CHAPTER 1

System Setup

Introduction

Cyber operations is about the configuration, defense, and attack of real systems. Publicly known vulnerabilities in deployed systems are patched, though perhaps not as rapidly as the security might hope. Any publicly known vulnerabilities that might be exploited in currently deployed systems are necessarily 0-days. In contrast, older systems can be attacked using a range of exploits that are known today, but were unknown when the systems were deployed. Thus, this book focuses on systems that were deployed between 2008 and 2013.

To configure, attack, and defend systems, a testing laboratory is required. Such a laboratory must not only allow systems to be built and run, but must provide a way to segregate them from the wider Internet; after all, older systems are known to be vulnerable to public exploits. One excellent solution is virtualization. A range of virtualization solutions exist; two commonly deployed solutions are VMWare and VirtualBox. This chapter begins with a review of these virtualization solutions.

The Notes and References lists the major Windows desktop and server operating systems released between 2008 and 2013; it also includes major releases from the CentOS, OpenSuSE, Ubuntu, and Mint Linux distributions. The section provides download locations for the various Linux distributions. This chapter shows how to build virtual machines running these operating systems.

A functioning computer system is more than just its operating system though; its entire ecosystem of installed applications must be considered. Desktop systems generally include a browser as well as plug-ins for various kinds of active web content. This chapter shows how to install three commonly used programs: Firefox, Java, and Adobe Flash Player on Windows and Linux workstations. These tools have been released in different versions and patch levels; the Notes and References lists release dates and download locations for these tools.

One advantage of modern operating systems and many major software packages is that they automatically download and install the latest security patches, often without user interaction. In almost every circumstance this is a good thing. To keep these test systems at a preferred patch level, this functionality must be disabled.

When this chapter is complete, the reader will have set up and configured a fully functional testing laboratory that can be used to run Windows and Linux virtual machines as they were deployed on a selected date between 2008 and 2013.

Virtualization Tools

A good testing laboratory needs a wide range of systems. Rather than use dedicated hardware for each system, it is much simpler to build systems using virtualization. Two of the most common tools for operating system virtualization are VMWare Workstation 10.0 and VirtualBox, while other choices include Hyper-V, Parallels, QEMU, and Xen. This section focuses solely on the first two of these. VMWare Workstation is

M. O'Leary, *Cyber Operations*, DOI 10.1007/978-1-4842-0457-3_1

a long-standing, solid commercial product that runs on Windows and Linux; it has a free version called VMWare Player with reduced functionality. VirtualBox is a free, open source alternative; it runs on Windows Linux, Macintosh, and Solaris. In its current version, it is comparable to VMWare Workstation in functionality.

VMWare Workstation

The simplest way to learn about VMWare Workstation 10.0 is to dive right in by installing and running a guest operating system.

Installing a guest

Grab the install disc for a Linux distribution—for example, the DVD for CentOS 6.0, and save that `.iso` file in some convenient location. Launch VMWare Workstation. If the home tab appears, select "Create a New Virtual Machine"; if it does not, then the same option is available from the File menu.

VMWare Workstation begins the process of creating a new virtual machine by presenting the user with the "New Virtual Machine Wizard." The "Typical" configuration is nearly always sufficient, so select it. The first question is the location of the install media; provide the location of the saved .iso file for the "Installer disc image file (iso)." In most, though not all cases, VMWare Workstation is able to recognize the operating system on the disc image. When VMWare Workstation moves to install a recognized operating system, it uses "Easy Install" and makes a number of choices for the user. This automated process is often convenient, however, it precludes the user from choosing some things, such as the system partition table or the precise collection of installed software; this can occasionally cause difficulty later.

When installing CentOS, VMWare Workstation asks for information about a system user: the user's full name, the username, and the password for that user. The same password for the user is also used for the root account on the system. VMWare Workstation asks for both the name of the virtual machine and the location in which it will be stored. The VMWare Workstation name is separate and distinct from any host name of the system; in fact it is used solely by VMWare Workstation. It is used to generate the names of the files that comprise the virtual machine and will appear as the machine's title within VMWare Workstation. When selecting the location of those files, note that there are many files for each virtual machine, so it is a very good idea to store each system in its own separate directory.

VMWare Workstation asks for the size of the virtual hard disk; it provides the option to split the virtual disk into smaller files. The rationale for this question is the limitation of some file systems, including FAT32. The FAT32 file system remains commonly used on flash drives, despite the fact that files in FAT32 are limited to less than 4GB in size. A virtual machine with a hard drive of 4GB or more could not be copied onto such a flash drive. When VMWare Workstation uses a split virtual disk, each file is no more than 2GB in size.

Be sure that your host has sufficient memory for all of the running guests.

Before creating the virtual machine, VMWare Workstation allows the hardware to be customized. Key settings that can be modified include the system's memory, the number of network cards it possesses, and installed peripherals such as CD/DVD or a USB controller.

When all of the choices have been made, VMWare Workstation installs the operating system.

Managing guests

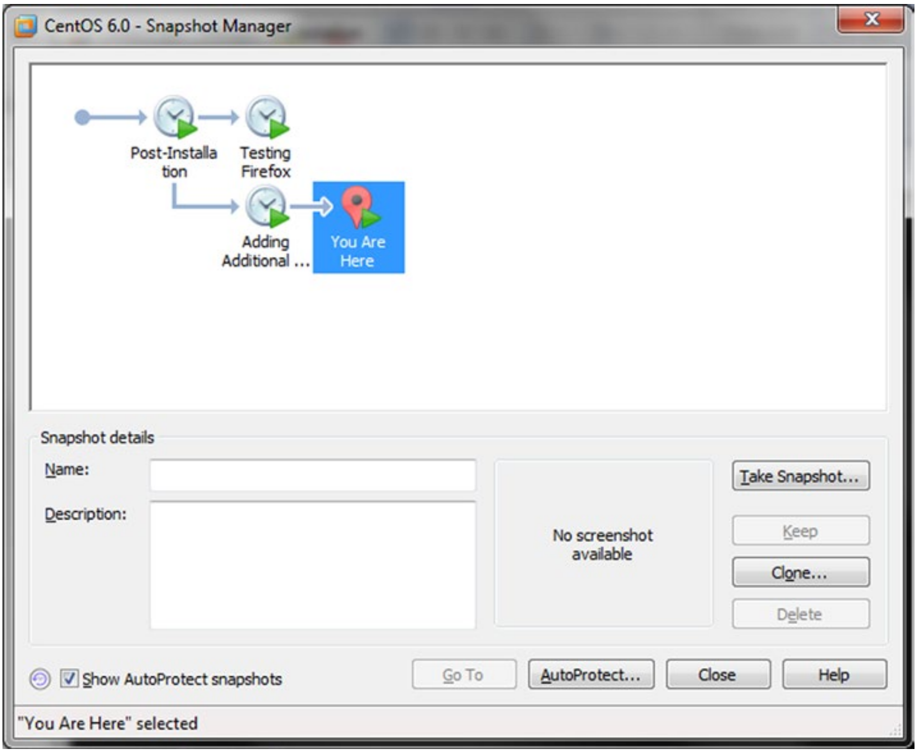
Once the guest operating system is installed, the guest will reboot. Interact with the guest as any other system; log on, providing the password selected during the installation process. The guest responds as if it were the only system currently running.

One issue that may arise is control of the keyboard and the mouse. This is not an issue for the CentOS 6.0 system when installed on VMWare Workstation 10.0, because VMWare Tools is installed on the guest as part of the installation process. In general, though, the keyboard combination CTRL+ALT, when pressed inside a guest returns control of the keyboard and the mouse to the host. Try it; if the cursor for the mouse in the CentOS 6.0 guest is different for the cursor for your host operating system, you will see the change.

Another problematic keyboard combination is CTRL+ALT+DEL. On a Windows host, that combination will be intercepted by the host operating system. To send that combination to the guest, use CTRL+ALT+INSERT instead.

Once the guest is running, it can be powered down from within the guest. VMWare Workstation also provides the ability to shut down or restart the guest from VMWare Workstation itself. It also provides the ability to suspend the guest, essentially pausing it. This can be convenient when the current state of the system is critical. The process of pausing and restarting guests is resource intensive and can be somewhat slow.

VMWare Workstation provides the ability to take a "Snapshot" of a system. In essence, this stores the complete current state of the system; it allows the user to later revert the system back to that precise state. Multiple snapshots can be taken and stored. Snapshots are managed through the Snapshot Manager, which can be accessed by navigating the VMWare Workstation main menu through VM ➤ Snapshot ➤ Snapshot Manager. See Figure 1-1.



No screenshot available

☑ Show AutoProtect snapshots

"You Are Here" selected

Figure 1-1. VMWare Workstation 10.0 Snapshot Manager

Once a virtual machine has been created, it can be copied and moved by copying and moving the underlying directory. When a moved or copied virtual machine is started for the first time, VMWare Workstation will prompt the user warning that the virtual machine may have been moved or copied, and asks the user to select either "I moved it" or "I copied it." One of the core differences between these two options is the MAC address of the guest. If the user selects "I moved it" then the guest is unchanged, but if "I copied it" is selected, then the guest's MAC address is modified. If this were not done, then the original system and its duplicate would have the same MAC address on the network, which is a recipe for amusing network mayhem if both are run at the same time.

Networking

A network adapter for a VMWare Workstation virtual machine can be configured in a number of different ways.

- It can be connected directly to the host's physical network (bridged). In this mode it acts as another system on the host's network.
- It can be connected to the host network via network address translation (NAT). In this case the guest can make outbound connections to the physical network, but inbound connections reach the guest only if explicitly allowed by port forwarding.
- It can be connected to a host-only network, which only allows network connections to/from other adapters on the host-only network, including the host.
- It can be connected to a different virtual network (VMNet2 - VMNet7; VMNet9 - VMNet19). All of the adapters connected to the same virtual network can communicate with each other and with the host, but by default cannot communicate with other guests or with systems on the physical network.

The configuration of a network adapter can be changed from the Settings dialog box for the virtual machine; that dialog box can be accessed by navigating the VMWare Workstation menu through VM ➤ Settings. From the Hardware tab, select Network Adapter to modify the settings.

The settings for each network are controlled through the Virtual Network Editor; it can be launched by navigating the VMWare Workstation Menu through Edit ➤ Virtual Network Editor. This tool configures the network type, its assigned address range, and its subnet mask. It also controls whether VMWare Workstation should act as a DHCP server on that network, and if it is a NAT network, any port forwarding.

The address of the host on each network can be found by using command-line tools on the host. In its default configuration, a Windows host should have Ethernet adapters for both the VMNet1 (host-only) and the VMNet8 (NAT) networks and their addresses can be found using `ipconfig`.

VMWare Tools

To improve the interaction between the guest and the host, some modification of the guest is required. In VMWare Workstation, this is done by VMWare tools. If VMWare Workstation recognized the operating system during the install, then VMWare tools is installed on the guest as part of the "Easy Install" process. For some Linux distributions, including Kali 1.0.7, VMWare Tools must be manually installed after the guest operating system is running.

One feature provided by VMWare Tools is that it enables copying and pasting between guests and the host. It allows for drag and drop, so that files from the host can be dragged and dropped onto a guest (and vice versa) where they will be copied. Both of these features can be disabled though; navigate to Virtual Machine Settings from the main menu through VM ➤ Settings, then from the Options tab select Guest Isolation.

VMWare Workstation can adjust the screen size of a guest with VMWare Tools. The user can resize the VMWare Workstation application and the size and screen resolution of the guest will be adjusted accordingly. VMWare Tools also enables "Unity Mode." In unity mode, the background of the guest is not shown at all; instead its windows are shown in the host as if they were natively hosted windows.

VMWare Tools enables the use of Shared Folders. A shared folder is a folder on the host operating system that also exists at a different mount point, in the guest. This feature is enabled and controlled through Virtual Machine Settings (Main Menu ➤ VM ➤ Settings) in the Options Tab, under Shared Folders. To enable a shared folder, determine how long the shared folder should be enabled (permanently, or until the next guest reboot). The Add button will start the Add Shared Folder Wizard. Select a directory on the host – say `D:\Shared`, and then a name for the share – for example, shared. On a Linux system, that folder will be mounted in the file system at `/mnt/hgfs/shared`. Here `/mnt` is the usual location for external file systems, `hgfs` stands for host-guest-file-system and `shared` is the name of the share that was created. If the guest is a Windows system rather than a Linux system, the process is similar, though the shared folder appears as `\\vmware-host\Shared Folders\Shared` if automatic drive mapping is not selected, and as `E:\Shared` if it is.

VirtualBox

One of the big advantages of VirtualBox over VMWare Workstation is that VirtualBox is a free, open source product. There was a time when VMWare Workstation had significantly more features than VirtualBox, but today they are comparable. The current downside of VirtualBox is that configuring a system to run in VirtualBox requires more manual effort.

Installing a guest

The simplest way to learn to use VirtualBox is to dive right in and install a guest – for example an Ubuntu 12.04 desktop system.

Be sure that the guest is allocated sufficient memory to run.

The process begins when the user presses the "New" button on the main menu. VirtualBox presents a dialog box, asking for the name and type of system. Like VMWare Workstation, the host name is used solely by VirtualBox itself. VirtualBox asks the user to select the amount of memory that the virtual machine will use and the size of the guest system's hard drive. The user can choose from a range of virtual hard disk formats, including VDI, the VirtualBox disk image, and VMDK, the format used by VMWare. One important difference between the formats is that although VMDK files can be split into smaller 2GB files to enable them to be stored on FAT32 partitions, VDI files cannot be split. Both VDI and VMDK files can be dynamically allocated, meaning that the file(s) containing the hard drive would only contain data for the parts of the hard disk that had been used. Finally, VirtualBox asks for the final size of the hard disk as well as the location on the host where the file(s) would be stored.

Unlike VMWare Workstation, the guest has not yet been installed; indeed the user is yet to even provide the location of the install media to VirtualBox. However, when the virtual machine is first started, VirtualBox asks the user for the location of a start-up disk. This can be a physical disk in the form of a CD/DVD; it can also be an `.iso` image. The VirtualBox guest will then boot from the install media as if it were a physical device. The user must navigate the install process manually. This provides more control than VMWare Workstation, but it also requires more manual intervention.

Managing guests

Once the guest is running, interact with it as if it were a physical machine. The keyboard and mouse are directed to the guest as if it were any other application. To manually change whether the host or the guest receives keyboard input, press the host key, which by default is the CTRL key on the right side of the keyboard. To change the host key, from the Oracle VM VirtualBox Manager navigate the main menu through File ➤ Preferences. Select Input from the left menu, then the Virtual Machine tab. The first displayed option is for the Host Key Combination.

To send the CTRL+ALT+DEL combination to a guest, use HOST+DEL (=RCTRL+DEL by default); like the host key itself, this key combination can be changed in the same preferences menu.

VirtualBox provides the ability to pause, reset, and shut down a guest from VirtualBox itself. VirtualBox also provides the ability to take a snapshot of a system, either running or shut down. These snapshots can be taken from the VirtualBox menu for the guest itself (navigate Machine ➤ Take Snapshot), or from the Oracle VM VirtualBox Manager. To use the VirtualBox Manager, select the virtual machine from the list on the left side of VirtualBox Manager, then press the Snapshots button on the top right. You are presented with a tree-like structure showing all of the available snapshots, as well as the current state of the system. To create a new snapshot, select the current state, and press the left-most camera icon. Restoring a snapshot requires the user to select the snapshot then the camera icon second from the left; however a system snapshot cannot be restored while the guest is running. See Figure 1-2.

