Cisco Nexus 3550-T NX-OS システム管理構成ガイド、リリース 10.6（x）

最終更新：2026 年 1 月 2 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 3550-T スイッチの関連資料

Cisco Nexus 3550-T スイッチ全体のマニュアル セットは、次の URL にあります。

https://www.cisco.com/c/en/us/support/switches/nexus-3550-series/series.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

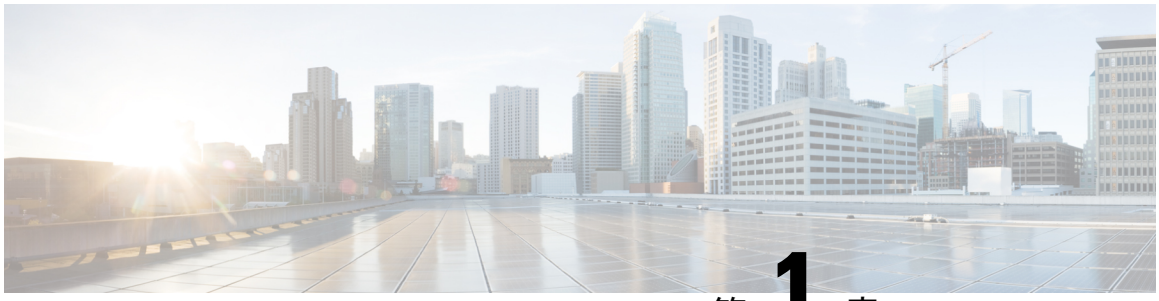
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新機能および変更された機能に関する情報

ここでは、このリリースで追加および変更された情報を示します。

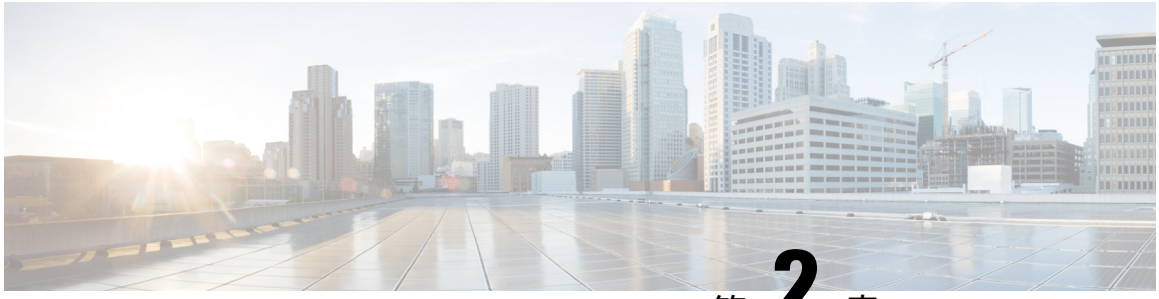
新機能および変更された機能に関する情報

次の表は、「Cisco Nexus 3550-T NX-OS システム管理構成ガイド、リリース 10.6(x)」に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 *1*: 新機能および変更された機能に関する情報

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.6(1)F	N/A

新機能および変更された機能に関する情報



第 2 章

システム管理の概要

ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1 つの NXOS ソフトウェア イメージで構成されています。このイメージは、すべての Cisco Nexus 3550-T スイッチで実行されます。

高精度時間プロトコル

高精度時間プロトコル（PTP）は、ネットワークに分散したノード間で時刻同期を行うプロトコルで、IEEE 1588 に定義されています。PTP を使用すると、イーサネット ネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。PTP は、境界クロック機能を備えた IPv4マルチキャスト、2 ステップマスター、バージョン 2 でのみサポートされます。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）を使用して、デバイスに直接接続されているすべてのシスコ製機器を検出し、情報を表示できます。CDP は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含む、シスコ製のあらゆる機器で動作します。CDP は、メディアにもプロトコルにも依存せず、ネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

Link Layer Discovery Protocol

リンク層検出プロトコル（LLDP）はベンダーに依存しない、単一方向のデバイス ディスカバリ プロトコルです。このプロトコルでは、ネットワーク上の他のデバイスにネットワーク デバイスから固有の情報をアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する2つのシステムで互いの情報を学習できます。LLDPはグローバルに、またはインターフェイスごとにイネーブルにすることができます。

Secure Erase

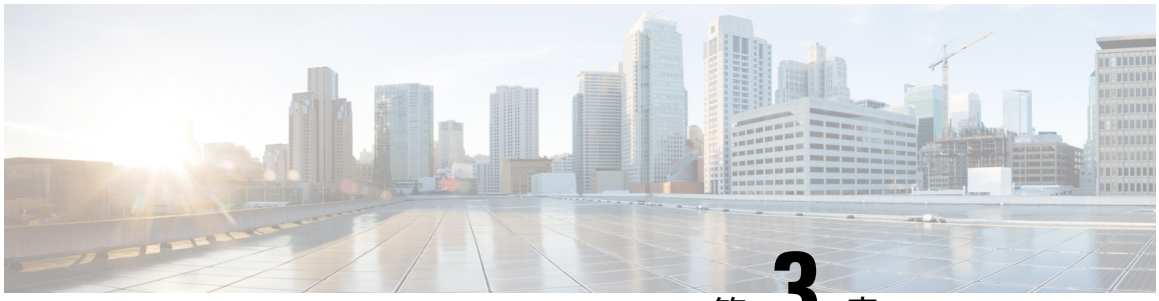
Secure Erase 機能は、 Nexus 3550-T スイッチのすべての顧客情報を消去します。Secure Eraseは、Return Merchandise Authorization（RMA）、アップグレードまたは交換、またはシステムのサポート終了により製品が削除された状態で、Cisco NX-OS デバイス上のすべての識別可能な顧客情報を削除する操作です。

高精度のタイムスタンピング

高精度タイムスタンプ（HPT）機能は、 Cisco Nexus N3550-T スイッチに入力されるパケットの高精度タイムスタンプを可能にします。タイムスタンプは、パケットがN3550-T前面パネルポートに到着した時刻に対応します。ファブリックを通過するデータ パケットのタイムスタンプがサポートされています。この機能は、任意の出力ポートで有効にできます。Rx タイムスタンプとも呼ばれます。

スイッチド ポート アナライザ

イーサネット スイッチド ポート アナライザ（SPAN）を設定すると、デバイスの入出力トラフィックをモニタできます。SPAN の機能を使用すると、送信元ポートから宛先ポートへのパケットを複製できます。



第 3 章

PTP の設定

この章では、Cisco NX-OS デバイスで高精度時間プロトコル（PTP）を設定する方法について説明します。

この章は、次の項で構成されています。

PTP について

PTP は、ネットワークに分散したノード間で時刻同期を行うプロトコルで、IEEE 1588 に定義されています。PTP を使用すると、イーサネット ネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。

PTP システムは、PTP および非 PTP デバイスの組み合わせで構成できます。PTP デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、通常のネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

PTP は、システムのリアルタイム PTP クロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスタークロック（階層の最上部にあるクロック）を持つマスター/スレーブ同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTP タイミング メッセージを交換することによって実現されます。PTP は、PTP ドメインと呼ばれる論理範囲内で動作します。

PTP は次の機能をサポートしています。

- マルチキャスト PTP 転送：マルチキャスト転送モードでは、PTP はデバイス間の通信に IEEE 1588 標準に従ってマルチキャスト宛先 IP アドレス 224.0.1.129 を使用します。送信元 IP アドレスの場合、PTP ドメインでユーザが設定可能なグローバル IP アドレスを使用します。
- PTP マルチキャスト設定は、L2 または L3 の物理インターフェイスでのみサポートされます。PTP は、ポートチャネル、SVI、トンネルなどの仮想インターフェイスではサポートされません。
- IP over UDP over PTP カプセル化：PTP は、IP 上のトランスポート プロトコルとして UDP を使用します。PTP はイベント メッセージに UDP ポート 319 を使用し、デバイス間の一般的なメッセージ通信に 320 を使用します。
- PTP プロファイル：PTP はデフォルト（1588）および SMPTE 2059-2 プロファイルをサポートします。すべての同期要求間隔と遅延要求間隔が異なります。デフォルトプロファイルの詳細については、IEEE 1588 を参照してください。SMPTE 2059-2 の詳細については、それぞれの仕様を参照してください。
- パス遅延測定：マスターとスレーブのデバイス間の遅延を測定する遅延要求および応答メカニズムをサポートします。
- メッセージ間隔：デバイス間でアナウンス、同期、および遅延要求メッセージを送信する必要がある間隔を設定できます。
- ベスト マスター クロック（BMC）の選択：BMC アルゴリズムは、1588 仕様に従って受信したアナウンス メッセージに基づいて、PTP 対応インターフェイスのマスター、スレーブ、およびパッシブ状態を選択するために使用されます。

PTP デバイス タイプ

PTP デバイス タイプは設定可能で、クロック タイプの設定に使用できます。

クロック

次のクロックは、一般的な PTP デバイスです。

オーディナリ クロック

エンド ホストと同様に、単一の物理ポートに基づいてネットワークと通信します。オーディナリ クロックはグランドマスター クロックとして動作できます。

境界クロック

通常、複数の物理ポートがあり、各ポートはオーディナリ クロックのポートのように動作します。ただし、各ポートはローカル クロックを共有し、クロックのデータ セットはすべてのポートに共通です。各ポートは、境界クロックのその他すべてのポートから使用可能な最善のクロックに基づいて、個々の状態を、マスター（それに接続されている他のポートを同期する）またはスレーブ（ダウンストリーム ポートに同期する）に決定します。同期とマスター/スレーブ階層の確立に関するメッセージは、境界クロックのプロトコル エンジンで終了し、転送されません。

