



## **Cisco IOSXE 17 タイミングおよび同期設定ガイド（Cisco Catalyst IR8340 高耐久性シリーズ ルータ）**

**First Published:** 2023-02-10

**Last Modified:** 2023-05-22

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### Full Cisco Trademarks with Software License ?

---

#### CHAPTER 1

### クロッキングとタイミングの設定 1

クロッキングおよびタイミングの概要 1

周波数同期 2

時刻または位相の同期 2

時刻 (ToD) と 1PPS 2

IRIG-B に関する情報 3

IRIG-B の設定 4

PRTC モードと GNSS 5

---

#### CHAPTER 2

### 高精度時間プロトコル (PTP) の設定 7

Precision Time Protocol について 7

PTP を使用する理由 8

メッセージベースの同期 8

PTP イベントメッセージ シーケンス 9

境界クロックとの同期 9

ピアツーピア透過クロックとの同期 10

ローカルクロックの同期 12

ベストマスタークロック アルゴリズム 12

PTP クロック 13

グランドマスタークロック 13

通常クロック 13

境界クロック 13

透過クロック	14
PTP プロファイル	15
Default プロファイルモード	16
Power プロファイルモード	16
802.1AS プロファイル	17
PTP プロファイルの比較	19
PTP パケットのタグ付け動作	19
IR8340 ルータでサポートされる PTP クロックモード	20
設定可能な境界クロック同期アルゴリズム	20
NTP から PTP への時間変換	21
クロック マネージャ	22
GMC ブロック	24
パケットフロー	25
注意事項と制約事項	25
PTP メッセージ	25
PTP モードとプロファイル	25
パケットのフォーマット	26
VLAN の設定	26
クロックの設定	27
PTP と他の機能との相互作用	27
NTP から PTP への変換	27
デフォルト設定	27
GMC モードの設定	28
Default プロファイルの GMC モードの設定	28
Power プロファイルの GMC モードの設定	29
PTP Default プロファイルの設定	29
通常クロッククライアントの設定	29
境界クロックの設定	31
透過クロックの設定	33
PTP Power プロファイルの設定	34
通常クロックの設定	34

境界クロックの設定	36
透過クロックの設定	37
802.1AS プロファイルの設定	39
境界クロックの設定	39
PTP の無効化	40
PTP マルチドメイン	41
設定の確認	41

---

**CHAPTER 3**

<b>ネットワーク タイム プロトコルの設定</b>	<b>45</b>
ネットワーク タイム プロトコルに関する制約事項	45
ネットワーク タイム プロトコルについて	46
ネットワーク タイム プロトコル	46
ポーリング ベースの NTP アソシエーション	48
ブロードキャスト ベースの NTP アソシエーション	49
NTP アクセス グループ	49
特定のインターフェイス上の NTP サービス	50
NTP パケットの送信元 IP アドレス	50
正規の NTP サーバとしてのシステム	51
ネットワーク タイム プロトコルの設定方法	51
NTP の設定	51
ポーリング ベースの NTP アソシエーションの設定	51
ブロードキャスト ベースの NTP アソシエーションの設定	52
外部基準クロックの設定	53
NTP 認証の設定	54
ネットワーク タイム プロトコルの確認	55
ネットワーク タイム プロトコルの設定例	56
例: ネットワーク タイム プロトコルの設定	56
ネットワーク タイム プロトコルの関連資料	57
関連資料	57
標準および RFC	57
シスコのテクニカル サポート	58

ネットワーク タイム プロトコルの機能情報 58

---

**CHAPTER 4****PTP クロックに基づく NTP タイミング 59**

NTP の基準クロックとしての PTP 59

NTP の基準クロックとしての PTP の有効化 59

PTP 基準クロックの検証 60

NTP 基準クロックとしての PTP のトラブルシューティング 61

PTP-NTP 同期の確認 61

トラブルシューティング コマンド 61

ピアリングの詳細の表示 62

---

**CHAPTER 5****G.8265.1 プロファイル 63**

G.8265.1 プロファイルに関する情報 63

G.8265.1 プロファイルマッピング 64

G.8265.1 サーバーとクライアントの通常クロックの設定 65

サーバーの通常クロックの設定 65

クライアントの通常クロックの設定 68

設定の確認 70

---

**CHAPTER 6****G.8275.1 プロファイル 73**

G.8275.1 に関する情報 73

同期モデル 73

PTP ドメイン 74

PTP メッセージと転送 74

ベスト マスター クロック アルゴリズム 75

G.8275.1 プロファイルの設定 76

T-GM の設定 76

T-TSC の設定 76

T-BC の設定 76

設定の確認 77

デバッグコマンド 79

---

<b>CHAPTER 7</b>	<b>同期イーサネット ESMC と SSM の設定</b>	<b>83</b>
	同期イーサネットについて	83
	クロック選択モード	84
	同期イーサネット ESMC と SSM の設定	84

---

<b>CHAPTER 8</b>	<b>グローバルナビゲーション衛星システムの設定</b>	<b>89</b>
	GNSS に関する情報	89
	GNSS シグナリング	91
	GNSS LED	91
	注意事項と制約事項	92
	GNSS 用の衛星コンステレーションの設定	92
	設定の確認	93





# CHAPTER 1

## クロッキングとタイミングの設定

IR8340 およびルータの用語は、このドキュメント全体のテキストおよび CLI の例に使用され、特に断りのない限り、Cisco Catalyst IR8340 高耐久性シリーズ ルータを指します。

- [クロッキングおよびタイミングの概要 \(1 ページ\)](#)
- [時刻 \(ToD\) と 1PPS \(2 ページ\)](#)
- [IRIG-B に関する情報 \(3 ページ\)](#)
- [PRTC モードと GNSS \(5 ページ\)](#)

## クロッキングおよびタイミングの概要

Cisco IR8340 ルータには、周波数と時刻の同期機能があります。ルータの WAN ポート (GigabitEthernet 0/0/0 および GigabitEthernet 0/0/1) は、周波数と位相の情報を配信できます。LAN ポート (GigabitEthernet 0/1/0 ~ GigabitEthernet 0/1/11) は、位相情報のみを配信できます。IR8340 は GPS ソースに同期できます。IR8340 ルータは、外部 IRIG-B インターフェイスおよび外部 ToD RS-485 インターフェイスを介して位相を配信することもできます。

IR8340 ルータは、Cisco IOS-XE リリース 17.9.1 以降、次のタイミングポートを備えたプラグブル タイミング モジュール (Cisco PID: IRM-TIMING-MOD) をサポートしています。

- ToD + 1 PPS 出力: 時刻 (ToD) メッセージまたは 1 Pulse-Per-Second (1 PPS) メッセージを提供または受信します。
- IRIG-B (アナログおよびデジタル入出力) インターフェイス
- GNSS 受信機



(注) すべてのタイミング機能 (GNSS、IRIG-B、および G.8265.1、G.8275.1、1558v2、Power および Dot1as プロファイルなどの PTP プロファイル) をサポートするには、IR8340 で Network-Advantage のライセンスが必要です。 **license boot level network-advantage** コマンドは、Network-Advantage ライセンスを有効にします。

タイミングモジュールのステータスを表示するには、**show inventory** コマンドを使用します。

```

IR8340#show inventory
+++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++
NAME: "Chassis", DESCR: "Cisco IR8340-K9 Chassis Type"
PID: IR8340-K9      , VID: V00  , SN: FDO2523J1BL
NAME: "Power Supply Module 0", DESCR: "150W AC Power Supply Module for Cisco IR8340-K9"
PID: PWR-RGD-AC-DC-H  , VID: V01  , SN: DTH251705BY
NAME: "module 0", DESCR: "Cisco IR8340 Built-In NIM controller"
PID: IR8340-K9      , VID: V00  , SN: FDO252207UG
NAME: "Timing", DESCR: "Timing Module"
PID: IRM-TIMING-MOD      , VID: V00  , SN: FDO253409KG
NAME: "NIM subslot 0/0", DESCR: "Front Panel 2 ports Gigabitethernet Module"
PID: IR8340K9-2x1GC   , VID: V01  , SN:

```

## 周波数同期

IR8340 は、次の入力ソースのいずれかから基準クロック周波数を復元できます。

- GNSS
- SyncE
- PTP Telecom プロファイル (G.8265.1/G.8275.1)
- 局部発振器

基準クロックが選択されると、SyncE または PTP Telecom プロファイル (G.8265.1/G.8275.1) を介して下流のネットワーク要素に伝搬されます。

## 時刻または位相の同期

異なるネットワークデバイス間で時刻を正確に同期することは重要です。これは、ネットワーク遅延の計算に不可欠です。

IR8340 の時間/位相同期は、次の入力ソースのいずれかによって行われます。

- GNSS
- PTP
- IRIG-B

## 時刻 (ToD) と 1PPS

IR8340 ルータで時刻 (ToD) と 1PPS ポートを使用すると、ToD クロッキングを交換できます。デフォルトでは、GNSS がソースでロック状態の場合、ToD は UBX フォーマットです。

ToD 情報を表示するには、**show ptp wan tod** コマンドを使用します。

```

IR8340#show ptp wan tod
PTPd ToD information:

```

Time: 01/05/22 11:35:21

## IRIG-B に関する情報

Inter-Range Instrumentation Group (IRIG) タイムコードは、1950年代の終わり頃、米軍が試験場のタイミングコードを標準化する必要があったことの結果としてできたものです。この標準化により、非互換性の問題を排除し、試験場間で同期されたテストデータを交換できるようにする共通のタイムコードセットが得られました。IRIG コードの6つのバリエーション (A、B、D、E、G、H) が開発され、そのうちの IRIG タイムコード B (IRIG-B) は、電力、産業用オートメーション、および制御業界での時刻配信に広く受け入れられるようになりました。

IRIG 標準は1960年に最初に公開され、最新バージョンの IRIG 標準 200-04 『IRIG Serial Time Code Formats』は2004年9月に更新されました。IRIG-B タイムプロトコルは、システムデバイス (電源ブレーカー、リレー、メーターなど) 間で時刻の同期を確立および維持するために、電力会社やその他の業界で広く使用されています。IRIG は1秒ごとに完全なタイムフレームを送信し、各フレームは100ビットで構成されています。これには、BCD形式の時間 (time-of-year) と年の情報、および (オプションで) SBS形式の秒 (seconds-of-day) が含まれています。信頼性が高く予測可能なタイミングソース配信フレームワーク (専用タイミング信号) であると考えられていますが、伝統的に GPS などの正確なタイミングソースに依存しています。

IR8340 の IRIG プロトコルは、IRIG 標準 200-04 に準拠したフォーマット B (IRIG-B) 用に実装されており、4Xアナログ (AM) および4Xデジタル (TTL) タイムコードフォーマット (以下の表を参照) を受信 (入力) または送信 (出力) する機能を備えています。

IR8340 IRIG-B モード		フォーマット ID	IRIG 信号
アナログ (AM)	AM02	AM-B122	振幅変調、1 kHz / 1 ms 分解能、BCD <sub>TOY</sub>
	AM03	AM-B123	振幅変調、1 kHz / 1 ms 分解能、BCD <sub>TOY</sub> 、SBS
	AM06	AM-B126	振幅変調、1 kHz / 1 ms 分解能、BCD <sub>TOY</sub> 、BCD <sub>YEAR</sub>
	AM07	AM-B127	振幅変調、1 kHz / 1 ms 分解能、BCD <sub>TOY</sub> 、BCD <sub>YEAR</sub> 、SBS
デジタル (TTL)	TTL02	TTL-B002	無変調、DCLS、パルス幅符号化、BCD <sub>TOY</sub>
	TTL03	TTL-B003	無変調、DCLS、パルス幅符号化、BCD <sub>TOY</sub> 、SBS
	TTL06	TTL-B006	無変調、DCLS、パルス幅符号化、BCD <sub>TOY</sub> 、BCD <sub>YEAR</sub>
	TTL07	TTL-B007	無変調、DCLS、パルス幅符号化、BCD <sub>TOY</sub> 、BCD <sub>YEAR</sub> 、SBS



- (注)
- BCD: 通日、時、分、秒。
  - BCD\_Year: BCD に 00 ~ 99 の年を加えた形式で、世紀は符号化されません。
  - SBS: Straight Binary Seconds、0 ~ 86339。

IR8340 ハードウェアには、アナログ（AM）用に1つとデジタル（TTL）用に1つの2つの物理インターフェイスがあり、インターフェイスごとに入力または出力の信号機能を備えています。

この IRIG-B 入力/出力シグナリングのサポートにより、IR8340 は複数のユースケースで中央タイミングデバイスになることができます。

- **入力:** IR8340 は、IRIG-B 時刻源から IRIG-B タイミングシグナリング（AM または TTL）を受信します（利用可能な場合、または必要な場合のみ）。この場合、IRIG-B を PTP（のみ）の IR8340 のクロックソースとして使用できます。IR8340 は、時刻配信用のグランドマスタークロック（GMC）として設定されます。
- **出力:** IR8340 は、他の正確なタイミングソース（GNSS/GPS、PTP、NTP など）をクロックソースとして利用します。IRIG-B インターフェイスは、その場所にある IRIG-B 依存デバイスにタイミング信号を送信するために使用できます。

IR8340 は、GNSS インターフェイスに加えて、IRIG-B 入力および IRIG-B 出力をサポートします。次の表は、時刻源と時刻配信プロトコル配置のマッピングを示しています（つまり、一方が他方に対する時刻源として機能します）。

時刻源	時刻配信
IRIG-B 入力	PTP
GNSS、PTP、NTP	IRIG-B 出力

## IRIG-B の設定

インターフェイスの IRIG モード（AM または TTL）と方向（IN または OUT）を設定するには、次のコマンドを使用します。

```
[no] irig mode {TTL2|TTL3|TTL6|TTL7|AM2|AM3|AM6|AM7} dir {in | out}
```

- TTL2 = IRIG-B002、TTL3 = IRIG-B003、TTL6 = IRIG-B006、TTL7 = IRIG-B007
- AM2 = IRIG-B122、AM3 = IRIG-B123、AM6 = IRIG-B126、AM7 = IRIG-B127

IRIG 機能をインターフェイス上で無効にするには、このコマンドの **no** 形式を使用します。



(注) 入力をデジタルからアナログに、またはその逆に切り替えるには、1つのポートで入力設定を削除してから、別のポートで入力を再設定する必要があります。

**show irig** コマンドを使用すると、IR8340 の IRIG-B モードと方向の設定を表示できます。

次に、出力時の IR8340 の表示例を示します。

```
IR8340#show irig
IRIG-B Digital mode disabled
IRIG-B Analog mode AM02 dir OUT
IRIG-B Clk Id 1 Source PTP time: Year: 2021 Day: 343 Hour 8 Min 33 Sec 35. //Source can
be different based on what it's getting (can be GNSS/NTP/PTP/HANDSET/NONE).
```

```
ns 1639038815645806587 [0x16BF091E6BA52FFB]
IRIG-B Virtual Clock State: INACTIVE
*** IRIG-B input is disabled ***
```

次に、入力時の IR8340 の表示例を示します。

```
IRIG-B Digital mode disabled
IRIG-B Analog mode AM02 dir IN
IRIG-B Clk Id 5 Source IRIG-B time: Year: 2021 Day: 343 Hour 8 Min 36 Sec 25. //Because
it's IN direction, the source is IRIG-B.
ns 1639038985184125000 [0x16BF0945E4EAA048]
IRIG-B Virtual Clock State: ACTIVE
*** IRIG-B AM input mode ***
B122 : Day 343 Hour 8 Min 36 Sec 24
NOTE: Input time shown is the last received frame time
```

## PRTC モードと GNSS

IR8340 は、GNSS がロックされ、Telecom プロファイルが設定されていない場合、プライマリ リファレンス タイミング クロック (PRTC) モードで動作できます。PRTC モードでは、IR8340 は UBX フォーマットの TOD で TOD + 1pps 出力を提供します。

IR8340 が PRTC モードになると、通常クロックと透過クロックは LAN プロファイルではサポートされません。LAN プロファイルのすべての境界クロックは GMC-BC モードになり、GNSS 入力に従ってタイムスタンプとグランドマスタークロックの詳細を取得します。

次のクロック品質値が、GMC-BC マスタークロックによって提供されます。

```
Clock Quality:
Class: 6 //----GNSS CLASS
Accuracy: Within 250ns //----GNSS Accuracy
Offset (log variance): 20061 //----GNSS Variance
```

PRTC モードは、PTP Default プロファイルおよび Power プロファイルでサポートされます。この変換は、GNSS がロック状態に移行すると自動的に行われます。



(注) 次のいずれかが設定されている場合、GNSS は設定できません。

- 802.1AS
- PTP TC モード
- GMC-BC オプション





## CHAPTER 2

# 高精度時間プロトコル（PTP）の設定

PTP 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。

- [Precision Time Protocol について](#)（7 ページ）
- [GMC モードの設定](#)（28 ページ）
- [PTP Default プロファイルの設定](#)（29 ページ）
- [PTP Power プロファイルの設定](#)（34 ページ）
- [802.1AS プロファイルの設定](#)（39 ページ）
- [PTP の無効化, on page 40](#)
- [PTP マルチドメイン](#)（41 ページ）
- [設定の確認](#)（41 ページ）

## Precision Time Protocol について

Precision Time Protocol (PTP) は、IEEE 1588 で、ネットワーク化された測定および制御システムのための高精度クロック同期として定義されており、さまざまな精度と安定性の分散デバイス クロックを含むパケットベース ネットワークでクロックを同期させるために開発されました。PTP は、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP 機能を有効にしたり、ルータで CLI を実行したりするには、Network Advantage ライセンスが必要です。

ライセンスレベルを network-advantage に設定するには、次の CLI を使用します。

### license boot level network-advantage

```
Router#config terminal  
Router(config)#license boot level network-advantage  
Do you want to accept terms? Y
```

## PTP を使用する理由

ピーク時課金、仮想発電機、停電の監視/管理などのスマートグリッド電力自動化アプリケーションは、非常に正確な時刻精度と安定性を必要とします。タイミングの精度は、ネットワーク監視の精度とトラブルシューティング能力を向上させます。

時刻精度および同期の提供に加えて、PTP メッセージベースプロトコルは、イーサネットネットワークなどのパケットベースネットワークに実装することもできます。イーサネットネットワークで PTP を使用する利点は次のとおりです。

- 既存のイーサネット ネットワークでコストを削減でき、セットアップも容易
- PTP データパケットは限られた帯域幅しか必要としない

## メッセージベースの同期

クロックの同期を確保するために、PTP では、時刻送信側 (グランドマスタークロック) と時刻受信側の間の通信パス遅延を正確に測定する必要があります。PTP は、遅延の測定結果を見極めるために、時刻源と時刻受信者の間でメッセージを送信します。次に、PTP は正確なメッセージ送受信時間を測定し、これらの時間を使用して通信パス遅延を計算します。その後、PTP は、計算された遅延に対してネットワーク データに含まれる現在の時刻情報を調整し、より正確な時刻情報を生成します。

この遅延測定原理によってネットワーク上のデバイス間のパス遅延が決定され、時刻源と時刻受信者の間で送信される一連のメッセージを使用して、この遅延に関してローカルクロックが調整されます。一方向の遅延時間は、送信メッセージと受信メッセージのパス遅延を平均化することによって計算されます。この計算は対称的な通信パスを前提としていますが、スイッチドネットワークは、バッファリング プロセスのために必ずしも対称的な通信パスを持つとはかぎりません。