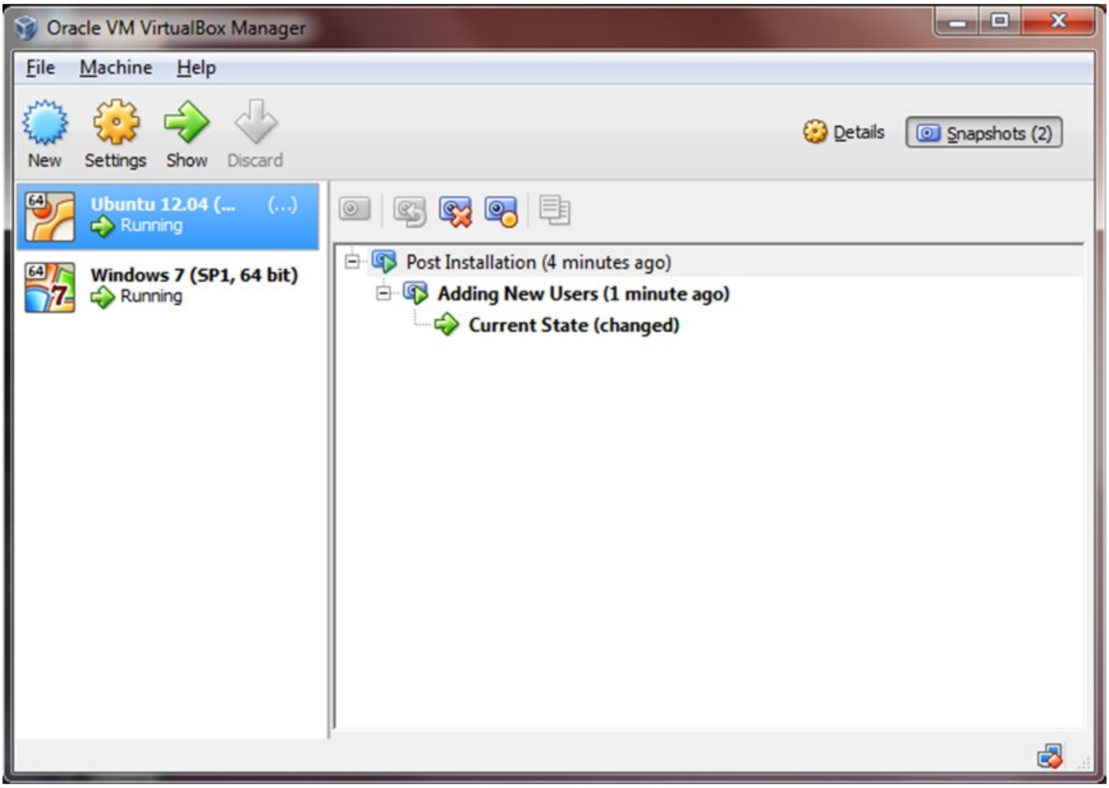
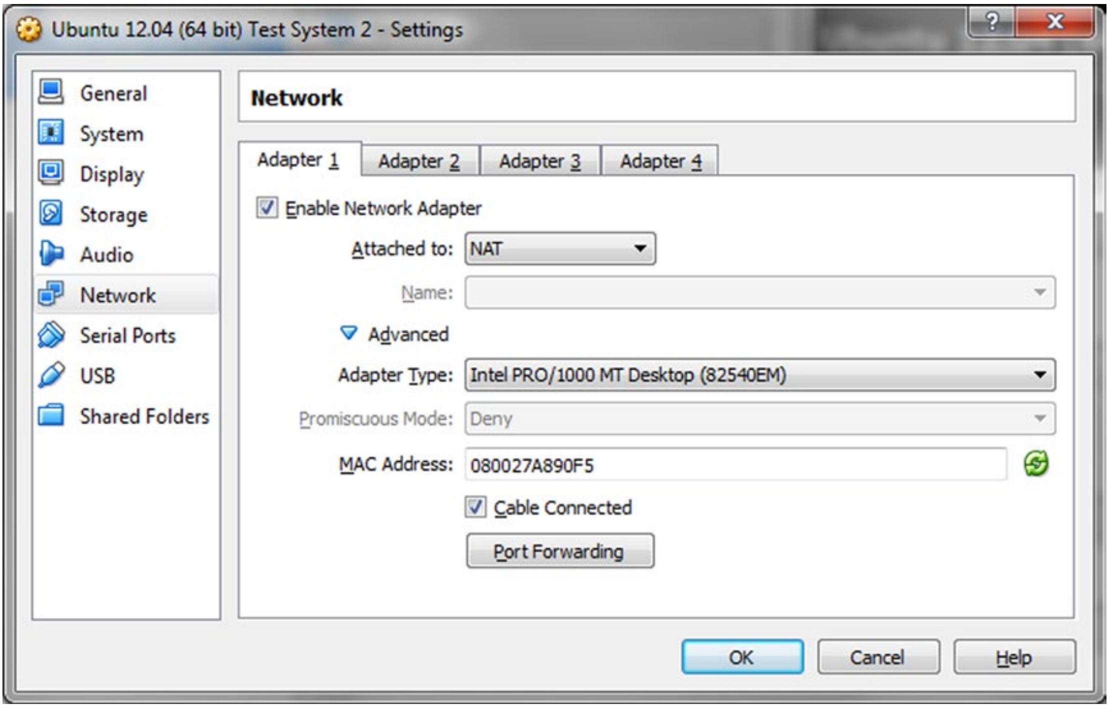


Figure 1-2. *Managing Snapshots in VirtualBox*

The process of copying and moving VirtualBox virtual machines depends on whether or not the copied guest will be used on the same host. To create a copy of a virtual machine for use on the same host, begin with a powered-down virtual machine. From VirtualBox Manager, select the virtual machine, then navigate the main menu through Machine ➤ Clone. Provide a new name for the system, and choose whether the new guest will have a different MAC address than the original guest; clearly this is required if both guests are to run at the same time on the same network. There are two types of clones: one where the original system is simply duplicated (full clone) and one where only the changes are recorded (linked clone). The clone can include all or none of the snapshots taken of the original guest.

A VirtualBox virtual machine can be copied to a different physical host by copying the directory containing the virtual machine's files. To add the copied guest to VirtualBox Manager on the destination host, navigate the main menu through Machine ➤ Add, then select the corresponding virtual machine file. Note that the copied system will still have the same MAC address as the original system. To change that MAC address, start with a powered-down guest. Navigate VirtualBox Manager's main menu through Machine ➤ Settings. Select Network on the left and the adapter. Open the Advanced submenu. The MAC address can be manually changed or a new random MAC address generated using the icon on the right of the MAC address. See Figure 1-3.



Ubuntu 12.04 (64 bit) Test System 2 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: NAT

Name:

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027A890F5

☑ Cable Connected

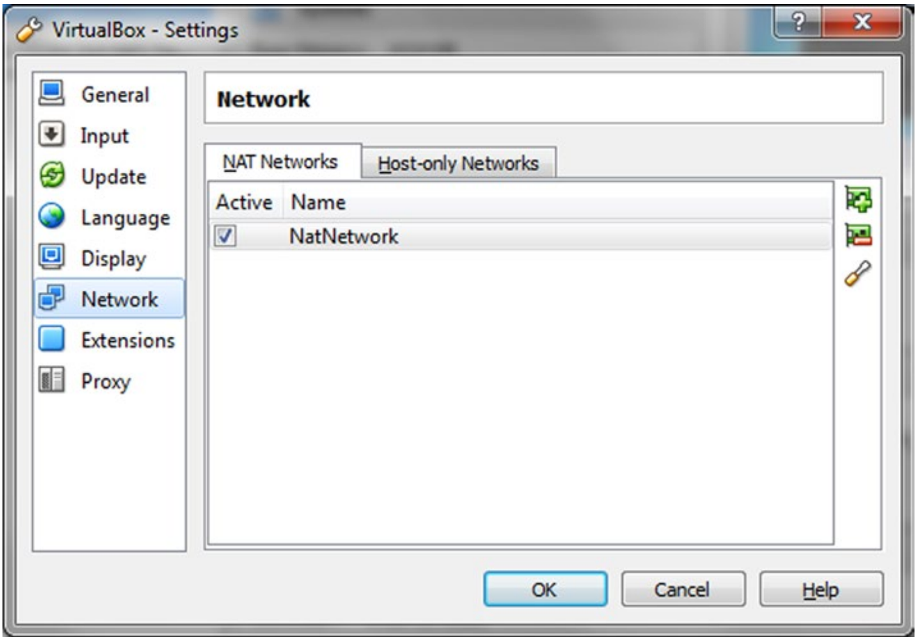
Figure 1-3. *Changing the MAC Address of a Guest in VirtualBox*

Networking

VirtualBox allows the user to choose from a range of hardware adapter types. The adapter(s) for a particular guest can be networked in different ways.

- The adapter can be connected to the host via network address translation (NAT). Unless changed manually, the first adapter connected to a NAT network will receive an address in 10.0.2/24, the second in 10.0.3/24 and so on. Though they can make outbound connections to the physical network, adapters connected via NAT cannot communicate with each other.

- The adapter can be connected to the host via NAT Network. To create a NAT Network, from the main menu for the VirtualBox Manager navigate File ➤ Preferences. Select Network from the left, then the NAT Networks tab. Use the green icon on the right to create a new NAT network, then use the screwdriver to set its properties. Key properties to set are the Network Name and its address range. By default, the first created network is named "NatNetwork," runs on 10.0.2/24, and has a DHCP server. See Figure 1-4.



Active	Name
☑	NatNetwork

Figure 1-4. *Creating a NAT Network in VirtualBox*

Once created, guest adapters can be connected to that particular NAT Network. These adapters can communicate with each other as well as make outbound connections to the physical network through a gateway at the .1 address.

- The adapter can be bridged to the same network as the host, and so act as another system on the physical network.

- The adapter can be connected to a host-only network. Adapters on this network can communicate with other adapters on the host-only network and with the host. The host usually has address 192.168.56.1 with other adapters in the range 192.168.56/24. By default, VirtualBox runs a DHCP server, giving out addresses in the range 192.168.56.101 – 192.168.56.254.
- The adapter can be connected to an internal network. Any adapter connected to an internal network with the same name can communicate with another, but adapters connected to internal networks with different names cannot communicate. Adapters on an internal network cannot communicate with the host.

VirtualBox Guest Additions

A number of features of VirtualBox require software to be installed on the guest itself; these tools are called VirtualBox Guest Additions. VirtualBox Guest Additions improve how the host and guest share the keyboard and mouse; after installation users can use the mouse to switch between the guest and other applications on the host rather than use the HOST key.

The additions also improve graphical performance in the guest, allowing the user to resize the window and having the guest automatically change its screen resolution to compensate. Another graphical improvement is called "Seamless Mode." It is controlled from the guest's VirtualBox main menu by navigating View ➤ Switch to Seamless Mode or via the shortcut key HOST+L. Once Seamless Mode is enabled, the guest's background is disabled, and windows displayed by the guest instead appear to be natively displayed by the host.

VirtualBox Additions provide simple ways the host and guest can share content. It provides the ability to drag and drop files between host and guest; it also provides the ability to share the clipboard so that things can be copied from the host then pasted to the guest and vice versa. Both features are controllable through the guest's VirtualBox main menu, under the Devices heading. Access can be granted from the host to the guest; from the guest to the host; bidirectional; or none, which is the default.

Another way the host and guest can share information after VirtualBox Guest Additions have been installed is through a shared folder. Configuration of shared folders is through the guest's VirtualBox main menu, under the Devices heading. To create a shared folder, choose the folder path on the host and the folder name which will be used to identify it to the guest. Permanent shares persist after the virtual machine is stopped while shares marked as auto-mount will be mounted into the file system when the guest starts. In the case of Windows guests, they receive a drive letter; in the case of Linux guests they appear in the `/media` directory with a name formed by prefixing `sf_` to the name of the share. Shares that are not automatically mounted can be found on a Windows guest as a networked file share in the location `\\VBOXSVR`. On a Linux system, suppose that the share has the name HostShare. Then the share can be mounted into any point in the file system (say `/media/HostShare`) with the commands

```
[root@localhost ~]# mkdir /media/HostShare
[root@localhost ~]# mount -t vboxsf HostShare /media/HostShare/
```

Building Linux Systems

There are a wide range of Linux distributions that are deployed in significant numbers. CentOS is a freely available open source version of Red Hat's commercial offerings, while OpenSuSE is a close relative of SuSE's commercial product. Ubuntu, developed by Canonical, is considered by many to be very end-user friendly. Mint is based on Ubuntu with different software choices, most notably a different desktop. It is hard to say which distribution is most popular, but Mint has been the most searched for distribution on distrowatch.com for some years. Kali is a specialized, penetration testing distribution that makes an excellent platform to learn more about offense. Each of these Linux distributions can be installed as a virtual machine, either in VMWare Workstation or in VirtualBox.

Configuring Software Repositories

These Linux distributions all use a package manager for software. The package manager is used when adding additional software to the system as well as managing security updates for the system. To keep these systems as they were deployed after installation and still retain the needed flexibility to install additional software, the package managers need to be configured to only use the original installation media as their source.[1] This process is slightly different for each distribution.

CentOS systems use yum to manage software; this package manager is configured in /etc/yum.conf and the configuration information for the stored repositories is contained in the directory /etc/yum.repos.d/ in files that end with .repo. CentOS 5.4 has two files in that directory

```
[root@localhost ~]# ls /etc/yum.repos.d/
CentOS-Base.repo  CentOS-Media.repo
```

while CentOS 6.0 has three

```
[root@localhost ~]# ls /etc/yum.repos.d/
CentOS-Base.repo  CentOS-Media.repo  CentOS-Debuginfo.repo
```

To configure CentOS to only use its installation media, change the extension of the files other than CentOS-Media.repo to something else; for example, rename CentOS-Base.repo to CentOS-Base.repo.unused. The file CentOS-Media.repo also needs to be modified, as in its default state the installation media repository is not enabled. Enable the repository and update the location of the base URL so that it correctly points to the location where the install discs are mounted. In CentOS 6.0, for example, this leads to a CentOS-Media.repo file with the contents

```
[c6-media]
name=CentOS-$releasever - Media
baseurl=file:///media/CentOS_6.0_Final/
gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

Validate that these settings are correct by running

```
[root@localhost ~]# yum repolist
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
repo id                         repo name                                   status
c6-media                        CentOS-6 - Media                            6,019
repolist: 6,019
```

to list all of the enabled repositories.

To configure CentOS, download packages online from the original sources, and create a new file in /etc/yum.repos.d/ – for example, /etc/yum.repos.d/online.repo. The file's contents should be similar to the following

[1] Systems kept in their initial state without any security patches are quite insecure; they should not be exposed on the Internet.

