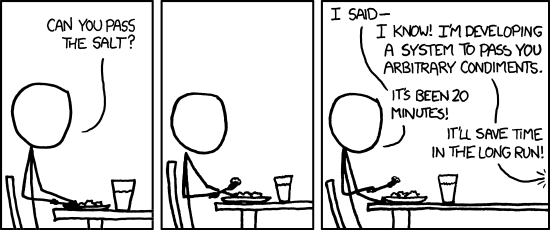
# Welcome!

Welcome to Linux for Networking Professionals! In this book we’ll explore how to support and troubleshoot your network using Linux and Linux based tools, as well as how to securely deploy common networking infrastructure on Linux Platforms.

Why would you want to use Linux for these purposes? To begin with, the architecture, history and culture of Linux “steers” administrators towards scripting and automating processes. While carrying this to extremes can get people into funny situations, scripting routine tasks can be a real time-saver:



(<https://xkcd.com/2138/>)

In fact, scripting non-routine tasks, for instance something that needs doing once per year, can be a life-saver as well – it means that administrators don’t need to re-learn how to do that thing they did 12 months ago.

Scripting routine tasks is even a bigger win. Over many years, Windows Administrators have learned that doing one task hundreds of times in a GUI (Graphical User Interface) is a guarantee to mis-click at least a few times. Scripting tasks like that, on the other hand is a guarantee of consistent results. Not only that, but over a network, where routinely administrators perform operations for hundreds or thousands of stations, scripting is often the only way to accomplish tasks at larger scales.

Another reason network administrators prefer Linux platforms is that Linux (and before that Unix) has been around since there were networks to be a part of. On the server side, Linux (or Unix) services are what defined those services, where the matching Windows services are copies that have over time mostly grown to feature parity.

On the workstation side, if you need a tool to administer or diagnose something on your network, it’s probably already installed. If the tool that you seek isn’t installed, it’s a one line command to get it installed and running, along with any other tools, libraries or other dependencies required. And adding that tool did not require a license fee - both Linux and any tools installed on Linux are almost without exception free and open source.

Lastly, on both the server and desktop side, Linux is free. License costs are not part of the Linux model at all, so standing up another server, especially if it’s virtualized, does not turn into a budget discussion. You may pay a subscription fee for support, but you don’t pay for the operating system itself.

## Why is Linux Important?

Over the years, one of the jokes in the information technology community is that next year was always going to be “the year of the Linux Desktop” – where we’d all stop paying license fees for desktops and business applications, and everything would be free and open source.

Instead what has happened is that Linux has been making steady inroads into the server and infrastructure side of many environments.

Linux has become a mainstay in most datacenters, even if those organizations think they are a “Windows only” environment. Many infrastructure components run Linux under the covers, with a nice web front-end to turn it into a vendor solution. If you have a SAN (Storage Area Network), that likely runs Linux, as do your Load Balancers, Access Points and Wireless Controllers. Many Routers and Switches run Linux, as do pretty much all of the new “Software Defined Networking” solutions.

Almost without fail Information Security products are based on Linux. Traditional Firewalls and “Next Generation” Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), SIEM (Security Information and Event Management) systems, Logging servers – Linux, Linux, Linux.

Why is Linux so pervasive? It’s a mature operating system, with an integrated patching and updating system. It’s a simple OS to configure, and since it’s almost entirely file-based, it’s fairly easy to keep it to a known baseline if you are a vendor who’s basing their product on Linux. You can build just about anything on top of Linux, given the right mix of (free and open source) packages, some scripting and maybe some custom coding. If you pick the right distribution, the OS itself is free, which is a great motivator for a vendor trying to maximize profit or a customer trying to reduce their costs.

If the new “infrastructure as code” movement is what draws you, then you’ll find that pretty much every coding language is represented in Linux and is seeing active development – from new languages like Go and Rust, all the way back to Fortran and Cobol. Even PowerShell and .Net, which grew out of Windows, are completely supported on Linux. Every orchestration engine (for instance, Ansible, Puppet or Terraform) started on and supported Linux first.

On the Cloud side of today’s IT infrastructure, the fact that Linux is free has seen the Cloud Service Providers “push” their clients towards that end of the spectrum almost from the start. If you’ve subscribed to any cloud service that is described as “Serverless” or “as a Service”, likely behind the scenes that solution is almost all Linux.

Finally, as we’ve seen the server and infrastructure side of IT move towards Linux, today’s cell phones are steadily becoming the largest “desktop” platform in today’s computing reality. In today’s world, cell phones are generally either iPhones or Android based, both of which are (you guessed it) Linux based! So the “Year of the Linux Desktop” has snuck up on us by changing the definition of “desktop”.