トランスペアレント クロック

通常のスイッチやルータなどのすべてのPTPメッセージを転送しますが、スイッチでのパケットの滞留時間（パケットがトランスペアレント クロックを通過するために要した時間）と、場合によってはパケットの入力ポートのリンク遅延を測定します。トランスペアレント クロックはグランドマスター クロックに同期する必要がないため、ポートの状態はありません。

次の 2 種類のトランスペアレント クロックがあります。

エンドツーエンド トランスペアレント クロック

PTPメッセージの滞留時間を測定し、PTPメッセージまたは関連付けられたフォローアップ メッセージの修正フィールドの時間を収集します。

ピアツーピア トランスペアレント クロック

PTPメッセージの滞留時間を測定し、各ポートと、リンクを共有する他のノードの同じように装備されたポートとの間のリンク遅延を計算します。パケットの場合、この着信リンクの遅延は、PTPメッセージまたは関連付けられたフォローアップ メッセージの修正フィールドの滞留時間に追加されます。

（注） PTPは境界クロック モードのみで動作します。シスコでは、スイッチに接続された、同期を必要とするクロックが含まれるサーバを使用して、グランドマスター クロック（10 MHz）アップストリームを配置することを推奨します。

エンドツーエンド トランスペアレント クロック モードとピアツーピア トランスペアレント クロック モードはサポートされません。

クロック モード

IEEE 1588 規格は、PTP をサポートするデバイスが 1 ステップと 2 ステップで動作するための 2 つのクロックモードを指定しています。

1 ステップ モード：

1 ステップ モードでは、クロック同期メッセージに、マスター ポートがメッセージを送信した時刻が含まれます。ASIC は、同期メッセージがポートを出るときにタイムスタンプを追加します。

スレーブ ポートは、同期メッセージの一部として送信されるタイムスタンプを使用します。

2 ステップ モード：

2 ステップ モードでは、同期メッセージがポートを出た時刻は後続のフォローアップ メッセージで送信されます。これは、デフォルトのモードです。

（注） Cisco Nexus 3550-T リリース 10.2（3t）は 2 ステップ モードのみをサポートします。

PTP プロセス

PTPプロセスは、マスター/スレーブ階層の確立とクロックの同期の2つのフェーズで構成されます。

PTPドメイン内では、オーディナリ クロックまたは境界クロックの各ポートが、次のプロセスに従ってステートを決定します。

- 受信したすべての（マスターステートのポートによって発行された）アナウンス メッセージの内容を検査します
- 外部マスターのデータ セット（アナウンス メッセージ内）とローカル クロックで、優先順位、クロック クラス、精度などを比較します
- 自身のステートがマスターまたはスレーブのいずれであるかを決定します

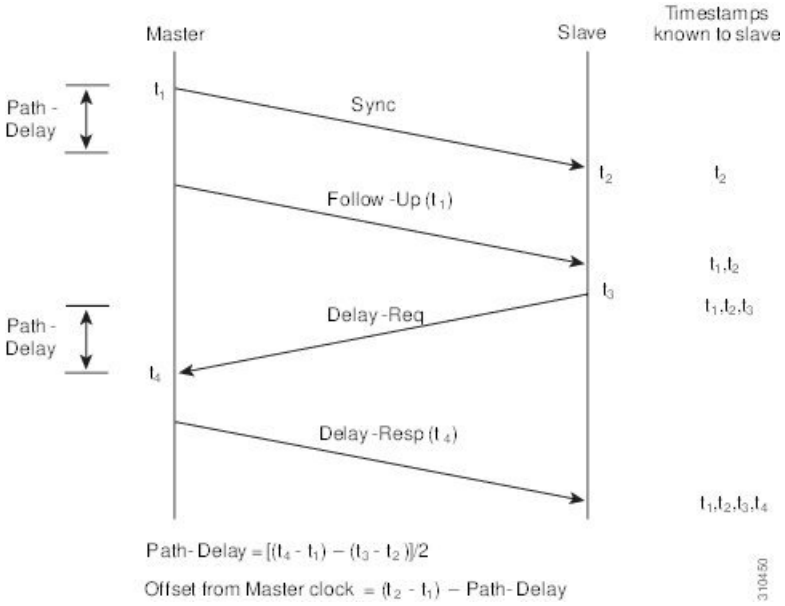
オーディナリ クロックと境界クロックは、**Sync**、**Delay_Req**、**Follow_Up**、**Delay_Resp**イベント メッセージを使用してタイミング情報を生成し、伝えます。

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. マスターが、スレーブに **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。1 ステップ **Sync** メッセージの場合、メッセージはマスターから送り出された時刻を示します。2 ステップ メッセージの場合、この時刻は、後続の **Follow-Up** イベントメッセージで送信されます。
2. スレーブは、**Sync** メッセージを受信し、受信した時刻 （t2）を記録します。
3. マスターはスレーブに対し、タイムスタンプ t1 を、**Follow_Up** イベント メッセージに埋め込むことにより送信します。
4. スレーブはマスターに対し、**Delay_Req** メッセージを送信し、送信した時刻 t3 を記録します。
5. マスターは **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. マスターはスレーブに対し、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って送信します。
7. このシーケンスの後、スレーブは 4 つすべてのタイムスタンプを所有します。これらのタイムスタンプを使用して、マスターに対するスレーブ 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。

   次の図は、タイミング情報を生成して通信する PTP プロセスのイベント メッセージを示しています。

図 *1 : PTP* プロセス



PTP のハイ アベイラビリティ

PTP のステートフル リスタートはサポートされません。リブート後に、実行中の構成が適用されます。

PTP の注意事項および制約事項

（注） スケールの情報については、リリース特定の『*Cisco Nexus 3550-T Series NX-OS Verified Scalability Guide*』を参照してください。

PTP 用 Cisco Nexus 3550 シリーズスイッチの注意事項と制約事項は次のとおりです。

- PTP が正常に機能するには、最新の SUP およびラインカードの FPGA バージョンを使用する必要があります。
- PTP はネットワークごとに 1 つのドメインに制限されます。
- ユーザ データグラム プロトコル（UDP）上の PTP 転送がサポートされます。
- PTP は境界クロック モードをサポートします。エンドツーエンド トランスペアレント クロック モードとピアツーピア トランスペアレント クロック モードはサポートされません。
- PTP はポートチャネル メンバー ポートで有効にできます。

- スレーブ ポートから受信したすべての管理メッセージは、すべてのPTP 対応ポートに転送されます。スレーブ ポートから受信した管理メッセージは処理されません。
- Cisco Nexus 3550-T シリーズ スイッチに PTP を設定する場合は、clock protocol ptp vdc 1コマンドを使用して、PTP を使用するようにクロック プロトコルを設定します。NTPは、Cisco Nexus 9000 シリーズ スイッチに設定された PTP と共存できません。
- PTP correction-range、PTP correction-range logging、および PTP mean-path-delay コマンドは、Cisco Nexus 3550-R ライン カードでサポートされます。
- PTP は、ステートフル高可用性ではサポートされません。
- PTP は、管理インターフェイスではサポートされません。
- 各ポートは、サポートされている任意の PTP プロファイルを使用して個別に構成できます。異なる PTP プロファイルは、インターフェイス上で共存できます。デフォルトの 1588 と SMPTE-2059-2 プロファイルの組み合わせがサポートされています。
- Cisco NX-OS 3550-Tリリース 10.2(3t) 以降、PTP メディア プロファイルは、Cisco Nexus 3550-T プラットフォーム スイッチでサポートされています。このプラットフォーム スイッチに関するいくつかの注意事項と制約事項を次に示します。
  - IPv4 マルチキャスト、2 ステップモード、および境界クロック機能を備えた PTPv2 がサポートされています。
  - +-500ns の修正範囲では、-3 ログ秒の PTP 同期間隔と PTP 遅延要求間隔が推奨されます。
  - ユニキャストやユニキャスト ネゴシエーションなどの他の PTP 機能はサポートされていません。

PTP のデフォルト設定

次の表に、PTP パラメータのデフォルト設定を示します。

表 *2:* デフォルトの *PTP* パラメータ

パラメータ	デフォルト
PTP	ディセーブル
PTP バージョン	2
PTP ドメイン	0
クロックをアドバタイズする場合、PTP プライオリティ 1 値	255

パラメータ	デフォルト
クロックをアドバタイズする場合、PTP プライオリティ 2 値	255
PTP アナウンス間隔	1 ログ秒
PTP アナウンス タイムアウト	3 アナウンス間隔
PTP 遅延要求間隔	• 0 ログ秒
PTP 同期間隔	• – 2 ログ秒
PTP VLAN	デフォルト VLAN は 1 です。

PTP の設定

PTP のグローバルな設定

デバイスでPTPをグローバルにイネーブルまたはディセーブルにできます。また、ネットワーク内のどのクロックがグランドマスターとして選択される優先順位が最も高いかを判別するために、さまざまな PTP クロック パラメータを構成できます。

