Configuring Network Time Protocol

Information About Network Time Protocol

Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients. With this synchronization, you can correlate events to the time that system logs were created and the time that other time-specific events occur. An NTP server must be accessible by the client switch.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock that is attached to a time server. NTP 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 one another.

NTP uses a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server has a radio or atomic clock that is directly attached, a stratum 2 time server receives its time from a stratum 1 time server, and so on. A machine running NTP automatically chooses as its time source the machine with the lowest stratum number that it is configured to communicate with through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP has two ways to avoid synchronizing to a machine whose time might be ambiguous:

- NTP never synchronizes to a machine that is not synchronized itself.
- NTP compares the time that is reported by several machines and does not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

The communications between machines running NTP, known as associations, are usually statically configured; each machine is given the IP addresses of all machines with which it should form associations. An associated pair of machines can keep accurate timekeeping by exchanging NTP messages between each other. However, in a LAN environment, you can configure NTP to use IP broadcast messages. With this alternative, you can configure the machine to send or receive broadcast messages, but the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

NTP Work Mode

NTP supports 4 working modes for clock synchronization:

- Client Mode:

  In this mode, the OLT device or client sends regularly time-of day requests to a configured NTP server

- Peer Mode:

  In this mode, an NTP-configured device establishes an association with another peer device and synchronizes the time with each other.

- Broadcast Mode:

  In this mode, the NTP server sends the time information to all connected clients in the same subnet as the server.

- Multicast Mode:

  In this mode, the NTP server and clients have multicast configured and the NTP server sends the time information to only multcast-configured clients

How to Configure NTP

The following sections provide configurational information about NTP.

Enabling NTP

To enable or disable NTP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. [**no**] **ntp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**] **ntp** **Example:**	Enables NTP. Use the **no** form of this command to disable NTP.

	Command or Action	Purpose
	`Device(config)# ntp`	

Configuring Reference Clocks

The device only supports local reference clock configurations. These configurations are generally only used for testing, and the purpose is to enable the device to perform synchronization testing as a server without other clock servers.

To configure reference clocks, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp reference-clock local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp reference-clock local** **Example:** `Device(config)# ntp reference-clock local`	Configures the local clock as reference clock. Use the **no** form of the command to remove the local clock as reference clock.

Configuring Client Mode

To configure client mode, perform the following steps:

Before you begin

- The NTP server can only be used as a time server to synchronize other devices after its own clock is synchronized.
- When the server is in an unsynchronized state or the clock level is greater than or equal to the client's clock level, it will not respond to the client's request.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ntp unicast server** *ip_address* [**authentication-keyid** *key_id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp unicast server** *ip_address* [**authentication-keyid** *key_id*] **Example:** `Device(config)# ntp unicast server 192.168.0.11`	Configures synchronization to an NTP server. Use the **no** form of the command to disable the NTP server on the device.

Configuring Peer Mode

To configure synchronization to an NTP-configured peer device, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp unicast peer** *ip_address* [**authentication-keyid** *key_id*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp unicast peer** *ip_address* [**authentication-keyid** *key_id*] **Example:** `Device(config)# ntp unicast peer 192.168.0.10`	Configures synchronization to an NTP-configured peer device. Use the **no** form of the command to remove synchronization to an NTP-configured peer device.

Configuring Broadcast Mode

In this mode, you need to enable the **ntp broadcast** command on the interface connecting the NTP server and the client device.

To configure broadcast mode, perform the following steps:

Before you begin

The NTP server clock must be synchronized before it can be used as a time server to synchronize client devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp broadcast server** [**authentication-keyid** *key_id*]
5. **exit**
6. **interface vlan-interface** *vlan-id*
7. **ntp broadcast client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp broadcast server** [**authentication-keyid** *key_id*] **Example:** `Device(config-if-vlaninterface-1)# ntp broadcast server`	Enables NTP broadcast on the NTP server.
Step 5	**exit** **Example:** `Device(config-if-vlaninterface-1)# exit`	Enters global configuration mode.
Step 6	**interface vlan-interface** *vlan-id* **Example:**	Creates a VLAN interface and enter interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface vlan-interface 1`	
Step 7	**ntp broadcast client** **Example:** `Device(config-if-vlaninterface-1)# ntp broadcast client`	Enables NTP broadcast on the client device.

Configuring Multicast Mode

In this mode, you need to enable the **ntp multicast** command on the interface connecting the NTP server and the client device.

