



NTP の実装

ネットワーク タイム プロトコル (NTP) は、ネットワーク内でデバイスの時刻同期を行うように設計されたプロトコルです。Cisco IOS XR ソフトウェアは、NTPv4 を実装しています。NTPv4 は以前の NTP バージョンである NTPv3、NTPv2 との後方互換性がありますが、セキュリティ脆弱性のため中止となった NTPv1 との互換性はありません。

- [NTP の実装について \(1 ページ\)](#)
- [NTP の設定 \(2 ページ\)](#)

NTP の実装について

NTP を使用すると、分散されたタイム サーバとクライアントの間で時刻が同期されます。同期化により、システムログ作成時または時間に関するイベントの発生時に、各イベントを関連付けることができます。

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。NTP の通信はすべて協定世界時 (UTC) を使用します。NTP のネットワークでは通常、タイムサーバに接続された電波時計や原子時計など正規の時刻源から時刻を取得します。NTP はこの時刻をネットワーク全体に配信します。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、各マシンが信頼できる時刻源から何 NTP ホップ隔たっているかを表すために「ストラタム」という概念を使用します。「Stratum 1」タイムサーバには通常、正規の時刻源（電波時計、原子時計、GPS 時刻源など）が直接接続されています。「Stratum 2」タイムサーバは、「Stratum 1」タイムサーバから NTP を介して時刻を受信し、それ以降のサーバも続きます。

NTP では、2 つの方法で時刻が間違っている可能性のあるマシンとの同期を回避します。まず、NTP はそれ自身で同期を行わないマシンとの同期を回避します。次に、複数のマシンから報告された時間と大幅に時間が異なっているマシンがある場合、ストラタムの番号が小さくても同期しません。このようにして、NTP サーバのツリーは効率よく自律的に編成されています。

シスコの NTP 実装では、ストラタム 1 サービスをサポートしていないため、電波時計や原子時計に接続することはできません（ただし、いくつかの特定のプラットフォームでは、GPS 時

時刻源デバイスに接続できます)。ネットワークのタイム サービスは、IP インターネットで行うことができる公開 NTP サーバから取得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、シスコの NTP 実装では、実際には他の方法で時刻を決定している場合でも、NTP を介して同期されているものとして動作するようにマシンを設定できます。これにより、他のマシンが NTP を介してそのマシンと同期できるようになります。

自社のホスト システムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。また、このソフトウェアにより UNIX 派生サーバは原子時計から時刻を直接取得することができ、シスコルータに時刻情報を伝えるようにすることもできます。

NTP を実行しているマシン間の通信 (アソシエーション) は通常、静的に設定されており、各マシンには、アソシエーションを形成する必要があるすべてのマシンの IP アドレスが通知されます。アソシエーションが設定されたマシンの各ペアの間で NTP メッセージを交換することにより、正確な時刻管理が可能になります。

シスコの NTP 実装では、ネットワーク デバイスがネットワーク上で NTP 時刻情報を取得できる 2 つの方法があります。

- ホスト サーバへのポーリング
- NTP ブロードキャストのリスニング

LAN 環境では、IP ブロードキャスト メッセージを使用するように NTP を設定できます。ポーリングと比べ IP ブロードキャスト メッセージではマシンごとにメッセージの送受信を設定するだけなので、複雑な設定作業が軽減されます。ただし、情報の流れが一方向に限定されるため、時刻管理の精度がわずかに低下します。

NTP ブロードキャスト クライアントは、指定した IPv4 アドレスにある NTP ブロードキャスト サーバから送信されるブロードキャスト メッセージをリスニングします。クライアントは最初に受信したブロードキャスト メッセージを使って、ローカルの時計を同期します。

マシン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。

複数の時刻源 (VINES、ハードウェア クロック、手動による設定) がある場合、NTP は常に信頼できる時刻源とされます。NTP の時刻は、他の方法による時刻に優先します。

NTP の設定

Poll-Based アソシエーションの設定

次に、ルータのシステム クロックが IP アドレス 192.168.22.33 のタイム サーバ ホストとのピア アソシエーションを形成し、IP アドレス 10.0.2.1 および 172.19.69.1 のタイム サーバ ホストによって同期されるように設定する、NTP の設定例を示します。

```
ntp
server 10.0.2.1 minpoll 5 maxpoll 7
peer 192.168.22.33
server 172.19.69.1
```

