NTP の設定

この章では、Cisco NX-OS デバイスで ネットワーク タイム プロトコル（NTP）を設定する方法について説明します。

この章は、次の項で構成されています。

NTP について

この項では、次のトピックについて取り上げます。

NTP の概要

ネットワーク タイム プロトコル（NTP）は、分散している一連のタイム サーバとクライアント間で 1 日の時間を同期させ、複数のネットワーク デバイスから受信するシステム ログや時間関連のイベントを相互に関連付けられるようにします。NTP ではトランスポート プロトコルとして、ユーザ データグラム プロトコル（UDP）を使用します。すべての NTP 通信は UTC を使用します。

NTP サーバは通常、タイム サーバに接続されたラジオ クロックまたは原子時計などの正規の時刻源から時刻を受信し、次にネットワークを介してこの時刻を配信します。NTP はきわめて効率的で、毎分 1 パケット以下で 2 台のマシンを相互に 1 ミリ秒以内に同期します。

NTP では層（stratum）を使用して、ネットワーク デバイスと正規の時刻源の距離を表します。

- ストラタム 1 のタイム サーバは、正規の時刻源（無線、原子時計、または GPS 時刻源など）に直接接続されます。
- ストラタム 2 NTP サーバは、ストラタム 1 タイム サーバから NTP を使用して時刻を受信します。

同期の前に、NTP は複数のネットワーク サービスが報告した時刻を比較し、1 つの時刻が著しく異なる場合は、それが Stratum 1 であっても、同期しません。Cisco NX-OS は、ラジオクロックまたはアトミック クロックに接続できず、Stratum 1 サーバとして動作することはできないため、インターネット上で利用できるパブリック NTP サーバを使用することを推奨します。ネットワークがインターネットから切り離されている場合、Cisco NX-OS では、NTP によって時刻が同期されていなくても、NTP で同期されているものとして時刻を設定できます。

（注） NTP ピア関係を作成して、サーバで障害が発生した場合に、ネットワーク デバイスを同期させて、正確な時刻を維持するための時刻提供ホストを指定できます。

デバイス上の時刻は重要な情報であるため、NTP のセキュリティ機能を使用して、不正な時刻を誤って（または悪意を持って）設定できないように保護することを強く推奨します。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

NTP アソシエーション

N TP アソシエーションは、次のいずれかになります。

- ピア アソシエーション：デバイスが別のデバイスに同期するか、別のデバイスをそのデバイスに同期させることができます。
- サーバ アソシエーション：デバイスは、サーバに同期します。

設定する必要があるのはアソシエーションの片側だけです。他方のデバイスは自動的にアソシエーションを確立できます。

タイム サーバとしての NTP

Cisco NX-OS デバイスでは、時刻を配信するために NTP を使用できます。他のデバイスは、これをタイム サーバとして設定できます。また、正規の NTP サーバとして機能するデバイスを設定して、外部の時刻源と同期されていない場合でも時間を配布するようにできます。

クロック マネージャ

クロックは、異なるプロセス間で共有する必要のあるリソースです。NTP などの複数の時刻同期プロトコルが、システムで稼働している可能性があります。

クロック マネージャを使用して、システム内のさまざまなクロックを制御するプロトコルを指定できます。いったんプロトコルを指定すると、システム クロックの更新が始まります。クロック マネージャの設定の詳細については、『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。

ハイ アベイラビリティ

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

仮想化のサポート

NTP は Virtual Routing and Forwarding（VRF）インスタンスを認識します。NTP サーバおよび NTP ピアに対して特定の VRF を設定していない場合、NTP はデフォルトの VRF を使用します。VRF の詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

NTP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	NTP にはライセンスは不要です。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS のライセンス スキームの詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

NTP の前提条件

NTP の前提条件は、次のとおりです。

- NTP を設定するには、NTP が動作している 1 つ以上のサーバに接続できなければなりません。

注意事項と制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- NTP サーバ機能はサポートされます。
- 別のデバイスとの間にピア アソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限られます。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、いくつかのデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピア アソシエーションを設定すると、信頼性の高い NTP 構成になります。
- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。
- 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。
- VRF で NTP を設定する場合は、NTP サーバおよびピアが、設定された VRF を介して相互にアクセスできることを確認します。

- ネットワーク全体の NTP サーバおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信する必要があります。

