

4978 - Setting the System Time on Dynamically from an SNTP Unicast Server on SG200, SG300, and SG500 Switches

Objective:

System time can be set manually by the user, dynamically from a Simple Network Time Protocol (SNTP) Unicast/ Multicast/Anycast server, or synchronized from the PC running the GUI. Synchronized system clocks provide a frame of reference for all devices on the network. Network time synchronization is critical to managing, securing, and debugging networks. Synchronized Time also plays an important role in shared file systems because it eliminates confusion with version differences and modification times. The switch always configures the time, time zone and GUI as part of the boot process.

The objective of this document is to show you how to configure the time settings on the SG200, SG300 and SG500 Series switches for SNTP Network Time Synchronization.

Applicable Devices:

- Cisco Small Business 200 series Managed Switches
- Cisco Small Business 300 series Managed Switches
- Cisco Small Business 500 series Managed Switches

Software Versions:

- 1.3.0.59

Setting the System Time:

Step 1. Log in to the web configuration utility. The default username is “cisco” and the default password is “cisco”.

Step 2. Navigate to **Administration > Time Settings > System Time**. The *System Time* page opens:

System Time
Dynamic Time Zone and Daylight Saving Time configurations from DHCP, if received, override manual configurations.

Actual Time (Static): 16:49:12; 2013-Mar-14;
Last Synchronized Server: Unsynchronized

Clock Source Settings

Main Clock Source (SNTP Servers): Enable
Alternate Clock Source (PC via active HTTP/HTTPS sessions): Enable

Manual Settings

Set the date and time manually, or click [here](#) to import them from your computer.

Date: 2013-Mar-14 YYYY-MM-DD
Local Time: 16:49:12 HH:MM:SS

Time Zone Settings

Get Time Zone from DHCP: Enable
Time Zone from DHCP: N/A
Time Zone Offset: UTC
Time Zone Acronym: (0/4 Characters Used)

Daylight Savings Settings

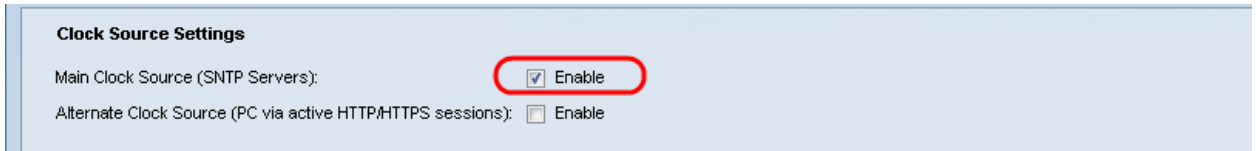
Daylight Savings: Enable
Time Set Offset: 60 min (Range: 1 - 1440, Default: 60)
Daylight Savings Type: USA European By dates Recurring

From: YYYY-MM-DD HH:MM
To: YYYY-MM-DD HH:MM
From: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
To: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM

At the top of the page the following fields are displayed:

- **Actual Time (Static)** – Displays the actual time on the device. It also displays the time zone if specified.
- **Last Synchronized Server** – Displays information from the SNTP Server including the address, stratum, and type of server. If your device does not connect to an SNTP server this field displays “Unsynchronized”.

Step 3. Under Clock Source Settings, click the Enable check box to the right of the *Main Clock Source (SNTP Servers)*.



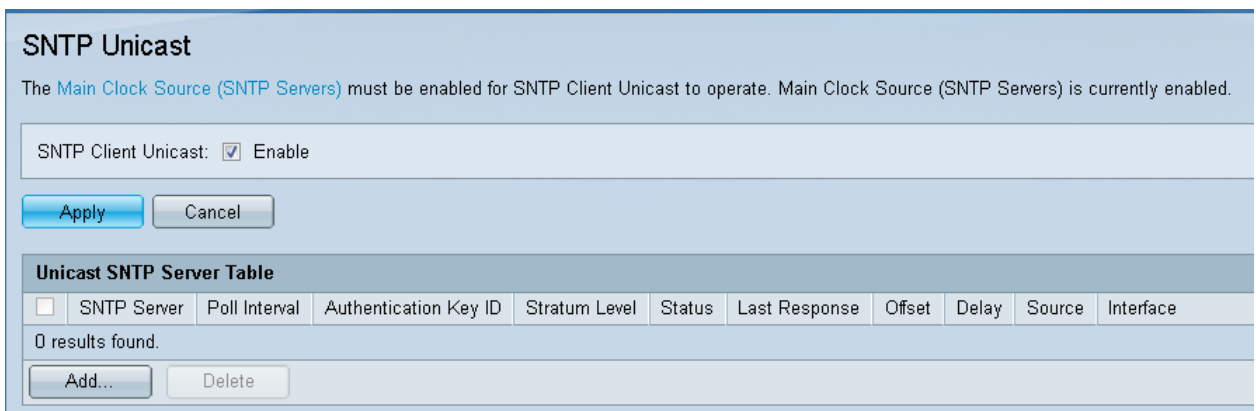
Clock Source Settings

Main Clock Source (SNTP Servers): Enable

Alternate Clock Source (PC via active HTTP/HTTPS sessions): Enable

Step 4. At the bottom of the *System Time* page to save the current settings, click **Apply**.

