PERIODIC TASKS AND LOGS

UNIX Programming 2014 Fall by Euiseong Seo

Command Scheduling

- Scripting and automation are keys to consistency and reliability
- Some tasks of system management should be done periodically
  - Backup
  - Deletion of garbage data
  - Restarting of buggy services
- Some tasks require reservation
  - Expiring user account and remove user’s belongings after predetermined time

Daemon

- Demon?

- No, Daemon!
  - A background process (or a program for that purpose)
  - Similar to a service in Windows systems
  - Traditionally, daemon names end with letter "d"
    - httpd, sshd, ftpd and so on
- We will learn how to daemonize a process later

Cron

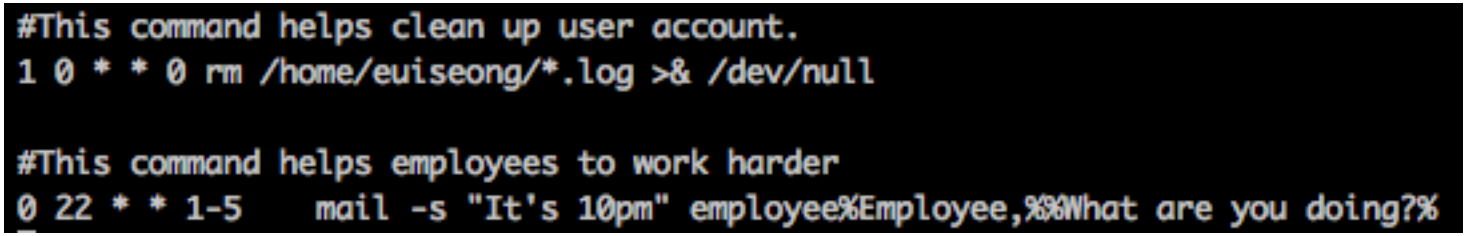
- Standard tool for running commands on a predetermined schedule
- Automatically starts when system boots
- cron configuration file - crontab
  - List of commands and their invocation times
  - cron invokes commands at the predefined times
  - Every user has his/her own crontab
  - Stored in /var/spool/cron

Crontab

- Comments line begin with a pound sign (#)
- Non comments line contain six fields
  - minute hour dom month weekday command
  - Each line represents one command
  - minute: minute of the hour (0 to 59)
  - hour: hour of the day (0 to 23)
  - dom: day of the month (1 to 31)
  - month: month of the year (1 to 12)
  - weekday: day of the week (0 to 6, 0 = Sunday)

Crontab

- Example



```
#This command helps clean up user account.
1 0 * * 0 rm /home/euiseong/*.log >& /dev/null

#This command helps employees to work harder
0 22 * * 1-5    mail -s "It's 10pm" employee%Employee,%%What are you doing?%
```

  - Note the use of the % character both to separate the comand from the input text and to martk line endings within the input
  - This is the convention for inserting new lines in crontab

