«Бездисковые рабочие станции на базе технологий ALT Linux»

Цель

В 2007 году появилась уникальная возможность полностью обновить одну из лабораторий кафедры ЭВМ БГУИР, при этом спонсор — компания «EffectiveSoft» — не просто закупила среднестатистическое оборудование, а позволила выбрать конфигурацию для компьютерного класса.

Поскольку студенты кафедры активно изучают не только прикладное, но и системное программирование, то часто возникает ситуация, когда для корректной работы лабораторной или курсовой требуется привилегии администратора. С другой стороны, такие привилегии студентам давать просто опасно, поскольку нередки ситуации, когда тестируемые программы выводят из строя ПО на компьютере. Кроме того, на кафедре изучается различные операционные системы и принципы их работы, поэтому каждый компьютер обязан поддерживать, как минимум 2 операционные системы: Linux и Windows.

Одной из дополнительных целей является обеспечение работы лаборатории в режиме кластера, для тестирования научных разработок, ведущихся на кафедре.

Таким образом образуется противоречие — необходимо позволить студентам делать на компьютерах все, что заблагорассудится, но при этом обеспечить стабильное функционирование различных операционных систем и прикладного ПО.

Аппаратное обеспечение

Для создания компьютерного класса была выбрана схема, представленная на рис. 1.

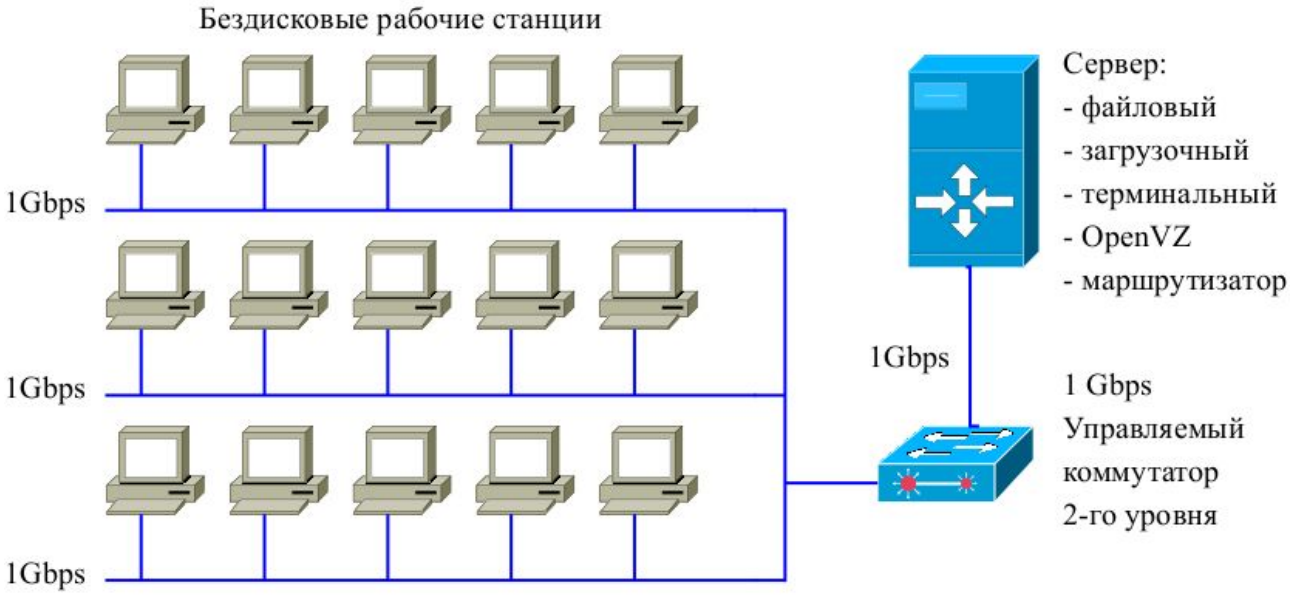

Рис.1: архитектура компьютерного класса.

Поскольку, рабочие станции являются бездисковыми, то, за счет экономии на жестких дисках для всего класса, появилась возможность установить достаточно объемный и надежный дисковый массив на сервере, а сеть построить на базе Gigabit Ethernet.

