



Cisco IOS XE Amsterdam 17.3.x (Catalyst 9400 スイッチ) インターフェイスおよびハードウェア コンポーネント コンフィギュレーション ガイド

初版 : 2020 年 7 月 31 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。

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.

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: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

インターフェイス特性の設定 1

インターフェイス特性の設定について 1

インターフェイス タイプ 1

ポートベースの VLAN 1

スイッチ ポート 2

スイッチの USB ポートの使用 7

USB ミニタイプ B コンソール ポート 7

コンソール ポート変更ログ 8

USB タイプ A ポート 8

USB 2.0 ホスト ポート 8

インターフェイスの接続 8

インターフェイス コンフィギュレーション モード 9

イーサネット インターフェイスのデフォルト設定 10

インターフェイス速度およびデュプレックス モード 12

速度とデュプレックス モードの設定時の注意事項 12

IEEE 802.3x フロー制御 13

レイヤ 3 インターフェイス 13

インターフェイス特性の設定方法 15

インターフェイスの設定 15

インターフェイスに関する記述の追加 16

インターフェイス範囲の設定 17

インターフェイス レンジ マクロの設定および使用方法 19

インターフェイス速度およびデュプレックス パラメータの設定 21

IEEE 802.3x フロー制御の設定 22

レイヤ 3 インターフェイスの設定	24
論理レイヤ 3 GRE トンネルインターフェイスの設定	25
SVI 自動ステート除外の設定	26
インターフェイスのシャットダウンおよび再起動	27
USB 無活動タイムアウトの設定	29
インターフェイス特性のモニタ	29
インターフェイス ステータスの監視	30
インターフェイスおよびカウンタのクリアとリセット	31
インターフェイス特性の設定例	31
例：インターフェイスの説明の追加	31
例：インターフェイスの範囲の設定	32
例：インターフェイス範囲のマクロ設定と使用方法	32
例：インターフェイス速度とデュプレックスモードの設定	32
例：レイヤ 3 インターフェイスの設定	33
例：USB 無活動タイムアウトの設定	33
インターフェイス特性の設定のその他の関連資料	34
インターフェイス特性の設定の機能履歴	34

第 2 章

Auto-MDIX の設定 35

Auto-MDIX の前提条件	35
Auto-MDIX の制約事項	35
Auto-MDIX の設定について	36
インターフェイスでの Auto-MDIX	36
Auto-MDIX の設定方法	36
インターフェイスでの Auto-MDIX の設定	36
Auto-MDIX の設定例	37
Auto-MDIX と動作状態	38
Auto-MDIX に関するその他の関連資料	38
Auto-MDIX の機能履歴	38

第 3 章

イーサネット管理ポートの設定 41

イーサネット管理ポートの前提条件	41
イーサネット管理ポートについて	41
デバイスへのイーサネット管理ポートの直接接続	41
イーサネット管理ポートおよびルーティング	42
サポートされるイーサネット管理ポートの機能	43
イーサネット管理ポートの設定方法	43
イーサネット管理ポートの無効化および有効化	43
イーサネット管理インターフェイスでの IP アドレスの設定例	44
イーサネット管理ポートのその他の関連資料	45
イーサネット管理ポートの機能履歴	45

第 4 章

ポート ステータスと接続の確認	47
接続されているモジュールの確認	47
インターフェイスステータスの確認	48
PORT SET ENABLED LED ステータスの表示	49
MAC アドレスの表示	50
Telnet の使用	51
タイムドメイン反射率計を使用したケーブルステータスの確認	52
TDR テストの実行	53
TDR に関する注意事項	53
ログアウトタイマーの変更	54
ユーザセッションのモニタリング	54
ping の使用	55
ping の機能	55
ping コマンドの実行	56
IP トレースルートの使用	56
IP トレースルートの機能	56
IP トレースルートの実行	57
レイヤ 2 トレースルート	58
レイヤ 2 トレースルートの使用上の注意事項	58
レイヤ 2 トレースルートの実行	59

ICMP の設定	60
ICMP プロトコル到達不能メッセージの有効化	60
ICMP マスク応答メッセージの有効化	60
ポートステータスと接続の確認の機能履歴	61

第 5 章

LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定 63

LLDP に関する制約事項	63
LLDP、LLDP-MED、およびワイヤード ロケーション サービスについて	64
LLDP	64
LLDP でサポートされる TLV	64
LLDP-MED	64
LLDP-MED でサポートされる TLV	65
ワイヤード ロケーション サービス	66
デフォルトの LLDP 設定	67
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定方法	68
LLDP の有効化	68
LLDP 特性の設定	69
LLDP-MED TLV の設定	71
Network-Policy TLV の設定	73
ロケーション TLV およびワイヤード ロケーション サービスの設定	75
デバイスでのワイヤード ロケーション サービスの有効化	78
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの設定例	79
Network-Policy TLV の設定：例	79
LLDP、LLDP-MED、ワイヤード ロケーション サービスのモニタリングとメンテナンス	80
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの追加情報	81
LLDP、LLDP-MED、およびワイヤード ロケーション サービスの機能履歴	81

第 6 章

システム MTU の設定 83

MTU について	83
システム MTU 値の適用	83
MTU の設定方法	84

システム MTU の設定	84
プロトコル固有 MTU の設定	84
システム MTU の設定例	85
例：プロトコル固有 MTU の設定	85
例：システム MTU の設定	86
システム MTU に関するその他の関連資料	86
システム MTU の機能履歴	86

第 7 章

ポート単位の MTU の設定	87
ポート単位の MTU の制約事項	87
ポート単位の MTU について	87
ポート単位の MTU の設定	88
例：ポート単位の MTU の設定	89
例：ポート単位の MTU の確認	89
例：ポート単位の MTU の無効化	89
ポート単位の MTU の機能履歴	90

第 8 章

EEE の設定	91
EEE の制約事項	91
EEE について	91
EEE の概要	91
デフォルトの EEE 設定	92
EEE の設定方法	92
EEE の有効化または無効化	92
EEE の監視	93
EEE の設定例	94
EEE に関するその他の関連資料	94
EEE 設定の機能履歴	94

第 9 章

Power over Ethernet の設定	97
PoE の前提条件	97

Power over Ethernet について	98
PoE および PoE+ ポート	98
サポート対象のプロトコルおよび標準規格	98
受電デバイスの検出と初期電力割り当て	100
電力管理モード	101
Cisco Universal Power Over Ethernet	105
PoE と UPOE の設定方法	105
PoE ポートの電力管理モードの設定	106
信号ペアとスペアペアの電源投入の有効化	108
電力ポリシングの設定	109
PoE 電力管理の設定	111
タイプ 3 UPOE モジュールでの 802.3bt モードの有効化	112
非準拠受電デバイスのサポート	113
電力ステータスのモニタ	113
PoE に関するその他の関連資料	117
Power over Ethernet の機能履歴	117

第 10 章

2 イベント分類の設定 121

2 イベント分類の制約事項	121
2 イベント分類について	121
2 イベント分類の設定	122
例 : 2 イベント分類の設定	122
2 イベント分類の機能情報	123

第 11 章

COAP プロキシ サーバの設定 125

COAP プロキシ サーバの制約事項	125
COAP プロキシ サーバについて	126
COAP プロキシ サーバの設定方法	126
COAP プロキシの設定	126
COAP エンドポイントの設定	129
COAP プロキシサーバの設定例	130

例 : COAP プロキシ サーバの設定	130
COAP プロキシ サーバのモニタリング	134
COAP の機能情報	135

第 12 章**外部 USB Bluetooth ドングルの設定 137**

外部 USB Bluetooth ドングルの設定の制約事項	137
外部 USB Bluetooth ドングルについて	137
サポートされている外部 USB Bluetooth ドングル	138
スイッチでの外部 USB Bluetooth ドングルの設定方法	138
スイッチでの Bluetooth 設定の確認	139
外部 Bluetooth ドングルの設定の機能履歴	139

第 13 章**M2 SATA モジュール 141**

Cisco Catalyst 9400 シリーズ スーパーバイザの M2 SATA モジュール	141
M2 SATA のファイル システムとストレージ	141
M2 SATA の制限事項	142
セルフモニタリング、分析、およびレポーティングテクノロジー システム (S.M.A.R.T.) への ルス モニタリング	142
M2 SATA のファイル システムへのアクセス	143
M2 SATA フラッシュ ディスクのフォーマット	143
SATA モジュールでの操作	143
M2 SATA モジュールの機能履歴と情報	145



第 1 章

インターフェイス特性の設定

- [インターフェイス特性の設定について \(1 ページ\)](#)
- [インターフェイス特性の設定方法 \(15 ページ\)](#)
- [インターフェイス特性の設定例 \(31 ページ\)](#)
- [インターフェイス特性の設定のその他の関連資料 \(34 ページ\)](#)
- [インターフェイス特性の設定の機能履歴 \(34 ページ\)](#)

インターフェイス特性の設定について

次の項では、インターフェイス特性について説明します。

インターフェイス タイプ

ここでは、デバイスでサポートされているインターフェイスのさまざまなタイプについて説明します。また、インターフェイスの物理特性に応じた設定手順についても説明します。

ポートベースの VLAN

VLAN は、ユーザの物理的な位置に関係なく、機能、チーム、またはアプリケーションなどで論理的に分割された、スイッチによるネットワークです。ポートで受信したパケットが転送されるのは、その受信ポートと同じ VLAN に属するポートに限られます。異なる VLAN 上のネットワーク デバイスは、VLAN 間でトラフィックをルーティングするレイヤ 3 デバイスがなければ、互いに通信できません。

VLAN に分割することにより、VLAN 内でトラフィック用の堅固なファイアウォールを実現します。また、各 VLAN には固有の MAC アドレス テーブルがあります。VLAN が認識されるのは、ローカル ポートが VLAN に対応するように設定されたとき、VLAN Trunking Protocol (VTP) トランク上のネイバーからその存在を学習したとき、またはユーザが VLAN を作成したときです。

VLAN を設定するには、`vlan vlan-id` グローバル コンフィギュレーション コマンドを使用して、VLAN コンフィギュレーション モードを開始します。標準範囲 VLAN (VLAN ID 1 ~ 1005) の VLAN 設定は、VLAN データベースに保存されます。VTP がバージョン 1 または 2 の場合

に、拡張範囲 VLAN (VLAN ID が 1006 ~ 4094) を設定するには、最初に VTP モードをトランスペアレントに設定する必要があります。トランスペアレントモードで作成された拡張範囲 VLAN は、VLAN データベースには追加されませんが、の実行コンフィギュレーションに保存されます。VTP バージョン 3 では、トランスペアレントモードの他に、クライアントモードまたはサーバモードで拡張範囲 VLAN を作成できます。これらの VLAN は VLAN データベースに格納されます。

switchport インターフェイス コンフィギュレーション コマンドを使用すると、VLAN にポートが追加されます。

- インターフェイスを特定します。
- トランク ポートには、トランク特性を設定し、必要に応じて所属できる VLAN を定義します。
- アクセス ポートには、所属する VLAN を設定して定義します。

スイッチポート

スイッチポートは、物理ポートに対応付けられたレイヤ 2 専用インターフェイスです。スイッチポートは 1 つまたは複数の VLAN に所属します。スイッチポートは、アクセスポートまたはトランクポートにも使用できます。ポートは、アクセスポートまたはトランクポートに設定できます。また、ポート単位で Dynamic Trunking Protocol (DTP) を稼働させ、リンクのもう一端のポートとネゴシエートすることで、スイッチポートモードも設定できます。スイッチポートは物理インターフェイスおよび対応レイヤ 2 プロトコルの管理に使用します。ルーティングやブリッジングは処理しません。

スイッチポートの設定には、**switchport** インターフェイス コンフィギュレーション コマンドを使用します。

アクセスポート

アクセスポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセスポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。アクセスポートがタグ付きパケット（スイッチ間リンク (ISL) またはタグ付き IEEE 802.1Q) を受信した場合、そのパケットはドロップされ、送信元アドレスは学習されません。

サポートされているアクセスポートのタイプは、次のとおりです。

- スタティックアクセスポート。このポートは、手動で VLAN に割り当てます (IEEE 802.1x で使用する場合は RADIUS サーバを使用します)。

また、Cisco IP Phone と接続するアクセスポートを、1 つの VLAN は音声トラフィック用に、もう 1 つの VLAN は Cisco IP Phone に接続しているデバイスからのデータトラフィック用に使用するように設定できます。

トランクポート

トランクポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバとなります。次のトランクポートタイプはサポートされています。

- ISL トランクポートでは、受信パケットはすべて ISL ヘッダーを使用してカプセル化されているものと見なされ、送信パケットはすべて ISL ヘッダーとともに送信されます。ISL トランクポートから受信したネイティブ（タグなし）フレームはドロップされます。
- IEEE 802.1Q トランクポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランクポートは、デフォルトのポート VLAN ID（PVID）に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。NULL VLANID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートのデフォルト PVID と等しい VLANID を持つパケットは、タグなしで送信されます。残りのトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランクポートは、VTP に認識されているすべての VLAN のメンバですが、トランクポートごとに VLAN の許可リストを設定して、VLAN メンバシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランクポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN（VLAN ID 1 ~ 4094）が許可リストに含まれます。トランクポートは、VTP が VLAN を認識し、VLAN が有効な状態にある場合に限り、VLAN のメンバになることができます。VTP が新しい有効になっている VLAN を認識し、その VLAN がトランクポートの許可リストに登録されている場合、トランクポートは自動的にその VLAN のメンバになり、トラフィックはその VLAN のトランクポート間で転送されます。VTP が、VLAN のトランクポートの許可リストに登録されていない、新しい有効な VLAN を認識した場合、ポートはその VLAN のメンバにはならず、その VLAN のトラフィックはそのポート間で転送されません。

トンネルポート

トンネルポートは IEEE 802.1Q トンネリングで使用され、サービスプロバイダーネットワークのカスタマーのトラフィックを、同じ VLAN 番号を使用するその他のカスタマーから分離します。サービスプロバイダーエッジスイッチのトンネルポートからカスタマーのスイッチの IEEE 802.1Q トランクポートに、非対称リンクを設定します。エッジスイッチのトンネルポートに入るパケットには、カスタマーの VLAN ですでに IEEE 802.1Q タグが付いており、カスタマーごとに IEEE 802.1Q タグの別のレイヤ（メトロタグと呼ばれる）でカプセル化され、サービスプロバイダーネットワークで一意的な VLAN ID が含まれます。タグが二重に付いたパケットは、その他のカスタマーのものとは異なる、元のカスタマーの VLAN が維持されてサービスプロバイダーネットワークを通過します。発信インターフェイス、およびトンネルポートでは、メトロタグが削除されてカスタマーのネットワークのオリジナル VLAN 番号が取得されます。

トンネルポートは、トランクポートまたはアクセスポートにすることができず、それぞれのカスタマーに固有の VLAN に属する必要があります。

ルーテッドポート

ルーテッドポートは物理ポートであり、ルータ上にあるポートのように動作しますが、ルータに接続されている必要はありません。ルーテッドポートは、アクセスポートとは異なり、特定の VLAN に対応付けられていません。VLAN サブインターフェイスをサポートしない点を除けば、通常のルータ インターフェイスのように動作します。ルーテッドポートは、レイヤ 3 ルーティングプロトコルで設定できます。ルーテッドポートはレイヤ 3 インターフェイス専用で、DTP や STP などのレイヤ 2 プロトコルはサポートしません。

ルーテッドポートを設定するには、**no switchport** インターフェイス コンフィギュレーション コマンドでインターフェイスをレイヤ 3 モードにします。次に、ポートに IP アドレスを割り当て、ルーティングを有効にして、**ip routing** および **router protocol** グローバル コンフィギュレーション コマンドを使用してルーティングプロトコルの特性を指定します。



- (注) **no switchport** インターフェイス コンフィギュレーション コマンドを実行すると、インターフェイスがいったんシャットダウンされてから再度有効になり、インターフェイスが接続されているデバイスに関するメッセージが表示されることがあります。レイヤ 2 モードのインターフェイスをレイヤ 3 モードにした場合、影響のあるインターフェイスに関連する以前の設定が消失する可能性があります。

ソフトウェアに、設定できるルーテッドポートの個数制限はありません。ただし、ハードウェアには限界があるため、この個数と設定されている他の機能の数との相互関係によって CPU パフォーマンスに影響が及ぶことがあります。

スイッチ仮想インターフェイス

スイッチ仮想インターフェイス (SVI) は、スイッチポートの VLAN を、システムのルーティング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN に対して SVI を設定するのは、VLAN 間でルーティングするため、またはデバイスに IP ホスト接続を提供するためだけです。デフォルトでは、SVI はデフォルト VLAN (VLAN 1) 用に作成され、リモートデバイスの管理を可能にします。追加の SVI は明示的に設定する必要があります。



- (注) インターフェイス VLAN 1 は削除できません。

SVI はシステムにしか IP ホスト接続を行いません。SVI は、VLAN インターフェイスに対して **vlan** インターフェイス コンフィギュレーション コマンドを実行した際に初めて作成されます。VLAN は、ISL または IEEE 802.1Q カプセル化トランク上のデータ フレームに関連付けられた VLAN タグ、あるいはアクセスポート用に設定された VLAN ID に対応します。トラフィックをルーティングするそれぞれの VLAN に対して VLAN インターフェイスを設定し、IP アドレスを割り当ててください。

interface range コマンドを使用して、範囲内の既存の VLAN SVI を設定できます。**interface range** コマンド下で入力したコマンドは、範囲内の既存の VLAN SVI すべてに適用されます。コマンド **interface range create vlan x-y** を入力すると、まだ存在しない指定された範囲内のすべての

vlan を作成できます。VLAN インターフェイスが作成されると、**interface range vlan id**を使用して VLAN インターフェイスを設定できます。

デバイスは合計 1,005 個の VLAN および SVI をサポートしますが、ハードウェアには限界があるため、SVI とルーテッドポートの数および設定されている他の機能の数との相互関係によって、CPU パフォーマンスに影響が及ぶことがあります。

物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

EtherChannel ポートグループ

EtherChannel ポートグループは、複数のスイッチポートを 1 つのスイッチポートとして扱います。このようなポートグループは、デバイス間、またはデバイスとサーバ間で高帯域接続を行う単一論理ポートとして動作します。EtherChannel は、チャンネルのリンク全体でトラフィックの負荷を分散させます。EtherChannel 内のリンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが残りのリンクに切り替えられます。複数のトランクポートを 1 つの論理トランクポートに、複数のアクセスポートを 1 つの論理アクセスポートに、複数のトンネルポートを 1 つの論理トンネルポートに、または複数のルーテッドポートを 1 つの論理ルーテッドポートにグループ化できます。ほとんどのプロトコルは単一のまたは集約スイッチポートで動作し、ポートグループ内の物理ポートを認識しません。例外は、DTP、Cisco Discovery Protocol (CDP)、およびポート集約プロトコル (PAgP) で、物理ポート上でしか動作しません。

EtherChannel を設定するとき、ポートチャンネル論理インターフェイスを作成し、EtherChannel にインターフェイスを割り当てます。レイヤ3 インターフェイスの場合は、**interface port-channel** グローバル コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成します。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを EtherChannel に手動で割り当てます。レイヤ2 インターフェイスの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャンネル論理インターフェイスを動的に作成します。このコマンドは物理および論理ポートをバインドします。

アップリンク ポート

スーパーバイザ モジュールには 1 ～ 10 の名前が付いた 10 個のアップリンク ポートがあります。最初の 8 つのアップリンク ポートである 1 ～ 8 は、Small Form-Factor Pluggable (SFP) トランシーバまたは SFP+ トランシーバを使用し、アップリンク 9 と 10 は Quad Small Form-Factor Pluggable (QSFP) トランシーバを使用します。ポート 1 ～ 8 は、10G と 1G の両方のトランシーバをサポートする 10 ギガビットイーサネットポートです。ポート 9 と 10 は、40 ギガビットイーサネットのアップリンクをサポートする QSFP ポートです。さらに、スーパーバイザ 1XL25 はポート 1 と 5 で 25 ギガビットイーサネットのアップリンクをサポートします。スーパーバイザ 1XL25 のこれらのポート 1 および 5 は SFP28 トランシーバを使用して 25 ギガビットモードをサポートします。

デフォルトでは、10 ギガビットイーサネット ポート 1 ～ 8 が有効になります。

Cisco Catalyst 9400 シリーズ スーパーバイザ 1XL25 モジュールのアップリンクポート

スーパーバイザ XL25 の10個のアップリンクポートは、異なる速度設定をサポートする2つのグループに分類されます。

ポートグループ 1 は、ポート 1～4 で 10G、ポート 1 で 25G、ポート 9 で 40G をサポートします。

ポートグループ 2 は、ポート 5～8 で 10G、ポート 5 で 25G、ポート 10 で 40G をサポートします。

スーパーバイザ 1XL25 のポートのグループ化と設定可能な速度については、次の表を参照してください。

表 1: Cisco Catalyst 9400 シリーズ スーパーバイザ 1XL25 のポートのグループ化

ポート グループ	ポート	速度
ポートグループ 1 (ポート 1、2、3、4、9)	1	10G または 25G
	2～4	10G
	9	40G
ポートグループ 2 (ポート 5、6、7、8、10)	5	10G または 25G
	6～8	10G
	10	40G

速度 10G、25G、および 40G はポートグループごとに相互に排他的です。ポートグループでは任意の 1 つの速度をいつでも有効にできます。

たとえば、ポート 1 で 25G を有効にすると、ポートグループ 1 の他のすべての速度は無効になります。ポート 10 で 40G を設定すると、ポートグループ 2 の残りのポートで 25G と 10G が無効になります。



(注) デュアルスーパーバイザ構成 (ハイアベイラビリティのシナリオ) では、ポートグループ 2 のポートは非アクティブです。ポートグループ 1 のポートだけがアクティブです。

例

次に、10 スロットシャーシに搭載されたスーパーバイザ 1XL25 モジュールのすべてのコマンドの例を示します。

次のコマンドはポート 1 で 25G を有効にします。

```
Switch(config)# interface twe5/0/1
Switch(config-if)# enable
Switch(config-if)#
```


次のコマンドはポート 1 で 25G を無効にします。

```
Switch(config)# interface twe5/0/1
Switch(config-if)# no enable
*Jun  4 11:55:54.316: %TRANSCIVER-6-REMOVED: R0/0: iomd: Transceiver module removed
from TwentyfiveGigabitEthernet5/0/1
```

次のコマンドは、25G がポート 1 にすでに設定されているときにポート 9 に 40G を設定しようとするため、エラーをスローします。

```
Switch(config)# interface fo5/0/9
Switch(config-if)# enable
Twe5/0/1 currently configured with enable command - remove this before enabling on Fo5/0/9
```

イーサネット経由の電力供給

Power over Ethernet (PoE) テクノロジーでは、PoE (802.3af 標準規格)、PoE+ (802.3at) ポートでデバイスの動作の電源を供給できます。

Cisco Universal Power Over Ethernet (Cisco UPOE) は IEEE PoE+ 標準規格を拡張し、ポートあたりの供給電力を 2 倍の 60 W にします。

詳細については、このガイドの「*PoE* の設定」の項を参照してください。

スイッチの USB ポートの使用

には、USB ミニタイプ B コンソールポートと USB タイプ A ポートの 2 つの USB ポートが前面パネルにあります。

USB ミニタイプ B コンソール ポート

デバイスには次のコンソールポートがあります。

- USB ミニタイプ B コンソール接続
- RJ-45 コンソール ポート

コンソール出力は両方のポートに接続されたデバイスに表示されますが、コンソール入力一度に 1 つのポートしかアクティブになりません。デフォルトでは、USB コネクタは RJ-45 コネクタよりも優先されます。



(注) Windows PC には、USB ポートのドライバが必要です。ドライバインストール手順については、ハードウェア インストールガイドを参照してください。

付属の USB タイプ A ツー USB ミニタイプ B ケーブルを使用して PC または他のデバイスをこのデバイスを接続します。接続されたデバイスには、ターミナルエミュレーションアプリケーションが必要です。デバイスが、ホスト機能をサポートする電源の入っているデバイス (PC など) への有効な USB 接続を検出すると、RJ-45 コンソールからの入力がただちに無効になり、USB コンソールからの入力が有効になります。USB 接続が削除されると、RJ-45 コンソール

ルからの入力はまだちに再度有効になります。デバイスの LED はどの接続が使用中であるかを示します。

コンソールポート変更ログ

ソフトウェア起動時に、ログに USB または RJ-45 コンソールのいずれがアクティブであるかが示されます。すべてのデバイスは常に RJ-45 メディアタイプを最初に表示します。

出力例では、デバイス 1 には接続された USB コンソールケーブルがあります。ブートローダが USB コンソールに変わらなかったため、デバイスからの最初のログは RJ-45 コンソールを示しています。少したってから、コンソールが変更され、USB コンソールログが表示されません。

USB ケーブルが取り外されるか、PC が USB 接続を非アクティブ化すると、ハードウェアは自動的に RJ-45 コンソールインターフェイスに変わります。

コンソールタイプが常に RJ-45 であるように設定でき、さらに USB コネクタの無活動タイムアウトを設定できます。

USB タイプ A ポート

USB タイプ A ポートは、外部 USB フラッシュ デバイス（サム ドライブまたは USB キーとも呼ばれる）へのアクセスを提供します。このポートは、容量 128 MB ~ 8 GB の Cisco USB フラッシュ ドライブ、USB 2.0、および USB 3.0 をサポートします（ポート密度 128 MB、256 MB、1 GB、4 GB、8 GB の USB デバイスがサポートされます）。USB 3.0 は、SuperSpeed USB とも呼ばれ、より高速なファイル転送速度を得るために使用されます。標準 Cisco IOS コマンドラインインターフェイス（CLI）コマンドを使用して、フラッシュデバイスの読み取り、書き込み、および、コピー元やコピー先として使用できます。を USB フラッシュドライブから起動するように設定することもできます。