```
[Online]
name = Online
baseurl = http://vault.centos.org/6.0/os/x86_64/
gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

The file begins with the name of the repository. Next is the URL that contains the software packages used during installation for CentOS; adjust the URI to match the version and the architecture of the system. By way of comparison, for a 32-bit CentOS 5.4 system, the baseurl is

```
baseurl = http://vault.centos.org/5.4/os/i386/
```

GPG checking of packages should be enabled. The repository GPG key is included with the repository in the file RPM-GPG-KEY-CentOS-6; however, this should match the GPG key used with the installation media.

To validate the settings are correct, the command yum repolist shows both repositories, and the command yum update results in no changes to the system.

```
[root@localhost yum.repos.d]# yum repolist
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
repo id                          repo name                                 status
Online                           Online                                    6,019
c6-media                         CentOS-6 - Media                          6,019
repolist: 12,038

[root@localhost yum.repos.d]# yum update
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
Setting up Update Process
No Packages marked for Update
```

If yum is run before the repository list is updated, it may retain data from the initial run, and will insist packages need to be updated. Clear the cache with the command

```
[root@localhost yum.repos.d]# yum clean all
```

The command yum list available will list all available packages; to search for packages that contains “php” in the name, run the command yum list available *php*. To install a package along with all of its dependencies, use the command yum install packagename.

On OpenSuSE systems, package management is handled by zypper. Configuration information is kept in the directory /etc/zypp, and the collection of known repositories is kept in /etc/zypp/repos.d in files with the extension .repo. The information about the installation disc is contained is a file named after the version; for example, on OpenSuSE 11.3, that file is named openSuSE-11.3 11.3-1.82.repo. Rename the extension on the other files, then verify that only the installation media is enabled by running

```
test-dbc6ddcc6d:/etc/zypp/repos.d # zypper repos
# | Alias                   | Name                    | Enabled | Refresh
--+-------------------------+-------------------------+---------+--------
1 | openSUSE-11.3 11.3-1.82 | openSUSE-11.3 11.3-1.82 | Yes     | No
```

To configure OpenSuSE to download packages online from original sources, create a new file in /etc/zypp/repos.d, for example, /etc/zypp/repos.d/online.repo with content in the form

```
[Online]
name=Online
enabled=1
autorefresh=1
baseurl=http://ftp5.gwdg.de/pub/opensuse/discontinued/distribution/11.3/repo/oss/
path=/
type=yast2
keeppackages=0
```

The base URL points to the packages for OpenSuSE 11.3 at one of the mirrors for discontinued versions of OpenSuSE; https://en.opensuse.org/openSUSE:Mirrors has the list. Not all packages provided by OpenSuSE are included on the installation media (like the GNU accounting tools used in Chapter 3), so if this is not done, then it will be occasionally necessary to manually download additional packages, along with their dependencies.

To validate the changes, check the list of installed repositories and verify that no new updates are required.

```
test-dbc6ddcc6d:/etc/zypp/repos.d # zypper repos
# | Alias                     | Name                      | Enabled | Refresh
--+---------------------------+---------------------------+---------+--------
1 | Online                    | Online                    | No      | Yes
2 | openSUSE-11.3 11.3-1.82   | openSUSE-11.3 11.3-1.82   | Yes     | No
vega:~ # zypper update
Loading repository data...
Reading installed packages...

Nothing to do.
```

The command zypper search findthis will list any packages with “findthis” in either the package name or its description. To install a package along with all of its dependencies, use the command zypper install packagename.

In Ubuntu systems including Ubuntu server, package management is handled by apt; configuration information is kept in the directory /etc/apt/ and the list of enabled repositories is in /etc/apt/sources.list. Edit this list and comment out all sources other than the installation media, and be sure that the line with the installation media (the first line) is uncommented. Update the repository list on the system by running

```
cjacobi@Ubuntu904:/etc/apt$ sudo apt-get update
[sudo] password for cjacobi:
Ign cdrom://Ubuntu 9.04 _Jaunty Jackalope_ - Release i386 (20090420.1) jaunty/main
Translation-en_US
Ign cdrom://Ubuntu 9.04 _Jaunty Jackalope_ - Release i386 (20090420.1) jaunty/restricted
Translation-en_US
Reading package lists... Done
```

Notice that the only listed sources are from the installation disc, as planned.

To configure Ubuntu to download packages online from the original sources, add two lines like the following to /etc/apt/sources.list.

```
deb http://old-releases.ubuntu.com/ubuntu/ jaunty main restricted universe
deb-src http://old-releases.ubuntu.com/ubuntu/ jaunty main restricted universe
```

The URLs point to the archive of older Ubuntu releases. The name jaunty comes from the name of the version of Ubuntu, which can be found online or directly from the system with the command

```
cjacobi@Ubuntu904:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 9.04
Release:        9.04
Codename:       jaunty
```

Ubuntu systems such as Ubuntu 12.04 (precise) are long-term support (LTS) releases. For such systems the appropriate lines in /etc/apt/sources.list are

```
deb http://us.archive.ubuntu.com/ubuntu/ precise main restricted universe
deb-src http://us.archive.ubuntu.com/ubuntu/ precise main restricted universe
```

that are present in the original file.

To validate the changes, verify that no additional updates are required by running

```
cjacobi@ Ubuntu904:/etc/apt$  sudo apt-get update
[sudo] password for cjacobi:
Ign cdrom://Ubuntu 9.04 _Jaunty Jackalope_ - Release i386 (20090420.1) jaunty/main
Translation-en_US
Ign cdrom://Ubuntu 9.04 _Jaunty Jackalope_ - Release i386 (20090420.1) jaunty/restricted
Translation-en_US
Hit http://old-releases.ubuntu.com jaunty Release.gpg
Ign http://old-releases.ubuntu.com jaunty/main Translation-en_US
Ign http://old-releases.ubuntu.com jaunty/restricted Translation-en_US
Hit http://old-releases.ubuntu.com jaunty Release
Hit http://old-releases.ubuntu.com jaunty/main Packages
Hit http://old-releases.ubuntu.com jaunty/restricted Packages
Hit http://old-releases.ubuntu.com jaunty/main Sources
Hit http://old-releases.ubuntu.com jaunty/restricted Sources
Reading package lists... Done
cjacobi@Ubuntu904:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

The command apt-cache search findthis will list any available package with “findthis” in either the package name or in the package description. To install a package along with all of its dependencies, use the command apt-get install packagename.

The situation with Mint is similar, though the installation media will not be included in sources.list. Instead the first entry is for Mint specific packages, while the remaining entries are for the corresponding Ubuntu repositories. Moreover, because of slight variations between Mint and Ubuntu, some small number of packages may be upgraded. For example, take a Mint 11 system, comment out all of the existing package sources, and add the proper source for old releases, giving a file /etc/apt/sources.list with the content

```
deb http://old-releases.ubuntu.com/ubuntu/ natty main restricted universe multiverse

#deb http://packages.linuxmint.com/ katya main upstream import
#deb http://archive.ubuntu.com/ubuntu/ natty main restricted universe multiverse
#deb http://archive.ubuntu.com/ubuntu/ natty-updates main restricted universe multiverse
#deb http://security.ubuntu.com/ubuntu/ natty-security main restricted universe multiverse
#deb http://archive.canonical.com/ubuntu/ natty partner
#deb http://extras.ubuntu.com/ubuntu natty main
#deb http://packages.medibuntu.org/ natty free non-free

#deb http://archive.getdeb.net/ubuntu natty-getdeb apps
#deb http://archive.getdeb.net/ubuntu natty-getdeb games
```

Then after running apt-get update, the upgrade process indicates two packages need to be updated.

```
acauchy@aldeberan ~ $ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  gtk2-engines-aurora yelp
2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 622 kB of archives.
After this operation, 2,089 kB disk space will be freed.
Do you want to continue [Y/n]?
```

Ubuntu Server

There is a known issue with VMWare Workstation detecting the wrong keyboard layout for some Ubuntu servers; for example, this can happen with VMWare Workstation 10 and Ubuntu 10.04. If this occurs, a number of keys will not function correctly, including some arrow keys. The solution is to log on to the system and run

```
egalois@ubuntu:~$ sudo dpkg-reconfigure console-setup
```

This drops the user to a setup program to choose the keyboard. Although problems with the arrow keys prevent simple navigation of the menu, select “g”; this brings up the first entry that begins with g, which is a generic 101 key keyboard and one that works well.

Ubuntu server does not install a graphical user interface; it also uses a very low (640x480) resolution for the plain text screen. This can be modified by editing /etc/default/grub. To change the resolution to something more palatable, for example, 1024x768 with 24 bit color, add the following two lines

```
GRUB_GFXMODE=1024x768x24
GRUB_GFXPAYLOAD_LINUX=keep
```

After making the change, run /usr/sbin/update-grub and reboot the system. Other resolutions are supported, including 800x600 and 1366x768x24.

Kali Linux is intended for use primarily as an attacking system, so it should be kept up to date with the latest patches and tools. It also uses apt to manage packages. Because Kali uses apt to distribute updates to many tools, most notably Metasploit, the commands apt-get update && apt-get dist-upgrade should be regularly run.

Virtualization Support

The process to provide virtualization support within the guest depends on whether the virtual machine is running within VMWare Workstation or VirtualBox.

VMWare Tools

For most Linux systems, VMWare Tools is installed by the VMWare Workstation Easy Install process; this is the case for CentOS, OpenSuSE, Ubuntu, and Mint systems.

VMWare Workstation does not use Easy Install when installing Kali 1.0.7, so VMWare Tools must be installed manually. Both a compiler and the kernel headers for the running kernel are necessary before the VMWare Tools installation script can complete. Kali 1.0.7 comes with gcc; the kernel headers can be downloaded via

```
root@kali:~# apt-get install linux-headers-`uname -r`
```

Navigate the main VMWare Workstation menu through VM ➤ Install VMWare Tools. This will configure a virtual CD-ROM in the guest operating system that contains the necessary software. Mount that device if it is not mounted automatically. Copy the VMWare Tools package to a convenient directory and unpack it. Enter that directory and run the installation script, named vmware-install.pl. [2]

```
root@kali:~# cp /media/cdrom/VMwareTools-9.6.0-1294478.tar.gz  ./
root@kali:~# tar -xzvf ./VMwareTools-9.6.0-1294478.tar.gz
--- output deleted ---
root@kali:~# cd vmware-tools-distrib/
root@kali:~/vmware-tools-distrib# ./vmware-install.pl
```

VirtualBox Guest Additions

VirtualBox Guest Additions must be installed manually on most Linux distributions. Because it requires special features in the system's kernel, it may require the ability to compile software as well as the headers for the running kernel.

To install VirtualBox Guest Additions on CentOS, begin by installing the compiler and kernel headers by running

```
[root@localhost ~]# yum groupinstall "development tools"
```

[2] The precise version of VMWare Tools may vary with the version of VMWare.

Some versions of CentOS (*e.g.,* 6.0) include the `kernel-devel` package in the development tools group, while others (*e.g.,* 5.4) do not. Install it if it is not present. Unmount any CD in the guest, then navigate the VirtualBox main menu for the guest through Devices ➤ Insert Guest Additions CD. On some CentOS systems (*e.g.,* 6.0) this will autorun the correct program; in others (*e.g.,* 5.4) it must be started manually. In the latter case, navigate to the location where the Guest Additions CD is mounted (`/media/VBOXADDITIONS_4.3.12_93733/`)[3] and run the installation script as root

```
[root@localhost VBOXADDITIONS_4.3.12_93733]# sh VBoxLinuxAdditions.run
```

If the process completes without errors, then the installation is complete after the system reboots.

The situation on OpenSuSE is somewhat simpler, as OpenSuSE includes a version of VirtualBox Guest Additions that is installed by default. For example, on an OpenSuSE 11.3 Desktop installation:

```
localhost:/etc/zypp/repos.d # zypper search virtualbox
Loading repository data...
Reading installed packages...

S | Name                              | Summary                          | Type
--+-----------------------------------+----------------------------------+--------
  | virtualbox-ose                    | VirtualBox OSE is an Emulator    | package
i | virtualbox-ose-guest-kmp-default  | Guest kernel modules for Virt->  | package
  | virtualbox-ose-guest-kmp-desktop  | Guest kernel modules for Virt->  | package
i | virtualbox-ose-guest-tools        | VirtualBox guest tools           | package
  | virtualbox-ose-host-kmp-default   | Host kernel module for Virtua->  | package
  | virtualbox-ose-host-kmp-desktop   | Host kernel module for Virtua->  | package
i | xorg-x11-driver-virtualbox-ose    | VirtualBox X11 drivers for mo->  | package
```

Unfortunately, these tools are incomplete. They are sufficient for graphics, including seamless mode; they also provide a shared clipboard. They are insufficient for dragging/dropping files to/from the host or for shared folders.

It is possible to recover the missing functionality by removing the older versions, installing the necessary compiler and kernel development tools, then installing the tools provided by VirtualBox.

The older software can be removed by running

```
localhost:/etc/zypp/repos.d # zypper rm virtualbox-ose-guest-kmp-default virtualbox-ose-
guest-tools xorg-x11-driver-virtualbox-ose
```

and rebooting. The required development tools are then installed with

```
localhost:~ # zypper install gcc make kernel-devel
```

Load the VirtualBox Guest Additions CD, move to the correct directory and run

```
localhost:/media/VBOXADDITIONS_4.3.12_93733 # sh VBoxLinuxAdditions.run
```

If the process completes without errors, then the installation is complete after the system reboots.

Installing VirtualBox Guest Additions on Ubuntu depends on the particular version of Ubuntu. In an older system such as Ubuntu 9.04 Desktop, all of the necessary packages are installed by default. Mount the VirtualBox Guest Additions CD, move to the correct directory, and run `sh VBoxLinuxAdditions.run`.

[3] The precise version may depend on the version of VirtualBox.

Later systems such as Ubuntu 11.04 Desktop or 12.04 Desktop use a slightly different process. They need the dkms package, which depends on the fakeroot package; fakeroot is installed by default on Ubuntu 11.04 but not on 12.04, and must be installed separately. Install dkms (and fakeroot if needed)

```
enoether@Ubuntu1104:~$ sudo apt-get install dkms
```

When the installation completes, load the VirtualBox Guest Additions CD. It will prompt the user to run automatically. Once it finishes, the installation is complete.

The process for Mint systems also varies with the version. For older systems such as Mint 11, all of the necessary prerequisite packages are installed. Mount the VirtualBox Guest Additions CD, move to the correct directory and run sh VBoxLinuxAdditions.run. Newer versions are even easier, as VirtualBox Guest Additions is installed by default.

To install VirtualBox Guest Additions on Kali 1.0.7, first install the kernel headers

```
root@kali:~# apt-get install linux-headers-`uname -r`
```

Mount the VirtualBox Guest Additions CD, move to the correct directory, and run
sh VBoxLinuxAdditions.run.

Networking and Basic Configuration

Though Linux systems share many common elements, different Linux distributions have customized and modified how to configure networking.

CentOS

If a CentOS 6 system is created by cloning a VirtualBox system or copying a VMWare Workstation system, then the network adapter in the system should be assigned a different MAC address than the original. Because the CentOS udev device manager tracks the MAC address assigned to each network card, the copied guest will not have an eth0 card, but will have an eth1 card. To modify this behavior, edit the file /etc/udev/rules.d/70-persistent-net.rules. In a cloned CentOS 6.0 system, this contains lines like

```
# PCI device 0x8086:0x100e (e1000) (custom name provided by external tool)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="08:00:27:19:7c:72",
ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"

# PCI device 0x8086:0x100e (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="08:00:27:59:cf:0e",
ATTR{type}=="1", KERNEL=="eth*", NAME="eth1"
```

The first line is the information for the adapter from before the system was copied/cloned, while the second is for the now-installed adapter. Delete the line for the original adapter, and update the name for the second, so the file instead contains

```
# PCI device 0x8086:0x100e (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="08:00:27:59:cf:0e",
ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
```

After reboot, the system will correctly identify the present adapter with eth0.

To set the host name on a CentOS system, two files must be modified. Suppose a CentOS 6.0 system is to be given the FQDN sirius.stars.example. The file /etc/sysconfig/network needs the content

```
NETWORKING=yes
HOSTNAME=sirius.stars.example
```

The file /etc/hosts also needs to be modified so that the loopback addresses have the correct hostname

```
127.0.0.1       localhost.localdomain   localhost sirius sirius.stars.example
::1             localhost6.localdomain6 localhost6 sirius sirius.stars.example
```

The situation in other CentOS systems is similar. A reboot of the system shows the new name reflected in the login screen and the bash command prompts.

If the hostname of the system differs from the contents in /etc/hosts, then apparently unrelated components may fail.

To set up a CentOS system with a static network address, update the file /etc/sysconfig/network-scripts/ifcfg-eth0 with the necessary information.

