基本的なシステム管理構成ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

基本的なシステム管理の実行 3

機能情報の確認 3

基本的なシステム管理の実行について 4

システム名 4

コマンド エイリアス 4

マイナー サービス 4

BOOTP サーバ 5

Finger プロトコル 5

Telnet アドレスの非表示化 6

EXEC 起動遅延 6

アイドル Telnet 接続 6

負荷データの間隔 6

TCP トランザクションの数 6

スイッチングおよびスケジューリング プラオリティ 7

システム バッファ サイズ 7

基本的なシステム管理の実行方法 7

基本的なシステム パラメータの設定 7

基本的なシステム管理の実行の設定例 14

その他の参考資料 14

基本的なシステム管理の実行の機能情報 16

ネットワーク タイム プロトコル 17

機能情報の確認 17

ネットワーク タイム プロトコルに関する制約事項 18

ネットワー タイム プロトコルについて 19

ネットワーク タイム プロトコル 19

ポーリング ベースの NTP アソシエーション 20

ブロードキャスト ベースの NTP アソシエーション 21
NTP アクセス グループ 21
特定のインターフェイス上の NTP サービス 23
NTP パケットの送信元 IP アドレス 23
正規の NTP サーバとしてのシステム 23
ネットワーク タイム プロトコルの設定方法 24
NTP の設定 24
ポーリング ベースの NTP アソシエーションの設定 24
ブロードキャスト ベースの NTP アソシエーションの設定 25
外部基準クロックの設定 26
NTP 認証の設定 28
ネットワーク タイム プロトコルの確認 29
ネットワーク タイム プロトコルの設定例 31
例：ネットワーク タイム プロトコルの設定 31
ネットワーク タイム プロトコルの関連資料 31
ネットワーク タイム プロトコルの機能情報 32
メモリしきい値通知 35
機能情報の確認 35
メモリしきい値通知について 35
メモリしきい値通知 36
メモリ予約 36
メモリしきい値通知の定義方法 36
空きメモリ不足しきい値の設定 36
重要な通知のためのメモリの予約 37
メモリしきい値通知の設定例 38
空きメモリ不足しきい値の設定：例 38
重要な通知のためのメモリの予約：例 38
その他の参考資料 38
メモリしきい値通知の機能情報 40
NTPv4 MIB 41
機能情報の確認 41
NTPv4 MIB について 42
NTPv4 MIB 42

NTPv4 MIB の確認方法 42
NTPv4 MIB の確認 42
NTPv4 MIB の設定例 43
例：NTP4 MIB の確認 43
その他の参考資料 45
NTPv4 MIB の機能情報 46

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

基本的なシステム管理の実行

このモジュールでは、Cisco IOS ソフトウェアの一般的なシステム機能（つまり、通常は特定のプロトコルに固有でない機能）を管理するために実行できる基本的な管理作業について説明します。

- 機能情報の確認，3 ページ
- 基本的なシステム管理の実行について，4 ページ
- 基本的なシステム管理の実行方法，7 ページ
- 基本的なシステム管理の実行の設定例，14 ページ
- その他の参考資料，14 ページ
- 基本的なシステム管理の実行の機能情報，16 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

基本的なシステム管理の実行について

システム名

システム名（ホスト名とも呼ばれます）は、ネットワーク内のシステムを一意に識別するために使用します。システム名は CLI プロンプトに表示されます。名前を設定していない場合は、システムのデフォルト名である Router になります。

コマンド エイリアス

コマンド エイリアスを使用して、コマンドの代替構文を設定できます。よく使用するコマンドや複雑なコマンドのエイリアスを作成することもできます。たとえば、エイリアス **save config** を **copy running-config startup-config** コマンドに割り当てると、タイプ量を減らすことができます。また、ユーザにとって **save config** コマンドの方が覚えやすいはずです。自分またはユーザ コミュニティのためにコマンド構文を調整する場合は、単語の置換または省略形を使用します。

設定するすべてのエイリアスはシステム上だけでイネーブルになること、および元のコマンド構文は設定ファイル内に表示されることに注意してください。

マイナー サービス

マイナーサービスは、ルーティングデバイス上で稼働する小規模なサービスであり、基本的なシステム テストおよび基本的なネットワーク機能の提供において役立ちます。マイナー サービスは、ネットワーク上の別のホストから接続テストを行う場合に便利です。

シスコのスモール サーバは、概念的にはデーモンと同じです。

Cisco IOS ソフトウェアベースのデバイスによって提供されるスモール サーバには、TCP、UDP、HTTP、ブートストラップ プロトコル（BOOTP）、Finger などがあります。HTTP サーバについては、『Cisco IOS Configuration Fundamentals Configuration Guide』の「Using the Cisco Web Browser User Interface」の章を参照してください。