デフォルト設定値

表 2-1 に、NTP パラメータのデフォルト設定を示します。

表 2-1　デフォルトの NTP パラメータ

パラメータ	デフォルト
NTP	イネーブル
NTP 認証	ディセーブル
NTP アクセス	イネーブル
NTP access group match all	ディセーブル
NTP ロギング	ディセーブル

NTP の設定

この項では、次のトピックについて取り上げます。

- 「NTP のイネーブル化/ディセーブル化」（P.2-4）
- 「正規の NTP サーバとしてのデバイスの設定」（P.2-5）
- 「NTP サーバおよびピアの設定」（P.2-6）
- 「NTP 認証の設定」（P.2-9）
- 「NTP アクセス制限の設定」（P.2-10）
- 「NTP ソース IP アドレスの設定」（P.2-12）
- 「NTP ソース インターフェイスの設定」（P.2-12）
- 「NTP ロギングの設定」（P.2-12）

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

NTP のイネーブル化/ディセーブル化

NTP をイネーブルまたはディセーブルにできます。NTP はデフォルトでイネーブルです。

手順の概要

1. **configure terminal**
2. **[no] feature ntp**
3. （任意）**show ntp status**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **feature ntp** **Example:** switch(config)# feature ntp	NTP をイネーブルまたはディセーブルにします。 NTP はデフォルトでイネーブルです。
ステップ 3	**show** ntp **status** **Example:** switch(config)# show ntp status Distribution: Enabled Last operational state: Fabric Locked	（任意）NTP アプリケーションのステータスを表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTP をディセーブルにする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no feature ntp
```

正規の NTP サーバとしてのデバイスの設定

正規の NTP サーバとして機能するデバイスを設定して、既存のタイム サーバと同期されていない場合でも時間を配布するようにできます。

手順の概要

1. **configure terminal**
2. [**no**] **ntp master** [*stratum*]
3. （任意）**show running-config ntp**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp master** [*stratum*] **Example:** switch(config)# ntp master	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントが時刻を同期する別のストラタム レベルを指定できます。範囲は 1 ～ 15 です。
ステップ 3	**show running-config** ntp **Example:** switch(config)# show running-config ntp	（任意）NTP の設定を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、別のストラタム レベルを使用する正規の NTP サーバとして Cisco NX-OS デバイスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp master 5
```

NTP サーバおよびピアの設定

NTP サーバおよびピアを設定できます。

はじめる前に

使用している NTP サーバと、そのピアの IP アドレスまたはドメイン ネーム システム（DNS）名がわかっていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
3. [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
4. （任意）**show ntp peers**
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] **Example:** switch(config)# ntp server 192.0.2.10	1 つのサーバと 1 つのサーバ アソシエーションを形成します。 NTP サーバとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 ピアをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 16 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 このサーバをデバイスの優先 NTP サーバにするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するよう NTP サーバを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数として、**default**、**management**、または大文字と小文字を区別した 32 文字までの任意の文字列を使用できます。 **（注）** NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。信頼できるキーの詳細については、「NTP 認証の設定」（P.2-9）を参照してください。

	コマンド	目的
ステップ 3	[**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] **Example:** `switch(config)# ntp peer 2001:0db8::4101`	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。 NPT ピアとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 ピアをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 17 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 このピアをデバイスの優先 NTP ピアにするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するよう NTP ピアを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数として、**default**、**management**、または大文字と小文字を区別した 32 文字までの任意の文字列を使用できます。
ステップ 4	**show ntp peers** **Example:** `switch(config)# show ntp peers`	（任意）設定済みのサーバおよびピアを表示します。 **（注）**　ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。
ステップ 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTP をイネーブルにして、同期応答の送信とアソシエーションの形成を実行し、NTP サーバおよびピアを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 192.0.2.10 key 10 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 prefer use-vrf Red
switch(config)# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  2001:0db8::4101                Peer (configured)
  192.0.2.10                    Server (configured)
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP 認証の設定

ローカル ロックを同期させる時刻源を認証するようデバイスを設定できます。NTP 認証をイネーブルにすると、**ntp trusted-key** コマンドによって指定されたいずれかの認証キーを時刻源が保持している場合のみ、デバイスはその時刻源と同期します。デバイスは、認証チェックに失敗したすべてのパケットをドロップし、それらのパケットでローカル クロックがアップデートされないようにします。NTP 認証はデフォルトでディセーブルになっています。

はじめる前に

この手順で指定する予定の認証キーによって、NTP サーバが設定されていることを確認します。詳細については、「NTP サーバおよびピアの設定」（P.2-6）を参照してください。