Step 5. Navigate to **Administration > Time Settings > SNTP Unicast**. The *SNTP Unicast* opens:



SNTP Unicast

The [Main Clock Source \(SNTP Servers\)](#) must be enabled for SNTP Client Unicast to operate. Main Clock Source (SNTP Servers) is currently enabled.

SNTP Client Unicast: Enable

Unicast SNTP Server Table

<input type="checkbox"/>	SNTP Server	Poll Interval	Authentication Key ID	Stratum Level	Status	Last Response	Offset	Delay	Source	Interface
0 results found.										

This page displays the following information for each Unicast SNTP server:

- **SNTP Server** — Specifies the SNTP server IP address, the preferred server, or the hostname that is chosen according to its stratum level.
- **Poll Interval** — Displays whether polling is enabled or disabled.
- **Authentication Key ID** — Key identification used to communicate between the SNTP server and the device.
- **Stratum Level** — Distance from the reference clock (expressed as a numerical value). An SNTP server cannot be the primary server (stratum level 1) unless polling interval is enabled.
- **Status** — SNTP server status. The possible values are:
 - **Up** — SNTP server is currently operating normally.
 - **Down** — SNTP server is currently not available.
 - **Unknown** — SNTP server is currently being searched for by the device.
 - **In Process** — Occurs when the SNTP server has not fully trusted its own time server (i.e. when first booting up the SNTP server).
- **Last Response** — Date and time of the last response received from this SNTP server.

- **Offset** — Specifies the average offset of the server's clock relative to the local clock (in milliseconds). The host determines the value of this offset using the algorithm described in RFC 2030.
- **Delay** — Average round-trip delay time of packets traveling over the network between server and local clocks (in milliseconds). The host determines the value of this delay using the algorithm described in RFC 2030.
- **Source** — How the SNTP server was defined.
- **Interface** — The interface on which packets are received.

Step 6. At the bottom of the *Unicast SNTP Server Table* field, click **Add**.



Step 7. After clicking **Add**, the *Add SNTP Server* page opens:

Step 8. In the *Server Definition* field, select **By IP address** if the SNTP server is going to be identified by its IP address, or **By name** if you are going to select a well-known SNTP server by name from the list. If **By name** is selected, skip to step 12.

Note: To specify a well-known SNTP server, the device must be connected to the Internet and be configured to use either a DNS server or DHCP to identify a DNS server (See DNS Settings).

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

* SNTP Server IP Address:

* SNTP Server:

Poll Interval: Enable

Authentication: Enable

Authentication Key ID:

Step 9. In the *IP Version* field, select the version of the IP address: Version 6 or Version 4. If Version 4 is selected, skip to step 12. Version 4 is selected by default.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

* SNTP Server IP Address:

* SNTP Server:

Poll Interval: Enable

Authentication: Enable

Authentication Key ID:

Step 10. (Optional) If you chose IPv6, select the IPv6 address type next to the *IPv6 Address Type* field. If **Global** is selected, skip to Step 12.

The screenshot shows a configuration window with the following fields and options:

- Server Definition: By IP address By name
- IP Version: Version 6 Version 4
- IPv6 Address Type: Link Local Global (This field is circled in red in the original image)
- Link Local Interface:
- * SNTP Server IP Address:
- * SNTP Server:
- Poll Interval: Enable
- Authentication: Enable
- Authentication Key ID:

At the bottom of the window are two buttons: "Apply" and "Close".

- Link Local — The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can only be used for communication on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- Global — The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

Step 11. If you chose IPv6 Address Type Link Local in step 10, select the link local interface from the list.

Server Definition: By IP address By name
IP Version: Version 6 Version 4
IPv6 Address Type: Link Local Global
Link Local Interface: VLAN 1
* SNTP Server IP Address:
* SNTP Server: time-a.timefreq.bldrdoc.gov
Poll Interval: Enable
Authentication: Enable
Authentication Key ID:

Step 12. If **By IP address** was selected in the *Server Definition* field, enter the SNTP server IP address in the *SNTP Server IP Address* field. The format depends on which address type was selected.

