ネットワーク タイム プロトコルの設定

ネットワーク タイム プロトコル（NTP）は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP バージョン 3 は、RFC 1305 に記載されています。

この章では、IR8340 で Network Time Protocol を設定する方法について説明します。

NTP の設定は、Cisco IOS XE リリース 17.7.x 以降でサポートされています。

ネットワーク タイム プロトコルに関する制約事項

Network Time Protocol（NTP）パッケージには、認証されていないリモート攻撃者がサービス妨害（DoS）状態を発生させる可能性がある脆弱性が含まれています。NTP バージョン 4.2.4p7 以前は脆弱です。

この脆弱性は、特定の不正メッセージの処理におけるエラーによるものです。認証されていないリモート攻撃者は、スプーフィングされた送信元 IP アドレスを使用して、悪意ある NTP パケットを脆弱なホストに送信する可能性があります。このパケットを処理するホストは、送信者に応答パケットを返信します。この処理により、2 つのホスト間でメッセージのループが開始される可能性があります。その結果、両方のホストは、過剰なCPUリソースを消費し、ログファイルへのメッセージの書き込みにディスク スペースを使い切り、ネットワーク帯域幅を消費します。これにより、影響を受けたホスト上で DoS 状態が発生する可能性があります。

詳細については、Web ページ「Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability」を参照してください。

NTPv4 をサポートしている Cisco ソフトウェア リリースは影響を受けません。この問題は、その他すべての Cisco ソフトウェア バージョンに影響を及ぼします。

デバイスが NTP を使用するように設定されているかどうかを表示するには、**show running-config | include ntp** コマンドを使用します。出力に次のいずれかのコマンドが返された場合、そのデバイスは DoS 攻撃に対して脆弱です。

- **ntp broadcast client**
- **ntp primary**
- **ntp multicast client**
- **ntp peer**
- **ntp server**

Cisco ソフトウェア リリースの詳細については、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

デバイスで NTP を無効にする以外にこの脆弱性に対する回避策はありません。この脆弱性を悪用できるのは、デバイス上の設定済み IP アドレスに宛てられたパケットだけです。中継トラフィックは、この脆弱性を悪用しません。

リリースによっては NTP モード 7 パケットが処理され、NTP のデバッグが有効になっている場合は「NTP: Receive: dropping message: Received NTP private mode 7 packet」というメッセージが表示されることがあります。NTP モード 7 パケットを処理するには、**ntp allow mode private** コマンドを設定します。このコマンドは、デフォルトで無効になっています。

（注） NTP ピア認証は回避策ではなく、脆弱な設定です。

NTP サービスは、デフォルトではすべてのインターフェイスで無効になっています。

NTP を実行しているネットワーキング デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーション モードで動作するように設定できます。ネットワーキング デバイスは、2 つの方法でネットワーク上の時刻情報を取得できます。それらは、ホスト サービスのポーリングと NTP ブロードキャストのリスニングです。

Line Aux 0 オプションはデフォルトで無効になっています。

ネットワー タイム プロトコルについて

ネットワーク タイム プロトコル

ネットワーク タイム プロトコル（NTP）は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP バージョン 3 は、RFC 1305 に記載されています。

NTP ネットワークは通常、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、正規の時刻源から時刻を取得します。NTP は、ネットワークにこの時刻を分配します。NTP

はきわめて効率的です。毎分 1 パケットだけで、2 台のマシンが相互に 1 ミリ秒以内の精度で同期します。

NTP では、信頼できるタイム ソースから各マシンが何 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が使用されます。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、Global Positioning System（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 は、次の 2 つの方法により、時刻が正確でない可能性があるマシンへの同期を回避します。NTP は、自身が同期されていないマシンには同期しません。また、NTP は、複数のマシンによって報告された時刻を比較し、時刻が他と大きく異なるマシンには、ストラタムが低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、Stratum 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 時刻源デバイスに接続できます）。ネットワークの時刻サービスは、IP インターネット上のパブリック 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。

多くの製造業者のホスト システムで、NTP ソフトウェアが導入されています。また、UNIX システム向けに公開されているバージョンもあります。また、このソフトウェアにより UNIX 派生サーバー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。