USB 2.0 ホスト ポート

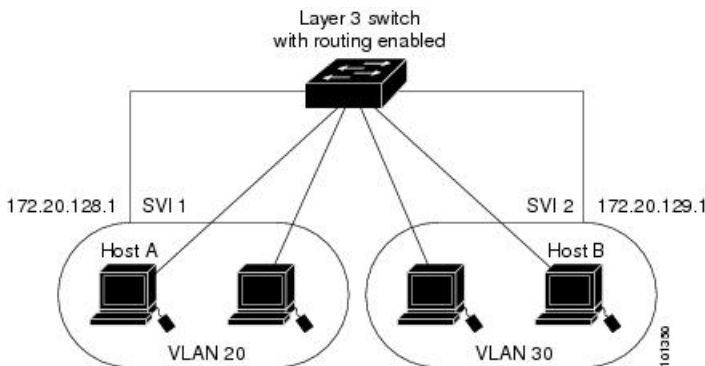
USB 2.0 ホスト ポートは、外部 USB フラッシュ デバイス（サム ドライブまたは USB キーとも呼ばれる）へのアクセスを提供します。このポートは、容量 128 MB ~ 8 GB の Cisco USB フラッシュ ドライブをサポートします（ポート密度 128 MB、256 MB、1 GB、4 GB、8 GB の USB デバイスがサポートされます）。標準 Cisco IOS コマンドラインインターフェイス（CLI）コマンドを使用して、フラッシュデバイスの読み取り、書き込み、および、コピー元やコピー先として使用できます。また、デバイスを USB フラッシュドライブから起動するように設定することもできます。

インターフェイスの接続

単一 VLAN 内のデバイスは、スイッチを通じて直接通信できます。異なる VLAN に属すポート間では、ルーティングデバイスを介さなければデータを交換できません。標準のレイヤ 2 デバイスを使用すると、異なる VLAN のポートは、ルータを通じて情報を交換する必要があります。ルーティングが有効に設定されたデバイスの使用により、IP アドレスを割り当てた SVI

で VLAN 20 および VLAN 30 の両方を設定すると、外部ルータを使用せずに、デバイスを介してホスト A からホスト B にパケットを直接送信できます。

図 1: スイッチと VLAN との接続



Network Advantage ライセンスがデバイスまたはアクティブなデバイスで使用されている場合は、そのデバイスがルーティング方式を使用してインターフェイス間のトラフィックを転送します。Network Essentials ライセンスがデバイスまたはアクティブなデバイスで使用されている場合は、基本ルーティング（静的ルーティングと RIP）だけがサポートされます。可能な場合は、高いパフォーマンスを維持するために、転送はデバイスハードウェアで実行されます。ただし、ハードウェアでルーティングされるのはイーサネット II カプセル化された IPv4 パケットだけです。

ルーティング機能は、すべての SVI およびルーテッドポートで有効にできます。デバイスは IP トラフィックだけをルーティングします。IP ルーティング プロトコルパラメータとアドレス設定が SVI またはルーテッドポートに追加されると、このポートで受信した IP トラフィックはルーティングされます。

インターフェイス コンフィギュレーション モード

デバイスは、次のインターフェイスタイプをサポートします。

- 物理ポート：デバイスポートおよびルーテッドポート
- VLAN：スイッチ仮想インターフェイス
- ポートチャネル：EtherChannel インターフェイス

インターフェイス範囲も設定できます。

物理インターフェイス（ポート）を設定するには、インターフェイスタイプ、モジュール番号、およびデバイスのポート番号を指定し、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。

- タイプ：10/100/1000 Mbps イーサネットポートの場合はギガビットイーサネット (GigabitEthernet または gi)、2.5 Gbps の場合は 2.5 ギガビットイーサネット (TwoGigabitEthernet または tw)、5 Gbps の場合は 5 ギガビットイーサネット (FiveGigabitEthernet または fi)、10 Gbps の場合は 10 ギガビットイーサネット

(TenGigabitEthernet または te)、25 Gbps の場合は 25 ギガビットイーサネット (TwentyFiveGigE or twe)、40 Gbps の場合は Small Form-Factor Pluggable (SFP) モジュールギガビットイーサネットおよび10ギガビットイーサネットインターフェイス、ならびに Quad Small Form-Factor Pluggable (QSFP) モジュール 40 ギガビットイーサネット。



(注) Cisco Catalyst 9300L シリーズ スイッチでは、タイプはギガビットイーサネットか、または 10 ギガビットイーサネットのいずれかです。

- スイッチ番号：特定のデバイスを識別する番号。番号の範囲はデバイスを初めて初期化するとき割り当てられます。
- モジュール番号：デバイス上のモジュールまたはスロット番号；スイッチ（ダウンリンク）ポートは 0 で、アップリンクポートは 1 です。
- SFP アップリンクポートを装着したデバイスの場合、モジュール番号は 1 で、ポート番号が振り直されます。たとえば、デバイスに 10/100/1000 ポートが 24 個ある場合、SFP モジュールポートは、GigabitEthernet1/1/1 ~ GigabitEthernet1/1/4、または TenGigabitEthernet1/1/1 ~ TenGigabitEthernet1/1/4 になります。

デバイス上のインターフェイスの位置を物理的に確認することで、物理インターフェイスを識別できます。show 特権 EXEC コマンドを使用して、スイッチ上の特定のインターフェイスまたはすべてのインターフェイスに関する情報を表示することもできます。以降、この章では、主に物理インターフェイスの設定手順について説明します。

イーサネット インターフェイスのデフォルト設定

インターフェイスがレイヤ3モードの場合に、レイヤ2パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ2モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度有効になり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ3モードのインターフェイスをレイヤ2モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。

次の表は、レイヤ2インターフェイスにのみ適用される一部の機能を含む、イーサネットインターフェイスのデフォルト設定を示しています。

表 2: レイヤ2イーサネットインターフェイスのデフォルト設定

機能	デフォルト設定
動作モード	レイヤ2 または スイッチングモード (switchport コマンド)。
VLAN 許容範囲	VLAN 1 ~ 4094

機能	デフォルト設定
デフォルト VLAN (アクセスポート用)	VLAN 1 (レイヤ 2 インターフェイスだけ)。
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1 (レイヤ 2 インターフェイスだけ)。
VLAN トランキング	Switchport mode dynamic auto (DTP をサポート) (レイヤ 2 インターフェイスだけ)。
ポート イネーブル ステート	すべてのポートが有効。
ポート記述	未定義。
速度	自動ネゴシエーション
デュプレックス モード	自動ネゴシエーション
フロー制御	フロー制御は receive: off に設定されます。送信パケットでは常にオフです。
EtherChannel (PAgP)	すべてのイーサネット ポートで無効。
ポートブロッキング (不明マルチキャストおよび不明ユニキャストトラフィック)	無効 (ブロッキングされない) (レイヤ 2 インターフェイスだけ)。
ブロードキャスト、マルチキャスト、およびユニキャストストーム制御	無効。
保護ポート	無効 (レイヤ 2 インターフェイスだけ)。
ポートセキュリティ	無効 (レイヤ 2 インターフェイスだけ)。
PortFast	無効。
Auto-MDIX	有効。 (注) IEEE 802.3af に完全には準拠していない Cisco IP 電話やアクセスポイントなど、準規格の受電デバイスについては、その受電デバイスをクロスケーブルでスイッチに接続する場合、スイッチでサポートされないことがあります。これは、スイッチポート上で Automatic Medium-Dependent Interface Crossover (Auto-MDIX) が有効かどうかは関係ありません。
Power over Ethernet (PoE)	有効 (auto)。

インターフェイス速度およびデュプレックスモード

スイッチのイーサネットのインターフェイスは、10 Mbps、100 Mbps、1000 Mbps、2.5 Gbps、5 Gbps、10 Gbps のいずれかの速度で、かつ全二重か半二重のどちらかのモードで動作します。全二重モードの場合、2つのステーションが同時にトラフィックを送受信できます。通常、10 Mbps ポートは半二重モードで動作します。つまり、ステーションはトラフィックの受信または送信のいずれかを交互に行います。

スイッチモジュールには、ギガビットイーサネット（10/100/1000 Mbps）ポートが搭載されています。また、スイッチには最大 2.5 Gbps（100/1000/2500 Mbps）、5 Gbps（100/1000/2500/5000 Mbps）、10 Gbps（100/1000/2500/5000/10000 Mbps）の速度をサポートするマルチギガビットイーサネットポート、最大 1 Gbps の速度をサポートする SFP モジュール、最大 10 Gbps の速度をサポートする SFP+ モジュール、最大 25 Gbps の速度をサポートする SFP28 モジュールが搭載されています。

速度とデュプレックスモードの設定時の注意事項

インターフェイス速度とデュプレックスモードを設定する際には、次のガイドラインに注意してください。

- イーサネット（10/100/1000 Mb/s）ポートとマルチギガビットイーサネットポート（2.5 Gb/s、5Gb/s、10Gb/s）は、すべての速度オプションとデュプレックスオプション（自動、半二重、全二重）をサポートします。ただし、1000 Mbps 以上で動作しているギガビットイーサネットポートは半二重モードをサポートしません。
- 回線の両側で自動ネゴシエーションがサポートされる場合は、デフォルト設定の **auto** ネゴシエーションの使用を強くお勧めします。
- 一方のインターフェイスが自動ネゴシエーションをサポートし、もう一方がサポートしない場合は、両方のインターフェイス上でデュプレックスと速度を設定します。サポートする側で **auto** 設定を使用しないでください。
- STP が有効な場合にポートを再設定すると、デバイスがループの有無を調べるために最大で 30 秒かかる可能性があります。STP の再設定が行われている間、ポート LED はオレンジに点灯します。ベストプラクティスとして、速度とデュプレックスのオプションをリンク上で自動に設定するか、リンク終端の両側で固定に設定することを推奨します。リンクの片側が自動に設定され、反対側が固定に設定されている場合、リンクは起動することも、起動しないこともあります。これは予期される動作です。



注意 インターフェイス速度とデュプレックスモードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再び有効になる場合があります。

IEEE 802.3x フロー制御

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィックレートを制御できます。あるポートで輻輳が生じ、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズフレームを受信すると、送信側デバイスはデータパケットの送信を中止するので、輻輳時のデータパケット損失が防止されます。



(注) スイッチポートは、ポーズフレームを受信できますが、送信はできません。

flowcontrol インターフェイス コンフィギュレーション コマンドを使用してインターフェイスのポーズフレームを **receive** する機能を **on**、**off**、または **desired** に設定できます。デフォルトの状態は **on** です。

desired に設定した場合、インターフェイスはフロー制御パケットの送信を必要とする接続デバイスか、または必要ではないもののフロー制御パケットを送信できる接続デバイスで動作できます。

デバイスのフロー制御設定には、次のルールが適用されます。

- **receive on** (または **desired**) : ポートはポーズフレームを送信できませんが、ポーズフレームを送信する必要がある、または送信できる接続デバイスと組み合わせて使用できます。ポーズフレームの受信は可能です。
- **receive off** : フロー制御はどちらの方向にも動作しません。輻輳が生じても、リンクの相手側に通知はなく、どちら側の装置も休止フレームの送受信を行いません。



(注) コマンドの設定と、その結果生じるローカルおよびリモートポートでのフロー制御解決の詳細については、このリリースのコマンドリファレンスに記載された **flowcontrol** インターフェイス コンフィギュレーション コマンドを参照してください。

レイヤ3 インターフェイス

デバイスは、次のレイヤ3 インターフェイスをサポートします。

- **SVI** : トラフィックをルーティングする **VLAN** に対応する **SVI** を設定する必要があります。SVI は、**interface vlan** グローバル コンフィギュレーション コマンドのあとに **VLAN ID** を入力して作成します。SVI を削除するには、**no interface vlan** グローバル コンフィギュレーション コマンドを使用します。インターフェイス **VLAN 1** は削除できません。



(注) 物理ポートと関連付けられていない場合、SVIを作成してもアクティブにはなりません。

SVIを設定するとき、SVIラインステータスステータスを判断する際に含めないようにするため、SVI自動ステート除外をSVIのポートに設定することもできます。

- ルーテッドポート：ルーテッドポートは、**no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ3モードになるように設定された物理ポートです。ルーテッドポートはVLANサブインターフェイスをサポートします。

VLANサブインターフェイス：802.1Q VLANサブインターフェイスは、ルーテッド物理インターフェイス上のVLAN IDに関連付けられた仮想Cisco IOSインターフェイスです。親インターフェイスは物理ポートです。サブインターフェイスはレイヤ3物理インターフェイス上のみ作成できます。サブインターフェイスは、IPアドレッシング、転送ポリシー、Quality of Service (QoS) ポリシー、セキュリティポリシーなどのさまざまな機能に関連付けることができます。親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスにIPアドレスやダイナミックルーティングプロトコルなど固有のレイヤ3パラメータを割り当てることができます。各サブインターフェイスのIPアドレスは、親インターフェイスの他のサブインターフェイスのサブネットとは異なります。

- レイヤ3 EtherChannel ポート：EtherChannel インターフェイスは、ルーテッドポートで構成されます。

レイヤ3 デバイスは、各ルーテッドポートおよびSVIに割り当てられたIPアドレスを持つことができます。

デバイスまたはデバイススタックで設定可能なSVIとルーテッドポートの数に対して定義された制限はありません。ただし、ハードウェアには限界があるため、SVIおよびルーテッドポートの個数と、設定されている他の機能の個数の組み合わせによっては、CPU利用率が影響を受けることがあります。デバイスが最大限のハードウェアリソースを使用している場合にルーテッドポートまたはSVIを作成しようとすると、次のような結果になります。

- 新たなルーテッドポートを作成しようとすると、デバイスはインターフェイスをルーテッドポートに変換するための十分なリソースがないことを示すメッセージを表示し、インターフェイスはスイッチポートのままとなります。
- 拡張範囲のVLANを作成しようとすると、エラーメッセージが生成され、拡張範囲のVLANは拒否されます。
- VLAN Trunking Protocol (VTP) が新たなVLANをデバイスに通知すると、使用可能な十分なハードウェアリソースがないことを示すメッセージを送り、そのVLANをシャットダウンします。**show vlan EXEC** コマンドの出力に、中断状態のVLANが示されます。
- デバイスが、ハードウェアのサポート可能な数を超えるVLANとルーテッドポートが設定されたコンフィギュレーションを使って起動を試みると、VLANは作成されますが、

ルーテッドポートはシャットダウンされ、デバイスはハードウェアリソースが不十分であるという理由を示すメッセージを送信します。



(注) すべてのレイヤ3 インターフェイスには、トラフィックをルーティングするための IP アドレスが必要です。次の手順は、レイヤ3 インターフェイスとしてインターフェイスを設定する方法およびインターフェイスに IP アドレスを割り当てる方法を示します。

物理ポートがレイヤ2 モードである（デフォルト）場合は、**no switchport** インターフェイス コンフィギュレーション コマンドを実行してインターフェイスをレイヤ3 モードにする必要があります。**no switchport** コマンドを実行すると、インターフェイスが無効化されてから再度有効になります。これにより、インターフェイスが接続しているデバイスに関するメッセージが生成されることがあります。さらに、レイヤ2 モードのインターフェイスをレイヤ3 モードにすると、影響を受けたインターフェイスに関連する前の設定情報は失われ、インターフェイスはデフォルト設定に戻る可能性があります。

インターフェイス特性の設定方法

次の項では、インターフェイス特性を設定する手順を構成するさまざまなタスクについて説明します。

インターフェイスの設定

次の一般的な手順は、すべてのインターフェイス設定プロセスに当てはまります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface 例：	インターフェイスタイプ、およびコネクタの数を識別します。

	コマンドまたはアクション	目的
	Device(config)# interface gigabitethernet1/0/1 Device(config-if)#	(注) インターフェイスタイプとインターフェイス番号の間にスペースを入れる必要はありません。たとえば、前の行では、 gigabitethernet 1/0/1 、 gigabitethernet1/0/1 、 gi 1/0/1 、または gi1/0/1 のいずれかを指定できます。
ステップ 4	各 interface コマンドの後ろに、インターフェイスに必要なインターフェイス コンフィギュレーション コマンドを続けて入力します。	インターフェイス上で実行するプロトコルとアプリケーションを定義します。別のインターフェイスコマンドまたは end を入力して特権EXECモードに戻ると、コマンドが収集されてインターフェイスに適用されます。
ステップ 5	interface range または interface range macro	(任意) インターフェイスの範囲を設定します。 (注) ある範囲内で設定したインターフェイスは、同じタイプである必要があります。また、同じ機能オプションを指定して設定しなければなりません。
ステップ 6	show interfaces	スイッチ上のまたはスイッチに対して設定されたすべてのインターフェイスのリストを表示します。デバイスがサポートする各インターフェイスまたは指定したインターフェイスのレポートが出力されます。

インターフェイスに関する記述の追加

インターフェイスの記述を追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/2	記述を追加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	description string 例： Device (config-if) # description Connects to Marketing	インターフェイスに記述を追加します。
ステップ 5	end 例： Device(config-if) # end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id description	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイス範囲の設定

同じ設定パラメータを持つ複数のインターフェイスを設定するには、**interface range** グローバル コンフィギュレーション コマンドを使用します。インターフェイス レンジ コンフィギュレーション モードを開始すると、このモードを終了するまで、入力されたすべてのコマンドパラメータはその範囲内のすべてのインターフェイスに対するものと見なされます。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>プロンプトが表示されたらパスワードを入力します。</p>
ステップ 2	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p>interface range {<i>port-range</i> macro <i>macro_name</i>}</p> <p>例 :</p> <pre>Device(config)# interface range macro</pre>	<p>設定するインターフェイス範囲 (VLAN または物理ポート) 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。</p> <ul style="list-style-type: none"> • interface range コマンドを使用すると、最大5つのポート範囲または定義済みマクロを1つ設定できます。 • macro 変数は、「インターフェイスレンジマクロの設定および使用方法」の項で説明されています。 • カンマで区切った <i>port-range</i> では、各エントリに対応するインターフェイスタイプを入力し、カンマの前後にスペースを含めます。 • ハイフンで区切った <i>port-range</i> では、インターフェイスタイプの再入力が必要ですが、ハイフンの前後にスペースを入力する必要があります。 <p>(注) この時点で、通常のコフィギュレーション コマンドを使用して、範囲内のすべてのインターフェイスにコンフィギュレーション パラメータを適用します。各コマンドは、入力されたとおりに実行されます。</p>

	コマンドまたはアクション	目的
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show interfaces [interface-id] 例： Device# show interfaces	指定した範囲内のインターフェイスの設定を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

インターフェイスレンジマクロの設定および使用方法

インターフェイスレンジマクロを作成すると、設定するインターフェイスの範囲を自動的に選択できます。**interface range macro** グローバルコンフィギュレーションコマンド文字列で **macro** キーワードを使用する前に、**define interface-range** グローバルコンフィギュレーションコマンドを使用してマクロを定義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	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	define interface-range macro_name interface-range 例：	インターフェイス範囲マクロを定義して、NVRAM に保存します。 <ul style="list-style-type: none"> • <i>macro_name</i> は、最大 32 文字の文字列です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> マクロには、カンマで区切ったインターフェイスを5つまで指定できます。 それぞれの <i>interface-range</i> は、同じポートタイプで構成されていなければなりません。 <p>(注) interface range macro グローバルコンフィギュレーションコマンド文字列で macro キーワードを使用する前に、define interface-range グローバルコンフィギュレーションコマンドを使用してマクロを定義する必要があります。</p>
ステップ 4	interface range macro macro_name 例： Device(config)# interface range macro enet_list	<p><i>macro_name</i> の名前でインターフェイス範囲マクロに保存された値を使用することによって、設定するインターフェイスの範囲を選択します。</p> <p>ここで、通常のコンフィギュレーションコマンドを使用して、定義したマクロ内のすべてのインターフェイスに設定を適用できます。</p>
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config include define 例： Device# show running-config include define	定義済みのインターフェイス範囲マクロの設定を表示します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

インターフェイス速度およびデュプレックスパラメータの設定

インターフェイスの速度とデュプレックスパラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/3	設定する物理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	speed {10 100 1000 auto [10 100 1000 10000] nonegotiate} 例： Device(config-if)# speed 10	インターフェイスに対する適切な速度パラメータを入力します。 <ul style="list-style-type: none"> • 10、100、1000、または 10000 を入力してインターフェイスに特定の速度を設定します。 • インターフェイスに接続されたデバイスと自動ネゴシエーションが行えるようにするには、auto を入力します。速度を指定しする際に auto キーワードも設定する場合、ポートは指定の速度でのみ自動ネゴシエーションを行います。 • nonegotiate キーワードを使用できるのは、SFP モジュールポートに対してだけです。SFP モジュールポートは 1000 Mbps だけで動作しますが、自動ネゴシエーションをサポートしていないデバイスに接続されて

	コマンドまたはアクション	目的
		いる場合は、ネゴシエートしないように設定できます。
ステップ 5	duplex {auto full half} 例 : <pre>Device(config-if)# duplex half</pre>	インターフェイスのデュプレックスパラメータを入力します。 半二重モードを有効にします (10 Mb/s または 100 Mb/s のみで動作するインターフェイスの場合)。半二重は、1000 Mb/s の速度に設定されたマルチギガビットイーサネットポートではサポートされていません。 デュプレックス設定を行うことができるのは、速度が auto に設定されている場合です。
ステップ 6	end 例 : <pre>Device(config-if)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	show interfaces interface-id 例 : <pre>Device# show interfaces gigabitethernet1/0/3</pre>	インターフェイス速度およびデュプレックスモードの設定を表示します。
ステップ 8	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

IEEE 802.3x フロー制御の設定

IEEE 802.3x フロー制御を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/1	設定する物理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	flowcontrol {receive} {on off desired} 例： Device(config-if)# flowcontrol receive on	ポートのフロー制御モードを設定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id 例： Device# show interfaces gigabitethernet1/0/1	インターフェイス フロー制御の設定を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

レイヤ3インターフェイスの設定

レイヤ3インターフェイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ3	interface { gigabitethernet interface-id } { vlan vlan-id } { port-channel port-channel-number } 例： Device(config)# interface gigabitethernet1/0/2	レイヤ3インターフェイスとして設定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	no switchport 例： Device(config-if)# no switchport	(物理ポートの場合のみ) レイヤ3モードを開始します。
ステップ5	ip address ip_address subnet_mask 例： Device(config-if)# ip address 192.20.135.21 255.255.255.0	IP アドレスおよび IP サブネットを設定します。
ステップ6	no shutdown 例： Device(config-if)# no shutdown	インターフェイスを有効にします。
ステップ7	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-if) # end	
ステップ 8	show interfaces [<i>interface-id</i>]	設定を確認します。
ステップ 9	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

論理レイヤ 3 GRE トンネルインターフェイスの設定

始める前に

総称ルーティング カプセル化 (GRE) は、仮想ポイントツーポイント リンク内でネットワーク層プロトコルをカプセル化するために使用されるトンネリングプロトコルです。GRE トンネルは、カプセル化のみを提供し、暗号化は提供しません。



- (注)
- GRE トンネルは、Cisco Catalyst 9000 スイッチのハードウェアでサポートされています。GRE でトンネル オプションを設定しない場合、パケットはハードウェアでスイッチングされます。GRE をトンネルオプション (キーやチェックサムなど) で設定すると、パケットはソフトウェアでスイッチングされます。最大 1000 個の GRE トンネルがサポートされます。
 - GRE トンネルではアクセスコントロールリスト (ACL) や Quality of Service (QoS) などのその他の機能はサポートされません。
 - GRE トンネルでは **tunnel path-mtu-discovery** コマンドはサポートされていません。フラグメンテーションを回避するには、**ip mtu 256** コマンドを使用して GRE トンネルの両端の最大伝送ユニット (MTU) を最小値に設定します。

GRE トンネルを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface tunnel number 例： Device(config)# interface tunnel 2	インターフェイスでトンネリングを有効にします。
ステップ 4	ip address ip_address subnet_mask 例： Device(config)# ip address 100.1.1.1 255.255.255.0	IP アドレスおよび IP サブネットを設定します。
ステップ 5	tunnel source {ip_address type_number} 例： Device(config)# tunnel source 10.10.10.1	トンネル送信元を設定します。
ステップ 6	tunnel destination {host_name ip_address} 例： Device(config)# tunnel destination 10.10.10.2	トンネル宛先を設定します。
ステップ 7	tunnel mode gre ip 例： Device(config)# tunnel mode gre ip	トンネル モードを設定します。
ステップ 8	end 例： Device(config)# end	設定モードを終了します。

SVI 自動ステート除外の設定

SVI 自動ステートを除外するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/2	レイヤ2インターフェイス（物理ポートまたはポート チャネル）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	switchport autostate exclude 例： Device(config-if)# switchport autostate exclude	SVI ライン ステート（アップまたはダウン）のステータスを定義する際、アクセスまたはトランク ポートを除外します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show running config interface interface-id	（任意）実行コンフィギュレーションを表示します。 設定を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスのシャットダウンおよび再起動

