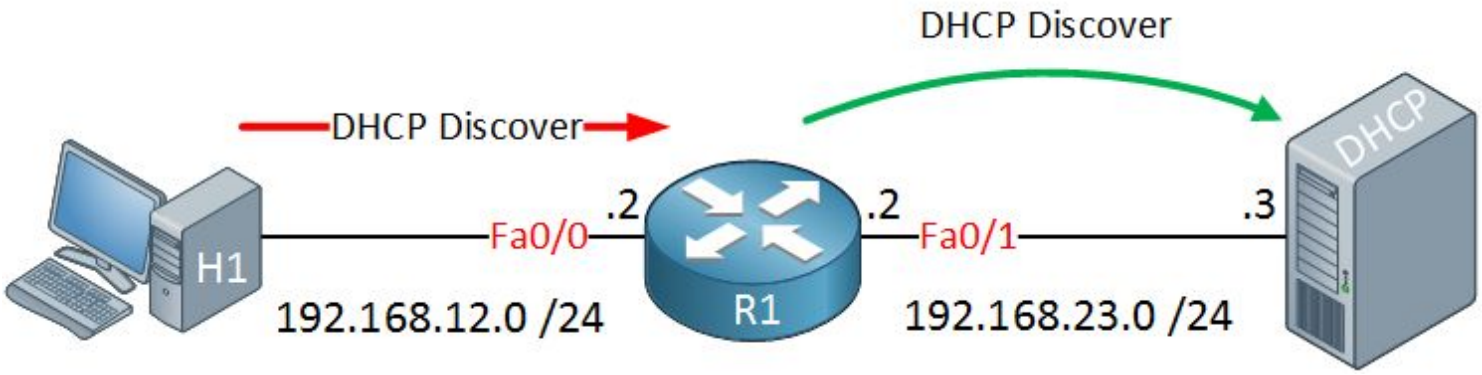
IP-адреса выдаются сервером DHCP на время, заданное в настройках сервера (от минут до месяца). После завершения половины времени аренды клиент пытается обновить аренду.

- RENEWING – клиент отправляет запрос на продление аренды. Сервер отвечает DHCPACK с подтверждением продолжения аренды и обновленными параметрами. В случае отказа от продолжения аренды сервер отправляет DHCPNACK, и клиент начинает инициализацию заново.
- REBINDING – при неполучении ответа клиент пытается продлить аренду через широковещательные запросы. Если и это не выходит, клиент заново ищет DHCP-сервер.

DHCP relay agent

По умолчанию запросы DHCP работают в пределах широковещательного диапазона, т.е. до ближайшего маршрутизатора.

➡ В случае если нужно отправлять DHCP пакеты в другие сети, необходимо настроить DHCP relay агента. Такую возможность чаще всего предоставляют маршрутизаторы.



Источник изображения: networklessons.com

Опции DHCP

Помимо IP-адреса, DHCP сервер также может сообщать клиенту дополнительные параметры для работы в сети.

Количество опций зависит от реализации сервера.

Список опций можно посмотреть, например, здесь или man dhcp-options.

Некоторые используемые опции:

- 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;

Настройка DHCP клиента

Специфическая настройка DHCP клиента производится редко.

В общем случае настройки по умолчанию должны работать лучше всего.

Базовые проверки для RHEL-based ОС:

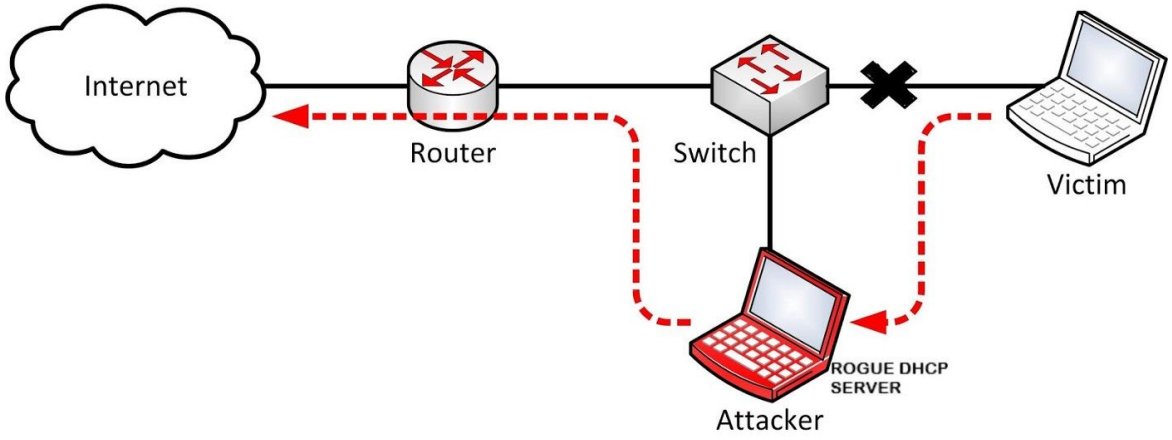
- /etc/sysconfig/network – убедитесь, что включена работа с сетью NETWORKING=yes;
- /etc/sysconfig/network-scripts/ifcfg-* – «DEVICE=eth0, BOOTPROTO=dhcp,ONBOOT=yes».

Безопасность DHCP

- Адреса могут быть исчерпаны злонамеренно при достаточном количестве запросов;
  - DHCP starvation;
  - Легитимные клиенты не могут получить настройки и подключиться к сети.
- Злоумышленник может установить свой DHCP сервер;
  - DHCP snooping;
  - Порты помечаются как доверенные и нет. Если на недоверенном порту появиться DHCP сервер, коммутатор заблокирует этот порт.
- ...

Безопасность DHCP

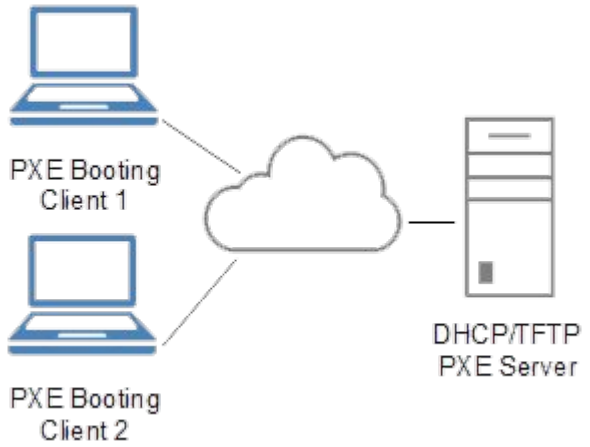
- DHCP сервер может быть подменен.
  - Rogue DHCP Server;
  - Клиента могут заставить работать через сетевые устройства злоумышленника, весь трафик может быть перехвачен.



PXE

Технология PXE

PXE (Preboot Execution Environment, среда предварительного исполнения) — технология, которая позволяет компьютеру загружаться и работать используя сетевую карту.



Загрузка компьютера

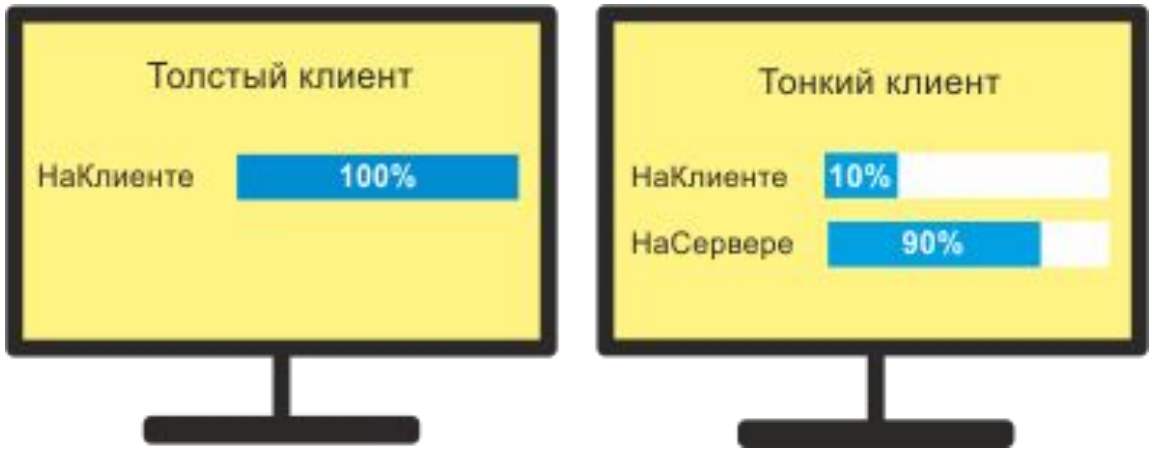
Т.е. для запуска компьютера достаточно иметь:

- Клиент, поддерживающий PXE – большинство современных компьютеров поддерживает PXE.
- DHCP-сервер – экземпляр сервера, который поддерживает необходимые опции и сконфигурированный для отправки ответов.
- TFTP-сервер – сервер, на котором размещены файлы загрузки.

Источник изображения: www.nix.ru

Тонкий и толстый клиенты

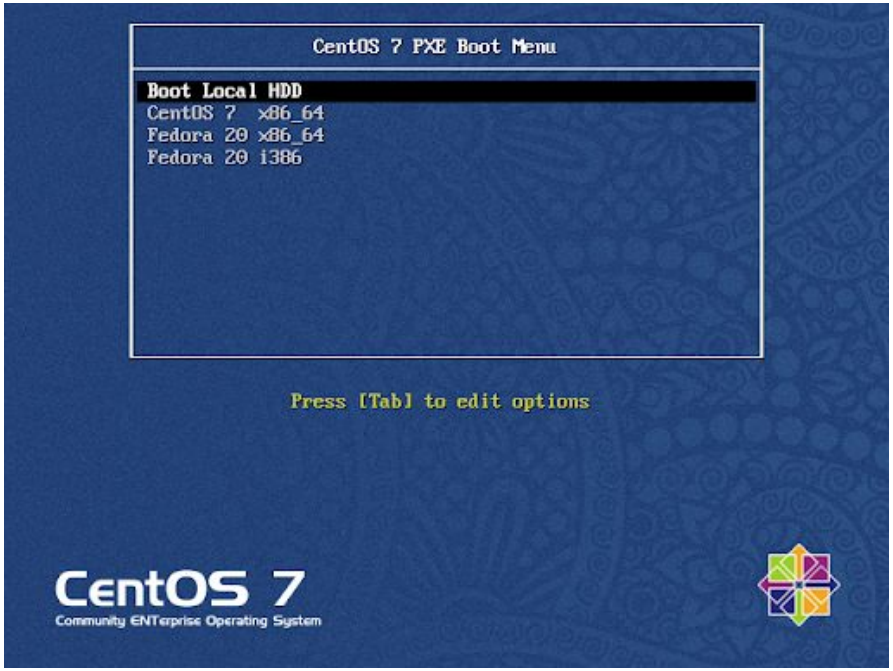
- Тонкий (thin client) – не может работать без сервера. Ограниченная функциональность.
- Толстый (rich client) – может работать и при обрыве связи с сервером. Многопользовательская работа.



Источник изображения: 1clenta.ru

Варианты использования

- Установка – можно использовать для установки ОС на компьютеры через сеть;
- Загрузка – для работы с ОС или с программным обеспечением через сеть.



Источник изображения: geekface.ca/

Перехват пакета DHCP и просмотр содержимого

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.

DHCPv6

DHCPv6

DHCPv6 — это новая версия протокола для работы в сетях на основе IPv6.

Протокол описан в RFC3315 (1997 г).

Работает на 546/547 портах поверх UDP.

DHCP НЕ является дополнением протокола BOOTP и использует отличные от DHCPv4 пакеты.

Итоги

Итоги

Сегодня мы рассмотрели:

- устройство протокола DHCP;
- возможности и настройки DHCP-серверов;
- конфигурацию бездисковых станций для работы по сети через PXE.

.

Домашнее задание

Домашнее задание

Давайте посмотрим ваше домашнее задание.

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Артем Поневин

Артем Поневин