ただし、LAN 環境では、代わりに 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。この代替手段では、ブロードキャスト メッセージを送受信するように各マシンを設定できるので、設定の複雑さが緩和されます。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。

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（Virtual Integrated Network System（VINES）、ハードウェア クロック、手動による設定）がある場合、NTP は常により信頼できる時刻源と見なされます。NTP の時刻は、他の方法による時刻に優先します。

NTP サービスは、デフォルトではすべてのインターフェイスで無効になっています。

NTP の詳細については、次の項を参照してください。

ポーリング ベースの NTP アソシエーション

NTP を実行しているネットワーキング デバイスは、時刻を基準時刻源と同期する際にさまざまなアソシエーション モードで動作するように設定できます。ネットワーキング デバイスは、2 つの方法でネットワーク上の時刻情報を取得できます。それらは、ホスト サービスのポーリングと NTP ブロードキャストのリスニングです。ここでは、ポーリングベースのアソシエーション モードを中心に説明します。ブロードキャスト ベースの NTP アソシエーションの詳細については、「ブロードキャスト ベースの NTP アソシエーション」を参照してください。

最も一般的に使用される 2 つのポーリングベースのアソシエーション モードは次のとおりです。

- クライアント モード
- 対称アクティブ モード

クライアントモードと対称アクティブモードは、高レベルの時刻の精度と信頼性を提供するために NTP が必要になる場合に使用します。

クライアントモードで動作しているネットワーキングデバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得します。次に、ネットワーキング デバイスは、ポーリングされたすべてのタイム サーバーから、同期に使用するホストを選択します。この場合は、確立された関係がクライアントホスト関係なので、ホストがローカル クライアントデバイスから送信された時刻情報をキャプチャしたり使用したりすることはありません。このモードが最も適しているのは、他のローカル クライアントにどのような形式の時刻同期も提供する必要のない、ファイルサーバーおよびワークステーションのクライアントです。ネットワーキングデバイスを同期させるタイムサーバーを個別に指定し、クライアントモードで動作するようにネットワーキングデバイスを設定するには、**ntp server** コマンドを使用します。

対称アクティブモードで動作しているネットワーキングデバイスは、自身に割り当てられている時刻提供ホストをポーリングして現在の時刻を取得し、そのホストによるポーリングに応答します。これはピアツーピアの関係なので、ホストは、通信相手のローカルネットワーキングデバイスの時刻関連情報も保持します。このモードは、さまざまなネットワーク パスを経由で多数の冗長サーバーが相互接続されている場合に使用します。インターネット上のほとんどの Stratum 1 および Stratum 2 サーバーは、この形式のネットワーク設定を採用しています。ネットワーキングデバイスを同期させる必要がある時刻提供ホストを個別に指定し、対称アクティブモードで動作するようにネットワーキングデバイスを設定するには、**ntp peer** コマンドを使用します。

各ネットワーキングデバイスの設定モードを決定する際には、タイムキーピングデバイスとしてのそのデバイスの役割（サーバーかクライアントか）と、そのデバイスが Stratum 1 タイムキーピング サーバーにどれだけ近いかを主に考慮してください。

ネットワーキングデバイスは、クライアントモードでクライアントまたはホストとして動作する場合、または対称アクティブ モードでピアとして動作する場合にポーリングに関与します。通常、ポーリングによってメモリおよびCPUリソース（帯域幅など）に負荷が生じることはありませんが、システム上で進行または同時実行しているポーリングの数がきわめて多い場合には、システムの性能に深刻な影響があったり、特定のネットワークの性能が低下したりする可能性があります。過剰な数のポーリングがネットワーク上で進行することを防止するには、直接的なピアツーピア アソシエーションまたはクライアントからサーバーへのアソシエーションを制限する必

要があります。代わりに、局所的なネットワーク内にNTPブロードキャストを使用して時刻情報を伝播することを検討します。

ブロードキャスト ベースの NTP アソシエーション

ブロードキャストベースの NTP アソシエーションは、時刻の精度および信頼性要件が適度であり、ネットワークが局所的であり、クライアント数が20を超える場合に使用します。また、帯域幅、システム メモリ、またはCPUリソースが制限されているネットワークにおいても、ブロードキャストベースの NTP アソシエーションの使用をお勧めします。