```
DEVICE="eth0"
TYPE="Ethernet"
USERCTL="no"
ONBOOT="yes"
BOOTPROTO="none"
HWADDR="08:00:27:59:CF:0E"
IPADDR="10.0.2.10"
NETMASK="255.255.255.0"
GATEWAY="10.0.2.1"
IPV6INIT="no"
PEERDNS="no"
DNS1="8.8.8.8"
DNS2="8.8.4.4"
DOMAIN="stars.example"
```

The significance of most of these lines is self-explanatory, though CentOS provides additional documentation in the file /usr/share/doc/initscripts-x.yy.zz/sysconfig.txt (the directory varies with the version of CentOS). Be sure that the MAC address in the configuration file actually matches the hardware MAC address.

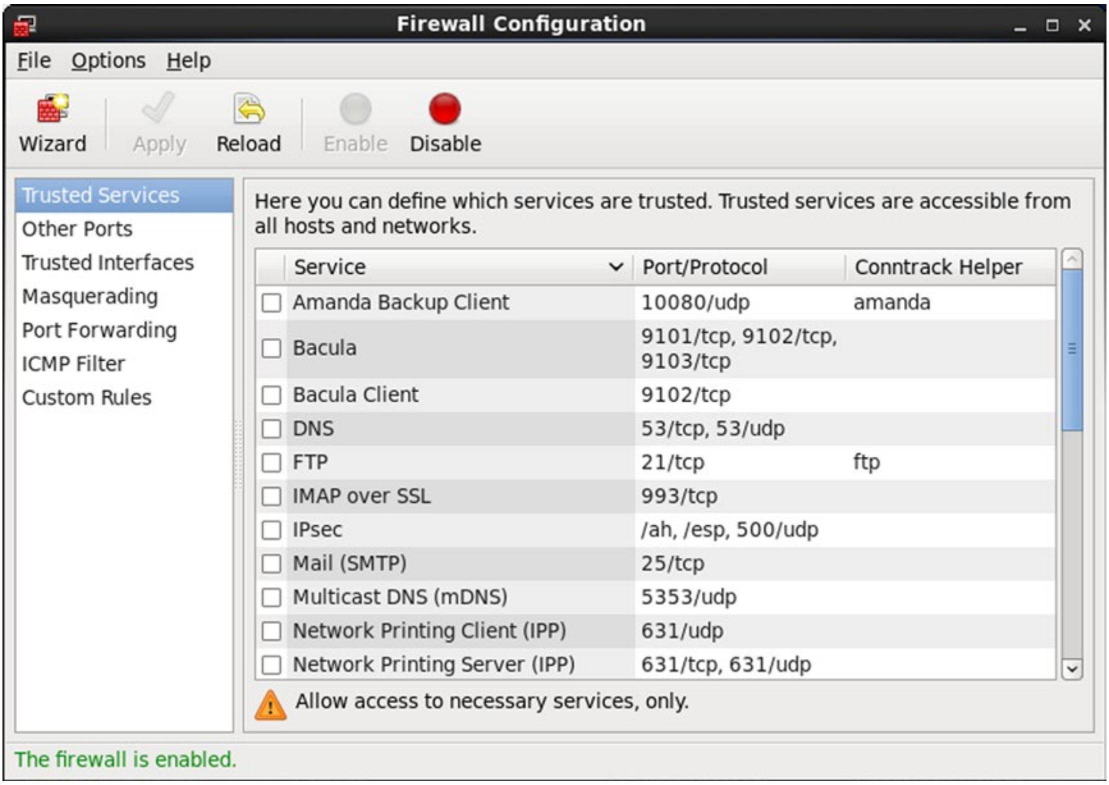
Linux systems can use aliases to provide more than one IP address for an adapter. Create a file named ifcfg-eth0:0 duplicated from /etc/sysconfig/network-scripts/ifcfg-eth0. Modify the DEVICE name in that file to read eth0:0, modify the static IP address to a new value, delete the line providing gateway information, and delete the DNS information. The resulting file looks something like the following.

```
[root@sirius ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0:0
DEVICE="eth0:0"
TYPE="Ethernet"
USERCTL="no"
ONBOOT="yes"
BOOTPROTO="none"
HWADDR="08:00:27:59:CF:0E"
IPADDR="10.0.2.12"
NETMASK="255.255.255.0"
IPV6INIT="no"
```

Aliased IP addresses cannot be configured using DHCP. After a system reboot both addresses are available.

```
[pfermat@sirius ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:CF:0E
          inet addr:10.0.2.10  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe59:cf0e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9036 (8.8 KiB)  TX bytes:5664 (5.5 KiB)

eth0:0    Link encap:Ethernet  HWaddr 08:00:27:59:CF:0E
          inet addr:10.0.2.12  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)
```

Both CentOs 5.x and 6.x have a graphical interface for the firewall; on CentOS 5.4 for example, it is started by navigating the main menu through System ➤ Administration ➤ Security Level and Firewall, while in CentOS 6.0 it is System ➤ Administration ➤ Firewall. Both offer roughly the same options; Figure 1-5 shows the configuration tool from CentOS 6.0.



Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

	Service	Port/Protocol	Conntrack Helper
□	Amanda Backup Client	10080/udp	amanda
□	Bacula	9101/tcp, 9102/tcp, 9103/tcp	
□	Bacula Client	9102/tcp	
□	DNS	53/tcp, 53/udp	
□	FTP	21/tcp	ftp
□	IMAP over SSL	993/tcp	
□	IPsec	/ah, /esp, 500/udp	
□	Mail (SMTP)	25/tcp	
□	Multicast DNS (mDNS)	5353/udp	
□	Network Printing Client (IPP)	631/udp	
□	Network Printing Server (IPP)	631/tcp, 631/udp	

⚠ Allow access to necessary services, only.

The firewall is enabled.

Figure 1-5. *The Firewall Configuration Tool in CentOS 6.0*

CentOS systems install SELinux by default. SELinux modifies the kernel to provide additional security features and finer-grained access control. Though effective and useful, it is also very difficult to configure, extremely difficult to debug, and many deployed systems ran with SELinux disabled.

Set SELinux to permissive mode by editing the file `/etc/selinux/config`; this will require a system reboot. In permissive mode, SELinux runs, but does not prevent access violations. SELinux can temporarily be set into permissive mode with either the command

```
[root@sirius ~]# setenforce permissive
```

or

```
[root@sirius ~]# echo 0 > /selinux/enforce
```

A change made this way persists only until the next system reboot.

OpenSuSE

OpenSuSE virtual machines in VMWare Workstation can be copied and moved in the same fashion as other virtual machines. However in VirtualBox, creating full clones of OpenSuSE virtual machines requires some preparation. The fundamental problem is that VirtualBox has an ID for each virtual machine, and on OpenSuSE this is tied to the identifier for the hard drive. When a full clone of the system is made, a new ID is generated for the system and the hard drive, but the configuration files within OpenSuSE continue to refer to the old ID. As a consequence the cloned system will not boot.

The simplest solution is to modify the system before it is cloned. Because mistakes in this process can render the original system unbootable, start by taking a recovery snapshot of the OpenSuSE system. Open the file `/etc/fstab`, which provides information about the various filesystems. For example, in an OpenSuSE 11.3 system, this file has the contents

```
/dev/disk/by-id/ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part1 swap    swap  defaults       0 0
/dev/disk/by-id/ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part2 /         t4  acl,user_xattr 1 1
/dev/disk/by-id/ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part3 /home   ext4  acl,user_xattr 1 2
proc                 /proc                proc       defaults              0 0
sysfs                /sys                 sysfs      noauto                0 0
debugfs              /sys/kernel/debug    debugfs    noauto                0 0
usbfs                /proc/bus/usb        usbfs      noauto                0 0
devpts               /dev/pts             devpts     mode=0620,gid=5       0 0
```

The precise layout seen here depends on both the version of OpenSuSE and the choices made during installation.

The problem can now be seen. The system is using the system ID to identify the different partitions on the hard drive; when that ID is changed by cloning it no longer points to the hard drive and the system does not boot. To solve the problem, notice that these are simply links in the file system

```
linux-md1b:~ # ls -l /dev/disk/by-id/
total 0
lrwxrwxrwx 1 root root  9 Jul  4 10:31 ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7 -> ../../sda
lrwxrwxrwx 1 root root 10 Jul  4 10:31 ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part1 -> ../../sda1
lrwxrwxrwx 1 root root 10 Jul  4 10:31 ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part2 -> ../../sda2
lrwxrwxrwx 1 root root 10 Jul  4 10:31 ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part3 -> ../../sda3
lrwxrwxrwx 1 root root  9 Jul  4 10:31 scsi-SATA_VBOX_HARDDISK_VBcf603ece-d2a3ecb7 -> ../../sda
lrwxrwxrwx 1 root root 10 Jul  4 10:31 scsi-SATA_VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part1 ->
../../sda1
lrwxrwxrwx 1 root root 10 Jul  4 10:31 scsi-SATA_VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part2 ->
../../sda2
lrwxrwxrwx 1 root root 10 Jul  4 10:31 scsi-SATA_VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part3 ->
../../sda3
```

To solve the problem, replace the links by their targets; in this example `/etc/fstab` becomes

```
/dev/sda1            swap                 swap       defaults              0 0
/dev/sda2            /                    ext4       acl,user_xattr        1 1
/dev/sda3            /home                ext4       acl,user_xattr        1 2
proc                 /proc                proc       defaults              0 0
sysfs                /sys                 sysfs      noauto                0 0
debugfs              /sys/kernel/debug    debugfs    noauto                0 0
usbfs                /proc/bus/usb        usbfs      noauto                0 0
devpts               /dev/pts             devpts     mode=0620,gid=5       0 0
```

Links using the system's ID are also used by the bootloader, grub. In the OpenSuSE 11.3 example system, the file /boot/grub/menu.1st has the contents

```
###Don't change this comment - YaST2 identifier: Original name: linux###
title openSUSE 11.3 - 2.6.34-12
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.34-12-default root=/dev/disk/by-id/ata-VBOX_HARDDISK_
VBcf603ece-d2a3ecb7-part2 resume=/dev/disk/by-id/ata-VBOX_HARDDISK_VBcf603ece-d2a3ecb7-part1
splash=silent quiet showopts vga=0x314
    initrd /boot/initrd-2.6.34-12-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- openSUSE 11.3 - 2.6.34-12
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.34-12-default root=/dev/disk/by-id/ata-VBOX_HARDDISK_
VBcf603ece-d2a3ecb7-part2 showopts apm=off noresume nosmp maxcpus=0 edd=off powersaved=off
nohz=off highres=off processor.max_cstate=1 nomodeset x11failsafe vga=0x314
    initrd /boot/initrd-2.6.34-12-default
```

The root directory is specified as a link in both boot menu entries, and the resume point is specified as a link in the first. Update this with the destination of the links so that it becomes

```
###Don't change this comment - YaST2 identifier: Original name: linux###
title openSUSE 11.3 - 2.6.34-12
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.34-12-default root=/dev/sda2 resume=/dev/sda1 splash=silent
quiet showopts vga=0x314
    initrd /boot/initrd-2.6.34-12-default

###Don't change this comment - YaST2 identifier: Original name: failsafe###
title Failsafe -- openSUSE 11.3 - 2.6.34-12
    root (hd0,1)
    kernel /boot/vmlinuz-2.6.34-12-default root=/dev/sda2 showopts apm=off noresume nosmp
maxcpus=0 edd=off powersaved=off nohz=off highres=off processor.max_cstate=1 nomodeset
x11failsafe vga=0x314
    initrd /boot/initrd-2.6.34-12-default
```

Save and reboot the system; it is then safe to clone.

Once an OpenSuSE virtual machine is copied (VMWare Workstation) or cloned (VirtualBox) and started, networking will not initially be functioning. Indeed, running ifconfig will show only the loopback interface; the command ifconfig -a is required to even see the network card. The issue is the same as it was for CentOS; the file /etc/udev/rules.d/70-persistent-net.rules contains information about the original adapter from the system before it was cloned as eth0, and information about the new, currently installed adapter as eth1. The system is set to only use the eth0 adapter, which now no longer exists.
The solution is to remove the no longer needed line for the original adapter and update the line for the new adapter to use eth0 as described for CentOS systems. Reboot the system and verify that the network functions.

To change the hostname of an OpenSuSE system, two files need to be changed. The first is the file /etc/HOSTNAME; it needs the FQDN of the system on a single line. The other file is /etc/hosts; the loopback addresses need to be updated with the system's new name. On an OpenSuSE 12.1 system named arcturus.stars.example, this results in an /etc/hosts file with the content

```
127.0.0.1       localhost arcturus arcturus.stars.example

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback arcturus arcturus.stars.example
fe00::0         ipv6-localnet
ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
```

Setting up OpenSuSE to use a static IP address with a defined name server and gateway requires editing three files. The first file is /etc/sysconfig/network/ifcfg-eth0, and it specifies only the properties of the adapter.

```
STARTMODE="auto"
BOOTPROTO="static"
IPADDR=10.0.2.14
NETMASK=255.255.255.0
USERCONTROL="no"
```

Other available options for this file are specified in /etc/sysconfig/network/ifcfg.template. To commit changes to the adapter settings, push the adapter down and then bring it up with the command pair.

```
arcturus:/etc/sysconfig/network # ifdown eth0
    eth0      device: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
arcturus:/etc/sysconfig/network # ifup eth0
    eth0      device: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
```

Because routing information is considered global information rather than a property of the interface, it is configured in a separate file. If the file /etc/sysconfig/network/routes does not exist, create it. It should contain a single line that specifies the (default) gateway (10.0.2.1 in this example) in the form

```
default 10.0.2.1
```

To commit this change to the routing table, push the routing table for eth0 down then up with the pair of commands

```
arcturus:~ # /etc/sysconfig/network/scripts/ifdown-route eth0
arcturus:~ # /etc/sysconfig/network/scripts/ifup-route eth0
```

Configuration for the name server is done in the third file /etc/sysconfig/network/config. This file contains a number of options; to set the locations for the DNS servers to 8.8.8.8 and 8.8.4.4, update the option.