All of this combines to make Linux very important to today’s Networking or IT professional. This book focuses on using Linux both as a desktop “toolbox” for the Networking Professional, as well as securely configuring and delivering various network services on a Linux platform.

## The History of Linux

To understand the origins of Linux, we have to first discuss the origins of Unix. Unix was developed in the late 1960’s and early 1970’s at Bell Labs, with Dennis Ritchie and Ken Thompson being the main developers. The name Unix was actually a pun on the name of a “Multics”, a previous operating system which inspired many of the Unix features.

In 1983, Richard Stallman started the GNU (“GNU’s Not Unix”) project, which aspired to create a Unix-like operating system available to all for free. In 1992 Linus Torvalds released Linux, the first full released a fully realized GNU kernel.

It’s important to note that Linux is not actually an operating system, rather it’s a kernel that can be used to create an operating system. Linux is still maintained with Linus Torvalds as the lead developer, but today there is a much larger team of individuals and corporations acting as contributors.

Since the 1970’s, hundreds of separate distributions (or distros) of Linux have been released. Some have been “mainstream” for a period of time, and some have been waned in popularity as time has gone one. The thing they all share is the Linux kernel, which they have each built on to create their own distribution. Many distro’s have based their operating system on another distro, customizing that enough to justify calling their implementation a new distribution. This trend has given us the idea of a “Linux Family Tree” – where dozens of distributions can grow from a common “root” - this is nicely explored on the “distrowatch” website, at <https://distrowatch.com/dwres.php?resource=family-tree> .

The exception to this is the BSD (which stands for “Berkeley Software Distribution”) Unix. BSD Unix is a descendent of the original Bell Labs Unix, it is not based on Linux at all. However, BSD and many of its derivatives are still free, and share many characteristics (and a fair amount of code) with Linux.

To this day, the emphasis of both Linux and BSD Unix is that both are freely available operating systems. While commercial versions and derivatives are certainly available, almost all of those commercial versions have matching free versions

## Mainstream Datacenter Linux

It’s important to note that Linux is not a single Operating System. Linux OS’s are all based on the same Kernel, but then are packaged by groups with different goals and philosophies, making for a wide variety of thousands of different “distributions”, or “distros”. A fairly complete list, with some of the “family tree” relationships, can be found on the DistroWatch website, at <https://distrowatch.com/dwres.php?resource=family-tree>.

The main distributions that we commonly see in modern datacenters are Redhat, SUSE, Ubuntu and FreeBSD. This is not to say that other distributions don’t crop up on desktops or datacenters, but these are the ones you’ll see most often. These all have both desktop and server versions – the server versions often being more “stripped down”, with the office productivity, media tools and often the GUI (Graphical User Interface) removed.

### Redhat

Redhat has recently been acquired by IBM (in 2019), but still maintains Fedora as its main project. Fedora has both server and desktop versions, and remains freely available. The commercial version of Fedora is Redhat Enterprise Linux (RHEL). RHEL is commercially licensed and has a formal support channel.

CentOS is a free, community supported version of Linux that is functionally compatible with the Redhat Enterprise version. This makes it very popular for server implementations in many organizations.

Oracle / Scientific Linux is also seen in many datacenters (and in Oracle’s cloud offerings). Oracle Linux is based on Redhat, and in fact advertise their product as fully compatible with Redhat Enterprise Linux. Oracle Linux is free to download and use, but support from Oracle is subscription based.

### SUSE

OpenSUSE is the community distribution that SUSE Linux is based on, similar to how Redhat Enterprise Linux is based on Fedora.

SUSE Linux Enterprise Server (commonly called SLES) was in the early days of Linux the mainly European competitor for the US based Redhat distribution. Those days are past however, and SUSE Linux is (almost) as likely to be found in Indiana as Italy in modern datacenters.

Similar to the relationship between Redhat and CentOS, SUSE maintains both a Desktop a Server version. In addition, they also maintain a “High Performance” version of the OS, which comes with optimizations and tools pre-installed for parallel computing. OpenSUSE

### Ubuntu

Ubuntu Linux is maintained by Canonical, and is freely downloadable, with no commercial option. It is based on Debian, and has a unique release cycle. New versions of both the server and desktop versions are released every 6 months. A “Long Term Support” (LTS) version is released every two years, with support for LTS versions of both the server and desktop running for 5 years from the release date. As with the other larger players, support is subscription based, though as with most distributions free support from the community is a viable option as well.

