



Cisco IOS リリース 15.2(7)Ex (Catalyst 1000 スイッチ) システム 管理コンフィギュレーションガイド

初版：2019 年 12 月 25 日

最終更新：2020 年 9 月 15 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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

システムの管理 1

デバイスの管理に関する情報	1
システム日時の管理	1
システムクロック	1
Real Time Clock (リアルタイムクロック)	2
ネットワークタイムプロトコル	2
NTPストラタム	4
NTPアソシエーション	4
NTPセキュリティ	4
NTPの実装	4
NTPバージョン	4 5
DNS	5
DNSのデフォルト設定値	6
ログインバナー	6
バナーのデフォルト設定	6
MACアドレステーブル	6
MACアドレステーブルの作成	7
MACアドレスおよびVLAN	7
MACアドレステーブルのデフォルト設定	7
ARPテーブルの管理	8
デバイスの管理方法	8
手動による日付と時刻の設定	8
システムクロックの設定	8
タイムゾーンの設定	9

夏時間の設定	10
システム名の設定	14
DNS の設定	15
Message-of-the-Day ログイン バナーの設定	16
ログイン バナーの設定	18
MAC アドレス テーブルの管理	19
アドレス エージング タイムの変更	19
MAC アドレス変更通知トラップの設定	20
MAC アドレス移動通知トラップの設定	23
MAC しきい値通知トラップの設定	25
スタティック アドレス エントリの追加および削除	27
ユニキャスト MAC アドレス フィルタリングの設定	28
デバイスのモニタリングおよび保守の管理	29
管理の設定例	31
例：システム クロックの設定	31
例：サマー タイムの設定	31
例：MOTD バナーの設定	31
例：ログイン バナーの設定	32
例：MAC アドレス変更通知トラップの設定	32
例：MAC しきい値通知トラップの設定	32
例：MAC アドレス テーブルへのスタティック アドレスの追加	33
例：ユニキャスト MAC アドレス フィルタリングの設定	33
デバイス管理の機能履歴と情報	33

第 2 章**のセットアップ設定の実行 35**

デバイスセットアップ設定の実行に関する情報	35
ブート プロセス	35
デバイス情報の割り当て	36
デフォルトのスイッチ情報	37
DHCP ベースの自動設定の概要	37
DHCP クライアントの要求プロセス	38

DHCP ベースの自動設定およびイメージアップデート	39
DHCP ベースの自動設定の制約事項	39
DHCP 自動設定	40
DHCP 自動イメージアップデート	40
DHCP サーバ設定時の注意事項	40
TFTP サーバの目的	41
DNS サーバの目的	42
コンフィギュレーション ファイルの入手方法	42
環境変数の制御方法	44
一般的な環境変数	45
ソフトウェア イメージのリロードのスケジューリング	47
デバイスセットアップ設定の実行方法	47
DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定	47
DHCP 自動イメージアップデート（コンフィギュレーション ファイルおよびイメージ） の設定	49
DHCP サーバからファイルをダウンロードするクライアントの設定	53
IP ルーティングがディセーブルの場合のルーティング支援機能	54
デフォルト ゲートウェイ	54
複数の SVI への IP 情報の手動割り当て	55
NVRAM バッファ サイズの設定	57
デバイスのスタートアップ コンフィギュレーションの変更	57
システム コンフィギュレーションを読み書きするためのファイル名の指定	57
スイッチの手動による起動	58
ソフトウェア イメージのリロードのスケジュール設定	60
デバイスのセットアップを実行する場合の設定例	61
例：デバイスを DHCP サーバとして設定	61
例：DHCP 自動イメージアップデートの設定	62
例：DHCP サーバから設定をダウンロードするためのデバイスの設定	62
例：NVRAM バッファ サイズの設定	62
デバイスセットアップ設定の実行に関する機能履歴と情報	63

第 3 章

sFlow の設定 65

- sFlow について 65
 - sFlow エージェント 65
- sFlow の前提条件 66
- 注意事項と制約事項 66
- sFlow のデフォルト設定 66
- sFlow の設定方法 67
 - sFlow エージェントの設定 67
 - sFlow コレクタの設定 68
 - フローサンプリングの設定 69
 - カウンタサンプリングの設定 70
- sFlow 設定の確認 71
- sFlow 統計情報のモニタリングとクリア 72
- sFlow の設定例 72
- sFlow の設定に関する機能情報 73

第 4 章

システム メッセージ ログの設定 75

- システム メッセージ ログの設定に関する制約事項 75
- システム メッセージ ログの設定に関する情報 75
 - システム メッセージ ロギング 75
 - システム ログ メッセージのフォーマット 76
 - デフォルトのシステム メッセージ ロギングの設定 77
 - Syslog トラップ メッセージのイネーブルング 78
- システム メッセージ ログの設定方法 78
 - メッセージ表示宛先デバイスの設定 78
 - ログ メッセージの同期化 80
 - メッセージ ロギングのディセーブル化 82
 - ログ メッセージのタイム スタンプのイネーブル化およびディセーブル化 83
 - ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化 84
 - メッセージ重大度の定義 84

履歴テーブルおよび SNMP に送信される syslog メッセージの制限	85
UNIX Syslog デーモンへのメッセージのロギング	86
システム メッセージ ログのモニタリングおよびメンテナンス	87
コンフィギュレーション アーカイブ ログのモニタリング	87
システム メッセージ ログの設定例	88
例：スイッチ システム メッセージ	88
例：サービスタイムスタンプログの表示	88
システム メッセージ ログに関する追加情報	88
システム メッセージ ログの機能履歴と情報	89

第 5 章
オンライン診断の設定 91

オンライン診断の設定に関する情報	91
オンライン診断	91
オンライン診断の設定方法	92
オンライン診断テストの開始	92
オンライン診断の設定	92
オンライン診断のスケジューリング	93
ヘルス モニタリング診断の設定	94
オンライン診断のモニタリングおよびメンテナンス	97
オンライン診断テストとテスト結果の表示	97
オンライン診断テストの設定例	97
オンライン診断テストの開始	97
例：ヘルス モニタリング テストの設定	98
オンライン診断のスケジューリング	98
オンライン診断の表示：例	100
オンライン診断の機能履歴と情報	102

第 6 章
Dying Gasp の設定 103

Dying Gasp の設定に関する制約事項	103
Dying Gasp の設定について	103
Dying Gasp の概要	103

Dying Gasp の設定方法	104
Dying Gasp の設定	104
Dying Gasp の設定例	105
例 : Dying Gasp の設定	105
Dying Gasp に関するその他の参考資料	106
Dying Gasp の機能履歴	106

第 7 章

Cisco IOS ファイル システム、コンフィギュレーション ファイル、およびソフトウェア イメージ
の操作 107

フラッシュ ファイル システムの操作	107
フラッシュ ファイル システムについて	107
使用可能なファイル システムの表示	107
デフォルト ファイル システムの設定	109
ファイル システムのファイルに関する情報の表示	109
ディレクトリの変更および作業ディレクトリの表示	110
ディレクトリの作成	111
ディレクトリの削除	111
ファイルのコピー	112
ファイルの削除	113
ファイルの作成、表示、および抽出	113
設定ファイルの取り扱い	116
コンフィギュレーション ファイルに関する情報	116
コンフィギュレーション ファイルの作成および使用上の注意事項	116
コンフィギュレーション ファイルのタイプおよび場所	117
テキスト エディタによるコンフィギュレーション ファイルの作成	117
TFTP によるコンフィギュレーション ファイルのコピー	118
TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	118
TFTP によるコンフィギュレーション ファイルのダウンロード	119
TFTP によるコンフィギュレーション ファイルのアップロード	120
デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー	121

FTP ユーザ名およびパスワードの概要	121
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	122
FTP によるコンフィギュレーション ファイルのダウンロード	122
FTP によるコンフィギュレーション ファイルのアップロード	123
RCP によるコンフィギュレーション ファイルのコピー	125
RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	125
RCP によるコンフィギュレーション ファイルのダウンロード	126
RCP によるコンフィギュレーション ファイルのアップロード	127
設定情報の消去	128
スタートアップ コンフィギュレーション ファイルの消去	129
格納されたコンフィギュレーション ファイルの削除	129
コンフィギュレーションの交換およびロールバック	129
コンフィギュレーションの置換とロールバックに関する情報	129
コンフィギュレーション アーカイブ	129
コンフィギュレーションの置換	130
設定のロールバック	130
設定時の注意事項	131
コンフィギュレーション アーカイブの設定	131
コンフィギュレーション置換またはロールバック動作の実行	133
ソフトウェア イメージの操作	134
ソフトウェア イメージの操作に関する情報	134
スイッチ上のイメージの場所	135
サーバまたは Cisco.com 上のイメージのファイル形式	135
ソフトウェアイメージのアップグレード履歴の表示	136
TFTP によるイメージ ファイルのコピー	136
TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備	137
TFTP によるイメージ ファイルのダウンロード	138
TFTP によるイメージ ファイルのアップロード	139
FTP によるイメージ ファイルのコピー	140

FTP によるイメージファイルのダウンロードまたはアップロードの準備	141
FTP によるイメージファイルのダウンロード	142
FTP によるイメージファイルのアップロード	144
RCP によるイメージファイルのコピー	145
RCP によるイメージファイルのダウンロードまたはアップロードの準備	146
RCP によるイメージファイルのダウンロード	147
RCP によるイメージファイルのアップロード	149

第 8 章

ソフトウェア設定のトラブルシューティング 151

ソフトウェア設定のトラブルシューティングに関する情報	151
スイッチのソフトウェア障害	151
デバイスのパスワードを紛失したか忘れた場合	151
Power over Ethernet (PoE) ポート	152
電力消失によるポートの障害	152
不正リンク アップによるポート障害	153
ping	153
レイヤ 2 traceroute	153
レイヤ 2 の traceroute のガイドライン	154
IP トレースルート	155
Time Domain Reflector ガイドライン	156
debug コマンド	157
スイッチのオンボード障害ロギング	157
CPU 使用率が高い場合に起こりうる症状	158
ソフトウェア設定のトラブルシューティング方法	158
ソフトウェア障害からの回復	158
パスワードを忘れた場合の回復	160
パスワード回復がイネーブルになっている場合の手順	161
パスワード回復がディセーブルになっている場合の手順	163
コマンドスイッチで障害が発生した場合の回復	165
故障したコマンドスイッチをクラスタ メンバーと交換する場合	166
故障したコマンドスイッチを他のスイッチと交換する場合	168

自動ネゴシエーションの不一致の防止	169
SFP モジュールのセキュリティと識別に関するトラブルシューティング	170
SFP モジュール ステータスのモニタリング	171
ping の実行	171
温度のモニタリング	171
物理パスのモニタリング	171
IP traceroute の実行	172
TDR の実行および結果の表示	172
デバッグおよびエラー メッセージ出力のリダイレクト	172
show platform forward コマンドの使用	173
OBFL の設定	173
ソフトウェア設定のトラブルシューティングの確認	174
OBFL 情報の表示	174
例：高い CPU 使用率に関する問題と原因の確認	175
ソフトウェア設定のトラブルシューティングのシナリオ	177
Power over Ethernet (PoE) に関するトラブルシューティングのシナリオ	177
ソフトウェアのトラブルシューティングの設定例	182
例：IP ホストの ping	182
例：IP ホストに対する traceroute の実行	183
例：すべてのシステム診断をイネーブるにする	184
ソフトウェア設定のトラブルシューティングに関する追加情報	184
ソフトウェア設定のトラブルシューティングの機能履歴と情報	185



第 1 章

システムの管理

- デバイスの管理に関する情報 (1 ページ)
- デバイスの管理方法 (8 ページ)
- デバイスのモニタリングおよび保守の管理 (29 ページ)
- 管理の設定例 (31 ページ)
- デバイス管理の機能履歴と情報 (33 ページ)