```
NETCONFIG_DNS_STATIC_SERVERS="8.8.8.8 8.8.4.4"
```

This is located in different locations within the file depending on the version of OpenSuSE; in a default install of OpenSuSE 11.3 it is line 267, while for OpenSuSE 12.1 it is line 297. To commit changes made to the location of the DNS server, run the command

```
arcturus:/etc/sysconfig/network # netconfig update
```

Additional IP addresses for an interface can be specified in /etc/sysconfig/network/ifcfg-eth0 by adding an appropriate suffix to the IPADDR variable; for example

```
STARTMODE="auto"
BOOTPROTO="static"
IPADDR=10.0.2.14
NETMASK=255.255.255.0
USERCONTROL="no"

IPADDR_2=10.1.2.16
NETMASK_2=255.255.255.0
```

Push the adapter down and back up to commit the change. The new address will not appear with ifconfig

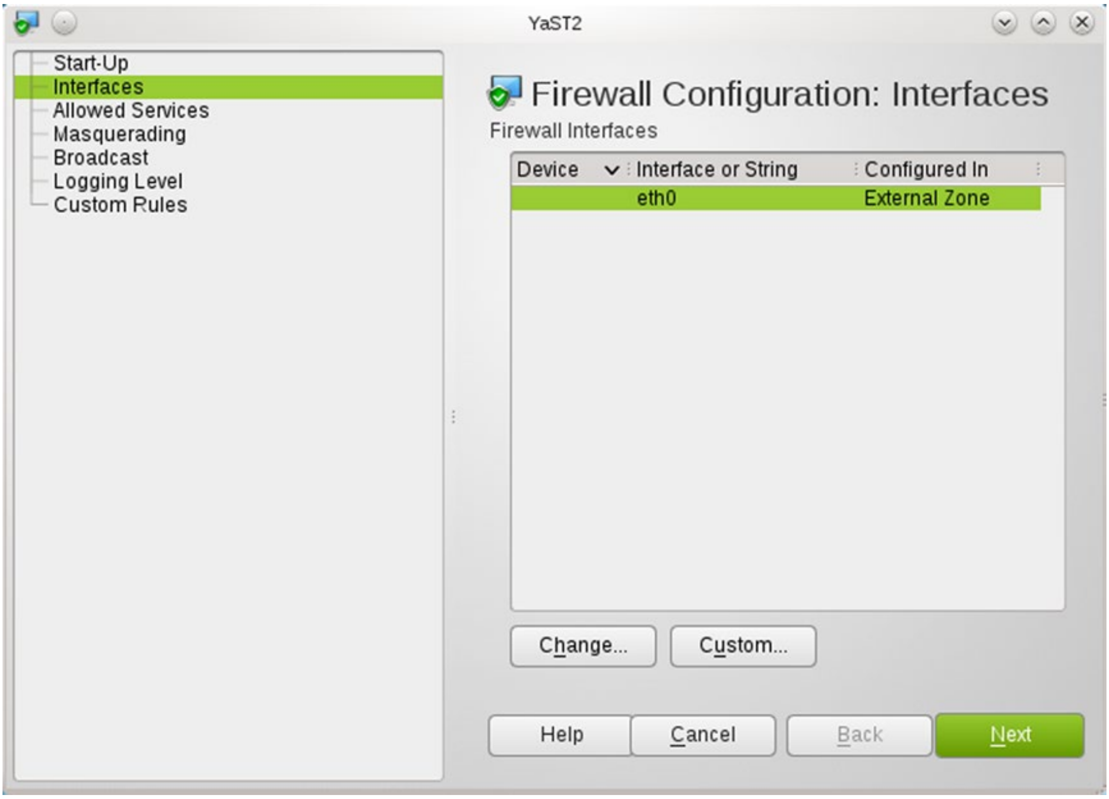
```
arcturus:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:E5:D2:0B
          inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:d20b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:219 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45279 (44.2 Kb)  TX bytes:19782 (19.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7201 (7.0 Kb)  TX bytes:7201 (7.0 Kb)
```

but will appear with ip

```
arcturus:~ # ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:e5:d2:0b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.14/24 brd 10.0.2.255 scope global eth0
    inet 10.0.2.16/24 brd 10.0.2.255 scope global secondary eth0
    inet6 fe80::a00:27ff:fee5:d20b/64 scope link
       valid_lft forever preferred_lft forever
```

It is even possible to set an OpenSuSE adapter to respond to an entire address range; see /etc/sysconfig/network/ifcfg.template for details.

OpenSuSE also comes with a full-featured graphical configuration tool called YaST; all of these network changes can be made through YaST. YaST also provides a graphical user interface to the firewall. Different interfaces can be placed in different zones, with different firewall rules applied to each zone. Figure 1-6 shows the YaST2 firewall configuration tool on OpenSuSE 12.1



Firewall Configuration: Interfaces

Firewall Interfaces

Device	Interface or String	Configured In
	eth0	External Zone

Figure 1-6. *The YaST Firewall Configuration Tool for OpenSuSE 12.1*

Ubuntu

Ubuntu systems also use the udev device manager, so cloned or copied systems may have their adapter on eth1 instead of eth0. The solution is to edit the file /etc/udev/rules.d/70-persistent-net.rules to delete the information from the adapter that was present before the system was cloned and to change the name for the present adapter from eth1 to eth0 as described for CentOS systems.

To update the hostname for an Ubuntu system, put the FQDN for the system in the file /etc/hostname. Modify the file /etc/hosts so that the loopback addresses for both IP and IPv6 refer to the chosen hostname. For example, if the system's FQDN is betelgeuse.stars.example, then /etc/hosts can have the content

```
127.0.0.1       localhost betelgeuse betelgeuse.stars.example

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback betelgeuse betelgeuse.stars.example
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Configuring Ubuntu systems to use static networking varies somewhat between versions, with servers behaving differently from desktop systems. The simplest cases are newer server systems, such as Ubuntu 12.04 server. In this case, update the file /etc/network/interfaces with content like

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 10.0.2.21
netmask 255.255.255.0
gateway 10.0.2.1
dns-nameservers 8.8.8.8 8.8.4.4
dns-search stars.example
```

The first two lines refer to the loopback interface; if they are removed then the loopback will not function, and that will cause some highly amusing system errors later.

To commit the changes to the system, restart the networking service by stopping and starting the service

```
egalois@achernar:~$ sudo /etc/init.d/networking stop
... Output Deleted ...
egalois@achernar:~$ sudo /etc/init.d/networking start
```

When complete, verify that the interface is correctly configured

```
egalois@achernar:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:38:d5:36 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.21/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe38:d536/64 scope link
       valid_lft forever preferred_lft forever
```

A check of the resolver file /etc/resolv.conf before the system is rebooted may reveal older data

```
egalois@achernar:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.1.1
nameserver 8.8.8.8
nameserver 8.8.4.4
search stars.example
```

Here, the first nameserver at 192.168.1.1 is not part of the configuration file /etc/networking/interfaces, but rather is older data from before the interface was changed:

```
egalois@achernar:~$ ls /run/resolvconf/interface
eth0.dhclient  eth0.inet
egalois@achernar:~$ cat /run/resolvconf/interface/eth0.dhclient
nameserver 192.168.1.1
```

When the system is rebooted, this older data will be removed.

The process is similar for older Ubuntu servers except that rather than specifying the nameserver in /etc/network/interfaces, the file /etc/resolv.conf must be manually configured. For example, on Ubuntu 10.04 server update the file /etc/networking/interface in the same fashion, then stop and start networking. Note that the contents of /etc/resolv.conf remain unchanged. Manually make the necessary modifications to that file so it contains

```
nameserver 8.8.8.8
nameserver 8.8.4.4
search stars.example
```

Reboot the system to verify that both the interface and the resolver function as expected.

Network settings on Ubuntu Desktop systems can be managed through a graphical user interface. It is possible to configure the network without using the graphical tool. On an Ubuntu 12.04 desktop, the process is the same as it is on an Ubuntu 12.04 server.

Command line network configuration of older desktop systems is a bit more problematic. As an example, consider an Ubuntu 11.04 Desktop system. Update the file /etc/network/interfaces in the now usual fashion, then stop and start the networking service. As was the case with older server systems, the file /etc/resolv.conf is not modified to contain new nameserver data. However, if that file is modified by hand, then the graphical tool (NetworkManager) will later overwrite the changes, even if NetworkManager is not managing any of the adapters on the system. To avoid the problem, the simplest solution is to make /etc/resolv.conf immutable after it is correctly configured.

```
enoether@procyon:~$ sudo chattr +i /etc/resolv.conf
```

To add additional addresses to an adapter, add the configuration information to /etc/network/interfaces as follows

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 10.0.2.19
netmask 255.255.255.0
gateway 10.0.2.1
dns-nameservers 8.8.8.8 8.8.4.4
dns-search stars.example

auto eth0:0
iface eth0:0 inet static
address 10.0.2.22
netmask 255.255.255.0
```

Stop and start networking; the alias interface should be visible with both ifconfig and ip.

Firewalls are disabled by default on Ubuntu systems, and Ubuntu desktop systems do not come installed with a graphical user interface to enable or manage firewalls.

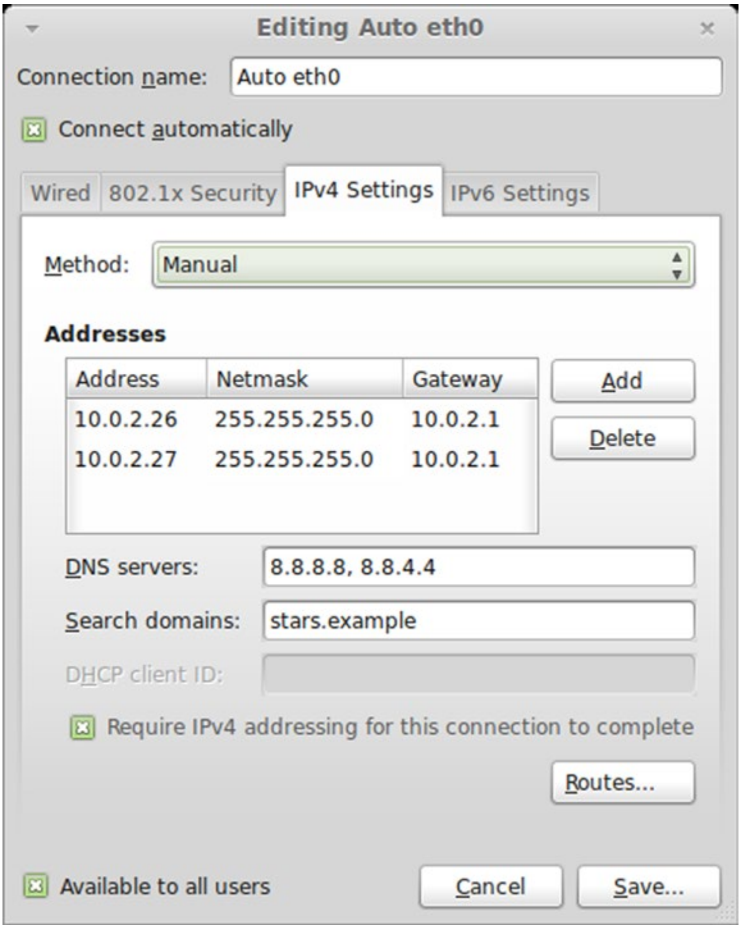
Mint

Mint systems also use the udev device manager, so cloned or copied systems may have their adapter on eth1 instead of eth0. The solution is to edit the file /etc/udev/rules.d/70-persistent-net.rules to delete the information from the adapter that was present before the system was cloned and to change the name for the present adapter from eth1 to eth0 as described for CentOS systems.

To update the hostname for a Mint system, proceed as if it were an Ubuntu system. Put the FQDN for the system in the file /etc/hostname, and modify the file /etc/hosts so that the loopback addresses for both IP and IPv6 refer to the chosen hostname.

Though it is possible to use the command line to configure networking on Mint systems, it is simpler to use the graphical tools. Moreover, these are the same graphical tools that would be used on an Ubuntu system.

For example, on a Mint 11 system, use the start menu to launch the control panel; then select Network Connections from the Internet and Network group. Edit the eth0 interface and update the IPv4 settings as desired. See Figure 1-7.



Connection name: Auto eth0

☒ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
10.0.2.26	255.255.255.0	10.0.2.1
10.0.2.27	255.255.255.0	10.0.2.1

DNS servers: 8.8.8.8, 8.8.4.4

Search domains: stars.example

DHCP client ID:

☒ Require IPv4 addressing for this connection to complete

☒ Available to all users

Figure 1-7. *Graphically Configuring the eth0 Interface in Mint 11*

The graphical tool allows setting multiple addresses for the same interface. However, the `ifconfig` command will only show one address; use `ip` to see all of the configured addresses.

```
acauchy@aldeberan ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f6:c2:82
          inet addr:10.0.2.26  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef6:c282/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:55002 (55.0 KB)  TX bytes:22435 (22.4 KB)
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.2 KB)  TX bytes:1200 (1.2 KB)

acauchy@aldeberan ~ $ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:f6:c2:82 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.26/24 brd 10.0.2.255 scope global eth0
    inet 10.0.2.27/24 brd 10.0.2.255 scope global secondary eth0
    inet6 fe80::a00:27ff:fef6:c282/64 scope link
       valid_lft forever preferred_lft forever
```

Like Ubuntu systems, the firewall on Mint systems is disabled by default and there is no simple graphical tool to configure it.

Kali

Unlike the other Linux systems described, Kali 1.0.7 systems do not use the file `/etc/udev/rules.d/70-persistent-net.rules` to store information about installed adapters, so no modification of this file is required.

Because Kali systems are used primarily as attack systems, they are usually configured by DHCP. To configure a Kali system to use a static IP address and fixed nameserver, modify the file `/etc/network/interfaces` as was done for Ubuntu servers. Kali systems can also be configured with additional IP addresses in the same fashion as Ubuntu systems. This can be useful to an attacker trying to disguise the source of an attack.

Browser Software

A deployed system is more than just its operating system; just as important to the security of the system is the collection of software installed on it. One of the most common uses of a desktop system is to browse the Internet. All of these Linux distributions, except Kali, ship with a version of Firefox.

Active web content is often displayed using either Java or Adobe Flash, but most Linux distributions require users to install the necessary software separately.

CentOS

CentOS systems include OpenJDK rather than Sun's Java, and do not include a plug-in for Firefox.

Many versions of Java can be installed on CentOS, but it is most reasonable to choose a Java version that was in common use at the same time as the operating system. For example, CentOS 5.4 was released in October 2009, while Java 6 Update 17 was released in November 2009; both CentOS 6.0 and Java 7 were released in July 2011.

