NTPv4 in IPv6 の実装

Network Time Protocol（NTP; ネットワーク タイム プロトコル）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 上で動作し、UDP は IPv4 上で動作します。NTP バージョン 4（NTPv4）は、NTP バージョン 3 を拡張したもので、IPv4 と IPv6 の両方をサポートします。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「NTPv4 in IPv6 を実装するための機能情報」（P.17）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

NTPv4 in IPv6 の実装に関する情報

NTPv4 in IPv6 を設定するには、次の概念を理解する必要があります。

NTP バージョン 4

Network Time Protocol（NTP; ネットワーク タイム プロトコル）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 上で動作し、UDP は IPv4 上で動作します。NTP バージョン 4（NTPv4）は、NTP バージョン 3 を拡張したものです。NTPv4 は IPv4 と IPv6 の両方をサポートし、NTPv3 との下位互換性があります。

NTPv4 には次の機能があります。

- NTPv4 は IPv6 をサポートしているため、IPv6 上での NTP 時刻同期が可能になります。
- NTPv3 よりもセキュリティが向上されています。NTPv4 プロトコルは、公開鍵暗号法および標準の X509 証明書に基づいたセキュリティ フレームワーク全体を提供します。
- NTPv4 では、特定のマルチキャスト グループを使用して、ネットワーク全体にわたる時刻分配階層を自動的に計算できます。NTPv4 では、最小の帯域幅コストで時刻の精度を最高にするために、サーバの階層を自動的に設定します。この機能では、サイトローカル IPv6 マルチキャスト アドレスが活用されます。

NTPv4 の概要

NTPv4 の動作は、NTP の動作とほとんど同じです。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 は、「Stratum」という概念を使用して、マシンが正規の時刻源から NTP「ホップ」数にしてどれだけ離れているかを表します。「Stratum 1」タイム サーバには、通常、正規の時刻源（ラジオ クロック、アトミック クロック、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ます。それ以降も同様に続きます。

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。まず最初に、NTP は、自己同期しないマシンには同期しません。2 番めに、NTP は、複数のマシンから報告された時刻を比較し、時刻が他と大きく異なっているマシンには、Stratum の番号が下位であっても同期しません。この方針により、NTP サーバの自己編成ツリーが効率的に構築されます。

NTP のシスコ実装では、Stratum 1 サービスをサポートしていません。つまり、ラジオ クロックやアトミック クロック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 時刻源デバイスを接続できます）。

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、NTP のシスコ実装では、実際には他の手段で時刻が決定されていても、NTP を介して同期されているかのようにマシンの動作を設定できます。これにより、他のマシンが NTP を介してそのマシンに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 およびその各種派生物を実行しているシステムに公開されているバージョンも入手可能です。また、このソフトウェアを使用すると、UNIX 派生サーバはアトミック クロックから直接時刻を取得できます。そのあと、アトミック クロックによって、時刻情報が Cisco ルータに伝播されます。

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、スタティックに設定されています。つまり、各マシンには、アソシエーションの形成に関与するすべてのマシンの IPv4 アドレスまたは IPv6 アドレスが割り当てられています。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、正確なタイムキーピングが可能になります。

NTPv4 の機能

NTPv4 には次の機能があります。

- 「IPv6 マルチキャスト モード」（P.3）
- 「NTP アクセス グループと対称キー認証」（P.3）
- 「IPv6 in NTPv4 での DNS のサポート」（P.3）

IPv6 マルチキャスト モード

NTPv3 は、IPv4 ブロードキャスト メッセージを使用したクロック アップデートの送受信をサポートしています。多くのネットワーク管理者は、この機能を使用して、最小のクライアント設定で LAN に時刻を分配しています。たとえば、シスコの企業 LAN では、ローカル ゲートウェイの IPv4 上でこの機能を使用しています。エンドユーザのワークステーションは、NTP ブロードキャスト メッセージをリッスンし、それに応じて各自のクロックを同期するように設定されています。

NTPv4 for IPv6 では、クロック アップデートの送受信に、IPv4 ブロードキャスト メッセージではなく IPv6 マルチキャスト メッセージが使用されます。

NTP アクセス グループと対称キー認証

NTPv3 アクセス グループ機能は、IPv4 番号付きアクセス リストに基づいています。NTPv4 アクセス グループ機能は、IPv4 番号付きアクセス リストだけでなく、IPv6 名前付きアクセス リストも受け入れます。