TCP スモール サーバは、次のマイナー サービスを提供します。

- chargen：ASCII データのストリームを生成します。このサービスをテストするには、リモート ホストから **telnet** *a.b.c.d* **chargen** コマンドを発行します。
- daytime：ネットワーク タイム プロトコル（NTP）が設定されている場合、または日付と時刻が手動で設定されている場合に、システムの日付と時刻を返します。このサービスをテストするには、リモート ホストから **telnet** *a.b.c.d* **daytime** コマンドを発行します。
- discard：入力内容をすべて破棄します。このサービスをテストするには、リモート ホストから **telnet** *a.b.c.d* **discard** コマンドを発行します。

- echo：すべての入力内容をエコーバックします。このサービスをテストするには、リモートホストから **telnet** *a.b.c.d* **echo** コマンドを発行します。

UDP スモール サーバは、次のマイナー サービスを提供します。

- chargen：送信されたデータグラムを廃棄し、CR+LF（復帰と改行）で終端された 72 文字の ASCII 文字列で応答します。
- discard：送信されたデータグラムを破棄します。
- echo：送信されたデータグラムのペイロードをエコーします。

マイナー サービスはデフォルトで無効になっています。

注意 マイナー サービスをイネーブルにすると、特定のタイプのサービス拒絶（DoS）攻撃（UDP 診断ポート攻撃など）が発生する可能性が生まれます。したがって、UDP、TCP、BOOTP または Finger サービスを提供するすべてのネットワーク デバイスをファイアウォールで保護するか、これらのマイナー サービスをディセーブルにしておく必要があります。UDP 診断ポート攻撃の防止については、Cisco.com で入手できる「Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks」というタイトルのホワイトペーパーを参照してください。

BOOTP サーバ

ルーティング デバイスの非同期回線ブートストラップ プロトコル（BOOTP）サービスをイネーブルまたはディセーブルにできます。このスモール サーバは、デフォルトでイネーブルになっています。セキュリティ上の考慮事項により、このサービスを使用しない場合はディセーブルにしておく必要があります。

DHCP は BOOTP に基づいているため、これらのサービスは、（インターネット標準および RFC に準拠して）ウェルノウン UDP サーバ ポート 67 を共有します。Cisco IOS ソフトウェアにおける DHCP コンフィギュレーションの詳細については、『Cisco IOS IP Addressing Configuration Guide』を参照してください。BOOTP の詳細については、RFC 951 を参照してください。BOOTP と DHCP の相互運用性は、RFC 1534 で規定されています。DHCP は、RFC 2131 で規定されています。

Finger プロトコル

Finger プロトコルを使用すると、ネットワーク全体のユーザは、現在特定のルーティング デバイスを使用しているユーザのリストを取得できます。表示される情報には、システムで稼働しているプロセス、回線番号、接続名、アイドル時間、終端位置などがあります。この情報は、Cisco IOS ソフトウェアの **show users** EXEC コマンドを通じて提供されます。

Telnet アドレスの非表示化

Telnet セッションの確立を試行する間、アドレスを非表示にできます。非表示機能によって、アドレスの表示が抑制され、接続の試行時に通常表示されるその他のすべてのメッセージ（接続に失敗した場合の詳細なエラー メッセージなど）は引き続き表示されます。

EXEC 起動遅延

ノイズの多い回線での EXEC プロセスの起動を、回線がアイドルになってから 3 秒後まで遅らせるには、グローバル コンフィギュレーション モードで **service exec-wait** コマンドを使用します。

このコマンドはモデム回線のノイズが多い場合や、回線に接続されたモデムで Microcom Networking Protocol（MNP）または V.42 ネゴシエーションを無視するように設定されている場合や、MNP または V.42 モデムがダイヤル イン方式で使用されている場合に便利です。これらのケースでは、ノイズや MNP/V.42 パケットが誤ってユーザ名やパスワードとして認識され、ユーザがユーザ名とパスワードを入力する前に認証に失敗する可能性があります。このコマンドは、非モデム回線や、ログインが設定されていない回線には役立ちません。

アイドル Telnet 接続

通常、現在は使用中でない Telnet 接続に送信されたデータは、受け入れ後に廃棄されます。**service telnet-zero-idle** コマンドがイネーブルになっていてセッションが中断状態になると（つまり、他の接続がアクティブになると）、TCP ウィンドウが 0 に設定されます。この処理により、リモートホストは、接続が再開されるまでデータを送信できません。このコマンドは、ホストから送信されたすべてのメッセージをユーザに表示する必要があり、ユーザが複数のセッションを使用する可能性がある場合に使用します。ホストが最終的にタイムアウトし、ウィンドウの値が 0 の TCP ユーザがログアウトする場合は、このコマンドを使用しないでください。

