Linux System Administration and Support

Training Material

Atlantic LINUX

License

Except where otherwise noted, this work is licensed under
http://creativecommons.org/licenses/by-nc-sa/3.0/

Atlantic LINUX

Contents

Contents

Contents

Atlantic LINUX

Contents

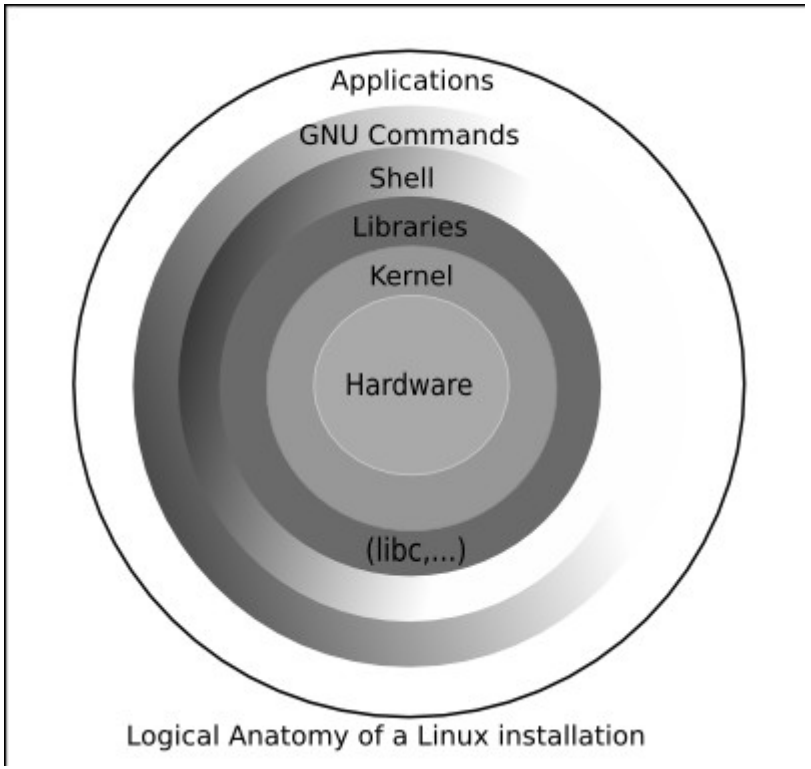
Contents

Atlantic LINUX

Introduction

What is Linux

- Kernel
  - 2.4.x
  - 2.6.x
- Distributions
  - Red Hat
  - Novell / SuSE
  - Debian
- GNU
  - compilers
  - libraries
  - editors and other tools



Logical Anatomy of a Linux installation

A brief history of Linux

Sep 1983 – Richard Stallman announces the GNU Project

Apr 1991 – Linus Torvalds announces he's working on a hobby OS

Sep 1991 – Linux Kernel 0.01

Mar 1994 – Linux Kernel 1.0 (i386)

Mar 1995 – Linux Kernel 1.2 (Alpha, Mips, Sparc)

June 1996 – Linux Kernel 2.0 (SMP, Tux the Penguin)

Jan 1999 – Linux Kernel 2.2 (64-bit, FAT32, NTFS)

Jan 2001 – Linux Kernel 2.4 (ISA PnP, PA-RISC, USB, PC Card)

Dec 2003 – Linux Kernel 2.6 (IA64, x86_64, em64t, embedded systems, NUMA)

Linux distributions (1/2)

- Red Hat
  - Enterprise Linux (Advanced Platform, Workstation, Desktop) v5
  - Enterprise Linux (AS, ES, WS, Desktop) v4
  - Enterprise Linux (AS, ES, WS) v3
  - Fedora Core
- Debian
  - Stable (4.0 - *Etch*)
  - Testing (*Lenny*)
  - Unstable (*Sid*)
  - Derivatives (Ubuntu, Xandros, Knoppix, Progeny)

Linux distributions (2/2)

- Novell / SuSE
  - SuSE Linux Enterprise Server 10
  - Novell Linux Enterprise Desktop 10 (formerly Novell Linux Desktop)
  - openSuSE 10.2
- Others
  - Gentoo
  - Mandriva
  - Ubuntu
  - Sun Java Desktop System
  - Slackware
  - Turbolinux

Who is using Linux?

- Dot coms
  - Google
  - Amazon
  - Paypal
- Financial
  - Irish Stock Exchange
  - First Trust Corporation
  - Central Bank of India
- Entertainment
  - Ticketmaster
  - Pixar
  - Industrial Light and Magic

What is system administration?

- Installation of the operating system.
- Installation of new hardware and software on the system.
- Maintaining the system with updates and patches.
- Configuring the system.
- Adding and removing users.
- Performing backups.
- Securing the system.
- Documenting the configuration of the system.
- Troubleshooting system problems.
- Performance tuning the system.
- Providing support to system users.

The super user

- Typical super-user activities
  - Filesystem maintenance
  - Software installation
  - Reviewing log-files
- su
- sudo
  - /etc/sudoers

System documentation (1/2)

- Distribution-specific documentation
  - Administration and install guides
  - User manuals
  - Reference guides
  - Release Notes
- man pages and the man command
  - *man [section] <page>*
  - *man -k <topic>*
  - *man -f <topic>* or *apropos <topic>*
  - *man man!*

System documentation (2/2)

- GNU info
- <command> -h, --help
- The Linux Documentation Project
  - http://www.tldp.org/
  - FAQs, HOWTOs, Guides
- Project specific documentation for Samba, Apache and others.

Editing system Files - introduction

- Typical editors on Linux systems
  - vi / vim
  - emacs / xemacs
- Starting vi
- Buffers
- vi modes
  - command mode
  - insert mode
  - switching modes
- Quitting vi

Editing system Files - navigation in vi

- Traditional navigation
- Cursor keys
- Paging
- Advanced navigation
  - start of line / end of line
  - next word
  - previous word
  - start of file / end of file
  - specifying particular lines

Editing system Files – cut and paste in vi

- Copy (yank)
  - single lines
  - multiple lines
- Paste
- Cut (delete)
  - lines
  - characters
- Inserting files

Editing system Files - finding text in vi

- Simple search
  - repeating
  - backwards
- Simple find and replace
- Advanced search
- Regular expressions

Editing system files - advanced vi

- Undo
- Starting editing on a particular line
- Replace mode

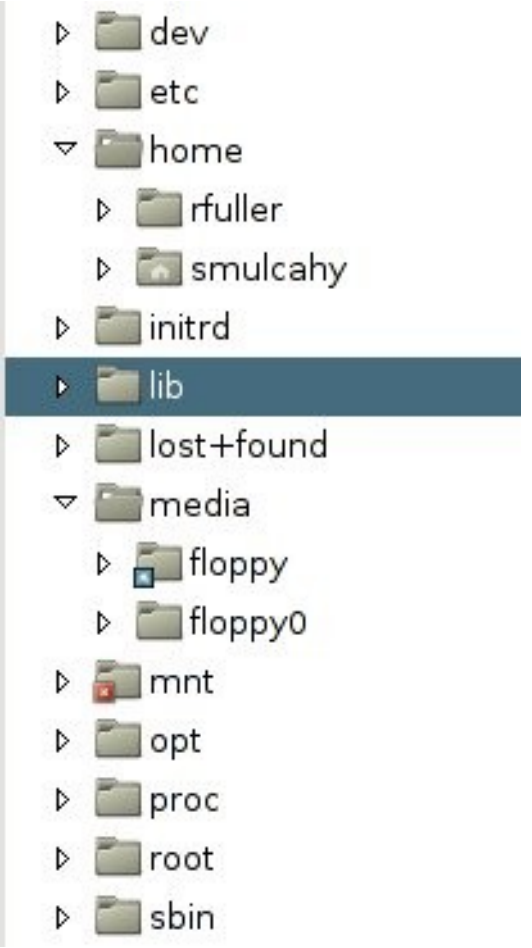
Exercise 1 - Editing

1) Create a text file containing a few sentences of text.
2) Copy a few lines of the file.
3) Use search and replace to replace all occurrences of the word “the” in your file with the string “xxxx”.
4) Copy /etc/passwd to a file in /var/tmp and practice navigating around it.
5) Remove the password for a user in the copied password file.

