6.3 LINUX

6.3.1 What is Linux?

Linux is an operating system that evolved from a kernel created by Linus Torvalds when he was a student at the University of Helsinki. Generally, it is obvious to most people what Linux is; however, both for political and practical reasons, it needs to be explained further. To say that Linux is an operating system means that it's meant to be used as an alternative to other operating systems like MS-DOS, the various versions of MS Windows, Mac OS, Solaris and others. Linux is not a program like a word processor and is not a set of programs like an office suite. [4]

6.3.2 A brief history of Linux

When Linus Torvalds was studying at the University of Helsinki, he was using a version of the UNIX operating system called 'Minix'. Linus and other users sent requests for modifications and improvements to Minix's creator, Andrew Tanenbaum, but he felt that they weren't necessary. That's when Linus decided to create his own operating system that would take into account users' comments and suggestions for improvements.

6.3.3 Free Software pre-Linux

This philosophy of asking for users comments and suggestions and using them to improve computer programs was not new. Richard Stallman, who worked at the Massachusetts Institute of Technology, had been advocating just such an approach to computer programming and use since the early 1970's. He was a pioneer in the concept of 'free software', always pointing out that 'free' means 'freedom', not zero cost. Finding it difficult to continue working under conditions that he felt went against his concept of 'free software' he left MIT in 1984 and founded GNU. The goal of GNU was to produce software that was free to use, distribute and modify. Linus Torvalds' goal 6 years later was basically the same: to produce an operating system that took into account user feedback.

6.3.4 Linux Distributions

A Linux "distribution" is version of the Linux operating system made especially by a company, organization or individual.[5] The one thing they all have in common is that they use the Linux kernel. From there on, each developer will add its own programs, tools and other applications. Some are dedicated to specific uses while others are intended for the general public.[5]Companies such as Red Hat, SUSE and Mandriva, and community projects such as Debian, Ubuntu, Gentoo, and the entirely-free Ututo, assemble and test the software before releasing their distribution.[6] There are currently over three hundred Linux distribution projects in active development, revising and improving their respective distributions.
6.3.5 Leading distributions [7]

Leading distributions have been around for a while and are well-established. Usually a variety of products are available from low-end x86 versions to high-end versions for IBM mainframes and the latest 64-bit technology. Most come from companies that supply service and support contracts for their products. They also tend to support many languages.

1. Debian GNU/Linux

Official website: http://www.debian.org/

The Debian Project is currently the largest volunteer based distribution provider. The distribution is supports many languages and hardware platforms. The old (still supported) version is 3.0 (woody), now up to the sixth revision. Debian 3.0r6 was released June 2, 2005. Debian 3.1 (sarge) was released June 6, 2005 and is now the current stable version.

2. Fedora

Official website: http://fedora.redhat.com/

The Fedora Project is Red Hat's community distribution. It is intended to be a fast-paced distribution for those that like to stay on the leading edge of technology. It is also a test-bed for Red Hat's Enterprise Linux products. The Fedora Core contains all the packages necessary to run a functional desktop or small server. The first Fedora Core release was dated November 5, 2003. Fedora Core 3 is still supported. The current stable version is Fedora Core 4, released June 13, 2005. FC5 Test1 was released November 23, 2005.

3. Gentoo Linux

Official website: http://www.gentoo.org/

Gentoo Linux is a source-based distribution that can be optimized and customized for just about any application or need. Gentoo offers extreme performance, configurability and a top-notch user and developer community. Users keep their systems up-to-date using Portage, which is based on BSD Ports. Gentoo is a meta-distribution with a large number of packages available (7000 as of July 2004). Gentoo Linux 2005.0 was released March 28, 2005, supporting Alpha, AMD64, PPC, PPC64, SPARC and X86 (IA64 and SPARC32 in progress). Gentoo Linux 2005.1-r1 was released November 21, 2005 for AMD64, PPC64, SPARC and x86.

4. Mandriva Linux

Official website: http://www.mandrivalinux.com/

Mandriva is a new name for two popular distribution companies resulting from the
merger of the French company Mandrakesoft and the Brazilian company Conectiva. Mandriva has also acquired Lycoris assets and hired Lycoris founder and CEO, Joseph Cheek on June 15, 2005. Mandriva Linux Limited Edition 2005 was released in April 2005 for x86, x86-64 and PPC. Multi Network Firewall (MNF), version 2 was released June 21, 2005. Mandriva Linux 2006 merges technology from Mandriva, Conectiva and Lycoris. It became available to Mandriva Club members on October 7, 2005, and generally availability October 13, 2005.