負荷データの間隔

一連のデータを負荷統計情報の計算に使用する期間を変更できます。ダイヤル バックアップなどの決定は、この統計情報に基づいて行われます。負荷間隔の値を減らすと、平均統計情報の計算期間が短くなり、トラフィックのバーストに対する応答性が高まります。

TCP トランザクションの数

標準の TCP 実装を使用してマシン間のキーストロークを送信する場合、TCP は入力されたキーストロークごとに 1 パケットを送信する傾向があります。これにより、帯域幅を使い果たし、大規模ネットワークにおける輻輳の一因となる可能性があります。

John Nagle のアルゴリズム（RFC 896）は、TCP の小さなパケットの問題を軽減するうえで役立ちます。接続の確立後に入力された最初の文字は単一のパケットで送信されますが、TCP では、受

信者が直前のパケットを確認するまで、その後入力されたすべての文字が保持されます。次に、より大きな 2 番めのパケットが送信され、確認応答が返信されるまで、その後入力されたすべての文字が保存されます。その効果は、文字をより大きなチャンクに蓄積し、任意の接続のラウンドトリップ時間と一致する速度にネットワークへの伝送速度を調整することです。この方法は、通常すべての TCP ベース トラフィックに推奨されます。

デフォルトでは、Nagle アルゴリズムはイネーブルになっていません。

スイッチングおよびスケジューリング プラオリティ

ネットワーク サーバの正常な動作では、スイッチング動作に必要なだけ中央処理装置を使用することが許容されます。プロセッサがルーティング プロトコルを処理する時間を許容しない、異常に重い負荷がネットワーク上で実行されている場合には、状況に応じて、システムプロセススケジューラにプライオリティを与える必要があります。

システム バッファ サイズ

バッファ プールの初期設定および一時バッファを作成および破棄する際の制限値を調整できます。

通常のシステム運用においては、パブリック バッファ プールとインターフェイス バッファ プールの 2 つがあります。これらは、次のように動作します。

- パブリック プール内のバッファは、要求に基づいて拡大および収縮します。一部のパブリック プールは一時的なものであり、必要に応じて作成および破棄されます。その他のパブリック プールは永続的に割り当てられているため、破棄できません。パブリック バッファ プールには、small、middle、big、very big、large、および huge のラベルが付けられています。
- インターフェイス プールは静的です。つまり、すべて永続的です。インターフェイスごとに 1 つのインターフェイス プールが存在します。たとえば、Cisco 4000 1E 4T 構成には、1 つのイーサネット バッファ プールと 4 つのシリアル バッファ プールがあります。

サーバには、キューイング エレメントのプールが 1 つと、異なるサイズのパケット バッファのパブリック プールが 6 つあります。サーバは、プールごとに、未処理のバッファの数、フリー リスト上のバッファの数、およびフリー リストに許容される最大バッファ数を記録しています。

基本的なシステム管理の実行方法

基本的なシステム パラメータの設定

基本的なシステム パラメータを設定するには、次の手順を実行します。次の手順は、システムのカスタマイズ要件に応じて実行できます。

手順の概要

1. **hostname** *name*
2. **prompt** *string*
3. **alias** *mode alias-name alias-command-line*
4. **service tcp-small-servers**
5. **service udp-small-servers**
6. **no ip bootp server**
7. **ip finger**
8. **ip finger rfc-compliant**
9. **service hide-telnet-address**
10. **line** *line-number*
11. exit
12. **exit**
13. **busy-message** *hostname message*
14. **service exec-wait**
15. **service telnet-zero-idle**
16. **load-interval** *seconds*
17. **service nagle**
18. **scheduler interval** *milliseconds*
19. **scheduler allocate** [*network-microseconds process-microseconds*]
20. **scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**}
21. **buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *typenumber*} {**permanent** | **max-free** | **min-free** | **initial**} *number*
22. exit
23. **show aliases** [*mode*]
24. **show buffers**

手順の詳細

ステップ 1 **hostname** *name*

デバイスに名前を割り当てる基本的なシステム管理作業を実行するには、**hostname** *name* コマンドを使用します。

例：

```
Router(config)# hostname host1
```

ステップ 2 **prompt** *string*

または

no service prompt config

デフォルトでは、CLI プロンプトは、システム名とそれに続く山カッコ（>）（ユーザ EXEC モードの場合）またはポンド記号（#）（特権 EXEC モードの場合）で構成されます。システムの CLI プロンプトをカスタマイズするには、**prompt** *string* または **no service prompt config** コマンドを使用します。

例：

```
Router(config)# prompt Router123
```

または

例：

```
Router(config)# no service prompt config
```

ステップ 3 **alias** *mode alias-name alias-command-line*

コマンド エイリアスを作成するには、**alias** *mode alias-name alias-command-line* コマンドを使用します。

例：

```
Router(config)# alias exec save config copy running-config startup-config
```

