NTP の設定

この章は、次の項で構成されています。

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 クロックやアトミック クロックなどの正規の時刻源から時刻を受信し、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 ではストラタム（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、信頼できる時刻源に直接接続されます（無線時計や原子時計または GPS 時刻源など）。

- ストラタム 2 の NTP サーバは、ストラタム 1 のタイム 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、無線時計や原子時計に接続できず、ストラタム 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。

タイム サーバーとしての NTP

他のデバイスからタイム サーバとして設定できます。デバイスを正規の NTP サーバとして動作するよう設定し、外部の時刻源と同期していないときでも時刻を配信させることもできます。

CFS を使用した NTP の配信

Cisco Fabric Services（CFS）は、ローカル NTP コンフィギュレーションをネットワーク内のすべてのシスコ デバイスに配信します。

デバイス上で CFS をイネーブルにすると、NTP コンフィギュレーションが起動された場合には常に、ネットワーク全体のロックが NTP に適用されます。NTP コンフィギュレーションを変更した後で、これらの変更を破棄することもコミットすることもできます。

いずれの場合でも、CFS のロックはこのときに NTP アプリケーションから解放されます。

クロック マネージャ

クロックはさまざまなプロセス間で共有する必要のあるリソースです。

NTP や高精度時間プロトコル（PTP）といった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。

高可用性

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。

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。

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。

NTP の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。

- **show ntp session status** CLI コマンドには、最後のアクションのタイムスタンプ、最後のアクション、最後のアクションの結果、および最後のアクションの失敗理由は表示されません。
- NTP サーバー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 サーバー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、サーバー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。
- サーバーが 1 台だけの場合は、すべてのデバイスをそのサーバー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（サーバーおよびピア）は、最大 64 です。

- NTP に対して CFS がディセーブルになっていると、その NTP からコンフィギュレーションは配信されず、ネットワーク内の他のデバイスからの配信も受け入れません。
- NTP に対して CFS 配信をイネーブルにしても、**commit** コマンドを入力するまで、NTP コンフィギュレーション コマンドのエントリは NTP コンフィギュレーションに対してネットワークをロックします。ロック中は、ネットワーク内の（ロックを保持しているデバイス以外の）すべてのデバイスは NTP コンフィギュレーションを変更できません。
- CFS を使用して NTP をディセーブルにする場合、ネットワーク内のすべてのデバイスは、NTP に対して使用するよう設定したものと同じ VRF を持っている必要があります。
- VRF で NTP を設定する場合は、NTP サーバーおよびピアが、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 サーバーおよび 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。
- スイッチをエッジ デバイスとして使用して NTP を利用したい場合は、**ntp access-group** コマンドを使用して必要なエッジ デバイスにのみ NTP をフィルタリングすることを推奨します。
- システムに **ntp passive**、**ntp broadcast client**、または **ntp multicast client** コマンドが設定されている場合、対称アクティブの着信パケット、ブロードキャスト パケット、マルチキャスト パケットを NTP が受信する際に、送信者と同期させるための一時的なピア アソシエーションを設定できます。

（注） 上記コマンドのいずれかを有効にする前に必ず **ntp authenticate** を指定してください。そうしないと、上記のパケット タイプのいずれかを送信する任意のデバイス（悪意のある攻撃者に制御されたデバイスを含む）とデバイスが同期される可能性があります。

- **ntp authenticate** コマンドが指定されている場合、対称アクティブ パケット、ブロードキャスト パケット、マルチキャスト パケットが受信されても、**ntp trusted-key** グローバル コンフィギュレーション コマンドで指定された認証キーの 1 つがパケットで運ばれていない限り、システムとピアの同期は行われません。
- **ntp access-group** コマンドなど他の方法で、デバイスの NTP サービスと非承認ホストとの通信防止の措置が取られている場合を除き、非承認のネットワーク ホストとの同期を避けるには、**ntp passive**、**ntp broadcast client**、**ntp multicast client** コマンドを指定した段階で随時 **ntp authenticate** コマンドを指定する必要があります。
- **ntp authenticate** コマンドは、**ntp server** および **ntp peer** コンフィギュレーション コマンドで設定されたピア アソシエーションを認証しません。**ntp server** および **ntp peer** アソシエーションを認証するには、**key** キーワードを指定します。

- 時刻の精度および信頼性要件が厳密ではない場合、NTP ブロードキャストまたはマルチキャストアソシエーションを使用すると、ネットワークがローカル化され、ネットワークは 20 以上のクライアントを持ちます。帯域幅、システム メモリ、または CPU リソースが限られているネットワークでは NTP ブロードキャストまたはマルチキャスト アソシエーションの使用をお勧めします。
- 1 つの NTP アクセス グループに最大 4 つの ACL を設定できます。

