

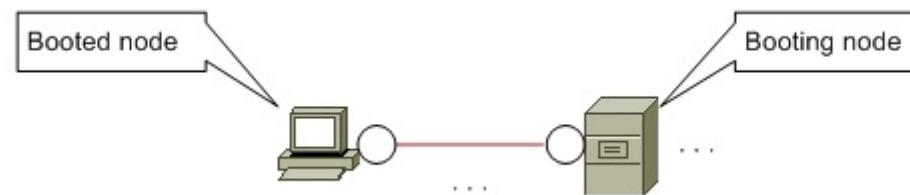
УДАЛЕННАЯ ЗАГРУЗКА

4.0.1.1

Термин *удаленная загрузка* (remote boot) означает, что по крайней мере ядро ОС некоторой станции загружается не с локальных накопителей, а по сети -- с удаленной станции.

Удаленная загрузка как правило используется для бездисковых пользовательских станций, не предназначенных для хранения информации (stateless). Каждый раз загружается «заготовка» ОС.

Таким образом, в состав сети с удаленной загрузкой входит как минимум две станции, которые обычно расположены в одном сегменте.



4.0.1.2

Для решения проблемы эмуляции системного диска используют два подхода:

1. Поддержка виртуального диска в памяти (RAM Drive).
2. Поддержка сетевого виртуального диска.

4.0.2.1

Существует специальное соглашение: если сетевому интерфейсу присвоен IP-адрес 0.0.0.0, то ему должен быть назначен динамический адрес.

4.0.3.1a

В настоящее время существуют несколько семейств технологий, связанных с удаленной загрузкой (используется клиент-серверная модель, включая поддержку со стороны BIOS/UEFI и загрузчиков Linux, в первую очередь выражены в соответствующих протоколах):

1. Для IPX: RPL (Remote Program Load) плюс ПО от Novell, Microsoft и другое.
2. Для IPv4: BOOTP (BOOTstrap Protocol) (RFC 951) -> DHCP (Dynamic Host Configuration Protocol) (RFC 2131) -> PXE (Preboot eXecution Environment) (открытый стандарт Intel) плюс ПО от 3COM, Intel, InCom -- Bootix, Microsoft, Rembo -- IBM, Venturcom -- Ardence -- Citrix, Qualystem -- Neoware -- HP, Youngzsoft и другое.
3. Для IPv6: DHCPv6 -> Netboot6 (PXE на базе IPv6, открытый стандарт UEFI Forum) плюс ПО от Citrix, Microsoft и другое.

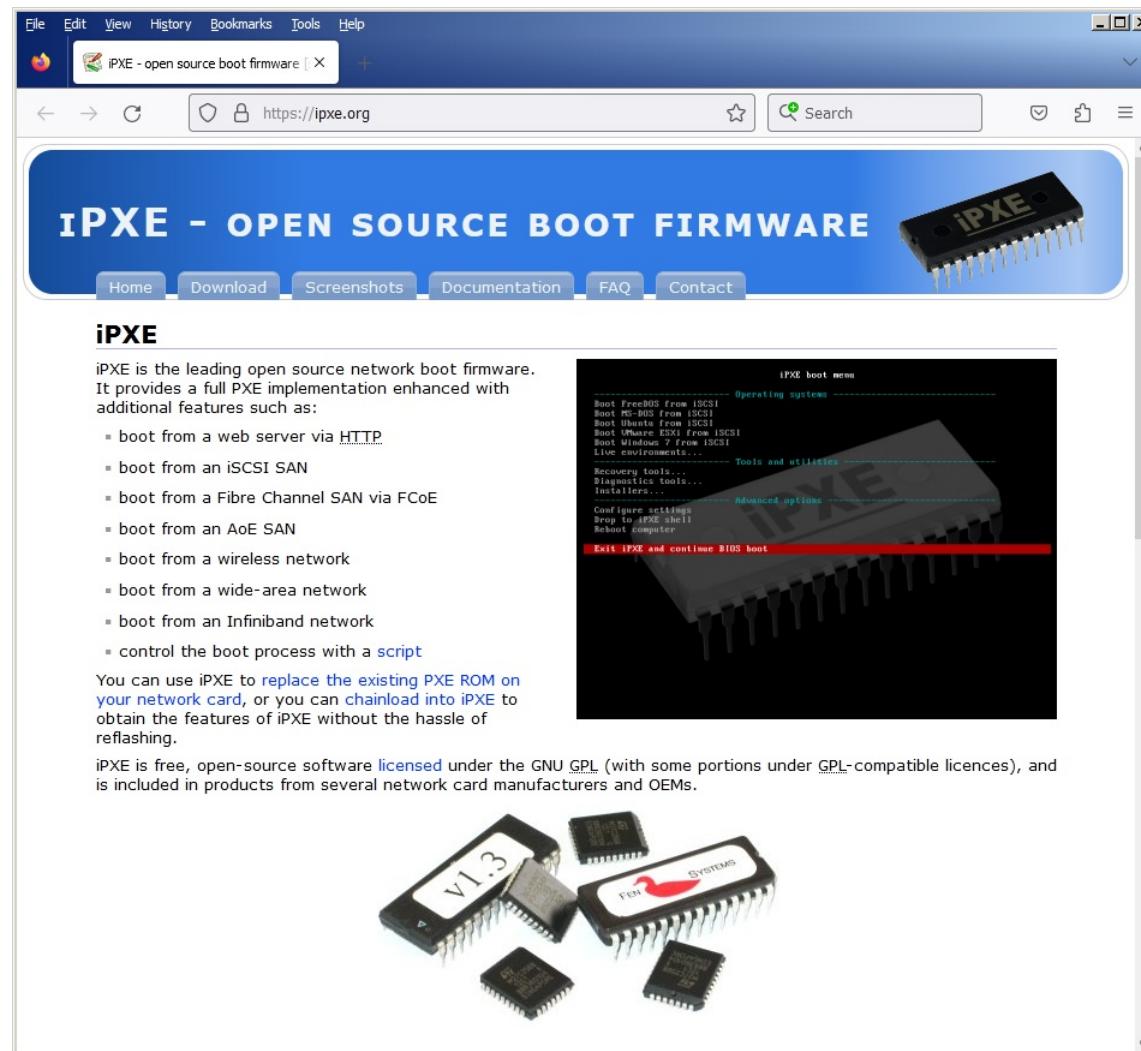
4.0.3.1b

4. Для IPv4/IPv6: iSCSI (internet SCSI) Boot и FCoE (Fibre Channel Over Ethernet) Boot плюс ПО от emBoot -- Double-take -- StarWind, Cisco, Microsoft, Intel и другое.

5. Для IPv4/IPv6: HTTP Boot плюс ПО от HPE, IBM, Dell и другое.

6. Для IPv4/IPv6: Прочие протоколы плюс как правило свободно распространяемое ПО, например, gPXE -- iPXE (альтернатива PXE, но поддерживает PXE плюс другие протоколы).

4.0.3.2



The screenshot shows a Firefox browser window with the URL <https://ipxe.org>. The page title is "iPXE - OPEN SOURCE BOOT FIRMWARE". The main content area features a large image of an iPXE chip with the word "iPXE" printed on it. Below the chip, there is a screenshot of the iPXE boot menu interface, which lists various boot options like "Boot FreeDOS from iSCSI" and "Boot Windows 7 from iSCSI". The menu also includes sections for "Operating systems", "Tools and utilities", and "Advanced options". At the bottom of the menu, a red bar displays the text "Exit iPXE and continue BIOS boot". To the left of the main content, there is a sidebar with links for "Home", "Download", "Screenshots", "Documentation", "FAQ", and "Contact". The main text area describes iPXE as the leading open source network boot firmware, mentioning its ability to boot from various network sources and control the boot process with scripts. It also notes that iPXE can be used to replace existing PXE ROMs or chainloaded into iPXE.

iPXE project site

4.0.4.1

Вплоть до появления UEFI на всех Intel-совместимых ПК и серверах (исключая платформу Itanium) использовался традиционный BIOS, в основе которого лежит BIOS для компьютерных систем с процессорами i8086.

