

Клонирование компьютеров в локальной сети с использованием свободного программного обеспечения

Н.В. Касаткин, А.О. Сергеев

Администрирование большого количества современных компьютеров невозможно без использования метода клонирования. В государственных учреждениях применение коммерческих систем клонирования нецелесообразно и функционально не оправдано. В данной работе предложен и описан метод улучшения существующей открытой технологии клонирования, позволяющий интегрировать систему в локальную сеть без внесения изменений в существующие службы.

Ключевые слова: локальные сети, обработка данных, передача данных, сетевые технологии, клонирование, свободное программное обеспечение.

Введение

Администрирование большого числа современных компьютеров, объединённых в локальную сеть, сопряжено с большими трудозатратами со стороны системных администраторов. Помимо первоначальной установки операционной системы, необходимо регулярно обновлять набор программного обеспечения на всех или части компьютеров. Производители операционных систем (ОС) и программного обеспечения (ПО) предлагают разнообразные методы и программы по автоматизации установки и обновления своих продуктов. Но часто эти подходы оказываются неэффективными, особенно, когда на компьютерах установлено больше одной ОС или используется широкий набор разнообразного прикладного ПО.

В подобных ситуациях в системном администрировании используют технологии клонирования компьютеров [1]. Суть метода заключается в точном копировании жёсткого диска (по секторам) эталонного компьютера на неограниченное количество целевых компьютеров. Особенно эффективен данный метод, когда набор ПО должен быть унифицированным в пределах какого-либо крупного сегмента локальной сети.

Существует большое количество коммерческих программ клонирования, например, Acronis True Image, Symantec Ghost, и т.д. Программы такого рода удобны в использовании, обладают широкой функциональностью, но их использование сопровождается крупными финансовыми затратами, а их лицензии не позволяют в полной мере адаптировать ПО под частные задачи.

В государственных учреждениях, а особенно в образовательных, целесообразно использование свободного программного обеспечения (СПО) для выполнения тех же функций. Такие преимущества СПО, как наличие исходных текстов и сообщество разработчиков, позволяют использовать данный вид ПО в образовательном процессе, например в работах студентов на практических и лабораторных занятиях. В общую стоимость владения такой системой входят только затраты на работу системного администратора. Благодаря свободному типу лицензии (GNU GPL) [2] и наличию исходных текстов можно улучшать программу и модифицировать её под конкретные требования [3].

Рассмотрим решение задачи интеграции системы клонирования в локальную сеть без внесения изменений в существующие службы на примере внедрения подобной системы в локальную сеть СПбГУ ИТМО.

Интеграция системы клонирования в локальную сеть

Для решения данной задачи были выбраны сервер сетевой загрузки DRBL и набор программ клонирования Clonezilla от Free Software Labs, NCHC (лаборатории свободных программ тайваньского национального центра высокопроизводительных вычислений) [4].

Выбранную систему клонирования необходимо было интегрировать в локальную сеть

факультета ИТиП ИТМО. Развёртывание системы клонирования затрагивало часть сети, состоящую из центрального сервера (сервер R), двух вспомогательных серверов (серверы D и V) и 10 компьютерных классов, выделенных в подсети класса C. На серверах установлены операционные системы Linux Centos и Linux Ubuntu Server, на рядовых компьютерах в классах установлена операционная система Windows XP и набор прикладного ПО. Общее число клонируемых компьютеров составляло 181 шт.

Сервер R предоставляет несколько служб, в частности DHCP (Dynamic Host Configuration Protocol) [5], которая задействована в системе клонирования. Компьютер V представляет из себя хранилище резервных копий и сервер виртуальных машин, одна из которых — эталонный компьютер для клонирования, на котором происходит обновление ПО. Сервер D является непосредственно сервером клонирования.

Выбранная система клонирования опирается на протокол сетевой загрузки PXE (Preboot eXecution Environment, Intel) [6], используемый практически в любой компьютерной сети. Протокол PXE является надстройкой над протоколом DHCP, и использует те же самые порты и методы передачи информации. Современные DHCP-серверы могут функционировать и как PXE-серверы, при соответствующей настройке. Сервер сетевой загрузки DRBL может выступать как сервер PXE и, соответственно, DHCP (Рис. 1).