（注） 情報の流れが一方向に限定されるため、NTP ブロードキャスト アソシエーションでは、時刻の精度がわずかに低下します。

デフォルト設定

次に、NTP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
NTP	すべてのインターフェイスでイネーブル
NTP passive（アソシエーションを形成するために NTP をイネーブルにする）	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 ブロードキャスト サーバー	ディセーブル
NTP マルチキャスト サーバ	ディセーブル
NTP マルチキャスト クライアント	ディセーブル
NTP ロギング	ディセーブル

NTP の設定

インターフェイスでの NTP のイネーブル化またはディセーブル化

特定のインターフェイスで NTP をイネーブルまたはディセーブルにできます。NTP は、すべてのインターフェイスでデフォルトでイネーブルに設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# **[no] ntp disable** {**ip** | **ipv6**}	指定のインターフェイスで NTP IPv4 または IPv6 をディセーブルにします。 インターフェイス上でNTPを再度イネーブルにするにはこのコマンドの **no** 形式を使用します。
ステップ 4	（任意） switch(config-if)# **copy running-config startup-config**	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。

例

次に、インターフェイスで NTP をイネーブルまたはディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp disable ip
switch(config-if)# copy running-config startup-config
```

正規の NTP サーバとしてのデバイスの設定

デバイスを正規の NTP サーバーとして動作するよう設定し、既存のタイム サーバーと同期していないときでも時刻を配信させることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	[**no**] **ntp master** [*stratum*]	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントがこれらの時間を同期するのと別の階層レベルを指定できます。指定できる範囲は 1 ～ 15 です。

	コマンドまたはアクション	目的
ステップ 3	（任意） **show running-config ntp**	NTP コンフィギュレーションを表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	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。

例

次に、正規の NTP サーバーとして Cisco NX-OS デバイスを別の階層レベルで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 サーバーおよびピアを設定できます。

始める前に

NTP サーバーとそのピアの IP アドレスまたは DNS 名がわかっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	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。 サーバ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ー16（2 の累乗として設定されます。つまり、実質的に16ー65536秒）で、デフォルト値はそれぞれ 6 と 4 です

	コマンドまたはアクション	目的
		（*maxpoll* デフォルト = 64秒、*minpoll* デフォルト= 16秒）。 デバイスに対して対象の NTP サーバーを優先サーバーにするには、**prefer keyword** を使用します。 指定された VRF を介して通信するように 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 文字までの任意の英数字の文字列を使用できます。 （注） NTP サーバー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。
ステップ 3	switch(config)# [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	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。 NTP 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。 サーバ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ー16（2 の累乗として設定されます。つまり、実質的に 16ー131072 秒）で、デフォルト値はそれぞれ 6 と 4 です（*maxpoll* デフォルト = 64秒、*minpoll* デフォルト= 16秒）。 デバイスに対して対象の NTP ピアを優先にするには、**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に NTP ピアを設定するには、**use-vrf**

	コマンドまたはアクション	目的
		キーワードを使用します。*vrf-name* 引数には、**default**、**management**、または大文字と小文字が区別される最大 32 文字の任意の英数字文字列を指定できます。
ステップ 4	（任意） switch(config)# **show ntp peers**	設定された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	（任意） switch(config)# **copy running-config startup-config**	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。

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。

始める前に

NTP サーバーと NTP ピアの認証は、**key** キーワードを各 **ntp server** および **ntp peer** コマンドで使用することにより、アソシエーションごとに設定されます。この手順で指定する予定の認証キーによって、すべての NTP サーバーとピア アソシエーションが設定されていることを確認します。**ntp server** または **ntp peer** コマンドで **key** キーワードを指定しない場合、認証なしでの動作が続けられます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`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* 例：	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**

	コマンドまたはアクション	目的
	`switch(config)# ntp authentication-key 42 md5 aNiceKey`	**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。
ステップ 3	**ntp server** *ip-address* **key** *key-id* 例： `switch(config)# ntp server 192.0.2.1 key 1001`	指定された NTP サーバーで認証を有効にし、サーバーとの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。 認証を必須とする場合は、**key** キーワードを使用する必要があります。**ntp server** または **ntp peer** コマンドで **key** キーワードを指定しない場合、認証なしでの動作が続けられます。
ステップ 4	（任意） **show ntp authentication-keys** 例： `switch(config)# show ntp authentication-keys`	設定済みの NTP 認証キーを表示します。
ステップ 5	[**no**] **ntp trusted-key** *number* 例： `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。デバイスを時刻源と同期させるには、未設定のリモート シンメトリック、ブロードキャスト、およびマルチキャストの時刻源を NTP パケット内に入力する必要があります。trusted key 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 6	（任意） **show ntp trusted-keys** 例： `switch(config)# 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。

	コマンドまたはアクション	目的
ステップ 7	[**no**] **ntp authenticate** 例： `switch(config)# ntp authenticate`	ntp passive、ntp broadcast client、および ntp multicast で認証を有効または無効にします。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 8	（任意） **show ntp authentication-status** 例： `switch(config)# show ntp authentication-status`	NTP 認証の状況を表示します。
ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。

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、デバイスで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。

Cisco NX-OS リリース 7.0(3)I7(3) 以降では、アクセス グループは次の方法で評価されます。

- **match-all** キーワードがない場合、パケットは permit が見つかるまでアクセス グループに対して（以下に示す順で）評価されます。permit が検出されない場合、パケットはドロップされます。
- **match-all** キーワードがある場合、パケットはすべてのアクセス グループに対して（以下に示す順で）評価され、最後に成功した評価（ACL が設定されている最後のアクセス グループ）に基づいてアクションが実行されます。

アクセス グループとパケットのタイプのマッピングは次のとおりです。

- peer：クライアント、対称アクティブ、対称パッシブ、サービス、コントロール、およびプライベート パケット（すべてのタイプ）を処理
- serve：クライアント、コントロール、およびプライベート パケットを処理
- serve-only：クライアント パケットだけを処理
- query-only：コントロールおよびプライベート パケットだけを処理

アクセス グループは、次の降順で評価されます。

1. peer（すべてのパケット タイプ）
2. serve（クライアント、コントロール、およびプライベート パケット）
3. query only（クライアント パケット）または query-only（コントロールおよびプライベート パケット）

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp access-group match-all** | {{**peer** | **serve** | **serve-only** | **query-only** }*access-list-name*}	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。 アクセス グループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。ただし、ピアに設定された拒否 ACL ルールに NTP が一致した場合、ACL 処理は停止し、次のアクセス グループ オプションへと継続しません。 • **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 リストで指定されているサーバーと同期するようにします。 • **serve** キーワードは、アクセス リストに指定されているサーバーからの時刻要求と NTP 制御クエリーをデバイスが受信できるようにしますが、指定されたサーバーとは同期しないようにします。 • **serve-only** キーワードは、デバイスがアクセス リストで指定されたサーバーからの時刻要求だけを受信するようにします。 • **query-only** キーワードは、デバイスがアクセス リストで指定されたサーバーからの NTP 制御クエリーのみを受信するようにします。

	コマンドまたはアクション	目的
		• **match-all** キーワードを使用すると、アクセス グループ オプションが、制限の最も緩いものから最も厳しいもの、peer、serve、serve-only、query-only の順序でスキャンされるようにできます。着信パケットが peer アクセス グループの ACL に一致しない場合、パケットは serve アクセス グループに送信され、処理されます。パケットが serve アクセス グループの ACL に一致しない場合、serve-only アクセス グループに送られ、これが継続されます。 （注） **match-all** キーワードは、Cisco NX-OS リリース 7.0(3)I6(1) 以降で使用可能です。
ステップ 3	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	（任意） switch(config)# **copy running-config startup-config**	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。

例

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	[**no**] **ntp source** *ip-address*	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。

例

次に、NTP ソース IP アドレスに 192.0.2.2 を設定する例を示します。