インターフェイスをシャットダウンすると、指定されたインターフェイスのすべての機能が無効になり、使用不可能であることがすべてのモニタ コマンドの出力に表示されます。この情報は、すべてのダイナミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。ルーティング アップデートには、インターフェイス情報は含まれません。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>プロンプトが表示されたらパスワードを入力します。</p>
ステップ 2	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
ステップ 3	<p>interface { vlan <i>vlan-id</i> } { gigabitethernet <i>interface-id</i> } { port-channel <i>port-channel-number</i> }</p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet1/0/2</pre>	<p>設定するインターフェイスを選択します。</p>
ステップ 4	<p>shutdown</p> <p>例 :</p> <pre>Device(config-if)# shutdown</pre>	<p>インターフェイスをシャットダウンします。</p>
ステップ 5	<p>no shutdown</p> <p>例 :</p> <pre>Device(config-if)# no shutdown</pre>	<p>インターフェイスを再起動します。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config-if)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 7	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>

USB 無活動タイムアウトの設定

無活動タイムアウトを設定している場合、USB コンソールポートがアクティブ化されているものの、指定された時間内にポートで入力アクティビティがないときに、RJ-45 コンソールポートが再度アクティブになります。タイムアウトのために USB コンソールポートは非アクティブ化された場合、USB ポートを切断し、再接続すると、動作を回復できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	line console 0 例： Device(config)# line console 0	コンソールを設定し、ライン コンフィギュレーションモードを開始します。
ステップ 4	usb-inactivity-timeout switch <i>switch_number timeout-minutes</i> 例： Device(config-line)# usb-inactivity-timeout switch 1 30	コンソールポートの無活動タイムアウトを指定します。指定できる範囲は 1 ~ 240 分です。デフォルトでは、タイムアウトが設定されていません。
ステップ 5	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイス特性のモニタ

ここでは、インターフェイス特性のモニタリングについて説明します。

インターフェイス ステータスの監視

特権 EXEC プロンプトにコマンドを入力することによって、ソフトウェアおよびハードウェアのバージョン、コンフィギュレーション、インターフェイスに関する統計情報などのインターフェイス情報を表示できます。

表 3: インターフェイス用の *show* コマンド

コマンド	目的
show interfaces interface-id status [err-disabled]	インターフェイスのステータスまたは error-disabled ステータスにあるインターフェイスのリストを表示します。
show interfaces [interface-id] switchport	スイッチング（非ルーティング）ポートの管理上および動作上のステータスを表示します。このコマンドを使用すると、ポートがルーティングまたはスイッチングのどちらのモードにあるかが判別できます。
show interfaces [interface-id] description	1つのインターフェイスまたはすべてのインターフェイスに関する記述とインターフェイスのステータスを表示します。
show ip interface [interface-id]	IP ルーティング用に設定されたすべてのインターフェイスまたは特定のインターフェイスについて、使用できるかどうかを表示します。
show interface [interface-id] stats	インターフェイスのパスごとに入出力パケットを表示します。
show interfaces interface-id	（任意）インターフェイスの速度およびデュプレックスを表示します。
show interfaces transceiver dom-supported-list	（任意）接続 SFP モジュールの Digital Optical Monitoring (DOM) ステータスを表示します。
show interfaces transceiver properties	（任意）インターフェイスの温度、電圧、電流量を表示します。
show interfaces [interface-id] [{transceiver properties detail}] module number]	SFP モジュールに関する物理および動作ステータスを表示します。
show running-config interface [interface-id]	インターフェイスに対応する RAM 上の実行コンフィギュレーションを表示します。
show version	ハードウェア設定、ソフトウェアバージョン、コンフィギュレーション ファイルの名前と送信元、およびブートイメージを表示します。

コマンド	目的
show controllers ethernet-controller interface-id phy	インターフェイスの Auto-MDIX 動作ステータスを表示します。

インターフェイスおよびカウンタのクリアとリセット

表 4: インターフェイスの *clear* コマンド

コマンド	目的
clear counters [interface-id]	インターフェイス カウンタをクリアします。
clear interface interface-id	インターフェイスのハードウェアロジックをリセットします。
clear line [number console 0 vty number]	非同期シリアル回線に関するハードウェアロジックをリセットします。



(注) **clear counters** 特権 EXEC コマンドは、簡易ネットワーク管理プロトコル (SNMP) を使用して取得されたカウンタをクリアしません。**show interface** 特権 EXEC コマンドで表示されるカウンタのみをクリアします。

インターフェイス特性の設定例

この項では、インターフェイス特性の設定例を示します。

例：インターフェイスの説明の追加

次に、インターフェイスの説明を追加する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# description Connects to Marketing
Device(config-if)# end
Device# show interfaces gigabitethernet1/0/2 description
Interface Status          Protocol Description
Gi1/0/2    admin down        down      Connects to Marketing
```

例：インターフェイスの範囲の設定



- (注) インターフェイスレンジモードで複数のコンフィギュレーションコマンドを入力した場合、各コマンドは入力した時点で実行されます。インターフェイスレンジモードを終了した後で、コマンドがバッチ処理されるわけではありません。コマンドの実行中にインターフェイスレンジコンフィギュレーションモードを終了すると、一部のコマンドが範囲内のすべてのインターフェイスに対して実行されない場合もあります。コマンドプロンプトが再表示されるのを待ってから、インターフェイス範囲コンフィギュレーションモードを終了してください。

例：インターフェイス範囲のマクロ設定と使用方法

次に、インターフェイス範囲のマクロ *enet_list* に対するインターフェイスレンジコンフィギュレーションモードを開始する例を示します。

```
Device# configure terminal
Device(config)# interface range macro enet_list
Device(config-if-range)#
```

次に、インターフェイス範囲のマクロ *enet_list* を削除し、処理を確認する例を示します。

```
Device# configure terminal
Device(config)# no define interface-range enet_list
Device(config)# end
Device# show run | include define
Device#
```

例：インターフェイス速度とデュプレックスモードの設定

次に、10/100/1000 Mbps ポートでインターフェイス速度を 10 Mbps、デュプレックスモードを全二重にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# speed 10
Device(config-if)# duplex full
```

次に、10/100/1000 Mbps ポートでインターフェイス速度を 100 Mbps に設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# speed 100
```

例：レイヤ3インターフェイスの設定

次に、レイヤ3インターフェイスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 192.20.135.21 255.255.255.0
Device(config-if)# no shutdown
```

例：USB 無活動タイムアウトの設定

次に、無活動タイムアウトを30分に設定する例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# usb-inactivity-timeout switch 1 30
```

次に、設定を無効にする例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no usb-inactivity-timeout switch 1
```

設定された分数の間に USB コンソールポートで（入力）アクティビティがなかった場合、無活動タイムアウト設定が RJ-45 ポートに適用され、ログにこの発生が示されます。

```
*Mar 1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

この時点で、USB コンソールポートを再度アクティブ化する唯一の方法は、ケーブルを取り外し、再接続することです。

スイッチの USB ケーブルが取り外され、再度接続された場合、次のようなログが表示されま

```
*Mar 1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

インターフェイス特性の設定のその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9400 Series Switches)</i> の「 <i>Interface and Hardware Commands</i> 」の項を参照してください。

インターフェイス特性の設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	インターフェイス特性	インターフェイス特性には、インターフェイスタイプ、接続、設定モード、速度、およびデバイスの物理インターフェイスの設定に関するその他の側面が含まれます。
Cisco IOS XE Everest 16.6.4	IEEE 802.3x フロー制御	flowcontrol インターフェイス コンフィギュレーション コマンドのデフォルト値はこのシリーズのすべてのモデルで on に変更されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 2 章

Auto-MDIX の設定

- [Auto-MDIX の前提条件](#) (35 ページ)
- [Auto-MDIX の制約事項](#) (35 ページ)
- [Auto-MDIX の設定について](#) (36 ページ)
- [Auto-MDIX の設定方法](#) (36 ページ)
- [Auto-MDIX の設定例](#) (37 ページ)
- [Auto-MDIX と動作状態](#) (38 ページ)
- [Auto-MDIX に関するその他の関連資料](#) (38 ページ)
- [Auto-MDIX の機能履歴](#) (38 ページ)

Auto-MDIX の前提条件

インターフェイスがレイヤ3モードの場合に、レイヤ2パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ2モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度有効になり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ3モードのインターフェイスをレイヤ2モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があります。インターフェイスはデフォルト設定に戻ります。

デフォルトで Automatic Medium-Dependent Interface Crossover (Auto-MDIX) 機能が有効に設定されます。

Auto-MDIX の制約事項

受電デバイスがクロスケーブルでデバイスに接続されている場合、そのデバイスはIEEE 802.3af に完全には準拠しておらず、Cisco IP Phone やアクセスポイントなどの準規格の受電デバイスをサポートしていない場合があります。これは、スイッチポート上で Automatic Medium-Dependent Interface Crossover (Auto-MDIX) が有効かどうかは関係ありません。

Auto-MDIX の設定について

インターフェイスでの Auto-MDIX

自動メディア依存型インターフェイスクロスオーバー (MDIX) が有効になっているインターフェイスでは、必要なケーブル接続タイプ (ストレートまたはクロス) が自動的に検出され、接続が適切に設定されます。Auto-MDIX 機能を使用せずにデバイスを接続する場合、サーバ、ワークステーション、ルータなどのデバイスの接続にはストレートケーブルを使用し、他のデバイスやリピーターの接続にはクロスケーブルを使用する必要があります。Auto-MDIX が有効になっている場合、他のデバイスとの接続にはどちらのケーブルでも使用でき、ケーブルが正しくない場合はインターフェイスが自動的に修正を行います。ケーブル接続の詳細については、ハードウェア インストレーション ガイドを参照してください。



(注) Auto-MDIX はデフォルトで有効になっています。

次の表に、Auto-MDIX の設定およびケーブル接続ごとのリンク ステータスを示します。

表 5: リンク状態と Auto-MDIX の設定

ローカル側の Auto-MDIX	リモート側の Auto-MDIX	ケーブル接続が正しい場合	ケーブル接続が正しくない場合
オン	オン	リンク アップ	リンク アップ
オン	オフ	リンク アップ	リンク アップ
オフ	オン	リンク アップ	リンク アップ
オフ	オフ	リンク アップ	リンク ダウン

Auto-MDIX の設定方法

インターフェイスでの Auto-MDIX の設定

デフォルトで Auto MDIX はオンです。ポートで Auto MDIX を無効にするには、インターフェイス コンフィギュレーション モードで **no mdix auto** コマンドを使用します。デフォルトに戻すには、インターフェイス コンフィギュレーション モードで **mdix auto** コマンドを使用します。次に、Auto MDIX を有効にする手順を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/1	設定する物理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	mdix auto 例： Device(config-if)# mdix auto	Auto MDIX 機能を有効にします。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Auto-MDIX の設定例

次の例では、ポートの Auto MDIX を有効にする方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# mdix auto
Device(config-if)# end
```

Auto-MDIX と動作状態

表 6: Auto-MDIX と動作状態

インターフェイスでの Auto-MDIX 設定と動作状態	説明
Auto-MDIX on (operational: on)	Auto-MDIX は有効になっており、フル機能しています。
Auto-MDIX on (operational: off)	このインターフェイスでは Auto-MDIX は有効になっていますが、機能していません。Auto-MDIX 機能を正常に動作させるには、インターフェイス速度を自動ネゴシエーションに設定する必要があります。
Auto-MDIX off	no mdix auto コマンドにより、Auto-MDIX が無効になっています。

Auto-MDIX に関するその他の関連資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9400 Series Switches)</i>
電源装置に関する情報。	<i>Cisco Catalyst 9400 シリーズ スイッチ ハードウェア 設置ガイド</i>

Auto-MDIX の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	インターフェイスでの Auto-MDIX	自動メディア依存型インターフェイスクロスオーバー (Auto-MDIX) 対応のインターフェイスは必要なケーブル接続タイプ (ストレートまたはクロス) を自動的に検出し、接続を適切に設定します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 3 章

イーサネット管理ポートの設定

- [イーサネット管理ポートの前提条件 \(41 ページ\)](#)
- [イーサネット管理ポートについて \(41 ページ\)](#)
- [イーサネット管理ポートの設定方法 \(43 ページ\)](#)
- [イーサネット管理インターフェイスでの IP アドレスの設定例 \(44 ページ\)](#)
- [イーサネット管理ポートのその他の関連資料 \(45 ページ\)](#)
- [イーサネット管理ポートの機能履歴 \(45 ページ\)](#)

イーサネット管理ポートの前提条件

PC をイーサネット管理ポートに接続するときに、最初に IP アドレスを割り当てる必要があります。

イーサネット管理ポートについて

Gi0/0 または *GigabitEthernet0/0* ポートとも呼ばれるイーサネット管理ポートは、PC を接続する VRF (VPN ルーティング/転送) インターフェイスです。ネットワークの管理にデバイスコンソールポートの代わりとしてイーサネット管理ポートを使用できます。

スイッチを管理するときに、PC を Catalyst 9400 シリーズスイッチ上のイーサネット管理ポートに接続します。

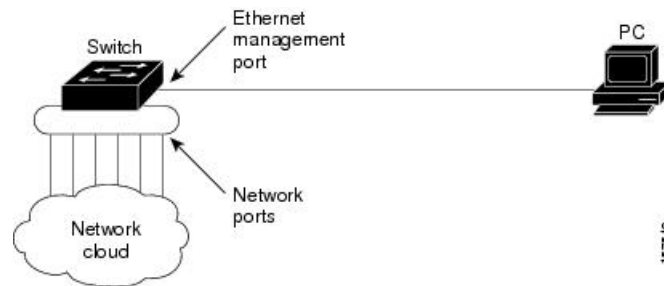


(注) PC をイーサネット管理ポートに接続するときに、IP アドレスを割り当てる必要があります。

デバイスへのイーサネット管理ポートの直接接続

図 2: PC へのデバイスの接続

次の図に、デバイスまたはスタンドアロンデバイス用に PC をイーサネット管理ポートに接続する方法を示します。

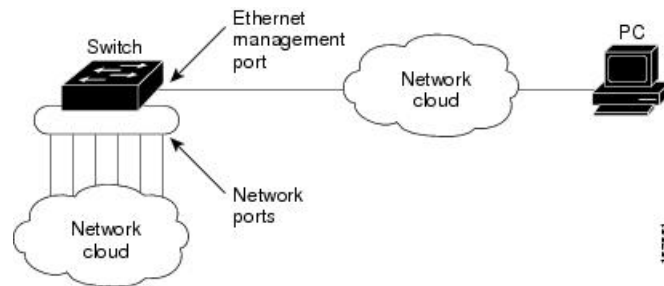


イーサネット管理ポートおよびルーティング

デフォルトでは、イーサネット管理ポートは有効です。デバイスは、イーサネット管理ポートからネットワークポートへ、およびその逆に、パケットをルーティングできません。イーサネット管理ポートはルーティングをサポートしていませんが、ポート上でルーティングプロトコルを有効にすることが必要となる場合もあります。

図 3: ルーティングプロトコルを有効にしたネットワーク例

PC とデバイスが複数ホップ分離されていて、パケットが PC に到達するには複数のレイヤ 3 デバイスを経由する必要がある場合、イーサネット管理ポート上のルーティングプロトコルを有効にします。せ



上記の図では、イーサネット管理ポートとネットワークポートが同じルーティングプロセスに関連付けられている場合、ルートは次のように伝達されます。

- イーサネット管理ポートからのルートは、ネットワークポートを通してネットワークに伝播されます。
- ネットワークポートからのルートは、イーサネット管理ポートを通してネットワークに伝播されます。

イーサネット管理ポートとネットワークポートの間ではルーティングはサポートされていないため、これらのポート間のトラフィックの送受信はできません。このような状況になると、これらのポート間にデータパケットループが発生し、スイッチおよびネットワークの動作が中断されます。このループを防止するには、イーサネット管理ポートとネットワークポートの間のルートを回避するためにルートフィルタを設定してください。

サポートされるイーサネット管理ポートの機能

イーサネット管理ポートは次の機能をサポートします。

- Express Setup (デバイススタック内のみ)
- Network Assistant
- パスワード付きの Telnet
- TFTP
- セキュア シェル (SSH)
- Dynamic Host Configuration Protocol (DHCP) ベースの自動設定
- SNMP (ENTITY-MIB および IF-MIB だけ)
- IP ping
- インターフェイス機能
 - 速度：10 Mb/秒、100 Mb/秒、および自動ネゴシエーション
 - デュプレックス モード：全二重、半二重、自動ネゴシエーション
 - ループバック検出
- Cisco Discovery Protocol (CDP)
- DHCP リレー エージェント
- IPv4 および IPv6 アクセス コントロール リスト (ACL)



注意

イーサネット管理ポートの機能を有効にする前に機能がサポートされていることを確認してください。イーサネット管理ポートでサポートされていない機能を設定しようとすると、機能は正しく動作せず、デバイスに障害が発生するおそれがあります。

イーサネット管理ポートの設定方法

イーサネット管理ポートの無効化および有効化

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 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
	Device# configure terminal	
ステップ 2	interface gigabitethernet0/0 例： Device(config)# interface gigabitethernet0/0	CLIでイーサネット管理ポートを指定します。
ステップ 3	shutdown 例： Device(config-if)# shutdown	イーサネット管理ポートを無効にします。
ステップ 4	no shutdown 例： Device(config-if)# no shutdown	イーサネット管理ポートを有効にします。
ステップ 5	exit 例： Device(config-if)# exit	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ます。
ステップ 6	show interfaces gigabitethernet0/0 例： Device# show interfaces gigabitethernet0/0	リンクステータスを表示します。 PCへのリンクステータスを調べるには、イーサネット管理ポートのLEDをモニタします。リンクがアクティブな場合、LEDはグリーン（オン）であり、リンクが停止中の場合は、LEDはオフです。POSTエラーがある場合は、LEDはオレンジです。

次のタスク

イーサネット管理ポートを使用したデバイスの管理または設定に進みます。「ネットワーク管理」の項を参照してください。

イーサネット管理インターフェイスでの IP アドレスの設定例

次に、GigabitEthernet0/0 管理インターフェイスで IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet0/0
Device(config-if)# vrf forwarding Mgmt-vrf
Device(config-if)# ip address 192.168.247.10 255.255.0.0
Device(config-if)# end
```

```
Device# show running-config interface Gi0/0
Building configuration...

Current configuration : 118 bytes
!
interface GigabitEthernet0/0
vrf forwarding Mgmt-vrf
ip address 192.168.247.10 255.255.0.0
negotiation auto
end
```

次に、TenGigabitEthernet0/1 管理インターフェイスで IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# interface TenGigabitEthernet0/1
Device(config-if)# vrf forwarding Mgmt-vrf
Device(config-if)# ip address 192.168.247.20 255.255.0.0
Device(config-if)# negotiation auto
Device(config-if)# end
```

```
Device#show running-config interface Te0/1
Building configuration...

Current configuration : 118 bytes
!
interface TenGigabitEthernet0/1
vrf forwarding Mgmt-vrf
ip address 192.168.247.20 255.255.0.0
negotiation auto
end
```

イーサネット管理ポートのその他の関連資料

関連資料

関連項目	マニュアルタイトル
ブートローダ設定	このガイドの「システム管理」の項を参照してください。
ブートローダコマンド	『 <i>Command Reference (Catalyst 9200 Series Switches)</i> 』の「 <i>System Management Commands</i> 」の項を参照

イーサネット管理ポートの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	イーサネット管理ポート	イーサネット管理ポートは、PC を接続できる VRF インターフェイスです。ネットワークの管理にデバイスコンソールポートの代わりとしてイーサネット管理ポートを使用できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 4 章

ポートステータスと接続の確認

- 接続されているモジュールの確認 (47 ページ)
- インターフェイスステータスの確認 (48 ページ)
- PORT SET ENABLED LED ステータスの表示 (49 ページ)
- MAC アドレスの表示 (50 ページ)
- Telnet の使用 (51 ページ)
- タイムドメイン反射率計を使用したケーブルステータスの確認 (52 ページ)
- ログアウトタイマーの変更 (54 ページ)
- ユーザセッションのモニタリング (54 ページ)
- ping の使用 (55 ページ)
- IP トレースルートの使用 (56 ページ)
- レイヤ 2 トレースルート (58 ページ)
- ICMP の設定 (60 ページ)
- ポートステータスと接続の確認の機能履歴 (61 ページ)

接続されているモジュールの確認

Catalyst 9400 シリーズスイッチはモジュラシステムです。取り付けられているモジュールと各モジュールの MAC アドレスの範囲とバージョン番号を表示するには `show module` コマンドを入力します。特定のモジュール番号を指定し、そのモジュールの詳細情報を表示するには、`mod_num` 引数を使用します。

次に、スイッチ上のすべてのモジュールのステータスを確認する例を示します。

```
Device# show module
Chassis Type: C9410R
```

Mod	Ports	Card Type	Model	Serial No.
1	48	48-Port 10/100/1000 (RJ-45)	C9400-LC-48T	JAE2107023L
2	24	24-Port 10 Gigabit Ethernet (SFP+)	C9400-LC-24XS	JAE210706JV
3	48	48-Port UPOE 10/100/1000 (RJ-45)	C9400-LC-48U	JAE2107050E
4	24	24-Port 10 Gigabit Ethernet (SFP+)	C9400-LC-24XS	JAE210706KD
5	10	Supervisor 1 Module	C9400-SUP-1	JAE21150399
6	10	Supervisor 1 Module	C9400-SUP-1	JAE21150399
7	24	24-Port 10 Gigabit Ethernet (SFP+)	C9400-LC-24XS	JAE210706KE

```

8 48 48-Port 10/100/1000 (RJ-45)          C9400-LC-48T  JAE211703QZ
9 48 48-Port 10/100/1000 (RJ-45)          C9400-LC-48T  JAE2107023V
10 48 48-Port UPOE 10/100/1000 (RJ-45)    C9400-LC-48U  JAE210704ZZ

```

```

Mod MAC addresses          Hw  Fw          Sw          Status
-----+-----+-----+-----+-----
1  E4AA.5D54.6DA4 to E4AA.5D54.6DD3 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
2  E4AA.5D54.8280 to E4AA.5D54.8297 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
3  E4AA.5D54.75C0 to E4AA.5D54.75EF 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
4  E4AA.5D54.8550 to E4AA.5D54.8567 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
5  CC16.7EAA.722C to CC16.7EAA.7235 0.6  16.6.1r [FC BLD_V166_THROTTLE_LA ok
6  CC16.7EAA.7236 to CC16.7EAA.723F 0.6  16.6.1r [FC BLD_V166_THROTTLE_LA ok
7  E4AA.5D54.82F8 to E4AA.5D54.830F 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
8  E4AA.5D54.C9FC to E4AA.5D54.CA2B 0.6  16.6.1r [FC BLD_V166_THROTTLE_LA ok
9  E4AA.5D54.603C to E4AA.5D54.606B 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok
10 E4AA.5D54.7200 to E4AA.5D54.722F 0.5  16.6.1r [FC BLD_V166_THROTTLE_LA ok

```

```

Mod Redundancy Role      Operating Redundancy Mode Configured Redundancy Mode
-----+-----+-----+-----+-----
5  Active              sso                          sso
6  Standby             sso                          sso

```

```
Switch#
```

インターフェイスステータスの確認

スイッチポートのサマリーまたは詳細情報を表示する場合は、**show interface status** コマンドを使用します。スイッチ上のすべてのポートに関するサマリー情報を確認するには、**show interface status** コマンドを引数なしで入力します。特定のモジュール番号を指定すると、そのモジュールのポート情報だけが表示されます。特定のポートの詳細情報を表示するには、モジュール番号とポート番号を入力します。

特定のポートにコンフィギュレーションコマンドを適用するには、適切な論理モジュールを指定する必要があります。

次に、トランシーバを含む Catalyst 9400 シリーズ スイッチ上のすべてのインターフェイスのステータスを表示する例を示します。

```
Switch# show interface status
```

```

Port      Name          Status      Vlan      Duplex  Speed Type
-----+-----+-----+-----+-----+-----
Gi1/0/1   connected    1          a-full   a-1000 10/100/1000BaseTX
Gi1/0/2   connected    1          a-full   a-1000 10/100/1000BaseTX
Gi1/0/3   connected    1          a-full   a-1000 10/100/1000BaseTX
Gi1/0/4   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/5   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/6   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/7   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/8   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/9   notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/10  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/11  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/12  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/13  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/14  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/15  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/16  notconnect   1          auto     auto   10/100/1000BaseTX
Gi1/0/17  notconnect   1          auto     auto   10/100/1000BaseTX

```

```

Gi1/0/18                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/19                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/20                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/21                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/22                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/23                notconnect  1          auto   auto  10/100/1000BaseTX
Gi1/0/24                notconnect  1          auto   auto  10/100/1000BaseTX

```

次に、`error-disabled` ステートのインターフェイスのステータスを表示する例を示します。