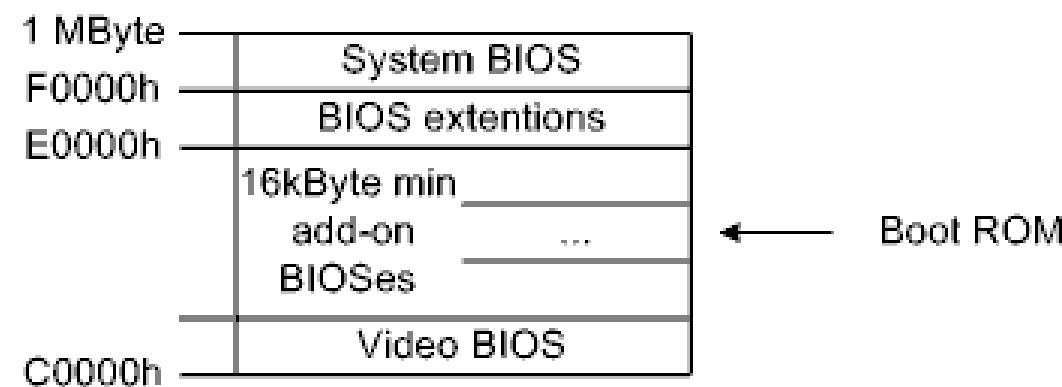
BIOS работает в реальном режиме с 16-тиразрядной адресацией и имеет совсем немного реализаций (AMI, Award, Phoenix и еще пару) с разными модификациями и «обертками».

Спустя десятилетия BIOS «оброс» расширениями (PnP BIOS Extension, PCI BIOS Extension и другие), но его суть от этого не изменилась.

В BIOS, еще при изначальной разработке, была заложена возможность включать сторонние дополнения -- add-on BIOSes (примерами могут служить BIOSes RAID-контроллеров и так далее).

Для обеспечения удаленной загрузки на стороне клиентской станции в состав add-on BIOSes необходимо включить boot ROM -- специальное загрузочное ПЗУ.

4.0.4.2



Добавление boot ROM

4.0.4.3

Поскольку удаленная загрузка связана с использованием ЛКС, физически boot ROM традиционно располагается на сетевом адаптере, хотя туда можно прошить произвольный программный код.

Микросхема boot ROM может быть припаяна к плате сетевого адаптера либо может быть установлена посредством разъема.

Если сетевой адаптер интегрирован на материнскую плату, то содержимое boot ROM как правило имеется и интегрировано в основной BIOS.

4.0.4.4

«Прошивку» boot ROMs готовят производители микросхем -- сетевых контроллеров.

Касательно IP, boot ROMs ориентированы только на IPv4, IPv6 не поддерживают. Иногда ориентированы на IPv4/RPL (Intel).

Первое поколение boot ROMs поддерживало только БООТР (например, TCP/IP BOOT-PROM от InCom, хотя TCP только в названии). Затем появились boot ROMs с поддержкой DHCP. Наконец, с поддержкой PXE и альтернативных протоколов.

Последняя и устоявшаяся версия стандарта PXE (2.1) допускает разбиение программного кода PXE на части (PXE split ROM): BC (Base-Code) -- обязательная, UNDI (Universal Network Driver Interface) -- должна быть по крайней мере одна, соответствующая данному сетевому интерфейсу, и BUSD (BUS/Device) -- нужна только для поддержки адаптера, подключаемого посредством CardBus. Части связаны, но являются отдельными add-on BIOSes.

Как правило в boot ROM на сетевом адаптере «прошиваются» полноценную поддержку PXE (либо iPXE, либо iSCSI Boot, либо FCoE Boot).

4.0.4.5a

После включения загружаемой станции выполняется так называемый POST (Power On Self Test).

При этом BIOS сканирует память в диапазоне C0000h -- EE000h (куда отображаются add-on BIOSes) с инкрементом, равным 2 kByte (2048 Byte), в поисках сигнатуры 55AAh, которая свидетельствует о наличии add-on BIOS.

Если сигнатура найдена, то третий байт, содержащий размер add-on BIOS в 512-тибайтовых страницах, используется для проверки контрольной суммы (код Sum16).

Если контрольная сумма равна нулю, то осуществляется вызов подпрограммы по адресу, расположенному со смещением +3 (четвертый байт). В случае с boot ROM, вызванный код используется для подмены обработчика прерывания 18h (ROM BASIC).

4.0.4.5b

После просмотра всего диапазона, BIOS выполняет инструкцию INT 18h (перезагрузка).

Затем, вернув управление, новый обработчик копирует основное содержимое boot ROM (loader) в оперативную память и передает ему управление.

Затем, загрузчик loader с помощью подпрограмм boot ROM загружает простейший сетевой протокол, получает код загрузчика bootstrap от загружающей станции и передает ему управление.

Дальнейшие действия зависят от реализации.

4.0.5.1

UEFI имеет более сложную структуру и намного больше «оберток» в сравнении с BIOS. При этом подразумевается поддержка даже сложных сетевых протоколов, в том числе необходимых для удаленной загрузки.

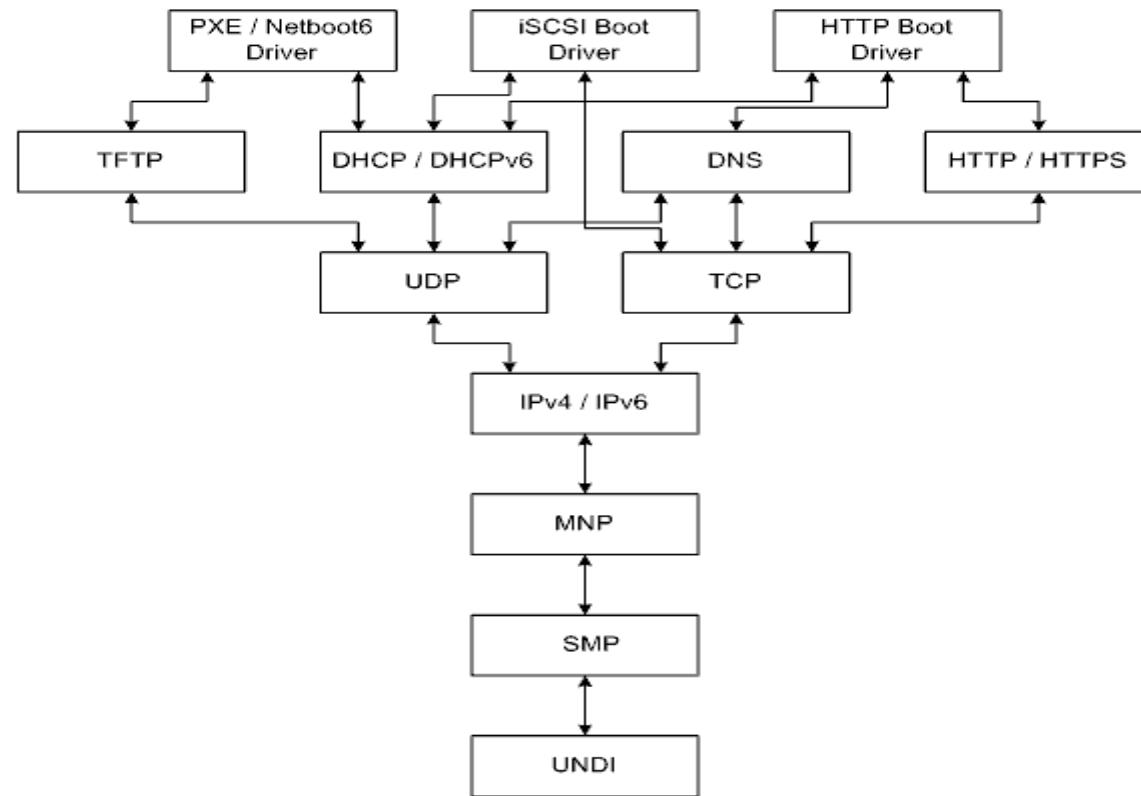
UEFI переходит в защищенный режим с 32-ух- либо 64-ехразрядной адресацией.