ブロードキャスト クライアント モードで動作しているネットワーキング デバイスはポーリングに関与しません。代わりに、ブロードキャスト タイム サーバーによって転送される NTP ブロードキャスト パケットを待ち受けます。その結果、時刻情報の流れが一方向に限られるため、時刻の精度がわずかに低下する可能性があります。

ネットワークを通じて伝播されるNTPブロードキャストパケットを待ち受けるようにネットワーキングデバイスを設定するには、**ntp broadcast client** コマンドを使用します。ブロードキャストクライアントモードが動作するためには、ブロードキャストサーバーとそのクライアントが同じサブネット上に存在する必要があります。**ntp broadcast** コマンドを使用して、対象デバイスのインターフェイスでNTPブロードキャストパケットを送信するタイムサーバーを有効にする必要があります。

NTP アクセス グループ

アクセス リストベースの制限スキームを使用すると、ネットワーク全体、ネットワーク内のサブネット、またはサブネット内のホストに対し、特定のアクセス権限を許可または拒否できます。NTP アクセスグループを定義するには、グローバル コンフィギュレーション モードで **ntp access-group** コマンドを使用します。

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。

1. **ipv4**：IPv4 アクセスリストを設定します。
2. **ipv6**：IPv6 アクセスリストを設定します。
3. **peer**：時刻要求と NTP 制御クエリを許可し、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することを許可します。
4. **serve**：時刻要求と NTP 制御クエリを許可しますが、システムがアクセスリストの基準を満たすアドレスを持つ別のシステムに同期することは許可しません。
5. **serve-only**：アクセスリストの基準を満たすアドレスを持つシステムからの時刻要求のみを許可します。
6. **query-only**：アクセスリストの基準を満たすアドレスを持つ別のシステムからのNTP制御クエリのみを許可します。

送信元 IP アドレスが複数のアクセス タイプのアクセス リストに一致する場合は、最初のアクセス タイプのアクセスが認可されます。アクセス グループが指定されていない場合は、すべてのシ

ステムへのアクセスがすべてのアクセスタイプに対して認可されます。アクセス グループが指定されている場合は、指定されたアクセス タイプに対してのみアクセスが認可されます。

NTP 制御クエリーの詳細については、RFC 1305（NTP バージョン 3）を参照してください。

信頼できる形式のアクセス コントロールが必要な場合は、暗号化されたNTP認証方式を使用する必要があります。IPアドレスに基づくアクセスリストベースの制約方式とは異なり、暗号化認証方式では、認証キーと認証プロセスを使用して、ローカル ネットワーク上の指定されたピアまたはサーバーによって送信されたNTP同期パケットが信頼できると見なされるかどうかを、一緒に伝送された時刻情報を受け入れる前に判断します。

認証プロセスは、NTPパケットが作成されるとすぐに開始されます。暗号チェックサム キーは、Message-Digest Algorithm 5（MD5）を使用して生成され、受信側クライアントに送信されるNTP同期パケットに埋め込まれます。パケットがクライアントによって受信されると、暗号チェックサム キーが復号され、信頼できるキーのリストに対してチェックされます。一致する認証キーがパケットに含まれる場合、受信側クライアントは、パケットに含まれるタイムスタンプ情報を受け入れます。一致するオーセンティケータ キーが含まれていないNTP同期パケットは無視されます。

（注） 信頼できるキーを多数設定する必要がある大規模なネットワークでは、信頼できるキーの範囲設定機能を使用して複数のキーを同時に有効にすることができます。

NTP認証で使用される暗号化および復号化プロセスでは、CPUに非常に大きな負荷がかかる場合があり、ネットワーク内で伝播される時刻の精度が大きく低下する可能性があることに注意してください。より包括的なアクセスコントロールモデルを使用できるネットワーク構成の場合は、アクセス リスト ベースのコントロール方式を使用することを検討してください。