```

Device# show interfaces status err-disabled
Port Name Status Reason
Fa9/4 err-disabled link-flap
informational error message when the timer expires on a cause
-----
5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on
Fa9/4
Switch#

```

PORT SET ENABLED LED ステータスの表示

スーパーバイザ前面プレートには 4 つの PORT SET ENABLED LED があります。

- ポート番号 1 ～ 4 用に 1 つ (G1)
- ポート番号 5 ～ 8 用に 1 つ (G2)
- ポート番号 9 用に 1 つ (G3)
- ポート番号 10 用に 1 つ (G4)

ポート 1 ～ 8 は 10 ギガビットポートで、ポート 9 と 10 は 40 ギガビットポートです。

スタンドアロンスーパーバイザ

スタンドアロンスーパーバイザでは、前述のように 1 つのスーパーバイザがアクティブになっており、ポートは 10 個あります。グループ G1 とグループ G3 は相互に排他的です。つまり、ポート 1 ～ 4 がアクティブになっているか、またはポート 9 がアクティブになっています。同様に、グループ G2 とグループ G4 は相互に排他的です。つまり、ポート 5 ～ 8 がアクティブになっているか、またはポート 10 がアクティブになっています。グループのステータスは、40 ギガビットインターフェイスの設定によって決まります。

スタンドアロンスーパーバイザ モードでの PORT SET ENABLED LED の表示

次の設定例では、40 ギガビットポート番号 10 を有効にします。

```

interface FortyGigabitEthernet4/0/9
end

interface FortyGigabitEthernet4/0/10
  enable
end

```

次に `show hardware led` コマンドの出力を示します。

```

SUPERVISOR: ACTIVE
PORT STATUS: (10) Te4/0/1:BLACK Te4/0/2:BLACK Te4/0/3:BLACK Te4/0/4:BLACK Te4/0/5:BLACK

```

```
Te4/0/6:BLACK Te4/0/7:BLACK Te4/0/8:BLACK Fo4/0/9:BLACK Fo4/0/10:BLACK
```

```
BEACON: BLACK
```

```
GROUP LED: UPLINK-G1:GREEN UPLINK-G2:BLACK UPLINK-G3:BLACK UPLINK-G4:GREEN
```

この例では、グループ 4 がアクティブ (GREEN) であるため、グループ 2 は非アクティブ (BLACK) であることがわかります。グループ 3 は有効になっておらず非アクティブ (BLACK) であるため、グループ 1 がアクティブ (GREEN) です。

ハイアビリティモードまたはデュアルスーパーバイザモード

デュアルスーパーバイザモードでは、1〜4 (G1) の 10 ギガビットポートと 9 (G3) の 40 ギガビットポートが両方のスーパーバイザで動作できます。デフォルトでは、5〜8 (G2) のその他の 10 ギガビットポートと 10 (G4) の 40 ギガビットポートが無効になっています。相互に排他的なグループ G1 と G3 のうち、いずれかのグループが 40 ギガビットポート番号 9 の設定に基づいてアクティブになります。

デュアルスーパーバイザモードでの PORT SET ENABLED LED の表示

```
Switch#show run int fo4/0/9
Building configuration...
```

```
Current configuration : 52 bytes
!
interface FortyGigabitEthernet4/0/9
  enable
end
```

```
Switch#
```

```
SUPERVISOR: STANDBY
PORT STATUS: (10) Te3/0/1:BLACK Te3/0/2:BLACK Te3/0/3:BLACK Te3/0/4:BLACK Te3/0/5:BLACK
Te3/0/6:BLACK Te3/0/7:BLACK Te3/0/8:BLACK Fo3/0/9:BLACK Fo3/0/10:BLACK
```

```
BEACON: BLACK
```

```
GROUP LED: UPLINK-G1:GREEN UPLINK-G2:BLACK UPLINK-G3:BLACK UPLINK-G4:BLACK
```

```
SUPERVISOR: ACTIVE
PORT STATUS: (10) Te4/0/1:BLACK Te4/0/2:BLACK Te4/0/3:BLACK Te4/0/4:BLACK Te4/0/5:BLACK
Te4/0/6:BLACK Te4/0/7:BLACK Te4/0/8:BLACK Fo4/0/9:BLACK Fo4/0/10:BLACK
```

```
BEACON: BLACK
```

```
GROUP LED: UPLINK-G1:BLACK UPLINK-G2:BLACK UPLINK-G3:GREEN UPLINK-G4:BLACK
```

MAC アドレスの表示

show module コマンドを使用してモジュールの MAC アドレスの範囲を表示する以外に、**show mac-address-table address** コマンドと **show mac-address-table interface** コマンドを使用して、特定の MAC アドレスまたはスイッチの特定のインターフェイスの MAC アドレス テーブル情報を表示できます。

次に、すべての MAC アドレスの MAC アドレス テーブル情報を表示する例を示します。

```
Switch# show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0100.0ccc.cccc   STATIC    CPU
All     0100.0ccc.cccd   STATIC    CPU
All     0180.c200.0000   STATIC    CPU
All     0180.c200.0001   STATIC    CPU
All     0180.c200.0002   STATIC    CPU
All     0180.c200.0003   STATIC    CPU
All     0180.c200.0004   STATIC    CPU
All     0180.c200.0005   STATIC    CPU
All     0180.c200.0006   STATIC    CPU
All     0180.c200.0007   STATIC    CPU
All     0180.c200.0008   STATIC    CPU
All     0180.c200.0009   STATIC    CPU
All     0180.c200.000a   STATIC    CPU
All     0180.c200.000b   STATIC    CPU
All     0180.c200.000c   STATIC    CPU
All     0180.c200.000d   STATIC    CPU
All     0180.c200.000e   STATIC    CPU
All     0180.c200.000f   STATIC    CPU
All     0180.c200.0010   STATIC    CPU
All     0180.c200.0021   STATIC    CPU
All     ffff.ffff.ffff   STATIC    CPU
      1     188b.45eb.cc01   DYNAMIC   Gi1/0/1
Total Mac Addresses for this criterion: 22
Switch#
```

次に、特定のインターフェイスの MAC アドレス テーブル情報を表示する例を示します。

```
Switch# show mac address-table interface Gi1/0/1
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
      1     188b.45eb.cc01   DYNAMIC   Gi1/0/1
Total Mac Addresses for this criterion: 1
Switch#
```

Telnet の使用

スイッチのコマンドライン インターフェイス (CLI) には、Telnet を使用してアクセスできます。また、Telnet ではネットワーク内の他のデバイスにアクセスすることができます。最大 8 つの Telnet セッションを同時に実行できます。

スイッチとの Telnet セッションを設定する前に、まずスイッチの IP アドレス (場合によりデフォルト ゲートウェイも) を設定する必要があります。IP アドレスとデフォルト ゲートウェイの設定については、「スイッチの初回設定」に関する項を参照してください。



- (注) ホスト名を使用してホストとの Telnet 接続を確立するには、ドメインネームシステム (DNS) を設定して有効にします。

スイッチからネットワーク上の別のデバイスへの Telnet 接続を確立するには、次のコマンドを入力します。

```
Switch# telnet host [port]
```

次に、スイッチからリモート ホスト labsparc への Telnet 接続を確立する例を示します。

```
Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.
UNIX(r) System V Release 4.0 (labsparc)
login:
```

タイムドメイン反射率計を使用したケーブルステータスの確認

タイムドメイン反射率計 (TDR) 機能を使用すると、障害発生時にケーブルが OPEN か SHORT かを判断できます。

TDR により、Catalyst 9400 シリーズスイッチの場合は 48 ポート 10/100/1000 BASE-T モジュール上の銅線ケーブルのステータスを確認できます。TDR は、信号をケーブルに送信し、反射して戻ってきた信号を読み取ることによりケーブルの障害を検出します。すべてまたは一部の信号は、ケーブルの障害によって反射されて戻される可能性があります。



- (注) カテゴリ 5 ケーブルには 4 つのペアがあります。各ペアは、次のステート (オープン (接続されていない)、損傷、ショート、または終端) のいずれかであると想定できます。TDR テストは、4 つのすべての状態を検知し、最初の 3 つを「障害」状態と表示し、4 番目を「終了」と表示します。CLI 出力が表示されても、ケーブル長は状態が「不良」である場合にのみ表示されます。

TDR 機能は次のモジュールでサポートされています。

- C9400-LC-48U
- C9400-LC-48T
- C9400-LC-48P

TDR は、ワイヤに沿って信号を送信することでケーブル障害を検出します。反射信号に応じて、ケーブル障害が発生した場所を大まかに判断できます。TDR 信号がどのように反射してくるかによって、TDR の結果が決まります。Catalyst 9400 シリーズスイッチでは、2 種類のケー

ブル障害タイプ（OPEN または SHORT）のみが検出されます。たとえば、ケーブルが正しく終端されている場合のステータスは「Terminated」と表示されます。

TDR テストの実行

TDR テストを開始するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	test cable-diagnostics tdr {interface { interface-number}}	TDR テストを開始します。
ステップ 2	show cable-diagnostics tdr { interface interface-number}	TDR テストのカウンタ情報を表示します。

TDR に関する注意事項

TDR を使用する場合は、次の注意事項が適用されます。

- TDR テストの実行中はポート設定を変更しないでください。
- TDR テストを実行中のポートと Auto-MDIX が有効になっているポートを接続した場合、この TDR 結果は無効となる可能性があります。この場合、TDR テストを開始する前にデバイス上のポートを管理上のダウンにする必要があります。
- TDR テストを実行中のポートとデバイス上のポートなど 100BASE-T ポートを接続する場合、未使用のペア（4～5 と 7～8）はリモートエンドで終端処理されないため、障害として報告されます。
- ケーブルの特性から、正確な結果を入手するには TDR テストを複数回行う必要があります。
- 結果が不正確となる可能性があるため、（近端または遠端のケーブルを取り外すなど）ポートステータスを変更しないでください。
- TDR は、テストケーブルをリモートポートから外している場合に正しく動作します。それ以外の場合は、正確な結果が得られない可能性があります。
- TDR は 4 本の導線を対象とします。ケーブルの状態によっては、1 組の導線ペアのステータスが OPEN または SHORT と表示され、他のすべてのペアのステータスが faulty と表示される場合があります。この動作は、1 組の導線ペアが OPEN または SHORT であればケーブル不良と宣言する必要があるため、許容範囲です。
- TDR の目的は、不良ケーブルを特定することではなく、ケーブルがどのように不適切な機能をしているかを確認することです。
- TDR でケーブル不良が検出された場合でも、オフラインケーブル診断ツールを使用して、より詳しく問題を診断する必要があります。

- TDR の結果は、TDR 実装の分解能が異なる Catalyst 9400 モジュールで実行すると異なる場合があります。このような場合は、オフラインのケーブル診断ツールを参照してください。

ログアウトタイマーの変更

ログアウトタイマーは、ユーザが指定された時間よりも長くアイドル状態にあるとき、自動的にスイッチから切断します。ログアウトタイマーを設定するには、次のコマンドを入力します。

```
Switch(config-line)# exec-timeout minutes seconds
```

このコマンドでログアウトタイマーの値を変更します（タイムアウト値に0を指定すると、アイドル状態のセッションが自動的に切断されるのを防ぎます）。

デフォルト値に戻すには、**no** キーワードを使用します。

ログアウトを 10 分 10 秒に設定するには、次のコマンドを入力します。

```
Switch(config)# line console 0
Switch(config-line)# exec-timeout 10 10
```

コンソールセッションにログアウトタイマーを設定しない場合は、次のコマンドを入力します。

```
Switch(config)# line console 0
Switch(config-line)# exec-timeout 0 0
```

ユーザセッションのモニタリング

show users コマンドを使用すると、スイッチ上で現在アクティブなユーザセッションを表示できます。このコマンドは、スイッチでアクティブなすべてのコンソールポートと Telnet セッションのリストを出力します。

スイッチのアクティブなユーザセッションを表示するには、次のコマンドを入力します。

```
Switch# show users [all]
```

スイッチのアクティブなユーザセッションを切断するには、次のコマンドを入力します。

```
Switch# disconnect { console | ip_address }
```

例

次に、コンソールと Telnet セッションでローカル認証が有効になっていりう場合の、**show users** コマンドの出力例を示します（アスタリスク [*] が現在のセッションを示します）。

```
Switch# show users
Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address
```



```
Switch# show users all
  Line      User  Host(s)  Idle           Location
*  0  con  0           idle    00:00:00
  1  vty  0           00:00:00
  2  vty  1           00:00:00
  3  vty  2           00:00:00
  4  vty  3           00:00:00
  5  vty  4           00:00:00
Interface User Mode  Idle           Peer Address
Switch#
```

次に、アクティブなコンソールポートのセッションとアクティブな Telnet セッションを切断する例を示します。

```
Switch> disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Switch# show users
Session User Location
-----
telnet jake jake-mac.bigcorp.com
* telnet suzy suzy-pc.bigcorp.com
Switch#
```

ping の使用

ここでは、IP ping を使用する手順について説明します。

ping の機能

ping コマンドでは、リモートホストとの接続を確認することができます。異なる IP サブネットワークのホストに ping を実行する場合、ネットワークへのスタティックルートを定義するか、サブネットワーク間をルーティングするルータを設定する必要があります。

ping コマンドは、ユーザモードおよび特権 EXEC モードから設定できます。ping は次のいずれかの応答を返します。

- 正常な応答：正常な応答 (hostname is alive) は、ネットワークトラフィックに応じて 1 ～ 10 秒で戻ります。
- 宛先の応答なし：ホストが応答しない場合、No Answer メッセージが返されます。
- ホスト不明：ホストが存在していない場合、Unknown Host メッセージが返されます。
- 宛先到達不能：デフォルトゲートウェイが指定されたネットワークに到達できない場合、Destination Unreachable メッセージが返されます。
- ネットワークまたはホスト到達不能：ホストまたはネットワークにルートテーブルが存在しない場合、Network または Host Unreachable メッセージが返されます。

実行中の ping を停止するには、Ctrl+C を押します。

ping コマンドの実行

スイッチからネットワーク上の別のデバイスに ping を実行するには、ユーザモードおよび特権 EXEC モードで次のコマンドを入力します。

```
Switch# ping host
```

リモートホストとの接続を確認します。

次に、ユーザモードからリモートホストに ping を実行する例を示します。

```
Switch# ping labsparc
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

```
Switch# ping 72.16.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 72.16.10.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Switch#
```

次に、特権 EXEC モードで ping コマンドを使用してパケット数、パケットサイズ、タイムアウト時間を指定する例を示します。

```
Switch# ping
Protocol [ip]: ip
Target IP address: 1.1.1.1
Repeat count [5]: 10
Datagram size [100]: 100
Timeout in seconds [2]: 10
Extended commands [n]: n
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1.1.1.1, timeout is 10 seconds:
!!!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms
Switch#
```

IP トレースルートの使用

IP トレースルートの機能

IP traceroute では、パケットがネットワークで通過するパスをホップバイホップベースで特定することができます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ3）デバイスが表示されます。

レイヤ2スイッチは、trace コマンドの送信元または宛先として参加できますが、trace コマンド出力ではホップとして表示されません。

trace コマンドは IP ヘッダーの Time To Live (TTL) フィールドを使用して、ルータとサーバで特定のリターンメッセージが生成されるようにします。traceroute の実行は、ユーザデータグラムプロトコル (UDP) データグラムを、TTL フィールドが 1 に設定されている宛先ホスト

へ送信することから始まります。ルータが 1 または 0 の TTL 値を検出すると、ルータはデータグラムをドロップしてインターネット制御メッセージプロトコル (ICMP) Time-Exceeded メッセージを送信側に返します。tracert は、ICMP Time-Exceeded メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判断します。

ネクスト ホップを識別するために、tracert は TTL 値が 2 の UDP パケットを送信します。1 番目のルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番目のルータは TTL の値 1 を確認し、データグラムをドロップして、送信元に Time-Exceeded メッセージを返します。このプロセスは、データグラムが宛先ホストに到達できるだけの値まで TTL が増加するか、最大 TTL に到達するまで続けられます。

データグラムが宛先に到達したことを判断するために、トレースルートはデータグラムの UDP 宛先ポートを宛先ホストが使用する可能性が低い大きな値に設定します。ホストが未確認のポート番号を指定したデータグラムを受け取ると、送信元に ICMP Port Unreachable エラーメッセージを送信します。Port Unreachable エラーメッセージは、宛先に到達していることを tracert に通知します。

IP トレースルートの実行

パケットがネットワークで通過するパスを追跡するには、EXEC モードまたは特権 EXEC モードで次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>tracert [protocol] [destination]</code>	IP トレースルートを実行して、ネットワークでパケットが通過するパスを追跡します。

例

次に、tracert コマンドを使用して、パケットがネットワークを通過して宛先に到達するまでのルートを表示する例を示します。

```
Switch# tracert ip ABA.NYC.mil
Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0  DEBRIS.CISCO.COM (192.180.1.6)  1000 msec  8 msec  4 msec
 1  BARRNET-GW.CISCO.COM (192.180.16.2)  8 msec  8 msec  8 msec
 2  EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225)  8 msec  4 msec  4 msec
 3  BB2.SU.BARRNET.NET (192.200.254.6)  8 msec  8 msec  8 msec
 4  SU.ARC.BARRNET.NET (192.200.3.8)  12 msec  12 msec  8 msec
 5  MOFFETT-FLD-MB.in.MIL (192.52.195.1)  216 msec  120 msec  132 msec
 6  ABA.NYC.mil (26.0.0.73)  412 msec  628 msec  664 msec
Switch#
```

レイヤ2トレースルート

レイヤ2トレースルート機能により、パケットが通過する送信元デバイスから宛先デバイスまでの物理パスを識別できます。レイヤ2トレースルートは、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内のスイッチが保持する MAC アドレス テーブルを使用してパスを判別します。スイッチがレイヤ2トレースルートをサポートしないデバイスをパスで検出すると、スイッチはレイヤ2トレースキューを送信し続けてタイムアウトにしまいます。

スイッチが送信元デバイスのホストから宛先デバイスのホストへのパスを追跡する場合、スイッチは送信元デバイスから宛先デバイスへのパスのみを識別します。パケットが通過する送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

レイヤ2トレースルートの使用上の注意事項

レイヤ2トレースルートの使用上の注意事項を次に示します。

- Cisco Discovery Protocol は、ネットワーク上のすべてのデバイスで有効になっている必要があります。レイヤ2 `traceroute` が適切に動作するために、CDP を無効にしないでください。
物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。
- 物理パス内のすべてのスイッチは IP 接続が可能でなければなりません。スイッチが別のスイッチから到達可能である場合、特権 EXEC モードで `ping` コマンドを使用して接続をテストできます。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスへの物理パスにないスイッチでは、特権 EXEC モードで `traceroute mac` コマンドまたは `traceroute mac ip` コマンドを入力できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- `traceroute mac` コマンドの出力結果としてレイヤ2パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ2パスは識別されず、エラーメッセージが表示されます。
- マルチキャストの送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラーメッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラーメッセージが表示されます。

- 指定した送信元および宛先の IP アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力にレイヤ2パスが表示されます。IP アドレスを指定する場合、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。
 - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
 - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。
- 複数のデバイスがハブを介して1つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ2 **traceroute** 機能はサポートされません。複数の CDP ネイバーが1つのポートで検出された場合、レイヤ2パスは特定されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

レイヤ2トレースルートの実行

送信元デバイスから宛先デバイスへ送られるパケットが通過する物理パスを表示するには、次のいずれかのコマンドを入力します。

```
Switch# traceroute mac source-mac-address destination-mac-address
```

または

```
Switch# traceroute mac ip source-ip destination-ip
```

次に、**traceroute mac** コマンドと **traceroute mac ip** コマンドを使用して、パケットが宛先に到達するまでに通過するネットワークの物理パスを表示する例を示します。

```
Switch# traceroute mac cc16.7eaa.7203 188b.45eb.cc64
Source cc16.7eaa.7203 found on Switch
1 Switch (1.1.1.1) : V11 => Gi1/0/1
Destination 188b.45eb.cc64 found on Switch
Layer 2 trace completed.
Switch#
```

```
Switch# traceroute mac ip 1.1.1.1 1.1.1.2 detail
Translating IP to mac .....
1.1.1.1 => cc16.7eaa.7203
1.1.1.2 => 188b.45eb.cc64
```

```
Source cc16.7eaa.7203 found on Switch[C9410R] (1.1.1.1)
1 Switch / C9410R / 1.1.1.1 :Gi1/0/1 [auto, auto]
Destination 188b.45eb.cc64 found on Switch[C9410R] (1.1.1.1)
Layer 2 trace completed.
Switch#
```

ICMP の設定

ICMP は、IP 接続を制御および管理するための多くのサービスを提供します。インターネットヘッダーに問題が検出された場合に、ICMP メッセージがルータまたはアクセスサーバによってホストまたはその他のルータに送信されます。ICMP の詳細については、RFC 792 を参照してください。

ICMP プロトコル到達不能メッセージの有効化

Cisco IOS ソフトウェアが不明なプロトコルを使用する非ブロードキャスト パケットを受け取ると、送信元に ICMP Protocol Unreachable メッセージを返します。

同様に、宛先アドレスまでのルートを確認していないため最終的な宛先に届かないパケットをソフトウェアが受け取ると、送信元に ICMP Host Unreachable メッセージを返します。この機能は、デフォルトで有効にされています。

ICMP Protocol Unreachable と Host Unreachable メッセージの生成を有効にするには、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

```
Switch (config-if)# [no] ip unreachable
```

ICMP 宛先到達不能メッセージを無効にするには、**no** キーワードを使用します。



(注) **no ip unreachable** コマンドを入力すると、パス MTU 検出機能が停止します。ネットワークの中のルータは、パケットを強制的に分割します。

インターネット制御メッセージプロトコル (ICMP) 宛先到達不能メッセージが生成されるレーートを制限するには、次のコマンドを入力します。

```
Switch (config)# [no] ip icmp rate-limit unreachable [df] milliseconds
```

レート制限を削除し、CPU 利用を低減させるには、**no** キーワードを使用します。

ICMP マスク応答メッセージの有効化

ネットワーク デバイスがインターネットワークの特定のサブネットワークに関して、サブネットマスクを認識していなければならない場合があります。この情報を取得するために、デバイスは ICMP Mask Request メッセージを送信します。これらのメッセージには、要求された情報を保有するデバイスの ICMP Mask Reply メッセージが応答します。Cisco IOS ソフトウェアは、ICMP マスクが有効になっている場合に、ICMP マスク要求メッセージに応答できます。応答機能が有効になっています。

Cisco IOS ソフトウェアが ICMP マスク応答メッセージを送信して、ICMP マスク要求に応答するように指定するには、次のコマンドを入力します。

```
Switch (config-if)# [no] ip mask-reply
```

この機能を無効にするには、**no** キーワードを使用します。

ポートステータスと接続の確認の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	ポートステータスと接続の確認	この機能には、モジュールとインターフェイスのステータスを確認する手順が含まれます。また、ネットワーク内のデバイス間の接続を確認する方法も含まれています。
Cisco IOS XE Fuji 16.8.1a	LED ステータスを表示するコマンド	LEDのステータスを表示するために show hardware led コマンドが導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 5 章

LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定

- [LLDP に関する制約事項 \(63 ページ\)](#)
- [LLDP、LLDP-MED、およびワイヤードロケーションサービスについて \(64 ページ\)](#)
- [LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定方法 \(68 ページ\)](#)
- [LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定例 \(79 ページ\)](#)
- [LLDP、LLDP-MED、ワイヤードロケーションサービスのモニタリングとメンテナンス \(80 ページ\)](#)
- [LLDP、LLDP-MED、およびワイヤードロケーションサービスの追加情報 \(81 ページ\)](#)
- [LLDP、LLDP-MED、およびワイヤードロケーションサービスの機能履歴 \(81 ページ\)](#)

LLDP に関する制約事項

- インターフェイスがトンネルポートに設定されていると、LLDPは自動的に無効になります。
- 最初にインターフェイス上にネットワーク ポリシー プロファイルを設定した場合、インターフェイス上に **switchport voice vlan** コマンドを適用できません。 **switchport voice vlan vlan-id** がすでに設定されているインターフェイスには、ネットワーク ポリシー プロファイルを適用できます。このように、そのインターフェイスには、音声または音声シグナリング VLAN ネットワーク ポリシー プロファイルが適用されます。
- ネットワーク ポリシープロファイルを持つインターフェイス上では、スタティックセキュア MAC アドレスを設定できません。
- Cisco Discovery Protocol と LLDP が両方とも同じスイッチ内で使用されている場合、Cisco Discovery Protocol が電源ネゴシエーションに使用されているインターフェイスで LLDP を無効にする必要があります。LLDP は、コマンド **no lldp tlv-select power-management** または **no lldp transmit / no lldp receive** を使用してインターフェイスレベルで無効にすることができます。

LLDP、LLDP-MED、およびワイヤードロケーションサービスについて

LLDP

Cisco Discovery Protocol (CDP) は、すべてのシスコ製デバイス（ルータ、ブリッジ、アクセスサーバ、スイッチ、およびコントローラ）のレイヤ2（データリンク層）上で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、ネットワーク接続されている他のシスコ デバイスを自動的に検出し、識別できます。

デバイスでは他社製のデバイスをサポートして他のデバイス間の相互運用性を確保するために、IEEE 802.1AB リンク層検出プロトコル (LLDP) をサポートしています。LLDP は、ネットワークデバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。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 でサポートされる TLV

LLDP は一連の属性をサポートし、これらを使用してネイバーデバイスを検出します。属性には、Type、Length、および Value の説明が含まれていて、これらを TLV と呼びます。LLDP をサポートするデバイスは、ネイバーとの情報の送受信に TLV を使用できます。このプロトコルは、設定情報、デバイス機能、およびデバイス ID などの詳細情報をアドバタイズできます。