Сложность требует наличия ПЗУ соответствующего объема, что во времена BIOS было «роскошью».

Место add-on BIOSes заняли специальные UEFI-драйверы.

Для обеспечения удаленной загрузки от производителей сетевых контроллеров требуется только написание драйверов. Как правило это UNDI-драйверы, совместимые с UEFI API.

4.0.5.2



Где: MNP -- Managed Network Protocol, SNP -- Simple Network Protocol
(внутренние протоколы и интерфейсы UEFI для предоставления сеансов взаимодействия с сетевым интерфейсом и формирования пакетов соответственно).

4.0.5.3

Драйвер может быть как «прошит» в ПЗУ на плате сетевого адаптера, так и интегрирован в UEFI.

4.0.5.4

Типичные UEFI ориентированы на IPv4/IPv6 и поддерживает комплекс протоколов: PXE, Netboot6, iSCSI Boot, FCoE Boot, HTTP Boot, а также фильтрацию и аутентификацию.

4.0.6.1а

Первым протоколом, который массово использовали для динамического назначения IP-адресов, является BOOTP.

Как альтернативу BOOTP, для нахождения IP-адресов по MAC-адресам, изредка использовали протокол RARP (Reverse ARP) (RFC 903) -- в современных реализациях практически не поддерживается (как и его экспериментальные расширения, описанные в RFC 1931 под названием *dynamic RARP extensions*).

DHCP представляет собой расширение BOOTP.

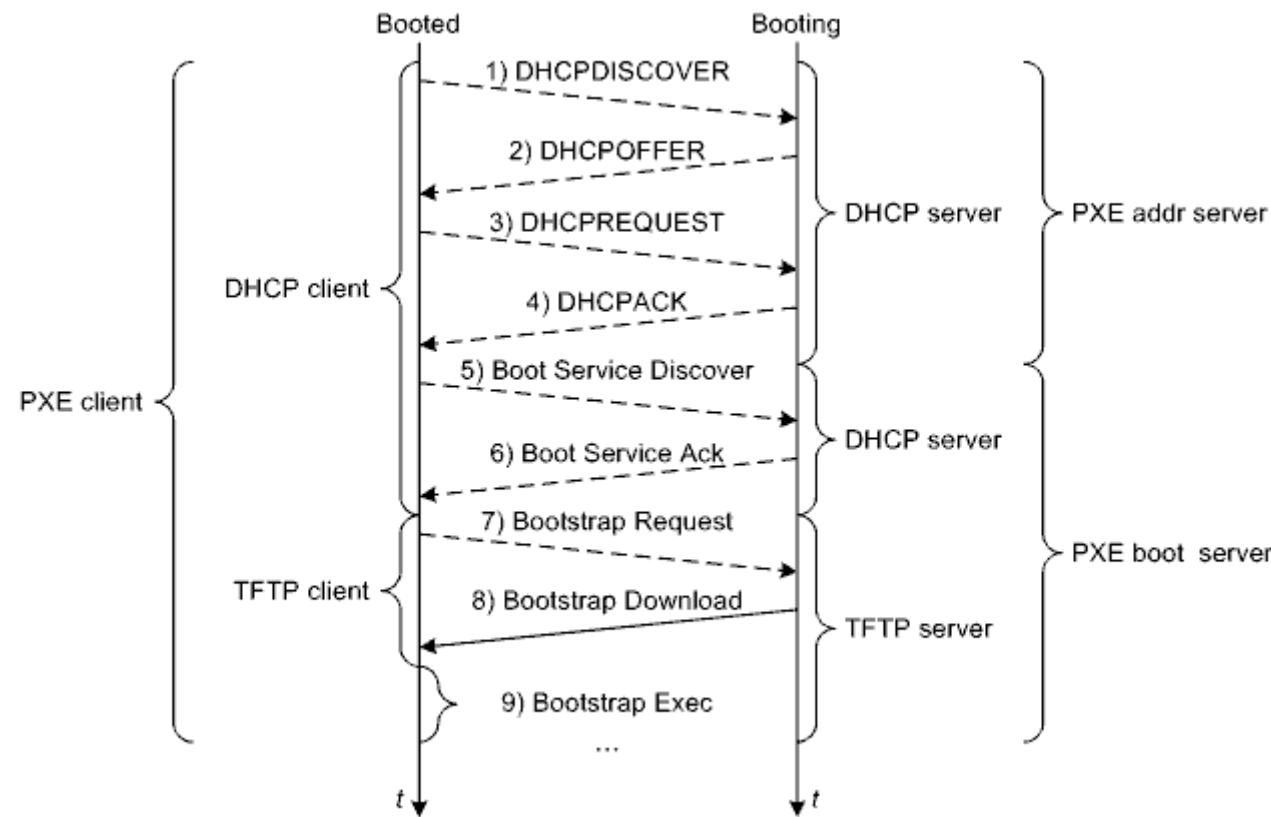
	BOOTP	DHCP
Открытость стандарта	Да	Да
Возможность обновления IP-адреса	Нет	Да (Lease Time)
Поддержка динамического пула IP-адресов	Нет	Да
Количество конфигурационных параметров (кроме IP-адреса)	Меньше (называют vendor extensions)	Больше (называют options)

4.0.6.1b

PXE представляет собой своеобразную надстройку над DHCP, формализующую три основные вещи:

1. Протокол взаимодействия клиентской станции с сервисами адресации и загрузочными сервисами.
2. Набор APIs, которые образуют «продвинутую» загрузочную среду на клиентской станции.
3. Структуру boot ROM.

4.0.7.1a



Клиент-серверное взаимодействие по протоколу PXE

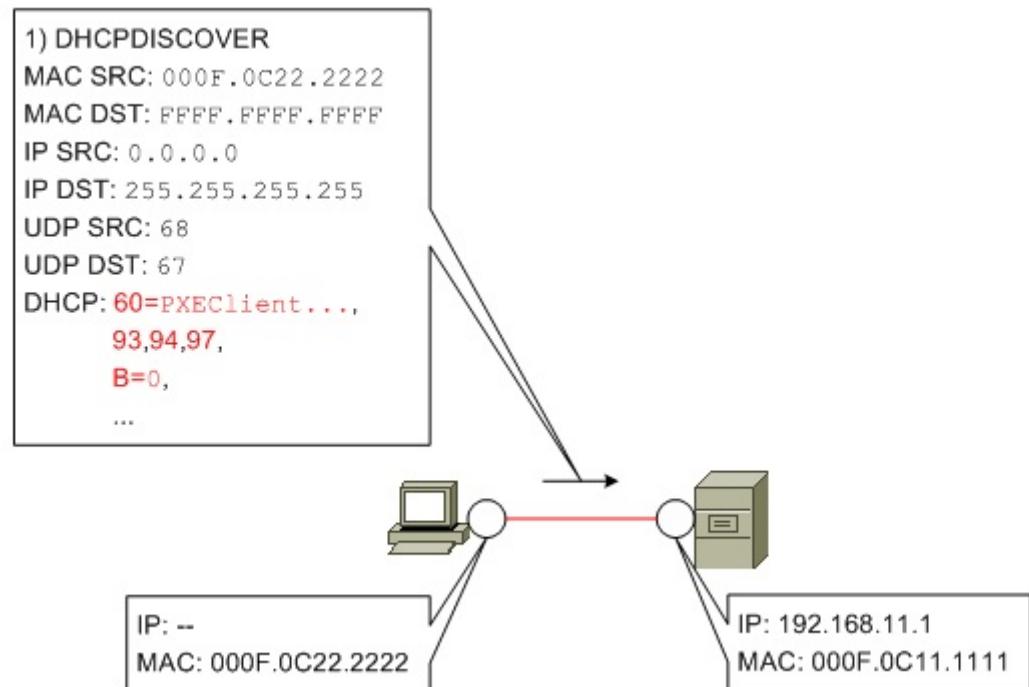
4.0.7.1b

1. DHCPDISCOVER -- DHCP-клиент в составе PXE-клиента посылает броадкаст-запрос с целями анонсирования своего «возникновения» и поиска сервиса адресации, коим является DHCP-сервер. Стандартный порт на стороне DHCP-сервера: UDP 67.