（注） PTP プロトコルによって更新されるローカル クロックのクロック プロトコル PTP vdc1 を常に設定する必要があります。設定は、**show running-config clock_manager** コマンドを使用して確認できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature ptp** 例： `switch(config)# feature ptp`	デバイス上で PTP を有効または無効にします。 （注） スイッチの PTP をイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。

	コマンドまたはアクション	目的
ステップ 3	（任意）[**no**] **ptp domain** *number* 例： `switch(config)# ptp domain 1`	このクロックで使用するドメイン番号を構成します。PTP ドメインを使用すると、1 つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。 指定できる数の範囲は 0 ～ 127 です。
ステップ 4	（任意）[**no**] **ptp priority1** *value* 例： `switch(config)# ptp priority1 1`	このクロックをアドバタイズするときに使用する priority1 の値を構成します。この値はベスト マスター クロック選択のデフォルトの基準（クロック品質、クロック クラスなど）を上書きします。低い値が優先されます。 *value* の範囲は 0 ～ 255 です。 （注） スイッチが外部グランド マスター クロックと同期するには、ローカル スイッチの PTP 優先順位の値を外部グランドマスタークロック の優先順位の値よりも大きく設定する必要があります。
ステップ 5	（任意）[**no**] **ptp priority2** *value* 例： `switch(config)# ptp priority2 1`	このクロックをアドバタイズするときに使用する priority2 の値を構成します。この値は、デフォルトの基準では同等に一致する 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。 *value* の範囲は 0 ～ 255 です。 （注） スイッチが外部グランド マスター クロックと同期するには、ローカル スイッチの PTP 優先順位の値を外部グランドマスタークロック の優先順位の値よりも大きく設定する必要があります。

	コマンドまたはアクション	目的

ステップ 6	[**no**] **ptp management**
	例：
	`switch(config)# ptp management`
	`switch(config-ptp-profile)#`
		PTP管理パケットのサポートを設定します。このコマンドは、デフォルトでイネーブルになっています。
		no：管理パケットのサポートを無効にします。

ステップ 7	（任意） [**no**] **ptp delay tolerance** { **mean-path** | **reverse-path** } *variation*
	例：
	`switch(config)# ptp delay tolerance mean-path 50.5`
	`switch(config)#`
		PTP 遅延平均パス/リバース パスの許容差の変動を設定します。
		mean-path：PTP BMC アルゴリズムによって計算された平均パス遅延（MPD）のスパイクを無視します。
		reverse-path：PTP BMC アルゴリズムによって計算された（t4-t3）のスパイクを無視します。
		variation:：スパイクの許容度を定義するパーセンテージ。単一の 10 進数の数値を使用します。範囲は 1.0ー100.0 です。

ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

インターフェイスでの PTP の設定

PTP をグローバルにイネーブルにしても、デフォルトで、サポートされているすべてのインターフェイス上でイネーブルになりません。PTP インターフェイスは個別にイネーブルに設定する必要があります。

始める前に

スイッチ上でグローバルに PTP をイネーブルにし、PTP 通信の送信元 IP アドレスを設定したことを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		PTP を有効にする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。

ステップ 3	[**no**] **ptp** 例： `switch(config-if)# ptp`	インターフェイスで PTP を有効または無効にします。
ステップ 4	（任意） [**no**] **ptp announce** {**interval** *log-seconds* | **timeout** *count*} 例： `switch(config-if)# ptp announce interval 3`	インターフェイス上の PTP アナウンス メッセージ間の間隔またはタイムアウトがインターフェイスで発生する前の PTP 間隔の数を設定します。 PTP アナウンス間隔の範囲は 0 ～ 4 ログ秒で、間隔のタイムアウトの範囲は 2 ～ 4 間隔です。
ステップ 5	（任意） [**no**] **ptp delay-request minimum interval** *log-seconds* 例： `switch(config-if)# ptp delay-request minimum interval -1`	ポートがマスター ステートの場合に PTP 遅延メッセージ間で許可される最小間隔を設定します。 範囲は log（–1）ー log（6）秒です。ここで、log（–1）は毎秒 2 フレームです。
ステップ 6	（任意） [**no**] **ptp delay-request minimum interval** [**smpte-2059-2**] *log-seconds* 例： `switch(config-if)# ptp delay-request minimum interval smpte-2059-2-1`	ポートがマスター ステートの場合に PTP 遅延メッセージ間で許可される最小間隔を設定します。 **表 *3: PTP* 遅延要求の最小間隔の範囲とデフォルト値**

オプション	範囲	デフォルト値
smpte-2059-2	-4 ー 5 ログ秒	0 ログ秒
smpte-2059-2 オプションなし	–1 ～ 6 ログ秒（ここで、–1 = 2 フレーム毎秒）	0 ログ秒

	コマンドまたはアクション	目的
ステップ 7	（任意） **[no] ptp sync interval** *log-seconds* 例： `switch(config-if)# ptp sync interval 1`	インターフェイス上の PTP 同期メッセージの送信間隔を設定します。 範囲は、log（–3）ーlog（1）秒です。メディア関連のプロファイル情報については、『メディア ソリューション ガイド向け Cisco NX-OS IP ファブリック』を参照してください。
ステップ 8	（任意） **[no] ptp sync interval [smpte-2059-2]** *log-seconds* 例： `switch(config-if)# ptp sync interval smpte-2059-2 -1`	インターフェイス上の PTP 同期メッセージの送信間隔を設定します。 **表 *4 : PTP* 同期間隔の範囲とデフォルト値** **オプション** / **範囲** / **デフォルト値** **smpte-2059-2** / -4 ー -1 ログ秒 / -2 ログ秒 **smpte-2059-2** オプションなし / -3 ー 1 ログ秒 / -2 ログ秒
ステップ 9	（任意） **[no] ptp vlan** *vlan-id* 例： `switch(config-if)# ptp vlan 1`	PTP をイネーブルにするインターフェイスの VLAN を指定します。インターフェイスの 1 つの VLAN でイネーブルにできるのは、1 つの PTP のみです。 指定できる範囲は 1 ～ 4094 です。
ステップ 10	（任意） **show ptp brief** 例： `switch(config-if)# show ptp brief`	PTP のステータスを表示します。
ステップ 11	（任意） **show ptp port interface** *interface slot/port* 例： `switch(config-if)# show ptp port interface ethernet 1/1`	PTP ポートのステータスを表示します。
ステップ 12	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

PTP プロファイルのデフォルト

次の表に、global コマンド **ptp profile** の設定時に自動的に設定されるコマンドの範囲とデフォルト値を示します。影響を受けるグローバル コマンドの範囲を、設定されたプロファイルで許可されている範囲を超えて変更することはできません。ただし、インターフェイス モードでは、**ptp profile-override**コマンドが設定されている場合は変更できます。

表 *5:* 範囲とデフォルト値

パラメータ	範囲またはコンフィギュレーション モード	デフォルトプロファイルでサポートされる値の範囲	デフォルト プロファイルのデフォルト値	インターフェイスで設定された「**ptp profile-override**」の値の範囲（デフォルトは設定されたプロファイルに基づく）
モード	グローバル	none	none	変更なし
domain	グローバル	0 ～ 63	0	変更なし
priority1	グローバル	0 ～ 255	255	変更なし
priority2	グローバル	0 ～ 255	255	変更なし
コスト	インターフェイス	設定不能	設定不能	0 ～ 255
トランスポート	インターフェイス	ipv4	ipv4	ethernet、ipv4
transmission	インターフェイス	multicast	multicast	変更なし
役割	インターフェイス	dynamic、master、slave	ダイナミック	変更なし
アナウンス間隔	インターフェイス	0 ～ 4 -3ー1（smpte-2059-2）	1	-3 ～ 4 -3ー1（smpte-2059-2）
delay-request minimum interval	インターフェイス	-1 ～ 6 -4 ー 5（smpte-2059-2）	0	-4 ～ 6 -4 ー 5（smpte-2059-2）
同期間隔	インターフェイス	-3 ～ -1 -7 ー 0（smpte-2059-2）	-2	-4 ー 1 -7 ー 0（smpte-2059-2）

PTP 通知の設定

始める前に

次の重要な PTP イベントの通知を有効化、無効化、およびカスタマイズできます。

- グランド マスター（GM）クロックの変更
- 親クロックの変更
- ポートの PTP ステートの変更
- 高 PTP クロック修正

通知は、PTPから受信した情報に基づいてDMEインフラストラクチャによって生成されます。

手順

	コマンドまたはアクション	目的

ステップ 1	[**no**] **ptp notification type gm-change**
	例：
	`switch(config)# ptp notification type gm-change`
	`switch(config)#`
		PTP グランド マスター クロックが変更された場合に、変更通知を送信するようにシステムを設定します。

ステップ 2	[**no**] **ptp notification type parent-change**
	例：
	`switch(config)# ptp notification type parent-change`
	`switch(config)#`
		PTPの親クロックが変更された場合に、変更通知を送信するようにシステムを設定します。

ステップ 3	[**no**] **ptp notification type port-state-change** [**category** { **all** | **master-slave-only** }] [**interval** { **immediate** | *seconds* [**periodic-notification** { **disable** | **enable** }] }]
	例：
	`switch(config)# ptp notification type port-state-change category master-slave-only`
	`switch(config)#`
		ポート ステート変更イベントが発生した場合に通知を送信するようにシステムを設定します。
		• **category**：通知を送信するために必要な状態変更を指定します。
		• **all**：すべてのポート状態の変更が報告されます。
		（注）
		all オプションを使用すると、多くの通知が表示されます。
		• **master-slave-only**：マスター スレーブ状態との間のポート状態の変更のみが報告されます。

