############################
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
-l option = include process ID in message

Example:
logger –l –p local1.err –t FFT “Job Failed – scratch disk full”

Facilities	Facility Codes†
auth	4
auth-priv	10
cron	9
daemon	3
kern	0
lpr	6
mail	2
mark	n/a
news	7
syslog	5
user	1
uucp	8
local[0–7]	16–23
* (*"any facility"*)	*n/a*

Priorities (in increasing order)	Priority Codes†
none	n/a
debug	7
info	6
notice	5
warning	4
err	3
crit	2
alert	1
emerg	0
* (*"any priority"*)	n/a

Actions

/some/file *(log to specified file)*
-/some/file *(log to specified file but don't sync after)*
|/some/pipe *(log to specified pipe)*
|/dev/some/tty_or_console *(log to specified console)*
@remote.hostname.or.IP *(log to specified remote host)*
username1, username2, etc. *(log to all user's screens)*

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'"

†Numeric codes should *not* be used in *syslog.conf* on Linux systems. They are provided here strictly as a reference. Should you need to configure a non-Linux syslog daemon which uses numeric codes only, e.g.: Cisco IOS, to send syslog messages to your log server.