デバイスの管理に関する情報

システム日時の管理

デバイスのシステム日時は、自動設定方式 (RTC および NTP) または手動設定方式を使用して管理できます。



(注) ここで使用するコマンドの構文および使用方法の詳細については、Cisco.com で、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

システムクロック

時刻サービスの基本となるのはシステムクロックです。このクロックはシステムがスタートアップした瞬間から稼働し、日時を常時トラッキングします。

システムクロックは、次のソースにより設定できます。

- RTC
- NTP
- 手動設定

システムクロックは、次のサービスに時刻を提供します。

- **user show** コマンド
- ログおよびデバッグ メッセージ

システムクロックは、グリニッジ標準時 (GMT) と呼ばれる協定世界時 (UTC) に基づいて内部的に時刻を追跡します。ローカルのタイムゾーンおよび夏時間に関する情報を設定することにより、時刻がローカルのタイムゾーンに応じて正確に表示されるようになります。

システムクロックは、時刻に信頼性があるかどうか (つまり、信頼できると見なされるタイムソースによって時刻が設定されているか) を常時トラッキングします。信頼性のない場合は、時刻は表示目的でのみ使用され、再配信されません。

Real Time Clock (リアルタイムクロック)

リアルタイムクロック (RTC) は、スイッチの現在時刻を追跡します。スイッチはクロッキングパラメータを再設定するまでは GMT 時間に設定された RTC を装備しています。

RTC の利点は次のとおりです。

- RTC はバッテリー電源式です。
- システム時刻は、停電時およびシステム リブート時に保持されます。

RTC と NTP クロックはスイッチに統合されます。NTP を有効にすると、RTC 時間が NTP クロックと定期的に同期化され、精度が保たれます。

ネットワーク タイム プロトコル

NTP は、ネットワーク上のデバイス間の時刻の同期化を目的に設計されています。NTP はユーザ データグラム プロトコル (UDP) で稼働し、UDP は IP 上で稼働します。NTP は RFC 1305 で規定されています。

NTP ネットワークは通常、タイム サーバに接続されたラジオクロックやアトミッククロックなど、正規の時刻源から時刻を取得します。NTP は、ネットワークにこの時刻を分配します。NTP はきわめて効率的で、1 分間に 1 パケットを使用するだけで、2 台のデバイスを 1 ミリ秒以内に同期化できます。

NTP では、信頼できるタイムソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイムサーバには、ラジオクロックまたは原子時計が直接接続されており、ストラタム 2 タイムサーバは、NTP を使用してストラタム 1 タイムサーバから時刻を取得します (以降のストラタムも同様です)。NTP が稼働するデバイスは、タイムソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

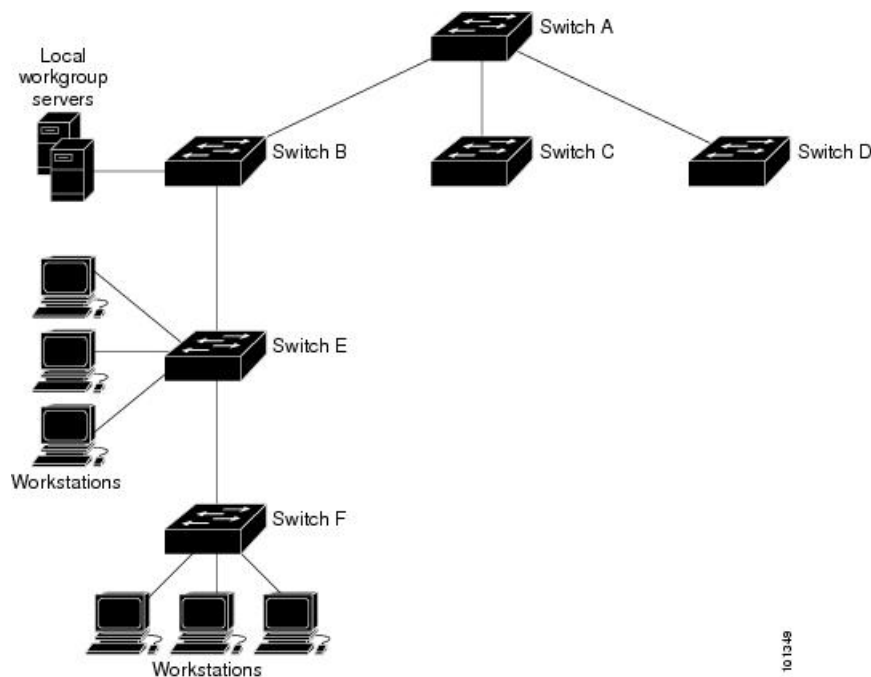
NTPが稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスのIPアドレスが与えられます。アソシエーションのペアとなるデバイス間でNTPメッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN環境では、代わりにIPブロードキャストメッセージを使用するようにNTPを設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方向に限られます。

デバイス上で維持される時刻は、重要なリソースです。NTPのセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されないようにしてください。その方法として、アクセスリストベースの制約方式と暗号化認証方式があります。

シスコによるNTPの実装では、ストラタム1サービスをサポートしていないため、ラジオクロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IPインターネット上のパブリックNTPサーバから取得することを推奨します。

次の図にNTPデバイスを使用した一般的なネットワークの例を示します。AはプライマリNTP、デバイスB、C、DがNTPサーバモードに設定されている（デバイスAとの間にサーバアソシエーションが設定されている）場合のNTPマスターです。デバイスEは、アップストリームデバイス（デバイスB）とダウンストリームデバイス（デバイスF）のNTPピアとして設定されます。

図 1: 一般的な NTP ネットワークの構成



ネットワークがインターネットから切り離されている場合、シスコのNTPによって、実際には、他の方法で時刻を学習しているにもかかわらず、デバイスがNTPを使用して同期化しているように動作を設定できます。他のデバイスは、NTPによりこのデバイスと同期化されます。

複数のタイムソースがある場合は、NTP は常に、より信頼性があると見なされます。NTP の時刻は、他の方法による時刻に優先します。

自社のホストシステムに NTP ソフトウェアを組み込んでいるメーカーが数社あり、UNIX システム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホストシステムも時間が同期化されます。

NTP ストラタム

NTP では、信頼できるタイムソースから各マシンが何 NTP ホップ隔たっているかを表すために、ストラタムという概念が使用されます。ストラタム 1 タイムサーバには、ラジオクロックまたは原子時計が直接接続されており、ストラタム 2 タイムサーバは、NTP を使用してストラタム 1 タイムサーバから時刻を取得します（以降のストラタムも同様です）。NTP が稼働するデバイスは、タイムソースとして、NTP を使用して通信するストラタム番号が最小のデバイスを自動的に選択します。この方法によって、NTP 時刻配信の自動編成型ツリーが効率的に構築されます。

NTP では、同期化されていないデバイスと同期化しないことによって、時刻が正確でないデバイスとの同期化を防ぎます。また、NTP では、複数のデバイスから報告される時刻を比較して、ストラタムの番号が小さくても、時刻が他のデバイスと大幅に異なるデバイスとは同期化しません。

NTP アソシエーション

NTP が稼働するデバイス間の通信（アソシエーション）は、通常静的に設定されます。各デバイスには、アソシエーションを作成すべきすべてのデバイスの IP アドレスが与えられます。アソシエーションのペアとなるデバイス間で NTP メッセージを交換することによって、正確な時刻の維持が可能になります。ただし、LAN 環境では、代わりに IP ブロードキャストメッセージを使用するように NTP を設定できます。各デバイスを、単にブロードキャストメッセージを送受信するように設定すればよいので、この代替手段によって設定の複雑さが緩和されます。ただし、情報の流れは一方方向に限られます。

NTP セキュリティ

デバイス上で維持される時刻は、重要なリソースです。NTP のセキュリティ機能を使用して、不正確な時刻が誤って、あるいは意図的に設定されることがないようにしてください。その方法として、アクセスリストベースの制約方式と暗号化認証方式があります。

NTP の実装

NTP の実装では、ストラタム 1 サービスがサポートされないため、ラジオクロックまたは原子時計に接続できません。ネットワークの時刻サービスは、IP インターネット上のパブリック NTP サーバから取得することを推奨します。

ネットワークがインターネットから切り離されている場合、NTP によって、実際には、他の方法で時刻を取得している場合でも、NTP を使用した同期化と同様にデバイスの動作を設定できます。他のデバイスは、NTP によりこのデバイスと同期化されます。

複数のタイムソースがある場合は、NTPは常に、より信頼性があると見なされます。NTPの時刻は、他の方法による時刻に優先します。

自社のホストシステムにNTPソフトウェアを組み込んでいるメーカーが数社あり、UNIXシステム用のバージョンやその派生ソフトウェアも一般に入手できます。このソフトウェアによって、ホストシステムも時間が同期化されます。

NTP バージョン 4

デバイスには、NTPバージョン4が実装されています。NTPv4はNTPバージョン3の拡張版です。NTPv4はIPv4とIPv6の両方をサポートし、NTPv3との下位互換性があります。

NTPv4は次の互換性を提供します。

- IPv6のサポート。
- NTPv3よりさらに向上したセキュリティ。NTPv4プロトコルは、公開キー暗号化および標準X509認証に基づくセキュリティフレームワークを提供します。
- ネットワークに対する時間分布ヒエラルキーの自動計算。特定のマルチキャストグループを使用して、NTPv4は、最も低い帯域幅コストで最高の時間精度を達成するサーバのヒエラルキーを自動的に設定します。この機能では、サイトローカルIPv6マルチキャストアドレスが活用されます。

NTPv4の設定の詳細については、『Cisco IOS IPv6 Configuration Guide, Release 12.4T』の「Implementing NTPv4 in IPv6」の章を参照してください。

DNS

DNSプロトコルは、ドメインネームシステム（DNS）を制御します。DNSとは分散型データベースであり、ホスト名をIPアドレスにマッピングできます。デバイスにDNSを設定すると、**ping**、**telnet**、**connect**などのすべてのIPコマンドを使用する場合や、関連するTelnetサポート操作時に、IPアドレスの代わりにホスト名を使用できます。

IPによって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IPで**com**というドメイン名に分類される商業組織なので、ドメイン名は**cisco.com**となります。このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは、**ftp.cisco.com**で表されます。

IPではドメイン名をトラッキングするために、ドメインネームサーバという概念が定義されています。ドメインネームサーバの役割は、名前からIPアドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名をIPアドレスにマッピングするには、まず、ホスト名を明示し、ネットワーク上に存在するネームサーバを指定し、DNSをイネーブルにします。

DNS のデフォルト設定値

表 1: DNS のデフォルト設定値

機能	デフォルト設定
DNS イネーブル ステート	イネーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

ログインバナー

Message-of-The-Day (MoTD) バナーおよびログイン バナーを作成できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログインバナーも接続されたすべての端末に表示されます。表示されるのは、MoTD バナーの後で、ログインプロンプトが表示される前です。



(注) ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*』を参照してください。

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MAC アドレス テーブル

MAC アドレステーブルには、デバイスがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- **ダイナミックアドレス**：デバイスが取得し、使用されなくなった時点で期限切れとなる送信元の MAC アドレス
- **スタティックアドレス**：手動で入力され、期限切れにならず、デバイスのリセット時にも消去されないユニキャストアドレス

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。



(注) ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

MAC アドレス テーブルの作成

すべてのポートでサポートされる複数の MAC アドレスを使用して、他のネットワークデバイスにデバイス上のすべてのポートを接続できます。デバイスは、各ポートで受信するパケットの送信元アドレスを取得し、アドレステーブルにアドレスとそれに関連付けられたポート番号を追加することによって、動的なアドレス指定を行います。ネットワークでデバイスの追加または削除が行われると、デバイスによってアドレステーブルが更新され、新しいダイナミックアドレスが追加され、使用されていないアドレスは期限切れになります。

エージング インターバルは、グローバルに設定されています。ただし、デバイスは VLAN ごとにアドレステーブルを維持し、STP によって VLAN 単位で有効期間を短縮できます。