NTP アクセス グループは、NTP 許可グループを Cisco IOS アクセス リストに割り当てる場合に非常に役立ちます。たとえば、サブネット内のすべてのホストを、ルータから各自のクロックの同期は行うが、クロック アップデートをルータに提供しないように設定できます。NTP アクセス グループは、Cisco IOS アクセスリスト インフラストラクチャに基づいて構築され、柔軟性の高いアクセスリスト ベースのマッチング機能を提供します。

アクセス グループは、NTP 対称キー認証より柔軟性が高く、展開が容易でありながら、同レベルのセキュリティを提供します。NTP 対称キー認証では、暗号化による強力な認証メカニズムが提供されますが、ネットワークの NTP デバイスにキーを手動で配布する必要があります。

また、異なるピアと関連付けることができる許可のタイプに関しては、NTP 対称キー認証の方がアクセス グループよりも柔軟性が低くなります。NTP 対称キー認証の主な目的は、ローカル ルータが侵入者からの誤ったクロック情報で更新されないようにすることです。

IPv6 in NTPv4 での DNS のサポート

NTPv4 は、IPv6 に対して DNS のサポートを追加します。NTPv3 は、設定時（コマンドの解析時）にホスト名を IPv4 アドレスに解決します。これにより、解決済みの IPv4 アドレスだけがメモリに残り、NVGEN 中に NVRAM に格納されます。ユーザにより指定されたホスト名は、失われます。

NTPv4 は、NVGEN 中に保存できるように、ホスト名をメモリ内に保持します。ホスト名とともに保存されている設定は、引き続き NTPv3 から読み取り可能です。

NTPv4 in IPv6 の実装方法

NTP サービスは、すべてのインターフェイスでデフォルトでディセーブルになっています。ここでは、ネットワーキング デバイスで実行可能な任意の作業について説明します。

ポーリングベースの NTPv4 アソシエーションの設定

NTPv4 を実行しているネットワーキング デバイスは、参照時刻源を使用して時刻同期を行う際に、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 デバイスがネットワークで時刻情報を取得する方法には、ホスト サーバをポーリングする方法と、NTPv4 ブロードキャストをリッスンする方法の 2 つがあります。ここでは、ポーリングベースのアソシエーション モードの設定方法について説明します。

ポーリングベースのアソシエーション モードのうち最も広く使用されているのは、次の 2 つです。

- 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 モードで動作しているネットワーキング デバイスは、割り当てられた時刻提供ホストをポーリングして現在の時刻を問い合せます。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 デバイスで同期に使用する時刻提供ホストを個別に指定し、ネットワーキング デバイスをクライアント モードで動作するように設定する場合は、**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、割り当てられた時刻提供ホストをポーリングして現在の時刻を問い合せ、ホストからの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 デバイスに関する時刻関連情報も保持します。相互に冗長な複数のサーバがダイバース ネットワーク パスを使用して相互に接続されている場合は、このモードを使用してください。現在のインターネットでは、Stratum 1 サーバおよび Stratum 2 サーバのほとんどが、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 デバイスで同期に使用する時刻提供ホストを個別に指定し、ネットワーキング デバイスを対称アクティブ モードで動作するように設定する場合は、**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、それが 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。

対称アクティブ モード

ここでは、対称アクティブ モードと呼ばれるポーリングベースのアソシエーション モードの設定方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp peer** {**vrf** *vrf-name* | *ip-address* | *ipv6 address* | **ipv4** | **ipv6** | *hostname*} [**normal-sync**][**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp peer** {**vrf** *vrf-name* | *ip-address* | *ipv6 address* | **ipv4** | **ipv6** | *hostname*}[**normal-sync**][**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**] **例：** `Router(config)# ntp peer 2001:0DB8:0:0:8:800:200C:417A version 4`	ピアを同期するように、またはピアにより同期されるようにソフトウェア クロックを設定します。

クライアント モードの設定

ここでは、クライアント モードと呼ばれるポーリングベースのアソシエーション モードの設定方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp server** {**vrf** *vrf-name* | *ip-address* | *ipv6 address* | **ipv4** | **ipv6** | *hostname*}[**normal-sync**][**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp server** {**vrf** *vrf-name* | *ip-address* | *ipv6-address* | **ipv4** | **ipv6** | *hostname*}[**normal-sync**][**version** *number*] [**key** *key-id*] [**source** *interface*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**] **例：** `Router(config)# ntp server 2001:0DB8:0:0:8:800:200C:417A version 4`	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。