Server Definition: By IP address By name
IP Version: Version 6 Version 4
IPv6 Address Type: Link Local Global
Link Local Interface: VLAN 1
* SNTP Server IP Address: 192.168.1.100
* SNTP Server: time-a.timefreq.bldrdoc.gov
Poll Interval: Enable
Authentication: Enable
Authentication Key ID:

If **By Name** was selected in the *Server Definition* field, select the desired SNTP Server from the *SNTP Server* drop-down list.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface: VLAN 1

* SNTP Server IP Address: [Greyed out]

* SNTP Server: time-a.timefreq.bldrdoc.gov [Dropdown menu open with suggestions: time-a.timefreq.bldrdoc.gov, time-b.timefreq.bldrdoc.gov, time-c.timefreq.bldrdoc.gov, Other]

Poll Interval: [Greyed out]

Authentication: [Greyed out]

Authentication Key ID: [Greyed out]

Apply Close

When specifying an SNTP server, if choosing to identify it by hostname, three suggestions are given in the GUI:

- time-a.timefreq.bldrdoc.gov
- time-b.timefreq.bldrdoc.gov
- time-c.timefreq.bldrdoc.gov

Step 13. In the *Poll Interval* field, check the enable checkbox to allow polling for system time information on the SNTP server. All SNTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level (distance from the reference clock) that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the device polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

✱ SNTP Server IP Address:

✱ SNTP Server:

Poll Interval: Enable

Authentication: Enable

Authentication Key ID:

If you want to enable SNTP Authentication refer to *Enabling SNTP Authentication on SG Series Switches*

Step 14. Click **Apply** at the bottom of the current page to return to the *SNTP Unicast* page.

Server Definition: By IP address By name

IP Version: Version 6 Version 4

IPv6 Address Type: Link Local Global

Link Local Interface:

✱ SNTP Server IP Address:

✱ SNTP Server:

Poll Interval: Enable

Authentication: Enable

Authentication Key ID:

The page should show adjusted values in the *Unicast SNTP Server Table*

SNTP Unicast

The [Main Clock Source \(SNTP Servers\)](#) must be enabled for SNTP Client Unicast to operate. Main Clock Source (SNTP Servers) is currently enabled.

SNTP Client Unicast: Enable

[Apply](#) [Cancel](#)

SNTP Server	Poll Interval	Authentication Key ID	Stratum Level	Status	Last Response	Offset	Delay	Source	Interface
<input type="checkbox"/> 192.168.2.1	Enabled	0	255	Down	31.12.1899 0:0:0	0	0	Static	

[Add...](#) [Delete](#)

Step 15. In the *SNTP Client Unicast* field, click the **Enable** check box.

SNTP Client Unicast: Enable

[Apply](#) [Cancel](#)

Step 16. Click **Apply**.

The [Main Clock Source \(SNTP Servers\)](#) must be enabled for SNTP Client Unicast to operate. Main Clock Source (SNTP Servers) is currently enabled.

SNTP Client Unicast: Enable

[Apply](#) [Cancel](#)

Unicast SNTP Server Table

Step 17. From here, you can click **Save** located at the top right corner of the page, or the **Copy/Save Configuration** page link.

Small Business

SG300-20 20-Port Gigabit Managed Switch

[Save](#) [Cisco](#) Language: English

System Summary

- Interface
- Etherlike
- GVRP
- 802.1x: EAP
- TCAM Utilization
- RMON
- View Log
- Administration
- System Settings
- Console Settings
- Management Interfaces

SNTP Unicast

Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

The [Main Clock Source \(SNTP Servers\)](#) must be enabled for SNTP Client Unicast to operate. Main Clock Source (SNTP Servers) is currently enabled.

SNTP Client Unicast: Enable

[Apply](#) [Cancel](#)

Step 18. Save the running configuration into the startup configuration by choosing the **Running Configuration** in the *Source File Name* field and the **Startup Configuration** option in the *Destination File Name* field.

Copy/Save Configuration

All configurations that the switch is currently using are in the running configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source File Name: Running configuration
 Startup configuration
 Backup configuration
 Mirror configuration

Destination File Name: Running configuration
 Startup configuration
 Backup configuration

Sensitive Data: Exclude
 Encrypted
 Plaintext
Available sensitive data options are determined by the current user's SSD rules

Save Icon Blinking: Disabled

Step 19. At the bottom of the *Copy/Save Configuration* page click **Apply** to save the configuration settings.

Copy/Save Configuration

All configurations that the switch is currently using are in the running configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source File Name: Running configuration
 Startup configuration
 Backup configuration
 Mirror configuration

Destination File Name: Running configuration
 Startup configuration
 Backup configuration

Sensitive Data: Exclude
 Encrypted
 Plaintext
Available sensitive data options are determined by the current user's SSD rules

Save Icon Blinking: Disabled