デバイスは、受信したパケットの宛先アドレスに基づいて、任意の組み合わせのポート間でパケットを送信します。デバイスは、MAC アドレステーブルを使用することによって、宛先アドレスに関連付けられたポートに限定してパケットを転送します。宛先アドレスがパケットを送信したポート上にある場合は、パケットはフィルタリング処理され、転送されません。デバイスは、常にストアアンドフォワード方式を使用します。このため、完全なパケットをいったん保存してエラーがないか検査してから転送します。

MAC アドレスおよび VLAN

すべてのアドレスは VLAN と関連付けられます。1つのアドレスを複数の VLAN に対応付け、それぞれで異なる宛先を設定できます。たとえば、ユニキャストアドレスを VLAN 1 のポート 1 および VLAN 5 のポート 9、10、1 に転送するといったことが可能です。

VLAN ごとに、独自の論理アドレス テーブルが維持されます。ある VLAN で認識されているアドレスが別の VLAN で認識されるには、別の VLAN 内のポートによって学習されるか、または別の VLAN 内のポートにスタティックに対応付けられる必要があります。

MAC アドレス テーブルのデフォルト設定

次の表に、MAC アドレス テーブルのデフォルト設定を示します。

表 2: MAC アドレスのデフォルト設定

機能	デフォルト設定
エージング タイム	300 秒
ダイナミック アドレス	自動学習
スタティック アドレス	未設定

ARP テーブルの管理

デバイスと通信するには（イーサネット上のデバイスなど）、ソフトウェアは最初にそのデバイスの 48 ビット MAC アドレスまたはローカルデータリンク アドレスを学習する必要があります。IP アドレスからローカルデータリンク アドレスを学習するプロセスを、アドレス解決といいます。

アドレス解決プロトコル（ARP）は、ホスト IP アドレスを、該当するメディアまたは MAC アドレスおよび VLAN ID に対応付けます。IP アドレスを使用して、ARP は対応する MAC アドレスを見つけます。MAC アドレスが見つかると、IP と MAC アドレスとの対応を ARP キャッシュに格納し、すばやく検索できるようにします。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。イーサネット以外の IEEE 802 ネットワークにおける IP データグラムのカプセル化および ARP 要求/応答については、サブネットワークアクセスプロトコル（SNAP）で規定されています。IP インターフェイスでは、標準的なイーサネット形式の ARP カプセル化（**arpa** キーワードで表される）がデフォルトでイーサネットに設定されています。

手動でテーブルに追加された ARP エントリは期限切れにならないので、手動で削除する必要があります。

CLI（コマンドライン インターフェイス）の手順については、*Cisco.com* で Cisco IOS Release 12.4 のマニュアルを参照してください。

デバイスの管理方法

ここでは、デバイスの管理に役立つタスクについて説明します。

手動による日付と時刻の設定

正確なシステム時刻は再開と再起動により保持されますが、日付と時刻はシステムが再開してから手動で設定できます。

手動設定は必要な場合にのみ使用することを推奨します。デバイスが同期できる外部ソースがある場合は、システムクロックを手動で設定する必要はありません。

システムクロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステムクロックを設定する必要はありません。

システムクロックを設定するには、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"> • 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	次のいずれかを使用します。 <ul style="list-style-type: none"> • clock set hh:mm:ss day month year • clock set hh:mm:ss month day year 例 : Device# clock set 13:32:00 23 March 2013	次のいずれかの書式を使ってシステムクロックを手動で設定します。 <ul style="list-style-type: none"> • <i>hh:mm:ss</i> : 時間 (24 時間形式)、分、秒を指定します。指定された時刻は、設定されたタイムゾーンに基づきます。 • <i>day</i> : 月の日で日付を指定します。 • <i>month</i> : 月を名前で指定します。 • <i>year</i> : 年を指定します (略式表記で指定しないでください)。

タイムゾーンの設定

タイムゾーンを手動で設定するには、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。
ステップ 3	clock timezone zone hours-offset [minutes-offset] 例 :	時間帯を設定します。 内部時間は、協定世界時 (UTC) で維持されるため、このコマンドは表示専用

	コマンドまたはアクション	目的
	Device(config)# clock timezone AST -3 30	で、時刻を手動で設定するときだけに使用されます。 <ul style="list-style-type: none"> • <i>zone</i> : 標準時が適用されているときに表示されるタイムゾーンの名前を入力します。デフォルトは UTC です。 • <i>hours-offset</i> : UTCからのオフセット時間数を入力します。 • (任意) <i>minutes-offset</i> : UTCからのオフセット分数を入力します。ローカルタイムゾーンが UTC と 1 時間の差の割合である場合に指定できます。
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	show running-config 例 : Device# show running-config	入力を確認します。
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。

夏時間の設定

毎年特定の日に夏時間が開始および終了する地域に夏時間を設定するには、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	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<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	clock summer-time zone date date month year hh:mm date month year hh:mm [offset] 例： Device(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00	毎年指定された日に開始および終了する夏時間を設定します。
ステップ 4	clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]] 例： Device(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00	<p>毎年指定された日に開始および終了する夏時間を設定します。すべての時刻は、現地のタイムゾーンを基準にしています。開始時間は標準時を基準にしています。</p> <p>終了時間は夏時間を基準にしています。夏時間はデフォルトでディセーブルに設定されています。パラメータなしで clock summer-time zone recurring を指定すると、夏時間のルールは米国のルールにデフォルト設定されます。</p> <p>開始月が終了月より後の場合は、システムでは南半球にいると見なされます。</p> <ul style="list-style-type: none"> zone : 夏時間が有効な場合に表示される時間帯名 (PDT など) を指定します。 (任意) week : 月の週 (1 ~ 4、first、または last) を指定します。 (任意) day : 曜日 (Sunday、Monday など) を指定します。 (任意) month : 月 (January、February など) 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"> • (任意) <i>hh:mm</i> : 時および分単位で時間 (24時間形式) を指定します。 • (任意) <i>offset</i> : 夏時間中に追加する分数を指定します。デフォルトは 60 です。
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 例 : Device# show running-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。
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。

ユーザの居住地の夏時間が定期的なパターンに従わない (次の夏時間のイベントの正確な日時を設定する) 場合は、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	<p>clock summer-time zone date [<i>month date year hh:mm month date year hh:mm [offset]</i>] or clock summer-time zone date [<i>date month year hh:mm date month year hh:mm [offset]</i>]</p>	<p>最初の日付で夏時間開始の日付を、2番目の日付で終了の日付を設定します。</p> <p>夏時間はデフォルトでディセーブルに設定されています。</p> <ul style="list-style-type: none"> • <i>zone</i> には、夏時間が施行されているときに表示されるタイムゾーンの名前（たとえば PDT）を入力します。 • （任意）<i>week</i> には、月の何週目かを指定します（1～5、または last）。 • （任意）<i>day</i> には、曜日を指定します（Sunday、Monday など）。 • （任意）<i>month</i> には、月を指定します（January、February など）。 • （任意）<i>hh:mm</i> には、時刻を時間（24時間形式）と分で指定します。 • （任意）<i>offset</i> には、夏時間の間、追加する分数を指定します。デフォルトは 60 です。
ステップ 4	<p>end</p> <p>例：</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 5	<p>show running-config</p> <p>例：</p> <pre>Device# show running-config</pre>	<p>（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。</p>
ステップ 6	<p>copy running-config startup-config</p> <p>例：</p> <pre>Device# copy running-config startup-config</pre>	<p>（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。</p>

システム名の設定

システム名を手動で設定するには、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。
ステップ 3	hostname name 例： Device(config)# hostname remote-users	システム名を設定します。システム名を設定すると、システム プロンプトとしても使用されます。 デフォルト設定は Switch です。 名前は ARPANET ホスト名のルールに従う必要があります。このルールではホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。名前には 63 文字まで使用できます。
ステップ 4	end 例： remote-users(config)# end remote-users#	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
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。

DNS の設定

デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため、DNS クエリは発生しません。ピリオド (.) なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、**ip domain-name** グローバル コンフィギュレーション コマンドによって設定される値です。ホスト名にピリオド (.) がある場合は、Cisco IOS ソフトウェアは、ホスト名にデフォルトのドメイン名を追加せずに IP アドレスを検索します。

DNS を使用するように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	ip domain-name name 例： Device(config)# ip domain-name Cisco.com	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、デバイスの設定が BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 4	ip name-server server-address1 [server-address2 ... server-address6] 例：	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。

	コマンドまたはアクション	目的
	<pre>Device(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300</pre>	<p>最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリサーバです。デバイスは、プライマリサーバへ DNS クエリを最初に送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。</p>
ステップ 5	<p>ip domain-lookup [nsap source-interface interface]</p> <p>例 :</p> <pre>Device(config)# ip domain-lookup</pre>	<p>(任意) デバイス上で、DNS に基づくホスト名からアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。</p> <p>ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config)# 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>
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(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。</p>

Message-of-the-Day ログインバナーの設定

デバイスにログインしたときに画面に表示される 1 行以上のメッセージバナーを作成できます。

MOTD ログインバナーを設定するには、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	banner motd c message c 例： Device(config)# banner motd # This is a secure site. Only authorized users are allowed. For access, contact technical support. #	MoTD を指定します。 <i>c</i> : ポンド記号 (#) など、目的のデリミタを入力して Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 <i>message</i> : 255 文字までのバナーメッセージを入力します。メッセージ内には区切り文字を使用できません。
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 running-config 例： Device# show running-config	入力を確認します。
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。

ログインバナーの設定

接続されたすべての端末でログインバナーが表示されるように設定できます。バナーが表示されるのは、MoTD バナーの後で、ログインプロンプトが表示される前です。

ログインバナーを設定するには、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	banner login c message c 例： Device(config)# banner login \$ Access for authorized users only. Please enter your username and password. \$	ログイン メッセージを指定します。 <i>c</i> : ポンド記号 (#) など、目的のデリミタを入力して Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 <i>message</i> : 255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
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 running-config 例： Device# show running-config	入力を確認します。
ステップ 6	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# copy running-config startup-config	

MAC アドレス テーブルの管理

アドレス エージング タイムの変更

ダイナミックアドレステーブルのエージングタイムを設定するには、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	mac address-table aging-time [0 10-1000000] [routed-mac vlan vlan-id] 例： Device(config)# mac address-table aging-time 500 vlan 2	ダイナミック エントリが使用または更新された後、MAC アドレス テーブル内に保持される時間を設定します。 指定できる範囲は 10 ~ 1000000 秒です。デフォルトは 300 です。0 を入力して期限切れをディセーブルにすることもできます。スタティック アドレスは、期限切れになることもテーブルから削除されることもありません。 <i>vlan-id</i> : 有効な ID は 1 ~ 4094 です。
ステップ 4	end 例： Device(config)# 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 5	show running-config 例： Device# show running-config	入力を確認します。
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。

MAC アドレス変更通知トラップの設定

NMS ホストに MAC アドレス変更通知トラップを送信するように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。 <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	snmp-server host host-addr community-string notification-type { informs traps } {version {1 2c 3}} { vrf vrf instance name} 例： Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	トラップメッセージの受信側を指定します。 <ul style="list-style-type: none"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : サポートする SNMP バージョンを指定します。informs には