The Filesystem

Linux Files

- Everything is a file!
  - Docs, pictures, executables
  - Directories
  - Devices
  - Kernel internals
  - .dot files
  - hard links
  - soft (symbolic) links
- Filesystem Hierarchy Standard (FHS)
- Hard and soft links



File Hierarchy Standard - /

- /
- /bin
- /boot
- /dev
- /etc
- /home
- /lib

File Hierarchy Standard - /

- /mnt (and the mount command)
- /opt
- /root
- /sbin
- /tmp
- /usr
- /var

File Hierarchy Standard - /usr

- /usr/bin
- /usr/include
- /usr/lib
- /usr/local
- /usr/sbin
- /usr/share
- /usr/src

File Hierarchy Standard - /var

- /var/cache
- /var/lib
- /var/lock
- /var/log
- /var/mail
- /var/opt
- /var/run
- /var/spool
- /var/tmp

A brief look at Linux filesystems

- Simple
  - UFS
  - EXT2
- Journalling (Logging)
  - EXT3
  - ReiserFS
  - XFS
  - JFS
- Performance
  - File sizes
  - I/O Profile (read or write)

Configuring filesystems

- mkfs(8)
- mount(8)
- umount(8)
- /etc/fstab

```
# <file system> <mount point>   <type>  <options>                       <dump>  <pass>
proc            /proc           proc    defaults                        0       0
/dev/hda2       /               ext3    defaults,errors=remount-ro      0       1
/dev/hda5       none            swap    sw                              0       0
/dev/hdc        /media/cdrom0   iso9660 ro,user,noauto                  0       0
```

Quotas (1/2)

- Specified per filesystem
  - User quotas
  - Group quotas
- Soft quotas
  - Enforced after a grace period
- Hard quotas
  - Immediately stops any writes
- Can send email notifications to users over quota

Quotas (2/2)

- Quota commands
  - quotacheck
  - edquota
  - warnquota

```
Disk quotas for user smulcahy (uid 1000):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/sda2                      1230       2000       3000        553        0        0
```

File permissions and ownership (1/2)

- Setting permissions
  - Symbolic mode

  chmod <groups> <add/remove/set> <permissions> <file>

  e.g.

  chmod u=rwx,g=rx,o=rx foo

  chmod u=r,g=r,o= foo

  - Octal mode

  chmod <mode> <file>

  e.g.

  chmod 0755 foo

  chmod 0440 foo

File permissions and ownership (2/2)

- Changing file ownership
  - chown
- Changing file group
  - chgrp

- Special permissions
  - The sticky bit
  - The setuid/setgid bit
  - File owner

Monitoring free space and inodes

- Files and directories
  - du
- Mounted filesystems
  - df
- -h option improves readability

Filesystem maintenance

- Tuning
  - tune2fs and reiserfstune
- Repair
  - fsck and reiserfsck
  - debugfs and debugreiserfs
- Filesystem identifiers
  - device names
  - labels
  - UUIDs
- Resizing
  1. partitions
  2. filesystems

Exercise 2.1 - Files

1) Review a full directory listing (ls -la) for the following directories,
   - /
   - /var/log
   - /etc
2) Using the man page for the ls command, explain the contents of each column.
3) Review some files under /var/log using the less command.
4) Create a hard link and a symbolic link for a file in your home directory.
5) Create a file in your home directory containing some text.

Exercise 2.2 - Files

6) Create a symbolic link and a hard link to this file.

7) Remove the original file and explain whether each link still exists and what it points to.

8) Where in the filesystem should the following files be?

- a configuration file
- a large 3rd party software package
- documentation for a standard system package
- a log file for a system daemon
- a file related to booting
- a user's email

Exercise 2.3 – Files

9) **Using both symbolic mode and octal mode, set the following permissions on sample files in your home directory (see the touch command for creating test files),**

- **readable and writeable by you only**
- **readable and executable by you only**
- **readable, writeable and executable by you and readable and writeable by everyone else**

Exercise 2.4 - Files

10) **Create a new filesystem.**
11) **Add an entry in /etc/fstab for the filesystem, so that its default mount point is /mnt/new**
12) **Enable quotas on a filesystem.**
13) **Create a quota for a user giving them a soft limit of 1MB and a hard limit of 1.2MB**
14) **Report the space used by your home directory and the free space available on your filesystems.**
15) **Run a filesystem check.**

Booting

The boot process

BIOS → MBR

MBR → **Boot Loader**

Boot loader → **Linux kernel**

Linux kernel → **init**

init → **getty**.

getty → **login**

login → **shell**

Boot loaders

- LILO
  - ease of installation
  - physical location of kernel
  - 1024 cylinder limit
  - /etc/lilo.conf
- GRUB
  - filesystem aware
  - interactive mode
  - broad range of operating systems
  - /boot/grub/menu.lst
- NTLDR (Windows)
  - Capable of loading other operating systems

Boot options

- Passed via
  - Bootloader config file
  - Boot prompt
- General options
  - single
  - root=<device>
  - acpi=off
  - init=<program>
- Hardware-specific
  - PCI
  - SCSI, IDE
  - Ethernet

Runlevels, init and rc.d

- Starting/stopping
- Adding new ones
- `/etc/init.d`
- Run-levels
  - `/etc/inittab`
  - `/etc/init.d/rc`*n*`.d`
- Distribution differences
  - SuSE / Novell Linux Desktop
  - Red Hat
  - Debian

Shutdown and rebooting

- shutdown
  - -r
  - -h
  - time
    - now
    - hh:mm
    - +m
- reboot
- halt
- warm vs. cold reboots

Dual boot configurations

- Overview
- Not limited to 2 operating systems
- Windows on primary partition
- Issues
  - 1024 cylinder limit
  - MBR reset
  - Kernel changes
- Advanced
  - Partition hiding
  - Partition re-ordering

Exercise 3 - Booting

1. Review the ps man page and run the ps command with options showing the hierarchy of processes.
2. Change the default runlevel on your system to the non-graphical mode and reboot the system.
3. Add an option to the boot loader to boot the operating system in single user mode.
4. Add a new service to be started up in your default runlevel (either manually or using *chkconfig* on Redhat/ SuSE, *update-rc.d* on Debian)
5. Disable the service again.
6. Perform a shutdown of the system at a specific time in the future using either time format.

Adding hardware

Useful commands

- Diagnostic commands
  - dmesg
  - lspci
  - lsusb
  - hwinfo
  - dmidecode
- Loading kernel modules
  - modprobe
  - hotplug

General issues

- Unrecognised devices
  - unrecognised device id
  - attempt manual unload
  - information on device chipset required
  - hardware compatibility databases
- Device firmware
  - required for proper operation of device
  - usually available from vendor or driver developer
- Resource conflicts
  - PCI (interrupts allocated by BIOS, shared interrupts ok)
  - ISA, PCMCIA (probing issues and conflicts)

/dev filesystem

- /dev
  - major and minor numbers
  - mknod
  - MAKEDEV
- udev
  - /dev files created on the fly
  - persistent device naming possible
- sysfs
  - kernel interface to device information

/proc filesystem

- /proc/NNN/
  - one per process
- /proc/cpuinfo
  - processor information
- /proc/version
  - kernel version
- /proc/meminfo
  - memory details
- /proc/devices
  - device drivers and major numbers
- /proc/bus
  - a tree of information about system buses (pci, usb, ...)

Storage devices

- IDE
  - /dev/hd*
- SCSI
  - /dev/sd*
- SATA
  - /dev/sd*
- Commands
  - scsiinfo
  - lsscsi
  - hdparm

Network devices

- Device names
  - /dev/ethN (/dev/trN, /dev/loN, /dev/sitN, /dev/pppN)
- Linux 2.4 device detection
- Linux 2.6 device detection
- Device ordering
  - module load order
  - PCI BIOS Ids
- Commands
  - ifconfig
  - nameif
  - mii-tool

Exercise 4.1 – Adding Hardware

1. Identify the network card installed on the system using the lspci tool.
2. List the USB devices attached to the system and identify which types of USB controllers are attached to the system.
3. Identify how many CPUs are installed in your system and what type they are (processor model, manufacturer and speed).
4. Retrieve the system model and serial number using either the hwinfo or dmidecode commands.
5. Review the contents of the /dev system and indicate whether the system is using udev or a traditional static /dev.