PTP は、透過クロックを使用し、スイッチをネットワーク上の時刻源と時刻受信者ノードに対して一時的に透過的にして、ネットワーク タイミング パケットの時間間隔フィールドの遅延を測定し、割り出す方式を提供します。エンドツーエンド透過クロックは、スイッチと同じ方法で、ネットワーク上のすべてのメッセージを転送します。

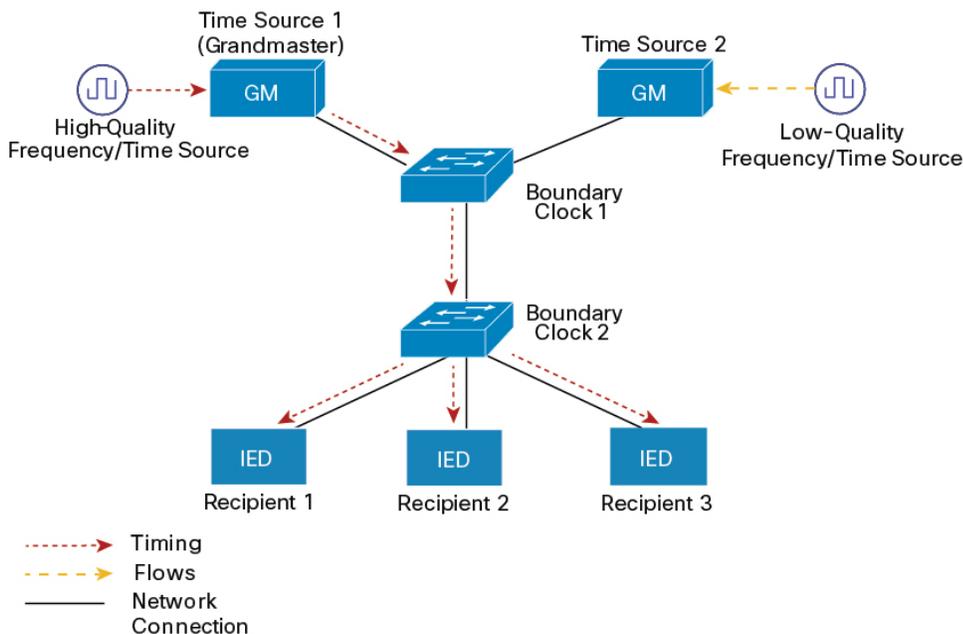


(注) Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。

同期メッセージの詳細については、[PTP イベントメッセージシーケンス \(9 ページ\)](#) を参照してください。透過クロックがネットワーク遅延を計算する方法の詳細については、[透過クロック \(14 ページ\)](#) を参照してください。

次の図に、グランドマスタークロック、境界クロックモードのスイッチ、およびデジタルリレーや保護デバイスなどのインテリジェント電子装置 (IED) を含む標準的な 1588 PTP ネットワークを示します。この図では、Time Source 1 がグランドマスタークロックです。Time Source 1 が使用できなくなった場合、時刻受信者の境界クロックは同期のために Time Source 2 に切り替わります。

図 1: PTP ネットワーク



## PTP イベントメッセージシーケンス

ここでは、同期中に発生する PTP イベントメッセージシーケンスについて説明します。

### 境界クロックとの同期

遅延要求/応答メカニズム用に設定された通常クロックと境界クロックは、次のイベントメッセージを使用してタイミング情報を生成し、伝えます。

- Sync
- Delay\_Req
- Follow\_Up
- Delay\_Resp

これらのメッセージは、次のシーケンスで送信されます。

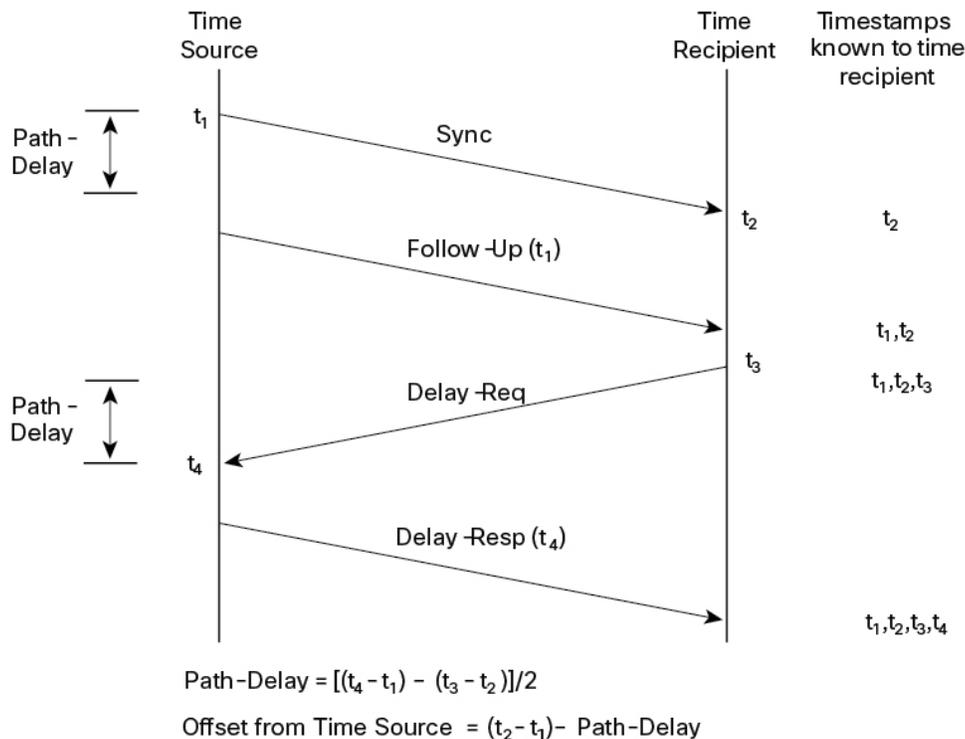
1. 時刻源が、時刻受信者に Sync メッセージを送信し、それが送信された時刻 (t1) を記録します。
2. 時刻受信者が、Sync メッセージを受信し、受信した時刻 (t2) を記録します。
3. 時刻源が、Follow\_Up メッセージにタイムスタンプ t1 を組み込むことによって、タイムスタンプ t1 を時刻受信者に伝えます。
4. 時刻受信者が、時刻源に Delay\_Req メッセージを送信し、それが送信された時刻 (t3) を記録します。

5. 時刻源が、Delay\_Req メッセージを受信し、受信した時刻 (t4) を記録します。
6. 時刻源は、タイムスタンプ t4 を Delay\_Resp メッセージに埋め込むことにより、タイムスタンプ t4 を時刻受信者に伝達します。

このシーケンスの後、時刻受信者は4つのタイムスタンプをすべて保有します。これらのタイムスタンプを使用して、時刻源に対する時刻受信者クロックのオフセットと、2つのクロック間のメッセージの平均伝達時間を計算できます。

オフセット計算は、メッセージが時刻源から時刻受信者に伝達される時間が時刻受信者から時刻源に伝達されるために必要な時間と同じであるという前提に基づいています。この前提は、非対称的なパケット遅延時間のためにイーサネット ネットワーク上では必ずしも妥当ではありません。

図 2: 詳細な手順: 境界クロック同期



## ピアツーピア透過クロックとの同期

ネットワークの階層内に複数のレベルの境界クロックが含まれており、それらの間に非 PTP 対応デバイスがある場合は、同期の精度が低下します。

ラウンドトリップ時間は  $\text{mean\_path\_delay}/2$  と等しいことが前提となっていますが、この前提はイーサネット ネットワークでは必ずしも妥当ではありません。精度を向上させるために、各中間クロックの滞留時間がエンドツーエンド透過クロックのオフセットに追加されます。ただし、滞留時間にはピア間のリンク遅延が考慮されていません。ピア間のリンク遅延はピアツーピア透過クロックによって処理されます。

ピアツーピア透過クロックは、ピア遅延メカニズムを実装する2つのクロックポート間のリンク遅延を測定します。リンク遅延は、Sync メッセージと Follow\_Up メッセージのタイミング情報を補正するために使用されます。

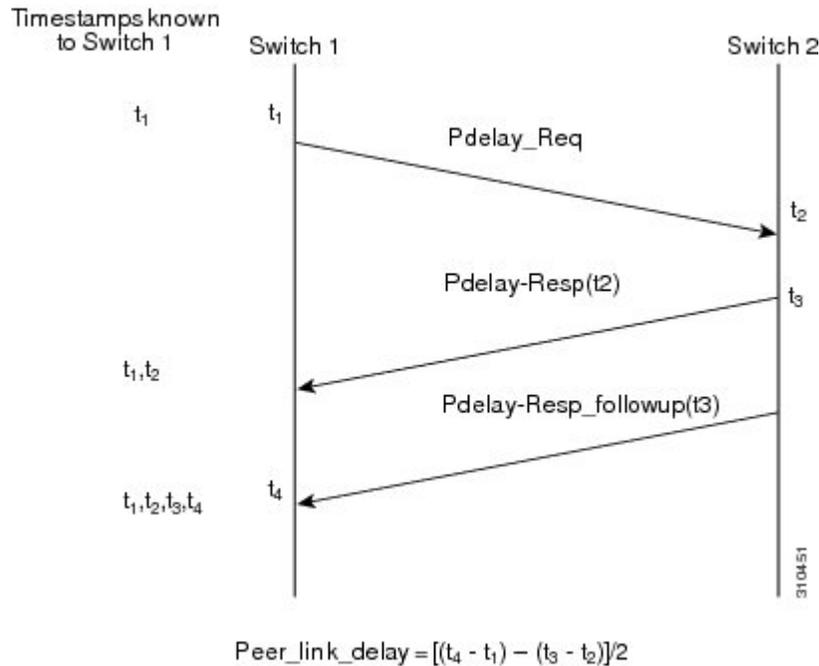
ピアツーピア透過クロックは、次のイベントメッセージを使用します。

- Pdelay\_Req
- Pdelay\_Resp
- Pdelay\_Resp\_Follow\_Up

これらのメッセージは、次のシーケンスで送信されます。

1. ポート 1 が、Pdelay\_Req メッセージのタイムスタンプ  $t_1$  を生成します。
2. ポート 2 が、このメッセージを受信してタイムスタンプ  $t_2$  を生成します。
3. ポート 2 が、Pdelay\_Resp メッセージを返してタイムスタンプ  $t_3$  を生成します。  
2つのポート間の周波数オフセットによるエラーを最小限に抑えるために、ポート 2 は、Pdelay\_Req メッセージを受信した後に、できるかぎり迅速に Pdelay\_Resp メッセージを返します。
4. ポート 2 が、Pdelay\_Resp メッセージと Pdelay\_Resp\_Follow\_Up メッセージでそれぞれタイムスタンプ  $t_2$  とタイムスタンプ  $t_3$  を返します。
5. ポート 1 が、Pdelay\_Resp メッセージを受信した後に、タイムスタンプ  $t_4$  を生成します。その後、ポート 1 が、4つのタイムスタンプ ( $t_1$ 、 $t_2$ 、 $t_3$ 、 $t_4$ ) を使用して平均リンク遅延を計算します。

図 3: 詳細な手順: ピアツーピア透過クロック同期



## ローカルクロックの同期

理想的な PTP ネットワークでは、時刻源クロックと時刻受信者クロックは同じ周波数で動作します。ただし、このネットワークでは「ばらつき」が発生する可能性があります。ドリフトは、時刻源クロックと時刻受信者クロックの周波数差です。デバイスハードウェアのタイムスタンプ情報とフォローアップメッセージ（スイッチで代行受信）を使用してローカルクロックの周波数を調整し、時刻源クロックの周波数と一致させることによって、ばらつきを補うことができます。

## ベストマスタークロック アルゴリズム

ベストマスタークロックアルゴリズム (BMCA) は PTP 機能の基盤です。BMCA は、ネットワーク上の各クロックが、そのサブドメイン内で認識できるすべてのクロック（そのクロック自体を含む）のうちで最適な時刻送信側クロックを決定する方法を指定します。BMCA はネットワーク上で継続的に動作し、ネットワーク構成における変更に対して迅速に調整します。

BMCA は、次の基準を使用して、サブドメイン内の最適な時刻送信側クロックを決定します。

- クロック品質（たとえば、GPS は最高品質とみなされます）
- クロックの時刻基準のクロック精度。
- 局部発振器の安定性
- グランドマスターに最も近いクロック

BMCAは最適な時刻送信側クロックを特定するのみでなく、次のことを保証して、PTPネットワーク上でのクロック競合の発生を確実に防止します。

- クロックが相互にネゴシエートする必要がない。
- 時刻送信側クロックの識別プロセスの結果として、時刻送信側クロックが2つある、または時刻送信側クロックがないなどの誤設定をしない。

## PTP クロック

PTP ネットワークは、PTP 対応デバイスと PTP を使用していないデバイスで構成されます。PTP 対応デバイスは、通常、次のクロック タイプで構成されます。

### グランドマスター クロック

グランドマスタークロックは、サーバーの時刻源に物理的に接続されているネットワークデバイスです。すべてのクロックはグランドマスタークロックと同期します。

PTP ドメイン内では、グランドマスタークロックが、PTP によるクロック同期の主時刻源です。グランドマスタークロックは、通常、GPS や原子時計などの非常に正確な時刻源を持っています。ネットワークが外部時刻リファレンスを必要とせず、内部で同期する必要のみがある場合、グランドマスタークロックはフリーランできます。

### 通常クロック

通常クロックは、単一の PTP ポートを持つ 1588 クロックで、次のいずれかのモードで動作できます。

- サーバーモード：ネットワーク経由で1つまたは複数のクライアントクロックにタイミング情報を配信します。その結果、クライアントはクロックをサーバーに同期させることができます。
- クライアントモード：クロックをサーバークロックに同期させます。2つの異なるサーバークロックに接続するために、最大2つのインターフェイスでクライアントモードを同時に有効にできます。

通常クロックは、同期が必要なデバイスに接続されているネットワーク上のエンドノードとして使用されるため、PTP ネットワーク上で最も一般的なクロックタイプです。

### 境界クロック

PTP ネットワークにおける境界クロックは、標準のネットワークにおけるスイッチやルータに代わる動作をします。境界クロックには複数の PTP ポートがあり、各ポートは個別の PTP 通信パスへのアクセスを提供します。境界クロックは、PTP ドメイン間のインターフェイスを提供します。このクロックは、すべての PTP メッセージを代行受信して処理し、他のすべてのネットワークトラフィックを通過させます。また、境界クロックは、BMCA を使用して、任意のポートから見えるクロックから最善のものを選択します。選択したポートは非マスターモードに設定されます。

マスターポートは下流に接続されたクロックを同期させ、非マスターポートは上流のマスタークロックと同期します。

## 透過クロック

PTP ネットワークの透過クロックの役割は、PTP イベントメッセージの一部である時間間隔フィールドを更新することです。この更新により、スイッチの遅延が補われ、1 ピコ秒未満の精度が実現されます。

次の 2 種類の透過クロックがあります。

**エンドツーエンド (E2E) 透過クロック**は、SYNC メッセージと DELAY\_REQUEST メッセージに関して PTP イベントメッセージ中継時間（「滞留時間」とも呼ばれる）を測定します。この測定された中継時間は、対応するメッセージのデータフィールド（補正フィールド）に追加されます。

- SYNC メッセージの測定された中継時間は、対応する SYNC メッセージまたは FOLLOW\_UP メッセージの補正フィールドに追加されます。
- DELAY\_REQUEST メッセージの測定された中継時間は、対応する DELAY\_RESPONSE メッセージの補正フィールドに追加されます。

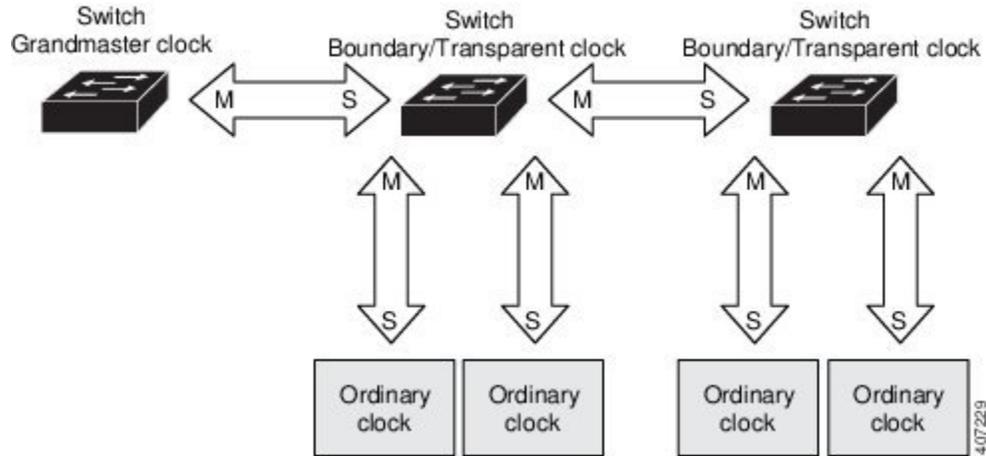
時刻受信側は、時刻受信側の時刻と時刻送信側の時刻間のオフセットを決定するときにこの情報を使用します。E2E 透過クロックは、リンク自体の伝播遅延は補正しません。

**ピアツーピア (P2P) 透過クロック**は、前述のように、E2E 透過クロックと同じ方法で PTP イベントメッセージ中継時間を測定します。さらに、P2P 透過クロックは上流リンク遅延を測定します。上流リンク遅延は、上流の隣接する P2P 透過クロックと考慮対象の P2P 透過クロックの間の推定パケット伝搬遅延です。

これらの 2 つの時間（メッセージ中継時間と上流リンク遅延時間）は両方とも PTP イベントメッセージの補正フィールドに追加され、時刻受信者によって受信されるメッセージの補正フィールドにはすべてのリンク遅延の合計が含まれます。理論的には、これは、SYNC パケットのエンドツーエンドの遅延の合計（時刻源から時刻受信者まで）です。

次の図に、PTP ネットワーク内の時刻源/時刻受信者階層に含まれる PTP クロックを示します。

図 4: PTP クロック階層



## PTP プロファイル

ここでは、ルータ上で使用できる次の PTP プロファイルについて説明します。

- Default プロファイル
- Power プロファイル
- 802.1AS プロファイル

Cisco IOS-XE リリース 17.7.1 は、Power プロファイル 2011 をサポートします。これは、PC37.238-2011: 電力システムアプリケーションでの IEEE 1588 Precision Time Protocol の使用に関する IEEE ドラフト標準プロファイルで定義されています。このマニュアルでは、この IEEE 1588 プロファイルおよび関連設定値を参照する際に、Power プロファイルモードと Default プロファイルモードという用語を使用します。

Cisco IOS-XE リリース 17.8.1 以降、Power プロファイル 2011 と Power プロファイル 2017 の 2 つの Power プロファイルがサポートされています。Power プロファイル 2017 は、電力システムアプリケーションでの IEEE 1588 Precision Time Protocol の使用に関する IEEE 標準 C37.238™-2017 (IEEE Std C37.238-2011 の改訂版) で定義されています。