	コマンドまたはアクション	目的
		<p>バージョン 1 (デフォルト) を使用できません。</p> <ul style="list-style-type: none"> • <i>community-string</i> : 通知処理で送信する文字列を指定します。 snmp-server host コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、snmp-server community 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から、snmp-server host コマンドを使用することを推奨します。 • <i>notification-type</i> : mac-notification キーワードを使用します。 • <i>vrf vrf</i> インスタンス名 : このホストの VPN ルーティング/転送インスタンスを指定します。
ステップ 4	snmp-server enable traps mac-notification change 例 : <pre>Device(config)# snmp-server enable traps mac-notification change</pre>	デバイスが MAC アドレス変更通知を NMS に送信できるようにします。
ステップ 5	mac address-table notification change 例 : <pre>Device(config)# mac address-table notification change</pre>	MAC アドレス変更通知機能をイネーブルにします。
ステップ 6	mac address-table notification change [interval value] [history-size value] 例 : <pre>Device(config)# mac address-table notification change interval 123 Device(config)# mac address-table notification change history-size 100</pre>	トラップ インターバル タイムと履歴テーブルのサイズを入力します。 <ul style="list-style-type: none"> • (任意) <i>interval value</i> : NMS に生成されるトラップの各セット間の通知トラップインターバルを秒単位で指定します。指定できる範囲は 0 ~ 2147483647 秒です。デフォルトは 1 秒です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) history-size value : MAC 通知履歴テーブルの最大エントリ数を指定します。指定できる範囲は 0 ~ 500 です。デフォルトは 1 です。
ステップ 7	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/2	インターフェイス コンフィギュレーション モードを開始し、SNMP MAC アドレス通知トラップをイネーブルにするレイヤ 2 インターフェイスを指定します。
ステップ 8	snmp trap mac-notification change {added removed} 例 : Device(config-if)# snmp trap mac-notification change added	インターフェイス上で MAC アドレス変更通知トラップをイネーブルにします。 <ul style="list-style-type: none"> • MAC アドレスがインターフェイスに added された場合にトラップをイネーブルにします。 • MAC アドレスがインターフェイスに removed された場合にトラップをイネーブルにします。
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 running-config 例 : Device# show running-config	入力を確認します。
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。

MAC アドレス移動通知トラップの設定

MAC移動通知を設定する場合は、MACアドレスが、同じVLAN内のあるポートから別のポートに移動すると常に、SNMP通知が生成されてネットワーク管理システムに送信されます。

次の手順に従い、デバイスを設定し、NMSホストにMACアドレス移動通知トラップを送信するようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	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	snmp-server host host-addr {traps informs} {version {1 2c 3}} community-string notification-type 例： Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	トラップ メッセージの受信側を指定します。 <ul style="list-style-type: none"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : サポートする SNMP バージョンを指定します。informs にはバージョン1 (デフォルト) を使用できません。 community-string : 通知処理で送信する文字列を指定します。snmp-server host コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、snmp-server community 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から、snmp-server host コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>notification-type</i> : mac-notification キーワードを使用します。
ステップ 4	snmp-server enable traps mac-notification move 例 : Device(config)# snmp-server enable traps mac-notification move	デバイスが NMS に MAC アドレス移動通知トラップを送信できるようにします。
ステップ 5	mac address-table notification mac-move 例 : Device(config)# mac address-table notification mac-move	MAC アドレス移動通知機能をイネーブルにします。
ステップ 6	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	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。

次のタスク

MAC アドレス移動通知トラップの送信をディセーブルにするには、**no snmp-server enable traps mac-notification move** 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。MAC アドレス移動通知機能をディセーブルにするには、**no mac address-table notification mac-move** 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。

設定を確認するには、**show mac address-table notification mac-move** 特権 EXEC コマンドを入力します。

MAC しきい値通知トラップの設定

MAC しきい値通知を設定する場合は、MAC アドレス テーブルのしきい値の制限値に達するか、その値を超えると、SNMP通知が生成されてネットワーク管理システムに送信されます。

NMS ホストに MAC アドレス テーブルしきい値通知トラップを送信するように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。 <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	snmp-server host host-addr { traps / informs } { version { 1 2c 3 } } community-string notification-type 例 : Device(config)# snmp-server host 172.20.10.10 traps private mac-notification	トラップ メッセージの受信側を指定します。 <ul style="list-style-type: none"> host-addr : NMS の名前またはアドレスを指定します。 traps (デフォルト) : ホストに SNMP トラップを送信します。 informs : ホストに SNMP 情報を送信します。 version : サポートする SNMP バージョンを指定します。informs にはバージョン1 (デフォルト) を使用できません。 community-string : 通知処理で送信する文字列を指定します。snmp-server host コマンドを使用してこの文字列を設定できますが、この文字列を定義するには、snmp-server community 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から、snmp-server host コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>notification-type</i> : mac-notification キーワードを使用します。
ステップ 4	snmp-server enable traps mac-notification threshold 例 : Device(config)# snmp-server enable traps mac-notification threshold	NMS への MAC しきい値通知トラップをイネーブルにします。
ステップ 5	mac address-table notification threshold 例 : Device(config)# mac address-table notification threshold	MAC アドレスしきい値通知機能をイネーブルにします。
ステップ 6	mac address-table notification threshold [limit percentage] [interval time] 例 : Device(config)# mac address-table notification threshold interval 123 Device(config)# mac address-table notification threshold limit 78	MAC アドレスしきい値使用状況モニタリングのしきい値を入力します。 <ul style="list-style-type: none"> • (任意) limit percentage : MAC アドレステーブルの使用率を指定します。有効値は 1 ~ 100% ですデフォルト値は 50% です。 • (任意) interval time : 通知の間隔を指定します。有効値は 120 秒以上です。デフォルトは 120 秒です。
ステップ 7	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# copy running-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。

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

スタティック アドレス エントリの追加および削除

スタティック アドレスを追加するには、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 : 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	mac address-table static mac-addr vlan vlan-id interface interface-id 例 : Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1	MAC アドレス テーブルにスタティック アドレスを追加します。 <ul style="list-style-type: none"> mac-addr : アドレス テーブルに追加する宛先 MAC ユニキャストアドレスを指定します。この宛先アドレスを持つパケットが指定した VLAN に着信すると、指定したインターフェイスに転送されます。 vlan-id : 指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。 interface-id : 受信パケットが転送されるインターフェイスを指定します。有効なインターフェイスは、物理ポートまたはポートチャネルです。スタティック マルチキャストアドレスの場合、複数のインターフェイス ID を入力できます。スタティック ユニキャストアドレスの場合、インターフェイスは同時に 1

	コマンドまたはアクション	目的
		つしか入力できません。ただし、同じ MAC アドレスおよび VLAN ID を指定すると、コマンドを複数回入力できます。
ステップ 4	end	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
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。

ユニキャスト MAC アドレス フィルタリングの設定

デバイスが送信元または宛先ユニキャスト スタティック アドレスをドロップするよう設定するには、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。

	コマンドまたはアクション	目的
ステップ 3	mac address-table static mac-addr vlan vlan-id drop 例 : Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop	ユニキャスト MAC アドレスフィルタリングをイネーブルにし、デバイスが指定した送信元または宛先ユニキャストスタティック アドレスを持つパケットをドロップするように設定します。 <ul style="list-style-type: none"> • <i>mac-addr</i> : 送信元または宛先ユニキャスト MAC アドレス (48 ビット) を指定します。この MAC アドレスを持つパケットはドロップされます。 • <i>vlan-id</i> : 指定された MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。
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	show running-config 例 : Device# show running-config	入力を確認します。
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。

デバイスのモニタリングおよび保守の管理

コマンド	目的
clear mac address-table dynamic	すべてのダイナミックエントリを削除します。
clear mac address-table dynamic address mac-address	特定の MAC アドレスを削除します。

コマンド	目的
clear mac address-table dynamic interface <i>interface-id</i>	指定された物理ポートまたはポートチャネル上のすべてのアドレスを削除します。
clear mac address-table dynamic vlan <i>vlan-id</i>	指定された VLAN 上のすべてのアドレスを削除します。
show clock [<i>detail</i>]	時刻と日付の設定を表示します。
show ip igmp snooping groups	すべての VLAN または指定された VLAN に対するレイヤ 2 マルチキャスト エントリを表示します。
show mac address-table address <i>mac-address</i>	指定された MAC アドレスの MAC アドレステーブル情報を表示します。
show mac address-table aging-time	すべての VLAN または指定された VLAN のエージング タイムを表示します。
show mac address-table count	すべての VLAN または指定された VLAN で存在しているアドレス数を表示します。
show mac address-table dynamic	ダイナミック MAC アドレス テーブル エントリのみを表示します。
show mac address-table interface <i>interface-name</i>	指定されたインターフェイスの MAC アドレス テーブル情報を表示します。
show mac address-table move update	MAC アドレス テーブル 移動更新情報を表示します。
show mac address-table multicast	マルチキャストの MAC アドレスのリストを表示します。
show mac address-table notification {change mac-move threshold}	MAC 通知パラメータおよび履歴テーブルを表示します。
show mac address-table secure	セキュア MAC アドレスを表示します。
show mac address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。
show mac address-table vlan <i>vlan-id</i>	指定された VLAN の MAC アドレス テーブル情報を表示します。

管理の設定例

例：システムクロックの設定

次の例は、システムクロックを手動で設定する方法を示しています。

```
Device# clock set 13:32:00 23 July 2013
```

例：サマータイムの設定

次に、サマータイムが3月10日の02:00に開始し、11月3日の02:00に終了する場合の設定を例として示します。

```
Device(config)# clock summer-time PDT recurring PST date  
10 March 2013 2:00 3 November 2013 2:00
```

次に、サマータイムの開始日と終了日を設定する例を示します。

```
Device(config)#clock summer-time PST date  
20 March 2013 2:00 20 November 2013 2:00
```

例：MOTD バナーの設定

次の例は、開始および終了デリミタにポンド記号 (#) を使用して、MOTD バナーを設定する方法を示しています。

```
Device(config)# banner motd #  
  
This is a secure site. Only authorized users are allowed.  
For access, contact technical support.  
  
#  
Device(config)#
```

次に、前の設定により表示されたバナーの例を示します。

```
Unix> telnet 192.0.2.15  
  
Trying 192.0.2.15...  
Connected to 192.0.2.15.  
Escape character is '^]'.  
  
This is a secure site. Only authorized users are allowed.
```

```

For access, contact technical support.

User Access Verification

Password:

```

例：ログインバナーの設定

次の例は、開始および終了デリミタにドル記号 (\$) を使用して、にログインバナーを設定する方法を示しています。

```

Device(config)# banner login $

Access for authorized users only. Please enter your username and password.

$

Device(config)#

```

例：MAC アドレス変更通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、NMS への MAC アドレス通知トラップの送信をイネーブルにし、MAC アドレス変更通知機能をイネーブルにし、インターバルタイムを 123 秒に設定し、履歴サイズを 100 エントリに設定し、特定のポートで MAC アドレスが追加された場合のトラップをイネーブルにする例を示します。

```

Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification change
Device(config)# mac address-table notification change
Device(config)# mac address-table notification change interval 123
Device(config)# mac address-table notification change history-size 100
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# snmp trap mac-notification change added

```

例：MAC しきい値通知トラップの設定

次に、NMS として 172.20.10.10 を指定し、MAC アドレスしきい値通知機能をイネーブルにし、インターバルタイムを 123 秒に設定し、制限を 78% に設定する例を示します。

```

Device(config)# snmp-server host 172.20.10.10 traps private mac-notification
Device(config)# snmp-server enable traps mac-notification threshold
Device(config)# mac address-table notification threshold
Device(config)# mac address-table notification threshold interval 123
Device(config)# mac address-table notification threshold limit 78

```

例：MAC アドレス テーブルへのスタティック アドレスの追加

次の例では、MAC アドレス テーブルにスタティック アドレス c2f3.220a.12f4 を追加する方法を示します。VLAN4でこのMACアドレスを宛先アドレスとして持つパケットを受信すると、パケットは指定されたポートに転送されます。



- (注) 複数のインターフェイスに同じ静的 MAC アドレスを関連付けることはできません。コマンドを別のインターフェイスで再度実行すると、新しいインターフェイス上で静的 MAC アドレスが上書きされます。

```
device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 1/0/1
```

例：ユニキャスト MAC アドレス フィルタリングの設定

次に、ユニキャスト MAC アドレス フィルタリングをイネーブルにし、c2f3.220a.12f4 の送信元または宛先アドレスを持つドロップパケットを設定する例を示します。送信元または宛先としてこの MAC アドレスを持つパケットが VLAN4 上で受信された場合、パケットがドロップされます。