スイッチは、次の基本管理 TLV をサポートします。これらは必須の LLDP TLV です。

- ポート記述 TLV
- システム名 TLV
- システム記述 TLV
- システム機能 TLV
- 管理アドレス TLV

次の IEEE 固有の LLDP TLV もアドバタイズに使用されて LLDP-MED をサポートします。

- ポート VLAN ID TLV (IEEE 802.1 に固有の TLV)
- MAC/PHY コンフィギュレーション/ステータス TLV (IEEE 802.3 に固有の TLV)

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) は LLDP の拡張版で、IP 電話などのエンドポイントデバイスとネットワーク デバイスの間で動作します。特に VoIP アプリケーションをサポートし、検出機能、ネットワーク ポリシー、Power over Ethernet (PoE)、インベントリ管

理、およびロケーション情報に関する TLV を提供します。デフォルトで、すべての LLDP-MED TLV が有効になります。

LLDP-MED でサポートされる TLV

LLDP-MED では、次の TLV がサポートされます。

- LLDP-MED 機能 TLV

LLDP-MED エンドポイントは、接続装置がサポートする機能と現在有効になっている機能を識別できます。

- ネットワーク ポリシー TLV

ネットワーク接続デバイスとエンドポイントはともに、VLAN 設定、および関連するレイヤ 2 とレイヤ 3 属性をポート上の特定アプリケーションにアダプタイズできます。たとえば、スイッチは使用する VLAN 番号を IP 電話に通知できます。IP 電話は任意のデバイスに接続し、VLAN 番号を取得してから、コール制御との通信を開始できます。

ネットワーク ポリシー プロファイル TLV を定義することによって、VLAN、サービス クラス (CoS)、Diffserv コードポイント (DSCP)、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。その後、これらのプロファイル属性は、スイッチで中央集約的に保守され、IP 電話に伝播されます。

- 電源管理 TLV

LLDP-MED エンドポイントとネットワーク接続デバイスの間で拡張電源管理を可能にします。デバイスおよび IP 電話は、デバイスの受電方法、電源プライオリティ、デバイスに必要な消費電力などの電源情報を通知することができます。

LLDP-MED は拡張電源 TLV もサポートして、きめ細かな電力要件、エンドポイント電源プライオリティ、およびエンドポイントとネットワークの接続デバイスの電源ステータスをアダプタイズします。LLDP が有効でポートに電力が供給されているときは、電力 TLV によってエンドポイントデバイスの実際の電力要件が決定するので、それに応じてシステムの電力バジェットを調整することができます。デバイスは要求を処理し、現在の電力バジェットに基づいて電力を許可または拒否します。要求が許可されると、スイッチは電力バジェットを更新します。要求が拒否されると、デバイスはポートへの電力供給をオフにし、Syslog メッセージを生成し、電力バジェットを更新します。LLDP-MED が無効になっている場合や、エンドポイントが LLDP-MED 電力 TLV をサポートしていない場合は、初期割り当て値が接続終了まで使用されます。

電力設定を変更するには、**power inline {auto [max max-wattage] | never | static [max max-wattage] | consumption <4000-60000> milliwatts}** インターフェイス コンフィギュレーション コマンドを入力します。PoE インターフェイスはデフォルトで **auto** モードに設定されています。値を指定しない場合は、最大値 (60 W) が許可されます。

- インベントリ管理 TLV

エンドポイントは、デバイスにエンドポイントの詳細なインベントリ情報を送信できます。インベントリ情報には、ハードウェアリビジョン、ファームウェアバージョン、ソフ

トウェアバージョン、シリアル番号、メーカー名、モデル名、アセット ID TLV などがあります。

- ロケーション TLV

デバイスからのロケーション情報をエンドポイントデバイスに提供します。ロケーション TLV はこの情報を送信することができます。

- 都市ロケーション情報

都市アドレス情報および郵便番号情報を提供します。都市ロケーション情報の例には、地名、番地、郵便番号などがあります。

- ELIN ロケーション情報

発信側のロケーション情報を提供します。ロケーションは、緊急ロケーション識別番号 (ELIN) によって決定されます。これは、緊急通報を Public Safety Answering Point (PSAP) にルーティングする電話番号で、PSAP はこれを使用して緊急通報者にコールバックすることができます。

- 地理的なロケーション情報

スイッチの緯度、経度、および高度などのスイッチ位置の地理的な詳細を指定します。

- カスタム ロケーション

スイッチの位置のカスタマイズされた名前と値を入力します。

ワイヤードロケーションサービス

デバイスは、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine (MSE) に送信するのにロケーションサービス機能を使用します。トラッキングされたデバイスは、ワイヤレスエンドポイント、ワイヤードエンドポイント、またはワイヤードデバイスやワイヤードコントローラになります。デバイスは、MSE に Network Mobility Services Protocol (NMSP) のロケーション通知および接続通知を介して、デバイスのリンクアップイベントおよびリンクダウンイベントを通知します。

MSE がデバイスに対して NMSP 接続を開始すると、サーバポートが開きます。MSE がデバイスに接続する場合は、バージョンの互換性を確保する 1 組のメッセージ交換およびサービス交換情報があり、その後にロケーション情報の同期が続きます。接続後、デバイスは定期的にロケーション通知および接続通知を MSE に送信します。インターバル中に検出されたリンクアップイベントまたはリンクダウンイベントは、集約されてインターバルの最後に送信されます。

デバイスがリンクアップイベントまたはリンクダウンイベントでデバイスの有無を確認した場合は、スイッチは、MAC アドレス、IP アドレス、およびユーザ名のようなクライアント固有情報を取得します。クライアントが LLDP-MED または CDP に対応している場合は、デバイスは LLDP-MED ロケーション TLV または CDP でシリアル番号および UDI を取得します。

デバイス機能に応じて、デバイスは次のクライアント情報をリンクアップ時に取得します。

- ポート接続で指定されたスロットおよびポート。
- クライアント MAC アドレスで指定された MAC アドレス。
- ポート接続で指定された IP アドレス。
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステータスは *new* として指定されます。
- シリアル番号、UDI。
- モデル番号。
- デバイスによる関連付け検出後の時間（秒）。

デバイス機能に応じて、デバイスは次のクライアント情報をリンクダウン時に取得します。

- 切断されたスロットおよびポート。
- MAC アドレス
- IP アドレス
- 802.1X ユーザ名（該当する場合）。
- デバイス カテゴリは、*wired station* として指定されます。
- ステータスは *delete* として指定されます。
- シリアル番号、UDI。
- デバイスによる関連付け解除検出後の時間（秒）。

デバイスがシャットダウンするときに、MSE との NMSP 接続が終了する前に、ステータス *delete* および IP アドレスとともに接続情報通知が送信されます。MSE は、この通知をデバイスに関連付けられているすべてのワイヤードクライアントに対する関連付け解除として解釈します。

デバイス上のロケーションアドレスを変更すると、デバイスは、影響を受けるポートを識別する NMSP ロケーション通知メッセージ、および変更されたアドレス情報を送信します。

デフォルトの LLDP 設定

表 7: デフォルトの LLDP 設定

機能	デフォルト設定
LLDP グローバル ステータス	無効
LLDP ホールドタイム（廃棄までの時間）	120 秒
LLDP タイマー（パケット更新頻度）	30 秒

機能	デフォルト設定
LLDP 再初期化遅延	2 秒
LLDP tlv-select	無効 (すべての TLV との送受信)
LLDP インターフェイス ステート	無効
LLDP 受信	無効
LLDP 転送	無効
LLDP med-tlv-select	無効 (すべての LLDP-MED TLV への送信)。 LLDP がグローバルに有効になると、 LLDP-MED-TLV も有効になります。

LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定方法

LLDP の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	lldp run 例： Device (config)# lldp run	デバイスで LLDP をグローバルに有効にします。

	コマンドまたはアクション	目的
ステップ 4	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	LLDP 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 5	lldp transmit 例： Device(config-if)# lldp transmit	LLDP パケットを送信するようにインターフェイスを有効にします。
ステップ 6	lldp receive 例： Device(config-if)# lldp receive	LLDP パケットを受信するようにインターフェイスを有効にします。
ステップ 7	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 8	show lldp 例： Device# show lldp	設定を確認します。
ステップ 9	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

LLDP 特性の設定

LLDP 更新の頻度、情報を廃棄するまでの保持期間、および初期化遅延時間を設定できます。送受信する LLDP および LLDP-MED TLV も選択できます。



(注) ステップ 3 ~ 6 は任意であり、どの順番で実行してもかまいません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	lldp holdtime seconds 例： Device(config)# lldp holdtime 120	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する必要がある期間を指定します。 指定できる範囲は 0 ～ 65535 秒です。 デフォルトは 120 秒です。
ステップ 4	lldp reinit delay 例： Device(config)# lldp reinit 2	（任意）任意のインターフェイス上で LLDP の初期化の遅延時間（秒）を指定します。 指定できる範囲は 2 ～ 5 秒です。 デフォルトは 2 秒です。
ステップ 5	lldp timer rate 例： Device(config)# lldp timer 30	（任意）インターフェイス上で LLDP の更新の遅延時間（秒）を指定します。 指定できる範囲は 5 ～ 65534 秒です。 デフォルトは 30 秒です。
ステップ 6	lldp tlv-select 例： Device(config)# tlv-select	（任意）送受信する LLDP TLV を指定します。
ステップ 7	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	LLDP 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。

	コマンドまたはアクション	目的
ステップ 8	lldp med-tlv-select 例： Device(config-if)# lldp med-tlv-select inventory management	(任意) 送受信する LLDP-MED TLV を指定します。
ステップ 9	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 10	show lldp 例： Device# show lldp	設定を確認します。
ステップ 11	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

LLDP-MED TLV の設定

デフォルトでは、デバイスはエンドデバイスから LLDP-MED パケットを受信するまで、LLDP パケットだけを送信します。スイッチは、MED TLV を持つ LLDP も送信します。LLDP-MED エントリが期限切れになった場合は、スイッチは再び LLDP パケットだけを送信します。

lldp インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスが次の表にリストされている TLV を送信ないように設定できます。

表 8: LLDP-MED TLV

LLDP-MED TLV	説明
inventory-management	LLDP-MED インベントリ管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV
power-management	LLDP-MED 電源管理 TLV

インターフェイスで TLV を有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	LLDP 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 4	lldp med-tlv-select 例： Device(config-if)# lldp med-tlv-select inventory management	有効にする TLV を指定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

Network-Policy TLV の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	network-policy profile profile number 例： Device(config)# network-policy profile 1	ネットワーク ポリシープロファイル番号を指定し、ネットワーク ポリシーコンフィギュレーションモードを開始します。指定できる範囲は 1 ～ 4294967295 です。
ステップ 4	{voice voice-signaling} vlan [vlan-id { cos cvalue dscp dvalue}] [[dot1p { cos cvalue dscp dvalue}] none untagged] 例： Device(config-network-policy)# voice vlan 100 cos 4	ポリシー属性の設定： <ul style="list-style-type: none"> voice：音声アプリケーションタイプを指定します。 voice-signaling：音声シグナリングアプリケーションタイプを指定します。 vlan：音声トラフィックのネイティブ VLAN を指定します。 vlan-id：（任意）音声トラフィックの VLAN を指定します。指定できる範囲は 1 ～ 4094 です。 cos cvalue：（任意）設定された VLAN に対するレイヤ 2 プライオリティサービスクラス (CoS) を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。 dscp dvalue：（任意）設定された VLAN に対する DiffServ コードポ

	コマンドまたはアクション	目的
		<p>イント (DSCP) 値を指定します。指定できる範囲は0～63です。デフォルト値は46です。</p> <ul style="list-style-type: none"> • dot1p : (任意) IEEE 802.1p プライオリティタギングおよびVLAN 0 (ネイティブVLAN) を使用するように電話を設定します。 • none : (任意) 音声VLANに関してIP Phoneに指示しません。IP Phoneのキーパッドから入力された設定を使用します。 • untagged : (任意) IP Phoneを、タグなしの音声トラフィックを送信するよう設定します。これがIP Phoneのデフォルト設定になります。
ステップ 5	<p>exit</p> <p>例 :</p> <pre>Device(config)# exit</pre>	グローバル コンフィギュレーションモードに戻ります。
ステップ 6	<p>interface interface-id</p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet2/0/1</pre>	ネットワーク ポリシープロファイルを設定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 7	<p>network-policy profile number</p> <p>例 :</p> <pre>Device(config-if)# network-policy 1</pre>	ネットワーク ポリシープロファイル番号を指定します。
ステップ 8	<p>lldp med-tlv-select network-policy</p> <p>例 :</p> <pre>Device(config-if)# lldp med-tlv-select network-policy</pre>	ネットワーク ポリシー TLV を指定します。

	コマンドまたはアクション	目的
ステップ 9	end 例： Device (config) # end	特権 EXEC モードに戻ります。
ステップ 10	show network-policy profile 例： Device# show network-policy profile	設定を確認します。
ステップ 11	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ロケーション TLV およびワイヤードロケーションサービスの設定

エンドポイントのロケーション情報を設定し、その設定をインターフェイスに適用するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	location { admin-tag string civic-location identifier {id host} elin-location string identifier id custom-location identifier {id host} geo-location identifier {id host} } 例： Device (config) # location civic-location identifier 1 Device (config-civic) # number 3550 Device (config-civic) # primary-road-name "Cisco Way"	エンドポイントにロケーション情報を指定します。 <ul style="list-style-type: none"> • admin-tag : 管理タグまたはサイト情報を指定します。 • civic-location : 都市ロケーション情報を指定します。 • elin-location : 緊急ロケーション情報 (ELIN) を指定します。

	コマンドまたはアクション	目的
	<pre>Device(config-civic)# city "San Jose" Device(config-civic)# state CA Device(config-civic)# building 19 Device(config-civic)# room C6 Device(config-civic)# county "Santa Clara" Device(config-civic)# country US</pre>	<ul style="list-style-type: none"> • custom-location : カスタム ロケーション情報を指定します。 • geo-location : 地理空間のロケーション情報を指定します。 • identifier id : 都市、ELIN、カスタム、または地理ロケーションの ID を指定します。 • host : ホストの都市、カスタム、または地理ロケーションを指定します。 • string : サイト情報またはロケーション情報を英数字形式で指定します。
ステップ 3	<p>exit</p> <p>例 :</p> <pre>Device(config-civic)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 4	<p>interface interface-id</p> <p>例 :</p>	ロケーション情報を設定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 5	<p>location { additional-location-information word civic-location-id {id host} elin-location-id id custom-location-id {id host} geo-location-id {id host} }</p> <p>例 :</p> <pre>Device(config-if)# location elin-location-id 1</pre>	<p>インターフェイスのロケーション情報を入力します。</p> <ul style="list-style-type: none"> • additional-location-information : ロケーションまたは場所に関する追加情報を指定します。 • civic-location-id : インターフェイスにグローバル都市ロケーション情報を指定します。 • elin-location-id : インターフェイスに緊急ロケーション情報を指定します。 • custom-location-id : インターフェイスにカスタム ロケーション情報を指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • geo-location-id : インターフェイスに地理空間のロケーション情報を指定します。 • host : ホストのロケーション ID を指定します。 • word : 追加のロケーション情報を指定する語またはフレーズを指定します。 • id : 都市、ELIN、カスタム、または地理ロケーションの ID を指定します。指定できる ID 範囲は 1 ~ 4095 です。
ステップ 6	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。
ステップ 7	次のいずれかを使用します。 <ul style="list-style-type: none"> • show location admin-tag <i>string</i> • show location civic-location identifier <i>id</i> • show location elin-location identifier <i>id</i> 例 : Device# show location admin-tag または Device# show location civic-location identifier または Device# show location elin-location identifier	設定を確認します。
ステップ 8	copy running-config startup-config 例 :	(任意) コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	Device# <code>copy running-config startup-config</code>	

デバイスでのワイヤードロケーションサービスの有効化

始める前に

ワイヤードロケーションが機能するためには、まず、**ip device tracking** グローバル コンフィギュレーション コマンドを入力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	enable 例： Device> <code>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）。
ステップ 2	configure terminal 例： Device# <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。
ステップ 3	nmosp notification interval {attachment location} interval-seconds 例： Device(config)# <code>nmosp notification interval location 10</code>	NMSP 通知間隔を指定します。 attachment ：接続通知間隔を指定します。 location ：ロケーション通知間隔を指定します。 <i>interval-seconds</i> ：デバイスから MSE にロケーション更新または接続更新が送信されるまでの期間（秒）。指定できる範囲は 1～30 です。デフォルト値は 30 です。
ステップ 4	end 例： Device(config)# <code>end</code>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	show network-policy profile 例 : Device# show network-policy profile	設定を確認します。
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

LLDP、LLDP-MED、およびワイヤードロケーションサービスの設定例

Network-Policy TLV の設定 : 例

次に、CoS を持つ音声アプリケーションの VLAN 100 を設定して、インターフェイス上のネットワーク ポリシー プロファイルおよびネットワーク ポリシー TLV を有効にする例を示します。

```
Device# configure terminal
Device(config)# network-policy 1
Device(config-network-policy)# voice vlan 100 cos 4
Device(config-network-policy)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy profile 1
Device(config-if)# lldp med-tlv-select network-policy
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Device-config-network-policy)# voice vlan dot1p cos 4
Device-config-network-policy)# voice vlan dot1p dscp 34
```

LLDP、LLDP-MED、ワイヤードロケーションサービスのモニタリングとメンテナンス

以下は、LLDP、LLDP-MED、ワイヤードロケーションサービスのモニタリングとメンテナンスのコマンドです。

コマンド	説明
clear lldp counters	トラフィックカウンタを0にリセットします。
clear lldp table	LLDP ネイバー情報テーブルを削除します。
clear nmsp statistics	NMSP 統計カウンタをクリアします。
show lldp	送信頻度、送信するパケットのホールドタイム、LLDP 初期化の遅延時間のような、インターフェイス上のグローバル情報を表示します。
show lldp entry <i>entry-name</i>	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力すると、すべてのネイバーの表示、またはネイバーの名前の入力が可能です。
show lldp interface [<i>interface-id</i>]	LLDP が有効になっているインターフェイスに関する情報を表示します。 表示対象を特定のインターフェイスに限定できます。
show lldp neighbors [<i>interface-id</i>] [detail]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、ポート ID など、ネイバーに関する情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show lldp traffic	送受信パケットの数、廃棄したパケットの数、認識できない TLV の数など、LLDP カウンタを表示します。
show location admin-tag <i>string</i>	指定した管理タグまたはサイトのロケーション情報を表示します。

コマンド	説明
<code>show location civic-location identifier id</code>	特定のグローバル都市ロケーションのロケーション情報を表示します。
<code>show location elin-location identifier id</code>	緊急ロケーションのロケーション情報を表示します。
<code>show network-policy profile</code>	設定されたネットワークポリシープロファイルを表示します。
<code>show nmsp</code>	NMSP 情報を表示します。

LLDP、LLDP-MED、およびワイヤードロケーションサービスの追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『 <i>Command Reference (Catalyst 9400 Series Switches)</i> 』の「 <i>Interface and Hardware Commands</i> 」を参照してください。

LLDP、LLDP-MED、およびワイヤードロケーションサービスの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	Link Layer Discovery Protocol (LLDP)、LLDP-MED、ワイヤードロケーションサービス	<p>LLDP は、ネットワーク デバイスがネットワーク上の他のデバイスに自分の情報をアドバタイズするために使用するネイバー探索プロトコルです。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。</p> <p>LLDP-MED はエンドポイントとネットワークデバイス間で動作します。</p> <p>ワイヤードロケーションサービスでは、接続されているデバイスの追跡情報を Cisco Mobility Services Engine (MSE) に送信できます。</p>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 6 章

システム MTU の設定

- [MTU について \(83 ページ\)](#)
- [MTU の設定方法 \(84 ページ\)](#)
- [システム MTU の設定例 \(85 ページ\)](#)
- [システム MTU に関するその他の関連資料 \(86 ページ\)](#)
- [システム MTU の機能履歴 \(86 ページ\)](#)

MTU について

イーサネットフレームで受信し、すべてのデバイスインターフェイスで送信されるペイロードのデフォルトの最大伝送ユニット (MTU) サイズは 1500 バイトです。

システム MTU 値の適用

次の表では、MTU 値の適用方法を示します。

表 9: MTU の値

設定	system mtu コマンド
スタンドアロンスイッチ	スイッチで system mtu コマンドを入力できますが、システム MTU 値はスイッチに対しては有効になりません。これは、ファストイーサネットポートに影響します。 指定できる範囲は 1500 ~ 9198 バイトです。

MTU サイズの設定に関する詳細については、このリリースのコマンドリファレンスで **system mtu** グローバル コンフィギュレーション コマンドを参照してください。

Cisco IOS XE Amsterdam 17.3.x 以降、IPv6 システムの最小 MTU は RFC 8200 により 1280 に固定されています。

MTU の設定方法

システム MTU の設定

スイッチドパケットの MTU サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	system mtu bytes 例： Device(config)# system mtu 1900	(任意) すべてのインターフェイスの MTU サイズを変更します。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。
ステップ 6	show system mtu 例： Device# show system mtu	設定を確認します。

プロトコル固有 MTU の設定

ルーテッドインターフェイスのシステム MTU 値を上書きするには、各ルーテッドインターフェイスでプロトコル固有の MTU を設定します。ルーテッドポートの MTU サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface 例： Device(config)# interface gigabitethernet0/0	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	ip mtu bytes 例： Device(config-if)# ip mtu 68	IPv4 MTU サイズを変更します。
ステップ 4	ipv6 mtu bytes 例： Device(config-if)# ipv6 mtu 1280	(任意) IPv6 MTU サイズを設定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	コンフィギュレーション ファイルに設定を保存します。
ステップ 7	show system mtu 例： Device# show system mtu	設定を確認します。

システム MTU の設定例

例：プロトコル固有 MTU の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ip mtu 900
Device(config-if)# ipv6 mtu 1286
Device(config-if)# end
```

例：システム MTU の設定

```
Device# configure terminal
Device(config)# system mtu 1600
Device(config)# exit
```

システム MTU に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9400 Series Switches)</i> の「 <i>Interface and Hardware Commands</i> 」の項を参照してください。

標準および RFC

標準/RFC	タイトル
RFC 8200	『 <i>Internet Protocol, Version 6 (IPv6) Specification</i> 』

システム MTU の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	システム MTU	システム MTU は、スイッチのすべてのインターフェイスで送信されるフレームの最大伝送ユニットサイズを定義します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 7 章

ポート単位の MTU の設定

- [ポート単位の MTU の制約事項 \(87 ページ\)](#)
- [ポート単位の MTU について \(87 ページ\)](#)
- [ポート単位の MTU の設定 \(88 ページ\)](#)
- [例：ポート単位の MTU の設定 \(89 ページ\)](#)
- [例：ポート単位の MTU の確認 \(89 ページ\)](#)
- [例：ポート単位の MTU の無効化 \(89 ページ\)](#)
- [ポート単位の MTU の機能履歴 \(90 ページ\)](#)

ポート単位の MTU の制約事項

- ポート単位の MTU は、管理ポートでは設定できません。
- ポート単位の MTU は、SVL リンクでは設定できません。
- ポートチャネルのメンバーはポート単位の MTU を使用して設定できません。ポートチャネルの MTU 設定から MTU を取得します。
- ポート単位の MTU は、サブインターフェイスとポートチャネルサブインターフェイスではサポートされていません。

ポート単位の MTU について

system mtu コマンドを使用して、デバイス上のすべてのインターフェイスの MTU サイズを同時に設定できます。すべてのインターフェイスで送受信されるフレームのデフォルト最大伝送単位 (MTU) サイズは、1500 バイトです。**system mtu** コマンドはグローバルコマンドであり、MTU をポートレベルで設定することはできません。Cisco IOS XE 17.1.1 以降では、ポート単位の MTU を設定できます。ポート単位の MTU はポートレベルとポートチャネルレベルの MTU 設定をサポートします。ポート単位の MTU を使用すると、異なるインターフェイスと異なるポートチャネルインターフェイスに異なる MTU 値を設定できます。

ポートにポート単位の MTU 値が設定されると、そのポートのプロトコル固有の MTU もポート単位の MTU 値に変更されます。ポート上でポート単位の MTU が設定されている場合でも、インターフェイス上でプロトコル固有の MTU を 256 からポート単位の MTU 値の範囲で設定できます。

ポート単位の MTU が無効になっている場合、ポートの MTU はシステムの MTU 値に戻ります。

show interface mtu コマンドを使用して、インターフェイスのポート単位の MTU 設定を表示できます。

インターフェイスでポート単位の MTU 設定が変更された場合は、次のような動作が予期されます。

- ポートチャネルが PAgP モードか LACP モードの場合、インターフェイスがフラップしません。
- ポートチャネルが **on** モードの場合、インターフェイスはフラップしません。
- インターフェイスがポートチャネルでない場合、インターフェイスはフラップしません。

インターフェイス コンフィギュレーションモードで **mtubytes** コマンドの **no** 形式を使用して、ポート単位の MTU を無効にできます。

ポート単位の MTU の設定

インターフェイスの特定のポートのスイッチドパケットの MTU サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface <i>typeswitch-number/slot-number/port-number</i> 例： Device(config)# int FortyGigabitEthernet2/5/0/20	インターフェイスを設定し、インターフェイス コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	mtubytes 例： Device(config-if)# mtu 6666	インターフェイスの特定のポートの MTU サイズを設定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

例：ポート単位の MTU の設定

次に、インターフェイスでポート単位の MTU を設定する例を示します。