Соответственно, в результате мы получили 15 рабочих станций на базе Athlon 64 X2 3600+, 2GB RAM и сервер - Intel Xeon E5335 4x2 Ghz, 4GB RAM, 6x320GB hdd.

Бездисковая загрузка

Организация загрузки, достаточно стандартная для бездисковых систем [DAP01], показана на рис.2.

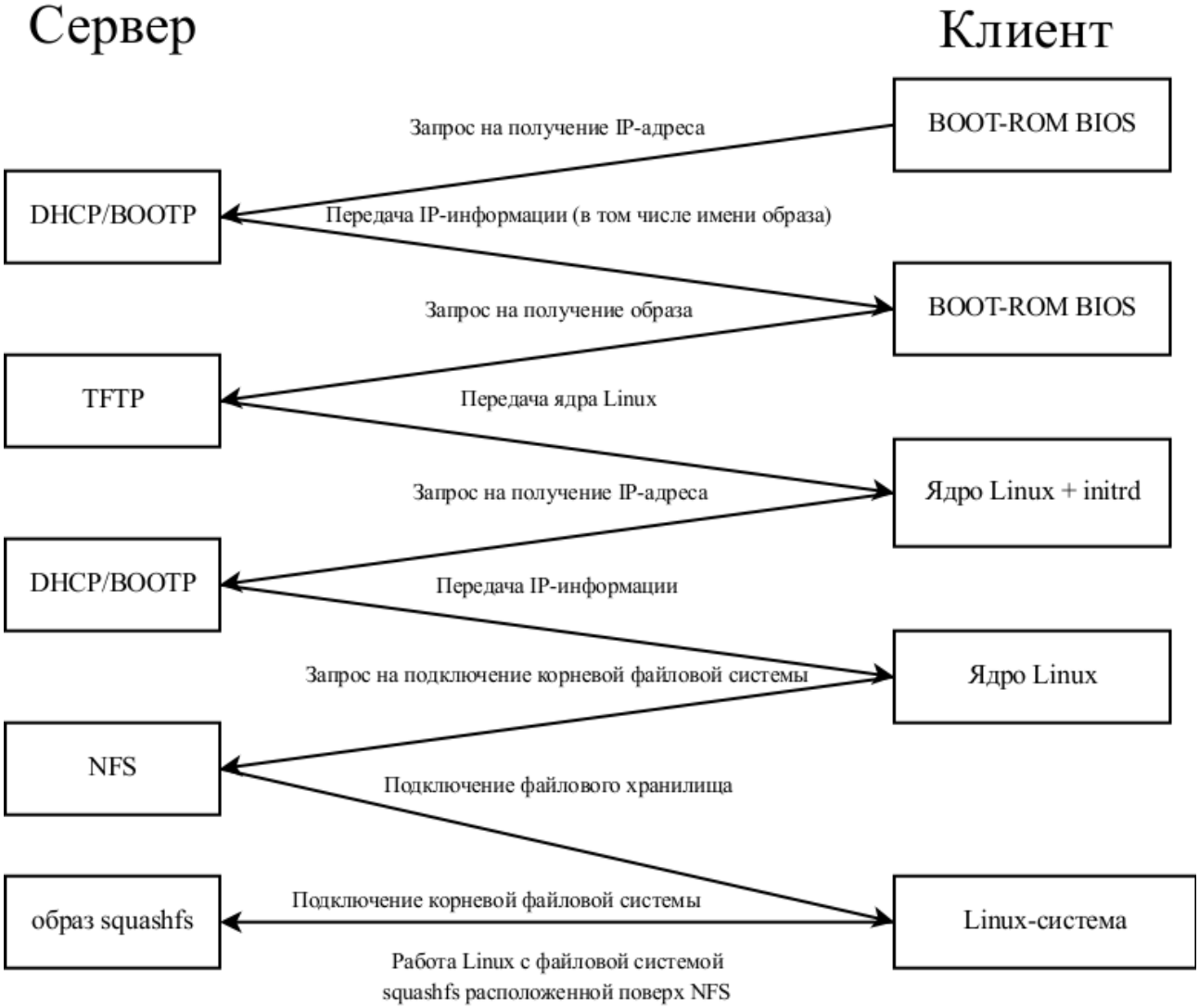

Рис. 2. Диаграмма загрузки бездисковых рабочих станций.