ブロードキャストベースのアソシエーションの設定

次に、インターフェイス 0/2/0/0 が NTP ブロードキャストパケットを受信するように設定し、NTP クライアントと NTP ブロードキャストサーバ間の推定ラウンドトリップ遅延を 2 マイクロ秒に設定する、NTP クライアントの設定例を示します。

```
ntp
interface tengige 0/2/0/0
broadcast client
exit
broadcastdelay 2
```

次に、インターフェイス 0/2/0/2 がブロードキャストサーバになるように設定する、NTP サーバの設定例を示します。

```
ntp
interface tengige 0/2/0/0
broadcast
```

NTP アクセスグループの設定

次に、以下のアクセスグループの制約事項が適用される NTP アクセスグループの設定例を示します。

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。

```
ntp
peer 10.1.1.1
peer 10.1.1.1
peer 10.2.2.2
peer 10.3.3.3
peer 10.4.4.4
peer 10.5.5.5
peer 10.6.6.6
peer 10.7.7.7
peer 10.8.8.8
access-group peer peer-acl
access-group serve serve-acl
access-group serve-only serve-only-acl
access-group query-only query-only-acl
exit
ipv4 access-list peer-acl
10 permit ip host 10.1.1.1 any
20 permit ip host 10.8.8.8 any
```

```
exit
ipv4 access-list serve-acl
 10 permit ip host 10.4.4.4 any
 20 permit ip host 10.5.5.5 any
exit
ipv4 access-list query-only-acl
 10 permit ip host 10.2.2.2 any
 20 permit ip host 10.3.3.3 any
exit
ipv4 access-list serve-only-acl
 10 permit ip host 10.6.6.6 any
 20 permit ip host 10.7.7.7 any
exit
```

NTP 認証の設定

次に、NTP 認証の設定例を示します。この例では、次のように設定されます。

NTP 認証がイネーブルになります。

2つの認証キーが設定されます（キー2およびキー3）。

ルータは、ソフトウェアクロックが、認証キー2を使用するIPアドレス10.3.32.154のピアのクロックと（またはその逆に）同期することを許可するように設定されます。

ルータは、ソフトウェアクロックが、認証キー3を使用するIPアドレス10.32.154.145のデバイスのクロックと同期することを許可するように設定されます。

ルータは、NTP パケットに認証キー3を提供するシステムのみと同期するように設定されます。

```
ntp
authenticate
authentication-key 2 md5 encrypted 06120A2D40031D1008124
authentication-key 3 md5 encrypted 1311121E074110232621
trusted-key 3
server 10.3.32.154 key 3
peer 10.32.154.145 key 2
```

インターフェイスでの NTP のディセーブル化

次に、0/2/0/0 インターフェイスをディセーブルにする NTP の設定例を示します。

```
ntp
interface tengige 0/2/0/0
  disable
  exit
authentication-key 2 md5 encrypted 06120A2D40031D1008124
authentication-key 3 md5 encrypted 1311121E074110232621
authenticate
trusted-key 3
server 10.3.32.154 key 3
peer 10.32.154.145 key 2
```

正規の NTP サーバとしてのシステムの設定

次に、外部の NTP ソースが使用不可になったときに、独自の NTP マスター クロックを使用してピアと同期するようにルータを設定する、NTP の設定例を示します。

```
ntp
  master 6
```

ハードウェア クロックの更新

次に、ルータが定期的にソフトウェア クロックからハードウェア クロックを更新するように設定する、NTP の設定例を示します。

```
ntp
  server 10.3.32.154
  update-calendar
```

VRF インターフェイス内での NTP サーバの設定



- (注) 特定のコマンドで NTP をイネーブルにすることはできません。NTP は、最初に実行する NTP コンフィギュレーション コマンドによってイネーブルになります。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ntp
RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A
RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A source bvi 70
RP/0/RP0/CPU0:router(config-ntp)# end
or
RP/0/RP0/CPU0:router(config-ntp)# commit
```