PTP プロファイルの IEEE 1588 定義は、「デバイスに適用可能な、許容される一連の PTP 機能」です。PTP プロファイルは、通常、特定のタイプのアプリケーションまたは環境に固有のものであり、次の値を定義します。

- ベストマスタークロック アルゴリズム オプション
- 設定管理オプション
- パス遅延メカニズム (ピア遅延または遅延要求/応答)
- すべての PTP 設定可能属性およびデータ セット メンバーの範囲とデフォルト値
- 必要な、許可される、または禁止されるトランスポート メカニズム

- 必要な、許可される、または禁止されるノードタイプ
- 必要な、許可される、または禁止されるオプション

## Default プロファイルモード

ルータのデフォルトの PTP プロファイルモードは、Default プロファイルモードです。このモードでは、次のようになります。

- IR8340 は、Default プロファイルで通常クロック (OC) スレーブ、境界クロック (BC)、および透過クロック (TC) をサポートします。
- IR8340 は OC マスターをサポートしません。
- バンドルまたはポートチャネルでのすべての PTP プロファイルは、IR8340 ではサポートされていません。

## Power プロファイルモード

IEEE Power プロファイルは、変電所で使用される PTP ネットワークの特定の値または許容値を定義します。定義される値には、最適な物理層、PTP メッセージ用のより高位のプロトコル、および優先されるベストマスタークロックアルゴリズムが含まれます。Power プロファイルの値は、変電所内、変電所間、および広い地理的領域にわたる一貫した信頼性のあるネットワーク時刻配信を保証します。

ルータは、次の方法で PTP 用に最適化されます。

- **ハードウェア:** ルータは PTP 機能のために FPGA と PHY を使用します。PHY は、ファストイーサネットポートとギガビットイーサネットポートにタイムスタンプを付与します。
- **ソフトウェア:** Power プロファイルモードでは、ルータは、IEEE 1588 Power プロファイル標準で定義されている設定値を使用します。

次の表に、IEEE 1588 Power プロファイルで定義されている設定値と、ルータが各 PTP プロファイルモードで使用する値を示します。

表 1: IEEE PTP Power プロファイルとルータモードの設定値

PTP フィールド	ルータ設定値	
	Power プロファイルモード	Default プロファイルモード

PTP フィールド	ルータ設定値	
メッセージ伝送	<p><b>アクセスポート:</b> タグなしレイヤ2パケット。</p> <p><b>トランクポート:</b> 802.1Qタグ付きレイヤ2パケット。PTPパケットはPTP VLANでタグ付けされます。PTP VLANが設定されていない場合、パケットはネイティブ VLAN上でタグなしになります。</p>	レイヤ3パケット。デフォルトでは、802.1qタグリングは無効になっています。
<b>MAC アドレス:</b> 非ピア遅延メッセージ	01-00-5e-00-01-81.	Default プロファイルは、すべての PTP メッセージに L3 トランスポート マルチキャスト アドレス 224.0.1.129 を使用します。同等の MAC アドレスは 01-00-5e-00-01-81 です。
<b>MAC アドレス:</b> ピア遅延メッセージ	01-80-C2-00-00-0E.	このモードには適用されません。
ドメイン番号	0.	0.
パス遅延計算	peer_delay メカニズムを使用するピアツーピア透過クロック。	delay_request メカニズムを使用するエンドツーエンド透過クロック。
BMCA	有効。	有効。
クロック タイプ	2 ステップ。	2 ステップ。
時間スケール	エポック。	エポック。
グランドマスター ID とローカル時刻の決定	グランドマスター ID を示す PTP 固有の TLV。	グランドマスター ID を示す PTP 固有のタイプ、長さ、値。
ネットワークホップを超えた時刻精度	16 ホップで、スレーブ デバイス同期精度は 1 usec (1 マイクロ秒) 未満です。	このモードでは適用されません。

## 802.1AS プロファイル

IEEE 802.1AS 標準規格『Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks』では、ブリッジ型および仮想ブリッジ型のローカルエリアネットワーク全体に時間的制約のあるアプリケーションの同期要件を確実に満たすために使用するプロトコルとプロシージャが規定されています。

802.1AS では、IEEE Std 802.1D-2004 と IEEE Std 802.1Q-2005.1 に照らして適用可能な場合に IEEE 1588 (PTP) 仕様を使用することが規定されています。802.1AS 標準規格は、3つの 802.1 AVB ド

ラフト標準規格の1つです。イーサネットでの802.1AS (802.3) は、IEEE 1588-2008のプロファイルとして認定されています。これは、IEEE 1588を簡素化し、さまざまなタイプのメディアでの同期を定義するものです。



(注) 802.1 AS は、IR8340 プラットフォームでのみドメイン 0 で設定できます。

802.1AS の主要な特徴は次のとおりです。

- イーサネット全二重リンクでは、ピア遅延メカニズムを使用します。
- ドメイン内のすべてのデバイスは、802.1AS 対応である必要があります。
- 802.1AS パケットの転送は VLAN タグが付されていない L2 マルチキャストのみです。
- これには2段階の処理が必要です (Follow\_Up メッセージと Pdelay\_Resp\_Follow\_Up メッセージを使用してタイムスタンプを伝えます)。
- 時間認識型ネットワークにはアクティブなグランドマスターが1つのみ存在します。つまり、802.1AS ドメインは1つのみです。
- BMCA (ベストマスタークロックアルゴリズム) は、次の例外を除き、IEEE 1588 で使用されているものと同じです。
  - 受信側の時刻認識型システムが送信したものではないアナウンスメッセージが時刻受信側ポート上で受信されると、そのメッセージはただちに使用されます。つまり、外部時刻送信側の認定はありません。
  - BMCA が時刻送信側ポートであると判断したポートはただちに時刻送信側の状態になります。つまり、時刻送信側より前の状態はありません。
  - キャリブレーションされていない状態は必要ないため、使用されません。
  - すべての時刻認識型システムは、(システムがグランドマスターに対応していない場合でも) 適切なマスターの選択に加える必要があります。

802.1AS は Time Sensitive Network (TSN) 機能で使用されます。ただし、正確なタイミング配分メカニズムとして、802.1AS は TSN の設定や入力なしで単独で動作します。802.1AS 機能ソフトウェアの実装は、FPGA の既存のタイムスタンプ機能に基づいており、ハードウェアに対する他の PTP プロファイルにはない新しい要件はありません。

802.1AS のエンドツーエンドの時刻同期性能は次のとおりです。

- 6つ以下の時刻認識型システム (つまり、7ホップ以下) で分離された2つの時刻認識型システムは、定常状態で動作中はピークツーピーク 1  $\mu$ s の以内で相互に同期されます。
- 7ホップを超える性能は定義されていません。

## PTP プロファイルの比較

表 2: IE スイッチの PTP プロファイルの比較

プロファイル	Default (*)		Power プロファイル 2011		Power プロファイル 2017	802.1AS
標準 (Standard)	IEEE1588 v2 (J.3)		IEEE C37.238-2011		IEEE C37.238-2017	IEEE802.1AS
モード	境界	エンドツーエンド透過	境界	ピアツーピア透過	ピアツーピア透過	**
パス遅延	遅延要求/応答	遅延要求/応答	ピア遅延要求/応答	ピア遅延要求/応答	ピア遅延要求/応答	ピア遅延要求/応答
PTP ドメイン内での PTP 以外のデバイスの許容	対応	対応	非対応	非対応	非対応	非対応
伝送方式	UDP over IP (マルチキャスト)		L2 マルチキャスト		L2 マルチキャスト	L2 マルチキャスト

\* Default PTP プロファイル遅延要求/応答 (IEEE1588 J.3 で定義)。

\*\* 802.1AS のモード設定はありません。数学的に、これは P2P 透過と同等ですが、透過クロックとは動作が異なります。

## PTP パケットのタグ付け動作

次の表に、Power プロファイルモードと Default プロファイルモードでのスイッチタグ付け動作を示します。

表 3: PTP パケットのタグ付け動作

スイッチポートモード	設定	Power プロファイルモード		Default プロファイルモード	
		動作	優先度	動作	優先度
トランクポート	<b>vlan dot1q tag native enabled</b>	スイッチがパケットをタグ付け	7	スイッチがパケットをタグ付け	7
トランクポート	<b>vlan dot1q tag native disabled</b>	PTP ソフトウェアがパケットをタグ付け	4	タグなし	なし

スイッチポートモード	設定	Power プロファイルモード		Default プロファイルモード	
アクセスポート	該当なし	タグなし	なし	タグなし	なし

## IR8340 ルータでサポートされる PTP クロックモード

PTP 同期動作は、ルータで設定する PTP クロックモードによって異なります。ルータは次のいずれかのグローバルモードに設定できます。

各クロックモードの設定のガイドラインについては、[注意事項と制約事項 \(25 ページ\)](#) を参照してください。

IR8340 は、次の PTP デバイスタイプをサポートします。

- Default プロファイル/IEEE 1588 の OC スレーブ、境界クロック、および透過クロック。
- Power プロファイルの境界クロックと透過クロック。
- Dot1as プロファイルの境界クロック。



(注) 現在、上記のプロファイルはすべて 2 ステップモードをサポートしていますが、IR8340 では 1 ステップモードをサポートしていません。

## 設定可能な境界クロック同期アルゴリズム

入力時刻エラーのフィルタリングと迅速な収束のどちらを優先させる必要があるかに応じて、さまざまな PTP 使用例に対応するように BC 同期アルゴリズムを設定できます。パケット遅延変動 (PDV) をフィルタリングする PTP アルゴリズムは、フィルタリングしない PTP アルゴリズムより収束に時間がかかります。

デフォルトでは、BC は線形フィードバックコントローラ (つまりサーボ) を使用して BC の時刻出力を次のクロックに設定します。線形サーボは、少量の PDV フィルタリングを提供し、平均時間内に収束します。BC は、収束時間を改善するために、TC フィードフォワードアルゴリズムを使用して、ネットワーク要素フォワーディングプレーン (外乱) によって加えられた遅延を測定し、その測定された遅延を使用して時刻出力を制御することができます。

フィードフォワード BC により境界クロックが劇的に迅速化されますが、フィードフォワード BC は PDV をフィルタリングしません。適応型 PDV フィルタは、PTP をサポートせず、PDV を大幅に増加させるワイヤレス アクセス ポイント (AP) およびエンタープライズスイッチ間で、PDV が存在する場合の高品質の時刻同期を実現します。

BC 同期には次の 3 つのオプション (すべて IEEE 1588-2008 に準拠) があります。

- フィードフォワード: 非常に迅速かつ正確な収束を実現します。PDV フィルタリングはありません。

- 適応型: PDV 特性、ハードウェア構成、および環境条件に関する一連の仮定を考慮し、可能な限り多くの PDV をフィルタリングします。



(注) 適応型フィルタを使用する場合、スイッチは、ITU-TG.8261 で規定されている時間性能要件を満たしません。

- 線形: 単純な線形フィルタリングを提供します (デフォルト)。

適応型モード (**ptp transfer filter adaptive**) は、Power プロファイルモードでは使用できません。

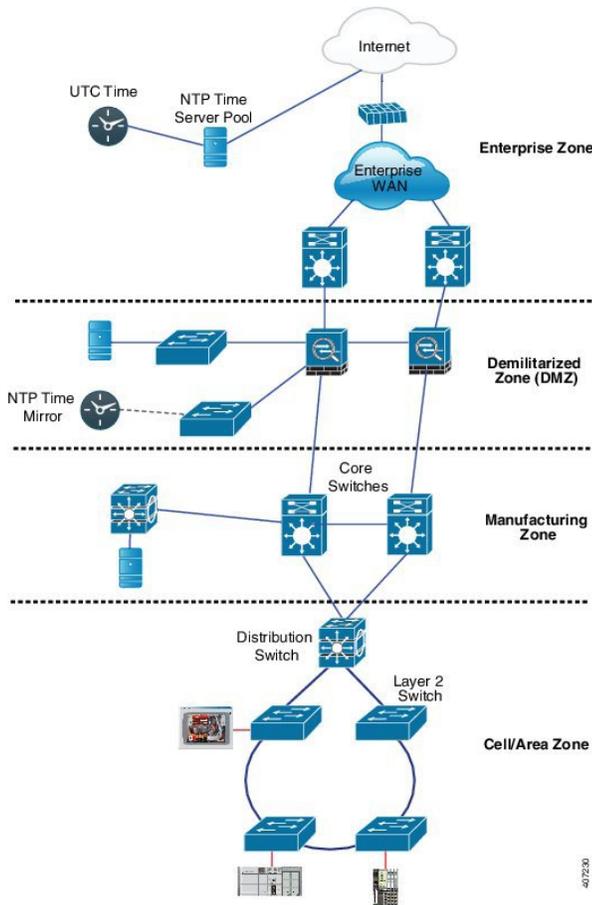
## NTP から PTP への時間変換

NTP から PTP への時刻変換機能により、Network Time Protocol (NTP) を PTP の時刻源として使用できます。サイト内で非常に正確な同期を実現するために PTP を使用するお客様は、正確な同期を必要としないサイト間で NTP を使用できます。

NTP は、パケットベースネットワーク間でクロックを同期させる従来の方法です。NTP は、時刻源とエンドデバイス間で双方向の時間転送メカニズムを使用します。NTP を使用すると、インターネットを介して数百ミリ秒以内に、緊密に制御された LAN では数ミリ秒以内にデバイスを同期させることができます。PTP の時刻源として NTP を使用できることで、お客様は、PTP ネットワークで生成されるデータと NTP が動作しているエンタープライズデータセンターのデータを関連付けることができます。

次の図に、産業自動化および制御システムリファレンスモデルに基づく産業ネットワークの例を示します。企業ゾーンと緩衝地帯では NTP が動作しており、製造ゾーンとセル/エリアゾーンでは NTP を時刻源として PTP が動作しています。NTP から PTP への変換機能を持つスイッチは、セル/エリアゾーン内のレイヤ 2 スイッチまたはディストリビューションスイッチのいずれかになります。

図 5: NTP と PTP を使用した産業ネットワーク



## クロック マネージャ

クロック マネージャは、NTP を PTP に変換するシスコのソフトウェア アーキテクチャに含まれるコンポーネントで、さまざまなタイム サービスを継続的に追跡し、時刻をアクティブに提供するクロックを選択します。クロック マネージャは、状態の変化、うるう秒、サマータイムといった重要な変化をタイム サービスに通知します。

また、クロック マネージャは、最初に NTP または手動設定のクロックを選択し、NTP がアクティブでなければ、その後に PTP およびリアルタイムクロックを選択します。次の表に、クロック 選択プロセスの結果を示します。

表 4: タイム サービスの選択

NTP (アクティブ) または手動設定	PTP (アクティブ)	リアルタイムクロック	選択される出力
True	考慮しない	考慮しない	NTP または手動設定
False	True	考慮しない	PTP

NTP (アクティブ) または手動設定	PTP (アクティブ)	リアルタイム クロック	選択される出力
False	False	True	リアルタイム クロック

一般に、クロックマネージャは、Cisco IOS コマンドの `show ptp lan clock` と `show clock` によって表示される時刻が一致することを保証します。`show clock` コマンドは常に上記の優先順位に従いますが、`show ptp lan clock` の時刻は、次の2つの例外的な状況下で異なる可能性があります。

- ルータがTCまたはBCのいずれかであり、ネットワーク上に他のアクティブなリファレンスが存在しない。下位互換性を保持するために、TCとBCはクロックマネージャから時刻を取得せず、ネットワークのPTP GMCからのみ時刻を取得する。アクティブなPTP GMCが存在しない場合、`show clock` コマンドと `show ptp lan clock` コマンドの出力で表示される時刻が異なる可能性がある。
- ルータが、同調元のTC、スレーブポートを持つBC、またはスレーブポートを持つGMC-BCであり、PTP GMCによって提供される時刻が、NTP またはユーザー（つまり手動設定）によって提供される時刻と一致しない。この場合、PTP クロックはPTP GMCからの時刻を転送する必要がある。PTP クロックがPTP GMCに従わない場合、PTP ネットワークには2つの異なる時刻基準が存在することになり、PTP を使用するイベントアプリケーションの制御ループまたはシーケンスが破綻する。

次の表に、Cisco IOS および PTP クロックがさまざまな設定でどのように動作するかを示します。ほとんどの場合、2つのクロックは一致します。ただし、場合によっては2つのクロックが異なります。それらの設定は、表で強調表示されています。

表 5: 予期される時刻フロー

IOS クロックの設定	PTP クロックの設定	IOS クロックのソース	PTP クロックのソース
カレンダー	BC モードの PTP BC、E2E TC、または GMC-BC	PTP	PTP
手動	BC モードの PTP BC、E2E TC、または GMC-BC	手動	PTP
NTP	BC モードの PTP BC、E2E TC、または GMC-BC	NTP	PTP
カレンダー	GM モードの GMC-BC	カレンダー	カレンダー
手動	GM モードの GMC-BC	手動	手動
NTP	GM モードの GMC-BC	NTP	NTP

## GMC ブロック

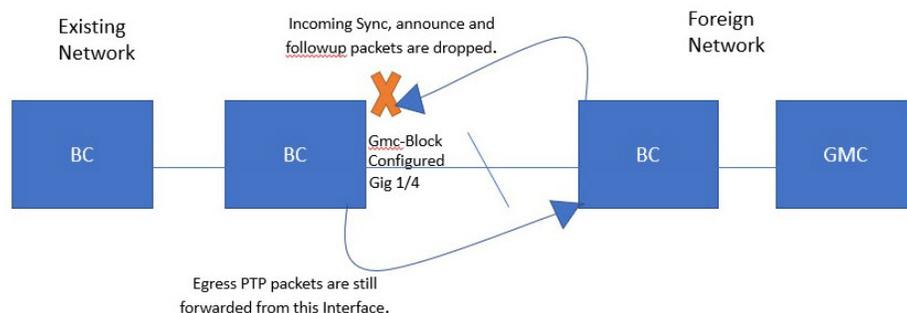
GMC ブロックは、ネットワーク内のデバイスと同期しようとする不正な GMC から既存のネットワークを保護します。この機能は、転送モードを除くすべての PTP クロックモードでサポートされます。インターフェイスでこの機能を有効にすると、送出されるアナウンス、同期、およびフォローアップの PTP パケットのみが許可され、すべての流入するアナウンス、同期、およびフォローアップのパケットがこのインターフェイスで破棄されます。これにより、ポート状態が時刻受信側へ遷移してしまうことが防止されます。

不正な GMC に関する情報は、パケットを破棄する前にパケットから取得します。ただし、このインターフェイスからの出力 PTP パケットは引き続き許可されるため、GMC として機能できません。不正デバイスを特定するために、IP アドレスやクロック ID などの詳細がそのインターフェイスを対象に保存され、表示されます。また、2 つの Syslog メッセージが生成され、不正デバイスの存在と除去を通知します。

複数の外部ネットワークが既存のシステムに接続されている疑いがある場合は、複数のポートで PTP gmc-block を設定できます。ポート単位の Syslog メッセージは、不正パケットを受信してから 30 秒後と、パケットの受信が停止してから 180 ~ 240 秒後に表示されます。リレーマイナーアラームと SNMP トラップも生成され、外部の不正デバイスの存在を通知します。