ステップ 4 **service tcp-small-servers**

Chargen、Daytime、Discard、Echo などのマイナー TCP サービスをイネーブルにするには、**service tcp-small-servers** コマンドを使用します。

（注） これらの基本的サービスがディセーブルになっている場合はコンフィギュレーション ファイルに **no** 形式の **service tcp-small-servers** コマンドが表示されます。

例：

```
Router(config)# service tcp-small-servers
```

ステップ 5 **service udp-small-servers**

Chargen、Daytime、Discard、Echo などのマイナー UDP サービスをイネーブルにするには、**service udp-small-servers** コマンドを使用します。

（注） これらの基本的サービスがディセーブルになっている場合はコンフィギュレーション ファイルに **no** 形式の **service udp-small-servers** コマンドが表示されます。

例：

```
Router(config)# service udp-small-servers
```

ステップ 6 **no ip bootp server**

プラットフォーム上の BOOTP サーバをディセーブルにするには、**no ip bootp server** コマンドを使用します。

例：

```
Router(config)# no ip bootp server
```

ステップ 7 **ip finger**

シスコ デバイスが Finger（ポート 79）要求に応答できるようにするには、**ip finger** コマンドを使用します。**ip finger** コマンドが設定されている場合、ルータはリモート ホストからの **telnet** *a.b.c.d* **finger** コマンドに応答し、**show users** コマンドの出力をただちに表示して接続を閉じます。

例：

```
Router(config)# ip finger
```

ステップ 8 **ip finger rfc-compliant**

RFC 1288 に準拠するように Finger プロトコルを設定するには、**ip finger rfc-compliant** コマンドを使用します。20 人以上のユーザが同時にログインするデバイスでは **ip finger rfc-compliant** コマンドを設定しないようにしてください。**ip finger rfc-compliant** コマンドを設定すると、ルータは、情報を表示する前に、入力を待ちます。その後、リモート ユーザは Return キーを押して **show users** コマンドの出力を表示したり、**/W** を入力して **show users wide** コマンドの出力を表示したりできます。この情報が表示されたら、接続が閉じます。

例：

```
Router(config)# ip finger rfc-compliant
```

ステップ 9 **service hide-telnet-address**

Telnet アドレスを表示しないようにルータを設定するには、**service hide-telnet-address** コマンドを使用します。

例：

```
Router(config)# service hide-telnet-address
```

ステップ 10 **line** *line-number*

ライン コンフィギュレーション モードを開始するには、line コマンドを使用します。

例：

```
Router(config)# line 1
```

ステップ 11 exit

ライン コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

例：

```
Router(config-line)# exit
```

ステップ 12 **exit**

ライン コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

例：

```
Router(config-line)# exit
```

ステップ 13 **busy-message** *hostname message*

Telnet 接続の試行中に表示される情報をカスタマイズするには、**busy-message** コマンドを **service hide-telnet-address** コマンドとともに使用します。接続試行が失敗した場合、ルータではアドレスが抑制され、**busy-message** コマンドで指定されたメッセージが表示されます。

例：

```
Router(config)# busy-message host1 message1
```

ステップ 14 **service exec-wait**

ノイズの多い回線での EXEC プロセスの起動を、回線がアイドルになってから 3 秒後まで遅らせるには、**service exec-wait** コマンドを使用します。

例：

```
Router(config)# service exec-wait
```

ステップ 15 **service telnet-zero-idle**

Telnet 接続がアイドル状態のときに TCP ウィンドウをゼロに設定するように Cisco IOS ソフトウェアを設定するには、**service telnet-zero-idle** コマンドを使用します。

例：

```
Router(config)# service telnet-zero-idle
```

ステップ 16 **load-interval** *seconds*

負荷統計情報の計算にデータ セットを使用する時間の長さを変更するには、**load-interval** *seconds* コマンドを使用します。

例：

```
Router(config)# load-interval 100
```

ステップ 17 **service nagle**

Nagle アルゴリズムをイネーブルにして TCP トランザクション数を減らすには、**service nagle** コマンドを使用します。

例：

```
Router(config)# load-interval 100
```

ステップ 18 **scheduler interval** *milliseconds*

優先度が最も低いシステム プロセスの実行を停止できる最大時間を定義するには、**scheduler interval** *milliseconds* コマンドを使用します。

例：

```
Router(config)# scheduler interval 100
```

ステップ 19 **scheduler allocate** [*network-microseconds process-microseconds*]

Cisco 7200 シリーズおよび Cisco 7500 シリーズ ルータで CPU が高速スイッチングとプロセスレベルの処理に費やす時間を変更するには、**scheduler allocate** コマンドを使用します。