5. Red Hat Enterprise

Official website: http://www.redhat.com/

Red Hat, Inc. provides one of the the best known distributions in the world. In 2003 the company announced its decision to drop its popular Red Hat Linux in order to concentrate on the Red Hat Enterprise Linux line. The Fedora Project (see above) has replaced the Red Hat Linux line for the home user or small business. Red Hat Linux 9 was released April 7, 2003, and official Red Hat support ended on May 1, 2004. Red Hat Enterprise Linux comes with service and support contracts for those Red Hat customers who require a stable, supported system. Red Hat Enterprise Linux 3 was released October 22, 2003. Red Hat Enterprise Linux 4 (Nahant) was released February 15, 2005.

6. Slackware Linux

Official website: http://www.slackware.com/

Slackware German forum: http://www.slackforum.de/
Slackware (Italian style) http://www.slack.z00.it/slack/slack.html
http://freshmeat.net/projects/slackware/

The Slackware project is headed by Patrick J. Volkerding, with a cast of volunteers and a loyal following. It is the oldest active Linux distribution with the first release dated July 16, 1993. The official Slackware project supports only x86 platforms, however others have made ports to other platforms. Slackware 10.2 was released September 14, 2005.

7. SuSE Linux

Official website: http://www.suse.com/

Nuremberg based SuSE Linux AG was the European UnitedLinux partner, and supplied much of the code base for UnitedLinux. SuSE was acquired by US company Novell (finalized January 12, 2004), but the company is still based in Germany. Novell Open Enterprise Server bundles SLES9 and Netware. SUSE Linux Enterprise Server (SLES) supports x86, x86-64, IPF (ia64), POWER (32 & 64bit, ppc & ppc64) and Mainframes (32 & 64bit, s390 & s390x). SUSE Linux Professional and Novell Linux Desktop are currently only available on x86 and x86-64. Current versions: SLES 9, SUSE LINUX Professional 9.3. SUSE Linux 10.0 was released October 6, 2005. SUSE Linux 10.1 Alpha3 was released November 17, 2005.
8. Ubuntu Linux

Official website: http://www.ubuntu-linux.org/

"Ubuntu" is an ancient African word, meaning "Humanity To Others". The Ubuntu Linux distribution brings the spirit of Ubuntu to the software world, providing a system which is freely available. Both community and professional support is available. Kubuntu is Ubuntu but with KDE instead of GNOME for the desktop. (K)Ubuntu is suitable for both desktop and server use. Edubuntu is a version for the classroom. The initial Ubuntu release (4.10 Preview released September 15, 2004) supports Intel x86 (IBM-compatible PC), AMD64 (Hammer) and PowerPC (Apple iBook and Powerbook, G4 and G5) architectures. Version 4.10 "The Warty Warthog Release" was released October 20, 2004. Ubuntu 5.04 "The Hoary Hedgehog" was released April 8, 2005. Kubuntu 5.04 was also released April 8, 2005. Ubuntu/Kubuntu/Edubuntu 5.10 "the Breezy Badger" final releases are out. Ubuntu 5.10 Server was released October 19, 2005.

6.3.6 LINUX Kernel

- The Linux kernel is a free software Unix-like operating system kernel that was begun by Linus Torvalds in 1991 and subsequently improved with the assistance of developers around the world.
- It was originally developed for the Intel 80386 processor but has since been ported to many other platforms. It is written almost entirely in C with some GNU C language extensions, along with snippets of assembly language (in the GNU Assembler's "AT&T-style" syntax).
- The kernel is best known as the core of GNU/Linux operating systems. Distributions of software based on this kernel are called GNU/Linux distributions.

6.3.6.1 History

- Originally, "Linux" was only the name of the kernel.
- The term "kernel" properly refers to the low-level system software that provides a hardware abstraction layer, disk and filesystem control, multi-tasking, load-balancing, networking and security enforcement.
- A kernel is not a complete operating system (as the term is usually understood). A complete system built around the Linux kernel is commonly known as the Linux operating system, although some prefer to call the system GNU/Linux.
- People often confuse the kernel with the operating system, leading to many mistaken notions, e.g. the idea that Torvalds wrote or coordinates other parts of the system than the kernel.