	コマンドまたはアクション	目的
		• **interval** *seconds*：ポート状態変更通知は、設定された間隔（1 ー 300 秒、粒度は1秒）で送信されます。 • **periodic-notification**：設定された間隔の間にポート ステートの変更が発生していない場合でも、定期的な通知を送信するかどうかを決定します。 **disable**：ポート状態変更通知は、現在の状態が以前に報告された状態と同じでない場合にのみ報告されます。設定された定期的な間隔中の中間状態の変更は無視されます。たとえば、ポートが時刻 X で MASTER であり、DISABLED に変更されてから X + periodic-interval が発生するまでに MASTER に戻る場合、その間のイベントは通知されません。 **enable**：ポート ステート変更通知は、ポート ステートの変更に関係なく、設定された間隔で送信されます。 • **interval immediate**：ポートの状態変化通知は、状態が変化すると送信されます。

ステップ 4	[**no**] **ptp notification type high-correction** [**interval** { *seconds* [**periodic-notification** { **disable** | **enable** }] | **immediate** }]
	例：
	`switch(config)# ptp notification type high-correction interval immediate`
	`switch(config)#`
		PTP 高補正イベントが発生した場合に高補正通知を送信するようにシステムを設定します。高修正イベントは、修正が **ptp correction-range** コマンドで設定された値を超えた場合です（次のオプションの手順を参照）。
		• **interval** *seconds*：設定された間隔（1 ー 300 秒、精度 1 秒）で高修正通知が送信されます。
		• **periodic-notification**：設定された間隔中に高度な修正が行われなかった場合でも、定期的な通

	コマンドまたはアクション	目的
		知を送信するかどうかを決定します。 **disable**：設定された定期的な間隔の間に高補正イベントが発生した場合にのみ通知を送信します。これがデフォルトの設定です。 **enable**：設定された定期的な間隔の間に高修正イベントの数に関係なく通知を送信します。そのようなイベントがない場合、ペイロードは定期的な間隔の間にゼロ修正イベントを示します。 • **interval immediate**：高度な修正イベントが発生するとすぐに通知を送信します。

ステップ 5	（任意）[**no**] **ptp correction-range** { *nanoseconds* | **logging** }
	例：
	`switch(config)# ptp correction-range 200000`
	`switch(config)#`
		超過すると、PTP 高補正が発生したことを示すしきい値を設定します。範囲は 10 ー 1000000000 です。デフォルト値は 100（マイクロ秒の 10 倍）です。

PTP 構成の確認

NTP 構成を表示するには、次のタスクのうちのいずれかを実行します。

表 *6 : PTP Show* コマンド

コマンド	目的
show ptp brief	PTP のステータスを表示します。
show ptp clock	ローカルクロックのプロパティ（クロック ID など）を表示します。

コマンド	目的
show ptp clock foreign-masters-record	PTP プロセスが認識している外部マスターの状態を表示します。外部マスターごとに、出力に、クロック ID、基本的なクロック プロパティ、およびクロックがグランドマスターとして使用されているかどうかが表示されます。
show ptp corrections	最後の数個の PTP 修正を表示します。
show ptp counters [**all** | **interface ethernet** *slot/port*]	すべてのインターフェイスまたは指定したインターフェイスの PTP パケットカウンタを表示します。
show ptp parent	PTP の親のプロパティを表示します。
show ptp port interface ethernet *slot/port*	スイッチの PTP ポートのステータスを表示します。
show ptp time-property	PTP クロック プロパティを表示します。
show running-config ptp [**all**]	PTP の実行コンフィギュレーションを表示します。
clear ptp counters [**all** | **interface ethernet** *slot/port*]	特定のインターフェイスまたは PTP が有効になっているすべてのインターフェイスで送受信されるすべての PTP メッセージをクリアします。

PTP の設定例

次に、デバイス上で PTP をグローバルに設定し、PTP 通信用の送信元 IP アドレスを指定し、クロックの優先レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
switch(config)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 0:22:55:ff:ff:79:a4:c1
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1
Priority2 : 1
```

```
Clock Quality:
  Class : 248
  Accuracy : 254
  Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Mon Dec 22 14:13:24 2014
```

次に、インターフェイス上で PTP を構成し、アナウンス、遅延要求、および同期メッセージの間隔を構成する例を示します。

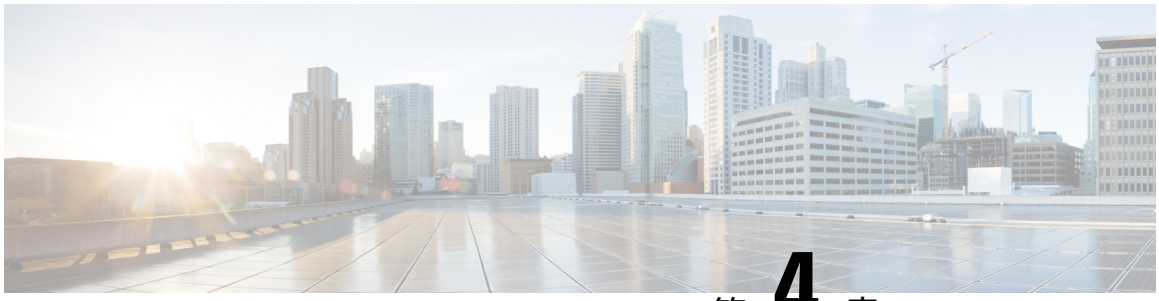
```
switch# configure terminal
switch(config)# interface Ethernet 1/1
switch(config-if)# ptp
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval smpte-2059-2 -3
switch(config-if)# ptp sync interval smpte-2059-2 -3
switch(config-if)# no shutdown
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
Eth1/1 Master
switch(config-if)# show ptp port interface ethernet 1/1
PTP Port Dataset: Eth1/1
Port identity: clock identity: 0:22:55:ff:ff:79:a4:c1
Port identity: port number: 1028
PTP version: 2
Port state: Master
Delay request interval(log mean): 4
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): 1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
1588 IEEE	1588 IEEE 標準

関連資料



第 4 章

CDP の設定

この章では、Cisco NX-OS デバイス上で Cisco Discovery Protocol（CDP）を設定する方法について説明します。

この章は、次の項で構成されています。

CDP について

Cisco Discovery Protocol（CDP）は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含め、シスコ製のあらゆる機器で動作する、メディアにもプロトコルにも依存しないプロトコルです。CDP を使用すると、デバイスに直接接続されているすべてのシスコ デバイスの情報を検出して表示できます。

CDP はネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

CDP が設定された各デバイスは、マルチキャスト アドレスに定期的にアドバタイズメントを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズメントには保持時間情報も含まれます。保持時間は、受信デバイスが CDP 情報を削除するまでに保持する時間の長さを表します。アドバタイズメントまたはリフレッシュ タイマーおよびホールド タイマーを設定できます。

CDP Version-2（CDPv2）では、接続デバイスとの間でネイティブ VLAN ID またはポート デュプレックス ステートが一致していないインスタンスを追跡できます。

CDP では、次の Type-Length-Value（TLV）フィールドがアドバタイズされます。

- デバイス ID

- アドレス
- ポート ID
- 機能
- バージョン
- プラットフォーム
- ネイティブ VLAN
- 全二重/半二重
- SysName
- SysObjectID
- 管理アドレス
- Physical Location

すべての CDP パケットに VLAN ID が含まれます。レイヤ 2 アクセス ポート上で CDP を設定した場合、そのアクセス ポートから送信される CDP パケットには、アクセス ポートの VLAN ID が含まれます。レイヤ 2 トランク ポート上で CDP を設定した場合は、そのトランク ポートから送信される CDP パケットに、トランク ポート上で許可設定されている最小の VLAN ID が含まれます。トランク ポートは、そのトランク ポートの許可 VLAN リストに指定されている VLAN ID であれば、どの VLAN ID が含まれている CDP パケットでも受信できます。VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

高可用性

Cisco NX-OS は、CDP のステートフルおよびステートレス両方のリスタートをサポートします。

仮想化のサポート

Cisco NX-OS は、CDP のインスタンスを 1 つサポートします。

CDP の注意事項と制約事項

CDP に関する設定時の注意事項および制約事項は、次のとおりです。

- 接続数が 256 のハブにポートを接続した場合、CDP はポートあたり最大 256 のネイバーを検出できます。
- デバイス上で CDP をイネーブルにする必要があります。イネーブルにしておかないと、インターフェイス上で CDP をイネーブルにできません。
- CDP を設定できるのは、物理インターフェイスおよびポート チャネル上に限られます。

CDP のデフォルト設定

次の表に、CDP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
CDP	グローバルおよびすべてのインターフェイスでイネーブル
CDP version	バージョン 2
CDP device ID	シリアル番号
CDP timer	60 秒
CDP hold timer	180 秒