Как правило, бездисковые системы используют в качестве корневого каталога сетевой ресурс NFS, расположенный на сервере. Такое подключение удобно, но имеет и свои недостатки.

При подключении ресурса с разрешением на запись — нет возможности предоставить пользователям полное управление Linux системой, да и, как показывает практика, студенты — одна из самых рискованных групп пользователей, соответственно, рано или поздно, такая система будет взломана и приведена в негодность.

Другая крайность — когда корневой раздел монтируется в режиме «только чтение» - решает проблему с изменением данных и доступом от имени администратора, но создает другую проблему — требуется серьезное вмешательство в работу дистрибутива.

Вторым вариантом является использование файловой системы типа unionfs для обеспечения, чтобы изменения в файловой системе, оставались в памяти компьютера и были видны только для данной конкретной машины. Такое решение на данный момент является наиболее популярным, но и здесь есть свои недостатки, например работа unionfs поверх NFS не отличалась стабильностью на момент создания класса.

Кроме того, существует еще и человеческий фактор — как показала практика использования, развернутый корень бездисковых систем провоцирует администраторов вносить мелкие, «временные» правки напрямую в развернутый образ, что приводит к проблемам при апгрейде систем для бездисковых машин и сильно затрудняет создание загрузочного образа «с нуля», при, например, смене базового дистрибутива. Кроме того есть неочевидная угроза для безопасности — в случае взлома сервера, будут скомпрометированы и развернутые корневые директории для бездисковых рабочих станций.

Нельзя не упомянуть о еще одной возможности для создания бездисковых систем — использование initrd в качестве корневой файловой системы. Достоинства такого подхода - нет необходимости использования NFS, вся система полностью помещается в память, это идеально подходящий вариант для бездисковых терминалов, но мало пригодный вариант для рабочих станций — неоптимально используется память, а размер образа ограничен размерами ОЗУ.

Live-CD

Очень похожую проблему приходится решать при создании Live-CD систем — здесь тоже необходимо загружать полноценную ОС с носителя, доступного в режиме «только чтение».

Но, в отличие от ситуации с бездисковыми системами, разработчики дистрибутивов напрямую заинтересованы в live-cd системах, как части дистрибутивов и, соответственно, уже существуют специальные программы для создания live-cd из репозитория ПО, например pbuilder для Debian, livecd-creator для Fedora Core и spt для ALT Linux.

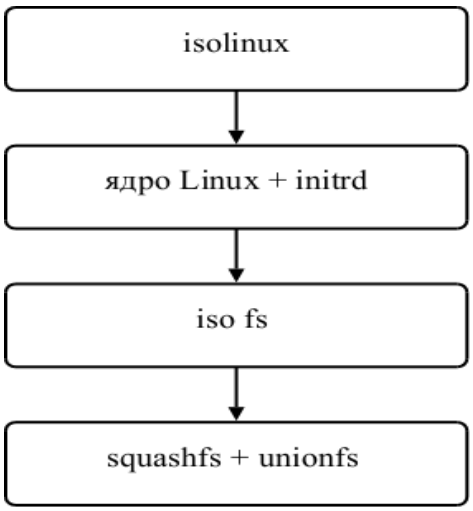

Рис.3. Последовательность загрузки Live-CD систем.

В общем случае, загрузка Live-CD представлена на рис.3. и выглядит следующим образом: сначала загружается загрузчик isolinux, который загружает в память ядро ОС Linux, и initrd, после чего передает управление ядру. Ядро, с помощью «мини-системы» находящейся в initrd, обеспечивает инициализацию минимально необходимого оборудования, в том числе привода CD, для доступа к файлу-имиджу, как правило в формате squashfs, и производит монтирование имиджа файловой системы в качестве корневой директории. Далее ядро передает управление программе «init», которая производит дальнейшую загрузку системы.

Одной из особенностей программ для создания Live-CD систем является то, что они не только создают корневую систему, но и модифицируют или дополняют, процесс загрузки таким образом, чтобы необходимые для работы в режиме записи каталоги были смонтированы с помощью unionfs или tmpfs.

Нетрудно понять, что программы для создания Live-CD разрабатываются с учетом специфики целевого дистрибутива. Поскольку, по ряду причин, в том числе и личного предпочтения автора, бездисковые системы, описываемые в статье строятся на базе технологий ALT Linux, то и речь далее пойдет именно о них.