### パケットフロー

次の図に、インターフェイスに GMC ブロック機能が設定された PTP ネットワークトポロジの例を示します。

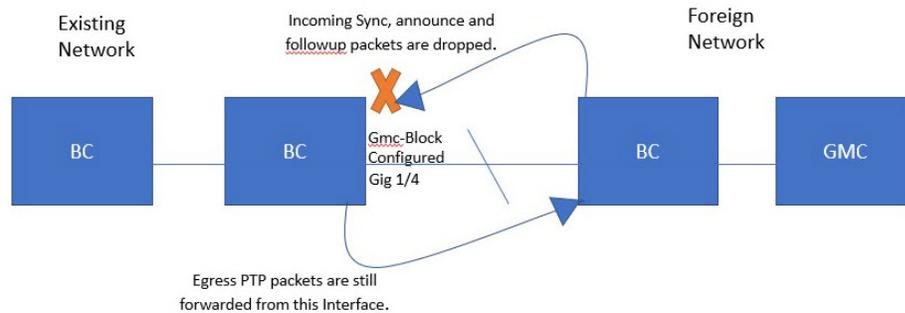


PTP パケットは、既存のネットワークと同期しようとする外部ネットワークの GMC から発信されます。GMC ブロックが設定されたポートに PTP パケットが到達すると、システムがパケットから必要な情報を取得した後にそれらのパケットは破棄されます。

外部ネットワークからのパケットは制限されているため、システムは既存のシステム内に存在するローカル GMC と同期します。GMC ブロックが設定されているポートから発信される PTP パケットは、このインターフェイスからの出力が引き続き許可されます。そのため、既存のネットワーク内のデバイスを GMC にすることができます。

## パケットフロー

次の図に、インターフェイスに GMC ブロック機能が設定された PTP ネットワークトポロジの例を示します。



PTP パケットは、既存のネットワークと同期しようとする外部ネットワークの GMC から発信されます。GMC ブロックが設定されたポートに PTP パケットが到達すると、システムがパケットから必要な情報を取得した後にそれらのパケットは破棄されます。

外部ネットワークからのパケットは制限されているため、システムは既存のシステム内に存在するローカル GMC と同期します。GMC ブロックが設定されているポートから発信される PTP パケットは、このインターフェイスからの出力が引き続き許可されます。そのため、既存のネットワーク内のデバイスを GMC にすることができます。

## 注意事項と制約事項

### PTP メッセージ

- Cisco PTP の実装では、2 ステップ クロックのみがサポートされ、1 ステップ クロックはサポートされません。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。

### PTP モードとプロファイル

- ルータとグランドマスタークロックは、同じ PTP ドメイン内にある必要があります。
- Power プロファイルモードが有効になっている場合、ルータは、*Organization\_extension* と *Alternate\_timescale* の 2 つのタイプ、長さ、値 (TLV) メッセージ拡張を含まない PTP アナウンスメッセージを破棄します。

グランドマスタークロックが PTP に準拠しておらず、これらの TLV なしでアナウンスメッセージを送信する場合は、次のコマンドを入力して、アナウンスメッセージを処理するようにルータを設定します。

```
ptp clock boundary domain 1 profile power
allow-without-tlv
```

- ルータが Power プロファイルモードになっている場合は、peer\_delay メカニズムのみがサポートされます。

Power プロファイル境界モードを有効にし、clock-port サブオプションを使用してインターフェイスを関連付けるには、次のコマンドを入力します。

```
ptp clock boundary domain 1 profile power
clock-port 1
transport ethernet multicast interface gi0/1/1
```

- Power プロファイル透過モードを無効にするには、次のコマンドを入力します。これにより、ルータは転送モードに戻ります。

```
no ptp clock transparent domain x profile power
```

- E2E 透過クロックを有効にするには、次のコマンドを使用します。

```
ptp clock transparent domain x profile default
```

- Default プロファイルモードでは、delay\_request メカニズムのみがサポートされます。

Default プロファイル境界クロックモードと、clock-port サブオプションに関連付けられたインターフェイスを有効にするには、次のコマンドを入力します。

```
ptp clock boundary domain 1 profile default
clock-port 1
transport ipv4 multicast interface gi0/1/1
```

- 802.1AS プロファイルにはクロックモード設定がありません。

## パケットのフォーマット

- PTP メッセージのパケットフォーマットには、802.1q タグ付きパケットまたはタグなしパケットを使用できます。
- ルータは 802.1q QinQ トンネリングをサポートしていません。
- Power プロファイルモードでは、次のようになります。
  - PTP インターフェイスがアクセスポートとして設定されている場合、PTP メッセージはタグなしのレイヤ 2 パケットとして送信されます。
  - PTP インターフェイスがトランクポートとして設定されている場合、PTP パケットはポートネイティブ VLAN で 802.1q タグ付きレイヤ 2 パケットとして送信されます。
- 時刻受信者 IED はタグ付きパケットとタグなしパケットをサポートする必要があります。
- PTP パケットが E2E 透過クロックモードのネイティブ VLAN で送信される場合、それらはタグなしパケットとして送信されます。タグ付きパケットとして送信するようにスイッチを設定するには、グローバルコマンドの **vlan dot1q tag native** を入力します。

## VLAN の設定

- トランクポートで PTP VLAN を設定します。範囲は 1 ~ 4094 です。デフォルトは、トランクポートのネイティブ VLAN です。

- 境界モードでは、PTP VLAN 内の PTP パケットのみが処理され、他の VLAN からの PTP パケットは破棄されます。
- インターフェイスで PTP VLAN を設定する前に、PTP VLAN を作成し、トランクポートで許可する必要があります。
- ほとんどのグランドマスター クロックは、デフォルトの VLAN 0 を使用します。Power プロファイルモードでは、ルータのデフォルト VLAN は VLAN 1 で、VLAN 0 は予約されています。デフォルトのグランドマスター クロック VLAN を変更する場合は、0 以外の VLAN に変更する必要があります。
- グランドマスター クロックで VLAN が無効になっている場合は、PTP インターフェイスをアクセス ポートとして設定する必要があります。

## クロックの設定

- すべての PHY PTP クロックはグランドマスター クロックと同期します。ルータシステム クロックは、PTP 設定およびプロセスの一部として同期しません。
- グランドマスター クロックで VLAN が有効になっている場合、グランドマスター クロックは、ルータ上の PTP ポートのネイティブ VLAN と同じ VLAN にある必要があります。
- グランドマスター クロックで VLAN が設定されている場合、グランドマスター クロックはタグなし PTP メッセージを破棄できます。ルータにタグ付きパケットをグランドマスター クロックに強制的に送信させるには、グローバルコマンドの `vlan dot1q tag native` を入力します。

## PTP と他の機能との相互作用

- IR8340 は、ポートチャネルでの PTP をサポートしていません。
- 次の PTP クロック モードは、単一の VLAN 上でのみ動作します。
  - e2transparent
  - p2transparent

## NTP から PTP への変換

- NTP から PTP への機能は、Default E2E プロファイルと Power プロファイルをサポートします。

## デフォルト設定

- ルータでは PTP がデフォルトで有効になっています。
- デフォルトでは、ルータは Default プロファイルで定義されている設定値を使用します (Default プロファイルモードが有効になっています)。

- ルータのデフォルトの PTP クロックモードは、E2E 透過クロック モードです。
- デフォルトの BC 同期アルゴリズムは、線形フィルタです。

## GMC モードの設定

次のセクションでは、Default プロファイルおよび Power プロファイルの GMC モードを設定する手順について説明します。

### Default プロファイルの GMC モードの設定

Default プロファイルの GMC モードを設定する手順は、次のとおりです。

#### SUMMARY STEPS

1. **ptp clock boundary domain *domain-number* profile default**
2. **gmc-bc default**
3. **clock-port *port-name***
4. **transport ipv4 multicast *interface-type interface-number***

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>ptp clock boundary domain <i>domain-number</i> profile default</b>  <b>Example:</b> router(config)# <b>ptp clock boundary domain 0 profile default</b>	Default プロファイル境界モードを有効にします。
Step 2	<b>gmc-bc default</b>  <b>Example:</b> router(config-ptp-clk)# <b>gmc-bc default</b>	GMC 境界クロックを有効にします。
Step 3	<b>clock-port <i>port-name</i></b>  <b>Example:</b> router(config-ptp-clk)# <b>clock-port port1</b>	新しいクロックポートを定義します。
Step 4	<b>transport ipv4 multicast <i>interface-type interface-number</i></b>  <b>Example:</b> router(config-ptp-port)# <b>transport ipv4 multicast interface Gi0/1/1</b>	クロックトラフィックの転送メカニズムを指定します。

## Power プロファイルの GMC モードの設定

Power プロファイルの GMC モードを設定するには、このセクションの手順を実行します。

### SUMMARY STEPS

1. `ptp clock boundary domain domain-number profile power`
2. `gmc-bc default`
3. `clock-port port-name`
4. `transport ethernet multicast interface-type interface-number`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>ptp clock boundary domain domain-number profile power</b></p> <p><b>Example:</b></p> <pre>router(config)# ptp clock boundary domain 0 profile power</pre>	Power プロファイル境界モードを有効にします。
Step 2	<p><b>gmc-bc default</b></p> <p><b>Example:</b></p> <pre>router(config-ptp-clk)# gmc-bc default</pre>	GMC 境界クロックを有効にします。
Step 3	<p><b>clock-port port-name</b></p> <p><b>Example:</b></p> <pre>router(config-ptp-clk)# clock-port port1</pre>	新しいクロックポートを定義します。
Step 4	<p><b>transport ethernet multicast interface-type interface-number</b></p> <p><b>Example:</b></p> <pre>router(config-ptp-port)# transport ethernet multicast interface gi0/1/1</pre>	クロックトラフィックの転送メカニズムを指定します。

## PTP Default プロファイルの設定

ここでは、ルータを Default プロファイルモードで動作するように設定する方法について説明します。

### 通常クロッククライアントの設定

ルータを通常クロッククライアントとして設定する手順は、次のとおりです。

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain *domain-number* profile default**
4. **clock-port *port-name* {master | slave}**
5. **transport ipv4 multicast interface *interface-type* *interface-number***
6. (オプション) **vlan *vlan-id***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	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	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーション モードに入ります。
Step 3	<b>ptp clock ordinary domain <i>domain-number</i> profile default</b> <b>Example:</b> Router(config)# <b>ptp clock ordinary domain 0 profile default</b>	PTP クロックを設定します。次のクロックタイプを作成できます。  • <b>ordinary:</b> 単一の PTP ポートを持つ 1588 クロックであり、サーバーモードまたはクライアントモードで動作できます。  • <b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。  • <b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。
Step 4	<b>clock-port <i>port-name</i> {master   slave}</b> <b>Example:</b> Router(config-ptp-clk)# <b>clock-port slave slave</b>	新しいクロックポートを定義し、ポートを PTP サーバーモードまたはクライアントモードに設定します。クライアントモードでは、ポートは PTP サーバークロックとタイミングパケットを交換します。
Step 5	<b>transport ipv4 multicast interface <i>interface-type</i> <i>interface-number</i></b> <b>Example:</b> Router(config-ptp-port)# <b>transport ipv4 multicast interface Gi0/1/11</b>	クロックトラフィックの転送メカニズムを指定します。

	Command or Action	Purpose
Step 6	(オプション) <code>vlan vlan-id</code>  <b>Example:</b> <code>vlan 100</code>	タグ付きパケットの VLAN を設定します。

**Example****タグなしの例**

```
ptp clock ordinary domain 0 profile default
clock-port slave slave
transport ipv4 multicast interface Gi0/1/11
```

**タグ付きの例**

```
ptp clock ordinary domain 0 profile default
clock-port slave slave
transport ipv4 multicast interface Gi0/1/11
vlan 100
```

## 境界クロックの設定

インターフェイスが BC クロックの一部として追加されない場合、PTP パケットを交換する転送モードになり、PTP の動作が不安定になります。これを回避するには、**no ptp enable** コマンドを使用して、そのようなすべてのインターフェイスで PTP を無効にすることをお勧めします。

ルータを境界クロックとして設定する手順は、次のとおりです。

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ptp clock boundary domain *domain-number* profile default**
4. **clock-port *port-name***
5. **transport ipv4 multicast interface *interface-type interface-number***
6. (オプション) **vlan *vlan-id***

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> <code>Router&gt; enable</code>	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	<b>configure terminal</b>  <b>Example:</b> <code>Router# configure terminal</code>	コンフィギュレーションモードに入ります。

	Command or Action	Purpose
<b>Step 3</b>	<p><b>ptp clock boundary domain</b> <i>domain-number</i> <b>profile default</b></p> <p><b>Example:</b></p> <pre>Router(config)# ptp clock boundary domain 0 profile default</pre>	<p>PTP クロックを設定します。次のクロックタイプを作成できます。</p> <ul style="list-style-type: none"> <li>• <b>ordinary:</b> 単一の PTP ポートを持つ 1588 クロックであり、サーバーモードまたはクライアントモードで動作できます。</li> <li>• <b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li> <li>• <b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。</li> </ul>
<b>Step 4</b>	<p><b>clock-port</b> <i>port-name</i></p> <p><b>Example:</b></p> <pre>Router(config-ptp-clk)# clock-port dyn1</pre>	新しいクロックポートを定義します。
<b>Step 5</b>	<p><b>transport ipv4 multicast interface</b> <i>interface-type interface-number</i></p> <p><b>Example:</b></p> <pre>Router(config-ptp-port)# transport ipv4 multicast interface Gi0/1/0</pre>	クロックトラフィックの転送メカニズムを指定します。
<b>Step 6</b>	<p>(オプション) <b>vlan</b> <i>vlan-id</i></p> <p><b>Example:</b></p> <pre>vlan 100</pre>	タグ付きパケットの VLAN を設定します。

## Example

### タグなしの例

```
ptp clock boundary domain 0 profile default
clock-port dyn1
transport ipv4 multicast interface Gi0/1/0
clock-port dyn2
transport ipv4 multicast interface Gi0/1/2
```

### タグ付きの例

```
ptp clock boundary domain 0 profile default
clock-port dyn1
transport ipv4 multicast interface Gi0/1/0
vlan 100
clock-port dyn2
transport ipv4 multicast interface Gi0/1/2
vlan 200
```

## 透過クロックの設定

設定が完了すると、すべてのインターフェイスが TC モードの一部になります。

ルータを透過クロックとして設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock transparent domain *domain-number* profile default**
4. (オプション) **vlan *vlan-id***

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
Step 3	<b>ptp clock transparent domain <i>domain-number</i> profile default</b> <b>Example:</b> Router(config)# <b>ptp clock transparent domain 0 profile default</b>	PTP クロックを設定します。次のクロックタイプを作成できます。 <ul style="list-style-type: none"> <li>• <b>ordinary:</b> 単一の PTP ポートを持つ 1588 クロックであり、サーバーモードまたはクライアントモードで動作できます。</li> <li>• <b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li> <li>• <b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。</li> </ul>
Step 4	(オプション) <b>vlan <i>vlan-id</i></b> <b>Example:</b> vlan 100	タグ付きパケットの VLAN を設定します。

**Example****タグなしの例**

```
ptp clock transparent domain 0 profile default
```

**タグ付きの例**

```
ptp clock transparent domain 0 profile default
vlan 100
```

**TLV 拡張を含まない例: Power プロファイル 2011**

```
ptp clock transparent domain 0 profile power
allow-without-tlv
```

**TLV 拡張を含まない例: Power プロファイル 2017**

```
ptp clock transparent domain 0 profile power-2017
allow-without-tlv
```

## PTP Power プロファイルの設定

ここでは、PTP Power プロファイルを使用するようにルータを設定する方法について説明します。

Power プロファイルは、レイヤ 2 ネットワーク、つまりイーサネットで実行することを意図した PTP のサブセットを定義しますが、インターネットプロトコルは定義しません。




---

(注) Power プロファイル 2017 は、透過クロック モードでのみサポートされます。

---

## 通常クロックの設定

ルータを通常クロックとして設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain *domain-number* profile power**
4. **clock-port *port-name* {master | slave}**
5. **transport ipv4 multicast interface *interface-type interface-number***
6. (オプション) **vlan *vlan-id***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
Step 3	<b>ptp clock ordinary domain domain-number profile power</b> <b>Example:</b> Router(config)# <b>ptp clock ordinary domain 0 profile power</b>	PTP クロックを設定します。次のクロックタイプを作成できます。 <ul style="list-style-type: none"> <li><b>ordinary:</b> 単一の PTP ポートを持つ 1588 クロックであり、サーバーモードまたはクライアントモードで動作できます。</li> <li><b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li> <li><b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。</li> </ul>
Step 4	<b>clock-port port-name {master   slave}</b> <b>Example:</b> Router(config-ptp-clk)# <b>clock-port slave slave</b>	新しいクロックポートを定義し、ポートを PTP サーバーモードまたはクライアントモードに設定します。クライアントモードでは、ポートは PTP サーバークロックとタイミングパケットを交換します。
Step 5	<b>transport ipv4 multicast interface interface-type interface-number</b> <b>Example:</b> Router(config-ptp-port)# <b>transport ipv4 multicast interface Gi0/1/11</b>	クロックトラフィックの転送メカニズムを指定します。
Step 6	(オプション) <b>vlan vlan-id</b> <b>Example:</b> vlan 100	タグ付きパケットの VLAN を設定します。

## Example

タグなしの例

```
ptp clock ordinary domain 0 profile power
clock-port slave slave
transport ipv4 multicast interface Gi0/1/11
```

### タグ付きの例

```
ptp clock ordinary domain 0 profile power
clock-port slave slave
transport ipv4 multicast interface Gi0/1/11
vlan 100
```

## 境界クロックの設定

インターフェイスが BC クロックの一部として追加されない場合、PTP パケットを交換する転送モードになり、PTP の動作が不安定になります。これを回避するには、**no ptp enable** コマンドを使用して、そのようなすべてのインターフェイスで PTP を無効にすることをお勧めします。

ルータを境界クロックとして設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock boundary domain *domain-number* profile power**
4. **clock-port *port-name***
5. **transport ethernet multicast interface *interface-type* *interface-number***
6. (オプション) **vlan *vlan-id***

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーション モードに入ります。
Step 3	<b>ptp clock boundary domain <i>domain-number</i> profile power</b> <b>Example:</b> Router(config)# <b>ptp clock boundary domain 0 profile default</b>	PTP クロックを設定します。次のクロックタイプを作成できます。 <ul style="list-style-type: none"> <li>• <b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li> <li>• <b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。</li> </ul>

	Command or Action	Purpose
Step 4	<b>clock-port</b> <i>port-name</i>  <b>Example:</b> Router(config-ptp-clk)# <b>clock-port dyn1</b>	新しいクロックポートを定義します。
Step 5	<b>transport ethernet multicast interface</b> <i>interface-type</i> <i>interface-number</i>  <b>Example:</b> Router(config-ptp-port)# <b>transport ethernet multicast interface Gi0/1/0</b>	クロックトラフィックの転送メカニズムを指定します。
Step 6	(オプション) <b>vlan</b> <i>vlan-id</i>  <b>Example:</b> vlan 100	タグ付きパケットの VLAN を設定します。

