1. Install syslog-ng

```
# apt-get install syslog-ng
```

2. Edit /etc/syslog-ng/syslog-ng.conf

Find the line:

```
# (this is equivalent to the "-r" syslogd flag)
# udp();
```

and change it to:

```
# (this is equivalent to the "-r" syslogd flag)
udp();
```

At the bottom of the file, add:

```
filter f_routers { facility(local5); };
log {
        source(s_all);
        filter(f_routers);
        destination(routers);
};

destination routers {
 file("/var/log/network/$YEAR/$MONTH/$DAY/$HOST-$YEAR-$MONTH-$DAY-$HOUR.log"
   owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes)
   template("$YEAR $DATE $HOST $MSG\n"));
};

destination swatch_log {
  file("/var/log/full/full.log"
    remove_if_older(518400) # overwrite if older than 6 days
  );
};
```

---

3. Create the directory /var/log/network/

```
# mkdir /var/log/network/
```

4. Restart syslog-ng:

```
# /etc/init.d/syslog-ng restart
```

5. See if messages are starting to appear under

```
/var/log/network/2008/03/XX/...
```

and

```
 /var/log/full/full.log
```

6. Install swatch

```
# apt-get install swatch
```

7. Create the configuration file /etc/swatchrc:

```
watchfor /%SYS-5-CONFIG/
     mail addresses=XXXX,subject=Configuration of router
```

   (XXXX should be the mail of your user, inst or training or ...)

8. Start swatch:

```
 # swatch -c /etc/swatchrc --daemon
```

9. Log in to your switch (using clogin from the Rancid exercise, or manually using SSH), and issue a "configure terminal" on the swich on your side of the room (10.10.1.253 or 10.10.2.253):

```
lan-sw#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
lan-sw(config)#
```

   Here just entre 'ctrl-Z' (CTRL key + 'z' key).

10. See if you are receiving mail:

```
tail /var/mail/XXXX
```