При этом ключевыми являются опции: 97 -- UUID/GUID-based Client Identifier (Universally/Globally Unique ID), 93 -- Client System Architecture, 94 -- Client Network Device Interface, 60 -- Class Identifier (в случае с PXE значение начинается с PXEClient).

Если DHCP-клиент по каким-либо причинам еще не готов полноценно обрабатывать юникаст-пакеты, он должен установить флаг B -- Broadcast Flag, так как форма ответной адресации выбирается исходя из значения этого флага.

4.0.7.1c



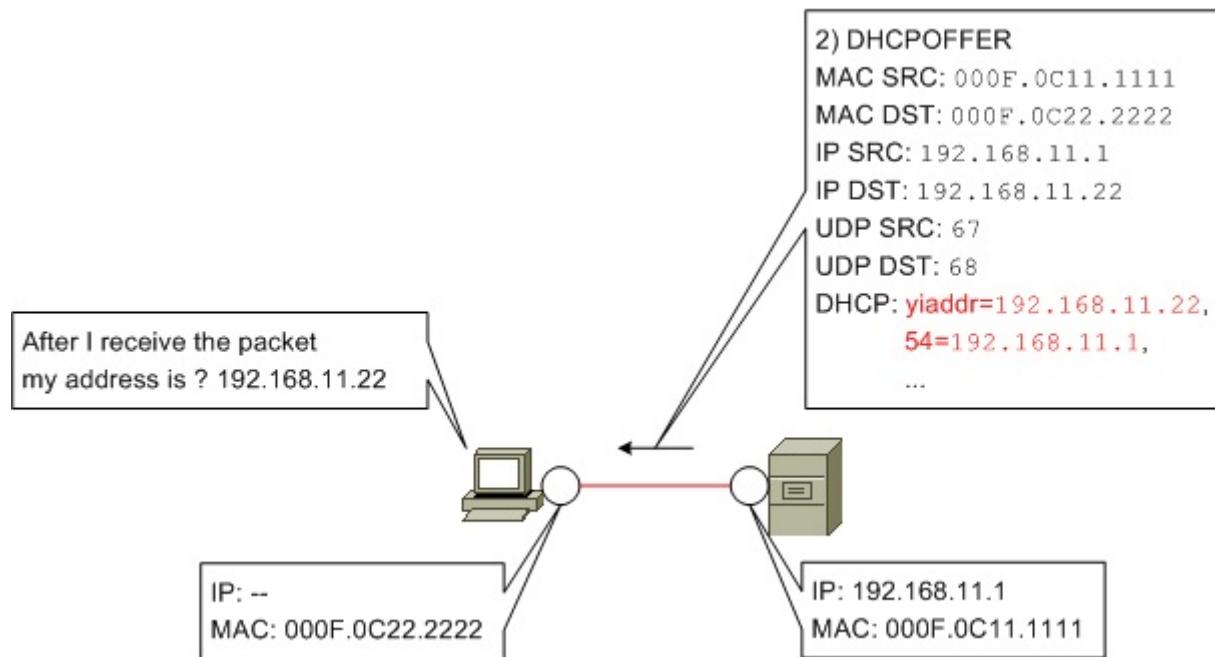
4.0.7.1d

2. DHCPOFFER -- DHCP-сервер сразу выдает DHCP-клиенту IP-адрес и в юникаст- либо броадкаст-форме отвечает о своей готовности. Стандартный порт на стороне DHCP-клиента: UDP 68.

При этом выданный IP-адрес DHCP-сервер указывает в поле yiaddr -- 'Your' (client) IP address, а свой IP-адрес указывает в опции 54 -- DHCP Server Identification.

В юникаст-случае выданный IP-адрес «вписывается» в пакет еще и как IP-адрес назначения.

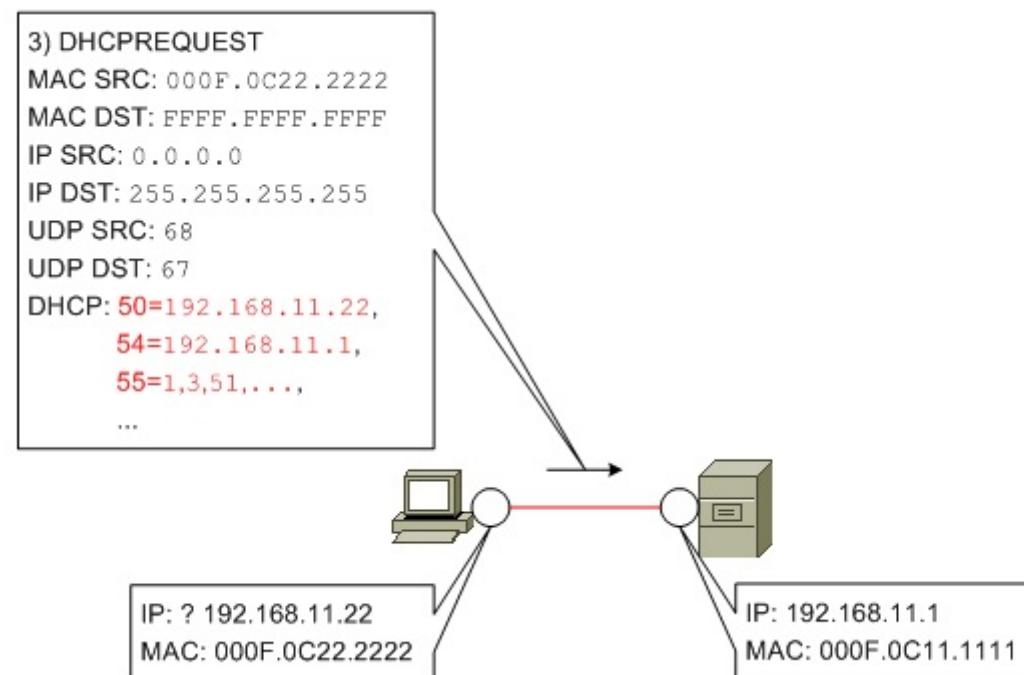
4.0.7.1e



4.0.7.1f

3. DHCPREQUEST -- DHCP-клиент, по-прежнему в бродкаст-форме, подтверждает, что он выбрал определенный DHCP-сервер, и параллельно собственно запрашивает IP-адрес и требующиеся ему конфигурационные параметры.

Выбранный DHCP-сервер отображен в опции 54. Другие ключевые опции: 50 -- Requested IP Address, 55 -- Parameter Request List.