Exercise 4.2 – Adding Hardware

6. **Identify the major and minor numbers of the cdrom device and the hard drive.**
7. **Using the /proc filesystem report the total amount of memory in the system, the kernel version in use and the interrupt used by the first network device.**
8. **What is the make and model of the first hard-drive?**
9. **What is the MAC address of your network device? What is its IP address?**

The X Window System

Overview of X

- Introduced in 1984
- Standard environment for UNIX Windowing systems
- Network-transparent graphical windowing system
- Capabilities:
  - Network transparent
  - Graphical capability
  - Not tied to any particular display software
- Server
  - The program that talks to the keyboard, mouse and graphics hardware
- Client
  - The program requesting draw operations
- X.Org and XFree86

Window Managers and Widget Libraries

- Xlib
- Window Managers
  - TWM
  - FVWM
  - Kwin
  - Metacity
- Client Applications
- Widget Libraries
  - Athena
  - Motif
  - GTK+
  - Qt

Desktop Environments

- Standard look and feel
- CDE
- KDE
  - Kwin window manager
  - Qt toolkit and KDE library
  - Kpanel launcher
  - Konqueror file manager
- GNOME
  - Metacity window manager
  - GTK+ toolkit
  - Gnome panel
  - Nautilus file manager

Installation and configuration

- Installation
  - Hardware is automatically detected
  - Choose desktop environment
  - Configuring display manager
- Configuration
  - SuSE / Novell Linux Desktop
    - yast2 (or sax2)
  - Red Hat
    - redhat-config-xfree86
  - Debian
    - dpkg-reconfigure xserver-xfree86
- Fonts

Display Managers

- Role of the display manager
  - login management
  - remote login
  - XDMCP
  - (configuration tool)
- Versions
  - XDM
  - GDM
  - KDM

Exercise 5 – X

1. Restart your session using a different desktop environment or Window manager and note some differences.
2. Change the resolution of your default desktop
3. Enable XDMCP on your display manager
4. Start the XDMCP chooser on your display manager and connect to another desktop
5. Identify the video driver being used in your X configuration (hint: Section is "Device")

Software packages

Overview

- Overview
  - Red Hat (rpm)
  - Novell Desktop Linux / SuSE (rpm)
  - Debian (deb)
  - Slackware (tgz)
- Dependencies
- Versions
- Package contents
  - Packaged software
  - Installation software
  - Package information
  - Dependency information

RPM

- Installing

  rpm -ivh <*package*>.rpm
- Listing

  rpm -qa
- Removing

  rpm -e <*package*>
- Advanced uses

  rpm -qi <package>

  rpm -qR

Advanced Package Management Tools

- Automatically download packages from network
- Resolve dependencies automatically
- Debian
  - apt
  - aptitude
  - synaptic
- RedHat
  - up2date
  - yum
- SUSE
  - RedCarpet

Red Hat Package Management Tool

- Graphical Tool for Managing Packages on Red Hat
  - Install
  - Remove
  - Update
  - Automated Dependency Management
- Invocation
  - Applications > System Settings > Add/Remove Applications
  - system-config-packages
- Package Groups
  - Standard packages
  - Extra packages

Red Hat Network

- Automatic System Updates from Red Hat
  - Security Alerts
  - Bug Fix Alerts
  - Enhancement Alerts
- Red Hat Update Agent
- https://rhn.redhat.com/
- Automatically updates 1 or more systems
- Requires a valid Red Hat subscription

Source packages

- Sources
  - author homepage
  - freshmeat.net and sourceforge.net
- Checksums
- Extraction
  - tar zxvf <package>.gz
  - tar jxvf <package>.bz2
- Development packages
- Steps
  - ./configure
  - make
  - make install (to /usr/local)

Managing shared libraries

- Libraries
  - static
  - shared
- Portability of static binaries (e.g. skype)
- Commands
  - ldd <command>
  - ldconfig -v
- Files
  - /etc/ld.so.conf
- Variables
  - LD_LIBRARY_PATH
  - LD_PRELOAD

Exercise 6 – Software packages

1. **List all installed packages**
2. **Display some information about the bash package**
3. **Display the dependencies the bash package has**
4. **Display the shared libraries that the bash binary uses.**
5. **Download and install the srm source package from sourceforge.net**

User and Group Management

System Accounts

- Users
  - uid
  - username
  - password
- Groups
  - gid
- /etc/passwd
- /etc/group
- Other authentication mechanisms

Account Settings

- Passwords
  - choosing good passwords
  - password expiry
  - password security
- Shell
- Home directories

Managing user accounts

- User files
  - /etc/passwd
  - /etc/shadow
- User commands
  - useradd and userdel
  - usermod
  - passwd
  - chpasswd
  - chage
  - chfn
  - chsh
  - vipw

Managing groups

- Group files
  - /etc/group
  - /etc/gshadow (*not used on SuSE/NLD*)
- Group commands
  - groupadd and groupdel
  - groupmod
  - gpasswd
  - grpck
  - vigr

Shell configuration files

- Bourne shells
  - /etc/profile
  - ~/.profile
  - ~/.bash_profile
  - ~/.bash_login
- C shells
  - /etc/csh.login
  - /etc/csh.cshrc
  - ~/.tcshrc
  - ~/.cshrc
- .bashrc (interactive and non-interactive shells)
- . and source

User resource limits

- Denial of service
- Kernel
  - /usr/include/linux/limits.h
- PAM
  - /etc/security/limits.conf
- Process limits
  - ulimit in bash
  - limit in tcsh

- Resources
  - core file size
  - cpu time
  - data segment size
  - file size
  - maximum locked memory
  - maximum memory
  - maximum user processes
  - open files
  - stack size
  - virtual memory

Scheduling jobs and managing user access

- Running jobs once at some future time
  - at
- Running jobs once when the system is under-used
  - batch
- Running jobs regularly
  - cron

```
0 7 * * * ~/bin/daily-backup.sh
0 7 * * 1 ~/bin/weekly-backup.sh
0 7 1 * * ~/bin/monthly-backup.sh
```

- Controlling access
  - allow
  - deny

Exercise 7.1 – User and group management

1. **Add a new user to the system**
2. **Change the user's home directory to /home/newhome and move the existing user directory**
3. **Add a second user to the system**
4. **Write a script to set the passwords of both new users to a new string**
5. **Remove this user from the system**
6. **Using the chage command, force one of the new users to change their password at next login.**
7. **Change the users shell to /bin/tcsh**
8. **Open 2 shells on your system as root. Start vipw in one. Leave that vipw session running and start a vipw session in the other window. Note any errors.**
9. **Add a new group.**

Exercise 7.2 – User and group management

10. **Change one of the users to be a member of this group.**
11. **Limit the file size that can be created for one of the new users to 1MB.**
12. **Login as this user and attempt to create a larger file (use dd /dev/zero ...) and note any errors.**
13. **Schedule a regular job to back up your home directory to a compressed archive in /var/tmp. The job should run at 5:00am every day except Sunday. Ensure no-one else can view or extract the file.**
14. **Explain the following cron entries**

```
25 4 * * 1 w
* * * * * /bin/monitor.sh
0 * * * * /bin/wall /0.txt
5 9-17 * * 1-5 /bin/work
```

Process Management

Processes and Threads

- Heavyweight process
- Lightweight process
- Speed of context switch
- Speed of creation
- Ease of sharing data
- Security
- NPTL

Shell job control

- foreground jobs
- background jobs (&)
- listing jobs
- switching
- suspending
- interrupting

Listing processes

```
# ps aux

USER       PID %CPU %MEM    VSZ  RSS TTY      STAT START   TIME COMMAND
 root         1  0.0  0.0   1492  104 ?        S    Aug28   0:04 init [2]
 root         2  0.0  0.0      0    0 ?        SW   Aug28   0:00 [keventd]
 root         3  0.0  0.0      0    0 ?        SWN  Aug28   0:00 [ksoftirqd_CPU0]
 root         4  0.0  0.0      0    0 ?        SW   Aug28   6:05 [kswapd]
 root         5  0.0  0.0      0    0 ?        SW   Aug28   0:24 [bdflush]
 root         6  0.0  0.0      0    0 ?        SW   Aug28   0:10 [kupdated]
 root       222  0.0  0.0      0    0 ?        SW   Aug28   0:10 [kjournald]
 root       223  0.0  0.0      0    0 ?        SW   Aug28   0:00 [kjournald]
 root       294  0.0  0.0      0    0 ?        SW   Aug28   0:00 [khubd]
 daemon    1508  0.0  0.0   1604   64 ?        S    Aug28   0:00 /sbin/portmap
 root      1564  0.0  0.2   1628  360 ?        S    Aug28   0:56 /sbin/syslogd
 root      1603  0.0  0.0   2152   80 ?        S    Aug28   0:02 /sbin/klogd
 root      1607  0.0  1.8  12644 2324 ?        S    Aug28   0:00 /usr/sbin/named
```