Live-CD через сеть

Если сравнить процесс загрузки ОС Linux до момента монтирования корневой файловой системы, то можно провести параллель между системами с сетевой загрузкой в режиме «только чтение» и Live-CD системами.

Этап загрузки	**Бездисковая система**	**Live-CD**
Загрузчик	pxelinux	isolinux
Инициализация	initrd	initrd
Базовая ФС	NFS	isofs
Корневая ФС	NFS+unionfs	squashfs+unionfs

Таб.1. Соответствие этапов загрузки

Загрузчики для обоих вариантов, на самом деле, являются разновидностью программы syslinux. Инициализация и подготовка доступа к базовой файловой системе происходит, в общем случае, в initrd. Различаются только базовая файловая система и, как следствие, образ файловой системы, использующийся в качестве корневого.

В ОС Linux любая файловая система представляется, как виртуальная файловая система, а работу на более низком уровне производит драйвер файловой системы. Поэтому принципиальной разницы, с точки зрения ядра, между базовыми файловыми системами также нет — лишь бы существовал соответствующий драйвер. Получается, что если в процессе инициализации в initrd можно смонтировать базовую файловую систему, то и на этом уровне разница теряется.

Поскольку в ALT Linux системах, еще со времен отделения от дистрибутива Mandrake, для базовой инициализации в initrd используется программа propagator, которая позволяет использовать в качестве базового носителя как CD, так и различные сетевые протоколы, включая NFS, то появляется возможность использовать тот же подход для загрузки бездисковых рабочих станций, что и для загрузки Live-CD.

Таким образом для создания системы загрузки через сеть с помощью технологий, применяемых для создания Live-CD, остается только создать свою собственную корневую систему на базе необходимого дистрибутива.

Создание корневой ФС

Как отмечалось выше, в каждом уважающем себя дистрибутиве имеется система создания дистрибутива из целостного пакетного репозитория. Для создания дистрибутивов из пакетной базы ALT Linux было разработано несколько утилит: separator, spt, spt3 и, наконец, mkimage. В настоящее время, для подготовки дистрибутивов, а также Live-CD ALT Linux используются две утилиты — это spt и mkimage.

SPT представляет собой набор shell-скриптов, а mkimage — набор правил для утилиты make. Не смотря на разницу в реализации, обе эти утилиты построены по схожим принципам (приводится с точки зрения создания Live-CD):

- на вход передается список пакетов, которые необходимо установить;
- используется утилита hasher для создания развернутой корневой системы будущего Live-CD;
- с помощью скриптов-обработчиков производится окончательная настройка загрузочного имиджа, в том числе и настройка монтирования unionfs;
- полученный каталог, содержащий развернутую систему загрузочного диска, упаковывается в образ, использующий файловую систему squashfs;
- подготавливается ядро и загрузочный initrd-образ;
- настраивается загрузочная конфигурация для isolinux;
- создается образ в формате iso, пригодный для записи на CD/DVD.

Все вышеперечисленные этапы могут настраиваться или вообще не использоваться, так, например, для создания загрузочного образа для работы по сети не требуется настройка isolinux, а также создание образа для записи на CD/DVD.

Важной особенностью является то, что для адаптации к конкретным условиям необходимо использовать дополнительные пакеты RPM и/или скрипты-обработчики, в которых содержатся дополнительные настройки конечного образа.

Для кафедры ЭВМ используется дополнительный пакет RPM, в котором содержатся:

- настройки локальных репозиториев для утилиты apt — чтобы студенты могли самостоятельно доустанавливать ПО из репозитория, если оно не включено в образ по умолчанию;
- настройки десктопа — по большей части, здесь содержится необходимая конфигурация для использования 3D десктопа по умолчанию, а также различные ярлыки, ведущие к наиболее часто используемым программам и ресурсам;
- модули ядра и настройки по умолчанию для виртуальной машины VMWare.

Не обошлось и без «подводных камней» - например конфигурирование сетевых интерфейсов в образе должно быть отключено. Если вернуться к рис.1, то становится ясно, что конфигурация загрузочного интерфейса происходит после инициализации ядра с помощью initrd, более того, на момент написания, попытка инициализировать сетевой интерфейс повторно может закончится плачевно. Дело в том, что сетевой интерфейс для бездисковых систем является своеобразным «шлейфом к загрузочному диску», а перед инициализацией сетевого интерфейса происходит сброс уже настроенных параметров. Таким образом фактически происходит аналог отключения загрузочного жесткого диска, а затем производится попытка прочитать и запустить утилиты для конфигурирования сети с этого отключенного диска.