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

デバイス管理の機能履歴と情報

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。

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

表 3: デバイス管理の機能履歴と情報

機能	リリース	機能情報
デバイス管理	Cisco IOS Release 15.2(7)E1	この機能が導入されました。



第 2 章

のセットアップ設定の実行

- [デバイスセットアップ設定の実行に関する情報](#) (35 ページ)
- [デバイスセットアップ設定の実行方法](#) (47 ページ)
- [デバイスのセットアップを実行する場合の設定例](#) (61 ページ)
- [デバイスセットアップ設定の実行に関する機能履歴と情報](#) (63 ページ)

デバイスセットアップ設定の実行に関する情報

IPアドレスの割り当ておよびDHCP自動設定を含む初期デバイス設定タスクを実行する前に、このモジュールのセクションを確認します。

ブート プロセス

デバイスを起動するには、スタートアップガイドやハードウェア設置ガイドの手順に従い、デバイスを設置して電源をオンにし、デバイスの初期設定（IPアドレス、サブネットマスク、デフォルトゲートウェイ、シークレット、Telnet パスワードなど）を行う必要があります。

ブートローダソフトウェアは、通常の起動プロセスを実行します。これには、次のアクティビティが含まれています。

- バンドルまたはインストールパッケージセットでブート可能（基本）パッケージを検索します。
- 下位レベルの CPU 初期化を行います。CPU レジスタを初期化することにより、物理メモリがマッピングされる場所、容量、速度などを制御します。
- CPU サブシステムの電源投入時セルフテスト（POST）を実行し、システム DRAM をテストします。
- システム ボード上のファイル システムを初期化します。
- デフォルトのオペレーティング システム ソフトウェア イメージをメモリにロードし、デバイスを起動します。

ブートローダによってフラッシュ ファイル システムにアクセスしてから、オペレーティング システムをロードします。ブートローダの使用目的は通常、オペレーティング システムのロード、展開、および起動に限定されます。オペレーティング システムが CPU を制御できるようになると、ブートローダは、次にシステムがリセットされるか電源が投入されるまでは非アクティブになります。

また、オペレーティング システムが使用不可能になるほどの重大な障害が発生した場合は、ブートローダはシステムにトラップドアからアクセスします。トラップドアからシステムへアクセスすることで、必要に応じて、フラッシュ ファイル システムのフォーマット、XMODEM プロトコルを使用したオペレーティング システムのソフトウェア イメージの再インストール、失われたパスワードの回復、そして最終的にオペレーティング システムの再起動ができます。

デバイス情報を割り当てるには、PC または端末をコンソールポートに接続するか、PC をイーサネット管理ポートに接続して、PC または端末エミュレーション ソフトウェアのボーレートおよびキャラクタフォーマットを、デバイスのコンソールポートの設定と一致させておく必要があります。

- デフォルトのボーレートは 9600 です。
- デフォルトのデータ ビットは 8 です。



(注) データ ビット オプションを 8 に設定した場合、パリティ オプションは「なし」に設定します。

- デフォルトのストップ ビットは 2 (マイナー) です。
- デフォルトのパリティ設定は「なし」です。

デバイス情報の割り当て

IP 情報を割り当てるには、デバイスのセットアッププログラムを使用する方法、DHCP サーバを使用する方法、または手動で実行する方法があります。

特定の IP 情報の設定が必要な場合、デバイスのセットアッププログラムを使用してください。このプログラムを使用すると、ホスト名とイネーブル シークレット パスワードを設定することもできます。

また、任意で、Telnet パスワードを割り当てたり (リモート管理中のセキュリティ確保のため)、スイッチをクラスタのコマンドまたはメンバスイッチとして、あるいはスタンドアロンスイッチとして設定したりできます。

サーバの設定後は DHCP サーバを使用して、IP 情報の集中管理と自動割り当てを行います。



- (注) DHCP を使用している場合は、デバイスが動的に割り当てられた IP アドレスを受信してコンフィギュレーションファイルを読み込むまでは、セットアッププログラムからの質問に回答しないでください。

デバイスの設定手順を熟知している経験豊富なユーザの場合は、デバイスを手動で設定してください。それ以外のユーザは、「ブート プロセス」で説明したセットアッププログラムを使用してください。

デフォルトのスイッチ情報

表 4: デフォルトのスイッチ情報

機能	デフォルト設定
IP アドレスおよびサブネットマスク	IP アドレスまたはサブネット マスクは定義されていません。
デフォルト ゲートウェイ	デフォルト ゲートウェイは定義されていません。
イネーブルシークレットパスワード	パスワードは定義されていません。
ホスト名	出荷時に割り当てられるデフォルトのホスト名は device です。
Telnet パスワード	パスワードは定義されていません。
クラスタ コマンド スイッチ機能	ディセーブル
クラスタ名	クラスタ名は定義されません。

DHCP ベースの自動設定の概要

DHCP は、インターネットホストおよびインターネットワーキングデバイスに設定情報を提供します。このプロトコルには、2つのコンポーネントがあります。1つは DHCP サーバからデバイスにコンフィギュレーションパラメータを提供するコンポーネント、もう1つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント/サーバモデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーションパラメータを提供します。デバイスは、DHCP クライアントおよび DHCP サーバとして機能できます。

DHCP ベースの自動設定では、デバイス (DHCP クライアント) は起動時に、IP アドレス情報およびコンフィギュレーションファイルを使用して自動的に設定されます。

DHCP ベースの自動設定を使用すると、デバイス上で DHCP クライアント側の設定を行う必要はありません。ただし、DHCP サーバで、IP アドレスに関連した各種リース オプションを設定する必要があります。

DHCP を使用してネットワーク上のコンフィギュレーションファイルの場所をリレーする場合は、TFTP サーバおよびドメインネームシステム (DNS) サーバの設定が必要になることがあります。

デバイスの DHCP サーバは、スイッチと同じ LAN 上に配置することも、そのデバイスとは別の LAN 上に配置することもできます。DHCP サーバが異なる LAN 上で動作している場合、デバイスと DHCP サーバ間に、DHCP のリレーデバイスを設定する必要があります。リレー デバイスは、直接接続されている 2 つの LAN 間でブロードキャストトラフィックを転送します。ルータはブロードキャストパケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。

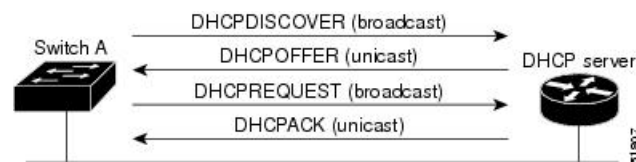
DHCP ベースの自動設定は、デバイスの BOOTP クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

デバイスを起動したときに、デバイスにコンフィギュレーションファイルがない場合、DHCP クライアントが呼び出され、DHCP クライアントが DHCP サーバに設定情報を要求します。コンフィギュレーションファイルが存在し、その設定に特定のルーテッドインターフェイスの **ip address dhcp** インターフェイス コンフィギュレーション コマンドが含まれる場合、DHCP クライアントが呼び出され、DHCP クライアントがインターフェイスに IP アドレス情報を要求します。

次は、DHCP クライアントと DHCP サーバの間で交換される一連のメッセージです。

図 2: DHCP クライアント/サーバ間のメッセージ交換



クライアントであるデバイス A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、DHCPOFFER ユニキャストメッセージによって、使用可能なコンフィギュレーションパラメータ (IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど) をクライアントに提示します。

DHCPREQUEST ブロードキャストメッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャストメッセージを受信した他のすべての DHCP サーバは、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャストメッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバウンドされ、クライアントはサーバから受信した設定情報を使用します。デバイスの受信する情報量は、DHCP サーバの設定方法によって異なります。

DHCPOFFER ユニキャスト メッセージによって送信されたコンフィギュレーション パラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーションパラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、またはDHCPOFFER メッセージに対するクライアントの応答が遅れている（DHCPサーバがパラメータを別のクライアントに割り当てた）という意味のDHCPNAK 拒否ブロードキャストメッセージを送信します。

DHCP クライアントは、複数の DHCP サーバまたは BOOTP サーバから提示を受け取り、そのうちの任意の1つを受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを確保しておきます。デバイスが BOOTP サーバからの応答を受け入れ、自身を設定する場合、デバイスはデバイス コンフィギュレーションファイルを取得するために、TFTP 要求をユニキャストするのではなくブロードキャストします。

クライアントにデフォルトのホスト名がある場合（`hostname name` グローバル コンフィギュレーション コマンドを設定していないか、`no hostname` 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ホスト名を削除していない場合）は、`ip address dhcp` 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すると、DHCP のホスト名オプションがパケットに含まれません。この場合、インターフェイスの IP アドレスを取得中にクライアントが DHCP との相互作用で DHCP ホスト名オプションを受信した場合、クライアントは DHCP ホスト名オプションを受け入れて、システムに設定済みのホスト名があることを示すフラグが設定されます。

DHCP ベースの自動設定およびイメージアップデート

DHCP イメージアップグレード機能を使用すると、ネットワーク内の1つ以上のデバイスに新しいイメージファイルおよび新しいコンフィギュレーションファイルをダウンロードするように DHCP サーバを設定できます。ネットワーク内のすべてのスイッチでのイメージおよびコンフィギュレーションの同時アップグレードによって、ネットワークに加えられたそれぞれの新しいデバイスが、同じイメージとコンフィギュレーションを確実に受信するようになります。

DHCP イメージアップグレードには、自動設定およびイメージアップデートの2つのタイプがあります。

DHCP ベースの自動設定の制約事項

- ネットワーク内に割り当てられた IP アドレスがなく、1つ以上のレイヤ3 インターフェイスが起動していない場合は、設定プロセスが保存された DHCP ベースの自動設定は停止します。
- タイムアウトを設定しない限り、設定機能を備えている DHCP ベースの自動設定は IP アドレスのダウンロードを無期限に繰り返します。
- コンフィギュレーションファイルをダウンロードできないか破損している場合は、自動インストールプロセスが停止します。

- TFTP からダウンロードされたコンフィギュレーションファイルは、実行コンフィギュレーション内の既存コンフィギュレーションとマージされますが、**write memory** または **copy running-configuration startup-configuration** 特権 EXEC コマンドを入力しない限り、NVRAM に保存されません。ダウンロードされたコンフィギュレーションがスタートアップコンフィギュレーションに保存された場合、後続のシステム再起動中にこの機能はトリガーされません。

DHCP 自動設定

DHCP 自動設定は、コンフィギュレーションファイルを DHCP サーバからネットワーク内の 1 つ以上のデバイスにダウンロードします。ダウンロードされたコンフィギュレーションファイルは、デバイスの実行コンフィギュレーションファイルになります。このファイルは、デバイスがリロードされるまで、フラッシュメモリに保存されたブートアップコンフィギュレーションを上書きしません。

DHCP 自動イメージアップグレード

DHCP 自動設定とともに DHCP 自動イメージアップグレードを使用すると、コンフィギュレーションおよび新しいイメージをネットワーク内の 1 つ以上のデバイスにダウンロードできます。新しいコンフィギュレーションおよび新しいイメージをダウンロードしている 1 つまたは複数のデバイスは、ブランク（つまり、出荷時のデフォルト設定がロードされている状態）にできます。

コンフィギュレーションをすでに持っているスイッチに新しいコンフィギュレーションをダウンロードすると、ダウンロードされたコンフィギュレーションは、スイッチに保存されているコンフィギュレーションファイルに追加されます（どの既存のコンフィギュレーションファイルも、ダウンロードされたファイルに上書きされません）。

デバイスの DHCP 自動イメージアップグレードをイネーブルにするには、イメージファイルおよびコンフィギュレーションファイルがある TFTP サーバを、正しいオプション 67（コンフィギュレーションファイル名）、オプション 66（DHCP サーバホスト名）、オプション 150（TFTP サーバアドレス）、およびオプション 125（Cisco IOS イメージファイルの説明）の設定で設定する必要があります。

