% Log Management Part 1: Using rsyslog
%
% Network Management & Monitoring

# Notes

* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.

# Exercise

The routers are able to send syslog messages to multiple destinations, so that 1 router can send messages to 4 or even 5 destinations. We therefore need to configure the router to send messages to each of the PCs in the group.

## Configure sending of syslog

Configure your virtual router to send syslog messages to every server in your group.

Everyone in your group should log into your group's router and do the following:

~~~~~~
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal

rtrX(config)# logging 10.10.Y.Y

... where X.Y is the IP of your PC (group + number).

rtrX(config)# logging facility local0
rtrX(config)# logging userinfo
rtrX(config)# exit
rtrX# write memory
~~~~~~

Now run `show logging` to see the summary of the log configuration.

The other participants in your group will be doing the same thing, so you should not be surprised if you see other destinations as well in the output of "show logging"

Logout from the router (exit):

~~~~~~
rtrX# exit
~~~~~~

That's it. The router should now be sending UDP SYSLOG packets to your PC on port 514.

To verify this log in on your PC and do the following:

~~~~~~
$ sudo bash
# tcpdump -s0 -n -i eth0 udp port 514
~~~~~~

Then have one person in your group log back in on the router and do the following:

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

You should see some output on your PC's screen from `tcpdump`. It should look something like:

```
02:20:24.942289 10.10.1.254.63515 > 10.10.1.1.514: SYSLOG local0.notice, length: 102
02:20:24.944376 10.10.1.254.53407 > 10.10.1.1.514: SYSLOG local0.notice, length: 102
```

When you have seen this, hit Ctrl-C to exit tcpdump.

(Aside: tcpdump would also show you the *content* of the syslog messages if you add `-v` to the command line)

Now you can configure the logging software on your PC to receive this information and log it to a new set of files.

## Configure rsyslog

Edit file `/etc/rsyslog.conf` and find and un-comment the following lines (that is, remove the initial '#' only)

```
#$ModLoad imudp
#$UDPServerRun 514

change to:

$ModLoad imudp
$UDPServerRun 514
```

Then change this line:

```
$PrivDropToGroup syslog

change to:

$PrivDropToGroup adm
```

Then save the file and exit.

Now, create a file named `/etc/rsyslog.d/30-routerlogs.conf` with the following lines (carefully copy and paste!)

```
$template   RouterLogs,"/var/log/network/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-%$HOUR%.log"
local0.*    -?RouterLogs
& ~
```

Save and exit, then:

~~~~~~
# mkdir /var/log/network
# chown syslog:adm /var/log/network
~~~~~~

Restart rsyslog:

~~~~~~
# service rsyslog restart
~~~~~~

## Test syslog

On your PC, See if messages are starting to appear under
`/var/log/network/<year>/<month>/<day>/`

~~~~~~
$ cd /var/log/network
$ ls
$ cd 2012
$ ls
... this will show you the directory for the month
... cd into this directory
... repeat for the next level (the day of the month)
~~~~~~

Then use 'tail' to look at the log file(s) in this directory. The names
are dynamic based on the sender and the host, so use the file that you see.
It may be something like this:

~~~~~~
$ ls
rtr8-16.log
$ tail rtr8-16.log
... logs are shown ...
~~~~~~

If not, try to login back into the router, and run some "config" commands,
then logout. e.g.

~~~~~~
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
~~~~~~

Be sure you log out of the router when you are finished. If too many people
log in without logging out then others cannot gain access to the router.

Another command to try while logged into the router, in config mode, is
to shutdown / no shutdown a Loopback interface, for example:

~~~~~~
rtrX# conf t
rtrX(config)# interface Loopback 999
rtrX(config-if) # shutdown
~~~~~~

wait a few seconds

~~~~~~
~~~~~~

```
rtrX(config-if) # no shutdown
```

Then exit, and save the config ("write mem")

Check the logs under `/var/log/network`

Still no logs?

Try the following command to send a test log message locally:

```
# logger -p local0.info "Hello World\!"
```

If a file has not been created yet under `/var/log/network`, then check your configuration for typos. Don't forget to restart the rsyslog service each time you change the configuration.

What other commands can you think of that you can run on the router (BE CAREFUL!) that will trigger syslog messages ?