CDP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があります。

CDP のグローバルな有効化または無効化

CDP はデフォルトで有効になっています。CDP をディセーブルにしてから、もう一度イネーブルにできます。

インターフェイス上で CDP をイネーブルにするには、先にデバイス上で CDP をイネーブルにしておく必要があります。CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **cdp enable** 例： `switch(config)# cdp enable`	デバイス全体で CDP 機能を有効または無効にします。デフォルトでは有効。

	コマンドまたはアクション	目的
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

インターフェイス上での CDP の有効化または無効化

CDP はデフォルトで、インターフェイス上でイネーブルです。インターフェイス上で CDP をディセーブルにできます。

CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**interface** *interface slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	[**no**] **cdp enable** 例： `switch(config-if)# cdp enable`	このインターフェイスで CDP を有効または無効にします。デフォルトでは有効。 （注） CDP がデバイス上でグローバルに有効になっていることを確認します。
ステップ 4	（任意） **show cdp interface** *interface slot/port* 例： `switch(config-if)# show cdp interface ethernet 1/2`	インターフェイスの CDP 情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

CDP オプション パラメータの設定

この手順でオプションのコマンドを使用して CDP を変更できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	（任意） **cdp advertise** {**v1** | **v2**} 例： `switch(config)# cdp advertise v1`	デバイスがサポートする CDP のバージョンを設定します。デフォルトは v2 です。
ステップ 3	（任意） **cdp format device-id** {**mac-address** | **serial-number** | **system-name**} 例： `switch(config)# cdp format device-id mac-address`	CDP デバイス ID を設定します。オプションは次のとおりです。 • **mac-address**：シャーシの MAC アドレスを指定します。 • **serial-number**：シャーシのシリアル番号/組織固有識別子（OUI） • **system-name**：システム名または完全修飾ドメイン名 デフォルトは **system-name** です。
ステップ 4	（任意） **cdp holdtime** *seconds* 例： `switch(config)# cdp holdtime 150`	CDP ネイバー情報を削除するまでに保持する時間を設定します。範囲は 10 ～ 255 秒です。デフォルト値は 180 秒です。
ステップ 5	（任意） **cdp timer** *seconds* 例：	CDP がネイバーにアドバタイズメントを送信するリフレッシュ タイムを設定

	コマンドまたはアクション	目的
	`switch(config)# cdp timer 50`	します。範囲は 5 ～ 254 秒です。デフォルトは 60 秒です。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

CDP コンフィギュレーションの確認

CDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show cdp all	CDP がイネーブルになっているすべてのインターフェイスを表示します。
show cdp entry {**all** | **name** *entry-name*}	CDP データベース エントリを表示します。
show cdp global	CDP グローバル パラメータを表示します。
show cdp interface *interface slot*/*port*	CDP インターフェイスのステータスを表示します。
show cdp neighbors {**device-id** | **interface** *interface slot*/*port*} [**detail**]	CDP ネイバーのステータスを表示します。
show cdp interface *interface slot*/*port*	インターフェイスの CDP トラフィック統計を表示します。

インターフェイスの CDP 統計情報を消去するには、**clear cdp counters** コマンドを使用します。

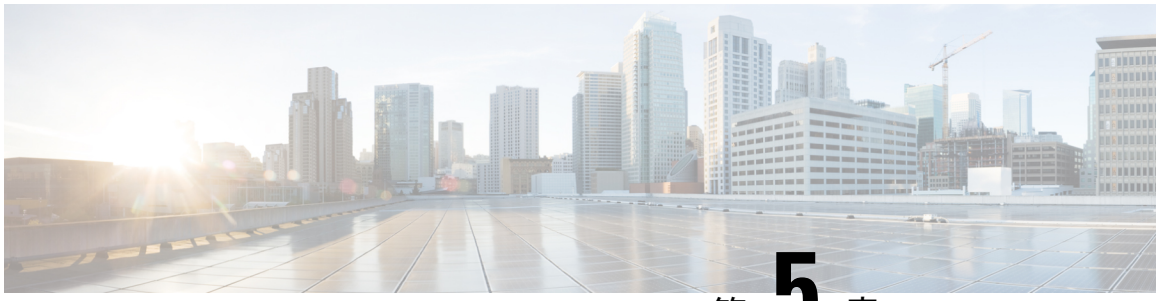
1 つまたはすべてのインターフェイスの CDP キャッシュを消去するには、**clear cdp table** コマンドを使用します。

show cdp neighbors detail コマンドを（**show cdp neighbors** コマンドの代わりに）使用することを推奨します。**show cdp neighbors** コマンドが表示するのは、プラットフォーム名の 13 文字だけです。完全なプラットフォーム名を表示するには、**show cdp neighbors detail** コマンドを使用します。

CDP のコンフィギュレーション例

CDP 機能を有効にして、リフレッシュ タイマーおよびホールド タイマーを設定する例を示します。

```
configure terminal
cdp enable
cdp timer 50
cdp holdtime 100
```



第 5 章

LLDP の構成

この章では、ローカル ネットワーク上の他のデバイスを検出するために、Link Layer Discovery Protocol（LLDP）を設定する方法について説明します。

（注） この章で使用するコマンドのシンタックスおよび使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび *Cisco IOS Configuration Fundamentals* コマンド リファレンス、リリース *12.2* の「システム管理コマンド」セクションを参照してください。

この章は、次の内容で構成されています。

LLDP について

Cisco Discovery Protocol（CDP）は、ネットワークに接続された他のシスコ デバイスを自動的に検出し学習することをネットワーク管理アプリケーションによって可能にするデバイス検出プロトコルです。Cisco Discovery Protocol（CDP）は、ネットワークに接続された他のシスコ デバイスを自動的に検出し学習することをネットワーク管理アプリケーションによって可能にするデバイス検出プロトコルです。

他社製デバイスのディスカバリを許可するために、スイッチは、IEEE 802.1ab 規格で定義されているベンダー ニュートラルなデバイス ディスカバリ プロトコルである Link Layer Discovery Protocol（LLDP）もサポートしています。LLDP を使用すると、ネットワーク デバイスはそれ自体のデバイスに関する情報を、ネットワーク上の他のデバイスにアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信する単一方向のプロトコルです。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

LLDP は一連の属性をサポートしており、これを使用して他のデバイスを検出します。これらの属性には、タイプ、長さ、および値（TLV）の説明が含まれています。LLDP デバイスは TLV を使用して、ネットワーク上の他のデバイスと情報を送受信できます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

LLDP は、デフォルトで次の TLV をアドバタイズします。

- 管理用アドレス
- ポートの説明
- ポートVLAN
- システム機能
- システムの説明
- システム名

高可用性

LLDP 機能はステートレス リスタートおよびステートフル リスタートをサポートします。リブート後に、実行中の構成が適用されます。

仮想化のサポート

Cisco Nexus® 3550-T スイッチでサポートされる LLDP のインスタンスは 1 つだけです。

LLDP に関する注意事項および制約事項

LLDP の設定のガイドラインおよび制限事項は、次のとおりです。

- インターフェイス上でLLDPをイネーブルまたはディセーブルにするには、事前にデバイス上で LLDP をイネーブルにしておく必要があります。
- LLDP は物理インターフェイスだけでサポートされています。
- LLDP は 1 つのポートにつき 1 つのデバイスを検出できます。

LLDP のデフォルト設定

この表は、LLDP のデフォルト設定を示します。

パラメータ	デフォルト
グローバル LLDP	無効
インターフェイス上の LLDP	イネーブル（LLDPがグローバルにイネーブルになった後）
LLDP 保持時間（ディセーブルになる前）	120 秒
LLDP 再初期化遅延	2 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 受信	イネーブル（LLDPがグローバルにイネーブルになった後）
LLDP 転送	イネーブル（LLDPがグローバルにイネーブルになった後）

LLDP の構成

この章では、Cisco Nexus® 3550-T スイッチに Link Layer Discovery Protocol（LLDP）を構成する方法について説明します。

LLDP をグローバルに有効化または無効化する

デバイスでLLDPをグローバルにイネーブルまたはディセーブルにできます。デバイスでLLDPパケットの送信および受信を可能にするには、LLDP をグローバルにイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature lldp** 例： `switch(config)# feature lldp`	デバイス上でLLDPをイネーブルまたはディセーブルにします。LLDPはデフォルトでディセーブルです。
ステップ 3	（任意） **show running-config lldp** 例： `switch(config)# show running-config lldp`	LLDP のグローバル コンフィギュレーションを表示します。LLDPが有効の場合、「feature lldp」と表示されます。

	コマンドまたはアクション	目的
		LLDP が無効の場合、「Invalid command」エラーが表示されます。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

インターフェイス上での LLDP の有効化または無効化

LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。ただし、LLDP パケットの送信だけ、または受信だけを実行するために、個々のインターフェイスでの LLDP のイネーブルまたはディセーブル、あるいはインターフェイスの選択的な設定を実行できます。

始める前に

デバイスで LLDP をグローバルにイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**interface** *interface slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		LLDP をイネーブルにする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。

ステップ 3	[**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	インターフェイス上で LLDP パケットの送信をイネーブルまたはディセーブルにします。LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。
ステップ 4	[**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	インターフェイス上で LLDP パケットの受信をイネーブルまたはディセーブルにします。LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポー

	コマンドまたはアクション	目的
		トされているすべてのインターフェイスで有効になります。
ステップ 5	（任意） **show lldp interface** *interface slot/port* 例： `switch(config-if)# show lldp interface ethernet 1/1`	インターフェイス上でLLDPの設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