マルチキャストベースの NTPv4 アソシエーションの設定

ここでは、マルチキャストベースの NTPv4 アソシエーションを設定するための次の作業について説明します。

- 「NTPv4 マルチキャスト パケットを送信するためのインターフェイスの設定」（P.6）
- 「NTPv4 マルチキャスト パケットを受信するためのインターフェイスの設定」（P.7）

NTPv4 マルチキャスト パケットを送信するためのインターフェイスの設定

NTP マルチキャスト パケットを送信するようにインターフェイスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp multicast** {*ip-address* | *ipv6-address*} [**key** *key-id*] [**ttl** *value*] [**version** *number*]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ntp multicast** {*ip-address* | *ipv6-address*} [**key** *key-id*] [**ttl** *value*] [**version** *number*] **例：** `Router(config-if)# ntp multicast FF02::1:FF0E:8C6C`	指定したインターフェイスで NTPv4 マルチキャスト パケットを送信するようにシステムを設定します。

NTPv4 マルチキャスト パケットを受信するためのインターフェイスの設定

NTPv4 マルチキャスト パケットを受信するようにインターフェイスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp multicast client** {*ip-address* | *ipv6-address*} [**novolley**]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ntp multicast client** {*ip-address* | *ipv6-address*} [**novolley**] **例：** `Router(config-if)# ntp multicast client FF02::2:FF0E:8C6C`	指定したインターフェイスで NTP マルチキャスト パケットを受信するようにシステムを設定します。

NTPv4 アクセス グループの定義

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て、特定のアクセス権限を許可または拒否できます。NTPv4 アクセス グループを定義するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} {*access-list-number* | *access-list-name*} [**kod**]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} {*access-list-number* | *access-list-name*} [**kod**] **例：** `Router(config)# ntp access-group serve acl1 kod`	システムでの NTPv4 サービスへのアクセスを制御します。

NTPv4 認証の設定

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 NTPv4 認証スキームを使用する必要があります。アクセス リストベースの制限スキームとは異なり、暗号化認証スキームでは、認証キーおよび認証プロセスを使用して、ローカル ネットワークで指定されたピアまたはサーバから送信された NTPv4 同期パケットが信頼できるかどうかを決定してから、伝送する時刻情報を受け入れます。

NTPv4 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、信頼できる時刻源だけを使用して、その時刻源との同期を行います。ネットワーキング デバイスが暗号化された同期パケットを送受信できるようにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* **md5** *value*
5. **ntp trusted-key** *key-number*

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp authenticate** **例：** `Router(config)# ntp authenticate`	NTPv4 認証をイネーブルにします。
ステップ 4	**ntp authentication-key** *number* **md5** *value* **例：** `Router(config)# ntp authentication-key 42 md5 keyname`	NTPv4 の認証キーを定義します。
ステップ 5	**ntp trusted-key** *key-number* **例：** `Router(config)# ntp trusted-key 42`	NTPv4 の同期に使用するシステムの ID を認証します。

特定インターフェイスでの NTPv4 サービスのディセーブル化

NTP および NTPv4 サービスは、すべてのインターフェイスでデフォルトでディセーブルになっています。

NTP コマンドを入力すると、NTP または NTPv4 がグローバルにイネーブルになります。選択した NTP または NTPv4 パケットを特定のインターフェイスで受信できないようにする場合は、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp disable** [**ipv4** | **ipv6**]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp disable** [**ipv4**	**ipv6**] **例：** `Router(config)# ntp disable ipv6`	システムでの NTPv4 サービスへのアクセスを制御します。

NTPv4 パケットの送信元 IPv6 アドレスの設定

システムにより NTPv4 パケットが送信されるとき、送信元 IPv6 アドレスは通常、NTPv4 パケットの送信に使用されるインターフェイスのアドレスに設定されます。IPv6 送信元アドレスとして使用する特定のインターフェイスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp source** *type number*

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp source** *type number* **例：** `Router(config)# ntp source FastEthernet 0/0`	NTPv4 パケット内で特定の送信元アドレスが使用されるように設定します。指定したインターフェイスは、IPv6 アドレスとともに設定されます。

正規の NTP サーバとしてのシステムの設定

システムを正規の NTP サーバとして設定する場合は、そのシステムを外部時刻源と同期しない場合でも、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp master** [*stratum*]

