Network Time Protocol (NTP)

Quick and Dirty
for AfNOG 2017

(Ayitey Bulley)

About NTP

- Network Time Protocol project
- http://ntp.org
- NTP is a protocol designed to synchronize the clocks of computers over a network.

About NTP

- NTP version 4, a significant revision of the previous NTP standard, is the current development version. It is formalized by RFCs released by the IETF.
  - RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification
  - RFC 5906: Network Time Protocol Version 4: Autokey Specification
  - RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)
  - RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6

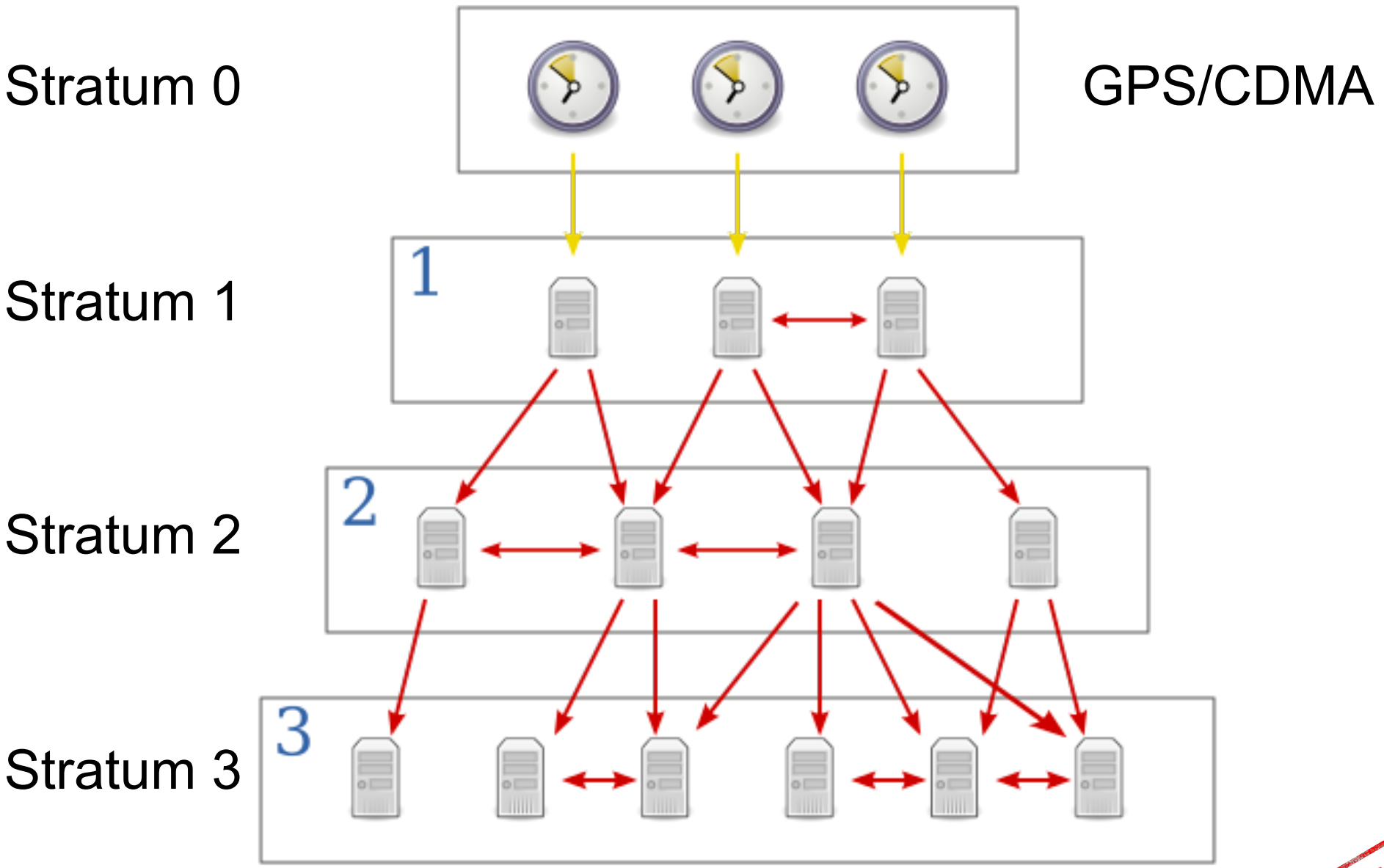
NTP and Time Synchronization

- Network Time Protocol (NTP) is used by organizations to synchronize the clocks of all its systems.
- Time synchronization is important for many reasons:
  - Application time stamps
  - Time stamps for log entries and audit trails.
- NTP provides an easy way to ensure that all systems will maintain the same time. This can significantly simplify the burden on system administrators and tech support.
- When an organization's systems all maintain different clock times, it becomes very difficult from a troubleshooting standpoint to determine when and under what conditions a particular event might be occurring.