手順の概要

1. **configure terminal**
2. [**no**] **ntp authentication-key** *number* **md5** *md5-string*
3. （任意）**show ntp authentication-keys**
4. [**no**] **ntp trusted-key** *number*
5. （任意）**show ntp trusted-keys**
6. [**no**] **ntp authenticate**
7. （任意）**show ntp authentication-status**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	Example:
	`switch# config terminal`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ntp authentication-key** *number* **md5** *md5-string* `switch(config)# ntp authentication-key 42 md5 aNiceKey`	認証キーを定義します。デバイスが時刻源と同期するのは、時刻源がこれらの認証キーのいずれかを持ち、**ntp trusted-key** *number* コマンドによってキー番号が指定されている場合だけです。 認証キーの範囲は 1 ～ 65535 です。MD5 文字列の場合は、最大 8 文字の英数字を指定できます。 認証キーの範囲は 1 ～ 65535 で、MD5 文字列は最大 15 文字の英数字です。
ステップ 3	**show ntp authentication-keys** **Example:** `switch(config)# show ntp authentication-keys`	（任意）設定済みの NPT 認証キーを表示します。

	コマンド	目的
ステップ 4	[no] **ntp trusted-key** *number* **Example:** switch(config)# ntp trusted-key 42	1 つ以上のキー（ステップ 2 で定義されているもの）を指定します。デバイスが時刻源と同期するために、時刻源はこのキーを NTP パケット内に提供する必要があります。信頼できるキーの範囲は 1 ～ 65535 です。 このコマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。
ステップ 5	**show ntp trusted-keys** **Example:** switch(config)# show ntp trusted-keys	（任意）設定済みの NTP の信頼されているキーを表示します。
ステップ 6	[no] **ntp authenticate** **Example:** switch(config)# ntp authenticate	NTP 認証機能をイネーブルまたはディセーブルにします。NTP 認証はデフォルトでディセーブルになっています。
ステップ 7	**show ntp authentication-status** **Example:** switch(config)# show ntp authentication-status	（任意）NTP 認証の状況を表示します。
ステップ 8	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTP パケット内で認証キー 42 を提示している時刻源とだけ同期するようデバイスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP アクセス制限の設定

アクセス グループを使用して、NTP サービスへのアクセスを制御できます。具体的には、デバイスを許可する要求のタイプ、およびデバイスが応答を受け取るサーバを指定できます。

アクセス グループを設定しない場合は、すべてのデバイスに NTP アクセス権が付与されます。何らかのアクセス グループを設定した場合は、ソース IP アドレスがアクセス リストの基準をパスしたリモート デバイスに対してだけ、NTP アクセス権が付与されます。

手順の概要

1. **configure terminal**
2. [**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name*
3. （任意）**show ntp access-groups**

4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name* **Example:** switch(config)# ntp access-group peer accesslist1	NTP のアクセスを制御し、基本の IP アクセス リストを適用するためのアクセス グループを作成または削除します。 NTP がピアに設定されている拒否 ACL ルールに一致した場合、ACL の処理は停止し、次のアクセス グループ オプションに継続されません。 • **peer** キーワードは、デバイスが時刻要求と NTP 制御クエリーを受信し、アクセス リストに指定されているサーバと同期できるようにします。 • **serve** キーワードは、デバイスがアクセス リストに指定されているサーバからの時刻要求と NTP 制御クエリーを受信できるようにしますが、指定されたサーバと同期できるようにはしません。 • **serve-only** キーワードは、アクセス リストで指定されたサーバからの時刻要求のみをデバイスが受信できるようにします。 • **query-only** キーワードは、アクセス リストで指定されたサーバからの NTP 制御クエリーのみをデバイスが受信できるようにします。
ステップ 3	**show ntp access-groups** **Example:** switch(config)# show ntp access-groups	（任意）NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、アクセス グループ「accesslist1」からピアと同期できるようデバイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ntp access-group peer accesslist1
switch(config)# show ntp access-groups
Access List        Type
----------------------------
accesslist1        Peer
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP ソース IP アドレスの設定

NTP は、NTP パケットが送信されたインターフェイスのアドレスに基づいて、すべての NTP パケットにソース IP アドレスを設定します。特定のソース IP アドレスを使用するよう NTP を設定できます。

NTP ソース IP アドレスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
[**no**] **ntp source** *ip-address* **Example:** switch(config)# ntp source 192.0.2.1	すべての NTP パケットにソース IP アドレスを設定します。*ip-address* には IPv4 または IPv6 形式を使用できます。