To configure multicast mode, perform the following steps:

Before you begin

The NTP server clock must be synchronized before it can be used as a time server to synchronize client devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp multicast server** [**authentication-keyid** *key_id*]
5. **exit**
6. **ntp multicast client**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp multicast server** [**authentication-keyid** *key_id*] **Example:**	Emables NTP multicast on the NTP server.

	Command or Action	Purpose
	`Device(config-if-vlaninterface-1)# ntp multicast server`	
Step 5	**exit** **Example:** `Device(config-if-vlaninterface-1)# exit`	Enters global configuration mode.
Step 6	**ntp multicast client** **Example:** `Device(config-if-vlaninterface-1)# ntp multicast client`	Emables NTP multicast on the client device.

Configuring Access Control

Through the access control configurations, you can specify the device's processing actions on the corresponding packets.

The supported actions are as follows:

- permit: Allow the continued processing of packets
- deny: Discard packets

You can configure multiple ACCESS control lists (ACLs). The lists are arranged in priority according to the maximum IP address and then the maximum mask. Packets are matched in sequence, and the first matching action shall prevail.

To configure access control for NTP services, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp access** *ip_address subnet_mask* {**permit** | **deny**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp access** *ip_address subnet_mask* {**permit** | **deny**} **Example:**	Configures access control for NTP.

	Command or Action	Purpose
	`Device(config)# ntp access 192.168.0.10 255.255.255.0 permit`	Use the **no** form of the command to disable access control for NTP.

Configuring Authentication

To configure authentication, perform the following steps:

Before you begin

- The authentication will only take effect after the authentication is enabled.
- In addition to these authentication configurations, the mode configuration needs to specify which key to use in the corresponding command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authentication**
4. **ntp authentication-keyid** *key_id* **md5** *string_value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp authentication** **Example:** `Device(config)# ntp authentication`	Enables NTP authentication. Use the **no** form of the command to disable authentication.
Step 4	**ntp authentication-keyid** *key_id* **md5** *string_value* **Example:** `Device(config)# ntp authentication-keyid 2 md5 cisco`	Configures the NTP authentication key. • *key_id* : The key ID. The value must be in the range of 1 to 65535. • *string_value*: The string value. The value must be alphanumeric and in the range of 1 to 64. Use the **no** form of the command to disable authentication key.

Disabling Incoming Packets

To disable incoming packets, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan-interface** *vlan-id*
4. **ntp disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**interface vlan-interface** *vlan-id* **Example:** `Device(config)# interface vlan-interface 1`	Creates a VLAN interface and enter interface configuration mode.
Step 4	**ntp disable** **Example:** `Device(config-if-vlaninterface-1)# ntp disable`	Disables incoming packets.

Configuring Maximum Number of Dynamic Sessions

If the number of dynamic sessions exceeds this number, new dynamic sessions will not be created.

To configure maximum number of dynamic sessions, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp max-dynamic-sessions** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device#configure terminal`	Enters global configuration mode.
Step 3	**ntp max-dynamic-sessions** *value* **Example:** `Device(config)# ntp max-dynamic-sessions 20`	Configures the maximum number of dynamic sessions. The value must be in the range of 11 to 100. Use the **no** form of the command to remove the configured maximum number of dynamic sessions.

Monitoring NTP

Use the following commands to monitor NTP.

Table 1: Commands to Monitor NTP

Command	Purpose
show ntp reference-clock	Displays the reference clock configurations.
show ntp unicast server	Displays the unicast server configurations
show ntp unicast peer	Displays the unicast peer configurations.
show ntp broadcast server	Displays the broadcast server configurations
show ntp multicast server	Displays the multicast server configurations
show ntp access	Displays the access configurations.
show ntp authentication	Displays the authentication configurations.
show ntp disable	Displays the disable configurations.
show ntp max-dynamic-sessions	Displays the configured maximum number of dynamic sessions.
show ntp status	Displays the NTP status.
show ntp sessions	Displays the NTP session details.

Example: Enabling Authentication and Configuring Broadcast Mode

The following example shows how to enable authentication and broadcast mode on an NTP server:

```
Device> enable
Device# configure terminal
Device(config)# interface vlan-interface 1
Device(config-if-vlanInterface-1)# ntp broadcast server
```

The following example shows how to enable authentication and broadcast mode on a client device:

```
Device> enable
Device# configure terminal
Device(config)# ntp
Device(config)# ntp authentication
Device(config)# ntp authentication-keyid 1 md5 123ABC
Device(config)# interface vlan-interface 1
Device(config-if-vlanInterface-1)# ntp broadcast client
```