To install Java 6 Update 17 on a 32 bit CentOS 5.4 system, download the Java runtime environment jre-6u17-linux-i586-rpm.bin from the Oracle Archive[4] at http://www.oracle.com/technetwork/java/archive-139210.html, then run it, accepting the license agreement.

```
[root@canopus ~]# sh /media/sf_Downloads/jre-6u17-linux-i586-rpm.bin
```

Although Oracle Java has been installed, OpenJDK remains the default Java provider.

```
[root@canopus /]# which java
/usr/bin/java
[root@canopus /]# ls -l /usr/bin/java
lrwxrwxrwx 1 root root 22 Jul  2 11:22 /usr/bin/java -> /etc/alternatives/java
[root@canopus /]# ls -l /etc/alternatives/java
lrwxrwxrwx 1 root root 39 Jul  6 10:45 /etc/alternatives/java -> /usr/lib/jvm/jre-1.6.0-
openjdk/bin/java
```

Checking further, there are in fact two different versions of Java already installed.

```
[root@canopus /]# alternatives --config java

There are two programs that provide 'java'.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/lib/jvm/jre-1.6.0-openjdk/bin/java
   2           /usr/lib/jvm/jre-1.4.2-gcj/bin/java

Enter to keep the current selection[+], or type selection number:
```

Oracle Java stores its binary in /usr/java/latest/bin/java; add it as the third alternative and set it as the default.

```
[root@canopus ~]# alternatives --install /usr/bin/java java /usr/java/latest/bin/java 3
[root@canopus ~]# alternatives --config java

There are three programs that provide 'java'.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/lib/jvm/jre-1.6.0-openjdk/bin/java
   2           /usr/lib/jvm/jre-1.4.2-gcj/bin/java
   3           /usr/java/latest/bin/java

Enter to keep the current selection[+], or type selection number: 3
```

To install the Oracle Java Firefox plug-in, provide a link to the Oracle Java library in the Firefox plug-in directory.

```
[root@canopus ~]# ln -s /usr/java/latest/lib/i386/libnpjp2.so /usr/lib/mozilla/plugins
```

[4] Registration is required to download.

Close Firefox if it is open, start Firefox, then check that the plug-in is installed by visiting about:plugins. Verify that the plug-in functions correctly by visiting one (or all) of

- http://java.com/en/download/installed.jsp
- http://www.javatester.org/
- http://whatversion.net

The process for a 64-bit CentOS 6.0 system with Java 7 is similar. Instead of coming as a binary, Java 7 comes as an .rpm for a 64-bit system; download it then install it.

```
[root@sirius ~]# rpm -i /media/sf_Downloads/jre-7-linux-x64.rpm
```

There is only one other version of Java installed by default on this version of CentOS, so add Oracle Java as the second option and set it as the default.

```
[root@sirius ~]# alternatives --install /usr/bin/java java /usr/java/latest/bin/java 2
[root@sirius ~]# alternatives --config java

There are two programs that provide 'java'.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/lib/jvm/jre-1.6.0-openjdk.x86_64/bin/java
   2           /usr/java/latest/bin/java

Enter to keep the current selection[+], or type selection number: 2
```

The Firefox plug-in is installed in the same fashion, except that on a 64-bit system; the library and Firefox plug-in directory are in slightly different locations.

```
[root@sirius ~]# ln -s /usr/java/latest/lib/amd64/libnpjp2.so /usr/lib64/mozilla/plugins
```

Restart Firefox; verify the plug-in is installed and that it functions correctly.

To install Adobe Flash player, begin by choosing an appropriate version. For example, download Adobe Flash Player 10.3.183.5 (released August 2011) from http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html for 32 bit CentOS 5.4 (released October 2009). For a 64-bit CentOS 6.0 system (released July 2011) use Adobe Flash Player 11.0.1.152 (released October 2011 with 64-bit support).

The downloaded archive file contains versions of Adobe Flash player for a variety of operating systems, including Windows, Linux, Macintosh, and Solaris. Unpack the Linux plug-in file (not the stand-alone file), then copy the file libflashplayer.so to the Firefox plug-in directory; the other files may be discarded. On a 32-bit CentOS 5.4 system, the process is

```
[root@canopus ~]# mkdir flash
[root@canopus ~]# cd flash
[root@canopus flash]# tar -xzf /media/sf_Downloads/fp_10.3.183.5_archive/10_3r183_5/
flashplayer10_3r183_5_linux.tar.gz
[root@canopus flash]# ls -l
total 12284
-rw-rw-r-- 1 501 501 12547684 Aug  5  2011 libflashplayer.so
drwxrwxr-x 5 501 501     4096 Aug  5  2011 usr
[root@canopus flash]# chown root:root ./libflashplayer.so
[root@canopus flash]# cp ./libflashplayer.so /usr/lib/mozilla/plugins/
```

On a 64-bit CentOS 6.0 system, the process is

```
[root@sirius flash]# tar -xzf /media/sf_Downloads/fp_11.0.1.152_archive/fp_11.0.1.152_
archive/11_0r1_152_64bit/flashplayer11_0r1_152_linux.x86_64.tar.gz
[root@sirius flash]# chown root:root ./libflashplayer.so
[root@sirius flash]# cp ./libflashplayer.so /usr/lib64/mozilla/plugins
```

In either case, restart Firefox. Visit the page about:plugins to ensure the plug-in was installed and visit

- https://www.adobe.com/software/flash/about/
- http://whatversion.net

to verify it is running correctly.

OpenSuSE

The installation of Java 6 Update 30 (released December 2011) on 64-bit OpenSuSE 12.1 (released November 2011) follows the same lines as a CentOS system, but it uses a different tool name (update-alternatives rather than alternatives) and a different place to store the plug-in (/usr/lib64/browser-plugins/).

Download the Java plug-in binary, and run it.

```
arcturus:~ # sh /media/sf_Downloads/jre-6u30-linux-x64-rpm.bin
```

Set Oracle Java as the default using update-alternatives

```
arcturus:~ # update-alternatives --config java
There is only one alternative in link group java: /usr/lib64/jvm/jre-1.6.0-openjdk/bin/java
Nothing to configure.
arcturus:~ # update-alternatives --install /usr/bin/java java /usr/java/latest/bin/java 2
arcturus:~ # update-alternatives --config java
There are 2 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                       Priority   Status
------------------------------------------------------------------------------
* 0            /usr/lib64/jvm/jre-1.6.0-openjdk/bin/java   17105     auto mode
  1            /usr/java/latest/bin/java                   2         manual mode
  2            /usr/lib64/jvm/jre-1.6.0-openjdk/bin/java   17105     manual mode

Press enter to keep the current choice[*], or type selection number: 1
update-alternatives: using /usr/java/latest/bin/java to provide /usr/bin/java (java) in
manual mode.
```

Link the Java library to the Firefox plug-ins directory.

```
arcturus:~ # ln -s /usr/java/latest/lib/amd64/libnpjp2.so /usr/lib64/browser-plugins/
```

Restart Firefox, verify the plug-in installed and that it functions correctly.

On some systems, like 32-bit OpenSuSE 11.3, the existing OpenJDK plug-in must be removed before the Oracle Java Firefox plugin will function correctly.

```
vega:~ # zypper search openjdk
Loading repository data...
Reading installed packages...

S | Name                        | Summary                                           | Type
--+-----------------------------+---------------------------------------------------+--------
i | java-1_6_0-openjdk          | Java runtime environment based on OpenJDK 6 and -> | package
  | java-1_6_0-openjdk-devel    | Java SDK based on OpenJDK 6 and IcedTea 6          | package
i | java-1_6_0-openjdk-plugin | Java web browser plugin based on OpenJDK 6 and I-> | package

vega:~ # zypper rm java-1_6_0-openjdk-plugin
```

The rest of the installation for 32-bit OpenSuSE 11.3 is standard. For example, to install Java 6 Update 21, download then run the binary

```
vega:~ # sh /media/sf_downloads/jre-6u21-linux-i586-rpm.bin
```

Update the default java version and link the plug-in.

```
vega:~ # update-alternatives --install /usr/bin/java java /usr/java/latest/bin/java 2
vega:~ # update-alternatives --config java

There are two alternatives that provide `java´.

  Selection    Alternative
-----------------------------------------------
*+        1    /usr/lib/jvm/jre-1.6.0-openjdk/bin/java
          2    /usr/java/latest/bin/java

Press enter to keep the default[*], or type selection number: 2
Using '/usr/java/latest/bin/java' to provide 'java'.
vega:~ # ln -s /usr/java/latest/lib/i386/libnpjp2.so /usr/lib/browser-plugins/
```

Restart Firefox, verify the plug-in installed and that it functions correctly.

To install Flash player, download an appropriate version- say Adobe Flash 10.1.85.3 (released September 2010) for OpenSuSE 11.3 (released July 2010), or Adobe Flash 11.1.102.55 (released November 2011) for 64 bit OpenSuSE 12.1 (released November 2011).

On 32 bit OpenSuSE 11.3 uncompress the appropriate archive and copy `libflashplayer.so` to the Firefox plugin directory; the other files may be discarded

```
vega:~/flash # tar -xf /media/sf_downloads/fp_10.1.85.3_and_9.0.283_archive/Flash\ Player\
10.1.85.3/10_1r85_3/flashplayer10_1r85_3_linux.tar.gz
vega:~/flash # chown root:root ./libflashplayer.so
vega:~/flash # cp ./libflashplayer.so /usr/lib/browser-plugins/
```

The approach on 64 bit OpenSuSE is the same, except for the different plug-in destination.

```
arcturus:~/flash # tar -xf /media/sf_Downloads/fp_11.1.102.55_archive/ 11_1r102_55_64bit/
flashplayer11_1r102_55_linux.x86_64.tar.gz
arcturus:~/flash # chown root:root ./libflashplayer.so
arcturus:~/flash # cp ./libflashplayer.so /usr/lib64/browser-plugins/
```

Restart Firefox, verify the plug-in installed and that it functions correctly.

Ubuntu

Installation of Java on Ubuntu is different, as it is not an .rpm-based distribution, but rather a .deb-based one, and Oracle does not distribute Java in this format.

Consider Java 6 Update 26 (released June 2011) on Ubuntu 11.04 (released April 2011). Download jre-6u26-linux-i586.bin from the Java Archive. When run, this will create the directory jre1.6.0_26/ containing all of the files required for Java to run. This directory be stored anywhere in the file system, but a natural place is under /opt, which is the standard location for add-on software.

```
enoether@procyon:~$ sudo sh /media/sf_downloads/jre-6u26-linux-i586.bin
enoether@procyon:~$ sudo mv ./jre1.6.0_26/ /opt
```

Create a link to the java binary and a link for the plug-in

```
enoether@procyon:~$ sudo ln -s /opt/jre1.6.0_26/bin/java /usr/bin/java
enoether@procyon:~$ sudo ln -s /opt/jre1.6.0_26/lib/i386/libnpjp2.so /usr/lib/mozilla/
plugins/
```

Restart Firefox, then verify the plug-in is installed and functioning correctly.

To install Adobe Flash Player for Ubuntu 11.04, download an appropriate version, for example, 10.3.181.14 (released May 2011). Uncompress it, identify the plug-in, give it the proper ownership, and copy it to the Firefox plug-in directory.

```
enoether@procyon:~$ mkdir flash
enoether@procyon:~$ cd flash/
enoether@procyon:~/flash$ sudo tar -xf /media/sf_downloads/fp_10.3.181.14_
archive/10_3r181_14/flashplayer10_3r181_14_linux.tar.gz
enoether@procyon:~/flash$ ls -l
total 12252
-rw-r--r-- 1 1003 users 12537796 2011-05-05 19:27 libflashplayer.so
-rw-r--r-- 1 1003 users     2009 2011-05-10 18:38 README
drwxr-xr-x 5 1003 users     4096 2011-05-05 19:27 usr
enoether@procyon:~/flash$ sudo chown root:root ./libflashplayer.so
enoether@procyon:~/flash$ sudo cp ./libflashplayer.so /usr/lib/mozilla/plugins/
```

Restart Firefox, then verify the plug-in is installed and functioning correctly. When complete, the remaining files can be deleted.

Mint

Some versions of Mint, like Mint 11 and Mint 12 install Oracle Java by default with a configured Firefox plug-in. Mint 13 uses open JDK and so Oracle Java must be manually configured.

```
pdirichlet@acrux ~ $ sudo tar -xzvf /media/sf_downloads/jre-7u5-linux-i586.gz
pdirichlet@acrux ~ $ sudo mv ./jre1.7.0_05/ /opt
pdirichlet@acrux ~ $ sudo update-alternatives --install /usr/bin/java java /opt/jre1.7.0_05/
bin/java 2
pdirichlet@acrux ~ $ sudo update-alternatives --config java
There are 2 choices for the alternative java (providing /usr/bin/java).
```

```
  Selection    Path                                           Priority   Status
------------------------------------------------------------------------------------
* 0            /usr/lib/jvm/java-6-openjdk-i386/jre/bin/java   1061      auto mode
  1            /opt/jre1.7.0_05/bin/java                       2         manual mode
  2            /usr/lib/jvm/java-6-openjdk-i386/jre/bin/java   1061      manual mode

Press enter to keep the current choice[*], or type selection number: 1
update-alternatives: using /opt/jre1.7.0_05/bin/java to provide /usr/bin/java (java) in
manual mode.
pdirichlet@acrux ~ $ sudo ln -s /opt/jre1.7.0_05/lib/i386/libnpjp2.so /usr/lib/mozilla/
plugins/
```

Mint 11, 12, and 13 all come with Adobe Flash installed by default.

Windows Systems

Windows systems such as Windows 7 and Windows 8 are commonly deployed desktop solutions, while Windows servers such as Window Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 form the backbone of many large organizations.

Virtualization Support

Both VirtualBox and VMWare Workstation provide extensive support for Windows operating systems. VMWare Workstation installs Windows systems using Easy Install, and automatically includes VMWare Tools.

The installation of VirtualBox Guest Additions must be performed manually. Once the guest has booted, navigate the guest's VirtualBox main menu through Devices ➤ Insert Guest Additions CD Image. This will load a virtual CD with the needed software in the guest. If the program does not run automatically, start the process by running `VBoxWindowsAdditions.exe` from the disc. The installation process requires a guest system reboot when complete.