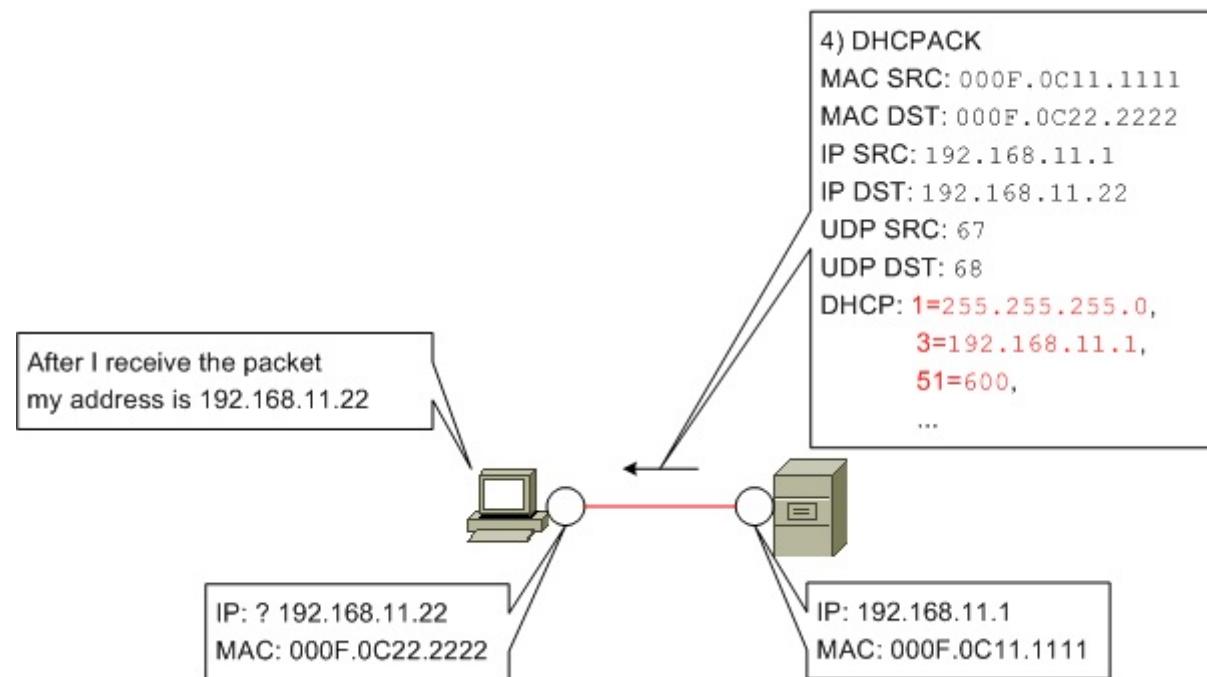
4.0.7.1g

Почему DHCPREQUEST именно в бродкаст-форме?

4.0.7.1h

4. DHCPACK -- DHCP-сервер в юникаст- либо броадкаст-форме подтверждает подтверждение и параллельно предоставляет значения всех предварительно сконфигурированных параметров из тех, что были запрошены.

Типичные опции: 1 -- Subnet Mask, 3 -- Router, 51 -- IP Address Lease Time и так далее (если в один пакет не помещаются, то передаются несколько пакетов).



4.0.7.1i

5. Boot Service Discover -- PXE-клиент посредством DHCP посылает запрос о предоставлении загрузочного сервиса. По сути аналогичен DHCPDISCOVER плюс DHCPREQUEST, но кодируется как DHCPREQUEST. Стандартные порты на стороне DHCP-сервера: UDP 67 (бродкаст), UDP 4011 (мультикаст-юникаст).

При этом параметры адресации должны были быть принудительно указаны при DHCPACK. Параметры адресации, а также все другие требующиеся параметры, являющиеся PXE-расширениями, выражаются как подопции опции 43 -- Vendor Specific. Ключевая подопция на данном шаге: 43 tag 8 -- PXE_BOOT_SERVERS.

6. Boot Service Ack -- DHCP-сервер, находящийся на стороне загрузочного сервиса, подтверждает предоставление услуг. Подтверждение кодируется как DHCPACK.

При этом ключевыми являются: поле file -- Boot File Name -- с названием файла -- загрузчика bootstrap и подопции опции 43, например, с параметрами протокола MTFTP (если используется MTFTP). Как альтернатива полю file, может использоваться опция 67 -- Boot File Name.

4.0.7.1j

7. Bootstrap Request -- TFTP-клиент в составе PXE-клиента посыпает запрос о предоставлении файла -- загрузчика bootstrap. Стандартный порт на стороне TFTP-сервера: UDP 69.

8. Bootstrap Download -- TFTP-клиент скачивает файл -- загрузчик bootstrap.

9. Bootstrap Exec -- загрузчик bootstrap исполняется.

4.0.7.2

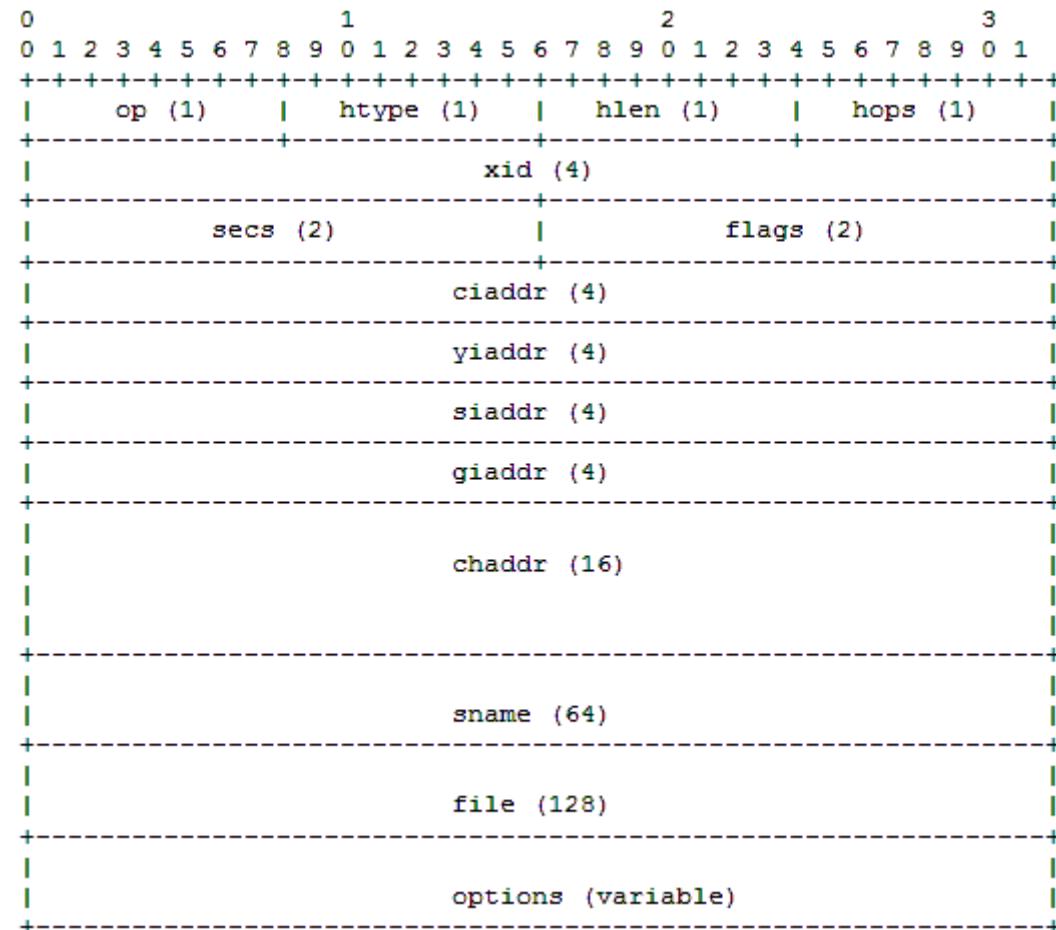
Четко видны две фазы взаимодействия: по протоколу DHCP и по протоколу TFTP. В общем случае сервисы DHCP и TFTP разделены.

Протокол BOOTP шаги 3 и 4 не предусматривает (только BOOTREQUEST и BOOTREPLY).

Шаги 5 и 6 нужны если TFTP-сервер физически не совпадает с DHCP-сервером, что встречается редко. Поэтому они обычно совмещаются с шагами 3 и 4.

4.0.7.3

По большому счету, в DHCP-заголовке передается только пара конфигурационных параметров, в первую очередь, IP-адрес. Остальные параметры передаются в виде DHCP-опций.