### Example

#### タグなしの例

```
ptp clock boundary domain 0 profile power
clock-port dyn1
transport ethernet multicast interface Gi0/1/0
clock-port dyn2
transport ethernet multicast interface Gi0/1/2
```

#### タグ付きの例

```
ptp clock boundary domain 0 profile power
clock-port dyn1
transport ethernet multicast interface Gi0/1/0
vlan 100
clock-port dyn2
transport ethernet multicast interface Gi0/1/2
vlan 100
```

## 透過クロックの設定

ルータを透過クロックとして設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock transparent domain** *domain-number* **profile power**
4. (オプション) **vlan** *vlan-id*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
Step 3	<b>ptp clock transparent domain domain-number profile power</b> <b>Example:</b> Router(config)# <b>ptp clock transparent domain 0 profile power</b>	PTP クロックを設定します。次のクロックタイプを作成できます。 <ul style="list-style-type: none"> <li><b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li> <li><b>transparent:</b> トラフィック転送時の遅延を考慮するように PTP 時間補正フィールドを更新します。これにより、クライアントでの 1588 クロックの精度が向上します。</li> </ul>
Step 4	(オプション) <b>vlan vlan-id</b> <b>Example:</b> vlan 100	タグ付きパケットの VLAN を設定します。

**Example****タグなしの例**

```
ptp clock transparent domain 0 profile power
```

**タグ付きの例**

```
ptp clock transparent domain 0 profile power
vlan 100
```

**TLV 拡張を含まない例: Power プロファイル 2011**

```
ptp clock transparent domain 0 profile power
allow-without-tlv
```

**TLV 拡張を含まない例: Power プロファイル 2017**

```
ptp clock transparent domain 0 profile power-2017
allow-without-tlv
```

## 802.1AS プロファイルの設定

このセクションでは、802.1AS プロファイルを使用するようにルータを設定する方法について説明します。

Generalized Precision Time Protocol (gPTP) は IEEE 802.1AS 標準規格で、AVB ネットワーク内でブリッジとエンドポイントデバイスのクロックを同期する機能を提供します。これにより、時間認識ブリッジと送話者およびリスナー間でグランドマスター クロック (BMCA) を選択するメカニズムが定義されます。グランドマスターは、時間認識ネットワークで確立され、下位のノードに時間を配信して同期を可能にする時間階層のルートです。

gPTP ドメイン (以降、単にドメインと呼びます) は、この標準の要件を満たし、IEEE 802.1AS プロトコルで定義されているように相互に通信する 1 つ以上の時刻認識型システムとリンクで構成されます。gPTP ドメインは、gPTP メッセージ通信の範囲、状態、操作、データセット、および期間を定義します。

gPTP ドメインのドメイン番号は 0 とします。

gPTP ドメインで使用される時刻認識型システムには、次の 2 つのタイプがあります。

- 時刻認識型エンドステーション
- 時刻認識型ブリッジ



(注) Dot1as プロファイルは、BC タイプのみをサポートします。TC および OC スレーブはサポートしていません。



(注) デバイスで GNSS が有効になっている場合、Dot1as プロファイルはサポートされません。

## 境界クロックの設定

インターフェイスが BC クロックの一部として追加されない場合、PTP パケットを交換する転送モードになり、PTP の動作が不安定になります。これを回避するには、**no ptp enable** コマンドを使用して、そのようなすべてのインターフェイスで PTP を無効にすることをお勧めします。

ルータを境界クロックとして設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock boundary domain *domain-number* profile dot1as**
4. **clock-port *port-name***

5. transport ethernet multicast interface *interface-type interface-number*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します (要求された場合)。</li></ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーションモードに入ります。
Step 3	<b>ptp clock boundary domain <i>domain-number</i> profile dot1as</b> <b>Example:</b> Router(config)# <b>ptp clock boundary domain 0 profile dot1as</b>	PTP クロックを設定します。次のクロックタイプを作成できます。 <ul style="list-style-type: none"><li><b>boundary:</b> グランドマスターからの PTP セッションを終端し、下流の PTP サーバークロックまたはクライアントクロックとして動作します。</li></ul>
Step 4	<b>clock-port <i>port-name</i></b> <b>Example:</b> Router(config-ptp-clk)# <b>clock-port dyn1</b>	新しいクロックポートを定義します。
Step 5	<b>transport ethernet multicast interface <i>interface-type interface-number</i></b> <b>Example:</b> Router(config-ptp-port)# <b>transport ethernet multicast interface Gi0/1/0</b>	クロックトラフィックの転送メカニズムを指定します。

## Example

```
ptp clock boundary domain 0 profile dot1as
clock-port dyn1
transport ethernet multicast interface Gi0/1/0
clock-port dyn2
transport ethernet multicast interface Gi0/1/2
```

## PTP の無効化

インターフェイスで PTP を無効にするには、このセクションの手順を実行します。



**Note** 次の手順は、Default モードと Power モードの両方に適用されます。

## SUMMARY STEPS

1. `interface interface-id`
2. `no ptp enable`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>interface interface-id</code> <b>Example:</b> <code>router(config)# interface gi0/1/1</code>	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 2	<code>no ptp enable</code>	インターフェイスで PTP を無効にします。

## PTP マルチドメイン

IR8340 は、最大 4 つの異なるクロックドメインを設定できます。すべてのドメインは、異なるプロファイルとロールにすることができます。一度にサポートされる TC は 1 つのみという制限がありますが、BC/OC ドメインは複数設定できます。

```
DUT1#show run | sec ptp
ptp clock boundary domain 1 profile default
  clock-port 1
  transport ipv4 multicast interface Gi0/1/0
ptp clock boundary domain 2 profile power
  clock-port mas
  transport ethernet multicast interface Gi0/1/1
ptp clock ordinary domain 3 profile default
  clock-port sl slave
  transport ipv4 multicast interface Gi0/1/2
ptp clock transparent domain 4 profile power
```

## GMC コマンド:

```
ptp clock boundary domain 2 profile power|default
Gmc-bc source 0 ntp or Gmc-bc source 0 ptp domain 1 --- we can specifically mention sources
Gmc-bc default --- This command will take NTP|Handset based on availability and class value.
```

## 設定の確認

次のコマンドを使用すると、PTP 設定を確認できます。

- `show ptp clock dataset parent`
- `show ptp clock dataset current`
- `show ptp clock dataset time-properties`
- `show ptp clock dataset default`

- show ptp clock running
- show ptp port dataset port
- show ptp lan clock
- show ptp lan port counters messages
- show ptp lan port counters errors
- show ptp lan foreign-master-record
- show ptp lan rogue-master-record
- show ptp lan histogram ?

delay: 平均パス遅延の PTP ヒストグラムを表示します。

offset: オフセットの PTP ヒストグラムを表示します。

time-error: 時刻エラーの PTP 履歴を表示します (過去 15 日間)。

- show ptp lan history ?

delay: 平均パス遅延の PTP 履歴を表示します (過去 15 日間)。

offset: オフセットの PTP 履歴を表示します (過去 15 日間)。

time-error: 時刻エラーの PTP 履歴を表示します (過去 15 日間)。

次に、Default プロファイルの設定例を示します。

```
DUT1#show ptp lan clock running
                PTP Boundary Clock [Domain 0] [Profile: default]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  1              7340           13877          Hot standby

                PORT SUMMARY

Name Tx Mode      Role      Transport      State      Sessions      PTP Master
1    mcast        negotiated Gi0/1/0        Slave      1             UNKNOWN
DUT1#
```

次に、Power プロファイルの設定例を示します。

```
DUT1#show ptp clock running
                PTP Boundary Clock [Domain 0] [Profile: power]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  1           193            46             Hot standby

                PORT SUMMARY

Name Tx Mode      Role      Transport      State      Sessions      PTP Master
1    mcast        negotiated Ethernet        Slave      1             UNKNOWN
DUT1#
```

次に、802.1AS プロファイルの設定例を示します。

```
DUT1#show ptp clock running
                PTP Boundary Clock [Domain 0] [Profile: dotlas]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  1           1193           1146          Hot standby

                PORT SUMMARY

Name Tx Mode      Role      Transport      State      Sessions      PTP Master
Port Addr
```

```
1      mcast      negotiated Ethernet Slave      1      UNKNOWN
DUT1#
```





## CHAPTER 3

# 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 \(45 ページ\)](#)
- [ネットワーク タイム プロトコルについて \(46 ページ\)](#)
- [ネットワーク タイム プロトコルの設定方法 \(51 ページ\)](#)
- [ネットワーク タイム プロトコルの設定例 \(56 ページ\)](#)
- [ネットワーク タイム プロトコルの関連資料 \(57 ページ\)](#)
- [ネットワーク タイム プロトコルの機能情報 \(58 ページ\)](#)

## ネットワーク タイム プロトコルに関する制約事項

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クングデバイスは、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。ネットワークング 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。

## ネットワーク 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ク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ク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

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ー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ます。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	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	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	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	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	<b>ntp peer ip-address [normal-sync] [version number] [key key-id] [prefer]</b> <b>Example:</b> Router(config)# <b>ntp peer 192.168.10.1 normal-sync version 2 prefer</b>	他のシステムとのピア アソシエーションを形成します。

## ブロードキャストベースの NTP アソシエーションの設定

	Command or Action	Purpose
Step 4	<b>ntp server</b> <i>ip-address</i> [ <b>version number</b> ] [ <b>key key-id</b> ] [prefer] <b>Example:</b> Router(config)# <b>ntp server 192.168.10.1 version 2</b> <b>prefer</b>	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	<b>end</b> <b>Example:</b> Router(config)# <b>end</b>	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	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	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	<b>interface</b> <i>type number</i> <b>Example:</b> Router(config)# <b>interface GigabitEthernet 0/0/0</b>	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	<b>ntp broadcast version</b> <i>number</i> <b>Example:</b> Router(config-if)# <b>ntp broadcast version 2</b>	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	<b>ntp broadcast client</b> <b>Example:</b> Router(config-if)# <b>ntp broadcast client</b>	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	<b>ntp broadcastdelay</b> <i>microseconds</i> <b>Example:</b> Router(config-if)# <b>ntp broadcastdelay 100</b>	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	<b>end</b> <b>Example:</b> Router(config)# <b>end</b>	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	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	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	<b>line aux</b> <i>line-number</i> <b>Example:</b> Router(config)# <b>line aux 0</b>	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	<b>end</b> <b>Example:</b> Router(config-line)# <b>end</b>	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	<b>show ntp associations</b> <b>Example:</b> Router# <b>show ntp associations</b>	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
<b>Step 6</b>	<b>show ntp status</b> <b>Example:</b> Router# <code>show ntp status</code>	NTP のステータスを表示します。
<b>Step 7</b>	<b>debug ntp refclock</b> <b>Example:</b> Router# <code>debug ntp refclock</code>	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
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>• パスワードを入力します（要求された場合）。</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# <code>configure terminal</code>	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。
<b>Step 3</b>	<b>ntp authenticate</b> <b>Example:</b> Router(config)# <code>ntp authenticate</code>	NTP 認証機能を有効にします。
<b>Step 4</b>	<b>ntp authentication-key number md5 key</b> <b>Example:</b> Router(config)# <code>ntp authentication-key 1 md5 key1</code>	認証キーを定義します。 <ul style="list-style-type: none"><li>• 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。</li></ul>
<b>Step 5</b>	<b>ntp authentication-key number md5 key</b> <b>Example:</b>	認証キーを定義します。

	Command or Action	Purpose
	Router(config)# <b>ntp authentication-key 2 md5 key2</b>	<ul style="list-style-type: none"> <li>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。</li> </ul>
<b>Step 6</b>	<b>ntp authentication-key number md5 key</b> <b>Example:</b> Router(config)# <b>ntp authentication-key 3 md5 key3</b>	認証キーを定義します。 <ul style="list-style-type: none"> <li>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。</li> </ul>
<b>Step 7</b>	<b>ntp trusted-key key-number [- end-key]</b> <b>Example:</b> Router(config)# <b>ntp trusted-key 1 - 3</b>	信頼できる認証キーを定義します。 <ul style="list-style-type: none"> <li>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。</li> </ul>
<b>Step 8</b>	<b>ntp server ip-address key key-id</b> <b>Example:</b> Router(config)# <b>ntp server 172.16.22.44 key 2</b>	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。
<b>Step 9</b>	<b>end</b> <b>Example:</b> Router(config)# <b>end</b>	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 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time DOCDE881.9A6A9005 (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
filtererror = 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)
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
filtererror = 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	<a href="#">『Cisco IOS Master Commands List, All Releases』</a>
基本的なシステム管理コマンド	<a href="#">『Basic System Management Command Reference』</a>
IPv6 の NTP4	<a href="#">『Cisco IOS Basic System Management Guide』</a>
IP 拡張アクセス リスト	<a href="#">『Cisco IOS IP Addressing Configuration Guide』</a>
IPX 拡張アクセス リスト	<a href="#">『Novell IPX Configuration Guide』</a>
NTP パッケージの脆弱性	<a href="#">『Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability』</a>
Cisco IOS および NX-OS ソフトウェア リリース	<a href="#">『White Paper: Cisco IOS and NX-OS Software Reference Guide』</a>

### 標準および RFC

標準および RFC	タイトル
RFC 1305	<a href="#">『Network Time Protocol (Version 3) Specification, Implementation and Analysis』</a>

## 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。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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](http://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 6: 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。



## CHAPTER 4

# PTP クロックに基づく NTP タイミング

- [NTP の基準クロックとしての PTP \(59 ページ\)](#)
- [NTP の基準クロックとしての PTP の有効化 \(59 ページ\)](#)
- [PTP 基準クロックの検証, on page 60](#)
- [NTP 基準クロックとしての PTP のトラブルシューティング \(61 ページ\)](#)

## NTP の基準クロックとしての PTP

IR8340 ルータで機能を有効にすることにより、Network Time Protocol (NTP) の基準クロックとして Precision Time Protocol (PTP) 時刻を設定できます。

PTP 時刻はストラタム 0 ソースとして機能し、Cisco IOS NTP サーバーはストラタム 1 デバイスとして機能します。サーバーはその後、NTP クライアント (ストラタム 2 および 3) にクロック情報を提供します。

この機能は、Cisco IOS-XE リリース 17.9.1 以降の Cisco Catalyst IR8340 高耐久性シリーズ ルータでサポートされています。Network Advantage ライセンスが必要です。

## NTP の基準クロックとしての PTP の有効化

PTP 基準クロック機能は、デフォルトで無効になっています。有効にするには、CLI コマンドを入力します。開始する前に、PTP を設定し、スレーブモードになっていることを確認します。設定手順については、このガイドの[高精度時間プロトコル \(PTP\) の設定 \(7 ページ\)](#)の章を参照してください。

NTP の基準クロックとして PTP を有効にするには、**ntp refclock ptp** コマンドを入力します。

PTP 基準クロック機能を無効にするには、**no ntp refclock ptp** コマンドを入力します。



- (注) IR8340 では、この機能は PTP Default プロファイル、Power プロファイル、および Dot1as プロファイルでのみサポートされます。ソースとしての Telecom プロファイル (8265.1/8275.1) はサポートされません。NTP は一度に 1 つの基準 (GNSS または PTP のいずれか) しか取得できないため、この機能を有効にできるのは **ntp refclock gnss** が無効になっている場合のみです。

ルータの PTP 基準クロック設定を検証するには、[PTP 基準クロックの検証 \(60 ページ\)](#) を参照してください。

## PTP 基準クロックの検証

NTP の基準クロックとして PTP を有効にしたら、CLI コマンドを入力して設定を検証できます。

**Step 1** PTP 基準クロックの設定が正しいこと、および機能が実行されていることを確認します。

### Example:

```
#show run | sec ptp|ntp
ntp refclock ptp
ntp clock boundary domain 0 profile power
  clock-port 1
  transport ethernet multicast interface Gi0/1/4
```

**Step 2** PTP がスレーブモードになっていること (つまり、PTP は位相が調整された状態であり、マスタークロックにロックされていることを意味します) を確認します。

### Example:

```
#show ptp clock running
                PTP Boundary Clock [Domain 0] [Profile: power]
                State      Ports      Pkts sent  Pkts rcvd  Redundancy Mode
PHASE_ALIGNED 1                629978    633        Hot standby

                PORT SUMMARY

Name Tx Mode      Role      Transport  State      Sessions  PTP Master
1    mcast        negotiated Ethernet    Slave     1         UNKNOWN
```

**Step 3** NTP が基準クロックとして PTP を使用していることを確認します。

### Example:

```
#show ntp status
Clock is synchronized, stratum 1, reference is .PTP.
nominal freq is 250.0000 Hz, actual freq is 249.9998 Hz, precision is 2**10
ntp uptime is 28233900 (1/100 of seconds), resolution is 4016
reference time is E6161FA8.FFB7988 (08:26:16.999 UTC Fri Apr 29 2022)
clock offset is 0.9998 msec, root delay is 0.00 msec
root dispersion is 3940.49 msec, peer dispersion is 3938.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000856 s/s
system poll interval is 64, last update was 4 sec ago.
#
```

# NTP 基準クロックとしての PTP のトラブルシューティング

## PTP-NTP 同期の確認

次の例に示すように、PTP および NTP クロックの時刻をチェックして、それらが同期されていることを確認できます。

```
#show ptp lan clock | inc time
Local clock time: 2022-4-29 8:48:39 UTC
#
#show clock detail
08:48:39.278 UTC Fri Apr 29 2022
Time source is NTP
#
```

## トラブルシューティング コマンド

表 7: トラブルシューティング コマンド

コマンド	説明
<b>ntp logging</b>	NTP からの syslog を有効にします。
<b>debug ntp all</b>	NTP プロセスの完全なデバッグログを提供します。
<b>debug platform software pd-ntp all</b>	PTP を基準クロックとすることに関連するスイッチのデバッグログを提供します。
<b>show ntp status</b>	NTP が基準クロックとして PTP を使用しているかどうかなど、詳細な NTP ステータスを表示します。
<b>show ntp association detail</b>	NTP ピアリングに関する詳細情報を表示します。
<b>show ptp clock running</b>	PTP がスレーブモードになっていること（つまり、PTP は位相が調整された状態であり、マスタークロックにロックされていることを意味します）を確認します。

## ピアリングの詳細の表示

NTP ピアリングに関する詳細情報をコマンド出力に表示します。コマンドを使用すると、最初のタイミングソースがダウンした後、プラットフォームが次に使用可能なタイミングソースに切り替えるのにかかる時間を確認できます。次の例では、NTP は 8X256 秒待機して次のソースに切り替えています。

```
#show ntp association detail
127.127.6.1 configured, ipv4, our_master, sane, valid, stratum 0
ref ID .PTP., time E61622E9.00000000 (08:40:09.000 UTC Fri Apr 29 2022)
our mode active, peer mode passive, our poll intvl 256, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 4.62
delay 0.00 msec, offset 0.9998 msec, dispersion 2.81, jitter 0.97 msec
precision 2**10, version 4
assoc id 63756, assoc name 127.127.6.1
assoc in packets 11, assoc out packets 17652, assoc error packets 0
org time E61622E8.FFBE7988 (08:40:08.999 UTC Fri Apr 29 2022)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time E61622E8.FFBE7988 (08:40:08.999 UTC Fri Apr 29 2022)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtoffset = 0.99 1.99 0.99 0.99 0.99 0.99 1.99 0.99
filtererror = 0.97 2.89 4.81 6.73 8.65 10.57 11.53 12.49
minpoll = 4, maxpoll = 10
```