NTP認証が適切に設定されると、ネットワーキング デバイスは、信頼できる時刻源と同期し、信頼できる時刻源だけに同期を提供します。

特定のインターフェイス上の NTP サービス

Network Time Protocol（NTP）サービスは、デフォルトではすべてのインターフェイスで無効になっています。なんらかのNTPコマンドを入力すると、NTPがグローバルに有効になります。特定のインターフェイスを通じて特定のNTPパケットを受信しないように設定するには、インターフェイス コンフィギュレーション モードで **ntp disable** コマンドを使用します。

NTP パケットの送信元 IP アドレス

システムが NTP パケットを送信すると、通常、送信元 IP アドレスは、その NTP パケットの送信元であるインターフェイスのアドレスに設定されます。IP送信元アドレスの取得元の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 **ntp source** interface コマンドを使用します。

このインターフェイスは、すべての宛先に送信されるすべてのパケットの送信元アドレスに使用されます。送信元アドレスを特定のアソシエーションで使用する場合は、**ntp peer** または **ntp server** コマンドで **source** キーワードを使用します。

正規の NTP サーバとしてのシステム

システムを正規の NTP サーバーにする場合は、グローバル コンフィギュレーション モードで **ntp** コマンドを使用します。これは、システムが外部の時刻源と同期されていない場合でも同じです。

（注） **ntp primary** コマンドの使用には注意が必要です。このコマンドを使用すると、有効な時刻源が容易に上書きされてしまいます。低いストラタム番号を設定する際には、特に注意が必要です。**ntp primary** コマンドを使用して同じネットワーク内の複数のマシンを設定した場合は、それらのマシンの時刻が一致していないと、時刻管理が不安定になることがあります。

ネットワーク タイム プロトコルの設定方法

NTP の設定

ポーリング ベースの NTP アソシエーションの設定

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**]
4. **ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
Step 2	**configure terminal** **Example:** `Router# configure terminal`	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。
Step 3	**ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Router(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer`	他のシステムとのピア アソシエーションを形成します。

	Command or Action	Purpose
Step 4	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Router(config)# ntp server 192.168.10.1 version 2 prefer`	他のシステムとのサーバー アソシエーションを形成します。
Step 5	**end** **Example:** `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ブロードキャスト ベースの NTP アソシエーションの設定

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp broadcast version** *number*
5. **ntp broadcast client**
6. **ntp broadcastdelay** *microseconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
Step 2	**configure terminal** **Example:** `Router# configure terminal`	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。
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
Step 4	**ntp broadcast version** *number* **Example:** `Router(config-if)# ntp broadcast version 2`	指定されたインターフェイスが NTP ブロードキャスト パケットを送信するように設定します。
Step 5	**ntp broadcast client** **Example:** `Router(config-if)# ntp broadcast client`	指定されたインターフェイスが NTP ブロードキャスト パケットを受信するように設定します。

	Command or Action	Purpose
Step 6	**ntp broadcastdelay** *microseconds* **Example:** `Router(config-if)# ntp broadcastdelay 100`	NTP ブロードキャストの推定ラウンドトリップ遅延を調整します。
Step 7	**end** **Example:** `Router(config)# end`	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、特権 EXEC モードに戻ります。

外部基準クロックの設定

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line aux** *line-number*
4. **end**
5. **show ntp associations**
6. **show ntp status**
7. **debug ntp refclock**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
Step 2	**configure terminal** **Example:** `Router# configure terminal`	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。
Step 3	**line aux** *line-number* **Example:** `Router(config)# line aux 0`	補助ポート 0 のライン コンフィギュレーション モードを開始します。
Step 4	**end** **Example:** `Router(config-line)# end`	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。
Step 5	**show ntp associations** **Example:** `Router# show ntp associations`	NTP アソシエーションのステータスを表示します（GPS 基準クロックのステータスを含みます）。

	Command or Action	Purpose
Step 6	**show ntp status** **Example:** `Router# show ntp status`	NTP のステータスを表示します。
Step 7	**debug ntp refclock** **Example:** `Router# debug ntp refclock`	デバッグを目的とした基準クロック動作の拡張モニタリングを許可します。