Process listing variations

- `ps -elf`
- `ps`
- `ps u`
- `ps ux`
- `ps x -o user,pid,ppid,cmd`

Process states

- Runnable (R)
- Sleeping (S)
- Uninterruptible Sleep (D)
- Traced or stopped (T)
- Defunct or zombie (Z)
- Additional BSD status codes
  - No resident pages (W)
  - High priority process (<)
  - Low priority process (N)
  - Process with pages locked in mem (L)

Monitoring processes

- top cpu processes
- cpu state information
- similar details to ps
- process priority and nice

Signals

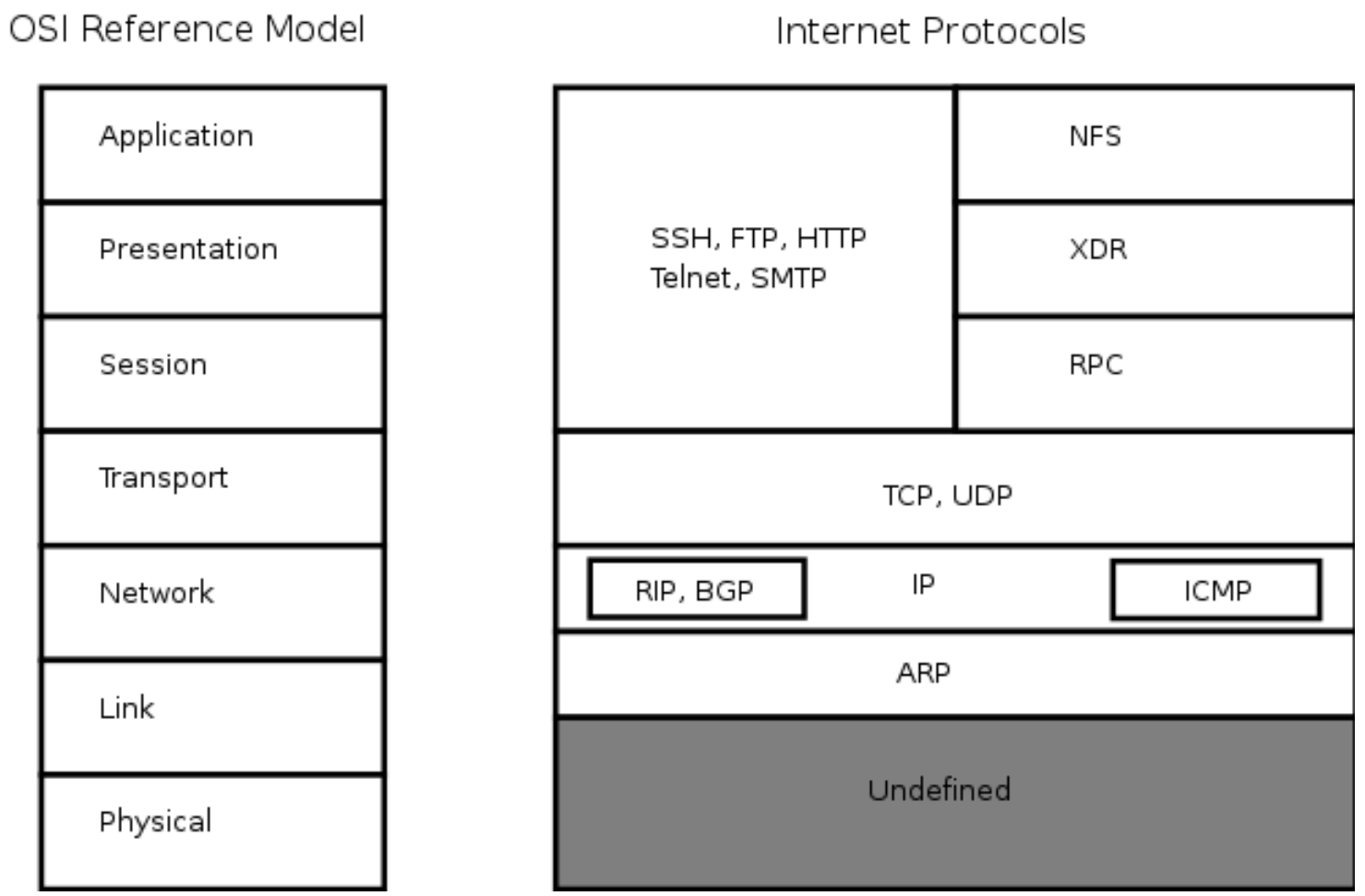
- What are they?
- What do they do?
- Sending signals via the keyboard
- Sending signals with the kill command
- Sending signals with system calls
- Common signals

Exercise 8 – Processes

1. **Review the man page for ps and do the following:**
   - **display only your processes**
   - **display all processes**
2. **Display processes in a hierarchy showing parent and child processes (hint: forest).**
3. **Identify some high priority tasks running on the system.**
4. **Identify some processor and memory intensive tasks.**
5. **Start a simple process of your own and experiment with running it in the background and bringing it to the foreground (echo).**
6. **Kill the process while it is running in the background.**

Network Configuration

Networking Concepts



IP Addresses

- Address (network part and host part)
- Netmask (used to identify the network part)
- Network
- Broadcast (address all hosts on a network)

Address	**192.168.0.1**	11000000.10101000.00000000. 00000001
Netmask	**255.255.255.0 = 24**	11111111.11111111.11111111. 00000000
Host part	**0.0.0.255**	00000000.00000000.00000000. 11111111
Network	**192.168.0.0/24**	11000000.10101000.00000000. 00000000
First Host	**192.168.0.1**	11000000.10101000.00000000. 00000001
Last Host	**192.168.0.254**	11000000.10101000.00000000. 11111110
Broadcast	**192.168.0.255**	11000000.10101000.00000000. 11111111

Devices and Tools

- Network devices
  - eth0, eth1, ...
- Tools
  - ifconfig
  - ping
  - telnet
  - traceroute
  - route
  - ipcalc

TCP/IP configuration and troubleshooting (1/4)

1. Is the network connected?
2. Is the device configured and enabled (static and dhcp)
   - ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:0F:FE:22:14:86
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20f:feff:fe22:1486/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:326397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:447519 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:210758569 (200.9 Mb)  TX bytes:401554909 (382.9 Mb)
          Interrupt:5
```

1. Is the address a valid one for your network?
2. Is anyone else using the address?
   - arping

TCP/IP configuration and troubleshooting (2/4)

5. Are the netmask and broadcast correct?
6. Are the routes correct?
   - Check with route -n

```
$ route -n
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
```

   - Check a path with traceroute