Windows SIDs

Each Windows system has its own Machine SID. An SID is a security identifier, and Microsoft systems have them for users, groups, computers, and other security principals. The command line tool `wmic` can be used to find the SID for local users on a Windows system. Here is the result run on a Windows 2012 R2 server.

```
C:\Users\Administrator>wmic useraccount get name, sid
Name           SID
Administrator  S-1-5-21-2662891359-98615007-2145025997-500
Elie Cartan    S-1-5-21-2662891359-98615007-2145025997-1001
Guest          S-1-5-21-2662891359-98615007-2145025997-501
```

The PSGetSid.exe tool from the Sysinternals PSTools suite (downloadable from Microsoft) can print the SID for the computer or an account on the computer. Running it on the same server, we obtain

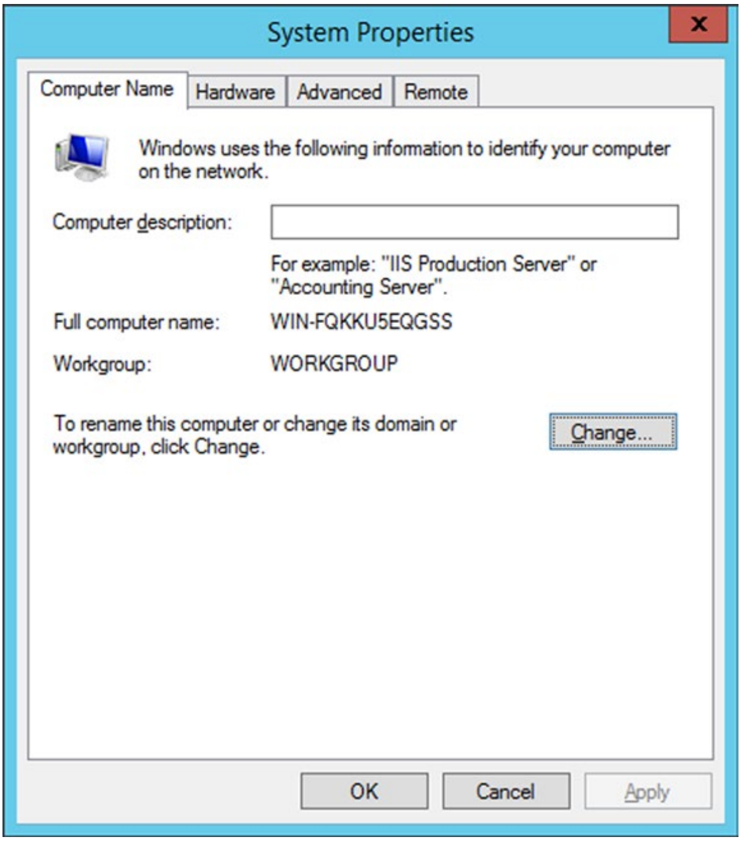
```
C:\Users\Administrator>Desktop\PSTools\PsGetsid.exe

PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright (C) 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\WIN-FQKKU5EQGSS:
S-1-5-21-2662891359-98615007-2145025997
```

Comparing these results, it is clear that the SID of the local user is just the SID of the system followed by a relative ID; administrator accounts have the relative ID of 500 (which is why renaming administrator accounts provides less security than might be imagined), the guest account has relative ID 501, and subsequent accounts start at 1000 and go up from there.

If a Windows system is duplicated, either by cloning a VirtualBox guest, or copying a VMWare Workstation guest, the system's Machine SID remains unchanged. The machine SID can be changed by running the Sysprep program located on the system at c:\Windows\System32\Sysprep\Sysprep.exe with the generalize option enabled.

Networking and Basic Configuration

To set the host name on a Windows system, start the Control Panel, and navigate through System and Security ➤ System. Use the Change settings link for the "Computer name, domain, and workgroup settings" section to obtain the System Properties dialog. See Figure 1-8.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-FQKKU5EQGSS

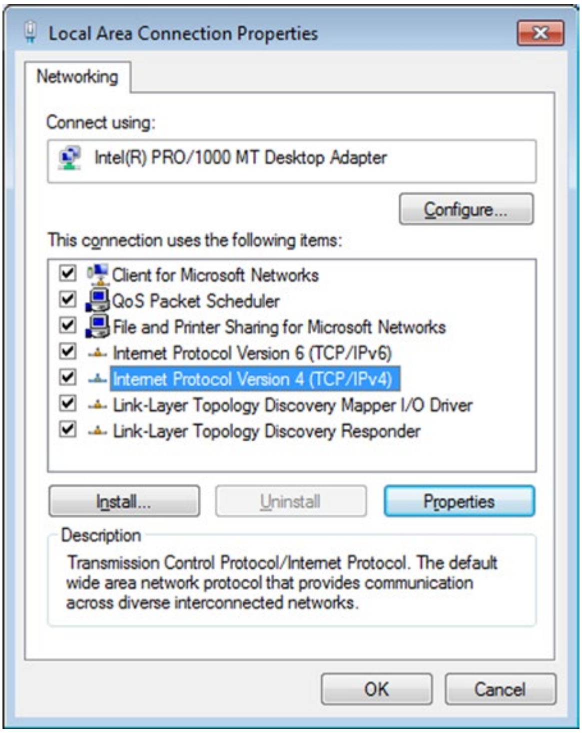
Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

Figure 1-8. *System Properties for Windows 2012 R2*

The Change button leads to a dialog box that allows the computer name to be changed including the primary DNS suffix of the system. Changing the system name necessitates a reboot.

To configure networking on a Windows system, start the Control Panel, and navigate through Network and Internet ➤ Network and Sharing center ➤ Change adapter settings. Right-click on an adapter to obtain a dialog box to change the settings. See Figure 1-9.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Figure 1-9. *Local Area Connection Properties on Windows 7*

To change the IPv4 Settings, highlight Internet Protocol Version 4, then press the Properties button. Manually specify the IP address and DNS sever for the adapter; additional IP addresses can be specified from another dialog found by pressing the Advanced button.

The command line tool `ipconfig` shows the status of the network adapters; it can be used to validate the settings made in the graphical interface.

```
C:\Users\Hermann Weyl>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::584b:daf6:2db2:983f%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.0.2.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1
```

```
Tunnel adapter isatap.{0F668234-DA71-4AFF-B938-BDAD62C42F90}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6abd:1879:3f65:f5ff:fd91
   Link-local IPv6 Address . . . . . : fe80::1879:3f65:f5ff:fd91%13
   Default Gateway . . . . . . . . . : ::

Tunnel adapter Reusable ISATAP Interface {C9EA8D2D-BFC2-4D80-A556-47CF773E338B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

To add a new IP address to an adapter from the command line, use the netsh command. For example, to add the address 10.0.2.113 to this interface, run

```
C:\Windows\system32>netsh interface ipv4 add address "Local Area Connection" 10.0.2.113
255.255.255.0
```

from a command prompt with Administrator privileges. The corresponding command

```
C:\Windows\system32>netsh interface ipv4 delete address "Local Area Connection" 10.0.2.113
255.255.255.0
```

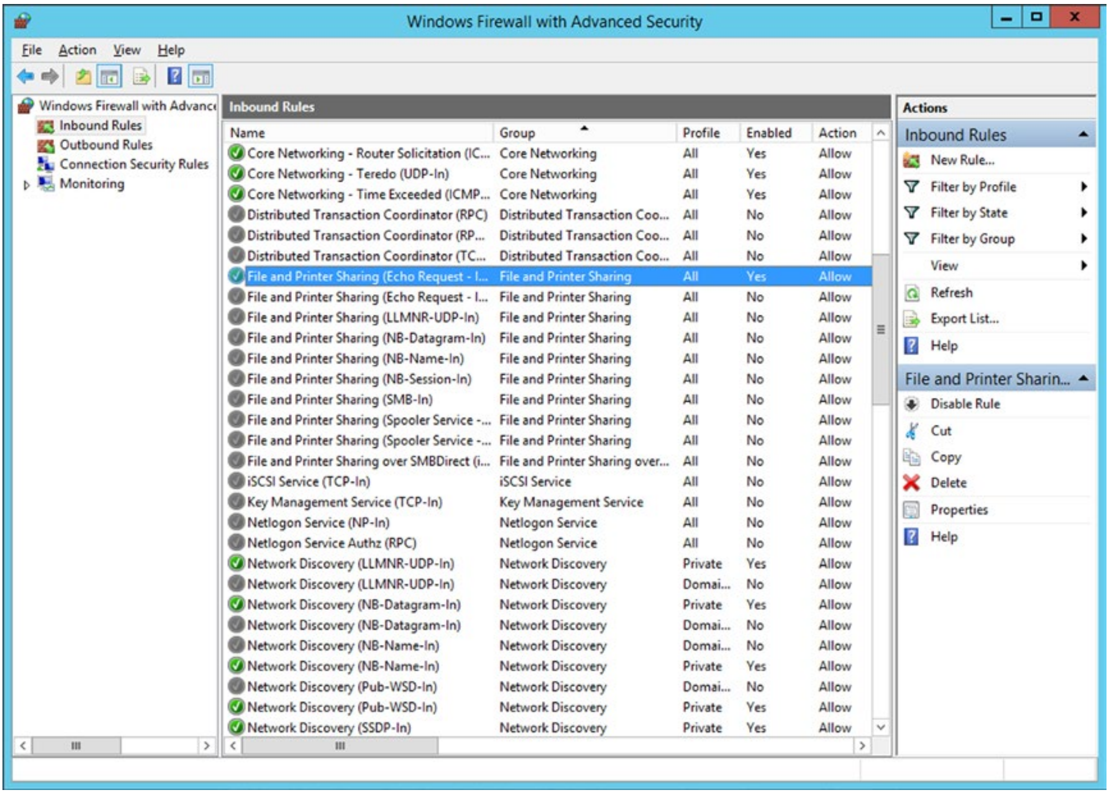
deletes that address.

When the properties of a network adapter are changed, the location of that network needs to be set as either “Home network,” “Work network,” or “Public Network.” When building test networks, usually “Work Network” is the most appropriate choice.

To keep systems as they were deployed after installation, the automatic installation of security patches by Windows must be disabled. To do so, navigate the Control Panel through Systems and Security ➤ Windows Update, and make the necessary changes.

The antivirus and antispyware tool Windows Defender is installed by default on Windows 8 systems. To keep the system as it was deployed after installation, disable the automatic update of this tool, or more simply disable it altogether.

The Windows Firewall is controlled through the Control Panel; navigate System and Security ➤ Windows Firewall. By default, Windows Firewall blocks ping requests and ping replies; this can make debugging networking problems more challenging. To permit responses to ping traffic, from the Windows Firewall dialog box in the Control Panel select Advanced Settings. From the list of Inbound Rules, select “File and Printer Sharing (Echo Request - ICMPv4-In),” right-click, and enable the rule from the Action Pane. See Figure 1-10.



Name	Group	Profile	Enabled	Action
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	No	Allow
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Allow
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	No	Allow
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	No	Allow
File and Printer Sharing over SMBDirect (i...	File and Printer Sharing over...	All	No	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	No	Allow
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow
Netlogon Service Authz (RPC)	Netlogon Service	All	No	Allow
Network Discovery (LLMNR-UDP-In)	Network Discovery	Private	Yes	Allow
Network Discovery (LLMNR-UDP-In)	Network Discovery	Domai...	No	Allow
Network Discovery (NB-Datagram-In)	Network Discovery	Private	Yes	Allow
Network Discovery (NB-Datagram-In)	Network Discovery	Domai...	No	Allow
Network Discovery (NB-Name-In)	Network Discovery	Domai...	No	Allow
Network Discovery (NB-Name-In)	Network Discovery	Private	Yes	Allow
Network Discovery (Pub-WSD-In)	Network Discovery	Domai...	No	Allow
Network Discovery (Pub-WSD-In)	Network Discovery	Private	Yes	Allow
Network Discovery (SSDP-In)	Network Discovery	Private	Yes	Allow

Figure 1-10. *Configuring Windows 2012 R2 to Reply to Ping Requests*

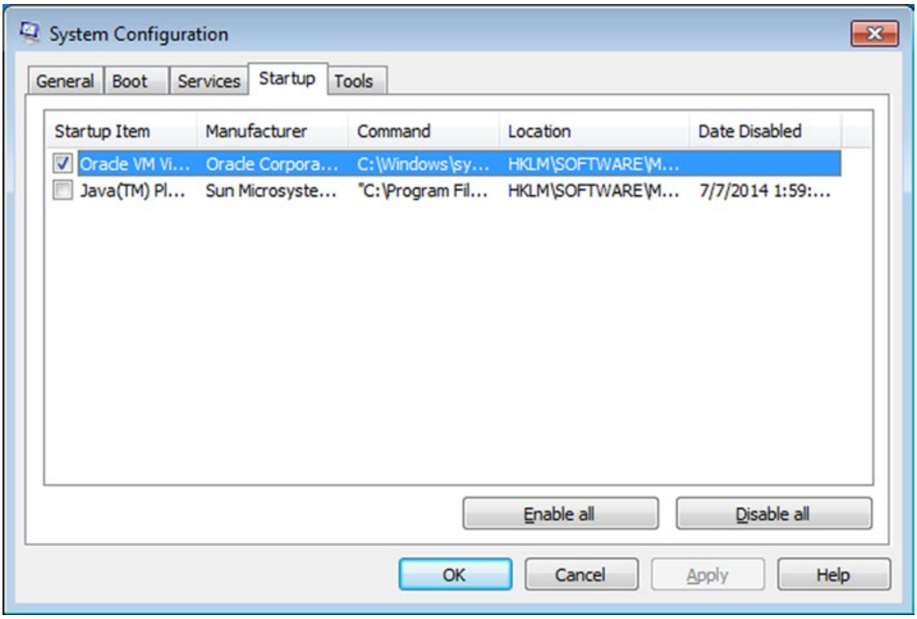
Windows systems ship with Internet Explorer as their default browser. Firefox can be installed by downloading and running the proper installer. To keep Firefox in its installed version, automatic updates must be disabled. Navigate the main menu through Tools ➤ Options ➤ Advanced ➤ Update, and disable the settings found there; they vary slightly with different versions of Firefox.

Recent versions of Firefox (*e.g.,* 17.0) ignore these settings, and simply determining the version of Firefox by navigating Help ➤ About Firefox will cause Firefox to download the latest version; each time Firefox then starts it will attempt to install this update. To prevent this behavior, make additional changes on the page `about:config` by ensuring each of the following values is set to false:

- app.update.auto
- app.update.enabled
- app.update.slient

The installation of Java is standard. Once installed, Java functions in both Firefox and Internet Explorer. Note that older versions of Internet Explorer and Firefox are 32 bit by default, and so a 32 bit version of Java is necessary for the plug-in to function correctly.

Both Java 6 and Java 7 will automatically attempt to update themselves. This behavior is controlled by `jusched.exe`, which launches when the system boots. To prevent the automatic updates, it is simplest to prevent `jusched.exe` from starting by running `msconfig.exe` to disable its automatic start. See Figure 1-11.



Startup Item	Manufacturer	Command	Location	Date Disabled
☑ Oracle VM Vi...	Oracle Corpora...	C:\Windows\sy...	HKLM\SOFTWARE\M...	
☐ Java(TM) Pl...	Sun Microsyste...	"C:\Program Fil...	HKLM\SOFTWARE\M...	7/7/2014 1:59:...

Figure 1-11. *Disabling the Java Update Scheduler with msconfig on Windows 7*

The installation of Adobe Flash on Windows is standard. The archives contain versions for Internet Explorer, which usually end `winax.exe` and versions for Firefox, which usually end `win.exe`; the stand-alone package typically ends `win_sa.exe`. The readme file in each archive provides guidance. Attempts to install some older versions of Flash may be prevented with an error stating that the version is out of date. To bypass this, run the installer from the command line with the -force option

```
c:\Users\Felix Klein\Desktop>flashplayer11_1r102_55_winax_32bit.exe -force
```

Windows 8 ships with Adobe Flash Player 11.3.372 already installed for Internet Explorer.

Adobe Flash will also automatically search online for updates. To disable this behavior, create the file `C:\Windows\System32\Macromed\Flash\mms.cfg` with the content

