NTP (Cisco/Juniper) cloudkod.com

- Stratum is just a hop-count, less hops is better
  - A hop count of 16 means infinite
  - Default stratum is 8 when just configuring **ntp master <cr>**
- The source local address is always one stratum lower than the configured value
  - Stratum is the tie-breaker. If two servers offer the same stratum, the **prefer** keyword can be added to prefer one over the other
- NTP Peers can act as a client or a server at the same time and offer bidirectional synchronization
  - When the connection to the NTP server fails, the peer will be regarded as the new server
    The offset value is the time difference in milliseconds between the local clock and the NTP server's reference clock.
- A insane peer is unsynchronized, a sane peer is synchronized
- The offset must be < 1000 msec (1 second) in order for the NTP source/server to be considered sane
- NTP does not shift the clock instantaneously, instead the router slowly drifts towards the time
- If the offset value between the client and the server is large, this process can take a long time
- After the offset value is < 1 second off, the router will adjust its stratum from 16 (infinite) to the appropriate stratum

Time Zones

- NTP updates are always sent in UTC/GMT
- EU and US summer time dates are different.
  - Default is US, configure with **clock summer-time US recurring**
- US summer time begins second Sunday in March, ends first Sunday in November
- EU summer time begins last Sunday in March, ends last Sunday in October

NTP Broadcast and Multicast

- Default multicast address is 224.0.1.1
- Defining an interface as broadcast/multicast will stop reception of NTP unicast requests on that interface

NTP Authentication

- The client authenticates the server, it is more important to receive time from the correct source over giving time to devices
  - Giving time to specific devices is done through NTP Access Control (see below)
- Other NTP clients will still be able to request time without authentication
- You only need to configure the **ntp authenticate** command on the client

NTP Access Control

- Default behavior is allow NTP access to everyone
- Defining and applying an ACL will implicitly deny all other NTP traffic
- NTP Control messages (QUERIES) are for reading and writing internal NTP variables and status information
  - QUERIES are not used for synchronization, REQUEST and UPDATE messages are used for time synchronization

- Access-groups are applied from most permissive to most restrictive
  - Peer is most permissive, serve-only is most restrictive
  - This means that defining the same host as peer and serve-only, the client will still be able to peer
- The **serve-only** keyword allows only time requests from NTP clients
- The **peer** keyword allows bidirectional synchronization, time requests and NTP control queries from clients/peers

SNTP

As its name implies, the Simplified Network Time Protocol (SNTP) offers a reduced set of NTP functions. When a switch is configured for SNTP, it operates as an NTP client only. In other words, the switch can synchronize its clock with an NTP server, but it cannot allow other devices to synchronize from its own clock. Time synchronization is also simplified, resulting in a slightly less accurate result.

- Remote NTP Server: 10.10.10.100/24

```
# Local users may interrogate the ntp server more closely.
```

```
# vi /etc/ntp.conf
add→ restrict 10.10.10.0 mask 255.255.255.0 nomodify notrap
allow→ sudo ufw allow from any to any port 123 proto tcp (and udp)
-- On NTP Linux server, if NTP is Failing, do following;
lsof -i | grep ntp    -  kill -9 29723 <process-id>
sudo service ntp restart   -  sudo service ntp status
# ntpq -pn
   root@cloudkod:~# timedatectl status
   System clock synchronized: yes
   systemd-timesyncd.service active: yes
```

Router R1 gets NTP from NTP-Server

```
#set system time-zone America/Los_Angeles
The NTP server with the IP address of 10.10.10.100 is the preferred NTP server.
#set system ntp server 10.10.10.100 version 4 prefer
#set system ntp server 192.168.86.230 version 4

You can specify that the system time is retrieved from the NTP server when the device
boots or enters a chassis cluster backup state.
#set system ntp boot-server 10.10.10.100

In this example, the date and time are retrieved from the NTP server 10.10.10.100:
user@host> set date ntp 10.10.10.100
26 Feb 11:53:57 ntpdate[5551]: step time server 10.10.10.100 offset 0.010381 sec

SHOW> show system uptime
               ➢ show ntp status
status=c035 sync_alarm, sync_unspec, 3 events, event_clock_reset,
version="ntpd 4.2.0-a Wed Jan 28 04:37:30 UTC 2015 (1)",
processor="i386", system="JUNOS14.1R4.8", leap=11, stratum=16,
precision=-21, rootdelay=0.000, rootdispersion=0.990, peer=0,
refid=STEP, reftime=00000000.00000000  Wed, Feb  6 2036 22:28:16.000,
poll=4, clock=e2014b98.02b06277  Wed, Feb 26 2020 11:55:04.010, state=3,
offset=0.000, frequency=0.000, jitter=0.000, stability=0.000

show ntp associations no-resolve
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.10.10.100    91.189.91.157    3 -   22   64    1    0.744    0.428   0.108

------

Additional Stuff:
```

Specify the key number, authentication type (MD5), and key for authentication:

```
[edit system ntp]
trusted-key [ key-numbers ];
authentication-key key-number type type value password;

[edit system]
user@switch# set ntp authentication-key 2 type md5 value "$ABC123"
```