```
$ traceroute -n www.google.com
traceroute to www.google.com (66.102.9.104), 30 hops max, 40 byte packets
 1  192.168.0.1  0.160 ms   0.141 ms   0.154 ms
 2  192.168.0.200  0.603 ms   0.818 ms   0.784 ms
 3  169.131.100.25  20.560 ms   32.542 ms   41.286 ms
 4  83.71.114.145  49.295 ms   57.287 ms   62.779 ms
```

TCP/IP configuration and troubleshooting (3/4)

7.Testing connections with ping

- Ping command
  - basic test of connection
  - measure of network latency
  - measure of packet loss
- Connections to test
  - own system
  - system on local subnet
  - local gateway
  - system on another subnet
  - system on the internet

TCP/IP configuration and troubleshooting (4/4)

8. Are there firewalls in use on the network?
   - Are they between you and the problem system
   - Have they logged any messages for your systems IP
9. Is this a DNS problem?
   - Are there DNS servers defined in /etc/resolv.conf?
   - Can you connect ok to an IP address?
   - Are your DNS servers working (dig or nslookup)?
10. Is the MAC address getting correctly mapped to the IP?
   - arp -v

Domain Name System - DNS

- Overview
- nsswitch.conf
- /etc/hosts
- /etc/resolv.conf
- host
- dig

  dig <hostname>

  dig -x <IP address>
- nslookup

  nslookup <hostname>

  nslookup <IP address>

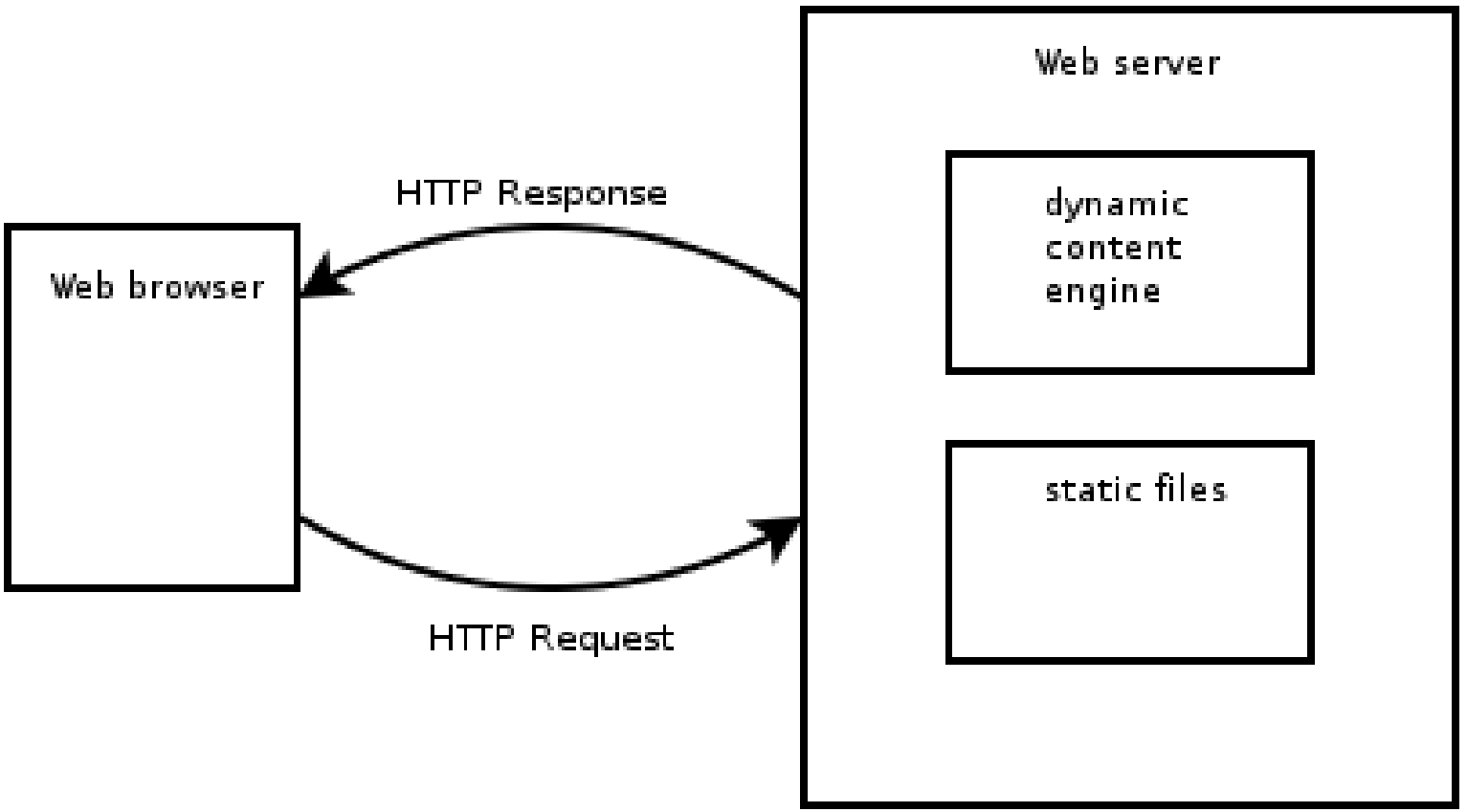
Network services

- Super-daemons
  - inetd
    - /etc/inetd.conf
    - /etc/services
    - disable by commenting line and restarting
  - xinetd
    - /etc/xinetd.conf
    - /etc/xinetd.d
    - disable by adding disabled line to config
- Standalone daemons

Mailserver overview

- Terminology
  - MTA
  - MSA
  - MUA
- Software
  - Sendmail
  - Postfix
  - Exim
- Configurations
  - Local mail only (*this should never be disabled*)
  - Satellite System
  - Internet mailserver

Webserver overview



The Apache Webserver - Introduction

- Versions
  - 1.3
  - 2.0
  - 2.2
- Configuration location
  - Debian
  - SuSE
  - Red Hat
- Main configuration file
  - httpd.conf
- Controlling apache with apachectl

The Apache Webserver – httpd.conf (1/5)

- Sections
  - Global environment
    - MPM Specific Settings
  - Main server configuration
  - Virtual hosts
- Global environment
  - ServerRoot
  - LockFile
  - PidFile
  - ScoreBoardFile
  - TimeOut
  - KeepAlive
  - MaxKeepAliveRequests
  - KeepAliveTimeout
  - Listen
  - LoadModule

The Apache Webserver – httpd.conf (2/5)

- MPM Specific Settings
  - MPM is core module for handling OS specific aspects of server
  - Several different MPMs available for Linux
  - MPM is determined at compile-time
    - Use *httpd -l* to determine what MPM is being used by apache
  - The following parameters should generally be changed if moving MPM:
    - StartServers
    - MinSpareServers
    - MaxSpareServers
    - MaxClients
    - ServerLimit
    - MaxRequestsPerChild

The Apache Webserver - httpd.conf(3/5)

- Main Server Configuration
  - User
  - Group
  - ServerAdmin
  - ServerName
  - DocumentRoot
  - <Directory ... >
  - AccessFileName
  - <Files ... >

The Apache Webserver – httpd.conf (4/5)

- Main Server Configuration (contd.)
  - HostnameLookups
  - ErrorLog
  - LogLevel
  - CustomLog
  - LogFormat
  - Alias
  - ScriptAlias

The Apache Webserver – httpd.conf (5/5)

- Virtual Hosts
  - Name based virtual hosts
  - IP based virtual hosts

```
<VirtualHost 10.1.2.3>
    ServerAdmin webmaster@support.example.com
    DocumentRoot /www/docs/support.example.com
    ServerName support.example.com
    ErrorLog logs/support.com.com-error_log
    TransferLog logs/support.example.com-access_log
</VirtualHost>
```

The Samba server - Introduction

- Windows interoperability
- SMB/CIFS protocol
- Features
  - File services
  - Print services
  - Domain services
- Web based configuration interface (SWAT)
- smbclient tool
  - -L <samba server>
  - //<samba server>/<sharename>

The Samba server – Security modes

- security = user
- security = share
- security = domain
- security = ADS
- security = server

The Samba server – Configuration (1/2)

- Samba daemons
  - smbd
  - nmbd
  - winbindd
- /etc/samba/smb.conf

```
[global]
workgroup = AWORKGROUP
netbios name = ASERVER
[share1]
path = /tmp
[share2]
path = /my_shared_folder
comment = Some random files
```

The Samba server – Configuration (2/2)

[global]

- workgroup
- server string
- log file
- security
- printing
- printcap name
- domain master

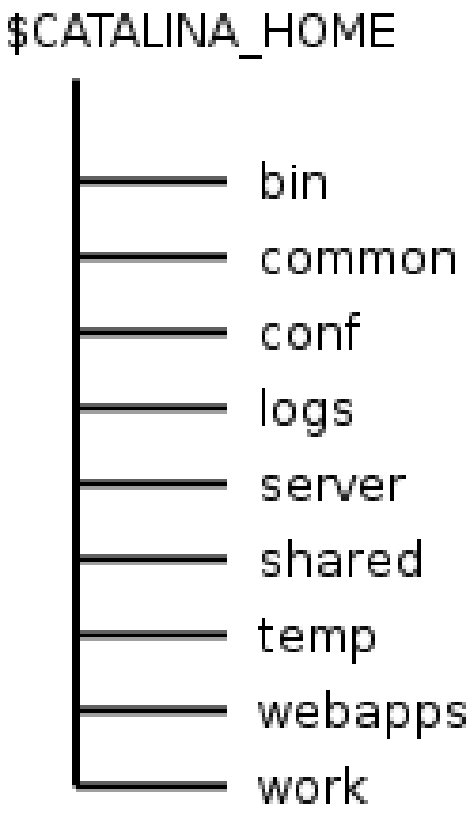
[*sharename]*

- path
- comment
- browseable
- writable
- create mode
- public

Jakarta Tomcat - Introduction

- Functions
  - Servlet container (Catalina)
  - JSP compiler
  - Implements Servlet and JSP specifications
  - Provides a standalone webserver
- Versions
  - 5.x
  - 4.x
  - 3.x
- Requirements
  - Java Development Kit 1.2 or later
  - Apache Ant tool

Jakarta Tomcat - Configuration



Network File System – NFS (1/2)

- Introduction
- Versions
  - 2
  - 3
  - 4
- User-space versus kernel NFS server
- Commands
  - mount
  - showmount
  - rpcinfo

Network File System – NFS (2/2)

- Client
  - /etc/fstab
  - mount options
- Server
  - /etc/exports
  - export options
- Configuration
  - security
  - performance
  - reliability

Secure shell – SSH (1/2)

- Features
  - remote login
  - remote execution
  - copying
- SSH versions
- Replaces telnet, rsh, rlogin
- Usage:

```
ssh <username>@<remote host>
scp <local file> <username>@<remote host>:<destination>
scp <username>@<remote host>:<destination> <local file>
```

- X11 Forwarding

Secure shell – SSH (2/2)

- SSH keys
  - Commands

    ```
    ssh-keygen -t rsa
    ssh-keygen -y
    ```

  - Files

    ```
    $HOME/.ssh/known_hosts
    $HOME/.ssh/id_rsa.pub
    $HOME/.ssh/id_rsa
    $HOME/.ssh/authorized_keys
    ```

- SFTP
- SSH tunnels
- Putty on Windows

File Transer Protocol (FTP)

- Overview of FTP
  - operation
  - transfer mode
  - anonymous ftp
- Security risks
  - plaintext passwords
  - anonymous upload
  - buffer overflow
- Server recommendations
  - vsftpd
  - detailed logging
  - anonymous only if required

Exercise 9.1 – Network Configuration

1. **Using the ipcalc tool if desired, suggest a scheme for splitting the network 10.1.1.0 into 3 subnets. List the address range for each one and the netmask and broadcast addresses.**
2. **Identify the latency between your system and a neighbour system and compare this to the latency between your system and www.google.com.**
3. **Identify the systems that a packet passes through on the way from your system to www.google.com**
4. **Using dig, check the IP address of www.example.com**
5. **Using dig, check the name for the IP address 86.43.67.77**
6. **Check if the daytime service is enabled on your system. If not, enable it and test the output from it.**

Exercise 9.2 – Network Configuration

7. **Find out what MPM the installed version of Apache is running.**
8. **Find out the location of the DocumentRoot.**
9. **Place a simple html page at this location and verify that you can view this through the webserver.**
10. **Login to a remote system using ssh.**
11. **Copy a file from your system to another system using scp.**
12. **Execute the host command on a remote system using.**
13. **Generate a key for yourself, add it to the remote system and repeat 9-11 without the use of a password.**

Backups

Backups (1/2)

- Introduction
- Backup cost versus reinstallation cost
- Frequency
  - hourly
  - daily
  - weekly
- Types
  - tape/network
  - onsite/offsite
- Media
  - tape
  - CD-R, DVD-R

Backups (2/2)

- Software
  - tar
  - kdat
  - amanda
  - bacula
- Testing of backups
- The tar command
  - `tar -c -f <tar file name> <files/directories to package>`
  - `tar -x -f <tar file name>`
  - `-v`
  - `-z and -j`

System Time

System Time

- The need for accurate time
- BIOS Time
  - localtime
  - UTC
- Timezone setting
- Network Time Protocol
  - http://www.ntp.org/
  - pool.ntp.org
  - /etc/ntp.conf
  - one server per network
  - ntpdate
- hwclock

Security

System logs

- syslogd
- /var/log
  - messages
  - syslog
  - apache/
  - ...
- Log rotation
- Reviewing
- dmesg

The sticky bit, setuid and setgid

- The sticky bit
  - chmod +t / chmod 1000
- setuid()
- The setuid bit
  - chmod u+s / chmod 4000
- setgid()
- The setgid bit
  - chmod g+s / chmod 2000
- Security implications of setuid() files with setuid bit

Password policies

- Policies
  - Disallow simple passwords
  - Require use of numbers and symbols
  - Password Encryption Method
  - Number of significant characters in password
  - Minimum Acceptable Password Length
  - Days to Password Change Warning
  - Days before Password Expires Warning
- Files
  - /etc/login.defs
  - /etc/security and /etc/pam.d
- passwd command

TCP wrappers

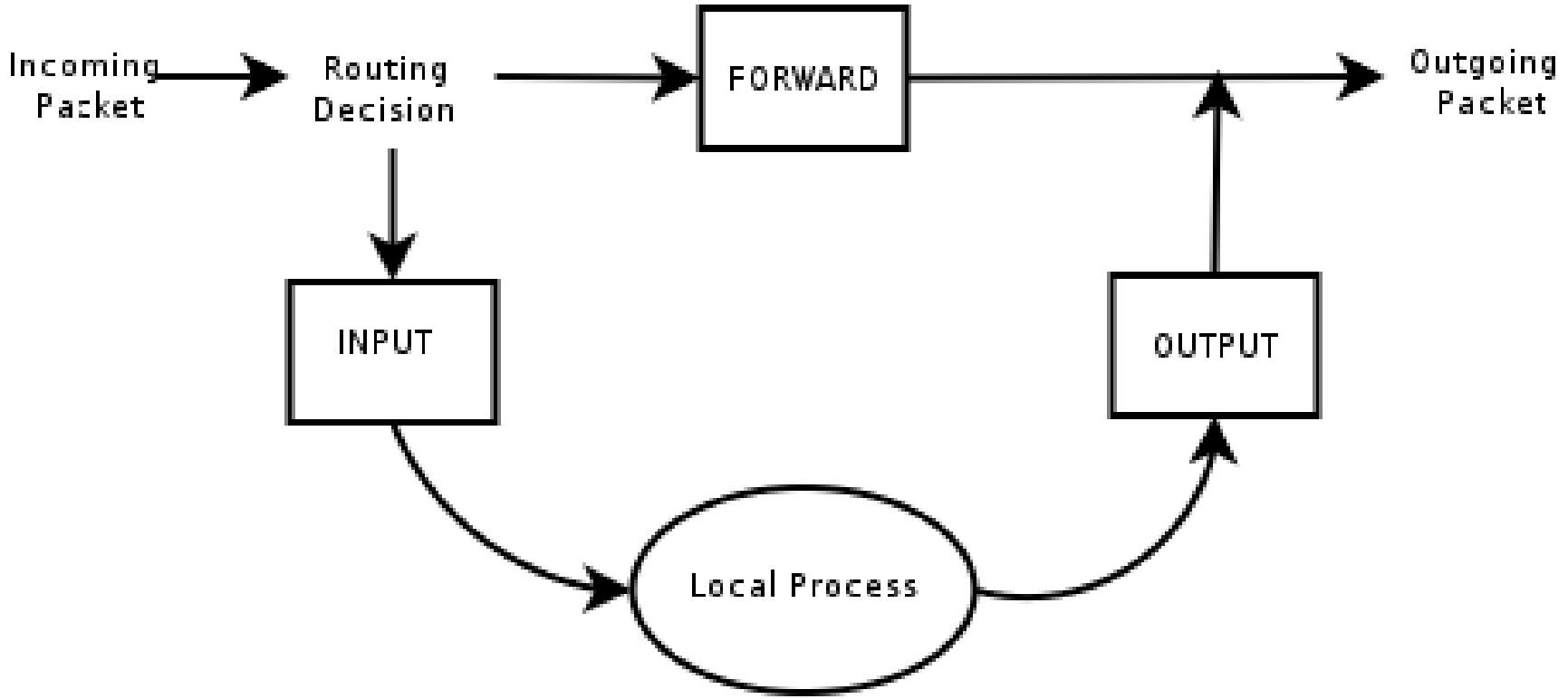
- Usage
  - inetd
  - libwrap
- Typical services
  - ssh, telnet, finger, ftp, exec, rsh, rlogin, tftp, talk, comsat
- Client request verification
- Access control
  - /etc/hosts.deny
  - /etc/hosts.allow
- Many services implement their own access control (Apache)

Firewalls - introduction

- Purpose
- Types
  - Hardware
  - Software
- Levels
  - Packet filtering
  - Stateful inspection
- Firewall design
  - Decide on a policy
  - *That which is not explicitly allowed is prohibited*
- iptables command
- NAT

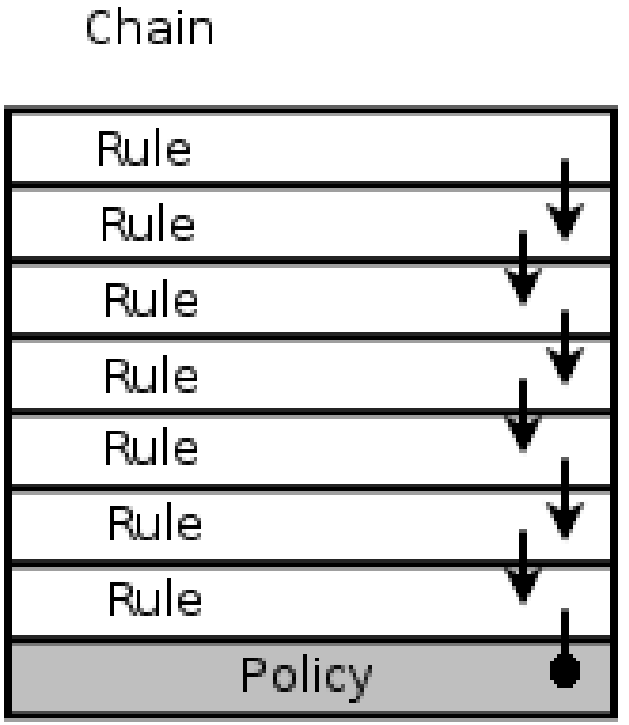
iptables - introduction

- Packets entering the kernel are passed through one of the default *firewall chains* (INPUT, OUTPUT and FORWARD)



iptables – firewall chains

- List of rules to be processed
- 3 default chains
  - INPUT
  - OUTPUT
  - FORWARD
- Each packet received by a chain is checked against the rules until a match occurs
- Each rule specifies an action to perform on a matching rule
- If no rules in a chain are matched, chain policy is applied

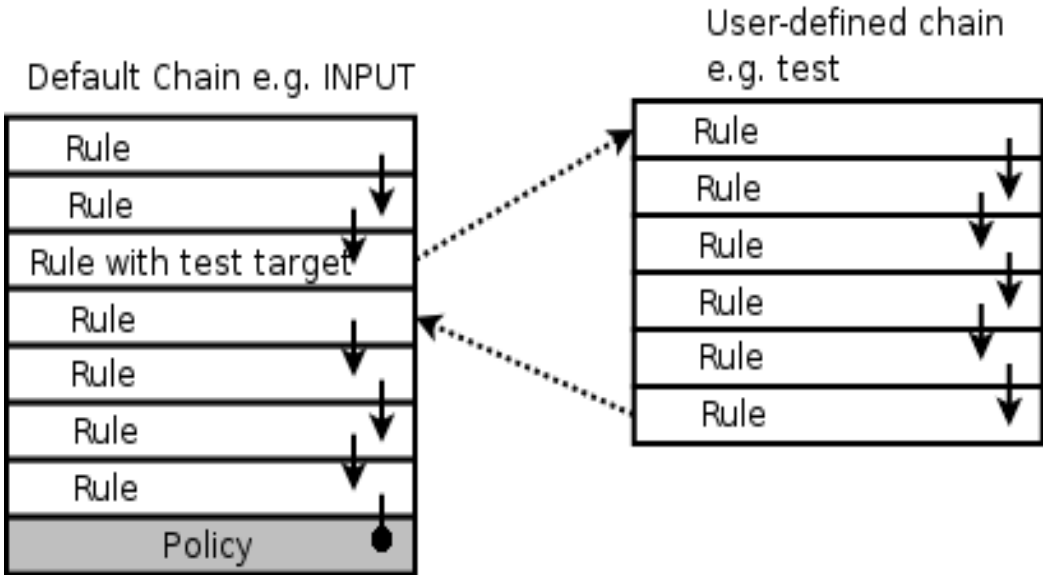


iptables – rule matches

- Matches
  - source or destination address
    - single addresses - 192.168.1.1
    - subnets - 192.168.1.0/24
  - protocol
    - udp, tcp, icmp
  - incoming or outgoing interface
    - INPUT rules should only reference incoming interface
    - OUTPUT rules should only reference outgoing interface
    - FORWARD rules can reference both
- ! for inverted rules
- + as wildcard

iptables – rule targets

- Built-in
  - ACCEPT
  - DROP
  - QUEUE
  - RETURN
- User-defined chains



iptables – extensions

- New matches
  - tcp
  - udp
  - icmp
  - mac
  - limit
  - owner
  - state (NEW, ESTABLISHED, RELATED, INVALID)
- New targets
  - LOG
  - REJECT

iptables – a simple example