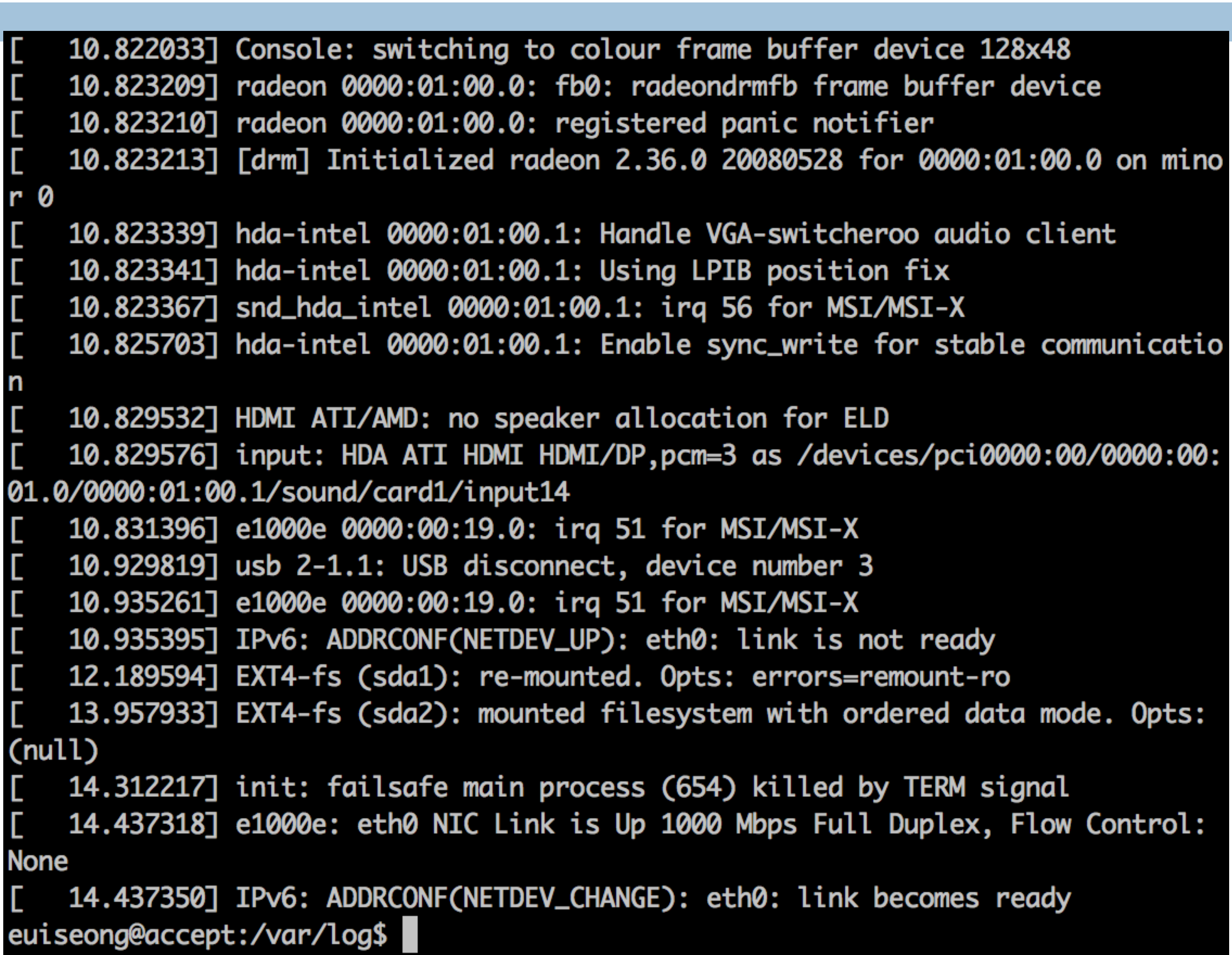
Cron Tab Management

- One user can have only one crontab
- `crontab` command manages your crontab
  - `crontab filename` installs filename as your crontab, replacing any previous version
  - `crontab -e` checks out a copy of your crontab, invokes editor on it, and then resubmits it as your crontab

