Log Management

Network Startup Resource Center
www.nsrc.org

Log Management & Monitoring

- Keep your logs in a secure place
- Where they can be easily inspected
- Watch your log files
- They contain important information
  - Many things happen
  - Someone needs to review them
  - It's not practical to do this manually

Log Management & Monitoring

On your routers and switches

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console by pr on
vty0 (203.200.80.75)

%CI-3-TEMP: Overtemperature warning

Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
```

And, on your servers

```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from
169.223.1.130 port 2039 ssh2
```

Log Management

- Centralize and consolidate log files
- Send all log messages from your routers, switches and servers to a single node – a *log server*.
- All network hardware and UNIX/Linux servers can be monitored using some version of *`syslog`* (we use either `syslog-ng` or `rsyslog` for this workshop).
- Windows can, also, use syslog with extra tools.
- Save a copy of the logs locally, but, also, save them to a central log server.

Syslog Basics

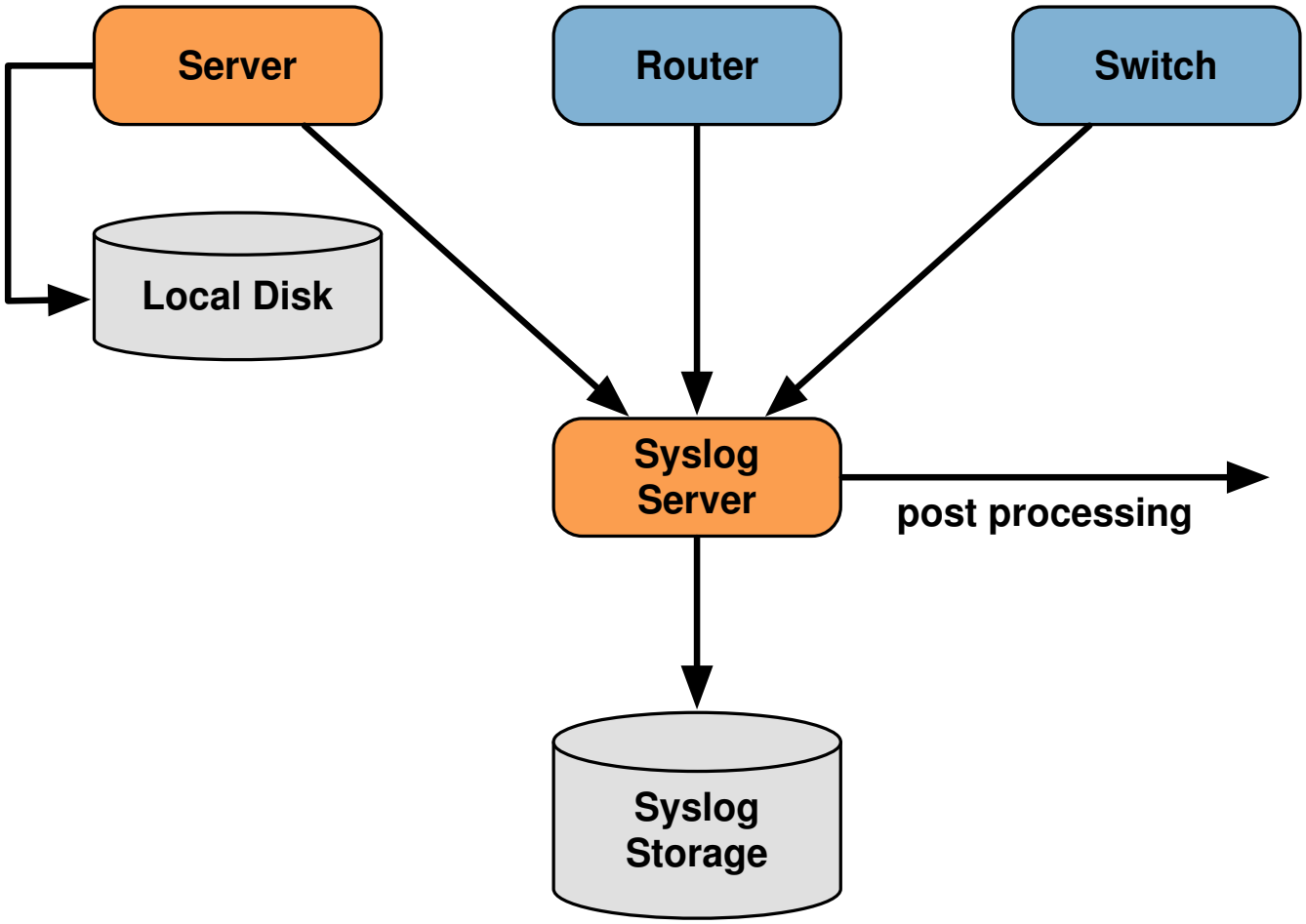
Uses UDP protocol, port 514

Syslog messages have two attributes (in addition to the message itself):

Facility			**Level**	
Auth	Security		Emergency	(0)
Authpriv	User		Alert	(1)
Console	Syslog		Critical	(2)
Cron	UUCP		Error	(3)
Daemon	Mail		Warning	(4)
Ftp	Ntp		Notice	(5)
Kern	News		Info	(6)
Lpr			Debug	(7)
Local0 ...Local7				

In addition there is a concept of ”Priority” which is a result of the combination of the facility and the level. See http://en.wikipedia.org/wiki/Syslog#Priority.

Centralized Logging



Configuring Centralized Logging

Cisco hardware

- At a minimum:

```
logging ip.of.logging.host
```

Unix and Linux nodes

- In syslogd.conf, or in rsyslog.conf, add:

```
*.*                @ip.of.log.host
```

- Restart syslogd, rsyslog or syslog-ng

Other equipment have similar options

- Options to control *facility* and *level*

Receiving Messages – syslog-ng

- Identify the *facility* that the equipment is going to use to send its messages.
- Reconfigure *syslog-ng* to listen to the network*
  - In Ubuntu update `/etc/syslog-ng/syslog-ng.conf`
- Create the following file*

  `/etc/syslog-ng/conf.d/10-network.conf`
- Create a new directory for logs:

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

- Restart the *syslog-ng* service:

```
# service syslog-ng restart
```

*See logging exercises for details

If Using rsyslog

- *rsyslog* is included by default in Ubuntu (but we prefer syslog-ng). It's a slightly different configuration – we have labs for this as well:
- Update ***/etc/rsyslog***
- Create the following file

  /etc/rsyslog.d/30-routerlogs.conf

- Create a new directory for logs and update permissions on the directory

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

- Restart the rsyslog service

```
# service rsyslog restart
```

Grouping Logs

- Using *facility* and *level* you can group by category in distinct files.
- With software such as *rsyslog* you can group by machine, date, etc. automatically in different directories.
- You can use *grep* to review logs.
- You can use typical UNIX tools to group and eliminate items that you wish to filter:

```
egrep -v '(list 100 denied|logging rate-limited)' mylogfile
```

- Is there a way to do this automatically?

Tenshi

- Simple and flexible log monitoring tool
- Messages are classified into queues, using regular expressions
- Each queue can be configured to send a summary e-mail within a time period
    - E.g. You can tell Tenshi to send you a summary of all matching messages every 5 minutes to avoid cluttering your mailbox

Sample Tenshi Configuration

```
set uid tenshi
set gid tenshi

set logfile /log/dhcp

set sleep 5
set limit 800
set pager_limit 2
set mailserver localhost
set subject tenshi report
set hidepid on

set queue dhcpd tenshi@localhost sysadmin@noc.localdomain [*/10 * * * *]

group ^dhcpd:
dhcpd ^dhcpd: .+no free leases
dhcpd ^dhcpd: .+wrong network
group_end
```

To Learn More About Syslog

- **RFC 3164:** *BSD Syslog Protocol*
  http://tools.ietf.org/html/rfc3164
- **RFC 5426:** Transmission of Syslog Messages over UDP
  http://tools.ietf.org/html/rfc5426
- Transmission of syslog messages over UDP draft-ietf-syslog-transport-udp-00
  http://tools.ietf.org/html/draft-ietf-syslog-transport-udp-00
- Wikipedia Syslog Entry
  http://tools.ietf.org/html/rfc3164
- Cisco Press: *An Overview of the Syslog Protocol*
  http://www.ciscopress.com/articles/article.asp?p=426638

References & links

Rsyslog

http://www.rsyslog.com/

SyslogNG

http://www.balabit.com/network-security/syslog-ng/

Windows Log to Syslog

http://code.google.com/p/eventlog-to-syslog/

http://www.intersectalliance.com/projects/index.html

Tenshi

http://www.inversepath.com/tenshi.html

Other software

http://sourceforge.net/projects/swatch/

http://www.crypt.gen.nz/logsurfer

http://simple-evcorr.sourceforge.net/

Questions?