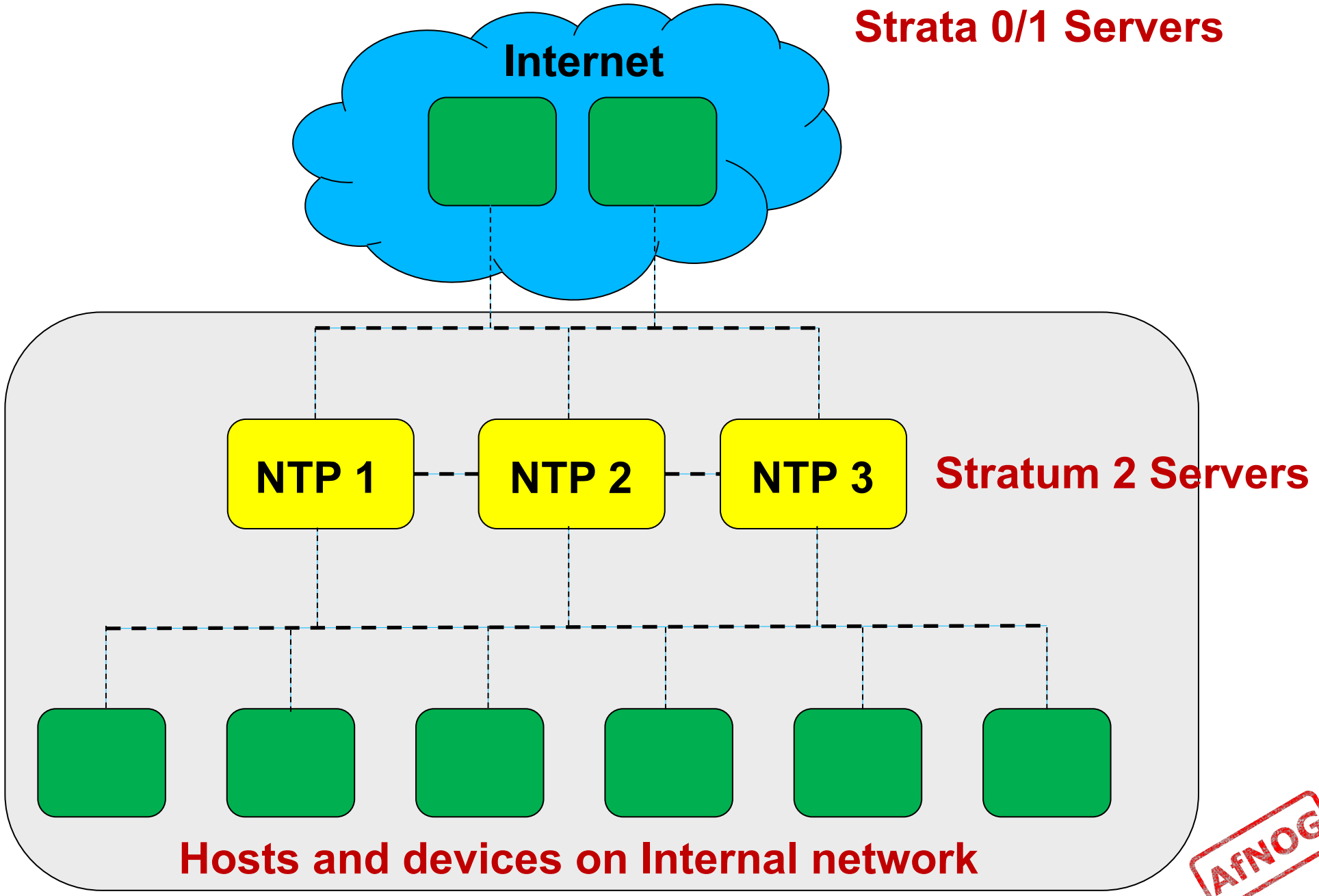
How NTP Works

- NTP works on the premise of synchronization with reference clocks, also known as ‘stratum 0‘ servers.
- All other NTP servers then become a lower level strata server based upon how far they are from a reference server.
- The start of the NTP chain is a stratum 1 server which is always directly connected to a stratum 0 reference clock.
- From here, lower level strata servers are connected via a network connection to a higher strata level server.