В результате работы утилиты spt, на выходе мы получаем 3 необходимых для загрузки файла: ядро, образ initrd и образ корневой файловой системы, сжатый с помощью squashfs.

Организация загрузки бездисковых рабочих станций

Для организации загрузки бездисковых рабочих станций необходимо настроить 3 сервера: tftp (пакет tftp-server), dhcp (пакет dhcp-server) и nfs (пакет nfs-server).

Сервер dhcp кроме распределения адресов также позволяет обслуживать протокол bootp, необходимый для передачи начального загрузчика pxelinux на рабочие станции. Для этого необходимо в секцию описания подсети конфигурационного файла сервера /etc/dhcp/dhcpd.conf добавить строки, изменив настройки для конфигурации своей подсети:

```
filename "pxelinux.0";
next-server 172.16.4.254;
pool {
    range dynamic-bootp 172.16.4.1 172.16.4.99;
}
```

Файл pxelinux.0 необходимо скопировать из «/usr/lib/syslinux/pxelinux.0», находящегося в пакете syslinux, в каталог «/var/lib/tftpboot/». Этот файл как раз и является начальным загрузчиком по сети для рабочих станций. Кроме того, необходимо создать конфигурационный файл, использующийся по умолчанию - «/var/lib/tftpboot/pxelinux.cfg/default», в котором находятся настройки для загрузки ядра и образа initrd. Пример типичной конфигурации для рабочей станции выглядит следующим образом:

```
label Linux Desktop 4.0
kernel alt/Desktop40/vmlinuz
append fastboot initrd=alt/Desktop40/full.cz automatic=method:nfs,network:dhcp,server:172.16.4.254,directory:/home/pub/netboot/Desktop40 stagename=live live fastboot splash=silent splashcount=15 vga=0x314 showopts
```

который фактически является копией настроек, используемых для Live-CD, за исключением, как видно из приведенного примера, сугубо сетевых настроек.

Настройки nfs-сервера абсолютно стандартны и единственной его задачей является создание сетевого ресурса в режиме «только для чтения», на котором располагается файл-образ корневой файловой системы.

Альтернативные ОС

Как уже упоминалось выше — кроме платформы на базе ОС Linux в лаборатории необходимо поддерживать и другие операционные системы, в частности из семейства Microsoft© Windows™.

Для обеспечения работы альтернативных операционных систем в образ корневой файловой системы включается VMware Player, на использование которого не накладывается никаких ограничений, но вместе с тем полноценно используются все возможности аппаратного обеспечения.

Как показала практика использования, никаких проблем при использовании студентами ОС семейства Windows не возникает, более того, благодаря особенностям виртуализации, данная ОС, даже в случае сбоя, все равно загружается в конфигурации, жестко заданной администратором. Одним из позитивных следствий виртуализации является принципиальная «неубиваемость» операционной системы как пользователями, так и вредоносными программами.

Кроме того все рабочие станции имеют возможность использовать гостевые операционные системы, которые также загружаются из одного и того же образа виртуальной машины не только с точки зрения конфигурации, но и с точки зрения файловых объектов на сервере, что значительно увеличивает скорость работы таких систем в целом.

Результат

В результате совместного использования стандартных программ и методов,

предлагаемых дистрибутивами ALT Linux, существует возможность развертывания класса бездисковых рабочих станций, при этом нет необходимости использовать специализированное программное обеспечение промежуточного уровня, например LTSP.

Кроме того достигаются дополнительные положительные результаты:

- снижается нагрузка на сеть, благодаря использованию сжатой файловой системы, с одновременным увеличением скорости работы файловой подсистемы для рабочих станций;
- для всех ОС используется режим «только для чтения», благодаря чему изменения внесенные пользователем или вредоносными программами имеют время жизни, ограниченное перезагрузками ОС;
- для загрузки рабочих станций возможно использовать сервер на базе любой ОС;
- простота конфигурирования;
- возможность использования ОС конечными пользователями в режиме администратора.