物理インターフェイスごとの複数の LLDP ネイバー

多くの場合、ネットワーク デバイスは複数のLLDPパケットを送信しますが、そのうちの1つは実際のホストからのものです。Cisco Nexusスイッチがデバイスと通信しているが、インターフェイスごとに1つのLLDPネイバーしか管理できない場合は、実際に必要なホストとのネイバーになることが失敗する可能性があります。これを最小限に抑えるために、Cisco Nexus スイッチ インターフェイスは複数の LLDP ネイバーをサポートできるため、正しいデバイスで LLDP ネイバーになる可能性が高くなります。

同じインターフェイスで複数のLLDPネイバーをサポートするには、LLDPマルチネイバー サポートをグローバルに設定する必要があります。

LLDP マルチネイバー サポートのイネーブル化またはディセーブル化

始める前に

インターフェイスでLLDPマルチネイバー サポートを有効にする前に、次の点を考慮してください。

- デバイスでLLDPをグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

（注） LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- 1 つのインターフェイスで最大 3 つのネイバーがサポートされます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	必須: [**no**] **lldp multi-neighbor**
	例：
	`switch(config)# lldp multi-neighbor`
	`switch(config)#`
		すべてのインターフェイスのLLDPマルチネイバーサポートをグローバルに有効または無効にします。

ステップ 3	**interface** *port* / *slot*
	例：
	`switch(config)# interface 1/1`
	`switch(config-if)#`
		LLDPをイネーブルにする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。

ステップ 4	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	インターフェイスでのLLDPパケットの送信をディセーブル（またはイネーブル）にします。 （注） このインターフェイスでのLLDPパケットの送信は、グローバル **feature lldp** コマンドを使用してイネーブルにされました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 5	（任意） [**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	インターフェイスでのLLDPパケットの受信をディセーブル（またはイネーブル）にします。 （注） このインターフェイスでのLLDPパケットの受信は、グローバル **feature lldp** コマンドを使用してイネーブルになりました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 6	（任意） **show lldp interface** *port* / *slot* 例：	インターフェイス上でLLDPの設定を表示します。

	コマンドまたはアクション	目的
	`switch(config-if)# show lldp interface 1/1`	
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

ポート チャネル インターフェイスでの LLDP サポートの有効化または無効化

始める前に

ポート チャネルで LLDP サポートを有効にする前に、次の点を考慮してください。

- デバイスで LLDP をグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

（注） LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- ポート チャネルに **lldp transmit** および **lldp receive** コンフィギュレーション コマンドを適用しても、ポート チャネルのメンバーの設定には影響しません。
- LLDP ネイバーは、LLDP 送受信がポート チャネルの両側で設定されている場合にのみ、ポート チャネル間で形成されます。

（注） LLDP の送受信コマンドは、MCT および VPC では機能しません。

LLDP ポート チャネル機能をグローバルに有効にすると、LLDP 設定はこれらのポート タイプのいずれにも適用されません。ポート チャネルから設定が削除された場合、またはポート タイプ機能がグローバルに無効になった場合は、**lldp port-channel** コマンドを使用して新しくサポートされたポート チャネルで有効にすることはできません。コマンドはすでに発行されています。問題のポート チャネルで LLDP ポート チャネルを有効にするには、**lldp transmit** および **lldp receive** を各ポート チャネルに対して設定します（次の手順のステップ 4、5、および 6 を参照）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	必須: [**no**] **lldp port-channel**
	例：
	`switch(config)# lldp port-channel`
	`switch(config)#`
		すべてのポート チャネルの LLDP 送受信をグローバルに有効または無効にします。

ステップ 3	**interface port-channel** [*port-channel-number* | *port-channel-range*]
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
	例：
	複数のポート チャネルで LLDP を設定する場合は、ポート チャネル番号の範囲を入力します。
	`switch(config)# interface port-channel 1-3`
	`switch(config-if-range)#`
		LLDP を有効にするインターフェイス ポートチャネルを指定し、インターフェイス設定モードを開始します。
		LLDP を有効にするインターフェイス ポートチャネル範囲を指定し、インターフェイス範囲設定モードを開始します。

ステップ 4	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	ポート チャネルまたはポート チャネルの範囲で LLDP パケットの送信を無効（または有効）にします。 （注） このポート チャネルでの LLDP パケットの送信は、ステップ 3 の **lldp port-channel** コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 5	（任意） [**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	ポート チャネルまたはポート チャネルの範囲での LLDP パケットの受信を無効（または有効）にします。 （注） このポート チャネルでの LLDP パケットの受信は、ステップ 3 の **lldp**

	コマンドまたはアクション	目的
		port-channel コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 6	（任意） **show lldp interface port-channel** *port-channel-number* 例： `switch(config-if)# show lldp interface port-channel 3`	ポートチャネル上の LLDP 設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

LLDP オプション パラメータの設定

LLDP の更新頻度、受信デバイスが情報を破棄するまでに保持している時間、および初期化の遅延時間を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	（任意） [**no**] **lldp holdtime** *seconds* 例： `switch(config)# lldp holdtime 200`	ユーザのデバイスから送信された情報が、受信側デバイスで廃棄されるまでに保持される時間を秒単位で指定します。 値の範囲は 10 ～ 255 秒で、デフォルト値は 120 秒です。
ステップ 3	（任意） [**no**] **lldp reinit** *seconds* 例： `switch(config)# lldp reinit 5`	任意のインターフェイス上で LLDP を初期化する際の遅延時間を秒単位で指定します。 指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。

	コマンドまたはアクション	目的
ステップ 4	（任意）[**no**] **lldp timer** *seconds* 例： `switch(config)# lldp timer 50`	LLDP アップデートの送信頻度を秒単位で設定します。 値の範囲は 5 ～ 254 秒で、デフォルト値は 30 秒です。
ステップ 5	（任意）**show lldp timers** 例： `switch(config)# show lldp timers`	LLDP の保持時間、遅延時間、更新頻度の設定を表示します。
ステップ 6	（任意）**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

LLDP 設定の確認

LLDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

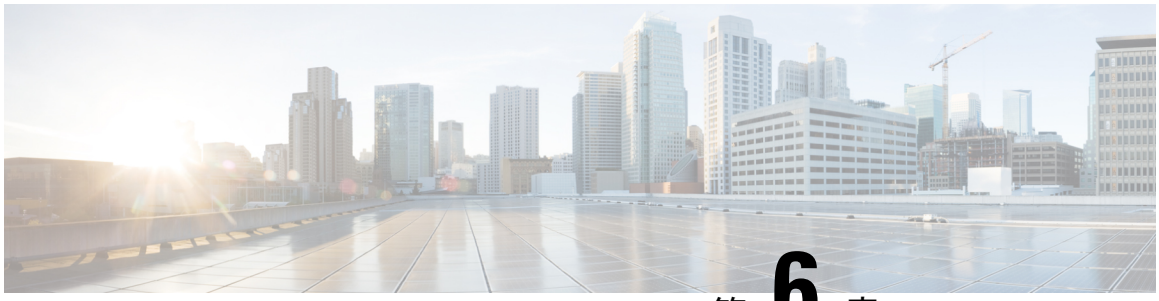
コマンド	目的
show running-config lldp	LLDP のグローバル コンフィギュレーションを表示します。
show lldp interface *interface slot*/*port*	LLDP のインターフェイス コンフィギュレーションを表示します。
show lldp timers	LLDP の保持時間、遅延時間、更新頻度の設定を表示します。
show lldp neighbors {**detail** | **interface** *interface slot*/*port*}	LLDP ネイバーのデバイス ステータスを表示します。
show lldp traffic interface *interface slot*/*port*	インターフェイス上で送信および受信された LLDP パケットの数を表示します。