```
switch# configure terminal
switch(config)# ntp source 192.0.2.2
```

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	[**no**] **ntp source-interface** *interface*	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。次のリストに、*interface* として有効な値を示します。 • ethernet • loopback • mgmt • port-channel • vlan

例

次に、NTP 送信元インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ntp source-interface ethernet
```

NTP ブロードキャスト サーバの設定

インターフェイス上で NTP IPv4 ブロードキャスト サーバを設定できます。デバイスは、そのインターフェイスを介してブロードキャストパケットを定期的に送信します。クライアントは応答を送信する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# **[no] ntp broadcast** [**destination** *ip-address*] [**key** *key-id*] [*version number*]	指定されたインターフェイスの IPv4 NTP ブロードキャスト サーバをイネーブルにします。 • **destination** *ip-address*：ブロードキャスト宛先 IP アドレスを設定します。 • **key** *key-id*：ブロードキャスト認証キー番号を設定します。有効な範囲は 1 ～ 65535 です。 • *version number*：NTP バージョンを設定します。範囲は 2 ～ 4 です。
ステップ 4	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	（任意） switch(config)# **[no] ntp broadcastdelay** *delay*	推定のブロードキャストラウンドトリップ遅延をマイクロ秒単位で設定します。範囲は 1 ～ 999999 です。
ステップ 6	（任意） switch(config)# **copy running-config startup-config**	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。