NTP 認証の設定

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* **md5** *key*
5. **ntp authentication-key** *number* **md5** *key*
6. **ntp authentication-key** *number* **md5** *key*
7. **ntp trusted-key** *key-number* [*- end-key*]
8. **ntp server** *ip-address* **key** *key-id*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
Step 2	**configure terminal** **Example:** `Router# configure terminal`	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。
Step 3	**ntp authenticate** **Example:** `Router(config)# ntp authenticate`	NTP 認証機能を有効にします。
Step 4	**ntp authentication-key** *number* **md5** *key* **Example:** `Router(config)# ntp authentication-key 1 md5 key1`	認証キーを定義します。 • キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
Step 5	**ntp authentication-key** *number* **md5** *key* **Example:**	認証キーを定義します。

	Command or Action	Purpose
	`Router(config)# ntp authentication-key 2 md5 key2`	• キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
Step 6	**ntp authentication-key** *number* **md5** *key* **Example:** `Router(config)# ntp authentication-key 3 md5 key3`	認証キーを定義します。 • キーごとに、キー番号、タイプ、および値を 1 つずつ指定します。
Step 7	**ntp trusted-key** *key-number* [- *end-key*] **Example:** `Router(config)# ntp trusted-key 1 - 3`	信頼できる認証キーを定義します。 • キーを信頼できる場合、このデバイスは、このキーを NTP パケット内で使用する別のシステムに同期できます。
Step 8	**ntp server** *ip-address* **key** *key-id* **Example:** `Router(config)# ntp server 172.16.22.44 key 2`	NTP タイム サーバーによってソフトウェア クロックが同期されるように設定します。
Step 9	**end** **Example:** `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ネットワーク タイム プロトコルの確認

show clock [detail]

このコマンドを使用すると、ソフトウェア クロックの現在の時刻が表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show clock detail

*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar
```

show ntp associations detail

このコマンドを使用すると、NTP アソシエーションのステータスが表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
```

```
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D0CDE881.9A6A9005 (18:42:09.603 UTC Tue Jan 4 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
192.168.45.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

show ntp status

このコマンドを使用すると、NTP のステータスが表示されます。次に、このコマンドの出力例を示します。

例：

```
Device# show ntp status

Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
reference time is D25AF07C.4B439650 (15:26:04.294 PDT Tue Oct 21 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 10 sec ago.
```

ネットワーク タイム プロトコルの設定例

例：ネットワーク タイム プロトコルの設定

次の例では、ハードウェア クロックを内蔵したデバイスが、他の 2 つのシステムとのサーバ アソシエーションを確立し、ブロードキャスト NTP パケットを送信し、ハードウェア クロックを定期的に更新し、時刻を VINES に再配信します。

```
clock timezone PST -8
clock summer-time PDT recurring

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
In the following example, a device with a hardware clock has no outside time source, so it
 uses the hardware clock as an authoritative time source and distributes the time via NTP
```

```
broadcast packets:


clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
The following example shows Line Aux 0 option is disabled by default.

config-register 0x0
reload
rommon 1 > set
rommon 2 >  AUX_PORT=1
rommon 3 > SYNC
rommon 4 > reset
rommon 1 > set
rommon 2 > confreg 0x2102
rommon 3 > reset
```

ネットワーク タイム プロトコルの関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
基本的なシステム管理コマンド	『Basic System Management Command Reference』
IPv6 の NTP4	『*Cisco IOS Basic System Management Guide*』
IP 拡張アクセス リスト	『*Cisco IOS IP Addressing Configuration Guide*』
IPX 拡張アクセス リスト	『*Novell IPX Configuration Guide*』
NTP パッケージの脆弱性	『*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability*』
Cisco IOS および NX-OS ソフトウェア リリース	『*White Paper: Cisco IOS and NX-OS Software Reference Guide*』

標準および **RFC**

標準および **RFC**	タイトル
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ネットワーク タイム プロトコルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* ネットワーク タイム プロトコルの機能情報

機能名	機能情報
ネットワーク タイム プロトコル	NTP は、ネットワーク接続されたマシンの時刻を同期させる目的で設計されたプロトコルです。NTP は UDP で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。

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。