CHAPTER 1

Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About NTP

This section includes the following topics:

NTP Overview

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. With the User Datagram Protocol (UDP) as its transport protocol, NTP uses standard Universal Time Coordinated (UTC).

An NTP server usually receives its time from a source such as a radio clock or an atomic clock attached to a time server and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as an atomic clock).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 NTP server.

Before synchronizing, NTP compares the time reported by several network devices and does not synchronize with one that is significantly different, even if it is a stratum 1.

Because the Cisco CG-OS software cannot connect to a radio or atomic clock and act as a stratum 1 server, Cisco recommends that you use the public NTP servers available on the Internet.

When the network is isolated from the Internet, the Cisco CG-OS software allows you to configure the time as though it were synchronized through NTP, even though it was not.

When the Cisco CG-OS router loses connectivity with the NTP server, the Cisco CG-OS router uses the latest synchronized time it received from the NTP server.

To use the local clock for the Cisco CG-OS router, you will need to delete the NTP client configuration using the **no** form of the commands (see Configuring an NTP Client, page 1-4).

Stateless Restarts

The Cisco CG-OS router supports stateless restarts for NTP. After a system reboot, the Cisco CG-OS software applies the running configuration to the Cisco CG-OS router.

Prerequisites for NTP

Router must have connectivity to at least one server that is running NTP.

NTP must be configured in the default VDC of the Cisco CG-OS router. No other VDCs are supported on the Cisco CG-OS router.

Guidelines and Limitations

The Cisco CG-OS router supports an NTP client and receives its clock source from an NTP server.

When you have only one NTP server, configure all the devices as clients to that NTP server.

You can configure up to 64 NTP servers.

Default Settings

Table 1-1 lists the default settings for NTP parameters.

Table 1-1 Default NTP Parameters

Parameters	Default
NTP protocol	Enabled
NTP authentication	Disabled

Table 1-1 Default NTP Parameters (continued)

Parameters	Default
NTP access	Enabled
NTP logging	Disabled

Configuring NTP

This section includes the following topics:

- Enabling or Disabling the NTP Protocol, page 1-3
- Configuring an NTP Client, page 1-4
- Configuring NTP Authentication, page 1-5
- Configuring NTP Access Restrictions, page 1-7
- Configuring NTP Logging, page 1-7
- Discarding NTP Configuration Changes, page 1-8

Enabling or Disabling the NTP Protocol

You can enable or disable NTP on the Cisco CG-OS router. NTP is enabled by default.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	[**no**] **ntp enable**	Enables or disables the NTP protocol on the Cisco CG-OS router. NTP is enabled by default.
Step 3	**show ntp status**	(Optional) Displays the status of the NTP application.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration

EXAMPLE

This example shows how to disable NTP on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no ntp enable
router(config)# copy running-config startup-config
```

Configuring an NTP Client

This section addresses how to configure the Cisco CG-OS router to serve as an NTP client.

BEFORE YOU BEGIN

Identify the IP address or DNS name for each NTP server that you want to define as a possible clocking reference for the Cisco CG-OS router.

When defining multiple NTP servers, determine which server will serve as the primary (preferred) NTP server.

Ensure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**[no] ntp server** {*ip-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**]	Defines the NTP server that provides the clocking source for the Cisco CG-OS router. You can specify multiple server associations. **key–**Configures a key to use while communicating with the NTP server. The range for the *key-id* argument is from 1 to 65535. **Note**: Only configure the key when you want the NTP server to provide authentication for the Cisco CG-OS router. **maxpoll, minpoll**–Configures the maximum and minimum intervals in which to poll a server. The range for the *max-poll* and *min-poll* arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively. **prefer**–Assigns the NTP server as the preferred NTP server for the Cisco CG-OS router. **Note**: When you configure a key for use in communicating with the NTP server, be sure that the key exists as a trusted key on the Cisco CG-OS router. For more information on trusted keys, see Configuring NTP Authentication, page 1-5.
Step 3	**[no] ntp source-interface [ethernet | cellular | wimax]** *slot/port*	Configures the interface that connects to the NTP server.
Step 4	**[no] ntp source** *ip-address*	Configures the source IP address for the source-interface that will receive all NTP packets. The *ip-address* must be in IPv4 format.

	Command	Purpose
Step 5	**exit**	Exits to the global configuration mode.
Step 6	**show ntp statistics** {**io** | **local** | **memory** | **peer** {**ipaddr** *ipv4-addr* | **name** *peer-name*}}	(Optional) Displays the configured NTP servers. Enter the NTP server name for the *peer-name* variable.
Step 7	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure an IPv4 client and assign the NTP server as the preferred clocking reference; and, define the cellular interface as the path to the NTP server.