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp master** [*stratum*] **例：** `Router(config)# ntp master`	Cisco IOS ソフトウェアを NTPv4 マスター クロックとして設定します。外部の NTPv4 ソースが使用可能でない場合、ピアはこのマスター クロックに同期します。

（注） **ntp master** コマンドは慎重に使用してください。特に、下位の番号の Stratum が設定されている場合、このコマンドの使用時に有効な時刻源を上書きしてしまうことがよくあります。**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。

ハードウェア クロックの更新

ハードウェア クロック（システム カレンダー）が搭載されたデバイスでは、ハードウェア クロックを、ソフトウェア クロックから定期的に更新されるように設定できます。NTPv4 を使用しているデバイスの場合、この設定を行うことを推奨します。ハードウェア クロックの時刻設定は時間の経過とともにわずかにドリフトする可能性があるので、（NTPv4 を使用して設定された）ソフトウェア クロックの日時の方が、ハードウェア クロックよりも正確になるためです。

ルーティング デバイスが NTPv4 を介して外部時刻源と同期している場合に、ハードウェア クロックを NTPv4 時刻と同期させるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ntp update-calendar**

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **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	**ntp update-calendar** **例：** `Router(config)# ntp update-calendar`	NTPv4 時刻源からハードウェア クロック（カレンダー）を定期的に更新します。

永続データ ファイル内のドリフト値のリセット

ドリフトは、ローカル クロック ハードウェアと Network Time Protocol version 4（NTPv4; ネットワーク タイム プロトコル バージョン 4）サーバからの正規時刻との間の周波数オフセットです。NTPv4 では自動的にこのドリフトを計算し、その値を使用してローカル クロックの欠陥を永続的に補完します。永続データ ファイル内のローカル クロック ドリフト値をリセットするには、次の作業を実行します。

手順の概要

1. **enable**
2. **ntp drift clear**

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**ntp drift clear** **例：** `Router# ntp drift clear`	永続データ ファイルに格納されているドリフト値をリセットします。

NTPv4 in IPv6 のトラブルシューティング

NTPv4 in IPv6 のトラブルシューティングには、必要に応じて次の任意のコマンドを使用します。

手順の概要

1. **enable**
2. **show clock** [**detail**]
3. **show ntp associations** [**detail**]
4. **show ntp status**
5. **debug ntp** {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **refclock** | **select** | **sync** | **validity**}

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**show clock** [**detail**] **例：** `Router# show clock`	システム ソフトウェア クロックからの日時を表示します。
ステップ 3	**show ntp associations** [**detail**] **例：** `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。

	コマンドまたはアクション	目的
ステップ 4	**show ntp status** **例：** `Router# show ntp status`	NTPv4 のステータスを表示します。
ステップ 5	**debug ntp** {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **refclock** | **select** | **sync** | **validity**} **例：** `Router# debug ntp`	NTPv4 機能のデバッグ メッセージを表示します。

NTPv4 in IPv6 の設定例

ここでは、次の設定例について説明します。

- 「NTPv4 アクセス グループの定義：例」（P.14）

NTPv4 アクセス グループの定義：例

次の IPv6 の例では、NTPv4 アクセス グループがイネーブルになり、アクセスグループ ポリシーと適合しないパケットの送信を試行するホストに対して KOD パケットが送信されます。

```
Router> enable
Router# configure terminal
Router(config)# ntp access-group serve acl1 kod
```

その他の関連資料

ここでは、NTPv4 in IPv6 機能の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
NTP for IPv4	『*Performing Basic System Management*』
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする • Product Alert の受信登録 • Field Notice の受信登録 • Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

NTPv4 in IPv6 を実装するための機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(2)T または 12.0(3)S 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifies for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアル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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IPv6 で選択的パケット廃棄を実装するための機能情報

機能名	リリース	機能情報
IPv6 NTPv4	12.4(20)T	次のコマンドが導入または変更されました。**debug ntp**、**ntp access-group**、**ntp authenticate**、**ntp authentication-key**、**ntp broadcast**、**ntp broadcast client**、**ntp broadcastdelay**、**ntp disable**、**ntp drift clear**、**ntp logging**、**ntp master**、**ntp max-associations**、**ntp multicast**、**ntp multicast client**、**ntp peer**、**ntp refclock**、**ntp server**、**ntp source**、**ntp trusted-key**、**ntp update-calendar**、**show clock**、**show ntp associations**、**show ntp status**