DHCP message [RFC]

4.0.7.4

Tag	Name	Data Length	Meaning	Reference
0	Pad	0	None	[RFC2132]
1	Subnet Mask	4	Subnet Mask Value	[RFC2132]
2	Time Offset	4	Time Offset in Seconds from UTC (note: deprecated by 100 and 101)	[RFC2132]
3	Router	N	N/4 Router addresses	[RFC2132]
4	Time Server	N	N/4 Timeserver addresses	[RFC2132]
5	Name Server	N	N/4 IEN-116 Server addresses	[RFC2132]
6	Domain Server	N	N/4 DNS Server addresses	[RFC2132]
7	Log Server	N	N/4 Logging Server addresses	[RFC2132]
8	Quotes Server	N	N/4 Quotes Server addresses	[RFC2132]
9	LPR Server	N	N/4 Printer Server addresses	[RFC2132]
10	Impress Server	N	N/4 Impress Server addresses	[RFC2132]
11	RLP Server	N	N/4 RLP Server addresses	[RFC2132]
12	Hostname	N	Hostname string	[RFC2132]
13	Boot File Size	2	Size of boot file in 512 byte chunks	[RFC2132]
14	Merit Dump File	N	Client to dump and name the file to dump it to	[RFC2132]
15	Domain Name	N	The DNS domain name of the client	[RFC2132]
16	Swap Server	N	Swap Server address	[RFC2132]
17	Root Path	N	Path name for root disk	[RFC2132]
18	Extension File	N	Path name for more BOOTP info	[RFC2132]
19	Forward On/Off	1	Enable/Disable IP Forwarding	[RFC2132]
20	SrcRte On/Off	1	Enable/Disable Source Routing	[RFC2132]
21	Policy Filter	N	Routing Policy Filters	[RFC2132]
22	Max DG Assembly	2	Max Datagram Reassembly Size	[RFC2132]
23	Default IP TTL	1	Default IP Time to Live	[RFC2132]
24	MTU Timeout	4	Path MTU Aging Timeout	[RFC2132]
25	MTU Plateau	N	Path MTU Plateau Table	[RFC2132]
26	MTU Interface	2	Interface MTU Size	[RFC2132]
27	MTU Subnet	1	All Subnets are Local	[RFC2132]
28	Broadcast Address	4	Broadcast Address	[RFC2132]
29	Mask Discovery	1	Perform Mask Discovery	[RFC2132]
30	Mask Supplier	1	Provide Mask to Others	[RFC2132]
...				
255	End	0	None	[RFC2132]

DHCP options [IANA]

4.0.7.5

Тип DHCP-сообщения определяется из значения опции 53 -- DHCP Message Type. Кроме уже упомянутых DHCPDISCOVER, DHCPOFFER, DHCPREQUEST и DHCPACK, есть еще:

DHCPDECLINE -- отказ со стороны клиента от IP-адреса, если клиент выявил, что этот IP-адрес уже используется.

DCHPNAK -- отказ со стороны сервера, если запрос DHCPREQUEST неправильный.

DHCPRELEASE -- сообщение от клиента к серверу об освобождении выделенных до этого DHCP-ресурсов, если эти ресурсы больше не нужны.

DHCPIINFORM -- запрос от клиента к серверу о некоторых конфигурационных параметрах, если собственно IP-адрес назначен «вручную».

DHCPFORCERENEW (RFC 3203) -- сообщение от сервера к клиенту о принудительном начале повторного взаимодействия по DHCP.

Остальные типы имеют отношение к опциональному расширению DHCP Leasequery (RFC 4388), позволяющему сторонней станции (не клиенту и не серверу) запрашивать информацию о DHCP-конфигурации.

4.0.7.6

По истечении времени валидности IP-адрес обновляется посредством целенаправленных (юникаст) DHCPREQUEST и DHCPACK.

4.0.7.7

Для пересылки файлов используется упрощенный и менее надежный вариант протокола FTP, называемый TFTP (Trivial FTP) (RFC 1350).

Существуют также более или менее модифицированные версии TFTP от различных разработчиков с разной степенью стандартизации, например, MTFTP (Multicast TFTP).

Существуют особые соглашения об использовании расширений загружаемых файлов (.Р и другие).

Первичный загрузчик bootstrap с помощью РХЕ может «подгружать» вторичные.

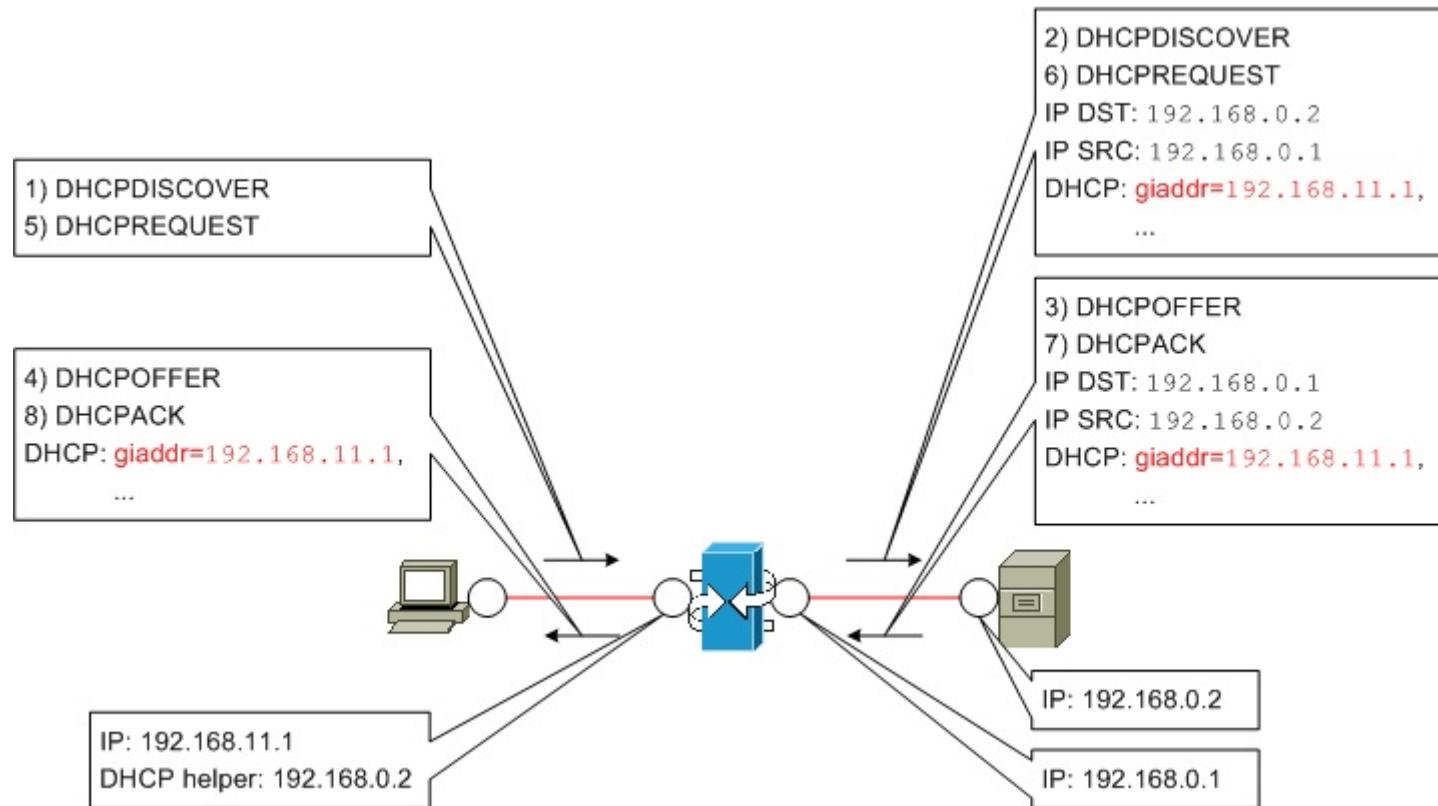
BOOTP, DHCP и TFTP используют транспорт UDP.

4.0.7.8a

DHCP relay позволяет разместить DHCP-клиент и DHCP-сервер в разных сегментах. При конфигурировании «обращенного» к DHCP-клиенту интерфейса шлюза, который и выполняет функцию DHCP relay, указывают IP-адрес DHCP-сервера, на который нужно перенаправлять запросы, то есть DHCP helper. При перенаправлении в поле giaddr -- relay agent IP address заносится IP-адрес DHCP relay, что в дальнейшем позволит DHCP-серверу определить «происхождение» запроса. Если DHCP-серверу для выдачи IP-адреса требуется дополнительная информация от DHCP relay, то она может быть передана посредством опции 82 -- Relay Agent Information.

DHCP proxy (в стандартах не выделяют) терминологически отличается тем, что работает прозрачно -- DHCP-клиент вместо IP-адреса DHCP-сервера «видит» IP-адрес DHCP proxy.

4.0.7.8b



4.0.8.1

Типичные реализации DHCP-клиентов кроме IP-адреса по умолчанию запрашивают и набор основных DHCP-опций.