6.3.6.2 Versions

Further developing his own code and integrating changes made by other programmers, Linus Torvalds keeps releasing new versions of the Linux kernel. These are called "vanilla" kernels, meaning they have not been modified by anyone. Many providers of GNU/Linux operating systems modify the kernels of their product, mainly in order to add support for drivers or features which have not officially been released as stable, while
some distributions, such as Slackware, rely on vanilla kernels.

**Version numbering**
The version number of the Linux kernel currently consists of four numbers, following a recent change in the long-standing policy of a three-number versioning scheme. For illustration, let it be assumed that the version number is composed thus: A.B.C[D] (e.g. 2.2.1, 2.4.13 or 2.6.12.3).

* The **A** number denotes the kernel version. It is changed least frequently, and only when major changes in the code and the concept of the kernel occur. It has been changed twice in the history of the kernel: In 1994 (version 1.0) and in 1996 (version 2.0).

* The **B** number denotes the major revision of the kernel. Even numbers indicate a stable release, i.e. one that is deemed fit for production use, such as 1.2, 2.4 or 2.6. Odd numbers are development releases, such as 1.1 or 2.5. They are for testing new features and drivers until they become sufficiently stable to be included in a stable release.

* The **C** number indicates the minor revision of the kernel. In the old three-number versioning scheme, this was changed when security patches, bugfixes, new features or drivers were implemented in the kernel. With the new policy, however, it is only changed when new drivers or features are introduced; minor fixes are handled by the **D** number.

* **D** number first occurred when a grave error, which required immediate fixing, was encountered in 2.6.8's NFS code. However, there were not enough other changes to legitimate the release of a new minor revision (which would have been 2.6.9). So, 2.6.8.1 was released, with the only change being the fix of that error. With 2.6.11, this was adopted as the new official versioning policy. Bug-fixes and security patches are now managed by the fourth number, whereas bigger changes are only implemented in minor revision changes (the C number).

**6.3.6.3 Programming languages**

- The Linux kernel is written in the version of the C programming language supported by the GNU GCC compiler (which supports a superset of standard C), together with relatively short sections of code written in the assembly language of the target architecture (and at last count Linux supported about 20 different processor families).

- Because of the extensions to C supported by the GCC compiler it was (in conjunction with its associated toolset) for long the only compiler capable of correctly building a Linux kernel. More recently Intel claims to have modified its C compiler so that it also is capable of compiling the kernel.

- Many other languages are used in some way, primarily in connection with the
kernel 'build' process (the methods whereby the bootable image is created from the sources). These include Perl, Python, and various shell scripting languages. Some drivers may also be written in C++, Fortran, or other languages, but this behavior is strongly discouraged. The kernels build system only supports GCC as kernel and driver compiler.

6.3.6.4 **Kernel panic**
In Linux, a "panic" is an unrecoverable system error detected by the kernel as opposed to similar errors detected by user space code. It is possible for kernel code to indicate such a condition by calling the panic function located in the header file sys/system.h. However, most panics are the result of unhandled processor exceptions in kernel code, such as references to invalid memory addresses. These are typically indicative of a bug somewhere in the call chain leading to the panic.

6.3.7 **Denial-of-service attack [15]**

A **denial-of-service attack** (also, **DoS attack**) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

6.3.7.1 **Effects of DoS**

Denial of Service attacks can also lead to problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by a DoS, meaning not only will the intended computer be compromised, but the entire network will also be disrupted.

If the DoS is conducted in a sufficiently large scale, entire geographical swathes of Internet connectivity can also be compromised by incorrectly configured or flimsy network infrastructure equipment without the attacker's knowledge or intent. For this reason, most, if not all ISPs ban the practice.

6.3.7.2 **Distributed Denial-of-Service Attacks**

In a distributed attack, the attacking computer hosts are often zombie computers with broadband connections to the Internet that have been compromised by viruses or Trojan horse programs that allow the perpetrator to remotely control the machine and direct the attack, often through a *botnet*. With enough such slave hosts, the services of even the largest and most well-connected websites can be denied.