Logfile and Logging

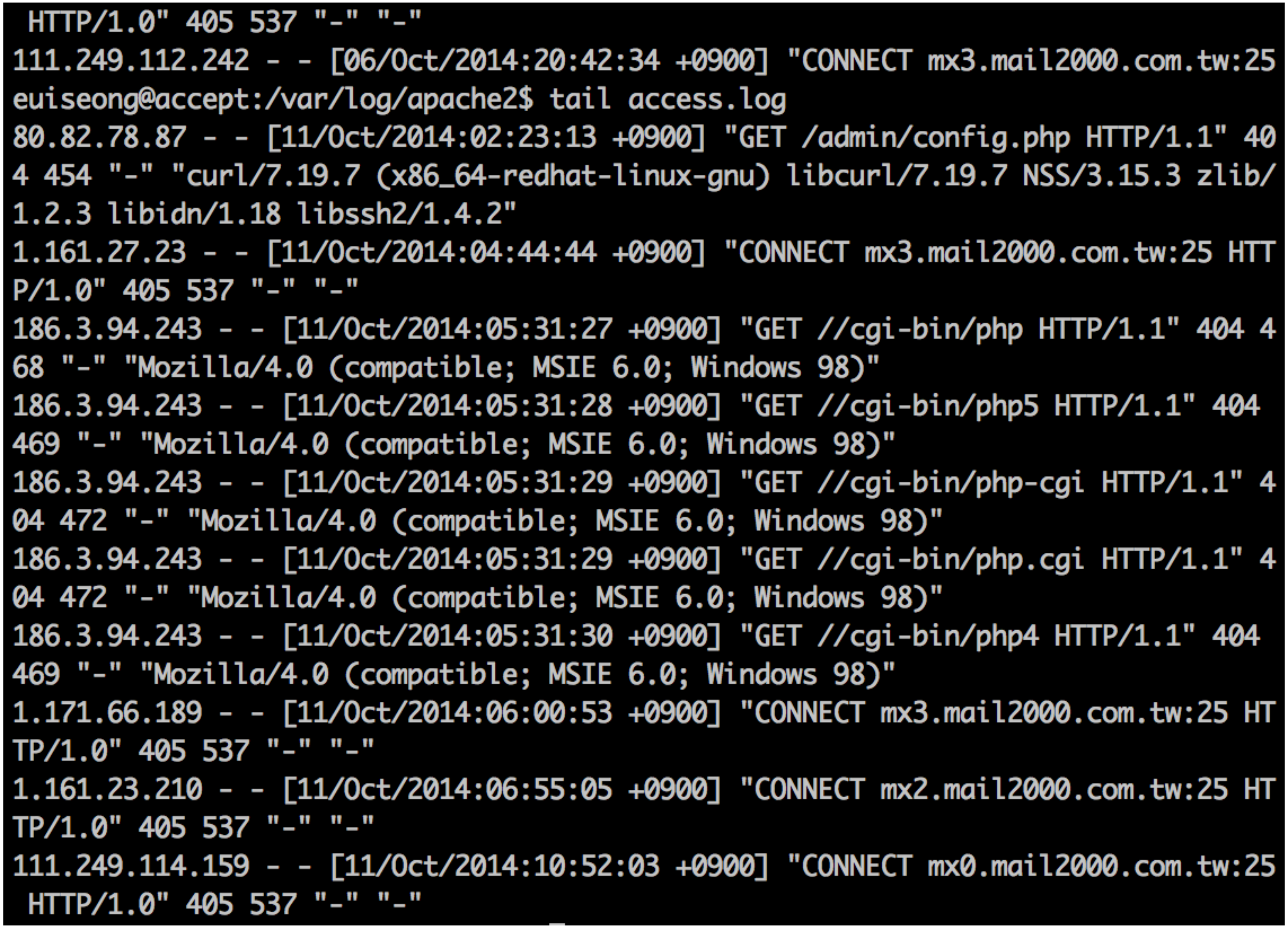
- Logfile or log
  - A file that records events of a system
- Examples
  - syslog: events of system software
  - dmesg: events of kernel
  - wtmp: events of login and logout of user accounts
- Importance of logs
  - Valuable hints for troubleshooting various problems
  - Early warning for possible system abuse
  - Critical evidence for detecting system intrusion

Example Log (dmesg for kernel)



```
[   10.822033] Console: switching to colour frame buffer device 128x48
[   10.823209] radeon 0000:01:00.0: fb0: radeondrmfb frame buffer device
[   10.823210] radeon 0000:01:00.0: registered panic notifier
[   10.823213] [drm] Initialized radeon 2.36.0 20080528 for 0000:01:00.0 on mino
r 0
[   10.823339] hda-intel 0000:01:00.1: Handle VGA-switcheroo audio client
[   10.823341] hda-intel 0000:01:00.1: Using LPIB position fix
[   10.823367] snd_hda_intel 0000:01:00.1: irq 56 for MSI/MSI-X
[   10.825703] hda-intel 0000:01:00.1: Enable sync_write for stable communicatio
n
[   10.829532] HDMI ATI/AMD: no speaker allocation for ELD
[   10.829576] input: HDA ATI HDMI HDMI/DP,pcm=3 as /devices/pci0000:00/0000:00:
01.0/0000:01:00.1/sound/card1/input14
[   10.831396] e1000e 0000:00:19.0: irq 51 for MSI/MSI-X
[   10.929819] usb 2-1.1: USB disconnect, device number 3
[   10.935261] e1000e 0000:00:19.0: irq 51 for MSI/MSI-X
[   10.935395] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[   12.189594] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro
[   13.957933] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts:
(null)
[   14.312217] init: failsafe main process (654) killed by TERM signal
[   14.437318] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control:
None
[   14.437350] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
euiseong@accept:/var/log$ █
```