```
Device# configure terminal
Device(config)# interface FortyGigabitEthernet2/5/0/20
Device(config-if)# mtu 6666
Device(config-if)# end
```

例：ポート単位の MTU の確認

次に、**show interface mtu** コマンドを使用してインターフェイスのポート単位の MTU を確認する例を示します。

```
Device# show interface mtu
Port          Name          MTU
Fo2/5/0/19   Name          1500
Fo2/5/0/20   Name          6666
Fo2/5/0/21   ixia_7_21    1500
```

例：ポート単位の MTU の無効化

次に、インターフェイスでポート単位の MTU を無効にする例を示します。

```
Device# configure terminal
Device(config)# interface FortyGigabitEthernet2/5/0/20
Device(config-if)# no mtu
Device(config-if)# end
```

ポート単位の MTU の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.1.1	ポート単位の MTU	ポート単位の MTU は、特定のポートまたはポートチャネルで送受信されるフレームの最大伝送ユニットサイズを定義します。 。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 8 章

EEE の設定

- [EEE の制約事項 \(91 ページ\)](#)
- [EEE について \(91 ページ\)](#)
- [EEE の設定方法 \(92 ページ\)](#)
- [EEE の監視 \(93 ページ\)](#)
- [EEE の設定例 \(94 ページ\)](#)
- [EEE に関するその他の関連資料 \(94 ページ\)](#)
- [EEE 設定の機能履歴 \(94 ページ\)](#)

EEE の制約事項

Energy Efficient Ethernet (EEE) には次の制限があります。

- EEE の設定を変更すると、デバイスがレイヤ1の自動ネゴシエーションを再起動しなければならないため、インターフェイスがリセットされます。
- 受信パスでデータを受け入れる前により長いウェイクアップ時間を必要とするデバイスのリンク層検出プロトコル (LLDP) を有効にする必要がある場合があります。これにより、デバイスは送信リンク パートナーから拡張システムのウェイク アップ時間についてネゴシエーションできます。
- マルチギガビットイーサネット ポートリンクが 100 Mbps の速度にネゴシエートされた場合、EEE はデバイスで省電力を開始しません。

EEE について

EEE の概要

Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネット ネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。

デフォルトの EEE 設定

EEE の設定方法

EEE 対応リンク パートナーに接続されているインターフェイスの EEE を有効または無効にできます。

EEE の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	設定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	power efficient-ethernet auto 例 : Device(config-if)# power efficient-ethernet auto	特定のインターフェイスで EEE を有効にします。EEE が有効になっている場合、デバイスはリンク パートナーに EEE をアダプタイズし、自動ネゴシエートします。
ステップ 4	no power efficient-ethernet auto 例 : Device(config-if)# no power efficient-ethernet auto	指定したインターフェイス上で EEE を無効にします。
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

EEE の監視

表 10: EEE 設定を表示するコマンド

コマンド	目的
show eee capabilities interface interface-id	指定インターフェイスの EEE 機能を表示します。
show eee status interface interface-id	指定したインターフェイスの EEE ステータス情報を表示します。
show eee counters interface interface-id	指定したインターフェイスの EEE 機能を表示します。 (注) Cisco IOS XE Gibraltar 16.12.1 では、マルチギガビットイーサネットポート (mGig) を搭載したラインカードについては show eee counters interface interface-id コマンドはサポートされません。

次に、**show eee** コマンドの例を示します。

```
Switch#show eee capabilities interface gigabitEthernet2/0/1
Gi2/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner : yes (100-Tx and 1000T auto)

ASIC/Interface : EEE Capable/EEE Enabled

Switch#show eee status interface gigabitEthernet2/0/1
Gi2/0/1 is up
EEE(efficient-ethernet): Operational
Rx LPI Status : Low Power
Tx LPI Status : Low Power
Wake Error Count : 0

ASIC EEE STATUS
Rx LPI Status : Receiving LPI
Tx LPI Status : Transmitting LPI
Link Fault Status : Link Up
Sync Status : Code group synchronization with data stream intact
```

```
Switch#show eee counters interface gigabitEthernet2/0/1

LP Active Tx Time (10us) : 66649648
LP Transitioning Tx : 462
LP Active Rx Time (10us) : 64911682
LP Transitioning Rx : 153
```

EEE の設定例

次に、インターフェイスで EEE を有効にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# power efficient-ethernet auto
```

次に、インターフェイスで EEE を無効にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# no power efficient-ethernet auto
```

EEE に関するその他の関連資料

EEE 設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	Energy Efficient Ethernet	Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネットネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。
Cisco IOS XE Gibraltar 16.12.1	マルチギガビット (mGig) イーサネットポートの EEE	mGig イーサネットポートを搭載したラインカードに Energy Efficient Ethernet が導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 9 章

Power over Ethernet の設定

- [PoE の前提条件](#) (97 ページ)
- [Power over Ethernet について](#) (98 ページ)
- [PoE と UPOE の設定方法](#) (105 ページ)
- [電力ステータスのモニタ](#) (113 ページ)
- [PoE に関するその他の関連資料](#) (117 ページ)
- [Power over Ethernet の機能履歴](#) (117 ページ)

PoE の前提条件

PoE 電源管理の前提条件

次の前提条件が PoE 電力管理機能に適用されます。

- この機能が動作するためのスーパーバイザ Field-Programmable Gate Array (FPGA) の最小バージョンは 19082605 です。FPGA のバージョンがこれより低い場合にユーザが **power inline auto-shutdown** コマンドを設定しようとする、次のメッセージが表示されます。

```
This FPGA version does not support power inline auto shutdown feature.  
Please upgrade to FPGA from year 2019 and above.
```

- インターフェイスに **power inline port priority** コマンドを設定できますが、PoE 電源管理機能を動作させるには、**power inline auto-shutdown** コマンドをグローバル コンフィギュレーション モードで設定する必要があります。
- ISSU を実行する前に、次のコマンドを無効にします。
 - **power inline auto-shutdown**
 - **power inline port priority** (設定されているすべてのインターフェイス上で)

Power over Ethernet について

次の項では、Power over Ethernet (PoE)、サポートされているプロトコルと標準規格、および電源管理について説明します。

PoE および PoE+ ポート

PoE 対応スイッチポートでは、回路に電力が供給されていないことをデバイスが検出した場合、接続している次のデバイスのいずれかに電力が自動的に供給されます。

- シスコ準規格の受電デバイス (Cisco IP Phone など)
- IEEE 802.3af 準拠の受電デバイス
- IEEE 802.3at 準拠の受電デバイス
- IEEE 802.3bt 準拠の受電デバイス

受電デバイスが PoE スwitchポートおよび AC 電源に接続されている場合、冗長電力として利用できます。受電デバイスが PoE ポートにだけ接続されている場合、受電デバイスには冗長電力は供給されません。

サポート対象のプロトコルおよび標準規格

デバイスは、PoE のサポートに次のプロトコルと標準規格を使用します。

- 電力消費を通知する CDP : 受電デバイスは、消費している電力量をデバイスに通知します。デバイスはこの電力消費に関するメッセージに応答しません。デバイスは、PoE ポートに電力を供給するか、このポートへの電力を取り除くだけです。
- Cisco Intelligent Power Management : 受電デバイスおよびデバイスは、電力ネゴシエーション CDP メッセージによって電力消費レベルについてネゴシエーションを行います。ネゴシエーションでは、現在の割り当てとは異なる電力レベルが必要なシスコの受電デバイスが動作できるようにします。受電デバイスはまず IEEE クラス電力、つまり 15.4 W (準規格のシスコ PD) でブートしてから電力をネゴシエートして、適切な電力レベルで動作します。受電デバイスの電力消費量は、デバイスから確認を受信した場合にのみ、要求した電源モードに切り替わります。

高電力装置は、電力ネゴシエーション CDP をサポートしないデバイスでは低電力モードで動作できます。

Cisco Intelligent Power Management は、電力消費に関して CDP との下位互換性があるため、デバイスは、受信する CDP メッセージに従って応答します。CDP はサードパーティの受電デバイスでサポートされません。このため、デバイスは IEEE 分類を使用して装置の消費電力を判断します。

- IEEE 802.3af : この規格の主な機能は、受電デバイスの検出、電力の管理、切断の検出です。オプションとして受電デバイスの電力分類があります。詳細については、この規格を参照してください。
- IEEE 802.3at : PoE+ 標準では、受電デバイスに供給される最大電力が、1ポートあたり 15.4 W から 30 W に増えました。
- Cisco UPOE 機能は、CDP や LLDP などのレイヤ 2 電力ネゴシエーションプロトコルを使用して、シグナルペアおよび RJ-45 イーサネットケーブルのスペアペアの両方に、最大 60 W の電力 (2 X 30 W) を供給します。4 線式 Cisco 独自開発スペアペア電力 TLV での 30 W 以上の LLDP および CDP 要求により、スペアペアに電力を供給できます。

IEEE 802.3bt モードで有効にすると、Cisco UPOE デバイスは 802.3bt タイプ 3 デバイスとして機能し、すべてのポートでクラス 6 までサポートします (このドキュメントの「IEEE 電力分類」の表を参照)。



(注) 次の UPOE ラインカードのみが IEEE 802.3bt 準拠のタイプ 3 デバイスです。

- C9400-LC-48U
- C9400-LC-48UX

- IEEE 802.3bt : IEEE 802.3bt 標準規格では、カテゴリ 5e 以上のケーブルを 4 ペアにわたって最大 90 W を受電デバイスに供給できます。また、この標準規格では追加のクラス (クラス 5 ~ 8) の給電機 (PSE) と受電デバイスが導入されました (PSE 出力電力が 45 ~ 90 W、受電デバイスの入力電力が 40 ~ 71.3 W)。新しいタイプの PSE または受電デバイス (タイプ 3 (60 W) とタイプ 4 (90 W)) が導入されています。IEEE 802.3bt 標準規格では、デュアルシグネチャ電源装置、シングルシグネチャ電源装置、およびシングルペア電源装置がサポートされます。また、タイプ 4 の受電デバイスがタイプ 3 の PSE に接続されているシナリオを処理するための電源の降格もサポートされています。

IEEE 802.3bt の詳細については、標準規格を参照してください。

- Cisco UPOE+ : Cisco UPOE+ 機能は、IEEE 802.3bt 準拠のタイプ 4 デバイスで最大 90 W の電力を供給できます。

タイプ 3 PSE は、60 W への電力降格によってタイプ 4 の受電デバイスに電源を投入できません。

Cisco IOS XE リリース 16.12.1 では、802.3bt 準拠のタイプ 4 デバイスである C9400-LC-48H が導入されています。

従来のシスコ給電デバイス (7910、7940、7960 IP Phone、AP350 ワイヤレスアクセスポイントなど) によっては、IEEE 802.3bt 規格で定義されているとおりのタイプ 4 の電源装置 (PSE) との互換性がない場合があります。接続されている場合、PSE は、受電デバイスに電力を供給する試みが定期的に試行されるたびに「Tstart」または「Imax」の障害を報

告します。これらの従来のシスコ給電デバイスを引き続き使用するには、それらを Cisco PoE+/UPOE PSE に接続します。

標準規格の検出シグニチャ容量を満たさない受電デバイス（CIVS-IPC-6000P など）は、POE+ デバイスや UPOE モードで動作している Cisco UPOE デバイスで正しく検出される場合がありますが、802.3bt モードで動作している場合は正しく検出されないことがあります。

受電デバイスの検出と初期電力割り当て

スイッチは、PoE 対応ポートがシャットダウン状態でなく、PoE が有効になっていて（デフォルト）、接続された装置が AC アダプタから電力供給されていない場合、シスコの準規格受電デバイスまたは IEEE 準拠の受電デバイスを検出します。

装置の検出後、スイッチは、次のように装置のタイプに応じて電力要件を判断します。

- 初期電力割り当ては、受電デバイスが要求する最大電力量です。スイッチは、受電デバイスを検出および電力供給する場合、この電力を最初に割り当てます。スイッチが受電デバイスから CDP メッセージを受信し、受電デバイスが CDP 電力ネゴシエーションメッセージを通じてスイッチと電力レベルをネゴシエートしたときに、初期電力割り当てが調整される場合があります。
- スイッチは検出した IEEE 装置を消費電力クラス内で分類します。スイッチは、電力バジェットに使用可能な電力量に基づいて、ポートに通電できるかどうかを決定します。次の「IEEE 電力分類」の表にこれらのレベルを示します。

表 11: IEEE 電力分類

クラス	デバイスから要求される最大電力レベル
0 (クラスステータスは不明)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W
5	45 W
6	60 W
7	75 W
8	90 W

スイッチは電力要求をモニタリングおよび追跡して必要な場合にだけ電力供給を許可します。スイッチはそれ自体の電力バジェット（PoEのデバイスで使用可能な電力量）を追跡します。

電力の供給許可または拒否がポートで行われると、スイッチはパワーアカウンティング計算を実行し、電力バジェットを最新に保ちます。

電力がポートに投入された後に、スイッチが CDP を使用して、接続されたシスコ受電デバイスの CDP 固有の電力消費要件を調べます。この要件は、CDP メッセージに基づいて割り当てられる電力量です。スイッチはこれに従って、CDP または LLDP を介して、電力バジェットを調整します。CDP はサードパーティ製の PoE デバイスには適用されません。スイッチは要件を処理して電力の供給または拒否を行います。要求が許可されると、スイッチは電力バジェットを更新します。要求が拒否された場合は、スイッチはポートの電源がオフになるようにし、syslog メッセージを生成します。受電デバイスはより多くの電力を得るために、スイッチとのネゴシエーションを行うこともできます。

PoE+ では、最大 30 W の電力をネゴシエートするために、受電デバイスが IEEE 802.3at と LLDP 電源をメディア依存インターフェイス (MDI) のタイプ、長さ、および値の説明 (TLV)

(Power-via-MDI TLV) とともに使用します。シスコの準規格デバイスとシスコの IEEE 受電デバイスは CDP または IEEE 802.3at Power-via-MDI 電力ネゴシエーションメカニズムを使用して最大 30 W の電力レベルを要求できます。



(注) ソフトウェア コンフィギュレーション ガイドおよびコマンドリファレンスでは、CDP 固有の電力消費要件を実際電力消費要件と呼んでいます。

不足電圧、過電圧、過熱、オシレータ障害、または短絡状態による障害をスイッチが検出した場合、ポートへの電力供給をオフにし、syslog メッセージを生成し、電力バジェットを更新します。

電力管理モード

デバイスでは、次の PoE モードがサポートされます。

- **auto** : 接続されているデバイスで電力が必要であるかどうか自動的に検出されます。ポートに接続されている受電デバイスをデバイスが検出し、デバイスに十分な電力がある場合は、電力を供給して電力バジェットを更新し、先着順でポートの電力供給をオンに切り替えます。

すべての受電デバイス用としてデバイスに十分な電力がある場合は、すべての受電デバイスが起動します。デバイスに接続された受電デバイスすべてに対し十分な電力が利用できる場合、すべてのデバイスに電力が供給されます。使用可能な PoE がない場合、または他の装置が電力供給を待機している間に装置の接続が切断されて再接続した場合、どの装置へ電力を供給または拒否されるかが判断できなくなります。

許可された電力がシステムの電力バジェットを超えている場合、デバイスは電力を拒否し、ポートへの電力がオフになっていることを確認したうえで syslog メッセージを生成します。電力供給が拒否された後、デバイスは定期的に電力バジェットを再確認し、継続して電力要求の許可を試みます。

デバイスにより電力を供給されている装置が、さらに壁面コンセントに接続している場合、デバイスは装置に電力を供給し続ける場合があります。このとき、装置がデバイスか

ら受電しているか、AC 電源から受電しているかにかかわらず、デバイスは引き続き装置へ電力を供給していることを報告し続ける場合があります。

受電デバイスが取り外された場合、デバイスは切断を自動的に検出し、ポートから電力を取り除きます。非受電デバイスを接続しても、そのデバイスに障害は発生しません。

ポートで許可される最大ワット数を指定できます。受電デバイスの IEEE クラス最大ワット数が、設定されている最大値より大きい場合、デバイスはそのポートに電力を供給しません。デバイスが受電デバイスに電力を供給する場合でも、受電デバイスが設定された最大値を超える電力を CDP メッセージを通じて後から要求すると、デバイスはポートへの電力供給を行いません。その受電デバイスに割り当てられていた電力は、グローバル電力バジェットに送られます。ワット数を指定しない場合、デバイスは最大値の電力を供給します。任意の PoE ポートで **auto** 設定を使用してください。auto モードがデフォルト設定です。

- **static** : デバイスは、受電デバイスが接続されていなくてもポートに電力をあらかじめ割り当て、そのポートで電力が使用できるようにします。デバイスは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの CDP メッセージによって調節されることはありません。これは、電力があらかじめ割り当てられていることから、最大ワット数以下の電力を使用するすべての受電デバイスが固定ポートに接続されている場合に電力が保証されるためです。ポートはもう先着順方式ではなくなります。

ただし、受電デバイスの IEEE クラスが最大ワット数を超えると、デバイスは装置に電力を供給しません。受電デバイスが最大ワット数を超える電力を消費していることを CDP メッセージによって知ると、デバイスは受電デバイスをシャットダウンします。

ワット数を指定しない場合、デバイスは最大数をあらかじめ割り当てます。デバイスは、受電デバイスを検出した場合に限り、ポートに電力を供給します。優先順位が高いインターフェイスには、**static** 設定を使用してください。

- **never** : デバイスは受電デバイスの検出を無効にして、電力が供給されていないデバイスが接続されても、PoE ポートに電力を供給しません。PoE 対応ポートに電力を絶対に適用せず、そのポートをデータ専用ポートにする場合に限り、このモードを使用してください。

ほとんどの場合、デフォルトの設定（自動モード）の動作は適切に行われ、プラグアンドプレイ動作が提供されます。それ以上の設定は必要ありません。ただし、優先順位の高い PoE ポートを設定したり、PoE ポートをデータ専用にしたり、最大ワット数を指定して高電力受電デバイスをポートで禁止したりする場合は、このタスクを実行します。

電力モニタリングおよび電力ポリシング

リアルタイム電力消費のポリシングを有効にした場合、受電デバイスが最大割り当て量（カットオフ電力値）を超えて電力を消費すると、デバイスはアクションを開始します。

PoE が有効になっている場合、デバイスは受電デバイスのリアルタイムの電力消費を検知します。接続されている受電デバイスのリアルタイム電力消費をデバイスが監視することを、電力モニタリングまたは電力検知といいます。また、デバイスは電力ポリシング機能を使用して消費電力をポリシングします。

電力モニタリングは、シスコのインテリジェントな電力管理および CDP ベースの消費電力に対して下位互換性があります。電力モニタリングはこれらの機能とともに動作して、PoE ポートが受電デバイスに電力を供給できるようにします。

デバイスは次のようにして、接続されている装置のリアルタイム電力消費を検知します。

1. デバイスは、個々のポートでリアルタイム消費電力をモニタリングします。
2. デバイスは、ピーク時の電力消費を含め、電力消費を記録します。デバイスは `CISCO-POWER-ETHERNET-EXT-MIB` を介して情報を報告します。
3. 電力ポリシングが有効になっている場合、デバイスはリアルタイムの消費電力を装置に割り当てられた最大電力と比較して、消費電力をポリシングします。最大消費電力は、PoE ポートでカットオフ電力とも呼ばれます。

デバイスがポートで最大電力割り当てを超える電力を使用すると、デバイスはポートへの電力供給をオフにしたり、またはデバイスの設定に基づいて受電デバイスに電力を供給しながらデバイスが `syslog` メッセージを生成することができます。デフォルトでは、すべての PoE ポートで消費電力のポリシングは無効になっています。

PoE の `error-disabled` ステートからのエラー回復が有効になっている場合、指定の時間の経過後、デバイスは PoE ポートを `error-disabled` ステートから自動的に回復させます。

エラー回復が無効になっている場合、`shutdown` および `no shutdown` インターフェイス コンフィギュレーション コマンドを使用して、手動で PoE ポートを有効にできます。

4. ポリシングが無効になっている場合、受電デバイスは PSE によって割り当てられた電力に基づいて最大電力を消費できます。受電デバイスが割り当てられた量を超える電力を消費すると、ポートは `Imax` エラーになり、障害状態になります。

電力消費値

ポートの初期電力割り当ておよび最大電力割り当てを設定することができます。ただし、これらの値は、デバイスが PoE ポートの電力供給をオンまたはオフにするタイミングを指定するために設定する値です。最大電力割り当ては、受電デバイスの実際の電力消費と同じではありません。デバイスによって電力ポリシングに使用される実際のカットオフ電力値は、設定済みの電力値と同等ではありません。

電力ポリシングが有効になっている場合、デバイスは、スイッチポートで受電デバイスの消費電力を超える消費電力ポリシングを行います。最大電力割り当てを手動で設定する場合、スイッチポートと受電デバイス間のケーブルでの電力損失を考慮する必要があります。カットオフ電力とは、受電デバイスの定格消費電力とケーブル上での最悪時の電力損失を合計したものです。

デバイスの PoE が有効になっている場合、電力ポリシングを有効にすることを推奨します。たとえば、クラス 1 デバイスの場合、ポリシングが無効になっており、`power inline auto max 6300` インターフェイス コンフィギュレーション コマンドを使用してカットオフ電力値を設定すると、PoE ポートに設定される最大電力割り当ては 6.3 W (6300 mW) になります。装置が最大で 6.3 W の電力を必要とする場合、デバイスはポートに接続されている装置に電力を供給します。CDP によるパワーネゴシエーション実施後の値または IEEE 分類値が設定済みカットオフ値を超えると、デバイスは接続されている装置に電力を供給しなくなります。デバイスは

PoEポートで電力供給をオンにした後、受電デバイスのリアルタイム電力消費のポリシングを行わないので、受電デバイスは最大割り当て量を超えて電力を消費できるようになり、デバイスと、他の PoE ポートに接続されている受電デバイスに悪影響を及ぼすことがあります。

PoE 電力管理

すべてのポートにはラインカードの論理スロット番号に基づいてデフォルトの PoE ポート優先順位が割り当てられます。ユーザは、インターフェイス コンフィギュレーション モードで **power inline port priority** コマンドを使用して、PoE ポートに新しい優先順位を明示的に割り当てることができます。電力不足のシナリオでは、PoE ポートが電力を失う順序が優先順位によって決まります。優先順位 7（最も低い優先順位）の PoE ポートが最初にシャットダウンし、優先順位 0（最も高い優先順位）の PoE ポートが最後にシャットダウンします。静的モードのポートの場合、PoE 負荷制限中に静的ポートが最後にシャットダウンされるように、設定された管理用の優先順位に関係なく、それらのポートの動作上の優先順位は 0 になります。PoE ポートは、ラインカードがシャットダウンされる前にシャットダウンされます。

システムは、9000 ワットの瞬間的な低下に耐えることができます。1つの PoE 優先順位に 6000 ワットを超える値を割り当てないことを推奨します。PoE の優先度レベルに 6000 ワットを超える値が設定されている場合は警告メッセージが表示され、PoE の優先度レベルに 9000 ワットを超える値が設定されている場合は重大なメッセージが表示されます。

次の表に、ラインカードのスロット番号とデフォルトの PoE ポートの優先順位を示します。

表 12: デフォルトの PoE ポートの優先順位

スロット番号	Cisco Catalyst C9404R スイッチ	Cisco Catalyst C9407R スイッチ	Cisco Catalyst C9410R スイッチ
1	0	0	0
2	スーパーバイザ	1	1
3	スーパーバイザ	スーパーバイザ	2
4	1	スーパーバイザ	3
5	–	2	スーパーバイザ
6	–	3	スーパーバイザ
7	–	4	4
8	–	–	5
9	–	–	6
10	–	–	7

Cisco Universal Power Over Ethernet

Cisco Universal Power Over Ethernet (Cisco UPOE) は、シグナルペア (導線 1、2、3、6) 付きの RJ-45 ケーブルのスペアペア (導線 4、5、7、8) を使用して、IEEE 802.3.at PoE 標準を拡張するシスコ独自のテクノロジーで、標準のイーサネット ケーブル配線インフラストラクチャ (クラス D 以上) により最大 60 W の電力を供給する機能を提供します。スペアペアの電力は、スイッチポートとエンドデバイスが Cisco UPOE 対応であることを CDP または LLDP を使用して相互に識別し、エンドデバイスがスペアペアの電力の有効化を要求したときに有効になります。スペアペアに給電されると、エンドデバイスは、CDP または LLDP を使用して、スイッチから最大 60 W の電力をネゴシエートできます。

エンドデバイスが信号ペアとスペアペアの両方で検出と分類をサポートしているても PoE 対応であるが、Cisco UPOE に必要な CDP または LLDP の拡張をサポートしていない場合、4 ペアの強制モード設定によりスイッチポートから信号ペアとスペアペアの両方の電力が自動的に有効になります。

Cisco UPOE デバイス (C9400-LC-48U と C9400-LC-48UX) をアップグレードして、タイプ 3 電源デバイスとして 802.3bt 標準規格をサポートできます。デバイスは同じポートで Cisco UPOE と 802.3bt タイプ 3 をサポートできます。802.3bt 準拠のタイプ 3 デバイスと Cisco UPOE デバイスはどちらも 60 W を提供しますが、動作が異なることに注意してください。802.3bt 準拠のデバイスは、物理分類時に最大電力要件を相互に識別します (「表 11: IEEE 電力分類」の表を参照)。802.3bt 準拠のタイプ 3 受電デバイスは、物理レイヤで要求される電力よりも多くの電力を LLDP で要求できません。つまり、802.3bt 準拠のクラス 4 受電デバイスは、CDP または LLDP を使用して 30 W を超える電力を要求できません。一方、802.3bt 準拠のクラス 6 受電デバイスは、データリンクレイヤが確立される前に、物理層から 60 W を要求します。

基本的に、802.3at デバイスは ALT-A (信号ペア) 30 W をサポートします。Cisco UPOE デバイスは、CDP または LLDP ネゴシエーションを通じて最大 60 W をサポートします。802.3bt 準拠のタイプ 3 の 4 ペアデバイスは、物理分類から直接、Alt-A と Alt-B (両方の有線ペア) で最大 60 W をサポートできます。802.3bt 準拠の Cisco UPOE PSE は、物理的に要求された受電デバイスをサポートします。さらに、Cisco UPOE PSE は引き続き UPOE 受電デバイスをサポートします。Cisco UPOE デバイスを 802.3bt モードにアップグレードする場合、アップグレードされた PSE に接続された UPOE 受電デバイスの動作に変更はありません。

PoE と UPOE の設定方法

次のタスクでは、PoE と UPOE の設定方法について説明します。

PoE ポートの電力管理モードの設定



(注) PoE 設定を変更するとき、設定中のポートでは電力が低下します。新しい設定、その他の PoE ポートの状態、電力バジェットの状態により、そのポートの電力は再びアップしない場合があります。たとえば、ポート1が自動でオンの状態になっていて、そのポートを固定モードに設定するとします。デバイスはポート1から電力を取り除き、受電デバイスを検出してポートに電力を再び供給します。ポート1が自動でオンの状態になっており、最大ワット数を 10 W に設定した場合、デバイスはポートから電力を取り除き、受電デバイスを再び検出します。デバイスは、受電デバイスがクラス 1、クラス 2、またはシスコ専用受電デバイスのいずれかの場合に、ポートに電力を再び供給します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">• プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、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	power inline {auto [max max-wattage] never static [max max-wattage] consumption milli-watts-consumption } 例： Device(config-if)# power inline auto	ポートの PoE モードを設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none">• auto : 受電デバイスの検出を有効にします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。これがデフォルト設定です。• max max-wattage : ポートで許可される電力を制限します。Cisco UPOE ポートの範囲は 4000 ~ 60000 mW です。値を指定しない場合は、最大電力が供給されます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • never : デバイス検出を無効にし、ポートへの電力供給を無効にします。 <p>(注) ポートにシスコの受電デバイスが接続されている場合は、power inline never コマンドでポートを設定しないでください。問題のあるリンクアップが発生し、ポートが error-disabled ステートになることがあります。</p> <ul style="list-style-type: none"> • static : 受電デバイスの検出を有効にします。デバイスが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます (確保します)。デバイスは、デバイスが接続されていなくてもこのポートに電力を予約し、デバイスの検出時に電力が供給されることを保証します。 • consumption : 特定のインターフェイスに接続された受電デバイスの PoE 電力消費量 (ミリワット単位) を設定します。電力消費量の許容範囲は、4000 ~ 90000 ミリワットです。 <p>電力消費量の自動調整を再び有効にするには、no キーワードを使用するか、または 60000 ミリワットを指定します。</p> <p>デバイスは、自動モードに設定されたポートに電力を割り当てる前に、固定モードに設定されたポートに PoE を割り当てます。</p>
ステップ 5	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	show power inline [<i>[interface-id]</i>] [detail] 例： Device# show power inline	デバイス、または指定したインターフェイスかの PoE ステータスを表示します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

信号ペアとスペアペアの電源投入の有効化



- (注) デバイスが接続されているラインカードが 802.3bt 準拠モードの場合は、このタスクを実行する必要はありません。これは、**power inline four-pair forced** コマンドが 802.3bt 準拠モードで冗長になっているためです。

エンドデバイスがスペアペアでインライン給電に未対応の場合か、またはエンドデバイスが Cisco UPOE の CDP または LLDP 拡張をサポートしている場合は、このタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、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	power inline four-pair forced 例： Device(config-if)# power inline four-pair forced	スイッチ ポートから信号ペアおよびスペアペアの両方の電力を有効にします。 (注) デバイスが接続されているラインカードが 802.3bt 準拠モードの場合は、この手順は不要です。

	コマンドまたはアクション	目的
ステップ 4	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。

電力ポリシングの設定

デフォルトでは、デバイスは接続されている受電デバイスの消費電力をリアルタイムでモニタリングします。消費電力に対するポリシングを行うようにデバイスを設定できます。デフォルトではポリシングは無効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">• プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、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	power inline police [action{log errdisable}] 例 : Device(config-if) # power inline police	ポートでリアルタイム消費電力が最大電力割り当てを超える場合、次のいずれかのアクションを実行するようにデバイスを設定します。 <ul style="list-style-type: none">• power inline police : PoE ポートをシャットダウンし、ポートへの電力供給をオフにし、PoE ポートを error-disabled ステートに移行します。

	コマンドまたはアクション	目的
		<p>(注) errdisable detect cause inline-power グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled の原因についてエラー検出を有効にできます。 errdisable recovery cause inline-power interval interval グローバル コンフィギュレーション コマンドを使用すると、PoE error-disabled ステートから回復するためのタイマーを有効にすることもできます。</p> <ul style="list-style-type: none"> • power inline police action errdisable : リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力供給をオフにします。 • power inline police action log : ポートへの電力供給を継続し、syslog メッセージを生成します。 <p>action log キーワードを入力しない場合、デフォルトのアクションによってポートがシャットダウンされ、error-disabled ステートになります。</p>
ステップ 5	exit 例 : Device(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	次のいずれかを使用します。 <ul style="list-style-type: none"> • errdisable detect cause inline-power • errdisable recovery cause inline-power • errdisable recovery interval interval 例 : Device(config)# errdisable detect cause inline-power	<p>(任意) PoE error-disabled ステートからのエラー回復を有効にし、PoE回復メカニズム変数を設定します。</p> <p>デフォルトでは、回復間隔は 300 秒です。</p> <p>interval interval には、error-disabled ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ~ 86400 です。</p>

	コマンドまたはアクション	目的
	<pre>Device(config)# errdisable recovery cause inline-power Device(config)# errdisable recovery interval 100</pre>	
ステップ 7	exit 例 : <pre>Device(config)# exit</pre>	特権 EXEC モードに戻ります。
ステップ 8	次のいずれかを使用します。 <ul style="list-style-type: none"> • show power inline police • show errdisable recovery 例 : <pre>Device# show power inline police Device# show errdisable recovery</pre>	電力モニタリングステータスを表示し、エラー回復設定を確認します。
ステップ 9	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

PoE 電力管理の設定

インターフェイスで PoE ポートの優先順位を設定する前に、**power inline auto-shutdown** コマンドをグローバル コンフィギュレーション モードで有効にする必要があります。このコマンドは、デフォルトで無効になっています。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例 : <pre>Device# configure terminal</pre>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	power inline auto-shutdown 例： Device(config)# power inline auto-shutdown	PoE ポートの自動シャットダウン制御を有効にします。
ステップ 4	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、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 5	power inline port priority value 例： Device(config-if)# power inline port priority 7	指定したインターフェイスの PoE ポートの優先順位を設定します。
ステップ 6	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

タイプ 3 UPOE モジュールでの 802.3bt モードの有効化

タイプ 3 受電デバイスの IEEE 802.3bt 標準規格をサポートする C9400-LC-48U モジュールと C9400-LC-48UX モジュールは、デフォルトで 802.3at モードになっています。 **hw-module slot slot upoe-plus** コマンドをグローバル コンフィギュレーション モードで使用すると、これらのデバイスで 802.3bt モードを有効にできます。 **hw-module slot slot upoe-plus** コマンドはモジュールの電源を再投入することに注意してください。