## CHAPTER 5

### G.8265.1 プロファイル

- [G.8265.1 プロファイルに関する情報 \(63 ページ\)](#)
- [G.8265.1 プロファイルマッピング \(64 ページ\)](#)
- [G.8265.1 サーバーとクライアントの通常クロックの設定 \(65 ページ\)](#)
- [設定の確認 \(70 ページ\)](#)

### G.8265.1 プロファイルに関する情報

G.8265.1 プロファイルは、電気通信ネットワークに固有の周波数配信要件を満たしています。G.8265.1 プロファイルの特徴は次のとおりです。

- **クロックのアダプタイズメント:** G.8265.1 は、PTP クロックをアダプタイズするためのアナウンスメッセージで使用される値の変更を規定します。クロッククラス値がクロックの QL をアダプタイズするために使用されますが、その他の値は使用されません。
- **クロック選択:** また、G.8265.1 プロファイルでは、ポート状態を選択するための代替のベストマスタークロックアルゴリズム (BMCA) が定義され、プロファイルにはクロックが定義されます。また、このプロファイルは、選択するクロックを認定するために、Sync メッセージ (およびオプションで Delay-Response メッセージ) を受信する必要があります。
- **ポート状態の決定:** ポートは、FSM を使用してポート状態を動的に設定するのではなく、静的にマスターまたはスレーブに構成されます。
- **パケットレート:** IEEE 1588-2008 規格で規定されたレートよりも高いパケットレートが使用されます。その内容は次のとおりです。
  - 同期/フォローアップ パケット: レートは 128 パケット/秒から 16 秒/パケット。
  - 遅延要求/遅延応答パケット: レートは 128 パケット/秒から 16 秒/パケット。
  - アナウンスパケット: レートは 8 パケット/秒から 64 秒/パケット。
- **転送メカニズム:** G.8265.1 は、PTP の転送メカニズムを IPv4 に制限します。G.8265.1 は、すべてのパケットをマルチキャストではなくユニキャストで送信するよう定めています。

- **クロックタイプ:** G.8265.1 は、サポートされるクロックタイプを通常クロック（単一の PTP ポートだけを使用するクロック）に制限します。G.8265.1 のスレーブ（単一のデバイス上ですべての PTP ポートが相互に独立して動作することを意味します）は、システム内の各通常クロックのコンテキスト外で行われるクロック選択などとして機能します。
  - **ドメイン番号:** G.8265.1 は、ドメイン番号の範囲を 4～23 の間に制限します。デフォルトは 4 です。
  - **ポート番号:** G.8265.1 は、PTP ポートのすべてのポート番号が 1 であることを規定しています。これは、G.8265.1 のネットワーク内のすべてのクロックが通常クロックであるためです。
- G.8265.1 はまた、ネットワークのクロックタイプもマスタークロックとスレーブクロックに制限します。つまり、境界クロックも透過クロックもサポートされません。このドキュメントでは、境界クロックをサポートするための G.8265.1 の拡張について説明しています。

#### 制限事項

- G.8265.1 はサブインターフェイスをサポートしていません。
- G.8265.1 は vrf インターフェイスをサポートしていません。
- G.8265.1 はポートチャネルインターフェイスをサポートしていません。

## G.8265.1 プロファイルマッピング

次の表に、SSM/ESMC および G.8265.1 QL 値のマッピングを示します。

表 8: G.8265.1 プロファイルマッピング

SSM QL	ITU-T G.781			クロック クラス
	オプション I	オプション II	オプション III	
0001		QL-PRS		80
0000		QL-STU	QL-UNK	82
0010	QL-PRC			84
0111		QL-ST2		86
0011				88
0100	QL-SSU-A	QL-TNC		90
0101				92
0110				94
1000	QL-SSU-B			96
1001				98
1101		QL-ST3E		100

SSM QL	ITU-T G.781			クロック クラス
1010		QL-ST3/QL-EEC2		102
1011	QL-SEC/QL-EEC1		QL-SEC	104
1100		QL-SMC		106
1110		QL-PROV		108
1111		QL-DUS		110

## G.8265.1 サーバーとクライアントの通常クロックの設定

### サーバーの通常クロックの設定

サーバーの通常クロックを設定する手順は、次のとおりです。

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain *domain-number* profile g8265.1**
4. **priority1 *priorityvalue***
5. **priority2 *priorityvalue***
6. **clock-port *port-name* master**
7. **transport ipv4 unicast interface *interface-type* *interface-number* [negotiation]**
8. **sync interval 間隔**
9. **announce interval 間隔**
10. **end**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	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	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーション モードを入力します。
Step 3	<b>ptp clock ordinary domain <i>domain-number</i> profile g8265.1</b>  <b>Example:</b>	PTP 通常クロックを設定します。 <b>profile</b> キーワードは、G.8265.1 プロファイルを使用するようにクロックを設定します。Telecom プロファイルを使用する

	Command or Action	Purpose
	Router(config)# <b>ptp clock ordinary domain 4 profile g8265.1</b>	には、クロックのドメイン番号が4～23である必要があります。
<b>Step 4</b>	<b>priority1 priorityvalue</b> <b>Example:</b> Router(config-ptp-clk)# <b>priority1 priorityvalue</b>	クロックのプリファレンスレベルを設定します。クライアントデバイスは、サーバークロックを選択するときに <b>priority1</b> 値を使用します。低い <b>priority1</b> 値は優先クロックを示します。 <b>priority1</b> の値は、他のクロック属性よりも上位であると見なされます。  有効値の範囲は0～255です。デフォルト値は128です。
<b>Step 5</b>	<b>priority2 priorityvalue</b> <b>Example:</b> Router(config-ptp-clk)# <b>priority1 priorityvalue</b>	クロックのセカンダリプリファレンスレベルを設定します。従属デバイスは、サーバークロックを選択するときに <b>priority2</b> 値を使用します。低い <b>priority2</b> 値は優先クロックを示します。ルータで、クロックの選択に <b>priority1</b> または他のクロック属性を使用できない場合にだけ、 <b>priority2</b> の値が考慮されます。  有効値の範囲は0～255です。デフォルト値は128です。
<b>Step 6</b>	<b>clock-port port-name master</b> <b>Example:</b> Router(config-ptp-clk)# <b>clock-port master master</b>	クロックポートをPTPサーバーマードに設定します。
<b>Step 7</b>	<b>transport ipv4 unicast interface interface-type interface-number [negotiation]</b> <b>Example:</b> Router(config-ptp-port)# <b>transport ipv4 unicast interface GigabitEthernet 0/0/0 negotiation</b>	クロックトラフィックの転送メカニズムを指定します。WANポートだけでなく、ループバックインターフェイスも使用できます。  クライアントルータのIPアドレスは、WANポートでPTPパケットを送受信できるように、WANインターフェイス（GigabitEthernet 0/0/0 または GigabitEthernet 0/0/1）経由で到達可能である必要があります。  <b>negotiation</b> キーワードは、使用可能なすべてのPTPクロックソースからPTPサーバークロックを検出するようにルータを設定します。
<b>Step 8</b>	<b>sync interval 間隔</b> <b>Example:</b> Router(config-ptp-port)# <b>sync interval -4</b>	PTP同期メッセージの送信に使用されるインターバルを指定します。インターバルは、2を底とする対数を使用して次のように設定されます。  <ul style="list-style-type: none"> <li>• 1: 2秒ごとに1パケット</li> <li>• 0: 1秒ごとに1パケット</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• -1: 1/2 秒ごとに1パケット、つまり、1秒ごとに2パケット</li> <li>• -2: 1/4 秒ごとに1パケット、つまり、1秒ごとに4パケット</li> <li>• -3: 1/8 秒ごとに1パケット、つまり、1秒ごとに8パケット</li> <li>• -4: 1/16 秒ごとに1パケット、つまり、1秒ごとに16パケット</li> <li>• -5: 1/32 秒ごとに1パケット、つまり、1秒ごとに32パケット</li> <li>• -6: 1/64 秒ごとに1パケット、つまり、1秒ごとに64パケット</li> <li>• -7: 1/128 秒ごとに1パケット、つまり、1秒ごとに128パケット</li> </ul>
Step 9	<p><b>announce interval</b> 間隔</p> <p><b>Example:</b></p> <pre>Router(config-ptp-port)# <b>announce interval 2</b></pre>	<p>PTP Announcement メッセージのインターバルを指定します。インターバルは、2を底とする対数を使用して次のように設定されます。</p> <ul style="list-style-type: none"> <li>• 3: 8 秒ごとに1パケット</li> <li>• 2: 4 秒ごとに1パケット</li> <li>• 1: 2 秒ごとに1パケット</li> <li>• 0: 1 秒ごとに1パケット</li> <li>• -1: 1/2 秒ごとに1パケット、つまり、1秒ごとに2パケット</li> <li>• -2: 1/4 秒ごとに1パケット、つまり、1秒ごとに4パケット</li> <li>• -3: 1/8 秒ごとに1パケット、つまり、1秒ごとに8パケット</li> </ul>
Step 10	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config-ptp-port)# <b>end</b></pre>	<p>コンフィギュレーション モードを終了します。</p>

## クライアントの通常クロックの設定

クライアントの通常クロックを設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain *domain-number* profile g8265.1**
4. **clock-port *port-name* slave**
5. **transport ipv4 unicast interface *interface-type* *interface-number* [negotiation]**
6. **delay-req interval** 間隔
7. **announce timeout** *value*
8. **clock source** *source-address*
9. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	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	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	コンフィギュレーションモードを入力します。
Step 3	<b>ptp clock ordinary domain <i>domain-number</i> profile g8265.1</b>  <b>Example:</b> Router(config)# <b>ptp clock ordinary domain 4 profile g8265.1</b>	PTP 通常クロックを設定します。 <b>profile</b> キーワードは、G.8265.1 プロファイルを使用するようにクロックを設定します。Telecomプロファイルを使用するには、クロックのドメイン番号が4～23である必要があります。
Step 4	<b>clock-port <i>port-name</i> slave</b>  <b>Example:</b> Router(config-ptp-clk)# <b>clock-port client slave</b>	クロックポートを PTP クライアントモードに設定します。
Step 5	<b>transport ipv4 unicast interface <i>interface-type</i> <i>interface-number</i> [negotiation]</b>  <b>Example:</b> Router(config-ptp-port)# <b>transport ipv4 unicast interface GigabitEthernet 0/0/0 negotiation</b>	クロックトラフィックの転送メカニズムを指定します。WANポートだけでなく、ループバックインターフェイスも使用できます。  サーバールータのIPアドレスは、WANポートでPTPパケットを送受信できるように、WANインターフェイス（GigabitEthernet 0/0/0 または GigabitEthernet 0/0/1）経由で到達可能である必要があります。

	Command or Action	Purpose
		<b>negotiation</b> キーワードは、使用可能なすべての PTP クロックソースから PTP サーバークロックを検出するようにルータを設定します。
<b>Step 6</b>	<b>delay-req interval</b> 間隔 <b>Example:</b> Router(config-ptp-port)# <b>delay-req interval -4</b>	ポートがサーバステータスの場合に PTP 遅延要求メッセージ間で許可される最小間隔を設定します。 インターバルは、2 を底とする対数を使用して次のように設定されます。 <ul style="list-style-type: none"> <li>• 3: 8 秒ごとに 1 パケット</li> <li>• 2: 4 秒ごとに 1 パケット</li> <li>• 1: 2 秒ごとに 1 パケット</li> <li>• 0: 1 秒ごとに 1 パケット</li> <li>• -1: 1/2 秒ごとに 1 パケット、つまり、1 秒ごとに 2 パケット</li> <li>• -2: 1/4 秒ごとに 1 パケット、つまり、1 秒ごとに 4 パケット</li> <li>• -3: 1/8 秒ごとに 1 パケット、つまり、1 秒ごとに 8 パケット</li> <li>• -4: 1/16 秒ごとに 1 パケット、つまり、1 秒ごとに 16 パケット</li> <li>• -5: 1/32 秒ごとに 1 パケット、つまり、1 秒ごとに 32 パケット</li> <li>• -6: 1/64 秒ごとに 1 パケット、つまり、1 秒ごとに 64 パケット</li> <li>• -7: 1/128 秒ごとに 1 パケット、つまり、1 秒ごとに 128 パケット</li> </ul>
<b>Step 7</b>	<b>announce timeout value</b> <b>Example:</b> Router(config-ptp-port)# <b>announce timeout 8</b>	セッションがタイムアウトする前の PTP Announcement インターバルの数を指定します。有効な値は 1 ~ 10 です。
<b>Step 8</b>	<b>clock source source-address</b> <b>Example:</b> Router(config-ptp-port)# <b>clock-source 8.8.8.1</b>	PTP サーバークロックのアドレスを指定します。
<b>Step 9</b>	<b>end</b> <b>Example:</b>	コンフィギュレーションモードを終了します。

Command or Action	Purpose
Router(config-ptp-port)# <b>end</b>	

## 設定の確認

次のコマンドを使用すると、クロッキング設定を確認できます。

- show ptp clock running domain <domain no>
- show ptp clock dataset default
- show ptp clock dataset parent
- show ptp port <name of virtual port>
- show ptp wan stat stream < stream id>
- show network-clock synchronization
- show ptp port dataset port
- show ptp wan tod
- show gnss time
- show gnss status

### 例

```
IR8340#show ptp clock running domain 4
                PTP Ordinary Clock [Domain 4] [Profile: g8265.1]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
      ACQUIRING  1                1543            4680            Hot standby
                PORT SUMMARY
Name Tx Mode      Role      Transport      State      Sessions      PTP Master
slave unicast    slave     Gi0/0/1        Slave       1             2.3.1.1
                SESSION INFORMATION
slave [Gi0/0/1] [Sessions 1]
Peer addr      Pkts in      Pkts out      In Errs      Out Errs
2.3.1.1        4680         1543          0            0
IR8340#

IR8340#show ptp clock running domain 4
                PTP Ordinary Clock [Domain 4] [Profile: g8265.1]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
      PHASE_ALIGNED 1                44752          135639          Hot standby
                PORT SUMMARY
Name Tx Mode      Role      Transport      State      Sessions      PTP Master
slave unicast    slave     Gi0/0/1        Slave       1             2.3.1.1
                SESSION INFORMATION
slave [Gi0/0/1] [Sessions 1]
Peer addr      Pkts in      Pkts out      In Errs      Out Errs
2.3.1.1        135639       44752         0            0
IR8340#

IR8340#show ptp clock dataset default
CLOCK [Ordinary Clock, domain 4]
```

```
Profile: g8265.1
Two Step Flag: No
Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
Number Of Ports: 1
Priority1: 128
Priority2: 128
Domain Number: 4
Slave Only: Yes
Clock Quality:
  Class: 255
  Accuracy: Unknown
  Offset (log variance): 0
IR8340#

IR8340#show ptp clock dataset parent
CLOCK [Ordinary Clock, domain 4]
Profile: g8265.1
Parent Clock Identity: 0x44:B6:BE:FF:FE:42:EF:13
Parent Port Number: 0
Parent Stats: No
Observed Parent Offset (log variance): 0
Observed Parent Clock Phase Change Rate: 0
Grandmaster Clock:
  Identity: 0x44:B6:BE:FF:FE:42:EF:13
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 104
    Accuracy: Unknown
    Offset (log variance): 52592
IR8340#

IR8340#show ptp clock dataset time-properties
CLOCK [Ordinary Clock, domain 4]

Current UTC Offset Valid: FALSE
Current UTC Offset: 37
Leap 59: FALSE
Leap 61: FALSE
Time Traceable: FALSE
Frequency Traceable: TRUE
PTP Timescale: TRUE
Time Source: Internal Oscillator
IR8340#

IR8340#show ptp port dataset port
PORT [slave]
Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
Clock Profile: g8265.1
Transport Interface: GigabitEthernet0/0/1
Port Number: 1
Port State: Slave
Min Delay Req Interval (log base 2): -4
Peer Mean Path Delay: 0
Announce interval (log base 2): 1
Announce Receipt Timeout: 3
Sync Interval (log base 2): -5
Delay Mechanism: End to End
Peer Delay Request Interval (log base 2): -4
PTP version: 2
IR8340#

IR8340#show ptp wan stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
Time elapsed since last packet: 0.0
```

```

Configured Interval : -5, Acting Interval -5
Tx packets : 0, Rx Packets : 96215
Last Seq Number : 30678, Error Packets : 0
Delay Req Packet Stats
Time elapsed since last packet: 0.0
Configured Interval : -4, Acting Interval : -4
Tx packets : 48107, Rx Packets : 0
Last Seq Number : 0, Error Packets : 0
Delay Response Packet Stats
Time elapsed since last packet: 0.0
Configured Interval : -4, Acting Interval : -4
Tx packets : 0, Rx Packets : 48107
Last Seq Number : 48106, Error Packets : 0
Announce Packet Stats
Time elapsed since last packet: 0.0
Configured Interval : 1, Acting Interval : 1
Tx packets : 0, Rx Packets : 1509
Last Seq Number 1508 Error Packets 0
Signalling Packet Stats
Time elapsed since last packet: 0.0
Configured Interval : 0, Acting Interval : 0
Tx packets : 12, Rx Packets : 12
Last Seq Number : 0, Error Packets : 0
Current Data Set
Offset from master : +0.000000000    Units      Within tolerance?
Mean Path Delay    : +0.000000027    seconds    Yes
Forward Path Delay : +0.000000027    seconds    Yes
Reverse Path Delay : +0.000000028    seconds    Yes
Steps Removed 1
IR8340#

IR8340#show ptp wan tod
PTPd ToD information:

Time: 01/05/22 11:35:21

IR8340#

```



## CHAPTER 6

# G.8275.1 プロファイル

- [G.8275.1 に関する情報 \(73 ページ\)](#)
- [G.8275.1 プロファイルの設定 \(76 ページ\)](#)
- [設定の確認 \(77 ページ\)](#)
- [デバッグコマンド \(79 ページ\)](#)

## G.8275.1 に関する情報

Precision Time Protocol (PTP) が定義されている IEEE 1588-2008 標準では、異なるシナリオでの使用に対して PTP を適応させるために、個別のプロファイルを定義することができます。ネットワークからのフルタイミングサポートを備えた ITU-T G.8275.1 は、テレコムネットワークで使用するための PTP プロファイルです。テレコムネットワークでは、位相または時刻の同期が必要であり、各ネットワークデバイスが PTP プロトコルに参加し、PHY レイヤの周波数サポートを提供します。

## 同期モデル

G.8275.1 に採用されているモデルは、「ホップバイホップ」同期です。マスターからスレーブへのパス上の各ネットワーク要素は、ローカルクロックを上流のデバイスに同期させ、下流のデバイスに同期を提供します。