Example Log (access.log from Apache)



```
 HTTP/1.0" 405 537 "-" "-"
111.249.112.242 - - [06/Oct/2014:20:42:34 +0900] "CONNECT mx3.mail2000.com.tw:25
euiseong@accept:/var/log/apache2$ tail access.log
80.82.78.87 - - [11/Oct/2014:02:23:13 +0900] "GET /admin/config.php HTTP/1.1" 40
4 454 "-" "curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3 zlib/
1.2.3 libidn/1.18 libssh2/1.4.2"
1.161.27.23 - - [11/Oct/2014:04:44:44 +0900] "CONNECT mx3.mail2000.com.tw:25 HTT
P/1.0" 405 537 "-" "-"
186.3.94.243 - - [11/Oct/2014:05:31:27 +0900] "GET //cgi-bin/php HTTP/1.1" 404 4
68 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
186.3.94.243 - - [11/Oct/2014:05:31:28 +0900] "GET //cgi-bin/php5 HTTP/1.1" 404
469 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
186.3.94.243 - - [11/Oct/2014:05:31:29 +0900] "GET //cgi-bin/php-cgi HTTP/1.1" 4
04 472 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
186.3.94.243 - - [11/Oct/2014:05:31:29 +0900] "GET //cgi-bin/php.cgi HTTP/1.1" 4
04 472 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
186.3.94.243 - - [11/Oct/2014:05:31:30 +0900] "GET //cgi-bin/php4 HTTP/1.1" 404
469 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
1.171.66.189 - - [11/Oct/2014:06:00:53 +0900] "CONNECT mx3.mail2000.com.tw:25 HT
TP/1.0" 405 537 "-" "-"
1.161.23.210 - - [11/Oct/2014:06:55:05 +0900] "CONNECT mx2.mail2000.com.tw:25 HT
TP/1.0" 405 537 "-" "-"
111.249.114.159 - - [11/Oct/2014:10:52:03 +0900] "CONNECT mx0.mail2000.com.tw:25
 HTTP/1.0" 405 537 "-" "-"
```