```
Device(config)# hw-module slot 4 upoe-plus
Performing oir to update poe fw on chassis 1 slot 4
Device#
*Mar 21 05:39:36.215: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 4/0, interfaces disabled
```



警告 **hw-module switch upoe-plus** コマンドはモジュールで活性挿抜 (OIR) を実行し、モジュールは OIR の間、アウトオブサービスになります。

コマンドの **no** 形式 (**no hw-module slot slot upoe-plus**) を使用すると 802.3at モードに戻すことができます。



(注) C9400-LC-48H モジュールは、IEEE 802.3bt 標準規格をサポートするタイプ 4 PSE です。C9400-LC-48H はデフォルトでは 802.3bt モードです。したがって、モード変換 CLI **hw-module slot slot upoe-plus** は C9400-LC-48H モジュールではサポートされません。

非準拠受電デバイスのサポート

power inline auto コマンドと **power inline static** コマンドを使用すると、両方のペアセットで電力を使用できる受電デバイスが IEEE 分類 (表 11: IEEE 電力分類) に従って物理レイヤ上で許可されているよりも多くの電力を使用できます。

次に、接続先のポートで最大 40 W を使用するように設定されたクラス 4 の受電デバイスの例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/14
Device(config-if)# power inline static 40000
Device(config-if)# end

Device# show power inline upoe gigabitEthernet 1/0/14
Codes: DS - Dual Signature device, SS - Single Signature device
       SP - Single Pairset device

Interface  Admin  Type Oper-State      Power(Watts)   Class  Device Name
          State      Alt-A,B    Allocated Utilized  Alt-A,B
-----
Gig1/0/14  static SS    on,on          40.0    36.7    4      Ieee PD
```

電力ステータスのモニタ

Power over Ethernet 設定をモニタリングおよび確認するには、次の **show** コマンドを使用します。

表 13: 電力ステータスの **show** コマンド

コマンド	目的
show power inline police	電力ポリシングのデータを表示します。
show power inline [[<i>interface-id</i>] [detail]]	スイッチ上のインタフェースの PoE ステータスを表示します。
show power inline consumption <i>interface-id</i>	そのインターフェイスの PoE 電力消費量を表示します。
show power inline upoe-plus [<i>interface-id</i>] [module]	802.3bt 準拠モードが有効になっているインターフェイスの PoE ステータスを表示します。
show power inline priority <i>interface-id</i>	そのインターフェイスの PoE の状態と優先順位を表示します。

例

次に、802.3bt 対応のインターフェイスの PoE ステータスを表示するコマンドの例を示します。

```

Device# show power inline upoe-plus gigabitEthernet 1/0/23

Codes: DS - Dual Signature device, SS - Single Signature device
       SP - Single Pairset device

Interface  Admin  Type Oper-State      Power(Watts)  Class  Device Name
          State                Alt-A,B    Allocated Utilized  Alt-A,B
-----
Gi1/0/4   auto   SP   on               4.0           3.8    1          Ieee PD
Gi1/0/15  auto   SS   on,on            60.0          10.5   6          Ieee PD
Gi1/0/23  auto   DS   on,on            45.4          26.9   3,4       Ieee PD

```

次に、**show power inline upoe-plus** コマンドの出力に表示されるフィールドについて説明します。

表 14: **show power inline upoe-plus** コマンドの出力に表示されるフィールド

フィールド	説明
Type	受電デバイスのタイプ：シングルペアセットデバイス (SP)、シングルシグネチャデバイス (SS)、デュアルシグネチャデバイス (DS)
Oper-State	ポート上の各ペアの状態
Power Allocated	ポートに割り当てられた電力
Power Utilized	ポート上の受電デバイスの消費電力
Class Alt-A, B	対応する信号ペアまたはスペアペア
Device Name	CDP によってアドバタイズされた受電デバイスの名前

show power inline detail コマンドは、デバイスの動作ステータス、デバイスの IEEE クラス、物理的に割り当てられたクラス、割り当てられた電力、ポートで測定された（電力）などの 802.3bt 準拠デバイスの情報を表示するように拡張されました。

クラス 5 シングルシグニチャ受電デバイスが LLDP を介して要求を送信し、PSE によって割り当てられた電力を低減する（このため、割り当てられた電力が 30 W に低下）シナリオを検討します。次に、このようなシナリオでの **show power inline detail** コマンドの出力を示します。

```

Device# show power inline gigabitEthernet 1/0/29 detail

Interface: Gi1/0/29
Inline Power Mode: auto
Operational status (Alt-A,B): on,on
Device Detected: yes
Device Type: Ieee PD
Connection Check: SS
IEEE Class (Alt-A,B): 5
Physical Assigned Class (Alt-A,B): 5
Discovery mechanism used/configured: Ieee and Cisco
Police: off

Power Allocated

```

```

Admin Value: 60.0
Power drawn from the source: 30.0
Power available to the device: 30.0
Allocated Power (Alt-A,B): 30.0

Actual consumption
Measured at the port(watts) (Alt-A,B): 10.5
Maximum Power drawn by the device since powered on: 10.5

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Power Negotiation Used: IEEE 802.3bt LLDP
LLDP Power Negotiation      --Sent to PD--      --Rcvd from PD--
Power Type:                  Type 2 PSE          Type 2 PD
Power Source:                 Primary           PSE
Power Priority:               low                critical
PD 4PID:                      0                  1
Requested Power(W):          25.5                25.5
Allocated Power(W):          25.5                40.0
Requested Power ModeA(W):    0.0                  6.5
Allocated Power ModeA(W):    0.0                25.5
Requested Power ModeB(W):    0.0                13.0
Allocated Power ModeB(W):    0.0                25.5
PSE Powering Status:        4 pair SS PD       Ignore
PD Powering Status:         Ignore             SS PD
PSE Power Pair ext:         Both Alternatives  Both Alternatives
DS Class Mode A ext:        SS PD              Class 2
DS Class Mode B ext:        SS PD              Class 4
SS Class ext:                Class 4            Class 5
PSE Type ext:                Type 3 PSE         Type 3 SS PD
PSE Max Avail Power:        51.0              51.2
PSE Auto Class Supp:        No                 No
PD Auto Class Req:          No                 No
PD Power Down Req:          No                 No
PD Power Down Time(sec):    0                  70

Four-Pair PoE Supported: Yes
Spare Pair Power Enabled: Yes
Four-Pair PD Architecture: Shared

```

次に、デュアルシグネチャ受電デバイスがPSEによって割り当てられた電力を低減する要求を送信する出力の例を示します。

```
Device#show power inline gigabitEthernet 1/0/23 detail
```

```

Interface: Gi1/0/23
Inline Power Mode: auto
Operational status (Alt-A,B): on,on
Device Detected: yes
Device Type: Ieee PD
Connection Check: DS
IEEE Class (Alt-A,B): 3,4
Physical Assigned Class (Alt-A,B): 3,4
Discovery mechanism used/configured: Ieee and Cisco
Police: off

Power Allocated
Admin Value: 60.0
Power drawn from the source: 22.4
Power available to the device: 22.4

```

```

Allocated Power (Alt-A,B): 7.0,15.4
  Actual consumption
Measured at the port(watts) (Alt-A,B): 2.7,2.7
Maximum Power drawn by the device since powered on: 5.5
  Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Power Negotiation Used: IEEE 802.3bt LLDP
LLDP Power Negotiation      --Sent to PD--      --Rcvd from PD--
Power Type:                  Type 2 PSE          Type 2 PD
Power Source:                Primary          PSE
Power Priority:              low                critical
PD 4PID:                     0                1
Requested Power(W):         19.9              0.0
Allocated Power(W):         19.9              0.0
Requested Power ModeA(W):   6.5                6.5
Allocated Power ModeA(W):   6.5              13.0
Requested Power ModeB(W):  13.0              13.0
Allocated Power ModeB(W):  13.0              25.5
PSE Powering Status:       4 pair DS PD      Ignore
PD Powering Status:        Ignore              2 pair DS PD
PSE Power Pair ext:        Both Alternatives  Both Alternatives
DS Class Mode A ext:       Class 2            Class 3
DS Class Mode B ext:       Class 3            Class 4
SS Class ext:              DS PD              Class 5
PSE Type ext:              Type 3 PSE         Type 3 SS PD
PSE Max Avail Power:       51.0              51.2
PSE Auto Class Supp:       No                No
PD Auto Class Req:         No                No
PD Power Down Req:         No                No
PD Power Down Time(sec):   0                70

Four-Pair PoE Supported: Yes
Spare Pair Power Enabled: Yes
Four-Pair PD Architecture: Independent

```

次に、**show power inline priority** コマンドの出力例を示します。

```

Device# show power inline priority gigabitEthernet 1/0/1

Interface  Admin   Oper      Admin   Oper
           State   State     Priority Priority
-----
Gig1/0/1   static on       5       7

Priority   Power Per
           Priority(Watts)
-----
0          0
1          1440
2          1440
3          2880
4          0
5          2880
6          0
7          0

Device# show power inline priority gigabitEthernet 1/0/45

```

```

Interface      Admin   Oper      Admin      Oper
              State   State     Priority    Priority
-----
Gi1/0/45      auto    on         5           5

Priority      Power Per
              Priority(Watts)
-----
0             0
1             1440
2             1440
3             2880
4             0
5             2880
6             0
7             0

```

次に、**show power inline priority** コマンドの出力に表示されるフィールドについて説明します。

表 15: **show power inline priority** コマンドの出力に表示されるフィールド

フィールド	説明
Admin State	管理モード : auto、off、static
Oper State	動作モード : on、off、faulty、power-deny
Admin Priority	管理優先順位レベル : 0 ~ 7
Oper Priority	動作優先順位レベル : 0 ~ 7
Power Per Priority(Watts)	PoE ポートの優先順位に割り当てられる電力

PoE に関するその他の関連資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドに関する完全な構文および使用方法の詳細について。	『 <i>Command Reference Guide</i> 』の「Interface and Hardware Commands」の項を参照してください。

Power over Ethernet の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	Power over Ethernet (PoE)	<p>Power over Ethernet (PoE) では、銅線イーサネットケーブル経由で LAN スイッチングインフラストラクチャがエンドポイント（受電デバイスという）に電力を供給できます。次のタイプのエンドポイントに PoE から電力を供給できません。</p> <ul style="list-style-type: none"> シスコ準規格受電デバイス IEEE 802.3af 準拠の受電デバイス IEEE 802.3at 準拠の受電デバイス
Cisco IOS XE Gibraltar 16.11.1	IEEE 802.3bt タイプ 3 PD のサポート（最大 60 W）	C9400-LC-48U および C9400-LC-48UX ラインカードで 802.3bt 準拠モードを有効にするために hw-module slot upoe-plus コマンドが導入されました。
Cisco IOS XE Gibraltar 16.12.1	IEEE 802.3bt タイプ 4 PD のサポート（最大 90 W）	802.3bt 準拠のタイプ 4 モジュール、C9400-LC-48H が導入されました。
Cisco IOS XE Amsterdam 17.3.1	PoE 電力管理	PoE 電力管理では、インターフェイスにポートの優先順位を設定して、停電時に最初にシャットダウンするインターフェイスを決定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 10 章

2 イベント分類の設定

- [2 イベント分類の制約事項 \(121 ページ\)](#)
- [2 イベント分類について \(121 ページ\)](#)
- [2 イベント分類の設定 \(122 ページ\)](#)
- [例: 2 イベント分類の設定 \(122 ページ\)](#)
- [2 イベント分類の機能情報 \(123 ページ\)](#)

2 イベント分類の制約事項

2 イベント分類には次の制約が適用されます。

- 2 イベント分類の設定は、エンドポイントを物理的に接続する前に行っておく必要があります。または、電力を供給しているポートの手動 shut/no-shut を行います。
- ポートへの電力供給は MCU ファームウェアのアップグレード時には中断され、ポートはアップグレード直後にバックアップされます。

2 イベント分類について

クラス 4 デバイスが検出されると、IOS は、CDP または LLDP のネゴシエーションを行うことなく 30W を割り当てます。これは、リンクがアップする前であっても、クラス 4 の電源デバイスは 30W を得ることを意味します。

また、ハードウェアレベルで、PSE は 2 イベント分類を行い、これにより、クラス 4 PD はハードウェアから 30W を供給する PSE の能力を検出し、それ自体を登録することができます。また、CDP/LLDP パケット交換を待つことなく最大 PoE+ レベルまで移動できます。

2 イベントがポートで有効になったら、ポートの遮断または開放を手動で行うか、または PD を再度接続して IEEE 検出を再度開始する必要があります。2 イベント分類がポートで有効になっている場合、クラス 4 デバイスの電力バジェット割り当ては 30W です。その他の場合は 15.4W です。

2 イベント分類の設定

2 イベント分類についてスイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、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	power inline port 2-event 例： Device(config-if)# power inline port 2-event	スイッチで 2 イベント分類を設定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

例：2 イベント分類の設定

次に、2 イベント分類を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# power inline port 2-event
Device(config-if)# end
```

2 イベント分類の機能情報

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

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

表 16: 2 イベント分類の機能情報

機能名	リリース	機能情報
2 イベント分類	Cisco IOS XE Everest 16.6.1	クラス 4 デバイスが検出されると、IOS は、CDP または LLDP のネゴシエーションを行うことなく 30W を割り当てます。これは、リンクがアップする前であっても、クラス 4 の電源デバイスは 30W を得ることを意味します。



第 11 章

COAP プロキシ サーバの設定

- COAP プロキシ サーバの制約事項 (125 ページ)
- COAP プロキシ サーバについて (126 ページ)
- COAP プロキシ サーバの設定方法 (126 ページ)
- COAP プロキシ サーバの設定例 (130 ページ)
- COAP プロキシ サーバのモニタリング (134 ページ)
- COAP の機能情報 (135 ページ)

COAP プロキシ サーバの制約事項

次の制約事項は、COAP プロキシ サーバに適用されます。

- スイッチは、ipv6 ブロードキャスト (CSCuW26467) を使用する CoAP クライアントとして自身をアダプタイズできません。
- 監視のサポートは実装されていません。
- Blockwise 要求はサポートされていません。シスコは、block-wise 応答を処理し、block-wise 応答を生成できます。
- DTLS サポートは、RawPublicKey および証明書ベースのモードに対してのみ有効です。
- スイッチは、DTLS クライアントとして動作しません。DTLS はエンドポイントに対してのみ。
- エンドポイントは、CBOR ペイロードを処理し、応答すると想定されています。
- クライアント側要求は、JSON であると想定されています。
- IPv6 ブロードキャストの問題により、スイッチは IPv6 として他のリソース ディレクトリに自身をアダプタイズすることはできません。

COAP プロキシサーバについて

COAP プロトコルは、制限されたデバイスで使用できるように設計されています。HTTP が情報にアクセスする際にサーバ上で動作するのと同じ方法で、COAP は制限されたデバイス上で動作します。

COAP と HTTP の比較を次に示します。

- Web サーバの場合、プロトコルは **HTTP**、トランスポートは **TCP**、転送される最も一般的な情報の形式は **HTML** です。
- 制約付きデバイスの場合、プロトコルは **COAP**、トランスポートは **UDP**、一般的な情報の形式は **JSON/link-format/CBOR** です。

COAP によって、HTTP の場合と同様に **GET/POST** メタファーと RESTful API を使用してデバイスにアクセスし、管理する手段が提供されます。

COAP プロキシサーバの設定方法

COAP プロキシサーバを設定するには、コンフィギュレーションモードで COAP プロキシと COAP エンドポイントを設定できます。

コマンドは **coap [proxy | endpoints]** です。

COAP プロキシの設定

スイッチで COAP プロキシを開始または停止するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	coap proxy 例：	COAP プロキシサブモードを開始します。

	コマンドまたはアクション	目的
	Device(config)# coap proxy	(注) coap proxy を停止して、 coap proxy の下にあるすべての設定を削除するには、 no coap proxy コマンドを使用します。
ステップ 4	<p>security [none [[ipv4 ipv6] {<i>ip-address ip-mask/prefix</i>} list {<i>ipv4-list name</i> / <i>ipv6-list-name</i>}] dtls [id-trustpoint {<i>identity-trustpoint label</i>}] [verification-trustpoint {<i>verification-trustpoint</i>} [ipv4 ipv6 {<i>ip-address ip-mask/prefix</i>}] list {<i>ipv4-list name</i> <i>ipv6-list-name</i>}]]</p> <p>例 :</p> <pre>Device(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0</pre>	<p>暗号化タイプを引数と見なします。サポートされる2つのセキュリティモードは none と dtls です。</p> <ul style="list-style-type: none"> none : そのポートにセキュリティがないことを示します。 <p>security none を使用すると、最大5つのIPv4アドレスと最大5つのIPv6アドレスを関連付けることができます。</p> <ul style="list-style-type: none"> dtls : DTLSセキュリティは、オプションであるRSAトラストポイントと検証トラストポイントを要します。検証トラストポイントがないと、通常の公開キー交換が行われます。 <p>security dtls を使用すると、最大5つのIPv4アドレスと最大5つのIPv6アドレスを関連付けることができます。</p> <p>(注) coap proxy のすべてのセキュリティ設定を削除するには、no security コマンドを使用します。</p>
ステップ 5	<p>max-endpoints {<i>number</i>}</p> <p>例 :</p> <pre>Device(config-coap-proxy)#max-endpoints 10</pre>	<p>(任意) スイッチで学習できるエンドポイントの最大数を指定します。デフォルト値は10です。指定できる範囲は1～500です。</p> <p>(注) coap proxy に設定されたすべての最大エンドポイントを削除するには、no max-endpoints コマンドを使用します。</p>

	コマンドまたはアクション	目的
ステップ 6	<p>port-unsecure {<i>port-num</i>}</p> <p>例 :</p> <pre>Device (config-coap-proxy) #port-unsecure 5683</pre>	<p>(任意) デフォルト 5683 以外のポートを設定します。指定できる範囲は 1 ~ 65000 です。</p> <p>(注) coap proxy のすべてのポート設定を削除するには、no port-unsecure コマンドを使用します。</p>
ステップ 7	<p>port-dtls {<i>port-num</i>}</p> <p>例 :</p> <pre>Device (config-coap-proxy) #port-dtls 5864</pre>	<p>(任意) デフォルト 5684 以外のポートを設定します。</p> <p>(注) coap proxy のすべて DTLS のポート設定を削除するには、no port-dtls コマンドを使用します。</p>
ステップ 8	<p>resource-directory [<i>ipv4</i> <i>ipv6</i>] {<i>ip-address</i> }]</p> <p>例 :</p> <pre>Device (config-coap-proxy) #resource-directory ipv4 192.168.1.1</pre>	<p>スイッチが COAP クライアントとして動作できるユニキャストアップストリームリソースのディレクトリサーバを設定します。</p> <p>resource-directory を使用すると、最大 5 つの IPv4 アドレスと最大 5 つの IPv6 アドレスを設定できます。</p> <p>(注) coap proxy のすべてのリソースディレクトリ設定を削除するには、no resource-directory コマンドを使用します。</p>
ステップ 9	<p>list [<i>ipv4</i> <i>ipv6</i>] {<i>list-name</i>}</p> <p>例 :</p> <pre>Device (config-coap-proxy) #list ipv4 trial_list</pre>	<p>(任意) ライトとリソースを学習できる IP アドレス範囲を制限します。上記の security [<i>none</i> <i>dtls</i>] コマンドオプションで使用する、IP アドレス/マスクの名前付きリストを作成します。</p> <p>list を使用して、IPv4 または IPv6 に関係なく、最大 5 つの IP リストを設定できます。IP リストにつき最大 5 つの IP アドレスを設定できます。</p> <p>(注) COAP プロキシサーバの IP リストを削除するには、no list [<i>ipv4</i> <i>ipv6</i>] {<i>list-name</i>} コマンドを使用します。</p>

	コマンドまたはアクション	目的
ステップ 10	start 例： Device (config-coap-proxy) # start	このスイッチで COAP プロキシを開始します。
ステップ 11	stop 例： Device (config-coap-proxy) # stop	このスイッチで COAP プロキシを停止します。
ステップ 12	exit 例： Device (config-coap-proxy) # exit	COAP プロキシサブモードを終了します。
ステップ 13	end 例： Device (config) # end	特権 EXEC モードに戻ります。

COAP エンドポイントの設定

複数の IPv4/IPv6 スタティック エンドポイントをサポートするように COAP プロキシを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	coap endpoint [ipv4 ipv6] {ip-address} 例 : Device(config)# coap endpoint ipv4 1.1.1.1 Device(config)# coap endpoint ipv6 2001::1	スイッチ上でスタティック エンドポイントを設定します。 <ul style="list-style-type: none"> • ipv4 : IPv4 スタティック エンドポイントを設定します。 • ipv6 : IPv6 スタティック エンドポイントを設定します。 (注) エンドポイントで coap proxy を停止するには、 no coap endpoint [ipv4 ipv6] {ip-address} コマンドを使用します。
ステップ 4	exit 例 : Device(config-coap-endpoint)# exit	COAP エンドポイント サブモードを終了します。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

COAP プロキシサーバの設定例

例 : COAP プロキシサーバの設定

次の例に、最大 10 のエンドポイントをサポートするようにポート番号 5683 を設定する方法を示します。