Работа PXE-сервера отличается от работы DHCP-сервера лишь наличием расширенных ответов на специальные PXE-запросы. Если клиент запрашивает помимо DHCP-параметров ещё и дополнительные (шаг 1 на Рис. 1), то такой клиент считается PXE-клиентом и ему высылается расширенный ответ (шаг 2 на Рис. 1), содержащий эти дополнительные параметры. Они обычно включают в себя адрес сервера загрузки и имя файла загрузки. Когда клиент их получает, он переходит к стадии загрузки указанного файла в память и передаёт ему управление (шаг 3 на Рис. 1).

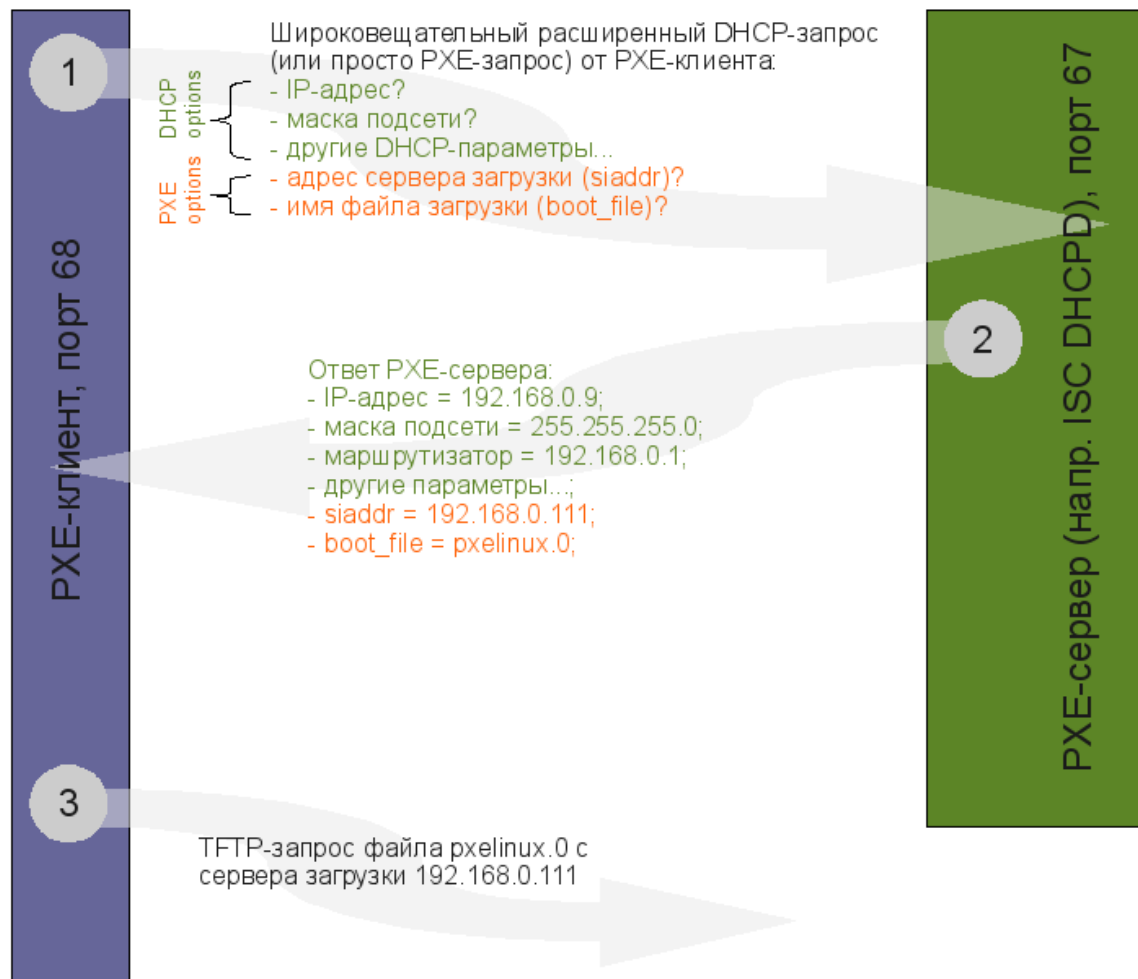


Рис. 1. Сетевая загрузка с использованием PXE-сервера

В локальной сети факультета ИТиП СПбГУ ИТМО уже существовал функционирующий DHCP-сервер, конфигурацию которого менять было нельзя, было решено отказаться от идущего в комплекте с DRBL PXE-сервера и использовать проху DHCP-службу (PXE redirection service) [6].

Сетевая загрузка с использованием проху DHCP-сервера, происходит следующим образом: в сеть с существующим сервером DHCP добавляется проху DHCP-сервер, принимающий дейтаграммы по протоколу UDP на тот же порт, что и DHCP-сервер (Рис. 2). Оба сервера, получив расширенный запрос от PXE-клиента (шаг 1 на Рис. 2), отвечают ему, но только своим набором параметров. DHCP-сервер отвечает набором DHCP-параметров (шаг 2а на Рис. 2), а проху DHCP-сервер — набором PXE-параметров (шаг 2б на Рис. 2). Клиенту для загрузки необходимы оба ответа, так как в них содержится вся необходимая информация. После их получения клиент переходит к стадии загрузки указанного файла в память и передаёт ему управление (шаг 3 на Рис. 2).