注意 **scheduler allocate** コマンドのデフォルト値は変更しないようにすることを推奨します。

例：

```
Router(config)# scheduler allocate 5000 200
```

ステップ 20 **scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**}

ループ プロセスの特性を設定するには、**scheduler process-watchdog** {**hang** | **normal** | **reload** | **terminate**} コマンドを使用します。

例：

```
Router(config)# scheduler process-watchdog hang
```

ステップ 21 **buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *typenumber*} {**permanent** | **max-free** | **min-free** | **initial**} *number*

システム バッファ サイズを調整するには、**buffers** {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *typenumber*} {**permanent** | **max-free** | **min-free** | **initial**} *number* コマンドを使用します。

例：

```
Router(config)# buffers small permanent 10
```

注意 ただし、これらのパラメータを調整することは推奨されません。不適切な設定は、システムのパフォーマンスに悪影響を及ぼします。

ステップ 22 exit

グローバル コンフィギュレーション モードを終了して特権 EXEC モードに戻るには、**exit** コマンドを使用します。

例：

```
Router(config)# exit
```

ステップ 23 **show aliases** [*mode*]

システムで現在設定されているコマンドエイリアスのリストと、それらのエイリアスの元のコマンド構文を表示するには、**show aliases** [*mode*] コマンドを使用します。

例：

```
Router# show aliases exec
```

ステップ 24 **show buffers**

バッファ情報を表示するには、**show buffers** コマンドを使用します。このコマンドの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

例：

```
Router# show buffers
Buffer elements:
     1119 in free list (1119 max allowed)
     641606 hits, 0 misses, 619 created
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     48 in free list (20 min, 150 max allowed)
     2976557 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Middle buffers, 600 bytes (total 25, permanent 25, peak 37 @ 2w0d):
     25 in free list (10 min, 150 max allowed)
     445110 hits, 4 misses, 12 trims, 12 created
     0 failures (0 no memory)
Big buffers, 1536 bytes (total 50, permanent 50):
     50 in free list (5 min, 150 max allowed)
     58004 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 10, permanent 10):
     10 in free list (0 min, 100 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 10 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Huge buffers, 18024 bytes (total 0, permanent 0):
     0 in free list (0 min, 4 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Interface buffer pools:
Syslog ED Pool buffers, 600 bytes (total 282, permanent 282):
     257 in free list (282 min, 282 max allowed)
     32 hits, 0 misses
IPC buffers, 4096 bytes (total 2, permanent 2):
     1 in free list (1 min, 8 max allowed)
     1 hits, 0 fallbacks, 0 trims, 0 created
     0 failures (0 no memory)
Header pools:
Header buffers, 0 bytes (total 511, permanent 256, peak 511 @ 2w0d):
     255 in free list (256 min, 1024 max allowed)
     171 hits, 85 misses, 0 trims, 255 created
     0 failures (0 no memory)
     256 max cache size, 256 in cache
     0 hits in cache, 0 misses in cache
```

```
Particle Clones:
     1024 clones, 0 hits, 0 misses
Public particle pools:
F/S buffers, 128 bytes (total 512, permanent 512):
     0 in free list (0 min, 512 max allowed)
     512 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
     512 max cache size, 512 in cache
     0 hits in cache, 0 misses in cache
Normal buffers, 512 bytes (total 2048, permanent 2048):
     2048 in free list (1024 min, 4096 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Private particle pools:
HQF buffers, 0 bytes (total 2000, permanent 2000):
     2000 in free list (500 min, 2000 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Serial2/0 buffers, 512 bytes (total 256, permanent 256):
     0 in free list (0 min, 256 max allowed)
     256 hits, 0 fallbacks
     256 max cache size, 132 in cache
     124 hits in cache, 0 misses in cache
     10 buffer threshold, 0 threshold transitions
Serial2/1 buffers, 512 bytes (total 256, permanent 256):
     0 in free list (0 min, 256 max allowed)
     256 hits, 0 fallbacks
     256 max cache size, 132 in cache
     124 hits in cache, 0 misses in cache
     10 buffer threshold, 0 threshold transitions
```

基本的なシステム管理の実行の設定例

基本的なシステム管理の実行に関連する設定例はありません。

その他の参考資料

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』
ネットワーク管理コマンド	『*Cisco IOS Network Management Command Reference*』
Cisco IOS の基本設定コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS の基本設定	『*Cisco IOS Configuration Fundamentals Configuration Guide*』

関連項目	マニュアル タイトル
UDP 診断ポートへの攻撃の防止	『Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks』
DHCP の設定	『*Cisco IOS IP Addressing Configuration Guide*』