DHCP-клиент в Windows запускается автоматически и активизируется при отсутствии статического IP-адреса.

Интерфейс для явного конфигурирования не предусмотрен.

Если назначить IP-адрес с помощью протокола DHCP не удалось, то назначается случайный IP-адрес -- Link Local.

4.0.8.2

На загружающей станции должны быть установлены и настроены как минимум два сервиса:

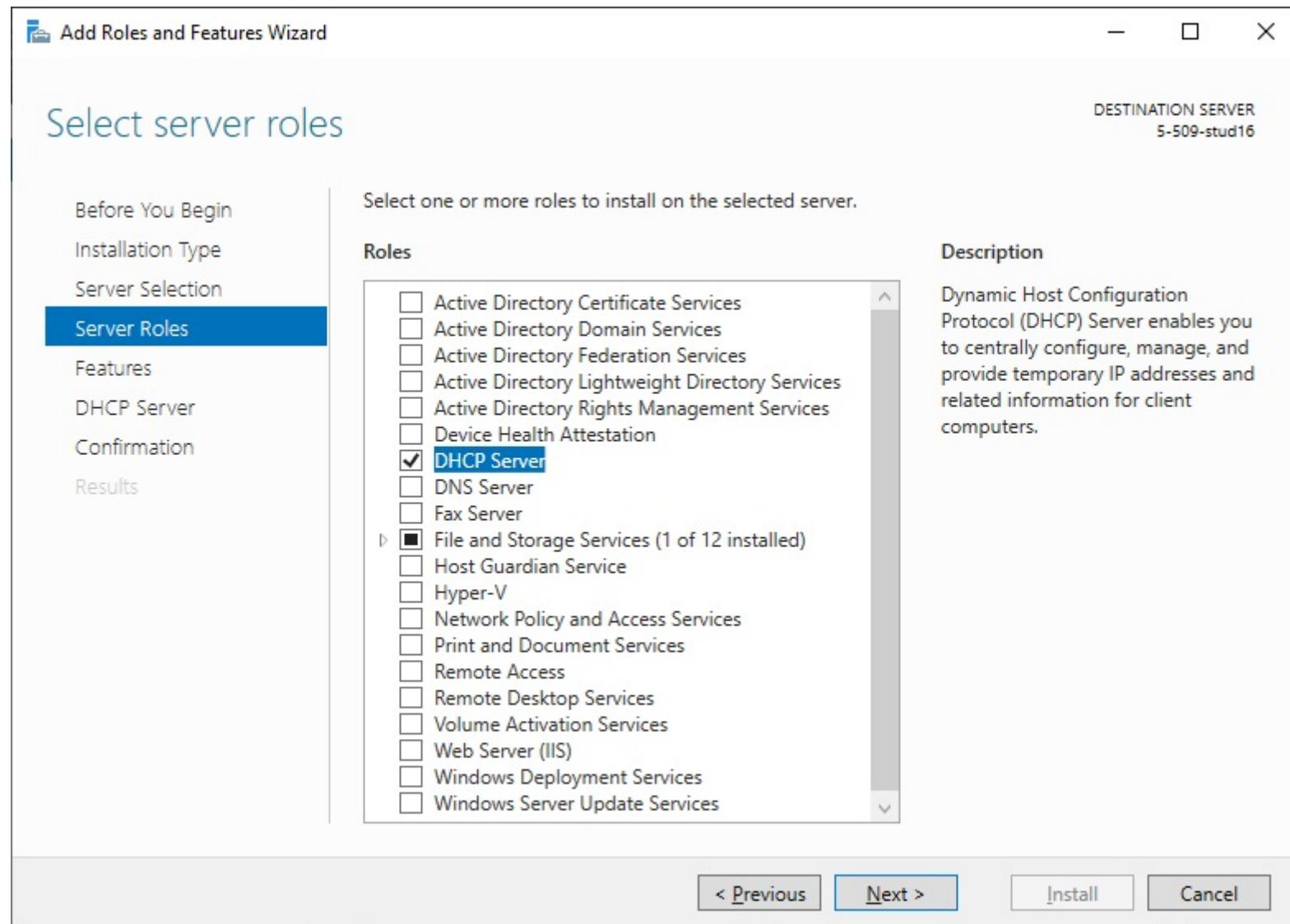
1. DHCP либо ему подобный.
2. TFTP либо ему подобный.

В серверных редакциях Windows имеется возможность установить собственный сервис DHCP. Начиная с Server 2008, предусмотрена роль DHCP Server. В Server 2003 R2 был компонент Dynamic Host Configuration Protocol (DHCP). Для конфигурирования используют оснастку DHCP (dhcpmgmt.msc).

Однако, сервис TFTP как отдельный полноценный компонент не поддерживается.

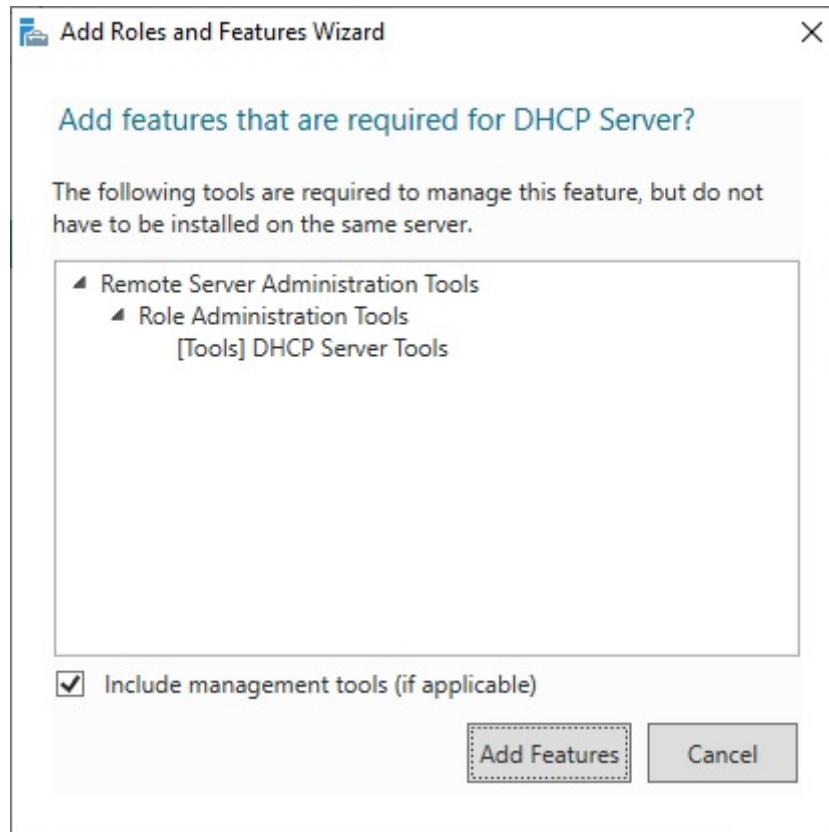
Поэтому для организации удаленной загрузки обычно используют стороннее, более «полноценное», ПО.

4.0.8.3a



Установка сервиса DHCP в Windows Server 2016/2019/2022

4.0.8.3b



4.0.8.3c

The screenshot displays two windows of the Windows Server 2016/2019/2022 DHCP Management Console. Both windows show the same configuration for a scope named 'Scope [192.168.1.192] test'.