デバイスをネットワークに設置すると、自動イメージアップグレード機能が開始します。ダウンロードされたコンフィギュレーションファイルはデバイスの実行コンフィギュレーションに保存され、新しいイメージがダウンロードされてデバイスにインストールされます。デバイスを再起動すると、このコンフィギュレーションがデバイスのコンフィギュレーションに保存されます。

DHCP サーバ設定時の注意事項

デバイスを DHCP サーバとして設定する場合、次の注意事項に従ってください。

- DHCP サーバには、デバイスのハードウェアアドレスによって各デバイスと結び付けられている予約済みのリースを設定する必要があります。

- デバイスに IP アドレス情報を受信させるには、DHCP サーバに次のリースオプションを設定する必要があります。
 - クライアントの IP アドレス (必須)
 - クライアントのサブネットマスク (必須)
 - DNS サーバの IP アドレス (任意)
 - ルータの IP アドレス (デバイスで使用するデフォルト ゲートウェイ アドレス) (必須)
- デバイスに TFTP サーバからコンフィギュレーションファイルを受信させる場合は、DHCP サーバに次のリースオプションを設定する必要があります。
 - TFTP サーバ名 (必須)
 - ブートファイル名 (クライアントが必要とするコンフィギュレーションファイル名) (推奨)
 - ホスト名 (任意)
- DHCP サーバの設定によっては、デバイスは IP アドレス情報またはコンフィギュレーションファイル、あるいはその両方を受信できます。
- 前述のリースオプションを設定しなかった場合、DHCP サーバは、設定されたパラメータのみを使用してクライアントの要求に応答します。IP アドレスおよびサブネットマスクが応答に含まれていないと、デバイスは設定されません。ルータの IP アドレスまたは TFTP サーバ名が見つからなかった場合、デバイスは TFTP 要求をユニキャストしないでブロードキャストする場合があります。その他のリースオプションは、使用できなくても自動設定には影響しません。
- デバイスは DHCP サーバとして動作することができます。デフォルトでは、Cisco IOS DHCP サーバおよび DHCP リレーエージェント機能はデバイス上でイネーブルにされていますが、設定されていません。(これらの機能は動作しません)

TFTP サーバの目的

DHCP サーバの設定に基づいて、デバイスは TFTP サーバから 1 つまたは複数のコンフィギュレーションファイルをダウンロードしようとします。TFTP サーバへの IP 接続に必要なすべてのオプションについてデバイスに応答するよう DHCP を設定している場合で、なおかつ、TFTP サーバ名、アドレス、およびコンフィギュレーションファイル名を指定して DHCP サーバを設定している場合、デバイスは指定された TFTP サーバから指定されたコンフィギュレーションファイルをダウンロードしようとします。

コンフィギュレーションファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーションファイルをダウンロードできなかった場合は、デバイスはファイル名と TFTP サーバアドレスをさまざまに組み合わせてコンフィギュレーションファイルをダウンロードしようとします。ファイルには、特定のコンフィギュレーションファイル名 (存在する場合) と次のファイルが指定されています。network-config、cisonet.cfg、hostname.config、ま

たは *hostname.cfg* です。この場合、*hostname* はデバイスの現在のホスト名です。使用される TFTP サーバアドレスには、（存在する場合）指定された TFTP サーバのアドレス、およびブロードキャストアドレス（255.255.255.255）が含まれています。

デバイスが正常にコンフィギュレーションファイルをダウンロードするには、TFTP サーバのベースディレクトリに1つまたは複数のコンフィギュレーションファイルが含まれていなければなりません。含めることのできるファイルは、次のとおりです。

- DHCP 応答で指定されているコンフィギュレーションファイル（実際のデバイスコンフィギュレーションファイル）。
- *network-config* または *cisconet.cfg* ファイル（デフォルトのコンフィギュレーションファイル）
- *router-config* または *ciscorttr.cfg* ファイル（これらのファイルには、すべてのデバイスに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されていれば、これらのファイルはアクセスされません）

DHCP サーバリース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定することも必要です。

使用する TFTP サーバが、デバイスとは異なる LAN 上にある場合、またはデバイスがブロードキャストアドレスを使用してアクセスした場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。適切な解決方法は、必要なすべての情報を使用して DHCP サーバを設定することです。

DNS サーバの目的

DHCP サーバは、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、デバイスのコンフィギュレーションファイルが存在します。

DHCP の応答時に IP アドレスを取得する DHCP サーバのリース データベースに、DNS サーバの IP アドレスを設定できます。リース データベースには、DNS サーバの IP アドレスを2つまで入力できます。

DNS サーバは、デバイスと同じ LAN 上に配置することも、別の LAN 上に配置することもできます。DNS サーバが別の LAN 上に存在する場合、デバイスはルータを介して DNS サーバにアクセスできなければなりません。

コンフィギュレーションファイルの入手方法

IP アドレスおよびコンフィギュレーションファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、デバイスは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーションファイル名が、デバイス用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されている場合

デバイスは DHCP サーバから、IP アドレス、サブネットマスク、TFTP サーバアドレス、およびコンフィギュレーションファイル名を受信します。デバイスは、TFTP サーバにユニキャストメッセージを送信し、指定されたコンフィギュレーションファイルをサーバのベースディレクトリから取得して、ブートアッププロセスを完了します。

- デバイスの IP アドレスおよびコンフィギュレーションファイル名が予約されているが、DHCP 応答に TFTP サーバアドレスが含まれていない場合（1 ファイル読み込み方式）。

デバイスは DHCP サーバから、IP アドレス、サブネットマスク、およびコンフィギュレーションファイル名を受信します。デバイスは、TFTP サーバにブロードキャストメッセージを送信し、指定されたコンフィギュレーションファイルをサーバのベースディレクトリから取得して、ブートアッププロセスを完了します。

- IP アドレスだけがデバイス用に予約され、DHCP 応答で提供されており、コンフィギュレーションファイル名は提供されない場合（2 ファイル読み込み方式）

デバイスは DHCP サーバから、IP アドレス、サブネットマスク、および TFTP サーバアドレスを受信します。デバイスは、TFTP サーバにユニキャストメッセージを送信し、`network-config` または `cisconet.cfg` のデフォルトコンフィギュレーションファイルを取得します（`network-config` ファイルが読み込めない場合、デバイスは `cisconet.cfg` ファイルを読み込みます）。

デフォルトコンフィギュレーションファイルには、デバイスのホスト名から IP アドレスへのマッピングが含まれています。デバイスは、ファイルの情報をホストテーブルに書き込み、ホスト名を入手します。ファイルにホスト名がない場合、デバイスは DHCP 応答で指定されたホスト名を使用します。DHCP 応答でホスト名が指定されていない場合、デバイスはデフォルトの *Switch* をホスト名として使用します。

デフォルトのコンフィギュレーションファイルまたは DHCP 応答からホスト名を入手した後、デバイスはホスト名と同じ名前のコンフィギュレーションファイル（`network-config` または `cisconet.cfg` のどちらが先に読み込まれたかに応じて、`hostname-config` または `hostname.cf`）を TFTP サーバから読み込みます。`cisconet.cfg` ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

`network-config`、`cisconet.cfg`、またはホスト名と同じ名前のファイルを読み込むことができない場合、デバイスは `router-config` ファイルを読み込みます。`router-config` ファイルを読み込むことができない場合、デバイスは `ciscortr.cfg` ファイルを読み込みます。



-
- (注) DHCP 応答から TFTP サーバを入手できなかった場合、ユニキャスト伝送によるコンフィギュレーションファイルの読み込みにすべて失敗した場合、または TFTP サーバ名を IP アドレスに変換できない場合には、デバイスは TFTP サーバ要求をブロードキャストします。
-

環境変数の制御方法

通常動作のデバイスでは、コンソール接続のみを通じてブートローダモードを開始します。スイッチの電源コードを取り外してから、もう一度電源コードを接続します。ブートローダスイッチのプロンプトが表示されるまで [MODE] を押し続けます。

デバイスのブートローダソフトウェアは不揮発性の環境変数をサポートするため、これらの環境変数を使用して、ブートローダまたはシステムで稼働する他のソフトウェアの機能を制御できます。ブートローダの環境変数は、UNIX または DOS システムで設定できる環境変数と類似しています。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保存されます。

ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。変数が存在しない場合は、変数の値はありません。値がヌルストリングと表示された場合は、変数に値が設定されています。ヌルストリング (たとえば "") が設定されている変数は、値が設定された変数です。多くの環境変数は事前に定義されており、デフォルト値が設定されています。

環境変数には 2 種類のデータが保存されます。

- Cisco IOS コンフィギュレーション ファイルを読み取らないコードを制御するデータ。たとえば、ブートローダの機能を拡張したり、パッチを適用したりするブートローダ ヘルパー ファイルの名前は、環境変数として保存できます。
- Cisco IOS コンフィギュレーション ファイルを読み取るコードを制御するデータ。たとえば、Cisco IOS コンフィギュレーション ファイル名は環境変数として保存できます。

環境変数の設定を変更するには、ブートローダにアクセスするか、Cisco IOS コマンドを使用します。通常的环境では、環境変数の設定を変更する必要はありません。

一般的な環境変数

この表では、最も一般的な環境変数の機能について説明します。

表 5: 一般的な環境変数

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
BOOT	<p>set BOOT <i>filesystem</i> <i>:/file-url ...</i></p> <p>自動起動時にロードして実行を試みる、セミコロンで区切られた実行可能ファイルのリスト。BOOT 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュファイルシステムで最初に検出した起動可能なファイルを起動しようとします。</p>	<p>boot system <i>{filesystem : /file-url ...</i></p> <p>次の起動時にロードする Cisco IOS イメージを指定します。このコマンドは、BOOT 環境変数の設定を変更します。</p>

変数	ブートローダ コマンド	Cisco IOS グローバル コンフィギュレーション コマンド
MANUAL_BOOT	<p>set MANUAL_BOOT yes</p> <p>スイッチの起動を自動で行うか手動で行うかを決定します。</p> <p>有効な値は1、yes、0、およびnoです。no または 0 に設定されている場合、ブートローダはシステムを自動的に起動しようとします。それ以外の値に設定されている場合は、ブートローダモードから手動でスイッチを起動する必要があります。</p>	<p>boot manual</p> <p>次回の起動時にスイッチを手動で起動できるようにします。MANUAL_BOOT 環境変数の設定が変更されます。</p> <p>次回のシステム再起動時には、スイッチはブートローダモードになります。システムを起動するには、boot flash:filesystem:/file-url ブートローダコマンドを使用してブート可能なイメージの名前を指定します。</p>
CONFIG_FILE	<p>set CONFIG_FILE flash:/file-url</p> <p>Cisco IOS がシステム コンフィギュレーションの不揮発性コピーの読み書きに使用するファイル名を変更します。</p>	<p>boot config-file flash:/file-url</p> <p>Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。このコマンドによって、CONFIG_FILE 環境変数が変更されます。</p>
BAUD	<p>set BAUD baud-rate</p>	<p>line console 0</p> <p>speedspeed-value</p> <p>ボー レートを設定します。</p>
ENABLE_BREAK	<p>set ENABLE_BREAK yes/no</p>	<p>boot enable-break switch yes/no</p> <p>このコマンドは、ENABLE_BREAK が yes に設定されている場合にフラッシュファイルシステムを初期化するときに発行できます。</p>

ソフトウェアイメージのリロードのスケジューリング

デバイス上でソフトウェアイメージのリロードを後で（深夜、週末などデバイスをあまり使用しないときに）行うように、スケジュールを設定できます。または（ネットワーク内のすべてのデバイスでソフトウェアをアップグレードする場合など）ネットワーク全体でリロードを同時に行うことができます。