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 896	『*Congestion Control in IP/TCP Internetworks*』
RFC 951	『*Algorithms for Synchronizing Network Clocks*』
RFC 1288	『*The Finger User Information Protocol*』
RFC 1534	『*Interoperation Between DHCP and BOOTP*』
RFC 2131	『*Dynamic Host Configuration Protocol*』

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

基本的なシステム管理の実行の機能情報

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*：基本的なシステム管理の実行の機能情報

機能名	リリース	機能情報
基本的なシステム管理の実行		このモジュールでは、Cisco IOS ソフトウェアの一般的なシステム機能を管理するための基本的作業について説明します。

第 3 章

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。

このモジュールでは、シスコ デバイスで Network Time Protocol を設定する方法について説明します。

- 機能情報の確認，17 ページ
- ネットワーク タイム プロトコルに関する制約事項，18 ページ
- ネットワー タイム プロトコルについて，19 ページ
- ネットワーク タイム プロトコルの設定方法，24 ページ
- ネットワーク タイム プロトコルの設定例，31 ページ
- ネットワーク タイム プロトコルの関連資料，31 ページ
- ネットワーク タイム プロトコルの機能情報，32 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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、[Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability] Web ページ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 master**
- **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 をディセーブル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 のデバッグがイネーブル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、デフォルトでディセーブルになっています。

（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ディセーブルになっています。

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。

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ディセーブルになっています。

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、システムのパフォーマンスに深刻な影響があったり、特定のネットワークのパフォーマンス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、NTP ブロードキャストを使用して、ローカライズされたネットワーク内で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、ネットワークがローカライズされ、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 サーバによって転送される NTP ブロードキャスト パケットをリッスンします。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 パケットをリッスン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 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、特定の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 サーバをイネーブル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 制御クエリーを許可し、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 制御クエリーを許可しますが、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 リストの条件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 制御クエリーのみを許可します。

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イネーブル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ディセーブルになっています。なんらかのNTPコマンドを入力すると、NTPがグローバルにイネーブルになります。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 master** 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 master** コマンドは慎重に使用してください。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 master** 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、これらのマシンの時刻が一致していないと、タイムキーピング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

手順の概要

1. **enable**
2. **configureterminal**
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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。
ステップ 3	**ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(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。
ステップ 4	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] 例： `Device(config)# ntp server 192.168.10.1 version 2 prefer`	他のシステムとのサーバ アソシエーションを形成します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(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

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **ntp broadcast version** *number*
5. **ntp broadcast client**
6. **ntp broadcastdelay** *microseconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。
ステップ 3	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 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。

	コマンドまたはアクション	目的
ステップ 4	**ntp broadcast version** *number* 例： `Device(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。
ステップ 5	**ntp broadcast client** 例： `Device(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。
ステップ 6	**ntp broadcastdelay** *microseconds* 例： `Device(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。
ステップ 7	**end** 例： `Device(config-if)# 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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。
ステップ 3	**line aux** *line-number* 例： `Device(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。
ステップ 4	**end** 例： `Device(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。
ステップ 5	**show ntp associations** 例： `Device# 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）。
ステップ 6	**show ntp status** 例： `Device# show ntp status`	NTP のステータスを表示します。
ステップ 7	**debug ntp refclock** 例： `Device# 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

手順の概要

1. **enable**
2. **configureterminal**
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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。
ステップ 3	**ntp authenticate** 例： `Device(config)# ntp authenticate`	NTP 認証機能をイネーブルにします。
ステップ 4	**ntp authentication-key** *number* **md5** *key* 例： `Device(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。
ステップ 5	**ntp authentication-key** *number* **md5** *key* 例： `Device(config)# ntp authentication-key 2 md5 key2`	認証キーを定義します。

	コマンドまたはアクション	目的
ステップ 6	**ntp authentication-key** *number* **md5** *key* 例： `Device(config)# ntp authentication-key 3 md5 key3`	認証キーを定義します。
ステップ 7	**ntp trusted-key** *key-number* [-*end-key*] 例： `Device(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。
ステップ 8	**ntp server** *ip-address* **key** *key-id* 例： `Device(config)# ntp server 172.16.22.44 key 2`	NTP タイム サーバ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。
ステップ 9	**end** 例： `Device(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

手順の概要

1. **show clock** [**detail**]
2. **show ntp associations detail**
3. **show ntp status**

手順の詳細

ステップ 1 **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
```

ステップ 2 **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
```

ステップ 3 **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
```

次の例では、ハードウェア クロックを内蔵したデバイスは外部の時刻源を持たないため、ハードウェアクロックを正規の時刻源として使用し、NTPブロードキャストパケットを介して時刻を配信します。