```
AutoUpdateDisable=1
SilentAutoUpdateDisable=0
```

EXERCISES

1. Build the desktop systems described in this chapter:
    - CentOS 5.4, Java 6 Update 17, Adobe Flash 10.3.183.5
    - CentOS 6.0, Java 7, Adobe Flash 11.0.1.152
    - Open SuSE 11.3, Java 6 Update 21, Adobe Flash 10.1.85.3
    - OpenSuSE 12.1, Java 6 Update 30, Adobe Flash 11.1.102.55

- Ubuntu 9.04, Java 6 Update 14, Adobe Flash 9.0.283
- Ubuntu 11.04, Java 6 Update 26, Flash Player 10.3.181.14
- Ubuntu 12.04, Java 7 Update 5, Flash Player 11.2.202.233
- Mint 11, Java 6 Update 24, Adobe Flash 10.3.180
- Mint 12, Java 6 Update 26, Adobe Flash 11.0.1
- Mint 13, Java 7 Update 5, Adobe Flash 11.0.1
- Windows 7 SP0, Firefox 3.6, Java 6 Update 17, Adobe Flash 10.0.1.85.3
- Windows 7 SP1, Firefox 5.0, Java 6 Update 26, Adobe Flash 10.2.153.1
- Windows 8, Firefox 17, Java 7 Update 10. Windows ships with Adobe Plash Player 11.3.372 installed for Internet Explorer. Install Adobe Flash Player 11.4.402.287 for Firefox.

2. Use the graphical tools on CentOS to configure a network adapter.
3. Use YaST on OpenSuSE to configure a network adapter.
4. Use the `ifconfig` and `route` commands to manually and temporarily configure a Linux network adapter with a static address, netmask, and gateway.
5. Use the `netsh` command to change the DNS server for a network adapter on Windows.
6. Use the command `wmic qfe list` to list all of the patches on a Windows system. Use the command `wusa /uninstall /kb:<kbnumber>` to uninstall a particular patch.

Notes and References

Introduction

Windows operating systems must be purchased from Microsoft. Limited time evaluation copies are available from Microsoft through the TechNet Evaluation Center (http://technet.microsoft.com/evalcenter). Students and educators can participate in the Microsoft DreamSpark program (https://www.dreamspark.com/What-Is-Dreamspark.aspx), which gives access to current as well as recent older versions of their operating systems.

Old versions of CentOS can be found at http://vault.centos.org/, but if you want the install images, this will redirect you to the mirror http://mirror.symnds.com/distributions/CentOS-vault/. Links to mirrors containing old versions of OpenSuSE can be found at http://en.opensuse.org/openSUSE:Mirrors. Old versions of Ubuntu can be found at http://old-releases.ubuntu.com/releases/. The Mint project provides links to current and older versions of Mint at http://www.linuxmint.com/oldreleases.php.

The easiest way to build a consistent test system is to be aware of the release dates of the various software components that are installed. See Table 1-1.

Table 1-1. *List of Operating Systems, by Release Date*

Operating System	Version	Release	Operating System	Version	Release
Windows Server	2008	2/2008	CentOS	5.6	4/2011
Ubuntu	8.04	4/2008	Ubuntu	11.04	4/2011
CentOS	5.2	6/2008	Mint	11	5/2011
Mint	5	6/2008	CentOS	6.0	7/2011
OpenSuSE	11.0	6/2008	CentOS	5.7	9/2011
Ubuntu	8.10	10/2008	Ubuntu	11.10	10/2011
Mint	6	12/2008	Mint	12	11/2011
OpenSuSE	11.1	12/2008	OpenSuSE	12.1	11/2011
CentOS	5.3	3/2009	CentOS	6.1	12/2011
Ubuntu	9.04	4/2009	CentOS	6.2	12/2011
Mint	7	5/2009	CentOS	5.8	3/2012
Windows Server	2008 SP2	5/2009	Ubuntu	12.04	4/2012
Windows Server	2008 R2	7/2009	Mint	13	5/2012
CentOS	5.4	10/2009	CentOS	6.3	7/2012
Ubuntu	9.10	10/2009	OpenSuSE	12.2	9/2012
Windows	7	10/2009	Windows Server	2012	10/2012
Mint	8	11/2009	Windows	8	10/2012
OpenSuSE	11.2	11/2009	CentOS	5.9	1/2013
Ubuntu	10.04	4/2010	CentOS	6.4	3/2013
CentOS	5.5	5/2010	OpenSuSE	12.3	3/2013
Mint	9	5/2010	Ubuntu	13.04	4/2013
OpenSuSE	11.3	7/2010	CentOS	5.10	10/2013
Ubuntu	10.10	10/2010	Windows	8.1	10/2013
Mint	10	11/2010	Ubuntu	13.10	10/2013
Windows	7 SP 1	2/2011	Windows Server	2012 R2	11/2013
Windows Server	2008 R2 SP1	2/2011	OpenSuSE	13.1	11/2013
OpenSuSE	11.4	3/2011	CentOS	6.5	12/2013

Sources:

- Windows release dates (including Service Packs) `http://windows.microsoft.com/en-us/windows/lifecycle`
- Windows Server 2008 Release dates (including service packs) `http://support.microsoft.com/lifecycle/search/default.aspx?sort=PN&alpha=Windows+Server+2008&Filter=FilterNO`
- Windows Server 2012 Release dates `http://support.microsoft.com/lifecycle/search/default.aspx?sort=PN&alpha=Windows+Server+2012&Filter=FilterNO`

- Ubuntu Release dates https://wiki.ubuntu.com/Releases
- Mint Release dates http://distrowatch.com/table.php?distribution=mint
- OpenSuSE Release dates http://distrowatch.com/table.php?distribution=suse
- CentOS Release dates http://en.wikipedia.org/wiki/CentOS

Old versions of Firefox can be downloaded from https://ftp.mozilla.org/pub/mozilla.org/firefox/releases/. See Table 1-2.

Table 1-2. *Firefox Versions, by Release Date*

Firefox Version	Release Date	Firefox Version	Release Date	Firefox Version	Release Date
3.0	6/2008	10.0	1/2012	19.0	2/2013
3.5	6/2009	11.0	3/2012	20.0	4/2013
3.6	1/2010	12.0	4/2012	21.0	5/2013
4.0	3/2011	13.0	6/2012	22.0	6/2013
5.0	6/2011	14.0	6/2012	23.0	8/2013
6.0	8/2011	15.0	8/2012	24.0	9/2013
7.0	9/2011	16.0	10/2012	25.0	10/2013
8.0	11/2011	17.0	11/2012	26.0	12/2013
9.0	12/2011	18.0	1/2013		

Source: https://wiki.mozilla.org/Releases/Old

Old versions of Java can be obtained from the Oracle Java Archive at http://www.oracle.com/technetwork/java/archive-139210.html. Users must sign on with Oracle before being permitted to download software. See Tables 1-3 and 1-4.

Table 1-3. *Java 6 Versions, by Release Date*

Java 6 Update	Release Date	Java 6 Update	Release Date	Java 6 Update	Release Date
U1	5/2007	U17	11/2009	U31	2/2012
U2	7/2007	U18	1/2010	U32	4/2012
U3	10/2007	U19	3/2010	U33	6/2012
U4	1/2008	U20	4/2010	U34	8/2012
U5	3/2008	U21	7/2010	U35	8/2012
U6	4/2008	U22	10/2010	U37	10/2012
U10	10/2008	U23	12/2010	U38	12/2012
U11	12/2008	U24	2/2011	U39	2/2013
U12	12/2008	U25	3/2011	U41	2/2012
U13	3/2009	U26	6/2011	U43	3/2013
U14	5/2009	U27	8/2011	U45	4/2013
U15	8/2009	U29	10/2011	U51	6/2013
U16	8/2009	U30	12/2011		

***Table 1-4.** Java 7 Versions, by Release Date*

Java 7 Update	Release Date	Java 7 Update	Release Date	Java 7 Update	Release Date
U0	7/2011	U6	8/2012	U15	2/2013
U1	10/2011	U7	8/2012	U17	3/2013
U2	12/2011	U9	10/2012	U21	4/2013
U3	2/2012	U10	12/2012	U25	6/2013
U4	4/2012	U11	1/2013	U40	9/2013
U5	6/2012	U13	2/2013	U45	10/2013

Sources: `https://www.java.com/en/download/faq/release_dates.xml` and `http://en.wikipedia.org/wiki/Java_version_history`

Both release dates and download links for old versions of Adobe Flash Player are available at `http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html`. See Table 1-5.

***Table 1-5.** Adobe Flash Versions, by Release Date*

Adobe Flash Version	Release Date	Adobe Flash Version	Release Date	Adobe Flash Version	Release Date
10.1.85.3	9/2010	11.3.300.265	7/2012	11.6.602.171	2/2013
10.1.102.64	11/2010	11.3.300.268	7/2012	11.2.202.275	3/2013
10.2.152.26	2/2011	11.4.402.265	8/2012	10.3.183.68	3/2013
10.2.152.32	2/2011	11.2.202.238	8/2012	11.6.602.180	3/2013
10.2.153.1	3/2011	11.3.300.271	8/2012	11.7.700.169	4/2013
10.2.159.1	4/2011	10.3.183.23	8/2012	11.2.202.280	4/2013
10.3.181.14	5/2011	10.3.183.25	9/2012	10.3.183.75	4/2013
10.3.181.16	5/2011	11.4.402.278	9/2012	11.2.202.285	5/2013
10.3.181.22	6/2011	11.3.300.273	10/2012	10.3.183.86	5/2013
10.3.181.26	6/2011	11.2.202.243	10/2012	11.7.700.202	5/2013
10.3.183.5	8/2011	10.3.183.29	10/2012	11.2.202.291	6/2013
10.3.183.7	8/2011	11.4.402.287	10/2012	10.3.183.90	6/2013
10.3.183.10	9/2011	11.5.502.110	11/2012	11.7.700.224	6/2013
11.0.1.152	10/2011	11.2.202.251	11/2012	11.2.202.297	7/2013
11.1.102.55	11/2011	10.3.183.43	11/2012	11.7.700.232	7/2013
10.3.183.11	11/2011	11.2.202.258	12/2012	11.8.800.94	7/2013
11.1.102.55	11/2011	10.3.183.48	12/2012	11.2.202.310	9/2013
10.3.183.15	2/2012	11.5.502.136	12/2012	11.7.700.242	9/2013
11.1.102.62	2/2012	11.2.202.261	1/2013	11.8.800.168	9/2013
11.2.202.223	3/2012	10.3.185.20	1/2013	11.8.800.174	9/2013

(*continued*)

Table 1-5. *(continued)*

Adobe Flash Version	Release Date	Adobe Flash Version	Release Date	Adobe Flash Version	Release Date
10.3.183.16	3/2012	11.5.502.146	1/2013	11.8.800.175	9/2013
11.1.102.63	3/2012	11.6.602.167	2/2013	11.9.900.117	10/2013
10.3.183.18	3/2012	11.2.202.262	2/2013	11.2.202.237	11/2013
11.2.202.233	4/2012	10.3.183.51	2/2013	11.7.700.252	11/2013
11.2.202.235	5/2012	11.2.202.270	2/2013	11.9.900.152	11/2013
11.3.300.257	6/2012	10.3.183.63	2/2013	11.2.202.332	12/2013
10.3.183.20	6/2012	11.2.202.273	2/2013	11.7.700.257	12/2013
11.3.300.262	6/2012	10.3.183.67	2/2013	11.9.900.170	12/2013

Adobe Flash is not available for Linux systems as a stand-alone product after version 11.2; see Adobe's 2012 announcement at http://blogs.adobe.com/flashplayer/2012/02/adobe-and-google-partnering-for-flash-player-on-linux.html

Virtualization Tools

VMWare Workstation can be purchased directly from VMWare at http://www.vmware.com/products/workstation/. Their free product, VMWare Player, is suitable for nearly all of this text; its primary limitations are that it does not provide the ability to take snapshots, and its support for virtual networks (which will be used extensively in Chapter 14, Firewalls) is limited. It can be downloaded from https://my.vmware.com/web/vmware/downloads.

VirtualBox can be downloaded from https://www.virtualbox.org/. VirtualBox has an excellent online manual available at https://www.virtualbox.org/manual/.

Sometimes when installing VirtualBox Guest Additions on a Linux system the CD will not mount automatically. Mount the device /dev/sr0 to a convenient place (for example, media/vb) manually to proceed. On other systems, the symbols and the headers for the kernel are in separate packages; this is the case for example with OpenSuSE 11.0, which (apparently) needs both kernel-syms and linux-kernel-headers to install VirtualBox Guest Additions.

Kali can use open source tools (open-vm-toolbox) instead of native VMWare tools; see http://docs.kali.org/general-use/install-vmware-tools-kali-guest.

In my experience, the drag-and-drop function provided by VirtualBox Guest Additions does not always function as intended. I have had difficulty with this feature in OpenSuSE systems, some Ubuntu systems, and some Mint systems. This is rarely a problem though, as the shared folder feature works well.

Building Linux Systems

Documentation for CentOS can be found on their wiki at http://wiki.centos.org/Documentation, while OpenSuSE keeps their documentation at http://doc.opensuse.org/. That set of documentation describes using NetworkManager to configure the network on OpenSuSE; I have found that the documentation they provide for their commercial product at https://www.suse.com/documentation/sles11/book_sle_admin/data/sec_basicnet_manconf.html is more helpful if NetworkManager is not going to be used. Documentation for Ubuntu can be found on their official site at https://help.ubuntu.com/ and on their wiki at https://help.ubuntu.com/community. In general, Mint is configured in the same fashion as Ubuntu; they do have installation and usage guides available for some versions of Mint at http://www.linuxmint.com/documentation.php.

I have occasionally had trouble validating older Linux installations of Flash Player by visiting Adobe's main site at https://www.adobe.com/software/flash/about/. You may wish to validate your Flash installation by visiting web sites that actually use Flash, such as https://disneyworld.disney.go.com/new-fantasyland/ or http://www.intel.com/museumofme/en_US/r/index.htm.

Documentation for iptables is available directly from http://www.netfilter.org/documentation/.

Building Windows Systems

The Sysinternals PsTools suite can be downloaded from Microsoft at http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx.

The question of what happens if there are two systems on a network with the same machine SID is an interesting one. There was a SysInternals tool to update a system Machine SID, but that has long since been discontinued. The tool's author, Mark Russinovich, back in 2009 wrote on his blog: "I became convinced that machine SID duplication – having multiple computers with the same machine SID – doesn't pose any problem, security or otherwise. I took my conclusion to the Windows security and deployment teams and no one could come up with a scenario where two systems with the same machine SID, whether in a Workgroup or a Domain, would cause an issue."[5]

Years of teaching a university course on these topics have convinced me that this is *almost* true. In particular, my students have noticed that on a Windows domain, if both a Windows 2008 domain controller and a (different) Windows 2008 file server have the same SID, then some difficult-to-track-down errors occur, errors that are not present if the two systems have different SIDs.

More information about the sysprep process can be found from Microsoft TechNet at http://technet.microsoft.com/en-us/library/cc721940(v=ws.10).aspx.

Microsoft has excellent documentation for the netsh command on TechNet at http://technet.microsoft.com/en-us/library/cc731521(v=ws.10).aspx.

The Control Panel on Windows systems contains an entry for Java. On systems with Java 6, one of the tabs is meant to configure Java's update behavior. It gives the option to disable automatic updates or to reschedule how often Java checks for updates. My experience however, is that this simply does not work. Uncheck the box labeled "Check for Updates Automatically" and restart the system. Go back to the Java entry for the Control Panel, and you will see the box has been rechecked for you, and that Java will automatically check for updates.

[5] Mark Russinovich, "The Machine SID Duplication Myth," Mark Russinovich's Blog: Microsoft TechNet., November 3, 2009. http://blogs.technet.com/b/markrussinovich/archive/2009/11/03/3291024.aspx.