リロードオプションには以下のものがあります。

- 指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされます。リロードは、約 24 時間以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。
- ソフトウェアのリロードが（24時間制で）指定された時間に有効になります。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。

reload コマンドはシステムを停止させます。手動で起動することが設定されていない限り、システムは自動的に再起動します。

手動で起動するようにデバイスが設定されている場合、仮想端末からリロードを実行しないでください。これはデバイスがブートローダモードになることでリモートユーザが制御を失う事態を防止するための制約です。

コンフィギュレーションファイルを変更すると、リロードの前にコンフィギュレーションを保存するように指示するプロンプトがデバイスにより表示されます。保存操作時に、CONFIG_FILE 環境変数がすでに存在しないスタートアップ コンフィギュレーション ファイルを示していた場合、保存を続行するかどうかという問い合わせがシステムから出されます。その状況のまま続けると、リロード時にセットアップモードが開始されます。

スケジュールがすでに設定されたリロードを取り消すには、**reload cancel** 特権 EXEC コマンドを使用します。

デバイスセットアップ設定の実行方法

DHCP を使用してデバイスに新しいイメージおよび新しいコンフィギュレーションをダウンロードするには、少なくとも 2 つのデバイスを設定する必要があります。1 つ目のデバイスは DHCP サーバおよび TFTP サーバと同じように機能し、2 つ目のデバイス（クライアント）は新しいコンフィギュレーション ファイル、または新しいコンフィギュレーション ファイルおよび新しいイメージファイルをダウンロードするように設定されています。

DHCP 自動設定（コンフィギュレーション ファイルだけ）の設定

このタスクでは、新しいデバイスの自動設定をサポートできるように、ネットワーク内の既存のデバイスで TFTP や DHCP の設定の DHCP 自動設定を行う方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	ip dhcp pool poolname 例： Device(config)# ip dhcp pool pool	DHCP サーバアドレスプールの名前を作成し、DHCP プール 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	boot filename 例： Device(dhcp-config)# boot config-boot.text	ブートイメージとして使用されるコンフィギュレーションファイルの名前を指定します。
ステップ 4	network network-number mask prefix-length 例： Device(dhcp-config)# network 10.10.10.0 255.255.255.0	DHCP アドレス プールのサブネットワーク番号およびマスクを指定します。 (注) プレフィックス長は、アドレスプレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワークマスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ (/) で開始する必要があります。
ステップ 5	default-router address 例： Device(dhcp-config)# default-router 10.10.10.1	DHCP クライアントのデフォルトルータの IP アドレスを指定します。
ステップ 6	option 150 address 例： Device(dhcp-config)# option 150 10.10.10.1	TFTP サーバの IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 7	exit 例： Device (dhcp-config) # 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 8	tftp-server flash:filename.text 例： Device (config) # tftp-server flash:config-boot.text	TFTP サーバ上のコンフィギュレーションファイルを指定します。
ステップ 9	interface interface-id 例： Device (config) # interface gigabitethernet 1/0/4	コンフィギュレーションファイルを受信するクライアントのアドレスを指定します。
ステップ 10	no switchport 例： Device (config-if) # no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 11	ip address address mask 例： Device (config-if) # ip address 10.10.10.1 255.255.255.0	IP アドレスとインターフェイスのマスクを指定します。
ステップ 12	end 例： Device (config-if) # end	特権 EXEC モードに戻ります。

DHCP 自動イメージアップデート（コンフィギュレーションファイルおよびイメージ）の設定

このタスクでは、新しいスイッチのインストールをサポートするように既存のデバイスで TFTP および DHCP を設定する DHCP 自動設定について説明します。

始める前に

最初にデバイスにアップロードするテキストファイル（たとえば、`autoinstall_dhcp`）を作成します。テキストファイルに、ダウンロードするイメージの名前を指定します（たとえば、`c3750e-ip-services-mz.122-44.3.SE.tar`、`c3750x-ip-services-mz.122-53.3.SE2.tar`）。このイメージは、`bin` ファイルでなく、`tar` ファイルである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： 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	ip dhcp pool poolname 例： Device(config)# ip dhcp pool pool1	DHCP サーバアドレスプールの名前を作成し、DHCP プール 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	boot filename 例： Device(dhcp-config)# boot config-boot.text	ブートイメージとして使用されるファイルの名前を指定します。
ステップ 4	network network-number mask prefix-length 例： Device(dhcp-config)# network 10.10.10.0 255.255.255.0	DHCP アドレス プールのサブネット ネットワーク番号およびマスクを指定します。 (注) プレフィックス長は、アドレスプレフィックスを構成するビット数を指定します。プレフィックスは、クライアントのネットワークマスクを指定する二者択一の方法です。プレフィックス長は、スラッシュ (/) で開始する必要があります。
ステップ 5	default-router address 例： Device(dhcp-config)# default-router	DHCP クライアントのデフォルトルータの IP アドレスを指定します。

	コマンドまたはアクション	目的
	10.10.10.1	
ステップ 6	option 150 address 例 : Device(dhcp-config)# option 150 10.10.10.1	TFTP サーバの IP アドレスを指定します。
ステップ 7	option 125 hex 例 : Device(dhcp-config)# option 125 hex 0000.0009.0a05.0866.1.7574.6f69.6e73.7461.6c6c.5664.686370	イメージファイルのパスを記述したテキストファイルのパスを指定します。
ステップ 8	copy tftp flash filename.txt 例 : Device(config)# copy tftp flash image.bin	デバイスに、テキストファイルをアップロードします。
ステップ 9	copy tftp flash imagename.bin 例 : Device(config)# copy tftp flash image.bin	デバイスに、新しいイメージの tar ファイルをアップロードします。
ステップ 10	exit 例 : Device(dhcp-config)# 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 11	tftp-server flash: config.text 例 : Device(config)# tftp-server flash:config-boot.text	TFTP サーバ上の Cisco IOS コンフィギュレーション ファイルを指定します。
ステップ 12	tftp-server flash: imagename.bin 例 : Device(config)# tftp-server	TFTP サーバ上のイメージ名を指定します。

	コマンドまたはアクション	目的
	<code>flash:image.bin</code>	
ステップ 13	tftp-server flash: filename.txt 例： Device(config)# tftp-server flash:boot-config.text	ダウンロードするイメージファイルの名前を記述したテキストファイルを指定します。
ステップ 14	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/4	コンフィギュレーションファイルを受信するクライアントのアドレスを指定します。
ステップ 15	no switchport 例： Device(config-if)# no switchport	インターフェイスをレイヤ 3 モードにします。
ステップ 16	ip address address mask 例： Device(config-if)# ip address 10.10.10.1 255.255.255.0	IP アドレスとインターフェイスのマスクを指定します。
ステップ 17	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 18	copy running-config startup-config 例： Device(config-if)# end	(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。

DHCP サーバからファイルをダウンロードするクライアントの設定



(注) レイヤ3インターフェイスだけを設定してイネーブルにする必要があります。保存されているコンフィギュレーションのDHCPベースの自動設定にIPアドレスを割り当てないでください。

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	boot host dhcp 例 : Device(conf)# boot host dhcp	保存されているコンフィギュレーションで自動設定をイネーブルにします。
ステップ 3	boot host retry timeout timeout-value 例 : Device(conf)# boot host retry timeout 300	(任意) システムがコンフィギュレーション ファイルをダウンロードしようとする時間を設定します。 (注) タイムアウトを設定しないと、システムは無期限にDHCPサーバからIPアドレスを取得しようとします。
ステップ 4	banner config-save ^C warning-message ^C 例 : Device(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C	(任意) コンフィギュレーション ファイルを NVRAM に保存しようとするときに表示される警告メッセージを作成します。
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	show boot 例： Device# show boot	設定を確認します。

IP ルーティングがディセーブルの場合のルーティング支援機能

次のメカニズムを使用することで、デバイスは、IP ルーティングが有効でない場合、別のネットワークへのルートを学習できます。

- デフォルト ゲートウェイ

デフォルト ゲートウェイ

ルートを特定するもう 1 つの方法は、デフォルト ルータ、つまりデフォルト ゲートウェイを定義する方法です。ローカルでないすべてのパケットはこのルータに送信されます。このルータは適切なルーティングを行う、または IP 制御メッセージ プロトコル (ICMP) リダイレクトメッセージを返信するという方法で、ホストが使用するローカルルータを定義します。デバイスはリダイレクトメッセージをキャッシュに格納し、各パケットをできるだけ効率的に転送します。この方法には、デフォルト ルータがダウンした場合、または使用できなくなった場合に、検出が不可能となる制限があります。

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	ip default-gateway ip-address 例： Device(config)# ip default gateway 10.1.5.1	デフォルト ゲートウェイ (ルータ) を設定します。

	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 ip redirects 例 : Device# show ip redirects	設定を確認するため、デフォルトゲートウェイルータのアドレスを表示します。
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。

複数の SVI への IP 情報の手動割り当て

このタスクでは、複数のスイッチ仮想インターフェイス (SVI) に IP 情報を手動で割り当てる方法について説明します。

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 vlan vlan-id 例 : Device(config)# interface vlan 99	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、IP 情報を割り当てる VLAN を入力します。指定できる範囲は 1 ~ 4094 です。
ステップ 3	ip address ip-address subnet-mask 例 : Device(config-vlan)# ip address 10.10.10.2 255.255.255.0	IP アドレスとサブネットマスクを入力します。

	コマンドまたはアクション	目的
ステップ 4	exit 例 : Device(config-vlan)# 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 5	ip default-gateway ip-address 例 : Device(config)# ip default-gateway 10.10.10.1	<p>デバイスに直接接続しているネクストホップのルーティンターフェイスの IP アドレスを入力します。このスイッチにはデフォルトゲートウェイが設定されています。デフォルトゲートウェイは、デバイススイッチから宛先 IP アドレスを取得していない IP パケットを受信しません。</p> <p>デフォルトゲートウェイが設定されると、デバイスは、ホストが接続する必要のあるリモートネットワークに接続できます。</p> <p>(注) IP でルーティングするようにデバイスを設定した場合、デフォルトゲートウェイの設定は不要です。</p>
ステップ 6	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces vlan vlan-id 例 : Device# show interfaces vlan 99	設定された IP アドレスを確認します。
ステップ 8	show ip redirects 例 : Device# show ip redirects	設定されたデフォルトゲートウェイを確認します。

NVRAM バッファ サイズの設定

デフォルトの NVRAM バッファ サイズは 512 KB です。コンフィギュレーションファイルが大きすぎて NVRAM に保存できない場合があります。より大きいコンフィギュレーションファイルをサポートできるように、NVRAM バッファのサイズを設定できます。



(注) NVRAM バッファサイズを設定後、スイッチをリロードします。

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	boot buffersize size 例： Device (config)# boot buffersize 524288	NVRAM のバッファ サイズを KB 単位で設定します。size の有効な範囲は、4096 ~ 1048576 です。
ステップ 3	end 例： Device (config)# end	特権 EXEC モードに戻ります。
ステップ 4	show boot 例： Device# show boot	設定を確認します。

デバイスのスタートアップ コンフィギュレーションの変更

システム コンフィギュレーションを読み書きするためのファイル名の指定

Cisco IOS ソフトウェアは、デフォルトで `config.text` ファイルを使用して、システム コンフィギュレーションの不揮発性コピーを読み書きします。別のファイル名を指定することもできます。次の起動時には、その名前のファイルが読み込まれます。

始める前に

このタスクではスタンドアロンのデバイスを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	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	boot flash:/file-url 例： Switch(config)# boot flash:config.text	次回の起動時に読み込むコンフィギュレーション ファイルを指定します。 <i>file-url</i> : パス (ディレクトリ) およびコンフィギュレーション ファイル名。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	show boot 例： Switch# show boot	入力を確認します。 boot グローバル コンフィギュレーション コマンドによって、CONFIG_FILE 環境変数の設定が変更されます。
ステップ 5	copy running-config startup-config 例： Switch# 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。