NTP ソース インターフェイスの設定

特定のインターフェイスを使用するよう NTP を設定できます。

NTP ソース インターフェイスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
[**no**] **ntp source-interface** *interface* **Example:** switch(config)# ntp source-interface ethernet 2/1	すべての NTP パケットに対してソースインターフェイスを設定します。**?** キーワードを使用します。

NTP ロギングの設定

重要な NTP イベントでシステム ログを生成するよう、NTP ロギングを設定できます。NTP ロギングはデフォルトでディセーブルになっています。

手順の概要

1. **configure terminal**
2. **[no] ntp logging**
3. （任意）**show ntp logging-status**

4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **Example:** switch# configure terminal Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp logging** **Example:** switch(config)# ntp logging	重要な NTP イベントでシステム ログを生成することをイネーブルまたはディセーブルにします。NTP ロギングはデフォルトでディセーブルになっています。
ステップ 3	**show ntp logging-status** **Example:** switch(config)# show ntp logging-status	（任意）NTP ロギングのコンフィギュレーション状況を表示します。
ステップ 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、重要な NTP イベントによってシステム ログを生成するよう、NTP ロギングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP の設定確認

NTP の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ntp access-groups	NTP アクセス グループのコンフィギュレーションを表示します。
show ntp authentication-keys	設定済みの NTP 認証キーを表示します。
show ntp authentication-status	NTP 認証の状況を表示します。
show ntp internal	内部の NTP 情報を表示します。
show ntp logging-status	NTP のロギング状況を表示します。
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。
show ntp peers	すべての NTP ピアを表示します。

コマンド	目的
show ntp rts-update	RTS アップデートの状況を表示します。
show ntp source	設定済みの NTP ソース IP アドレスを表示します。
show ntp source-interface	設定済みの NTP ソース インターフェイスを表示します。
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}	NTP 統計情報を表示します。
show ntp trusted-keys	設定済みの NTP の信頼されているキーを表示します。
show running-config ntp	NTP 情報を表示します。

NTP セッションをクリアするには、**clear ntp session** コマンドを使用します。

NTP 統計情報を消去するには、**clear ntp statistics** コマンドを使用します。

NTP の設定例

次に、NTP サーバおよびピアを設定し、NTP 認証をイネーブルにして、NTP ロギングをイネーブルにした後で、その設定をスタートアップに保存し、リブートとリスタートを通して保存されるようにする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  2001:db8::4101                Peer (configured)
  192.0.2.105                   Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----------------------------
 Auth key         MD5 String
-----------------------------
  42             aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

以下に、次の制限のある NTP アクセス グループの設定例を示します。

- peer の制限事項は、「peer-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve の制限事項は、「serve-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve-only の制限事項は、「serve-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- query-only の制限事項は、「query-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。

```
switch# configure terminal
switch(config)# ntp peer 10.1.1.1
switch(config)# ntp peer 10.2.2.2
switch(config)# ntp peer 10.3.3.3
switch(config)# ntp peer 10.4.4.4
switch(config)# ntp peer 10.5.5.5
switch(config)# ntp peer 10.6.6.6
switch(config)# ntp peer 10.7.7.7
switch(config)# ntp peer 10.8.8.8
switch(config)# ntp access-group peer peer-acl
switch(config)# ntp access-group serve serve-acl
switch(config)# ntp access-group serve-only serve-only-acl
switch(config)# ntp access-group query-only query-only-acl

switch(config)# ip access-list peer-acl
switch(config-acl)# 10 permit ip host 10.1.1.1 any
switch(config-acl)# 20 permit ip host 10.8.8.8 any

switch(config)# ip access-list serve-acl
switch(config-acl)# 10 permit ip host 10.4.4.4 any
switch(config-acl)# 20 permit ip host 10.5.5.5 any

switch(config)# ip access-list serve-only-acl
switch(config-acl)# 10 permit ip host 10.6.6.6 any
switch(config-acl)# 20 permit ip host 10.7.7.7 any

switch(config)# ip access-list query-only-acl
switch(config-acl)# 10 permit ip host 10.2.2.2 any
switch(config-acl)# 20 permit ip host 10.3.3.3 any
```

その他の関連資料

NTP の実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.2-15）
- 「MIB」（P.2-16）

関連資料

関連項目	マニュアル タイトル
Clock Manager	『*Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*』

MIB

MIB	MIB のリンク
NTP に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html