```
router# configure terminal
router(config)# ntp server 192.0.2.12 prefer
router(config)# ntp server 192.0.2.10 key 42
router(config)# ntp source-interface cellular 3/1
router(config-if)# exit
router# copy running-config startup-config
```

Configuring NTP Authentication

You can configure the Cisco CG-OS router to authenticate the time sources to which the local clock synchronizes. When you enable NTP authentication, the Cisco CG-OS router synchronizes to a time source only if the source carries one of the authentication keys specified by the **ntp trusted-key** command. The Cisco CG-OS router drops any packets that fail the authentication check and prevents them from updating the local clock.

By default, NTP authentication is disabled on the Cisco CG-OS router.

BEFORE YOU BEGIN

Configure the NTP server(s) with the authentication keys configured on the Cisco CG-OS router in this procedure.

Ensure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp authenticate**	Enables the NTP authentication feature. By default, NTP authentication is disabled on the Cisco CG-OS router.

	Command	Purpose
Step 3	**ntp authentication-key number md5** *md5-string*	Defines the authentication key. This key must match the value on the NTP server along with the **ntp trusted-key** *number* value of the Cisco CG-OS router in Step 4 below. The Cisco CG-OS router does not synchronize to the NTP server clocking source unless the **ntp authentication-key** and the **ntp trusted-key** values on the server and the Cisco CG-OS router match. The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters.
Step 4	**ntp trusted-key** *number*	Specifies one or more keys (defined in Step 3) that a time source (NTP server) must provide in its NTP packets in order for the Cisco CG-OS router to synchronize to it. The range for trusted keys is from 1 to 65535. This command provides protection against accidentally synchronizing the Cisco CG-OS router to a time source (NTP server) that is not trusted.
Step 5	**show ntp authentication-keys**	(Optional) Displays the configured NTP authentication keys.
Step 6	**show ntp trusted-keys**	(Optional) Displays the configured NTP trusted keys.
Step 7	**show ntp authentication-status**	(Optional) Displays the status of NTP authentication.
Step 8	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to synchronize only to NTP servers that provide authentication key 42 and authentication key 35 in their NTP packets.

```
router# configure terminal
router(config)# ntp authentication-key 42 md5 aNiceKey
router(config)# ntp trusted-key 42
router(config)# ntp authentication-key 35 md5 aBetterKey
router(config)# ntp trusted-key 35
router(config)# ntp authenticate
router(config)# copy running-config startup-config
router(config)#
```

Configuring NTP Access Restrictions

You can control access to NTP services by using access groups. Specifically, you can specify the types of requests that the Cisco CG-OS router allows and the servers from which it accepts responses.

When you do not configure any access groups, NTP access is granted to all devices. When you configure any access groups, NTP access is granted only to the remote device whose source IP address passes the access list criteria.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp access-group peer** *access-list-name*	Creates an access group to control NTP access and applies a basic IP access list. The **peer** keyword allows time requests and NTP control queries and allows the Cisco CG-OS router to synchronize only to a remote device whose IP address passes the access list criteria. The **no** form of this command removes the access group.
Step 3	**show ntp access-groups**	(Optional) Displays the NTP access group configuration.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to allow it to synchronize to a NTP server from access group, accesslist1.

```
router# configure terminal
router(config)# ntp access-group peer accesslist1
router(config)# copy running-config startup-config
router(config)#
```

Configuring NTP Logging

You can configure the Cisco CG-OS router to generate significant NTP events to the system log on the Cisco CG-OS router. NTP logging is disabled by default.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp logging**	Enables logging of significant NTP events to the system log on the Cisco CG-OS router. By default, NTP logging is disabled on the Cisco CG-OS router.
Step 3	**show ntp logging-status**	(Optional) Displays the NTP logging configuration status.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable NTP logging in order to log significant NTP events to the system log on the Cisco CG-OS router.

```
router# configure terminal
router(config)# ntp logging
router(config)# copy running-config startup-config
```

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes instead of committing them. When you discard the changes, the Cisco CG-OS software removes the pending (starting configuration) database changes.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

To discard NTP configuration changes, enter the following command in global configuration mode.

Command	Purpose
ntp abort	Discards the NTP configuration changes in the pending database. Enter this command on the Cisco CG-OS router in which you started the NTP configuration.

Verifying Configuration

To display the NTP configuration, enter any or all of the following commands.

Command	Purpose
show ntp access-groups	Displays the NTP access group configuration.
show ntp authentication-keys	Displays the configured NTP authentication keys.
show ntp authentication-status	Displays the status of NTP authentication.
show ntp internal	Displays internal NTP information.
show ntp logging-status	Displays the NTP logging status.
show ntp peer-status	Displays the status for all NTP servers.
show ntp peers	Displays all the NTP servers.
show ntp source	Displays the configured NTP source IP address.
show ntp source-interface	Displays the configured NTP source interface.
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** *ipv4-addr* | **name** *peer-name*}}	Displays the NTP statistics. Enter the NTP server name for the *peer-name* variable.
show ntp trusted-keys	Displays the configured NTP trusted keys.
show running-config ntp	Displays date and timestamp of last running configuration update.

Enter the **clear ntp session** command to clear the NTP sessions.

Enter the **clear ntp statistics** command to clear the NTP statistics.

Configuration Example

This example shows how to configure an NTP client, enable NTP authentication, enable NTP logging, and then save the configuration in the startup configuration file so that it is saved across reboots and restarts.

```
router# configure terminal
router(config)# ntp server 192.0.2.12 prefer
router(config)# ntp server 192.0.2.10 key 42
router(config)# ntp source-interface cellular 3/1
router(config-if)# exit
router(config)# ntp authenticate
router(config)# ntp authentication-key 42 md5 aNiceKey
router(config)# ntp trusted-key 42
router(config)# ntp logging
router(config)# copy running-config startup-config
```

Feature History

Table 1-2

Feature Name	Release	Feature Information
Network Time Protocol	Cisco CG-OS Release CG1(1)	Initial support of the feature on the CGR 1000 Series Routers.