LLDP の統計を消去するには、**clear lldp counters** コマンドを使用します。

LLDP の設定例

次に、1 つのデバイス上での LLDP の有効化、一部のインターフェイス上での LLDP の無効化の方法、オプションパラメータ（ホールド時間、遅延時間、更新頻度など）の構成方法の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet 1/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet 1/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
```



第 6 章

安全な消去の設定

安全に消去する（Secure Erase）機能に関する情報

Cisco Nexus 3550-T リリース 10.2(3t) 以降、Nexus 3550-T スイッチのすべての顧客情報を消去する 安全に消去する（Secure Erase）機能が導入されました。Secure Erase は、Return Merchandise Authorization（RMA）、アップグレードまたは交換、またはシステムのサポート終了により製品が削除された状態で、Cisco NX-OS デバイス上のすべての識別可能な顧客情報を削除する操作です。

Cisco Nexus 3550-T スイッチは、ストレージを消費して、システム ソフトウェア イメージ、スイッチ設定、ソフトウェア ログ、および動作履歴を保存します。これらの領域には、ネットワーク アーキテクチャや設計に関する詳細などの顧客固有の情報や、データ盗難の潜在的な標的が含まれている可能性があります。

安全に消去するプロセスは、次の 2 つのシナリオで使用されます。

- デバイスの返品許可（RMA）：RMA のためにデバイスをシスコに返送する必要がある場合は、そのデバイスの RMA 証明書を取得する前に、お客様固有のデータをすべて削除してください。
- 侵害を受けたデバイスのリカバリ：デバイスに保存されているキーマテリアルまたはクレデンシャルが侵害を受けた場合は、デバイスを初期設定にリセットし、デバイスを再設定してください。

（注） 安全に消去する機能では、外部ストレージのコンテンツは消去されません。

デバイスがリロードされて工場出荷時設定にリセットされ、ToR シャーシ モジュールがパワーダウン モードになります。工場出荷時設定にリセットすると、デバイスはすべての構成、ログ、およびストレージ情報を消去します。

安全な消去を実行するための前提条件

- 安全な消去操作を実行する前に、すべてのソフトウェアイメージ、構成、および個人データがバックアップされていることを確認してください。
- プロセスが進行中の場合は、電源の中断がないことを確認してください。

安全な消去の注意事項と制約事項

- ソフトウェア パッチは、デバイスにインストールされている場合、初期設定へのリセットプロセス後に復元されません。
- セッションを介して **factory-reset** コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

  トップ オブ ラック スイッチとスーパーバイザ モジュールは、ローダー プロンプトに戻ります。

安全な消去の設定

RMA に発送する前に必要なデータをすべて削除するには、次のコマンドを使用して安全な消去を設定します。

コマンド	目的
factory-reset module *mod* 例： `switch(config)# factory-reset [module <1>]`	**all** オプションを有効にしてコマンドを使用してください。**factory reset** コマンドを使用するために必要なシステム設定はありません。 オプション **mod** を使用して、起動構成をリセットします。 • top-of-rack（ToR; トップオブラック）スイッチの場合、コマンドは **factory-reset** または **factory-reset module 1** です。 工場出荷時の状態へのリセットプロセスが正常に完了すると、スイッチがリブートします。

factory-reset ログは次のように表示されます。

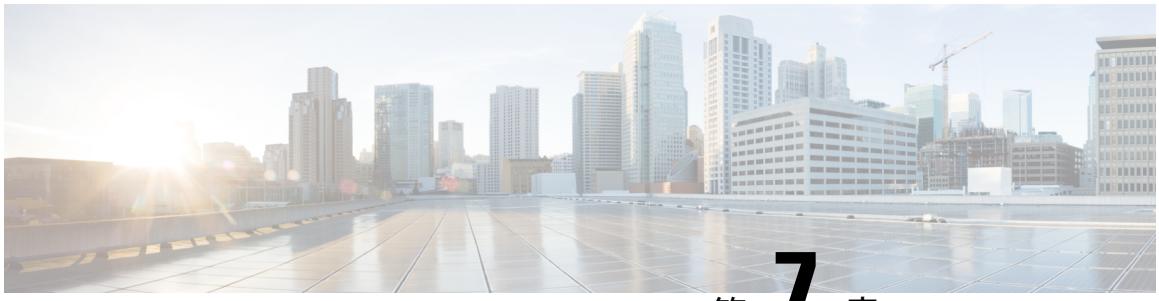
```
switch# factory-reset
!!!! WARNING !!!!
The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken in an effort to render data non-recoverable. Please, proceed
with
caution and understanding that this operation cannot be undone and will leave the system
 in
a fresh-from-factory state.
!!!! WARNING !!!!
Continue? (y/n) [n] y
A module reload is required for the reset operation to proceed.
Please, wait...

Factory reset requested! Please, do not power off module!

Python 3.7.10
Python Version 3 ...

>>>> Wiping all storage devices ...
+++ Starting NVMe secure erase for /dev/nvme0n1p +++
Using secure format for /dev/nvme0n1p...)
\
---> SUCCESS
+++ Starting cmos secure erase +++
\
 ---> SUCCESS
+++ Starting nvram secure erase +++
\
 ---> SUCCESS
>>>> Done
>>>> Initializing system to factory defaults ...
+++ Starting init-system +++
\
 ---> SUCCESS
All operations complete! Exiting..
```

安全な消去の設定



第 7 章

高精度タイムスタンピングを構成

このセクションには、次の詳細が含まれます：

概要

高精度タイムスタンプ（HPT）機能（Rx タイムスタンプとも呼ばれます）により、Cisco Nexus 3550-T スイッチの入力ポートに到着するパケットの高精度タイムスタンプが可能になります。これは、 Nexus 3550-T スイッチが受信したデータを追跡および/または記録するために使用されます。タイムスタンプは、（ホストとの間ではなく）ファブリックを通過するデータパケット用です。通常、タイムスタンプはスパン宛て先ポートで有効になっています。タイムスタンプ データ（HPT トレーラ）は、HPT 機能が有効になっているポートをパケットが出るときに追加されます。この出力ポートに接続されているアプリケーションがデータを復号化します。Githubで入手可能な N3550-timestamp-decoder を使用できます。または Wiresharkバージョン 3.0.0+ を使用 してデータをデコードできます。 *--trailer* および *--offset 20* オプションを使用してデコーダツールを実行できます。

HPTトレーラには、デバイスID、ポートID、タイムスタンプデータ、フラグおよびCRCが含まれます。デバイス ID とポート ID は、タイムスタンプデータをデバイスにマッピングするID目的で使用されます。

次に示すように、デコーダツールを活用。

```
[n3550-timestamp-decoder-master/build]$ ./timestamp-decoder --read
/users/<path-to-input-pcap>/HPT_90.cap --trailer --offset 20
```

サンプル出力は次のようになります。

```
2022/09/06-11:59:50.509047248389  (032:046)   106 bytes
```

最初の要素（日付と時間）は、タイムスタンプの詳細を表示します。次のフィールド（032:046）は、デバイス ID が 32、ポートが 46 であることを示しています。通常、ポート ID はインター

フェイス番号より 1 つ小さいため、この場合、パケットがインターフェイス e1/47 を通過したことを示しています。

Rx タイムスタンプは、デフォルトでは HW クロックと同じ期間になっています（たとえば、PTP は TAI で動作します）。NX- OSリリース 10.2(3v) 以降、新しいコマンド **time-stamp hpt utc-offset**が導入され、UTC オフセット修正を有効にして、Rx タイムスタンプが UTC期間になるようにしました。

（注） NX- OSデバイスで HPT トレーラを除去することはサポートされていません。

制限事項

HPT の制限事項は次のとおりです。

- HPTは、物理ポートまたはポートチャネルで有効にできます。ポートチャネルメンバー上で有効にすることはできません。
- ポートの HPT 構成は、ポートチャネルの一部にする前に削除する必要があります。

高精度のタイムスタンピングを有効化

この手順を活用、3550-T スイッチ ポートで HPT を有効にします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**time-stamp hpt device-id** *device_id* **例：** `switch(config)# time-stamp hpt device-id 10`	この手順は任意です。デフォルト ID の範囲は 0 ～ 255 です。デフォルトは 0 です。
ステップ 3	**interface** *interface-type interface-id* **例：** `switch(config)# interface ethernet 1/2`	インターフェイス コンフィギュレーション モードを開始する。

	コマンドまたはアクション	目的
ステップ 4	**time-stamp hpt** 例： `switch(config-if)# time-stamp hpt`	必要なインターフェイスでタイム スタンプをイネーブルにします。
ステップ 5	（任意） **time-stamp hpt utc-offset** 例： `switch(config-if)# time-stamp hpt utc-offset`	Rx タイムスタンプを UTC 形式に変換できるようにします。

ステップ 6	（任意） 設定された HPT の詳細を取得するには、 **show run interface** *type interface-id* または **show time-stamp hpt brief** コマンドのいずれかを活用。
	例：
	`switch# show run interface ethernet 1/5`
	`or`
	`switch# show time-stamp hpt brief`
		HPT の詳細を表示します。

設定例

次の例では、デバイス ID は 100 で、HPT はインターフェイスイーサネット1/47 上に設定されています。

```
switch# show time-stamp hpt brief
Time-stamp HPT Device ID : 100
Timestamp HPT port status
-----------------------
Port State
------- --------------
Eth1/47 hpt enabled
```

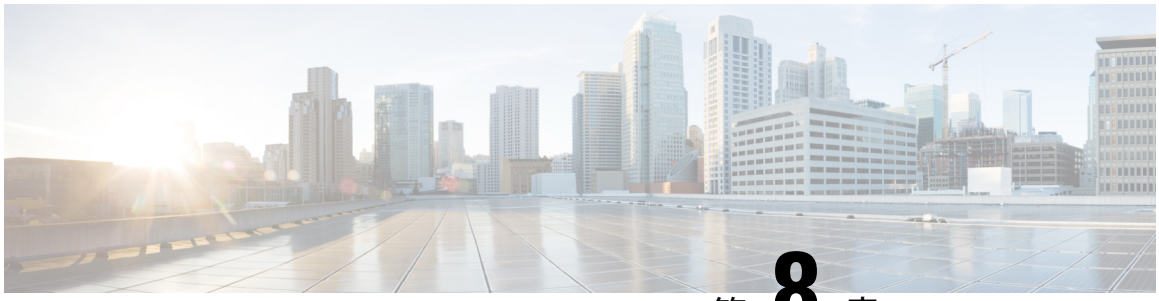
次の例では、HPT UTC タイムスタンプが 有効になっていることがわかります。

```
switch# sh time-stamp hpt brief
Time-stamp HPT Device ID : 0
Time-stamp HPT UTC Timestamp Enabled : enabled
Timestamp HPT port status
-----------------------
Port State
------- --------------
Eth1/4 hpt enabled
```

次の例では、HPT UTC タイムスタンプが 無効になっていることがわかります。