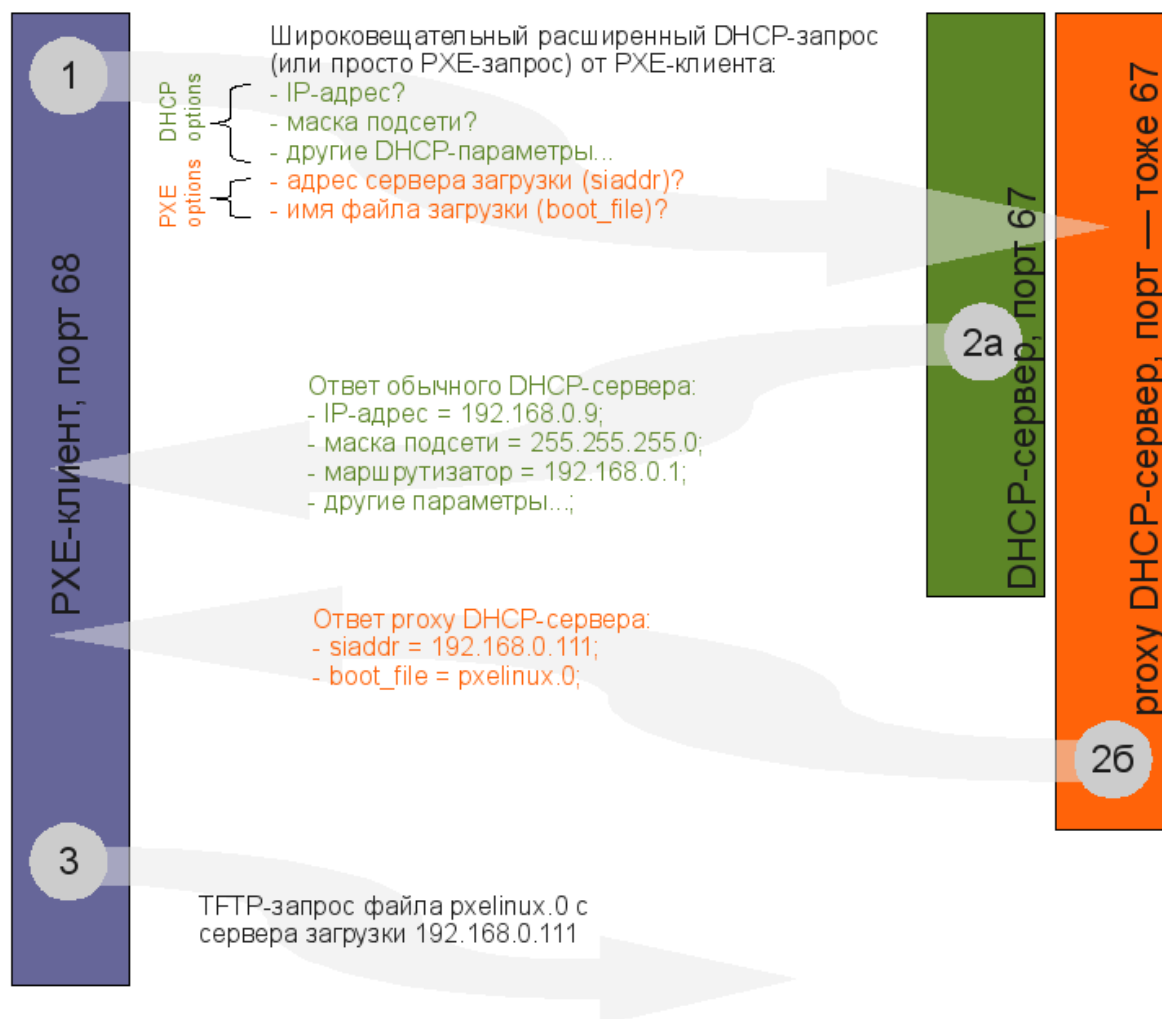


Рис. 2. Сетевая загрузка с использованием проxy DHCP-сервера

В качестве проxy DHCP-сервера был выбран сервер Dnsmasq [7], являющийся свободным ПО и выполняющим помимо прочего функцию сервера TFTP (Trivial File Transfer Protocol) [8]. В итоге, функциональная часть системы клонирования осталась неизменной, а изменился только процесс сетевой загрузки с сервера DRBL (сервер D).

После установки необходимого ПО на эталонный компьютер, производится его подготовка к снятию образа, в случае с операционной системой Windows — это сброс идентификаторов безопасности, добавление драйверов, программирование процедур на выполнение после клонирования. Затем виртуальная машина эталонного компьютера выключается и загружается по сети с использованием протокола PXE. Посылается широковещательный PXE-запрос, на который DHCP-сервер R отвечает набором DHCP-параметров (IP-адрес компьютера) в специальном образом настроенную ОС Linux [9]. Запускается процесс создания точной копии жёсткого диска (так называемого эталонного «образа») — копирование, сжатие, передача по сети и сохранение на сервере D (Рис. 3).