G.8275.1 では、次の 3 種類のクロックを使用できます。

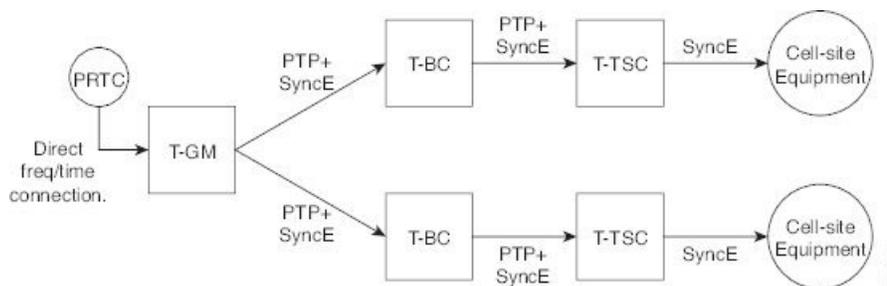
- **Telecom Grandmaster (T-GM)** : テレコムグランドマスターは、ネットワーク内の他のデバイスにタイミングを提供し、通常は、GPS アンテナなどのプライマリ基準時刻源に接続されています。ローカルクロックを他のネットワーク要素に同期させません。
- **Telecom Time Slave Clock (T-TSC)** : スレーブクロックは、ローカルクロックを別の PTP クロックに同期させ、他のデバイスには PTP を介して同期を提供しません。
- **Telecom Boundary Clock (T-BC)** : テレコム境界クロックは、ローカルクロックを T-GM または上流の T-BC に同期させ、タイミング情報を下流の T-BC または T-TSC に提供します。所定の時点で、T-BC が同期するために利用可能な高品質のクロックがない場合は、グランドマスターの機能を果たすことができます。G.8275.1 は、T-BC に仮想ポートの概念を導入して

います。仮想ポートは、ソース選択に参加できる、T-BC上の外部の周波数、位相、および時刻入力インターフェイスです。IR8340には、タイミングカードに載ったgnssモジュールがあります。gnssがロックされている場合、GNSSから時刻、位相、および周波数を取得する仮想ポートを使用するようにT-BCを設定できます。

非参加デバイス（PTP パケットを転送するだけのデバイス）およびPTP 透過クロックは許可されません。

PTP は、ネットワーク全体で位相/時刻の同期を提供するために使用されます。SyncE が G.8275.1 展開で使用され、位相/時刻の同期（いわゆる「ハイブリッドモード」）の周波数安定性が向上することが期待されます（必須ではありません）。

図 6: G.8275.1 トポロジの例



## PTP ドメイン

G.8275.1 ネットワーク内で使用できる PTP ドメイン番号は、24 ~ 43 の範囲です。デフォルトドメインは 24 です。

## PTP メッセージと転送

次の PTP 転送パラメータは、G.8275.1 で定義されています。

- マルチキャスト PTP over Ethernet を使用する必要があります。転送可能なマルチキャスト MAC アドレス (01-1B-19-00-00-00) または転送不可能なマルチキャスト MAC アドレス (01-80-C2-00-00-0E) のいずれかを使用できます。使用中の MAC アドレスは、設定によってポートごとに選択されます。
- 1 ステップまたは 2 ステップのクロックモードを使用できます。
- 位相/時刻配信を可能にするために、双方向の PTP 動作が必要です。遅延要求応答メカニズムが、伝播遅延測定に使用されます。ピア遅延メカニズムは使用されません。
- アナウンスメッセージの最小パケットレートは 8 パケット/秒です。同期、フォローアップ、遅延要求、および遅延応答メッセージの場合、最小レートは 16 パケット/秒です。
- シグナリングおよび管理メッセージは使用されません。



(注) G8275.1は、サブインターフェイス、dot1q、およびポートチャネルではサポートされていません。

## ベスト マスター クロック アルゴリズム

G.8275.1は、代替ベスト マスター クロック アルゴリズム (BMCA) を指定します。BMCAは、各デバイスが同期するクロック (存在する場合) を選択し、ローカルポートのポート状態を決定するために使用されます。

次の新しいパラメータは、G.8275.1の代替 BMCAの一部として定義されています。

- **「notSlave」フラグ:** notSlave フラグは、ポートごとに設定可能な boolean 値であり、ポートをスレーブモードにできるかどうかを示します。これが PTP クロックのポートの1つに設定されている場合、クロックはそのポートで受信したクロックに同期しません。
- **ローカルプライオリティ:** ローカルプライオリティはポートごとの設定項目であり、単一のネットワーク要素の範囲内で、異なるポートで受信したクロック間から PTP クロックが選択するときにタイブレーカーとして使用されます。ネットワーク要素のローカルクロックにも、設定可能なローカルプライオリティがあります。

G.8275.1 BMCA のクロック比較アルゴリズムは、次のパラメータに基づいています。

1. **クロッククラス:** プロファイルは、準拠するクロックで使用するための一連のクロッククラスを定義します。選択されるクロッククラスは、クロックのタイプ、クロックのトレーサビリティ、およびホールドオーバーステータスに依存します。
2. **クロック精度:** G.8275.1によって次のクロック精度値が使用されます。  
0x21: PRTC にロックされた T-GM はこの値を使用します。  
0xFE: ホールドオーバーの T-GM、または T-BC は、この値を使用します。
3. **オフセットスケール対数分散:** G.8275.1によって次のオフセットスケール対数分散値が使用されます。  
0x4E5D: PRTC にロックされた T-GM はこの値を使用します。  
0xFFFF: ホールドオーバーの T-GM、または T-BC は、この値を使用します。
4. **プライオリティ 2:** 元の 1588v2 BMCA と同様に使用されます。プライオリティ 1 は使用されません。
5. **ローカルプライオリティ:** 上記のように使用されます。
6. **クロック ID:** クロック ID は、異なるクロック間のタイブレーカーとして使用されます (元の 1588v2 BMCA と同様)。
7. **削除されたステップ:** 削除されたステップの値は、同じクロックを受信する異なるポート間で選択するために使用されます (元の 1588v2 BMCA と同様)。

8. **ポート ID:** ポート ID は、同じクロックの異なるポート間のタイブレーカーとして使用されま  
す。

G.8275.1 準拠のクロックは、受信したアナウンスメッセージの次の値を無視します。

- flag フィールドの代替マスター、ユニキャスト、およびプロファイル固有のメンバー
- control フィールド
- Priority1

## G.8275.1 プロファイルの設定

### T-GM の設定

PTP-OC-T-GM は、周波数と 1PPS の入力を取得し、上流のグランドマスターと同期することができます。

次に、T-GM の設定例を示します。

```
ptp clock ordinary domain 24 profile G.8275.1
tod R0 ubx
input 1pps R0 //GNSS is locked and TOD+1PPS are feeding into T-GM G.8275.1.
clock-port master-port master
transport ethernet multicast interface Gig 0/0/1
```

### T-TSC の設定

次に、T-TSC の設定例を示します。

```
ptp clock ordinary domain 24 hybrid g.8275.1
tod R0 cisco
output 1pps R0
clock-port slave-port slave
transport ethernet multicast interface Gig 0/0/0
```

### T-BC の設定

次に、T-BC の設定例を示します。

```
ptp clock boundary domain 24 hybrid profile g.8275.1
tod R0 cisco
output 1pps R0
clock-port bc-port-1
transport ethernet multicast interface Gig 0/0/0
clock-port bc-port-2
transport ethernet multicast interface Gig 0/0/1
```

## 設定の確認

次のコマンドを使用すると、クロッキング設定を確認できます。

- show ptp clock running domain <domain no>
- show ptp clock dataset default
- show ptp clock dataset parent
- show ptp port <name of virtual port>
- show ptp wan stat stream < stream id>
- show network-clock synchronization
- show ptp port dataset port
- show ptp wan tod
- show gnss time
- show gnss status

### 例

```
IR8340#show ptp clock running domain 24
PTP Ordinary Clock [Domain 24] [Hybrid] [Profile: g8275.1]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
      FREQ_LOCKED 1          56             146            Hot standby
                                PORT SUMMARY
                                PTP Master
Name Tx Mode      Role      Transport  State      Sessions  Port Addr
slave mcast     slave    Ethernet   Slave      1          UNKNOWN
IR8340#

IR8340#show ptp clock running
PTP Ordinary Clock [Domain 24] [Hybrid] [Profile: g8275.1]
      State      Ports      Pkts sent      Pkts rcvd      Redundancy Mode
      PHASE_ALIGNED 1          1176           2946           Hot standby
                                PORT SUMMARY
                                PTP Master
Name Tx Mode      Role      Transport  State      Sessions  Port Addr
slave mcast     slave    Ethernet   Slave      1          UNKNOWN
IR8340#

IR8340#show ptp clock dataset default
CLOCK [Ordinary Clock, domain 24]
Profile: g8275.1
Two Step Flag: No
Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
Number Of Ports: 1
Priority1: 128
Priority2: 128
Local Priority: 128
Domain Number: 24
Slave Only: Yes
Clock Quality:
Class: 255
Accuracy: Unknown
```

```

    Offset (log variance): 65535
IR8340#

IR8340#show ptp clock dataset parent
CLOCK [Ordinary Clock, domain 24]
  Profile: g8275.1
  Parent Clock Identity: 0x44:B6:BE:FF:FE:42:EF:13
  Parent Port Number: 0
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
    Identity: 0x44:B6:BE:FF:FE:42:EF:13
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 248
      Accuracy: Unknown
      Offset (log variance): 65535
IR8340#

IR8340#show ptp port dataset port
PORT [slave]
  Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
  Clock Profile: g8275.1
  Transport Interface: GigabitEthernet0/0/1
  Port Number: 1
  Port State: Slave
  Min Delay Req Interval (log base 2): -4
  Peer Mean Path Delay: 0
  Announce interval (log base 2): -3
  Announce Receipt Timeout: 3
  Sync Interval (log base 2): -4
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): -4
  PTP version: 2
  Local Priority: 128
  Not-slave: False
IR8340#

IR8340#show ptp wan stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -5, Acting Interval -5
  Tx packets : 0, Rx Packets : 96215
  Last Seq Number : 30678, Error Packets : 0
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 48107, Rx Packets : 0
  Last Seq Number : 0, Error Packets : 0
Delay Response Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 0, Rx Packets : 48107
  Last Seq Number : 48106, Error Packets : 0
Announce Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 1, Acting Interval : 1
  Tx packets : 0, Rx Packets : 1509
  Last Seq Number 1508 Error Packets 0
Signalling Packet Stats
  Time elapsed since last packet: 0.0

```

```

Configured Interval : 0, Acting Interval : 0
Tx packets : 12, Rx Packets : 12
Last Seq Number : 0, Error Packets : 0
Current Data Set                               Units      Within tolerance?
Offset from master : +0.000000000             seconds    Yes
Mean Path Delay   : +0.000000027             seconds    Yes
Forward Path Delay : +0.000000027             seconds    Yes
Reverse Path Delay : +0.000000028             seconds    Yes
Steps Removed 1
IR8340#

IR8340#show ptp wan tod
PTPd ToD information:

Time: 01/05/22 11:35:21

IR8340#

IR8340#show network-clocks synchronization detail
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/0/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-SEC
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (sf_change)->
  1A (ql_change)-> 1A
Nominated Interfaces
Interface          SigType      Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal          NA           NA/Dis       251   QL-SEC NA       NA
*Gi0/0/1          NA           Sync/En      1     QL-PRC -        -

```

## デバッグコマンド

設定をデバッグするには、次のコマンドを使用します。

- show esmc details
- show platform hardware network-clocks
- show network-clock synchronization detail
- show clocking details

### 例

```

IR8340#show esmc detail
Interface: GigabitEthernet0/0/0
Administrative configurations:
Mode: Asynchronous

```

```

ESMC TX: Disable
ESMC RX: Disable
QL TX: -
QL RX: -
Operational status:
  Port status: UP
  QL Receive: QL-DNU
  QL Transmit: -
  QL rx overridden: -
  ESMC Information rate: 1 packet/second
  ESMC Expiry: 5 second
  ESMC Tx Timer: Stopped
  ESMC Rx Timer: Stopped
  ESMC Tx interval count: 1
  ESMC INFO pkts in: 777
  ESMC INFO pkts out: 1068
  ESMC EVENT pkts in: 0
  ESMC EVENT pkts out: 2

IR8340#show esmc detail
IInterface: GigabitEthernet0/0/1
  Administrative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-PRC
    QL Transmit: QL-DNU
    QL rx overridden: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
    ESMC Tx Timer: Running
    ESMC Rx Timer: Running
    ESMC Tx interval count: 1
    ESMC INFO pkts in: 1169
    ESMC INFO pkts out: 1486
    ESMC EVENT pkts in: 0
    ESMC EVENT pkts out: 2

IR8340#

IR8340#show network-clocks synchronization detail
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/0/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-SEC
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (sf_change)->
  1A (ql_change)-> 1A
Nominated Interfaces
  Interface          SigType      Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx

```

```

Internal          NA          NA/Dis          251  QL-SEC  NA          NA
*Gi0/0/1         NA          Sync/En         1    QL-PRC  -          -

```

```
IR8340#show platform hardware network-clocks
```

```
Chassis Manager Netclk Status
```

```
-----
```

```
DPLL1 Status:
```

```
-----
```

```
Bandwidth: 1.7 Hz
```

```
Phase Slope Limit: 7500 ns/s
```

```
Current PLL1 Mode: MANUAL NORMAL
```

```
Current Input Selected: REF7 (CLK_REC_25M_WAN2)
```

```
Current PLL1 Holdover Status: OFF
```

```
Current PLL1 Lock Status: ON
```

```
IR8340#show platform hardware network-clocks
```

```
DPLL2 Status:
```

```
-----
```

```
Bandwidth: 0.029 Hz
```

```
Phase Slope Limit: 750 ns/s
```

```
Current PLL2 Mode: TOP CLIENT (NCO)
```

```
Current Input Selected: none
```

```
Current PLL2 Holdover Status: OFF
```

```
Current PLL2 Lock Status: OFF
```

```
IR8340#show platform hardware network-clocks
```

```
Current Input Status:
```

```
REF0 (CLK_LOOPBACK1) : OK
```

```
REF1 (CLK_LOOPBACK2) : OK
```

```
REF2 ((TDM_SYNC_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
```

```
REF3 (RSV_2_M_PLL) : FAIL (SCM, CFM, GST, PFM failed)
```

```
REF4 (CLK_PPS_GPS_PLL) : FAIL (SCM, CFM, GST, PFM failed)
```

```
REF5 (CLK_PPS_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
```

```
REF6 (CLK_REC_25M_WAN1) : FAIL (SCM, CFM, GST, PFM failed)
```

```
REF7 (CLK_REC_25M_WAN2) : OK
```

```
REF8 (CLK20M_OCXO) : OK
```

```
REF9 (RSV_1_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
```

```
IR8340#show platform hardware network-clocks
```

```
REF0 Freq Configured : 25 Mhz
```

```
REF1 Freq Configured : 25 Mhz
```

```
REF2 Freq Configured : 8 Khz
```

```
REF3 Freq Configured : 10 Mhz
```

```
REF4 Freq Configured : 1 Hz
```

```
REF5 Freq Configured : 1 Hz
```

```
REF6 Freq Configured : 25 Mhz
```

```
REF7 Freq Configured : 25 Mhz
```

```
REF8 Freq Configured : 20 Mhz
```

```
REF9 Freq Configured : 25 Mhz
```





## CHAPTER 7

# 同期イーサネット ESMC と SSM の設定

同期イーサネットは、クロック同期機能を組み込むことにより、従来の SONET/SDH および T1/E1 ネットワークで見られる信頼性をイーサネットパケットネットワークに提供するように設計されたイーサネットの拡張機能です。クロック同期機能は、同期イーサネットクロック同期に関する同期ステータスメッセージ (SSM) とイーサネット同期メッセージチャンネル (ESMC) をサポートしています。

- [同期イーサネットについて \(83 ページ\)](#)
- [クロック選択モード \(84 ページ\)](#)
- [同期イーサネット ESMC と SSM の設定, on page 84](#)

## 同期イーサネットについて

ITU G.781 に記述されている同期イーサネット (SyncE) により、必要な同期が物理レベルで実現します。SyncE では、イーサネットリンクは SONET/SDH と同じ方法で、高品質なストラタム 1 の追跡可能なクロック信号とビットクロックのタイミングをとることで同期されます。

イーサネット同期メッセージチャンネル (ESMC) には、同期オプティカル ネットワーキング (SONET) ネットワークと同期デジタル階層 (SDH) ネットワークで使用される同期ステータスメッセージ (SSM) が組み込まれています。SONET と SDH がフレーム内の固定位置に SSM を送信している間、ESMC はプロトコル IEEE 802.3 Organization-Specific Slow Protocol (OSSP) 標準を使用して SSM を送信します。

ESMC は、所定の同期イーサネットタイミングソースのクロック品質を識別する品質レベル (QL) 値を伝送します。クロック品質値は、同期イーサネット ノードが最も信頼性の高いソースからタイミングを取得し、タイミングのループを防止するのに役立ちます。

同期イーサネットを使用するように設定されている場合、ルータは使用可能な最適なクロックソースに同期します。使用可能な良好なクロック ソースがない場合、ルータは現在のクロックソースに同期されたままとなります。

ルータは、QL 対応と QL 非対応の 2 つのクロック選択モードをサポートしています。各モードは異なる基準を使用して、使用可能な最適なクロック ソースを選択します。

## クロック選択モード

IR8340 ルータは、次の 2 つのクロック選択モードをサポートしています。

- QL 有効モード: QL 有効モードでは、ルータはクロックソースを選択するときに次のパラメータを考慮します。
  - クロック品質レベル (QL)
  - クロックの可用性
  - プライオリティ
- QL 無効モード: QL 無効モードでは、ルータはクロックソースを選択するときに次のパラメータを考慮します。
  - クロックの可用性
  - プライオリティ

## 同期イーサネット ESMC と SSM の設定

Cisco IR8340 ルータで同期イーサネット ESMC および SSM を設定する手順は、次のとおりです。

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock eec {1|2}**
5. **network-clock ynchronization ssm option {1|2} {GEN1 | GEN2 } }**
6. **network-clock input-source priority {interfaceinterface\_id|ptp domain domain\_num|{external {R0 | R1 [ {t1 {sf | esf } linecode {ami | b8zs } line-build-out length} | e1 [crc4 | fas ] [125ohm | 75ohm ] linecode [hdb3 | ami ] } | 10m ] } }**
7. **network-clock synchronization mode ql-enabled**
8. **network-clock wait-to-restore seconds global**
9. **esmc process**
10. **network-clock quality-level {tx | rx} value {interface interface-id | controller [E1 | BITS ] slot/card/port | external [2m | 10m ] }**
11. **interface interface-id**
12. **network-clock source quality-level value {tx|rx}**
13. **synchronous mode**
14. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	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	<b>network-clock synchronization automatic</b> <b>Example:</b> Router(config)# <b>network-clock synchronization automatic</b>	ネットワーククロック選択アルゴリズムを有効にします。このコマンドを実行すると、シスコ固有のネットワーククロックプロセスが無効になり、G.781 ベースの自動クロック選択プロセスが有効になります。 <b>Note</b> このコマンドは、入力ソースの前に設定する必要があります。
Step 4	<b>network-clock eec {1 2}</b> <b>Example:</b> Router(config)# <b>network-clock eec 1</b>	イーサネット機器クロック（EEC）タイプを指定します。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>1: ITU-T G.8262 オプション 1（2048）</li> <li>2: ITU-T G.8262 オプション 2 および Telcordia GR-1244（1544）</li> </ul>
Step 5	<b>network-clock ynsynchronization ssm option {1 2 {GEN1   GEN2}}</b> <b>Example:</b> Router(config)# <b>network-clock synchronization ssm option 2 GEN1</b>	同期メッセージの送信に使用する G.781 同期オプションを設定します。このコマンドには、次のガイドラインが適用されます。 <ul style="list-style-type: none"> <li>オプション 1 は、ヨーロッパ向けに設計された G.781 同期ネットワークオプション 1 を示します。これはデフォルト値です。</li> <li>オプション 2 は、米国向けに設計された G.781 同期ネットワークオプション 2 を示します。</li> <li>GEN1 は、オプション 2 の第 1 世代同期を指定します。</li> <li>GEN2 は、オプション 2 の第 2 世代同期を指定します。</li> </ul>
Step 6	<b>network-clock input-source priority {interface interface_id   ptp domain domain_num   {external {R0   R1 [{t1 {sf   esf} linecode {ami   b8zs</b>	ルータの入力クロックとしてインターフェイスを選択できます。WAN インターフェイス（ギガビットイーサネット 0/0/0、ギガビットイーサネット