```
switch# sh time-stamp hpt brief
Time-stamp HPT Device ID : 0
Time-stamp HPT UTC Timestamp Enabled : disabled
Timestamp HPT port status
```

```
-----------------------
Port State
------- --------------
Eth1/4 hpt enabled
```



第 8 章

SPAN の設定

この章では、Cisco NX-OS デバイス上のポート間のトラフィックを分析するようにイーサネット スイッチド ポート アナライザ（SPAN）を設定する方法について説明します。

SPAN の概要

SPAN は、外付けアナライザが接続された宛先ポートに SPAN セッション トラフィックを送ることで、送信元ポート間のすべてのトラフィックを分析します。

ローカル デバイス上で、SPAN セッションでモニタする送信元と宛先を定義できます。

SPAN 送信元

トラフィックを監視できる監視元インターフェイスのことを SPAN 送信元と呼びます。送信元では、モニターするトラフィックを指定します。SPAN 送信元には次のものが含まれます。

- イーサネット ポート
- ポートチャネル

1 つの SPAN セッションに、上述の送信元を組み合わせて使用できます。

SPAN 送信元ポートの特性

- 送信元ポートとして設定されたポートは、宛て先ポートとして設定できません。

SPAN 宛先

SPAN 宛先とは、送信元ポートを監視するインターフェイスを指します。宛先ポートは SPAN 送信元からコピーされたトラフィックを受信します。SPAN 宛先には、次のものが含まれます。

- アクセス モードまたはトランク モードのイーサネット ポート
- アクセス モードまたはトランク モードのポート チャネル

SPAN 宛先ポートの特性

- 宛先ポートとして設定されたポートは、送信元ポートとして設定できません。
- 宛先ポートは、一度に 1 つの SPAN セッションだけで設定できます。
- 宛先ポートはスパニングツリーインスタンスに関与しません。SPAN 出力には、ブリッジ プロトコル データ ユニット（BPDU）スパニング ツリー プロトコル hello パケットを含みます。

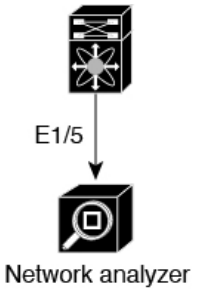
SPAN セッション

SPAN セッションを作成し、送信元と宛先をモニタに指定できます。

サポートされる SPAN セッション数に関する情報については、『*Cisco Nexus 3550-T* シリーズ *NX-OS* 検証済みスケーラビリティ ガイド』を参照してください。

この図では、SPAN 設定を示します。2 つのイーサネット ポート上のパケットが宛て先ポートのイーサネット 1/5 にコピーされます。コピーされるのは、指定した方向のトラフィックだけです。

図 *2: SPAN* の設定



Source Port	Direction	Destination Ports
1/2	Rx	1/5
1/3	Rx	1/5

504564

高可用性

SPAN機能はステートレスおよびステートフル リスタートをサポートします。リブート後に、実行中の構成が適用されます。

注意事項と制約事項

SPAN に関する設定時の注意事項および制約事項は、次のとおりです。

- ACL によって拒否されたトラフィックは、SPAN 宛先ポートに到達する可能性があります。これは、SPAN 複製が ACL の適用（ACL ドロップ トラフィック）の前に入力側で実行されるためです。
- 入力 SPAN のみがサポートされます。
- SPAN セッションの制限については、『*Cisco Nexus 3550-T NX-OS* 検証スケーラビリティ ガイド』を参照してください。
- すべての SPAN のレプリケーションはハードウェアで行われます。スーパーバイザ CPU は関与しません。
- SPAN セッションを設定できるのはローカル デバイス上だけです。
- FCS エラーがあるパケットは、SPAN セッションでミラーリングされません。
- SAPN セッションで 1 つの宛先ポートはのみ設定できます。
- 宛て先ポートは、一度に 1 つの SPAN セッションだけで構成できます。
- ポートを送信元ポートと宛先ポートの両方として設定することはできません。
- スパンド パケットには、ルーテッド パケットに対する VLAN タグの削除、宛先 MAC の書き換えなど、入力の書き換えが反映されます。また、span 出力パケットは常にタグなしです。
- SPAN 送信元ポートと宛先ポートでの単方向リンク検出（UDLD）の同時イネーブル化はサポートされていません。UDLD フレームがこのような SPAN セッションの送信元ポートでキャプチャされることが予想される場合は、SPAN セッションの宛先ポートで UDLD をディセーブルにします。
- SPAN は、レイヤ 2 モードおよびレイヤ 3 モードでサポートされています。
- SPAN は、管理ポートではサポートされません。
- SPAN MTU はサポートされていません。
- VLAN SPAN や VLAN ACL マップはサポートされていません。
- Cisco NX-OS は、送信元インターフェイスがホスト インターフェイス ポート チャネルでないときは、リンク層検出プロトコル（LLDP）またはリンク集約制御プロトコル（LACP）パケットをスパンしません。

SPAN の前提条件

SPAN の前提条件は、次のとおりです。

- 各デバイス上で、まず所定の SPAN 設定をサポートするポートを設定する必要があります。詳細については、『Cisco Nexus 3550-T NX-OS インターフェイス構成ガイド』を参照してください。

SPAN のデフォルト設定

次の表に、SPAN パラメータのデフォルト設定を示します。

パラメータ	デフォルト
SPAN セッション	シャット ステートで作成されます

SPAN セッションの設定

SPAN セッションを設定できるのはローカル デバイス上だけです。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

（注） 双方向性の従来のセッションでは、トラフィックの方向を指定せずにセッションを設定できます。

始める前に

アクセス モードまたはトランク モードで宛先ポートを設定する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

	コマンドまたはアクション	目的

ステップ 2	**interface** *ethernet slot/port*
	例：
	`switch(config)# interface ethernet 1/5`
	`switch(config-if)#`
		選択したスロットおよびポート上でインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	選択したスロットおよびポートまたはポート範囲でスイッチポート パラメータを設定します。
ステップ 4	**switchport monitor** 例： `switch(config-if)# switchport monitor`	SPAN 宛先としてスイッチポート インターフェイスを設定します。
ステップ 5	（任意） ステップ 2 ～ 4 を繰り返して、追加の SPAN 宛先でモニタリングを設定します。	—
ステップ 6	**no monitor session** *session-number* 例： `switch(config)# no monitor session 3`	指定した SPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 7	**monitor session** *session-number*[**rx**] [**shut**]
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	例：
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。オプションの shut キーワードは、選択したセッションに対して shut ステートを指定します。

ステップ 8	**description** *description* 例： `switch(config-monitor)# description my_span_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 9	**source** {**interface** *type* [**rx** 例： `switch(config-monitor)# source interface ethernet 1/3 rx`	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲またはポート チャネルの範囲を入力できます。

	コマンドまたはアクション	目的
		送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。 コピーするトラフィックの方向は、受信（rx）、送信（tx）、または両方（both）を設定できます。 単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。
ステップ 10	（任意） ステップ 9 を繰り返して、すべての SPAN 送信元を設定します。	
ステップ 11	必須: **destination interface** *type slot*/*port* **例**： `switch(config-monitor)# destination interface ethernet 1/5`	コピーする送信元パケットの宛先を設定します。 （注） SPAN 宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。 （注） 宛先ポートでモニタ モードを有効にする必要があります。
ステップ 12	必須: **no shut** **例**： `switch(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 13	（任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] **例**： `switch(config-monitor)# show monitor session 3`	SPAN 設定を表示します。
ステップ 14	（任意） **copy running-config startup-config** **例**： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

SPAN セッションのシャットダウンまたは再開

SPAN セッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断できます。1セッションをシャットダウンしてハードウェア リソースを解放し、別のセッションを有効にできます。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

SPAN セッションを再開（イネーブルに）すると、送信元から宛先へのパケットのコピーを再開できます。すでにイネーブルになっていて、動作状況がダウンの SPAN セッションをイネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブルにする必要があります。

SPAN セッションのシャット ステートおよびイネーブル ステートは、グローバルまたはモニタ コンフィギュレーション モードのどちらのコマンドでも設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **monitor session** {*session-range* | **all**} **shut** 例： `switch(config)# monitor session 3 shut`	指定の SPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。 コマンドの **no** 形式は、指定された SPAN セッションを再開（イネーブルに）します。デフォルトでは、セッションはシャット ステートで作成されます。 （注） モニタ セッションが有効で動作状況がダウンの場合、セッションを有効にするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

ステップ 3	**monitor session** *session-number*
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

	コマンドまたはアクション	目的
ステップ 4	**[no] shut** 例： `switch(config-monitor)# shut`	SPANセッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。 コマンドの **no** 形式は SPAN セッションを有効にします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 5	（任意） **show monitor** 例： `switch(config-monitor)# show monitor`	SPANセッションのステータスを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

SPAN 構成の確認

SPAN 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	SPAN セッションの設定を表示します。

設定例

ここでは、次の設定例を示します。

SPAN セッションのコンフィギュレーション例

SPAN セッションを設定するには、次の手順を実行します。

1. アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
```

```
switch(config)#
```

2. SPAN セッションを設定します。

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 1/9 rx
switch(config-monitor)# source interface port-channel 2 rx
switch(config-monitor)# destination interface ethernet 1/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
```

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。