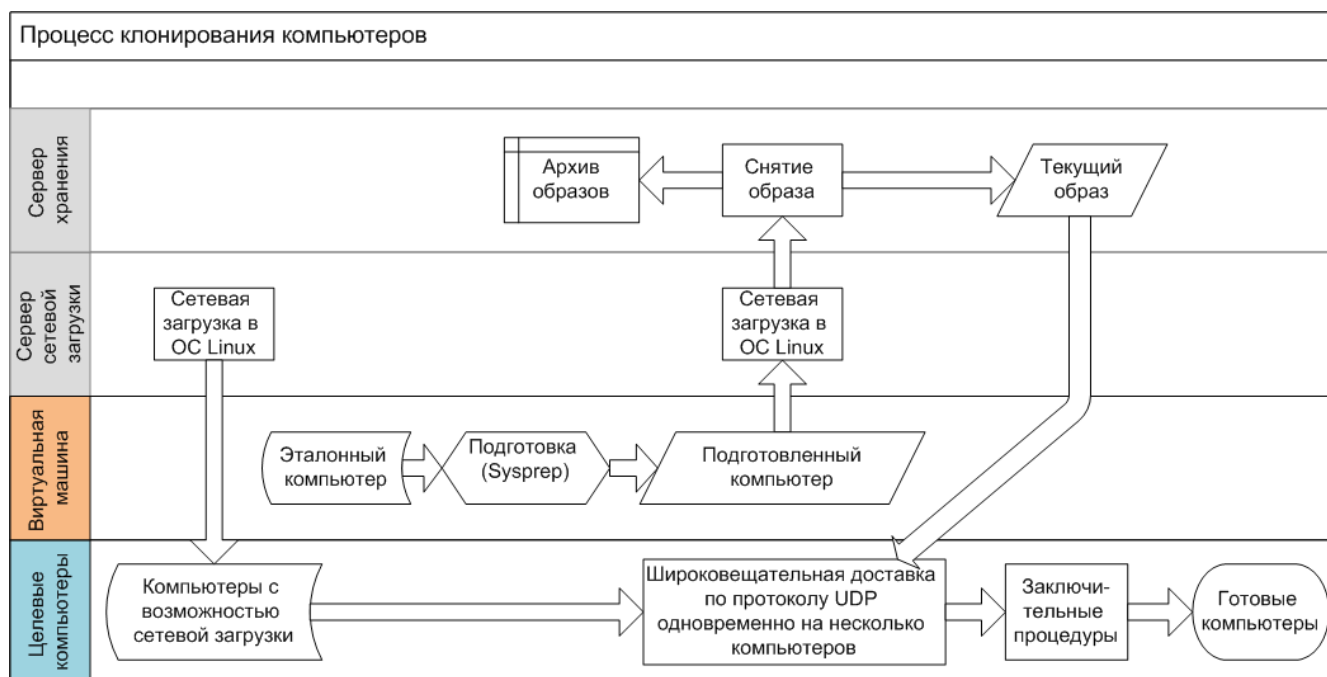


Рис. 3: Процесс клонирования компьютеров

В нашем случае при использовании данного метода компьютеры загружаются в режиме разворачивания системы из эталонного образа. Сервер D, передаёт в режиме широковещания файл образа, а клиентские компьютеры принимают его и распаковывают на локальные жёсткие диски. По завершению передачи, компьютеры автоматически перезагружаются и выполняют заключительные процедуры (устанавливают необходимые драйверы, устанавливают дополнительные программы, получают новое имя, присоединяются к домену и так далее).

Заключение

Интегрирование системы клонирования в локальную сеть СПбГУ ИТМО без внесения изменений в существующие службы производилась путём подбора и замены составных частей свободной системы с открытым исходным кодом DRBL и Clonezilla, была удалена функция PXE-сервера, вместо которой добавлена функция проху DHCP-сервера. При внедрении системы клонирования были учтены следующие особенности архитектуры локальной сети СПбГУ ИТМО: существующая система инвентаризации, отсутствие «гостевых» компьютеров, фильтрация по MAC-адресам, разделение полномочий системных администраторов, наличие нескольких подсетей.

Список литературы

1. Медведев Ю.Г. Технологии клонирования компьютеров / Медведев Ю.Г. - СПб.: BHV-Санкт-Петербург, 2006 - 304 с.: с.60-65 - ISBN 5-94157-733-8
2. Лицензия GPL <http://www.gnu.org/licenses/gpl.html>
3. Эви Немет. Руководство администратора Linux / Эви Немет, Гарт Снайдер, Трент Хейн - СПб.: Вильямс, 2007 - 1072 с.: с.204-223 - ISBN 978-5-8459-1093-6
4. Сайт разработчиков DRBL <http://drbl.sourceforge.net/>
5. Техническая спецификация протокола DHCP <http://www.ietf.org/rfc/rfc2131.txt>
6. Техническая спецификация протокола PXE
<http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf>
7. Сервер Dnsmasq <http://www.thekelleys.org.uk/dnsmasq/doc.html>
8. Техническая спецификация протокола TFTP <http://www.ietf.org/rfc/rfc2347.txt>
9. Тони Боттс. Linux руководство администратора сети / Тони Боттс, Терри Доусон, Грегор Н. Перди - М.: Кудиц-Пресс, 2006 - 368 с.: с.211-245 - ISBN 5-91136-018-7