例

次に、NTP ブロードキャスト サーバーを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp broadcast destination 192.0.2.10
switch(config-if)# exit
switch(config)# ntp broadcastdelay 100
switch(config)# copy running-config startup-config
```

NTP マルチキャスト サーバの設定

インターフェイスに対して NTP IPv4 または IPv6 マルチキャスト サーバを設定できます。デバイスは、そのインターフェイスを介してマルチキャスト パケットを定期的に送信します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# **[no] ntp multicast** [*ipv4-address* | *ipv6-address*] [**key** *key-id*] [*ttl value*] [*version number*]	指定したインターフェイスの NTP IPv4 または IPv6 マルチキャスト サーバーをイネーブルにします。 • *ipv4-address* または *ipv6-address*：マルチキャスト IPv4 または IPv6 アドレス。 • **key** *key-id*：ブロードキャスト認証キー番号を設定します。有効な範囲は 1 ～ 65535 です。 • *ttl value*：マルチキャスト パケットの存続可能時間値。範囲は 1 ～ 255 です。 • *version number*：NTP バージョン。範囲は 2 ～ 4 です。
ステップ 4	（任意） switch(config-if)# **copy running-config startup-config**	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。

例

次に、NTPマルチキャストパケットを送信するようにイーサネットインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/2
switch(config-if)# ntp multicast FF02::1:FF0E:8C6C
switch(config-if)# copy running-config startup-config
```

NTP マルチキャスト クライアントの設定

インターフェイス上でNTP マルチキャスト クライアントを設定できます。デバイスはNTP マルチキャストメッセージをリッスンし、マルチキャストが設定されていないインターフェイスからのメッセージを廃棄します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **interface** *type slot/port*	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# **[no] ntp multicast client** [*ipv4-address* | *ipv6-address*]	指定されたインターフェイスが NTP マルチキャスト パケットを受信できるようにします。
ステップ 4	（任意） switch(config-if)# **copy running-config startup-config**	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。

例

次に、NTPマルチキャストパケットを受信するようにイーサネットインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ntp multicast client FF02::1:FF0E:8C6C
switch(config-if)# copy running-config startup-config
```

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# [**no**] **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	（任意） switch(config)# **show ntp logging-status**	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	（任意） switch(config)# **copy running-config startup-config**	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。

例

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 用の CFS 配信のイネーブル化

NTP コンフィギュレーションを他の CFS 対応デバイスに配信するために、NTP 用の CFS 配信をイネーブルにできます。

始める前に

デバイスの CFS 配信をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp distribute**	CFS を介して配信される NTP コンフィギュレーションのアップデートをデバイ

	コマンドまたはアクション	目的
		スが受信することを、イネーブルまたはディセーブルにします。
ステップ 3	（任意） switch(config)# **show ntp status**	NTP CFS の配信状況を表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	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。

例

次に、デバイスが CFS を介して NTP 設定の更新を受信できるようにする例を示します。

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# copy running-config startup-config
```

NTP 設定変更のコミット

NTP コンフィギュレーションの変更をコミットすると、保留データベースのコンフィギュレーション変更によって有効なデータベースが上書きされ、ネットワーク内のすべてのデバイスが同じコンフィギュレーションを受け取ります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **ntp commit**	ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションの変更を配信し、CFS ロックを解放します。このコマンドは、保留データベースに対して行われた変更によって、有効なデータベースを上書きします。

NTP 設定変更の廃棄

コンフィギュレーション変更の後で、これらの変更をコミットせずに、破棄するよう選択することもできます。変更を破棄すると、Cisco NX-OS によって保留データベースの変更が削除され、CFS ロックが解放されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **ntp abort**	保留データベースで NTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。このコマンドは、NTP コンフィギュレーションを起動したデバイスで使用します。

CFS セッション ロックの解放

NTP コンフィギュレーションを実行したが、変更をコミットまたは破棄してロックを解放し忘れた場合は、自分で、または他の管理者がネットワーク内の任意のデバイスからロックを解放できます。また、この操作では、保留データベースの変更が破棄されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル設定モードを開始します。
ステップ 2	switch(config)# **clear ntp session**	保留データベースで NTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。

NTP の設定確認

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 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 peer	すべての NTP ピアを表示します。

コマンド	目的
show ntp pending	NTP 用の一時 CFS データベースを表示します。
show ntp pending-diff	保留 CFS データベースと現行の NTP コンフィギュレーションの差異を表示します。
show ntp rts-update	RTS アップデートの状況を表示します。
show ntp session status	NTP CFS配信セッションの情報を表示します。
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*} | **name** *peer-name*}}	NTP 統計情報を表示します。
show ntp status	NTP CFS の配信状況を表示します。
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 の設定例

NTP の設定例

次に、NTP サーバー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、そのスタートアップの設定を保存し、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 192.0.2.105
switch(config)# show ntp peers
-------------------------------------------------
Peer IP Address Serv/Peer
-------------------------------------------------
192.0.2.100 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)#
```

次に、以下の制約事項のある NTP アクセス グループの設定の例を示します。

- peer の制約事項は、「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 の制約事項は、「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 の制約事項は、「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 の制約事項は、「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
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。