	Command or Action	Purpose
	<pre>} line-build-out length}   e1 [crc4   fas ] [125ohm   75ohm ] ] linecode [hdb3   ami ] }   10m ] }</pre> <p><b>Example:</b></p> <pre>Router(config)# network-clock input-source 1 interface GigabitEthernet 0/0/0 Router(config)# network-clock input-source 1 external R0 1hz Router(config)# network-clock input-source 2 controller t1 0/2/0 Router(config)# network-clock input-source 3 ptp domain 4</pre>	<p>0/0/1)、T1/E1 コントローラ、または外部インターフェイスを選択できます。クロックソースの選択のプライオリティ（1が最高プライオリティ）。最高プライオリティを持つクロックソースに障害が発生した場合、次に高いプライオリティを持つクロックソースが選択されます。</p> <p><b>Note</b></p> <p>イーサネットインターフェイスをクロックソースとして設定する前に、インターフェイス設定で同期モードを設定する必要があります。</p> <p>SyncE は LAN インターフェイスではサポートされていません。</p>
<b>Step 7</b>	<p><b>network-clock synchronization mode ql-enabled</b></p> <p><b>Example:</b></p> <pre>Router(config)# network-clock synchronization mode ql-enabled</pre>	<p>品質レベル（QL）に基づいたクロックソースの自動選択を有効にします。</p>
<b>Step 8</b>	<p><b>network-clock wait-to-restore seconds global</b></p> <p><b>Example:</b></p> <pre>Router(config)# network-clock wait-to-restore 70 global</pre>	<p>（オプション）同期イーサネットクロックソースにグローバルな wait-to-restore タイマーを設定します。タイマーは、復元されたクロックソースをクロック選択プロセスに含める前にルータが待機する時間を指定します。</p> <p>有効値の範囲は 0 ～ 86400 秒です。デフォルト値は 300 秒です。</p>
<b>Step 9</b>	<p><b>esmc process</b></p> <p><b>Example:</b></p> <pre>Router(config)# esmc process</pre>	<p>ESMC プロセスをグローバルで有効にします。</p>
<b>Step 10</b>	<p><b>network-clock quality-level {tx   rx} value {interface interface-id   controller [E1   BITS ] slot/card/port   external [2m   10m ] }</b></p> <p><b>Example:</b></p> <pre>Router(config)# network-clock quality-level tx QL-SSU-A interface GigabitEthernet 0/0/0 Router(config)# network-clock quality-level rx QL-SSU-A interface GigabitEthernet 0/0/0 Router(config)# network-clock quality-level rx ql-prc external r0 1hz</pre>	<p>回線または外部クロックソースの品質レベルを指定します。</p> <p>利用可能な品質値は、<b>network-clock synchronization ssm option</b> コマンドで指定された G.781 同期設定によって異なります。</p> <ul style="list-style-type: none"> <li>オプション 1: 利用可能な値は QL-PRC、QL-SSU-A、QL-SSU-B、QL-SEC、および QL-DNU です。</li> <li>オプション 2、GEN1: 利用可能な値は QL-PRS、QL-STU、QL-ST2、QL-SMC、QL-ST4、および QL-DUS です。</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>オプション 2、GEN 2: 利用可能な値は QL-PRS、QL-STU、QL-ST2、QL-TNC、QL-ST3、QL-SMC、QL-ST4、および QL-DUS です。</li> </ul>
<b>Step 11</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> Device(config)# <b>interface</b> gigabitethernet 0/0/0	トランクインターフェイスを指定し、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。
<b>Step 12</b>	<b>network-clock source quality-level</b> <i>value</i> { <b>tx</b>   <b>rx</b> } <b>Example:</b> Router(config-if)# <b>network-clock source quality-level</b> QL-PRS <b>tx</b>	(任意) ローカルクロック選択プロセスに強制 QL 値を提供します。
<b>Step 13</b>	<b>synchronous mode</b> <b>Example:</b> Router(config-if)# <b>synchronous mode</b>	イーサネットインターフェイスを同期モードに設定し、インターフェイスで ESMC プロセスおよび QL プロセスを自動的に有効にします。
<b>Step 14</b>	<b>end</b> <b>Example:</b> Device(config-if)# <b>end</b>	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。





## CHAPTER 8

# グローバルナビゲーション衛星システムの 設定

- [GNSS に関する情報](#) (89 ページ)
- [注意事項と制約事項](#) (92 ページ)
- [GNSS 用の衛星コンステレーションの設定, on page 92](#)
- [設定の確認](#) (93 ページ)

## GNSS に関する情報

産業用オートメーションと制御、電力、および軍事ネットワークでは、正確かつ同期された時刻を得るために、ネットワーク内に多数のデバイスが必要です。IR8340 タイミングモジュールにはグローバルナビゲーション衛星システム (GNSS) 受信機が内蔵されているため、ルータは自分の位置を特定し、衛星コンステレーションから正確な時刻を取得できます。GNSS 機能は、ネットワーク同期の計画を簡素化し、階層型ネットワークにおけるネットワーク同期の問題を解決する柔軟性と復元性を提供します。

### GNSS ハードウェア

IR8340 タイミングモジュールは、ホストシステムに対して正確な周波数と位相を出力する GNSS 受信機を使用します。受信機には、外部の GNSS アンテナに接続して、GNSS 衛星信号を自動的に取得し、最大 32 個の GNSS 衛星を追跡し、位置、速度、方位、時間を計算するために必要なすべての回路が含まれます。正確な 1 Pulse-Per-Second (PPS) と安定した 10 MHz 周波数出力を提供します。詳細については、[GNSS シグナリング](#) (91 ページ) を参照してください。



(注) すべての GNSS アラームを確認できるように、GNSS には GPS LRM-400 ケーブルを選択することをお勧めします。サポートされるアンテナおよびケーブルのリストについては、『*Cisco Catalyst IR8340 Rugged Series Router Hardware Installation Guide*』を参照してください。

GNSS チップは、次の周波数帯域をサポートしています。

- 自動: GPS + QZSS + GLONASS (デフォルト)

- GPS
- GLONASS
- BeiDou
- Galileo

## ソフトウェア

GNSS 機能では、次の機能をサポートしています。

- 時刻モード：受信機の位置が既知で固定されている場合の特別な受信機モードで、利用可能なすべての衛星を使用して時刻のみが計算されます。
- 測量：時刻モードを使用する前に実行する手順。すべての有効な 3D 位置ソリューションの加重平均を算出することにより、静止した受信機の位置を決定します。受信機は、事前定義された標準偏差に達し、最小観測時間が経過するまで、長時間にわたって平均位置を計算します。その後、受信機は自動的に固定モードに設定され、タイミング機能がアクティブになります。
- 測量および固定位置ナビゲーションにより、信号レベルが低い場合でもタイミングジッターが減少し、たった 1 つの衛星が視界にあるだけで同期を維持できます。
- 時刻パルス精度：晴天時：20 ns | 屋内：500 ns。
- GNSS 受信機を設定します。
- 受信機がロックを取得した後、ソフトウェアは次の機能を 1 秒に 1 回実行します。
  - 新しい時刻/日付を読み取ります。
  - ハードウェアから対応する PPS タイムスタンプを読み取ります。
  - 時刻/日付と PPS タイムスタンプを GNSS 用のタイムサービス SW 仮想クロック/サーボにフィードします。

GNSS SW 仮想クロック時間は、PTP 出力を駆動するために使用できます。

**constellation** CLI を使用すると、これらのコンステレーションを選択できます。コンステレーションが変更されると、新しいコンステレーションにロックするために測量プロセスが再起動されます。詳細については、[GNSS 用の衛星コンステレーションの設定 \(92 ページ\)](#) を参照してください。

デフォルトの TOD 形式は **ubx** で、出力 1PPS は GNSS がロックされているとき（たとえば、PRTC モード）に取得できます。

周波数 1hz：ロックを有効にするには、次のコマンドが必要です。

```
Router(config)#network-clock synchronization automatic
```

```
Router(config)#network-clock synchronization mode QL-enabled
```

```
Router(config)#network-clock quality-level rx QL-PRC External R0 1hz
```

```
Router(config)#network-clock input-source 1 External R0 1hz
```

```
Router(config)#network-clock wait-to-restore 10 global
```

## GNSS シグナリング

GNSS 受信機が衛星を捕捉し、ホストシステムにタイミング信号を提供するプロセスには2つの段階があります。

- **自己測量モード:** リセット時、GNSS 受信機が自己測量モードで起動し、最低4つの異なる衛星にロックして、現在位置で3-D FIXを取得しようとします。これらの衛星では約2,000の異なる位置を計算します。これには約35分かかります。また、この段階で、GNSS 受信機は正確なタイミング信号を生成し、「正常 (GPS にロック)」状態を実現できます。自己測量モードで取得されたタイミング信号は、20秒間オフにすることができます。したがって、Cisco IOS は、OD モードでのみ PPS を収集します。

自己測量が完了すると、結果が GNSS 受信機フラッシュに保存されるため、次の自己測量の実行時に OD モードへの移行が高速化されます。**gnss self-survey restart** Cisco IOS コマンドを使用して、自己測量プロセスを手動で再起動できます。自己測量モードが再び完了すると、GNSS 受信機フラッシュの結果は更新された結果で上書きされます。

- **Over-Determined (OD) クロックモード:** 自己測量モードが完了し、位置情報がデバイスの不揮発性メモリに保存されると、デバイスはODモードに移行します。このモードでは、GNSS 受信機は、自己測量モードで取得した衛星位置に基づいてタイミング情報を出力します。

GNSS 受信機は、次のような理由があるまで OD モードのままです。

- 100 m を超えるアンテナの位置移動の検出。これにより、自己測量の自動再起動がトリガーされます。
- **gnss self-survey restart** コマンドを使用した自己測量の手動再起動。

GNSS 受信機が衛星システムにロックすると、10 ミリ秒幅の PPS パルスと、衛星システムに応じた現在の時刻/日付を Cisco IOS タイムサービスに送信します。

## GNSS LED

GNSS LED (ケーブル側と電源側の LED に「GPS」のラベルが付いています) は、GNSS ステータスを示します。次の表に、LED の色とその意味を示します。

表 9: GNSS LED

色	ステータス
緑の点滅	衛星 FIX を取得しようとしています。
緑の点灯	GNSS には有効な信号/FIX があります。
橙の点滅	アンテナ障害があります。

色	ステータス
消灯	GNSS は設定されていません。

## 注意事項と制約事項

- GNSS は、PTP の Default プロファイルと Power プロファイルのタイミングソースとしてのみ使用できます。
- GNSS は、PTP が GMC-BC モードの場合にのみ、PTP のタイミングソースとして使用できません。
- 次の GNSS イベントが発生すると、Syslog メッセージが送信されます。
  - GNSS が自己測量モードに入る
  - GNSS が OD モードに達する
  - GNSS のファームウェア アップグレードが進行中、完了、または失敗
- ルータが PTP グランドマスタークロックであり、アンテナ信号が失われると、クロック品質が低下し、グランドマスター クロック スイッチオーバーが行われます。
- GPS アンテナアラームは、外部リレーアラームをトリガーしません。

## GNSS 用の衛星コンステレーションの設定

GNSS 用の衛星コンステレーションを設定するには、次の手順を実行します。

### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Router# <b>configure terminal</b>	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 2	<b>gnss</b> <b>Example:</b> Router(config)# <b>gnss</b>	GNSS を有効にします。GNSS を有効にすると、GNSS プロセスが実行され、GNSS Pulse-Per-Second (PPS) タイムスタンプ情報が収集されます。  GNSS が無効になっている場合、チップは正常に動作しますが、GNSS タイムスタンプと PPS 情報を収集するソフトウェアプロセスは実行されません。

	Command or Action	Purpose
Step 3	<p><b>[no] constellation {auto   galileo   gps   glonass   beidou}</b></p> <p><b>Example:</b></p> <pre>Router(config-gnss)# <b>constellation gps</b></pre>	<p>(オプション) GNSS コンスタレーションを設定します。デフォルトは auto (GPS+GLONASS+QZSS) です。アクティブなコンスタレーションは常に 1 つだけです。</p>
Step 4	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-gnss)# <b>exit</b></pre>	<p>GNSS 設定モードを終了します。</p>

## 設定の確認

コマンド	目的
<b>show gnss status</b>	GNSS ステータスを表示します。 以下の出力例とフィールドの説明を参照してください。
<b>show gnss satellite {all   satellite-number}</b>	GNSS で追跡した衛星のステータスを表示します。 信号強度は、キャリア対ノイズ密度 (C/N0) の形式で表示されます。信号強度の単位は dB-Hz で、単位帯域幅 (Hz) あたりのキャリア電力とノイズ電力 (dB) の比率を表します。受信した衛星信号の電力は、ユーザーのアンテナ利得、衛星の垂直方向の角度、および衛星の経過時間によって異なります。典型的な C/N0 の範囲は 35 ~ 55 dB-Hz です。
<b>show gnss time</b>	GNSS 時刻を表示します。
<b>show gnss location</b>	GNSS 位置を表示します。
<b>show gnss device</b>	GNSS デバイス情報を表示します。
<b>show network-clocks synchronization</b>	ネットワーククロック同期ステータスを表示します。
<b>show platform hardware network-clocks</b>	ハードウェアのネットワーククロックを表示します。

次に、GNSS 受信機が自己測量モードを完了し、衛星システムからタイミング情報を提供した後の **show gnss status** の出力例を示します。

```
# show gnss status
GNSS status:
GNSS status: Enable
Clock Progress: Locked (GnssFixOK)
GNSS Fix Type: time only fix
Constellation: GLONASS
Satellite count: 9
PDOP: 99.989998 TDOP: 0.350000
HDOP: 99.989998 VDOP: 99.989998
Major Alarm: False
Minor Alarm: False
```

ステータスフィールドと可能な値は次のとおりです。

- GNSS ステータス
  - 有効
  - 無効
- 受信機ステータス
  - Auto: 2D/3D の自動モード
  - 1SV: 単一の衛星
  - 2SV: 水平 (2D)
  - 3SV: フルポジション (3D)
  - OD: Over-Determined
- 測定の進行状況: このフィールドには、測定の進行状況が、これまでに収集された FIX の割合として表示されます。自己測定の進行状況が 100% に達すると、自己測定は完了です。
- PDOP: 位置精度低下率
- HDOP: 水平精度低下率
- VDOP: 垂直精度低下率
- TDOP: 時間精度低下率
- アラーム
  - アンテナオープン
  - アンテナショート
  - 衛星を追跡していません
  - 測量中
  - 保存された位置がありません
  - うるう秒保留中



(注) GPSがアラーム状態にある場合、スイッチは衛星システムからのタイミング情報を提供していない可能性があります。

アラームは自動的に解除されます。

次に、**show gnss satellite** の出力例を示します。

```
IR8340#show gnss satellite all
All Satellites Info:

SV ID  Channel  Eph Flag  SV Used  CNR  Azimuth  Elevation  Health  Quality
-----
19      6         1        -        24   260      1          1        4
18      6         1        -        31   219      2          1        7
15      6         1        Used     46   223      42         1        7
14      6         1        Used     44   340      73         1        7
13      6         1        Used     36   22       20         1        7
4       6         1        Used     48   349      27         1        7
3       6         1        Used     48   53       51         1        7
2       6         1        Used     45   114      24         1        7
```

次に、**show gnss time** および **show gnss location** の出力例を示します。

```
IR8340# show gnss time
Current GNSS Time:
Time: 2021/12/09 07:11:59 UTC

IR8340# show gnss location
Current GNSS Location:
LOC: 12:56.187572 N 77:41.742096 E 832.44 m
```

次に、**show gnss device** の出力例を示します。

```
IR8340#show gnss device
GNSS device:
Model: NEO-M8T-0
Software version: EXT CORE 3.01 (111141)
Hardware version: 00080000
Protocol version: 22.00
Firmware version: TIM 1.10
Unique Chip ID: 311652325097
Major GNSS Satellites supported: GPS;GLO;GAL;BDS
```

次に、**show network-clocks synchronization** の出力例を示します。

```
IR8340#show network-clocks synchronization
Symbols:      En - Enable, Dis - Disable, Adis - Admin Disable
              NA - Not Applicable
              * - Synchronization source selected
              # - Synchronization source force selected
              & - Synchronization source manually switched
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
```

```

T0 : External R0 1hz
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Nominated Interfaces
  Interface          SigType      Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
  Internal           NA           NA/Dis       251   QL-SEC NA        NA
*External R0      1HZ        NA/Dis      1    QL-PRC NA      NA
IR8340#

```

次に、**show platform hardware network-clocks** の出力例を示します。

```

IR8340#show platform hardware network-clocks
DPLL1 Status:
-----
Bandwidth: 0.001 Hz
Phase Slope Limit: 885 ns/s
Current PLL1 Mode: MANUAL NORMAL
Current Input Selected: REF4 (CLK_PPS_GPS_PLL)
Current PLL1 Holdover Status: OFF
Current PLL1 Lock Status: ON
DPLL2 Status:
-----
Bandwidth: 0.001 Hz
Phase Slope Limit: 885 ns/s
Current PLL2 Mode: MANUAL NORMAL
Current Input Selected: REF4 (CLK_PPS_GPS_PLL)
Current PLL2 Holdover Status: OFF
Current PLL2 Lock Status: ON

IR8340#show platform hardware network-clocks
Current Input Status:
REF0 (CLK_LOOPBACK1) : OK
REF1 (CLK_LOOPBACK2) : OK
REF2 ((TDM_SYNC_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
REF3 (RSV_2_M_PLL) : FAIL (SCM, CFM, GST, PFM failed)
REF4 (CLK_PPS_GPS_PLL) : OK
REF5 (CLK_PPS_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
REF6 (CLK_REC_25M_WAN1) : FAIL (SCM, CFM, GST, PFM failed)
REF7 (CLK_REC_25M_WAN2) : FAIL (SCM, CFM, GST, PFM failed)
REF8 (CLK20M_OCXO) : OK
REF9 (RSV_1_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)

DCO Frequency:
Current_DCO_Freq_Offset: -0.033687

IR8340#

```

## 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。