Top Window (Actions: Address Pool):

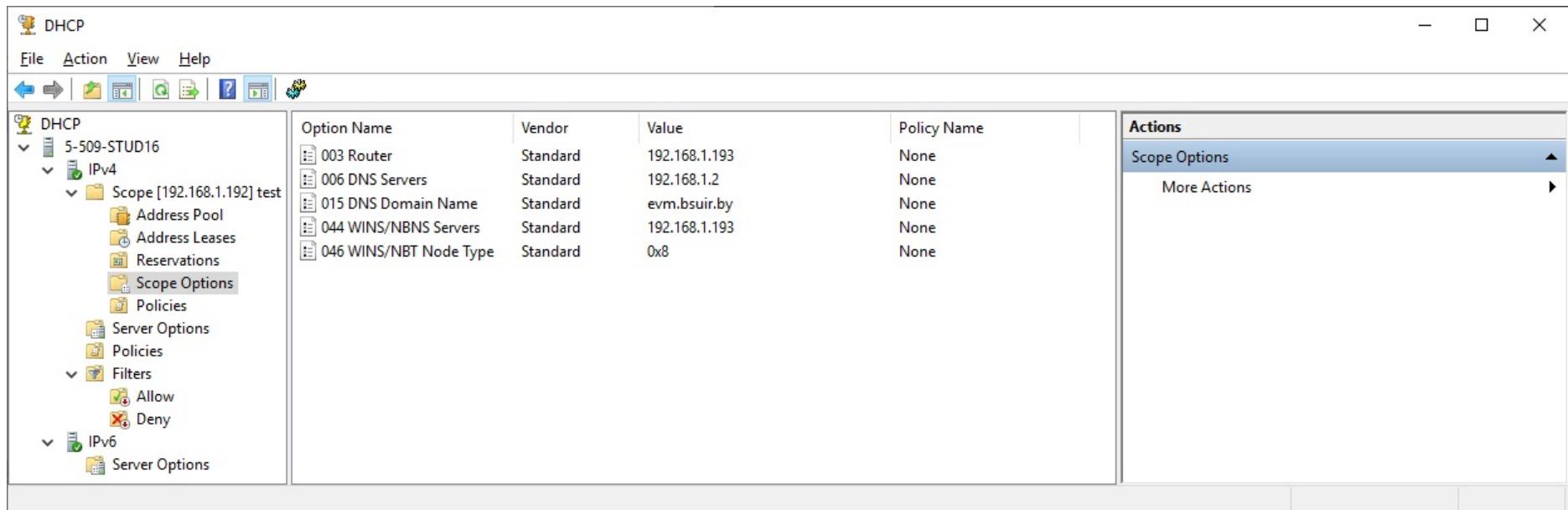
- IPv4 Scope [192.168.1.192] test:**
 - Address Pool:** Start IP Address: 192.168.1.194, End IP Address: 192.168.1.197, Description: Address range for distribution.
 - Filters:** Allow (selected), Deny.
- IPv6:** Server Options.

Bottom Window (Actions: Address Leases):

- IPv4 Scope [192.168.1.192] test:**
 - Address Leases:** Client IP Address: 192.168.1.194, Name: (empty), Lease Expiration: 31.03.2020 14:23:07, Type: DHCP, Unique ID: 636973636..., Description: (empty).
- IPv6:** Server Options.

Оснастка DHCP в Windows Server 2016/2019/2022

4.0.8.3d



Оснастка DHCP в Windows Server 2016/2019/2022

4.0.9.1

DHCP-клиент в Linux представлен демоном dhclient.

Для активизации dhclient (при загрузке) необходимо отредактировать соответствующую строку в соответствующем конфигурационном файле.

Для «тонкой» настройки дополнительно редактируют стандартный конфигурационный файл etc/dhclient.conf.

4.0.9.2

/etc/sysconfig/network-scripts/ifcfg-eth1 (**ветви Red Hat и SUSE**):

```
...
BOOTPROTO=dhcp
```

```
...
```

/etc/network/interfaces (**ветвь Debian**):

```
...
iface eth1 inet dhcp
```

```
...
```

/etc/dhclient.conf:

```
timeout 60;
reject 192.168.11.1;
```

```
interface "eth0" {
    send dhcp-lease-time 3600;
    require routers, subnet-mask, domain-name-servers;
}
```

Примеры настройки DHCP в конфигурационных файлах Linux

4.0.9.3

В Linux используют демоны bootpd и dhcpcd со стандартными конфигурационными файлами /tftpboot/bootptab и /etc/dhcpcd.conf соответственно.

А также демон tftpd, который не имеет конфигурационного файла (все что ему требуется -- это указание рабочего каталога при запуске, в качестве рабочего каталога принято использовать /tftpboot).

4.0.9.4

```
ether:\n  :hn:sm=255.255.255.224:vm=rfc1048:ht=ethernet:gw=192.168.11.193\n\nuser1:\\n  :tc=ether:ha=000CF1BF703F:ip=192.168.11.201:hd=/tftpboot:bf=mba.X:\\n  ...\\n
```

Пример файла bootptab

4.0.9.5

```
subnet 192.168.11.192 netmask 255.255.255.224 {  
    range 192.168.11.194 192.168.11.197;  
    option subnet-mask 255.255.255.224;  
    option routers 192.168.11.193;  
    option bootfile-name "/tftpboot/pxelinux.0";  
    option domain-name "evm.bsuir.by";  
    option domain-name-servers 192.168.11.3;  
    option netbios-name-servers 192.168.11.193;  
    default-lease-time 3600;  
    host user1 {  
        hardware ethernet 00:0c:f1:bf:70:3f;  
        fixed-address 192.168.11.201;  
    }  
    ...  
}
```

Пример файла `dhcpd.conf`

4.0.10.1

Запуск DHCP-клиента в Cisco IOS происходит с помощью соответствующего аргумента команды `ip address`.

Перед запуском DHCP-клиента можно настроить.

4.0.10.2

```
Router(config)#interface fa0
Router(config-if)#ip dhcp client lease 0 1 0 !Дни часы минуты
Router(config-if)#no ip dhcp client request tftp-server-address
Router(config-if)#ip address dhcp
Router(config-if)#exit
```

4.0.10.3

На маршрутизаторах Cisco поддерживается сервис DHCP. По умолчанию этот сервис запущен, для останова используют команду `no service dhcp`.

DHCP helper указывают командой `ip helper-address`.

Для просмотра состояния сервиса DHCP используют команды группы `show ip dhcp`: `show ip dhcp binding`, `show ip dhcp conflict`, `show ip dhcp pool`, `show ip dhcp server statistics` и другие.

Командой `tftp-server` (первым вводом) можно запустить сервис TFTP, однако маршрутизатор Cisco не предназначен для использования в качестве TFTP-сервера (как аргумент указывают путь к одному разрешаемому для пересылки файлу, сколько файлов -- столько раз нужно вводить команду).

4.0.10.4

```
Router(config)#ip dhcp excluded-address 192.168.11.193 !Исключаемые адреса

Router(config)#ip dhcp pool EXAMPLE-DHCP-DYNAMIC-POOL
Router(dhcp-config)# !Режим конфигурирования DHCP-пула
Router(dhcp-config)#network 192.168.11.192 255.255.255.224 !Вся подсеть
Router(dhcp-config)#default-router 192.168.11.193
Router(dhcp-config)#bootfile ardbp32.bin
Router(dhcp-config)#lease 0 4 !Минуты не указаны
Router(dhcp-config)#domain-name evm.bsuir.by
Router(dhcp-config)#dns server 192.168.11.3
Router(dhcp-config)#netbios-name-server 192.168.11.193
Router(dhcp-config)#option 19 hex 01 !Пример приватной DHCP-опции
Router(dhcp-config)#exit
```

4.0.10.5

```
Router(config)#ip dhcp pool EXAMPLE-DHCP-STATIC-POOL
```

```
...
```

```
Router(dhcp-config)#origin file flash:dhcp-static1
```

```
Router(dhcp-config)#exit
```

Файл dhcp-static1:

```
*time* Jan 22 2012 03:33 PM
```

```
*version* 2
```

!IP address	Type	Hardware address	Lease expiration
192.168.11.201/27	<u>1</u>	000c.f1bf.703f	Infinite !Это Ethernet

```
...
```

```
*end*
```

4.0.10.6

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                  Hardware address/
                  User name
192.168.11.195    0100.1b21.228e.72    Mar 31 2015 12:39 PM  Automatic
```

```
Router#show ip dhcp pool
```

```
Pool EXAMPLE-DHCP_DYNAMIC_POOL :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                  : 30
Leased addresses                 : 1
Pending event                    : none
1 subnet is currently in the pool :
Current index           IP address range          Leased addresses
192.168.11.193       192.168.11.193 - 192.168.11.222     1
```