```
clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
```

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 *2*：ネットワーク タイム プロトコルの機能情報

機能名	リリース	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。

第 4 章

メモリしきい値通知

メモリしきい値通知機能を使用すると、重要な通知のためにメモリを予約し、使用可能なメモリが指定したしきい値を下回ると通知を行うようルータを設定できます。

- 機能情報の確認，35 ページ
- メモリしきい値通知について，35 ページ
- メモリしきい値通知の定義方法，36 ページ
- メモリしきい値通知の設定例，38 ページ
- その他の参考資料，38 ページ
- メモリしきい値通知の機能情報，40 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

メモリしきい値通知について

メモリしきい値通知機能は、空きメモリが設定されたしきい値を下回っていることを示す通知を送信する方法と、重要な通知を行うために十分なメモリが使用できるようにメモリを予約する方法の 2 つの方法でルータ上のメモリ不足状態を軽減します。メモリしきい値通知機能を実装するには、次の概念を理解しておく必要があります。

メモリしきい値通知

メモリしきい値通知機能を使用すると、重要な通知のためにメモリを予約し、使用可能なメモリが指定したしきい値を下回ると通知を行うようルータを設定できます。

メモリ予約

重要な動作のメモリ予約によって、イベントロギングなどの管理プロセスがルータメモリが少なくなっても機能を続行できるようにします。

メモリしきい値通知の定義方法

空きメモリ不足しきい値の設定

空きメモリ不足しきい値を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **memory free low-watermark** [**processor** *threshold*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**memory free low-watermark** [**processor** *threshold* 例： `Router(config)#` **memory free low-watermark processor 20000**	空きプロセッサメモリのしきい値を KB 単位で指定します。メモリしきい値に使用できる値を表示するには、次のコマンドを入力します。 • **memory free low-watermark processor ?**

重要な通知のためのメモリの予約

ルータがプロセスによって過負荷になると、使用可能なメモリの量が重要な通知を行うのに十分でないレベルまで落ち込む場合があります。ルータが重要な通知を行う際に使用するメモリ領域を予約するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **memory reserve critical** *kilobytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `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。
ステップ 3	**memory reserve critical** *kilobytes* 例： `Router(config)#` **memory reserve critical 1000**	ルータが重要な通知を行えるよう、キロバイトで指定したメモリの量を予約します。 • 重要な通知のために予約できるメモリの量は、使用可能なメモリ合計の 25% 以上にはできません。

メモリしきい値通知の設定例

空きメモリ不足しきい値の設定：例

空きプロセッサメモリのしきい値

次の例では、空きプロセッサ メモリ 20000 KB を、ルータが通知を行うしきい値に指定します。

```
Router(config)# memory free low-watermark processor 20000
```

使用可能な空きメモリが指定したしきい値を下回ると、ルータが次のような通知メッセージを送信します。

```
000029: *Aug 12 22:31:19.559: %SYS-4-FREEMEMLOW: Free Memory has dropped below 20000k
Pool: Processor  Free: 66814056  freemem_lwm: 204800000
```

使用可能な空きメモリがしきい値を 5 % 上回ると、ルータが次のような通知メッセージを送信します。

```
000032: *Aug 12 22:33:29.411: %SYS-5-FREEMEMRECOVER: Free Memory has recovered 20000k
Pool: Processor  Free: 66813960  freemem_lwm: 0
```

重要な通知のためのメモリの予約：例

次の例では、重要な通知用にメモリを 1000 KB 予約します。