```
#coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10
```

次の例に、セキュリティ設定がされていない *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します。

```
Device(config-coap-proxy)# security ?
  dtls  dtls
  none  no security
```

```
Device(config-coap-proxy)#security none ?
  ipv4  IP address range on which to learn lights
```

```

ipv6      IPv6 address range on which to learn lights
list      IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 ?
A.B.C.D  {/nn || A.B.C.D}  IP address range on which to learn lights

Device(config-coap-proxy)#security none ipv4 1.1.0.0 255.255.0.0

```

次の例に、**dtls id trustpoint** セキュリティ設定がされている *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します。

```

Device(config-coap-proxy)#security dtls ?
id-trustpoint DTLS RSA and X.509 Trustpoint Labels
ipv4 IP address range on which to learn lights
ipv6 IPv6 address range on which to learn lights
list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
verification-trustpoint Certificate Verification Label
<cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Device(config-coap-proxy)#security dtls ?
id-trustpoint DTLS RSA and X.509 Trustpoint Labels
ipv4 IP address range on which to learn lights
ipv6 IPv6 address range on which to learn lights
list IP address range on which to learn lights

Device(config-coap-proxy)# security dtls ipv4 1.1.0.0 255.255.0.0

```



(注) **ipv4/ipv6/list** を設定するには、**id-trustpoint** と (任意) **verification-trustpoint** を事前に設定しておく必要があります。設定していない場合はエラーが表示されます。

次の例に、トラストポイントを設定する方法を示します。これは、**id trustpoint** 設定の COAP **security dtls** の前提条件です。

```

ip domain-name myDomain
crypto key generate rsa general-keys exportable label MyLabel modulus 2048

Device(config)#crypto pki trustpoint MY_TRUSTPOINT
Device(ca-trustpoint)#rsa keypair MyLabel 2048
Device(ca-trustpoint)#enrollment selfsigned
Device(ca-trustpoint)#exit

Device(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no

```

```
Generate Self Signed Router Certificate? [yes/no]: yes
```

次の例に、**dtls verification trustpoint** によって *ipv4 1.1.0.0 255.255.0.0* に COAP プロキシを設定する方法を示します（証明書または検証トラストポイントによる DTLS）。

```
Device(config-coap-proxy)#security dtls ?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Device(config-coap-proxy)#security dtls id-trustpoint ?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
  verification-trustpoint Certificate Verification Label
  <cr>

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT
verification-trustpoint ?
  WORD Identity TrustPoint Label

Device(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT
verification-trustpoint CA-TRUSTPOINT ?
  <cr>
```

次の例に、検証トラストポイントを設定する方法を示します。これは、**verification trustpoint** 設定の **COAP security dtls** の前提条件です。

```
Device(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12...
Source filename [hostA.p12]?
Reading file from flash:hostA.p12
CRYPTO_PKI: Imported PKCS12 file successfully.
```

次の例に、セキュリティ [**none** | **dtls**] コマンド オプションで使用する、**trial-list** という名前のリストを作成する方法を示します。

```
Device(config-coap-proxy)#list ipv4 trial_list
Device(config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Device(config-coap-proxy-iplist)#exit
Device(config-coap-proxy)#security none list trial_list
```

次の例に、**coap** プロキシ サブ モードで使用できるすべての拒否コマンドを示します。

```
Device(config-coap-proxy)#no ?
  ip-list          Configure IP-List
  max-endpoints    maximum number of endpoints supported
```

```
port-unsecure      Specify a port number to use
port-dtls          Specify a dtls-port number to use
resource-discovery Resource Discovery Server
security           CoAP Security features
```

次の例に、coap プロキシで複数の IPv4/IPv6 スタティック エンドポイントを設定する方法を示します。

```
Device(config)# coap endpoint ipv4 1.1.1.1
Device(config)# coap endpoint ipv4 2.1.1.1
Device(config)# coap endpoint ipv6 2001::1
```

次の例に、COAP プロトコルの詳細を表示する方法を示します。

```
Device#show coap version
CoAP version 1.0.0
RFC 7252
```

```
Device#show coap resources
Link format data =
</>
</1.1.1.6/cisco/context>
</1.1.1.6/cisco/actuator>
</1.1.1.6/cisco/sensor>
</1.1.1.6/cisco/lldp>
</1.1.1.5/cisco/context>
</1.1.1.5/cisco/actuator>
</1.1.1.5/cisco/sensor>
</1.1.1.5/cisco/lldp>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/lldp>
```

```
Device#show coap globals
Coap System Timer Values :
  Discovery   : 120 sec
  Cache Exp  : 5 sec
  Keep Alive  : 120 sec
  Client DB   : 60 sec
  Query Queue: 500 ms
  Ack delay   : 500 ms
  Timeout     : 5 sec

Max Endpoints      : 10
Resource Disc Mode : POST
```

```
Device#show coap stats
Coap Stats :
Endpoints : 2
Requests  : 20
Ext Queries : 0
```

```

Device#show coap endpoints
List of all endpoints :

Code : D - Discovered , N - New
#      Status   Age (s)   LastWKC (s)   IP
-----
1      D         10        94             1.1.1.6
2      D          6         34             1.1.1.5

Endpoints - Total : 2 Discovered : 2 New : 0

```

```

Device#show coap dtls-endpoints
#      Index State   String State   Value   Port IP
-----
1      3      SSLOK    3           48969   20.1.1.30
2      2      SSLOK    3           53430   20.1.1.31
3      4      SSLOK    3           54133   20.1.1.32
4      7      SSLOK    3           48236   20.1.1.33

```

次の例に、COAP プロトコルのデバッグに使用できるすべてのオプションを示します。

```

Device#debug coap ?
all          Debug CoAP all
database     Debug CoAP Database
errors       Debug CoAP errors
events       Debug CoAP events
packet       Debug CoAP packet
trace        Debug CoAP Trace
warnings     Debug CoAP warnings

```

COAP プロキシ サーバのモニタリング

COAP プロトコルの詳細を表示するには、次の表のコマンドを使用します。

表 17: COAP 固有のデータを表示するコマンド

show coap version	IOS COAP バージョンと RFC 情報を表示します。
show coap resources	スイッチのリソースと、スイッチが学習したリソースを表示します。
show coap endpoints	検出され、学習されたエンドポイントを表示します。
show coap globals	タイマー値とエンドポイント値を表示します。
show coap stats	エンドポイント、要求、および外部クエリのメッセージ数を表示します。
show coap dtls-endpoints	dtls エンドポイントのステータスを表示します。

表 18: COAP コマンドをクリアするコマンド

clear coap database	スイッチで学習された COAP、およびエンドポイント情報の内部データベースをクリアします。
----------------------------	---

COAP プロトコルをデバッグするには、次の表のコマンドを使用します。

表 19: COAP プロトコルをデバッグするコマンド

debug coap database	COAP データベース出力をデバッグします。
debug coap errors	COAP エラー出力をデバッグします。
debug coap events	COAP イベント出力をデバッグします。
debug coap packets	COAP パケット出力をデバッグします。
debug coap trace	COAP トレース出力をデバッグします。
debug coap warnings	COAP 警告出力をデバッグします。
debug coap all	すべての COAP 出力をデバッグします。



(注) デバッグを無効にする場合は、コマンドの前に「no」キーワードを追加します。

COAP の機能情報

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

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

表 20: COAP の機能情報

機能名	リリース	機能情報
COAP	Cisco IOS XE Everest 16.6.1	COAP プロトコルは、制限されたデバイスで使用できるように設計されています。HTTP が情報にアクセスする際にサーバ上で動作するのと同じ方法で、COAP は制限されたデバイス上で動作します。



第 12 章

外部 USB Bluetooth ドングルの設定

- [外部 USB Bluetooth ドングルの設定の制約事項 \(137 ページ\)](#)
- [外部 USB Bluetooth ドングルの設定について \(137 ページ\)](#)
- [スイッチでの外部 USB Bluetooth ドングルの設定方法 \(138 ページ\)](#)
- [スイッチでの Bluetooth 設定の確認 \(139 ページ\)](#)
- [外部 Bluetooth ドングルの設定の機能履歴 \(139 ページ\)](#)

外部 USB Bluetooth ドングルの設定の制約事項

- Bluetooth バージョン 4.0 のみがサポートされています。
- 外部 USB Bluetooth ドングルは、IPv4 アドレス範囲内で設定されている Cisco Catalyst 9000 シリーズ スイッチでのみサポートされます。
- スタッキングモードでは、外部 USB Bluetooth ドングルのアクティブなスイッチで有効にする必要があります。
- ステートフルスイッチオーバー (SSO) 後、外部 USB Bluetooth ドングルの新しいアクティブなスイッチインターフェイスで有効にする必要があります。
- 次の構成では、外部 USB Bluetooth ドングルはサポートされません。
 - Quality of Service (QoS)
 - アクセス コントロール リスト (ACL)

外部 USB Bluetooth ドングルについて

接続された外部 USB Bluetooth ドングルは外部デバイスの Bluetooth ホストとして動作し、スイッチ上の管理ポートとして機能します。外部 USB Bluetooth ドングルは、スマートフォン、ラップトップ、タブレットなどの Bluetooth 対応外部デバイスとペアリングできます。

外部 USB Bluetooth ドングルは、スタンドアロンモードまたはスタッキングモードの両方で設定されたスイッチでサポートされます。

サポートされている外部 USB Bluetooth ドングル

次の外部 USB Bluetooth ドングルがサポートされています。

- BTD-400 Bluetooth 4.0 アダプタ (Kinivo 社製)
- Bluetooth 4.0 USB アダプタ (ASUS 社製)
- ミニ Bluetooth ワイヤレス USB 4.0 ドングルアダプタ (Adnet 社製)
- Bluetooth 4.0 USB アダプタ (Insignia 社製)

スイッチでの外部 USB Bluetooth ドングルの設定方法

スイッチで外部 USB Bluetooth ドングルを設定するには、次の手順を実行します。

手順

ステップ 1 外部 USB Bluetooth ドングルをスイッチの USB タイプ A ポートに接続します。

(注) 外部 USB Bluetooth ドングルは、デバイスの電源を入れる前、またはデバイスの動作中に接続できます。

ステップ 2 スイッチでグローバルコンフィギュレーションモードを開始し、外部 USB Bluetooth ドングルがスイッチに接続されていることを確認します。

```
Device> enable
Device# show platform hardware bluetooth
Controller:0:1a:7d:da:71:13
Type:Primary
Bus:USB
State:DOWN
Name:HCI Version:
```

ステップ 3 インターフェイスコンフィギュレーションモードで **enable** コマンドを使用して Bluetooth インターフェイスを有効にします。

```
Device# configure terminal
Device(config)# interface bluetooth 0/4
Device(config-if)# enable
```

ステップ 4 **no shutdown** コマンドを入力し、デバイスの再起動後に Bluetooth インターフェイスを自動的に再起動します。

```
Device(config-if)# no shutdown
```

ステップ 5 **bluetooth pin pin** コマンドを使用してペアリングピンを設定します。

```
Device(config-if)# bluetooth pin 1111
```

または

```
Device(config-if)# exit
Device(config)# bluetooth pin 1111
```

(注) **bluetooth pin** コマンドはグローバル コンフィギュレーション モードで使用することをお勧めします。

ステップ 6 外部デバイスの Bluetooth 設定をオンにします。外部デバイスで、ホスト名に基づいて Bluetooth 対応スイッチを選択します。

ステップ 7 外部デバイスがインターネットに接続できるようにするには、外部デバイスのネットワーク設定を有効にします。

スイッチでの Bluetooth 設定の確認

Bluetooth 設定をモニタリングするには、特権 EXEC モードで次のコマンドを使用します。

表 21: デバイスでの Bluetooth 設定をモニタするコマンド

コマンド	目的
show ip interface bluetooth 0/4	Bluetooth インターフェイスのユーザビリティステータスを表示します。
show platform hardware bluetooth	Bluetooth インターフェイスに関する情報を表示します。
show running include pin	現在の Bluetooth ピンを表示します。

外部 Bluetooth ドングルの設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.12.1	外部 Bluetooth ドングルの設定	外部 USB Bluetooth ドングルは外部デバイスの Bluetooth ホストとして動作し、スイッチの管理ポートとして機能します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 13 章

M2 SATA モジュール

- [Cisco Catalyst 9400 シリーズ スーパーバイザの M2 SATA モジュール \(141 ページ\)](#)
- [M2 SATA のファイルシステムとストレージ \(141 ページ\)](#)
- [M2 SATA の制限事項 \(142 ページ\)](#)
- [セルフモニタリング、分析、およびレポーティングテクノロジー システム \(S.M.A.R.T.\) ヘルス モニタリング \(142 ページ\)](#)
- [M2 SATA のファイルシステムへのアクセス \(143 ページ\)](#)
- [M2 SATA フラッシュ ディスクのフォーマット \(143 ページ\)](#)
- [SATA モジュールでの操作 \(143 ページ\)](#)
- [M2 SATA モジュールの機能履歴と情報 \(145 ページ\)](#)

Cisco Catalyst 9400 シリーズ スーパーバイザの M2 SATA モジュール

Cisco Catalyst 9400 は、パケットの収集と分析、テスト、モニタリングなどのアプリケーションをホストできる次世代モジュラスイッチです。これらのアプリケーションに必要なストレージをサポートするため、Cisco Catalyst 9400 シリーズ スーパーバイザには 22 X 88 mm の M2 SATA フラッシュカードをホストする M2 コネクタが備わっています。SATA 設定の範囲は、240 GB、480 ~960 GB です。

M2 SATA のファイル システムとストレージ

SATA のデフォルトのファイルシステム形式はEXT4です。ただし、SATAはすべての拡張ファイルシステム (EXT2、EXT3、EXT4) をサポートしています。

SATA デバイスには次の特性があります。

- M2 SATA パーティションに格納されているファイルは、他のデバイスに格納されているファイルとの互換性があります。

- M2 SATA と、USB、eUSB、フラッシュ、その他の IOS-XE ファイル システムまたはストレージなどの別のタイプのデバイス間でファイルをコピーまたは格納できます。
- SATA デバイスの読み取り、書き込み、削除、およびフォーマットもできます。

。

M2 SATA の制限事項

- 非EXT ベースのファイルシステムは、M2 SATA ではサポートされません。
- スーパーバイザの電源を切らずに M2 SATA デバイスを取り外すことはできません。
- M2 SATA を使用してROMMON からイメージを起動できません。
- M2 SATA ドライブのファームウェアはアップグレードできません。
- M2 SATA を使用してイメージの緊急インストールを実行することはできません。

セルフモニタリング、分析、およびレポーティングテクノロジ システム (S.M.A.R.T.) ヘルス モニタリング

Cisco Catalyst IOS XE リリース 16.9.1 では、CLI を使用してデバイスの正常性をモニタリングできます。SATA デバイスの内部ホットスポット、フラッシュの消耗、およびハードウェア障害をモニタリングし、SATA 障害に関してユーザに警告できます。これらのユーザはデータをバックアップし、新しい SATA デバイスを取得できます。

SATA がスーパーバイザに挿入されると、Linux デーモンの `smartd` が起動します。デフォルトでは、ポーリング間隔はオフラインテストの場合は2日、短期テストの場合は6日、長期テストの場合は14日に設定されます。警告とエラーメッセージは `/crashinfo/tracelogs/smart_errors.log` に保存され、IOSd コンソールにも送信されます。

スイッチが SATA デバイスを検出すると、S.M.A.R.T. 機能と `smartd` デーモンはデフォルトで有効になります。



- (注) 挿入後に SATA が検出されない場合は、デバイス上の既存のファイルシステムを確認します。EXT ベースでない場合、SATA は検出されません。その場合は、ファイルシステムを EXT に変更し、SATA を再挿入します。

次の CLI は `smartd` デーモンからのログを示しています。

```
Switch# more crashinfo:tracelogs/smart_errors.log
%IOSXEBOOT-4-SMART_LOG: (local/local): Mon Jan 4 00:13:10 Universal 2016
INFO: Starting SMART daemon
```

次の CLI を使用してデバイスの全体的な状態をモニタできます。


```
Switch# more flash:smart_overall_health.log
smartctl 6.4 2015-06-04 r4109 [x86_64-linux-4.4.131] (local build)
Copyright (C) 2002-15, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
```

M2 SATA のファイル システムへのアクセス

マウントされたファイルシステムには SATA フラッシュ カードから `disk0:` でアクセスします。使用可能な各ファイルシステムの詳細を表示するには、`show file systems` コマンドを使用します。

`bootflash:` または `usbflash0:` に対するファイルのコピーがサポートされています。

M2 SATA フラッシュ ディスクのフォーマット

新しいフラッシュ ディスクをフォーマットするには、`format disk0:` コマンドを使用します。

`format` コマンドはデバイス上のすべてのファイルを再帰的に削除します。このコマンドは、実行中に何らかのファイルが開いている場合は失敗します。

```
Switch#format disk0: ? <cr> <cr>
      ext2      ext2 filesystem type
      ext3      ext3 filesystem type
      ext4      ext4 filesystem type
      secure    Securely format the file system
<cr> <cr>
```

```
Switch# format disk0:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "disk0:". Continue? [confirm] Format of disk0:
complete
```

SATA モジュールでの操作

次に、SATA で実行できるいくつかの操作を示します。

コマンド	説明
<code>dir filesystem</code>	指定されたファイル システムのディレクトリを表示します。
<code>copy source-file destination-url</code>	指定したコピー元から指定したコピー先にファイルをコピーします。
<code>delete</code>	指定したファイルを削除します。

コマンド	説明
format	ディスク上のファイルシステムをフォーマットします。
show disk0:	disk0: の内容と詳細を表示します。
show file information <i>file-url</i>	特定のファイルに関する情報を表示します。
show file systems	デバイスで使用可能なファイルシステムを表示します。
show inventory raw	スイッチ上の既存のモジュールの詳細を表示します。

次に操作の出力例を示します。

```
Switch# dir disk0:
Directory of disk0:/
 11 drwx          16384  May 11 2018 16:06:14 +00:00  lost+found
10747905 drwx          4096  May 25 2018 13:03:43 +00:00  test
236154740736 bytes total (224072925184 bytes free)
```

特定のシャーシの RP のステータスを表示します。

```
Switch# dir disk0-1-1:
Directory of disk0-1-1:/
 11 drwx          16384  Feb 1 2018 12:43:40 -08:00  lost+found
944994516992 bytes total (896892141568 bytes free)
```

ファイルを disk0: から USB にコピーします。

```
Switch# copy disk0:test.txt usbflash0:
Destination filename [test.txt]?
Copy in progress...C
17866 bytes copied in 0.096 secs (186104 bytes/sec)
```

```
Switch# dir usbflash0:
Directory of usbflash0:/
 12 -rw-          33554432  Jul 28 2017 10:12:58 +00:00  nvram_config
 11 drwx          16384  Jul 28 2017 10:09:46 +00:00  lost+found
 13 -rw-          17866  Aug 11 2017 09:52:16 +00:00  test.txt
189628416 bytes total (145387520 bytes free)
```

disk0: から test.txt ファイルを削除します。

```
Switch# delete disk0:test.txt
Delete filename [test.txt]?
Delete disk0:/test.txt? [confirm]

Switch# dir disk0:
Directory of disk0:/
No files in directory
118148280320 bytes total (112084135936 bytes free)
```

USB から disk0: に test.txt ファイルをコピーします。

```
Switch# copy usbflash0:test.txt disk0:
Destination filename [test.txt]?
Copy in progress...C
17866 bytes copied in 0.058 secs (308034 bytes/sec)
```

```
Switch# dir disk0:
Directory of disk0:/
 11 -rw-          17866 Aug 11 2017 09:53:03 +00:00 test.txt
118148280320 bytes total (112084115456 bytes free)
```

ディスクをフォーマットします。

ext4 ファイルシステムをフォーマットするには、次のコマンドを使用します。

```
Switch#format disk0: ext4
```

show コマンド

```
Switch# show disk0:
-#- --length-- -----date/time----- path
 2          17866 Aug 11 2017 09:54:06.0000000000 +00:00 test.txt
112084115456 bytes available (62513152 bytes used)
```

```
Switch# show file information disk0: test.txt
disk0:test.txt:
  type is image (elf64) []
  file size is 448 bytes, run size is 448 bytes
Foreign image, entry point 0x400610
```

```
Switch# show file systems
```

File Systems:

	Size (b)	Free (b)	Type	Flags	Prefixes
-	-	-	-	-	-
* 11250098176	9694093312		disk	rw	bootflash: flash:
1651314688	1232220160		disk	rw	crashinfo:
118148280320	112084115456		disk	rw	disk0:
189628416	145387520		disk	rw	usbflash0:
7763918848	7696850944		disk	ro	webui:
-	-	-	opaque	rw	null:
-	-	-	opaque	ro	tar:
-	-	-	network	rw	tftp:
33554432	33532852		nvrnm	rw	nvrnm:
-	-	-	opaque	wo	syslog:
-	-	-	network	rw	rcp:
-	-	-	network	rw	http:
-	-	-	network	rw	ftp:
-	-	-	network	rw	scp:
-	-	-	network	rw	https:
-	-	-	opaque	ro	cns:

```
Switch#show disk0: fileysys
Filesystem: disk0
Filesystem Path: /vol/disk0
Filesystem Type: ext4
Mounted: Read/Write
```

```
Switch#show inventory raw
NAME: "Slot 5 SATA Container", DESCR: "SATA Container"
PID:          , VID:          , SN:
```

M2 SATA モジュールの機能履歴と情報

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。

機能名	リリース	機能情報
M2 SATA モジュール	Cisco IOS XE Everest 16.6.1	M2 SATA カードはデバイスのストレージニーズに対応します。これは小型フォームファクタのカード/コネクタです。詳細については使用しているデバイスのハードウェアインストールガイドを参照してください。
M2 SATA モジュール	Cisco IOS XE Fuji 16.9.1	ストレージニーズをホストするアプリケーションのサポートが導入されました。