```
# Insert connection-tracking modules (not needed if built into kernel).
insmod ip_conntrack
insmod ip_conntrack_ftp

# Create chain which blocks new connections, except if coming from inside.
iptables -N block
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A block -m state --state NEW -i ! eth0 -j ACCEPT
iptables -A block -j DROP

# Jump to that chain from INPUT and FORWARD chains.
iptables -A INPUT -j block
iptables -A FORWARD -j block
```

iptables – final notes

- Some alternatives
  - Yast
  - Shorewall
  - Firestarter
  - Guarddog / Watchdog / Guidedog
  - Firewall Builder
- Testing
  - nmap tool
- Resources

Pluggable Authentication Modules - PAM

- History
- Users
  - ssh
  - xdm
  - login
- Authentication schemes
  - /etc/passwd
  - smart card
  - kerberos
  - biometrics
- Linux PAM
- Other PAM implementations

Security Advisories

- General
  - CERT - http://www.cert.org/advisories/
- Distribution-specific
  - Novell - http://www.novell.com/linux/security/advisories.html
  - Debian - http://www.debian.org/security/
  - Red Hat - https://www.redhat.com/security/updates/
- SANS Top 20 - http://www.sans.org/top20/

Exercise 10.1 – Security

1. **Attempt to login to your system with an incorrect password and find if this is logged in /var/log.**
2. **Compile the code in the notes as setuid-tester.c (change NEW_UID to another valid UID on your system) and perform the following exercises with the compiled binary,**
   - **a) Run this as yourself and check the ownership of /var/tmp/setuid.tester. Explain if the setuid() succeeded and why/why not. Explain what UID and GID are associated with /var/tmp/setuid.tester and why.**
   - **b) Run this as root and check the ownership of /var/tmp/setuid.tester. Explain if the setuid() succeeded and why/why not. Explain what UID and GID are associated with /var/tmp/setuid.tester and why.**

Exercise 10.2 – Security

c) Set the setuid bit on this file and run this as yourself and check the ownership of /var/tmp/setuid.tester. Explain if the setuid() succeeded and why/why not. Explain what UID and GID are associated with /var/tmp/setuid.tester and why.

d) Set the setuid bit on this file and change the owner of the file to root and run this as yourself and check the ownership of /var/tmp/setuid.tester. Explain if the setuid() succeeded and why/why not. Explain what UID and GID are associated with /var/tmp/setuid.tester and why.

3. Change the *password policy* setting to use MD5 instead of DES.

4. Change the *days to password change* setting to 15 days.

5. Change your user account such that you must specify a new password when you next login.

Exercise 10.3 – Security

6. **Suggest a firewall policy for a small company with 3 PCs and a router connected to the internet and the local PCs; including where the firewall will run, what traffic will be allowed in and what traffic will be allowed out.**
7. **Suggest a firewall rule (in iptables syntax) to drop all traffic from 192.168.1.1.**
8. **Suggest a firewall rule (in iptables syntax) to accept all traffic from 192.168.1.2.**
9. **Suggest a firewall rule (in iptables syntax) to allow only HTTP traffic from machines in the 192.168.x.x network.**
10. **Check what known vulnerabilities exist in the version of Linux running on your system, suggest a strategy for fixing each one.**

Basic troubleshooting

Where to start troubleshooting problems on Linux

1. Check the simple things first.
2. Review any changes recently made.
3. Review known problems for that release.
4. Don't make any assumptions.
5. For remote support, verify all information.
6. Establish a baseline when the system is working.
7. The symptom of the problem may be unrelated to the cause of the problem.
8. Follow a logical sequence of steps.

Boot problems (boot disks and recovery disks, LILO failures)

- System won't boot
  1. Is there media in the drive?
  2. Was a boot-loader installed?
  3. Have drives been moved?
  4. Did the system crash/fail?
- Panic mounting /
  1. Is the correct root specified?
  2. Is the filesystem type correct?
  3. Have drives been moved?
  4. Can you see / with a rescue disk?
- Are the partition tables corrupted?

Filesystem corruption

1. What is the filesystem type?
2. How severe is the corruption?
3. Have you run fsck?
4. Is there important data on the filesystem?
5. Are there backups?
6. Advanced techniques
    - strings
    - photorec
    - dd
7. Recovery tips
    - mount read-only
    - Do not boot windows

Lost passwords

- Do you have an open root session?
- Rescue CD
  1. boot
  2. mount partition with /etc on it
  3. edit /etc/passwd and blank the password field
- Physical removal of drive
- 3rd party rescue CDs
  1. Tomsrtbt - http://www.toms.net/rb/
  2. KNOPPIX - http://www.knopper.net/knoppix/

Printing problems

1. Verify network is working.
2. Verify printer is working.
3. Verify that user has access to printer.
4. Check Windows access.

The Linux kernel

Overview

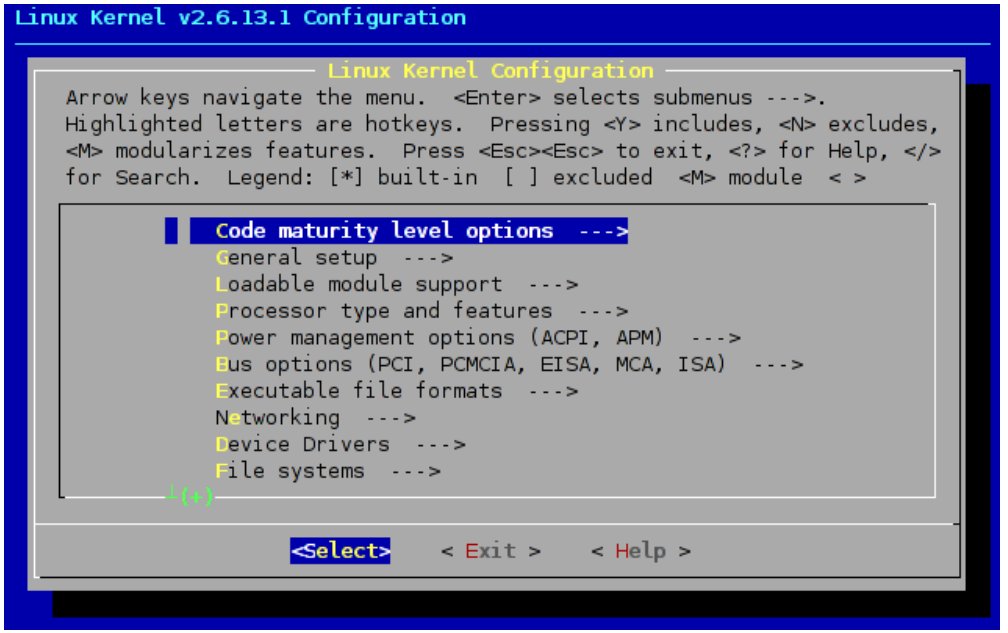
- Kernel functions
  - Interface to hardware
  - Manage processes
  - Scheduling
- Portability
- Vanilla kernels versus distribution kernels
- Versioning
  - 2.4.x
  - 2.6.x.x
- Kernel modules