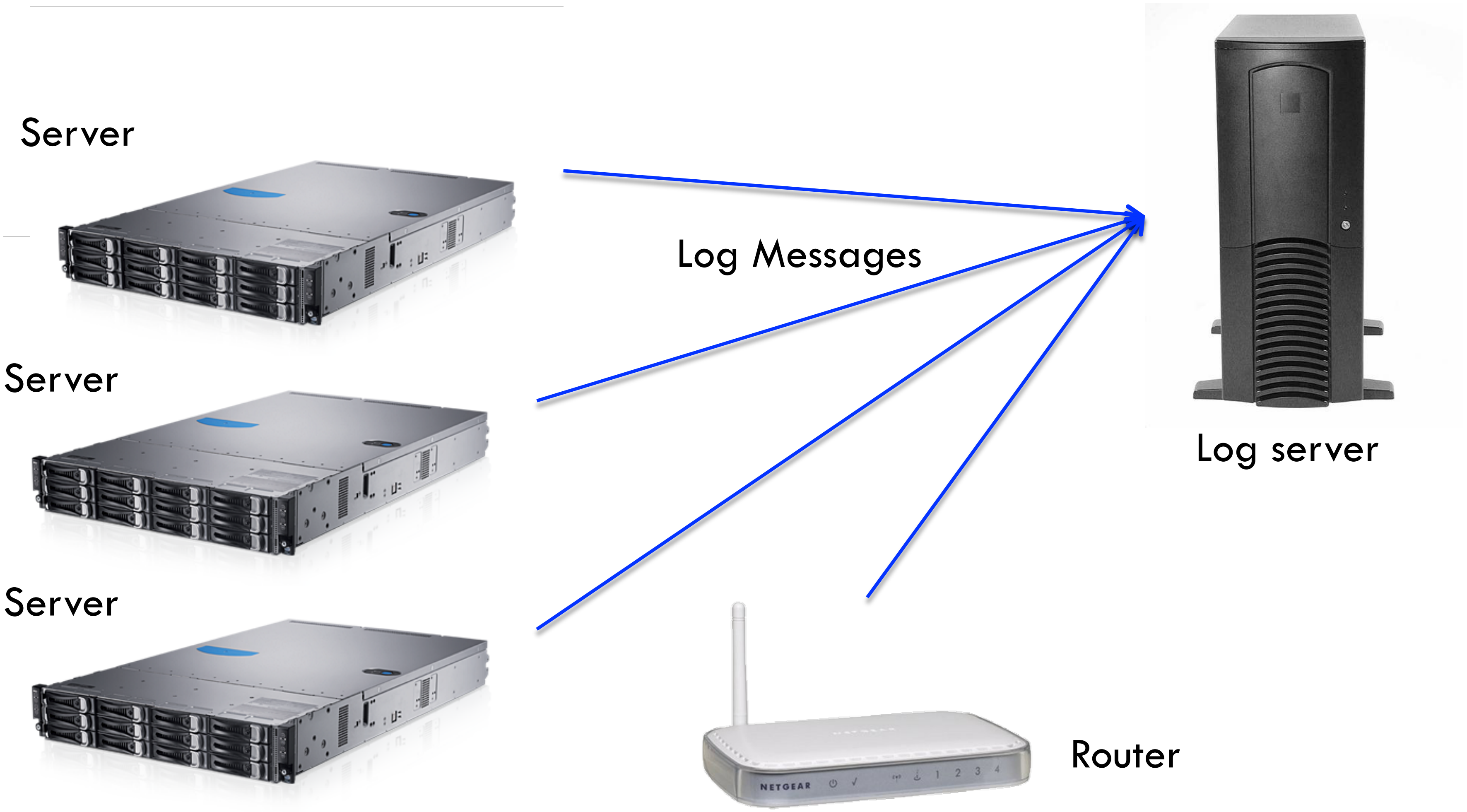
Syslog: The System Event Logger

- Comprehensive and centralized logging system
  - Liberate programmers from tedious mechanism of writing log files
  - Put administrators in control of logging
  - Enable remote logging
- Syslog consists of three parts
  - syslogd - daemon
  - openlog – library to submit messages to syslogd
  - logger – user-level command that submits log entries

Syslog Example Code

```
#include <syslog.h>

setlogmask (LOG_UPTO (LOG_NOTICE));

openlog ("exampleprog", LOG_CONS | LOG_PID | LOG_NDELAY, LOG_LOCAL1, user);

syslog (LOG_NOTICE, "Program started by User %d", getuid ());
syslog (LOG_INFO, "A tree falls in a forest");

closelog ();
```

Remote Log Server Configuration



Server

Server

Server

Log Messages

Log server

Router

Syslog Configuration

- Each line represents a rule
  - Rule = selector + action
  - Defines what to do for a selected log arrives

Syslog Configuration

- Selector
  - “Facility.priority”
    - “kern.warning”means all logs from kernel that has higher importance than warning
  - Facility: source of log
    - auth, authpriv, cron, daemon, kern, lpr, mail and so on
    - Default is user
    - Wildcard: * (*.warning)
  - Priority
    - debug, info, notice, warning, error, critical, alert and emergency
    - Wildcard: *, =, !
  - Multiple facilities with the same priority
    - kern,auth.*   kern,daemon.emergency

Syslog Configuration

- Action
  - Regular file
    - /var/adm/kernel
  - Console
    - /dev/console
  - Remote machine
    - @server_name
  - List of users
    - root, euiseong, someone
  - Everyone logged on
    - "*"
- Multple selectors for the same action
  - mail.*;mail.!=info /var/log/mail.log

Example Syslog Configuration

```
kern.*                          /var/adm/kernel
kern.crit                       @finlandia
kern.crit                       /dev/console
kern.info;kern.!err             /var/adm/kernel-info
```

Syslog Example Code

```
#include <syslog.h>

setlogmask (LOG_UPTO (LOG_NOTICE));

openlog ("exampleprog", LOG_CONS | LOG_PID | LOG_NDELAY, LOG_LOCAL1, user);

syslog (LOG_NOTICE, "Program started by User %d", getuid ());
syslog (LOG_INFO, "A tree falls in a forest");

closelog ();
```

Programming Advice

- It is highly recommended for system programmers to use syslogd to leave event logs