As you would expect, the server version of Ubuntu is focused more on the core OS, network and datacenter services. The GUI (Graphical User Interface) is often de-selected during the installation of the server version. The desktop version however has several packages installed for office productivity, media creation and conversion, as well as some simple games.

### BSD / FreeBSD / OpenBSD

<https://www.howtogeek.com/190773/htg-explains-whats-the-difference-between-linux-and-bsd/>

As discussed, the BSD “Tree” of the family is derived from Unix rather than from the Linux kernel, but there is definitely lots of shared code, especially once you look at the packages that aren’t part of the kernel.

FeeBSD and OpenBSD were historically viewed as “more secure” than the earlier versions of Linux. Because of this, many firewalls and network appliances were built based on the BSD OS family, and remain on this OS to this day. One of the more “visible” BSD variants is Apple’s commercial operating system OS X, which is based on Darwin, which s in turn a fork of BSD.

As time marched on however, Linux has grown into most of the same security capabilities as BSD, until it became a difference in, for any particular setting, BSD perhaps having the more secure default setting than most Linux alternatives. With SELinux or AppArmor available (and recommended) for most modern Linux distributions, the “more secure” footing is now mainly a historic perception rather than fact.

## Specialty Linux Distributions

### Open Source NAS and SAN providers

Most commercial NAS and SAN providers are based on Linux or BSD. The front runner on open source NAS/SAN services at the time of this writing seems to be TrueNAS (formerly FreeNAS) or XigmaNAS (formerly NAS4Free). Both have free and commercial offerings.

### Open Source Firewalls

Networking and Security companies offer a wide variety of Firewall appliances, most of which are based on Linux or BSD. Many companies do offer free firewalls, some of the more popular being pfSense (free versions and pre-built hardware solutions available), OpnSense (freely available, with donations) and Untangle (which also has a commercial version).

In this book we’ll explore using the on-board firewall in Linux to secure individual servers, or to secure a network perimeter.

### Kali Linux

Descended from Backtrack, and Knoppix before that, Kali Linux is a distribution based on Debian that is focused on Information Security. The underlying goal of this distribution is to collect as many useful Penetration Testing and Ethical Hacking tools as possible on one platform, and ensure that they all work without interfering with each other. The newer versions of the distribution has focused on maintaining this tool-interoperability as the OS and tools get updated (using the “apt” toolset).

### SIFT

SIFT is a distribution authored by the forensics team at the SANS institute, focused on digital forensics and incident response tools and investigations. Similar to Kali, the goal of SIFT is to be a “one stop shop” for free/open source tools in one field – digital forensics and incident response (DFIR for short). Historically this was a distribution based on Ubuntu, but in recent years this has changed – SIFT is now distributed as a script that installs the tools on Ubuntu Desktop or Windows Services for Linux (which is Ubuntu based).

### Security Onion

Security Onion is also similar to Kali Linux in that it contains several information security tools, but its focus is more from the defender’s point of view. This distribution centers on threat hunting, network security monitoring and log management. Tools included on this distribution include Suricata, Zeek, and Wazuh just to name a few.

## Virtualization

Virtualization has played a major role in the adoption of Linux and the ability to work with multiple distributions at once. With a local Hypervisor, a network professional is able to run dozens of different “machines” on their laptop or desktop computers. While VMware was the pioneer in this space (desktop virtualization), they have since been joined by XEN, KVM, VirtualBox and QEMU, just to name a few. While the VMware products are all commercial products (except for VMware Player), the other solutions listed are at the time of this writing still free.

## Picking a Linux Distribution for Your Organization

In many ways, which distribution you select for your datacenter is not important – the main distributions all have similar functions, often have identical components, and have similar vendor or community support options. However, because of the differences between the distros, what is important is that one distribution (or a set of similar distros) is selected.

The desired outcome is that your organization standardizes one distribution that your team can develop their expertise experts with. This also means that you can work with the same escalation team for more advanced support and troubleshooting, whether that is a consulting organization, a paid vendor support team, or a group of like-minded individuals in various internet forums. Many organizations purchase support contracts with one of “the big three” (Redhat, Suse or Canonical, depending on their distribution).

Where you don’t want to be is the situation I’ve seen a few clients end up in. Having hired a person who is eager to learn, a year later they found that each of the servers built that year were on a different Linux distribution, each built slightly differently. This is a short road to your infrastructure becoming the proverbial “science experiment” that never ends!

The main advice in picking a distribution is to stick to one of the larger distributions. If people on your team have strong feelings about one of another of these, then definitely take that into consideration. You will likely want to stay fairly close to one of the mainstream distributions for use within and organization, something that is regularly maintained and has a paid subscription model available for support – even if you don’t feel you need paid support, that may not always be the case.