```
Router# memory reserved critical 1000
```

（注） 重要な通知のために予約できるメモリの量は、使用可能なメモリ合計の 25% 以上にはできません。

その他の参考資料

CPU しきい値処理通知機能の詳細情報については、次の関連資料を参照してください。

関連資料

関連項目	マニュアル タイトル
SNMP トラップ	『*Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能では、新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
CISCO-PROCESS-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能では、新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

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

メモリしきい値通知の機能情報

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 *3*：メモリしきい値通知の機能情報

機能名	リリース	機能情報
メモリしきい値通知	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。

第 5 章

NTPv4 MIB

NTPv4 MIB 機能はシスコ ソフトウェアに Network Time Protocol バージョン 4（NTPv4）MIB を導入します。この機能では、NTP エンティティの現在のステータスを表すデータ オブジェクトが定義されています。これらのデータ オブジェクトへのアクセスには Simple Network Management Protocol（SNMP）が使用され、これらのデータ オブジェクトはローカル NTP エンティティの監視と管理に使用されます。

このモジュールでは、NTPv4 MIB について説明します。

- 機能情報の確認，41 ページ
- NTPv4 MIB について，42 ページ
- NTPv4 MIB の確認方法，42 ページ
- NTPv4 MIB の設定例，43 ページ
- その他の参考資料，45 ページ
- NTPv4 MIB の機能情報，46 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

NTPv4 MIB について

NTPv4 MIB

Network Time Protocol バージョン 4（NTPv4）MIB 機能では、RFC 5907 に基づき、NTP エンティティの現在のステータスを表すデータ オブジェクトが定義されています。これらのデータ オブジェクトへのアクセスには Simple Network Management Protocol（SNMP）が使用され、これらのデータ オブジェクトはローカル NTP エンティティの監視と管理に使用されます。

これらのデータ オブジェクトには NTP エンティティに関する次の情報が含まれます。

- アップストリーム NTP サーバおよびハードウェア基準クロックへの接続状態
- 製品
- ベンダー
- Version

これらのデータ オブジェクトに含まれる情報を使用すると、ネットワーク全体の時刻同期に影響が出る前に障害を検出することができます。

RFC 5907 で扱われている次のオブジェクト グループは NTPv4 MIB でサポートされています。

- ntpAssociation
- ntpEntInfo
- ntpEntStatus

RFC 5907 で扱われている次のオブジェクト グループは NTPv4 MIB でサポートされていません。

- ntpEntControl
- ntpEntNotifObjects

NTPv4 MIB の確認方法

この機能を使用するに当たって、特別な設定は必要ありません。この機能は、デフォルトでイネーブルにされています。

NTPv4 MIB の確認

NTPv4 MIB に関する情報を確認するには、次に示すコマンドのいずれか、またはすべてを任意の順序で実行します。

手順の概要

1. **show ntp associations** [**detail**]
2. **show ntp status**
3. **show ntp info**
4. **show ntp packets**

手順の詳細

ステップ 1 **show ntp associations** [**detail**]

例：
```
Device> show ntp associations detail
```
（任意）NTP アソシエーションの詳細なステータスを表示します。

ステップ 2 **show ntp status**

例：
```
Device> show ntp status
```
（任意）NTP のステータスを表示します。

ステップ 3 **show ntp info**

例：
```
Device> show ntp info
```
（任意）NTP エンティティに関する情報を表示します。

ステップ 4 **show ntp packets**

例：
```
Device> show ntp packets
```
（任意）NTP パケットに関する情報を表示します。

NTPv4 MIB の設定例

例：NTP4 MIB の確認

show ntp associations コマンドの出力例

```
Device> show ntp associations detail

172.31.32.2 configured, ipv4, our_master, sane, valid, stratum 1
```

```
ref ID .LOCL., time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 16.05
delay 0.00 msec, offset 0.0000 msec, dispersion 8.01, jitter 0.5 msec
precision 2**7, version 4
assoc ID 1, assoc name 192.0.2.1,
assoc in packets 60, assoc out packets 60, assoc error packets 0
org time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 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 =     7.81    8.05    8.29    8.53    8.77    9.01    9.25    9.49
minpoll = 4, maxpoll = 4

192.168.13.33 configured, ipv6, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 1024, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15951.96
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50,  jitter 1000.45 msec
precision 2**7, version 4
assoc ID 2, assoc name myserver
assoc in packets 0, assoc out packets 0, assoc error packets 0
org time D2351E93.2235F124 (05:56:35.133 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 IST 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 コマンドの出力例

```
Device> show ntp status

Clock is synchronized, stratum 2, reference assoc id 1, reference is 192.0.2.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**7
reference time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec, time resolution 1000 (1 msec),
root dispersion is 15.91 msec, peer dispersion is 8.01 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 6 sec ago.
system uptime (00:00:00.000) UTC,
system time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
leap time is D2352258.243DDF14 (24:00:00.000 IST Tue Dec 31 2011)
leap direction is 1
```

show ntp info コマンドの出力例

```
Device> show ntp info

Ntp Software Name: Example
NtP Software Version: ntp-1.1
Ntp Software Vendor: Example
Ntp System Type: Example_System
```

show ntp packets コマンドの出力例

```
Device> show ntp packets

Ntp In packets: 100
Ntp Out packets: 110
Ntp bad version packets: 4
Ntp protocol error packets: 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
基本的なシステム管理コマンド	『Basic System Management Command Reference』
基本的なシステム管理の設定作業	『*Basic System Management Configuration Guide*』の「Setting Time and Calendar Services」モジュール

標準および RFC

標準/RFC	タイトル
RFC 5907	『*Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)*』

MIB

MIB	MIB のリンク
NTPv4-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

NTPv4 MIB 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 *4*：*NTPv4 MIB* の機能情報

機能名	リリース	機能情報
NTPv4 MIB		NTPv4 MIB 機能はシスコ ソフトウェアに Network Time Protocol バージョン 4（NTPv4）MIB を導入します。この機能では、NTP エンティティの現在のステータスを表すデータ オブジェクトが定義されています。これらのデータ オブジェクトへのアクセスには Simple Network Management Protocol（SNMP）が使用され、これらのデータ オブジェクトはローカル NTP エンティティの監視と管理に使用されます。