```
###########################
# SYSLOG NOTES
###########################
###########################
# SYSLOG STARTUP OPTIONS
###########################
```

-r flag used to accept messages from remote machines

-h flag allows syslog to send messages to a remote machine

kill –HUP `/bin/cat /var/run/syslog.pid`

```
###########################
# SYSLOG.CONF FILE
###########################
```
Syntax: selector <TAB> action
selector = facility.level
action = where to log

Facilities (Programs):
- kern
- user (default)
- mail
- daemon
- auth
- lpr
- news
- uucp
- cron
- mark
- local0-7
- syslog
- authpriv
- ftp
- * (all or any) & none

Levels (Severity):
- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

- * (all or any) & none

Actions:
- filename
- @hostname
- @ipaddress
- user1
- *
- - symbol in front of file means synchronization & buffering

Examples:
```
# Enable remote logging
*.*        @192.168.0.3
*.*        @server4.bandwidthco.com

# enable this, if you want that root is informed
*.alert                         root

# all email-messages in one file
mail.*                          /var/log/mail

# email in separate files
mail.info                       /var/log/mail.info
mail.warn                       /var/log/mail.warn
mail.err                        /var/log/mail.err

# Warnings in one file
*.=warn;*.=err                  /var/log/warn
*.crit                          /var/log/warn

# save the rest in one file
*.*;mail.none;news.none         /var/log/messages
*.*                             /var/log/allmessages
```

```
###########################
# LOGGER COMMAND
###########################
```
Syntax: logger –p facility.level –t tag message | file filename

-p option = facility and severity level
-t option = identifying tag in message
-I option = include process ID in message

Example:
logger –I –p local1.err –t FFT "Job Failed – scratch disk full"

Facilities	Facility Codes†	Priorities (in increasing order)	Priority Codes†	Actions	
auth	4	none	n/a	/some/file	*(log to specified file)*
auth-priv	10	debug	7	-/some/file	*(log to specified file but don't sync after)*
cron	9	info	6		
dæmon	3	notice	5	|/some/pipe	*(log to specified pipe)*
kern	0	warning	4	|/dev/some/tty_or_console	
lpr	6	err	3		*(log to specified console)*
mail	2	crit	2	@remote.hostname.or.IP	
mark	n/a	alert	1		*(log to specified remote host)*
news	7	emerg	0	username1, username2, etc.	
syslog	5	* *("any priority")*	n/a		*(log to all user's screens)*
user	1				
uucp	8				
local{0–7}	16–23				
* *("any facility")*	n/a				

Usage of "!" and "=" As Prefixes With Priorities

*.notice (no prefix)	= "any event with priority of 'notice' or higher"
*.!notice	= "no event with priority of 'notice' or higher"
*.=notice	= "only events with priority 'notice'"
*.!=notice	= no events with priority of 'notice'"