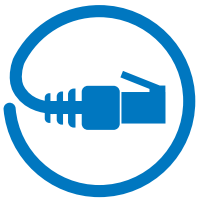
american time
Integrated Solutions

WHICH TIME SERVER OPTION IS BEST FOR SYNCHRONIZING YOUR CLOCKS?

REGARDING MASTER TIME CONTROLLERS AND IP NETWORK CLOCKS (ETHERNET OR WI-FI)



Any electronic device that automatically displays the current local time – your clocks, phone, tablet, computer and even most TVs – **has to pull that time from a time server.**

The time server acts as a messenger of sorts; it **reads the time from a reference clock** and distributes that information via a computer network to your device when the device requests it. The time server could be a **local network** time server or an **internet** time server.

SNTP, or Simple Network Time Protocol, is an internet standard protocol that **allows a clock or device to contact a server and get the current time**. It's a simplification of the more robust **NTP** (Network Time Protocol) and is used in most embedded devices and computers.

Once the device receives the current Coordinated Universal Time **(UTC)**, the device applies offsets such as **time zone or daylight saving time** considerations, as well as the time spent on the network retrieving the time, before displaying the accurate local time.

When it comes to syncing time for your organization's clocks, you have 3 options:

Let's take a look at how each of these options work, their pros and cons, and our recommendation.

Port 123 is reserved specifically for NTP/SNTP communication

1 External Server IP Address

The **NIST** – the U.S. Department of Commerce's National Institute of Standards and Technology – is the primary source for synchronizing time systems in the U.S.

Its servers can be found throughout the country and are most directly updated from the NIST atomic clocks. This makes it an **authoritative, readily available** source for synchronizing your clocks.

A list of available IP addresses can be found at **http://tf.nist.gov/tf-cgi/servers.cgi**.

The biggest concern with using an external server IP address is that any of the **addresses can go down** without warning due to large amounts of traffic, hardware failure or switching IP addresses.

Indeed, in 2017 we saw this happen when the NIST upgraded its servers and networks. The result was **new IP addresses** for some servers and the **discontinuation** of other servers.

So if you had a hard-coded connection to a server, the address may suddenly have stopped working and your **clocks weren't synching anymore** (many organizations realized this when their clocks didn't automatically update for the end of daylight saving time).

Pros

- Primary time sources from NIST
- Readily available

Cons

- Addresses may go down without warning
- External traffic for every device connecting
- Can cause problems for large organizations with thousands of devices, as the server may refuse service if queried too often from the same site

2 External Pool Server

External pool servers are like external server IP addresses, except they **link to a pool of servers** rather than to one specific server.

Although the NIST suggests using **https://nist.time.gov/** instead of linking to any one server, **some devices can only use IP addresses**.

If multiple devices contact different servers, they could be slightly off from each other and decrease synchronization by a small amount.

Pros
- Automatically handles changes to individual sites
- Readily available
- Primary time sources from NIST

Cons
- Devices read from different servers, potentially impacting synchronization accuracy
- Option not applicable to all devices
- External traffic for every device

3 Internal Server IP Address

Internal servers are accessible NTP servers that are hosted on **your organization's intranet**.

For a small facility with a couple of hundred devices or fewer, this can be as simple as enabling an NTP server on an existing local server. For large, multi-facility sites with thousands of devices, there are units built specifically to be NTP servers and can be located alongside existing servers.

By setting and controlling a static IP address, all of your devices on the network can be **set once** and will always **synchronize to the same source**. And if the NIST server source goes down, you only need to **update one device** (the server) instead of each individual device.

Pros
- All devices are synced to same source
- May be attainable with existing server
- Considerably less external traffic
- Single point if update required

Cons
- Devices synced to secondary source
- Single point of failure

Our Recommendation:

No matter the size of your organization or industry, we recommend using an **Internal Server IP Address** to maintain consistency across devices, decrease external reliance and decrease external network traffic.

The reliability, efficiency and security of an internal IP server address make it a great choice for most organizations.

140 3rd Street South • PO Box 707 • Dassel, MN 55325-0707
© 2018 AMERICAN TIME