- Kernel threads

Loadable kernel modules

- Purpose
  - device drivers
  - filesystem drivers
- Performance
- Commands
  - lsmod
  - insmod and rmmod
  - modprobe
  - depmod
- /lib/modules
- module versioning
- binary modules

Building custom kernels (1/2)

- http://www.kernel.org/
- `tar jxvf linux-2.6.13.1.tar.bz2`
- Software requirements
  - `Documentation/Changes`
- /usr/src
- Configuration
  - `make oldconfig`
  - `make config`
  - `make menuconfig`
  - `make xconfig`



Building custom kernels (2/2)

- Build
  - `make`
- Install loadable modules
  - `make modules_install`
  - `/lib/modules/<kernel ver>`
- Install kernel and related files
  - `cp arch/`uname -i`/bzImage /boot/vmlinuz-<kernel ver>`
  - `cp System.map /boot/System.map-<kernel ver>`
  - `cp .config /boot/config-<kernel ver>`
- Build initial ram disk
  - `mkinitrd -k vmlinux-<kernel ver> -i initrd-<kernel ver>`

    or
  - `mkinitrd /boot/initrd-<kernel ver> <kernel ver>`
- Configure boot-loader with new kernel

Kernel patches

- How patches are used
- diff
- patch
- A typical patch:

```
--- a/drivers/pci/setup-bus.c
+++ b/drivers/pci/setup-bus.c
@@ -40,7 +40,7 @@
   * FIXME: IO should be max 256 bytes.  However, since we may
   * have a P2P bridge below a cardbus bridge, we need 4K.
   */
-#define CARDBUS_IO_SIZE         (256)
+#define CARDBUS_IO_SIZE         (4*1024)
 #define CARDBUS_MEM_SIZE        (32*1024*1024)

 static void __devinit
```

Tuning the kernel

- /proc/sys
  - echo 1 > /proc/sys/net/ipv4/ip_forward
- sysctl
  - /etc/sysctl.conf
  - sysctl -A
- Subsystems
  - dev
  - fs
  - kernel
  - net
  - sunrpc
  - vm
  - net

Initial ram disk - initrd

1) The boot loader leads the kernel and the initial RAM disk specified with the initrd boot parameter.
2) The kernel copies the initial RAM disk image into memory as a normal RAM disk.
3) The kernel mounts the initial RAM disk as /
4) The kernel runs a script called /linuxrc by convention with root privileges.
5) The linuxrc script mounts the normal root file system (using
6) The linuxrc script places the root file system at the root directory using the pivot_root system call (the initrd root remains accessible)
7) The usual boot sequence (e.g. invocation of /sbin/init) is performed on the new root file system
8) The initrd file system is removed

Exercise 11 – The Kernel

1. **Download an extract a copy of the latest Linux kernel source.**
2. **Configure up the extracted kernel with some options (using your existing kernel config as a base).**
3. **Compile this kernel.**
4. **Install the kernel.**
5. **Restart your system using the new kernel.**
6. **List the modules running on the system.**
7. **Load the ntfs module into the system.**
8. **Check for any messages logged.**
9. **Remove the ntfs module from the running kernel.**

Atlantic LINUX

Scripting

Introduction

- When to use shell scripts
  - system maintenance
  - batch operations
  - easily automated repetitive tasks
- When not to use them
  - webserver scripts (CGI)
  - high security jobs
  - heavily loaded systems
- Alternatives
  - Perl
  - Python

Your first shell script

- #!/bin/sh
- Comments
- External commands
- Shell builtins
  - alias, bg, cd, echo, ...
- Shell constructs
  - if, for, while, ...
- Execute permissions

hello worlds

```
#!/bin/sh
# this is a hello world script
echo “hello world”
```

```
#!/bin/sh
# this is another hello world
# script
/bin/echo “hello world”
```

Running a script

- #!
- Running scripts through the shell command
- Debugging scripts
  - -x
  - -v

Shell variables

- Setting
- Using
- Rules for naming
- All variables of type string

Shell variables & quoting

- Single quote - '
- Double quote - "
- Back quote - `

Special Variables

- $0
- $1 - $n
- $#
- $*
- $@
- Backslash - \

Loops

- for
- while
- until

The if statement

- if
- else
- elif
- fi

case and test

- case
- test
  - STRING1 = STRING2
  - STRING1 != STRING2
  - INTEGER1 -eq INTEGER2
  - INTEGER1 -ne INTEGER2
  - -f FILE
  - ...

Exit codes,functions

- Exit status
  - checking
  - exit
  - $?
- ${VARIABLE}
- Functions
  - arguments
  - returning status

Special devices

- Useful special devices
  - /dev/null
  - /dev/zero
  - /dev/random and /dev/urandom

sed & awk

- Both perform text transformations
- Operate on standard input (from a pipeline) or files
- Can also be used to build scripts in their own right
- Come in different flavours
- Support regular expressions

sed 's/regexp/replacement text/{flags}'

e.g. sed 's/o/_/g' foo.txt

awk -F <chars> ' { print $n } ' filename

e.g. awk -F, '{print $3, $2, $1}' csv.txt

Atlantic LINUX

Exercise 12 – Scripting

1. **Write a script which, when run in a directory, renames all files in that directory to an all lowercase version of the original filename.**
2. **Write a script which takes and processes the following options. The script should display an error message when the arguments to the script are incorrect,**
   - **-h displays a help message**
   - **-l performs an ls (with each line preceded by the command name)**
   - **-d displays the date in the form "22:34 25-Dec-2004"**

In closing ...

- Summary
- Next steps
- Questionaire

Thank you and well done!