How NTP Works



Internal NTP Architecture



Step 1: Installation of NTP Server

- The first step to setting up an internal NTP structure is to install the NTP server software.

```
$ sudo apt-get install ntp ntpdate
```

- Check if the software is installed.

```
$ sudo dpkg --get-selections ntp
```

```
$ sudo dpkg -s ntp
```

- Update your system clock

```
$ sudo ntpdate 0.pool.ntp.org
```

Step 2: NTP Server Configuration

- Once NTP is installed, we can now configure our NTP server to synchronize with higher stratum servers.
- The configuration file for NTP is stored at '`/etc/ntp.conf`' and can be modified with any text editor.
- To start the configuration process, the higher level servers need to be configured. You can use the:
  - Debian default NTP pool servers in the configuration file.
  - ntp.org pool servers
  - List of NTP servers from NIST to specify certain servers.
  - NIST's servers in a round robin fashion (suggested method by NIST).

Step 2: NTP Server Configuration

- Debian default NTP pool servers in the configuration file.

```
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
```

- ntp.org pool servers

```
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
server 3.pool.ntp.org iburst
```

- List of NTP servers from NIST to pick specific servers.

  http://tf.nist.gov/tf-cgi/servers.cgi

Step 3: Configure NTP Restrictions

- NTP restrictions are used to allow or dis-allow hosts to interact with the NTP server.
- The default for NTP is serve time to anyone but do not allow configuration on both IPv4 and IPv6 connections.

```
# By default, exchange time with everybody, but don't
# allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquer
```

Step 3: Configure NTP Restrictions

- Now restrict who is allowed to query the server for time and what else they are allowed to do with the NTP server.

```
restrict 196.200.219.0 mask 255.255.255.0 limited kod
notrap nomodify nopeer noquery
restrict 2001:43f8:0220:219:: mask ffff:ffff:ffff:ffff::
limited kod notrap nomodify nopeer noquery
```

- We can also restrict the server from answering ntp queries

```
# By default don't answer anything
restrict default ignore
restrict -6 default ignore
```

Step 3: Configure NTP Restrictions

- Configure the server to unrestricted access to local users

```
restrict 196.200.219.0 mask 255.255.255.0 limited kod
notrap nomodify nopeer noquery
restrict 2001:43f8:0220:219:: mask
ffff:ffff:ffff:ffff:: limited kod notrap nomodify
nopeer noquery
```

- We can also restrict the server from answering ntp queries

```
# By default don't answer anything
restrict default ignore
restrict -6 default ignore
```

Step 3: Configure NTP Restrictions

- **`limited`:** Indicates that if a client should abuse the number of packets rate control, the packets will be discarded by the sever. If the Kiss of Death packet is enabled, it will be sent back to the abusive host. The rates are configurable by an admin but the defaults are assumed here.
- **`kod`:** Kiss of Death. If a host violates the limit of packets to the server, the server will respond with s KoD packet to the violating host.
- **`notrap`:** Decline mode 6 control messages. These control messages are used for remote logging programs.
- **`nomodify`:** Prevents ntpq and ntpdc queries that would modify the server's configuration but informational queries are still permitted.
- **`noquery`:** This option prevents hosts from querying the server for information. For example without this option hosts can use ntpdc or ntpq to determine where a particular time server is getting it's time from or other peer time servers that it may be communicating with.

Step 4: Starting NTP

- **Startup scripts are located at** `/etc/init.d/`
- **Take a look in startup script** `/etc/init.d/ntp`
- **Add ntp to startup i.e. ntp to start up on boot**

```
$ sudo update-rc.d ntp enable
```

- **To Run ntp**

```
$ sudo service ntp start
```

- **To Restart ntp**

```
$ sudo service ntp restart
```

Step 5: Start NTP!

- `$ sudo /etc/init.d/ntp start`
- Or
- `$ sudo service ntp start`
- Check that your server is synchronized with the ntp servers listed in /etc/ntp.conf
- `$ sudo ntpq -pn`

```
$ sudo ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*riditt.de       131.188.3.221    2 u   27   64    1  183.792    0.439   0.079
 lofn.fancube.co .INIT.          16 u    -   64    0    0.000    0.000   0.000
 service1-eth3.d 228.143.95.23    2 u   28   64    1  200.457   -1.965   0.035
 makaki.miuku.ne 218.186.3.36     2 u   28   64    1  377.207   -7.893   0.169
 noc.mtg.afnog.o 45.222.43.250    3 u   27   64    1    0.284    1.810   0.040
```

NTP Exercises