スイッチの手動による起動

スイッチはデフォルトで自動的に起動しますが、手動で起動するように設定することもできます。

始める前に

このタスクのスタンドアロン スイッチを使用します。

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	boot manual 例 : Device(config)# boot manual	次の起動時に、スイッチを手動で起動できるようにします。
ステップ 3	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 4	show boot 例 : Device# show boot	入力を確認します。 boot manual グローバルコマンドは、 MANUAL_BOOT 環境変数の設定を変更します。 次回、システムを再起動した際には、スイッチはブートローダ モードになり、ブートローダモードであることが switch: プロンプトによって示されます。システムを起動するには、 boot filesystem:/file-url ブートローダコマンドを使用します。 <ul style="list-style-type: none"> • filesystem : システムボードのフラッシュ デバイスに flash: を使用します。 Switch: boot flash: • file-url : パス (ディレクトリ) および起動可能なイメージの名前を指定します。 ファイル名およびディレクトリ名は、大文字と小文字を区別します。
ステップ 5	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
	<pre>Device# copy running-config startup-config</pre>	

ソフトウェアイメージのリロードのスケジュール設定

このタスクでは、ソフトウェアイメージを後でリロードするようにデバイスを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <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。
ステップ 2	<p>copy running-config startup-config</p> <p>例 :</p> <pre>copy running-config startup-config</pre>	reload コマンドを使用する前に、デバイスの設定情報をスタートアップコンフィギュレーションに保存します。
ステップ 3	<p>reload in [hh:]mm [text]</p> <p>例 :</p> <pre>Device(config)# reload in 12</pre> <p>System configuration has been modified. Save? [yes/no]: y</p>	指定した分数、または時間および分数が経過したときに、ソフトウェアがリロードされるようにスケジュールを設定します。リロードは、約 24 日以内に実行する必要があります。最大 255 文字で、リロードの理由を指定できます。
ステップ 4	<p>reload at hh: mm [month day day month] [text]</p> <p>例 :</p>	リロードを実行する時間を、時間数と分数で指定します。

	コマンドまたはアクション	目的
	Device(config)# reload at 14:00	(注) at キーワードを使用するのは、デバイスシステムクロックが (Network Time Protocol (NTP)、ハードウェアカレンダー、または手動で) 設定されている場合だけです。時刻は、デバイスに設定されたタイムゾーンに基づきます。リロードが複数のデバイスで同時に行われるようにスケジューリングするには、各デバイスの時間が NTP と同期している必要があります。
ステップ 5	reload cancel 例： device(config)# reload cancel	以前にスケジューリングされたリロードをキャンセルします。
ステップ 6	show reload 例： show reload	以前デバイスにスケジューリングされたリロードに関する情報、またはリロードがスケジューリングされているかを表示します。

デバイスのセットアップを実行する場合の設定例

例：デバイスを DHCP サーバとして設定

```
Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# interface gigabitethernet 1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end
```

例：DHCP 自動イメージアップデートの設定

```

Device# configure terminal
Device(config)# ip dhcp pool pool1
Device(dhcp-config)# network 10.10.10.0 255.255.255.0
Device(dhcp-config)# boot config-boot.text
Device(dhcp-config)# default-router 10.10.10.1
Device(dhcp-config)# option 150 10.10.10.1
Device(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
Device(dhcp-config)# exit
Device(config)# tftp-server flash:config-boot.text
Device(config)# tftp-server flash:image_name
Device(config)# tftp-server flash:boot-config.text
Device(config)# tftp-server flash:autoinstall_dhcp
Device(config)# interface gigabitethernet 1/0/4
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.10.1 255.255.255.0
Device(config-if)# end

```

例：DHCP サーバから設定をダウンロードするためのデバイスの設定

次に、VLAN 99 上のレイヤ 3 SVI インターフェイスを使用し、保存されているコンフィギュレーションで DHCP ベースの自動設定をイネーブルにする例を示します。

```

Device# configure terminal
Device(config)# boot host dhcp
Device(config)# boot host retry timeout 300
Device(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May
Cause You to No longer Automatically Download Configuration Files at Reboot^C
Device(config)# vlan 99
Device(config-vlan)# interface vlan 99
Device(config-if)# no shutdown
Device(config-if)# end
Device# show boot
BOOT path-list:
Config file:          flash:/config.text
Private Config file:  flash:/private-config.text
Enable Break:        no
Manual Boot:         no
HELPER path-list:
NVRAM/Config file
  buffer size:       32768
Timeout for Config
  Download:          300 seconds
Config Download
  via DHCP:          enabled (next boot: enabled)
Device#

```

例：NVRAM バッファ サイズの設定

```

Device# configure terminal

```

```
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# boot buffersize 600000
Device(config)# end
Device# show boot
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file   :
    buffer size:    600000
Timeout for Config :
    Download:       300 seconds
Config Download     :
    via DHCP:       enabled (next boot: enabled)
Device#
```

デバイスセットアップ設定の実行に関する機能履歴と情報

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E1	この機能が導入されました。



第 3 章

sFlow の設定

- [sFlow について \(65 ページ\)](#)
- [sFlow の前提条件 \(66 ページ\)](#)
- [注意事項と制約事項 \(66 ページ\)](#)
- [sFlow のデフォルト設定 \(66 ページ\)](#)
- [sFlow の設定方法 \(67 ページ\)](#)
- [sFlow 設定の確認 \(71 ページ\)](#)
- [sFlow 統計情報のモニタリングとクリア \(72 ページ\)](#)
- [sFlow の設定例 \(72 ページ\)](#)
- [sFlow の設定に関する機能情報 \(73 ページ\)](#)

sFlow について

サンプリングされた Flow (sFlow) を使用すると、スイッチやルータを含むデータネットワーク内のリアルタイムトラフィックをモニタできます。sFlow では、トラフィックをモニタするためにスイッチ上の sFlow エージェントソフトウェアでサンプリングメカニズムを使用して、サンプルデータを中央のデータコレクタに転送します。

コアの sFlow エージェントワークフローは次のとおりです。

1. 有効になっているインターフェイスからカウンタサンプル情報を収集するための定期的なポーリング。
2. フローサンプリングのために受信したパケットの処理。
3. sFlow データグラムの作成とエクスポート。

sFlow エージェント

sFlow エージェントは、サンプリングされるパケットのデータソースに関連付けられたインターフェイスカウンタを定期的にサンプリングまたはポーリングします。このデータソースは、イーサネット インターフェイス、またはある範囲に属するイーサネット インターフェイスです。

sFlow サンプルングをイネーブルにすると、サンプルングレートとハードウェア内部の乱数に基づいて、入力パケットと出力パケットが sFlow でサンプルングされたパケットとして CPU に送信されます。sFlow エージェントはサンプルングされたパケットを処理し、sFlow アナライザに sFlow データグラムを送信します。sFlow データグラムには、元のサンプルングされたパケットに加えて、入力ポート、出力ポート、および元のパケット長に関する情報が含まれます。sFlow データグラムには、複数の sFlow サンプルを含めることができます。

sFlow の前提条件

sFlow には、次の前提条件があります。

- コレクタの宛先が到達可能であることを確認します。
- IP ルーティングをデバイスでイネーブルにする必要があります。

注意事項と制約事項

sFlow には、次の注意事項があります。

- インターフェイスの sFlow をイネーブルにすると、入力、出力、または両方向で sFlow を実行できます。
- システムの sFlow の設定およびトラフィックに基づいてサンプルングレートを設定する必要があります。

sFlow には、次の制限事項があります。

- sFlow は物理インターフェイスでのみサポートされます。
- スイッチは 2 つの sFlow コレクタをサポートします。
- デバイスがスタックモードで起動する場合、sFlow はサポートされません。

sFlow のデフォルト設定

次の表に、sFlow パラメータのデフォルト設定を示します。

表 6: デフォルトの sFlow パラメータ

パラメータ	デフォルト
sFlow のサンプルングレート	2048
sFlow のサンプルングサイズ	116
sFlow カウンタのポーリング間隔	10

パラメータ	デフォルト
sFlow の最大データグラム サイズ	1024
sFlow のコレクタ ポート	6343

sFlow の設定方法

ここでは、sFlow の設定方法について説明します。

sFlow エージェントの設定

sFlow エージェントを有効にするには、インターフェイスで有効なユニキャスト IP アドレスを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： 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	[no] sflow agent { ip ipv4 address ipv6 ipv6 address } 例： Device(config)# sflow agent ip 10.1.1.1	インターフェイスに IP アドレスを設定し、sFlow エージェントを有効にします。sFlow エージェントをディセーブルにするには、このコマンドの no 形式を使用します。 IPv6 アドレスの場合は、グローバルユニキャストアドレスである必要があります。
ステップ 3	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 4	show sflow 例： Device# show sflow	(任意) グローバル sFlow コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 5	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。

sFlow コレクタの設定

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	sflow collector { id collector-id } { ip ipv4 address ipv6 ipv6 address } [port <port>] [datagram-size <max-datagram-size bytes>] 例 : Device(config)# sflow collector id 1 ip 10.1.1.2 port 6343 datagram-size 1024	sFlow コレクタを設定します。IP アドレスを指定する必要があります。 <ul style="list-style-type: none"> • <i>collector-id</i> : 値の範囲は <1 ~ 2> にする必要があります。 • <i>port</i> : ポート値は <1 ~ 65535> の範囲内である必要があります。デフォルトは 6343 です。 • <i>max-datagram-size bytes</i> : 最大データグラムサイズを <1024 ~ 9000> のバイト単位で設定します。デフォルトは 1024 です。
ステップ 3	[no] sflow collector { id collector-id } 例 : Device(config)# no sflow collector id 1	sFlow コレクタの設定を削除します。
ステップ 4	end 例 : Device(config)# 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 5	show sflow 例 : Device# show sflow	(任意) グローバル sFlow コンフィギュレーションを表示します。
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。

フローサンプリングの設定

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 gigabitethernet1/0/2	インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	sflow flow-sampling {input output } id collector-id [rate <rate>] [hdr-size <max-header-size bytes>] 例 : Device (config-if)# sflow flow-sampling input id 1 rate 256 hdr-size 200	そのインターフェイスからのパケットサンプルの送信先となる collector-id を指定します。 <ul style="list-style-type: none"> • <i>collector-id</i> : 値の範囲は <1 ~ 2> にする必要があります。 • <i>rate</i> : サンプリングレートは <256 ~ 1073741823> の範囲です。デフォルトは 2048 です。 • <i>max-header-size bytes</i> : コピーされる最大ヘッダーサイズ (バイト単位、<18 ~ 512> の範囲)。デフォルトは 116 です。

	コマンドまたはアクション	目的
ステップ 4	no sflow flow-sampling {input output } 例： Device(config-if)# no sflow flow-sampling input	インターフェイスのフローサンプリングの設定を削除します。
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 sflow interface 例： Device# show sflow interface gigabitethernet1/0/2	フローパケットサンプリングが有効になっているすべてのインターフェイスの sFlow 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。

カウンタサンプリングの設定

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 gigabitethernet1/0/2	インターフェイスコンフィギュレーション モードを開始します。
ステップ 3	sflow counter-sampling id collector-id [interval <interval>] 例：	そのインターフェイスからのカウンタサンプルの送信先となる collector-id を指定します。

	コマンドまたはアクション	目的
	<pre>Device(config-if)# sflow counter-sampling id 1 interval 15</pre>	<ul style="list-style-type: none"> • <i>collector-id</i> : 値の範囲は <1 ~ 2> にする必要があります。 • <i>interval</i> : カウンタのポーリング間隔 (秒単位、<2 ~ 86400> の範囲)。デフォルトは 10 秒です。
ステップ 4	no sflow counter-sampling 例 : <pre>Device(config-if)# no sflow counter-sampling</pre>	カウンタサンプリングを無効にします。
ステップ 5	end 例 : 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	show sflow interface 例 : <pre>Device# show sflow interface gigabitethernet1/0/2</pre>	カウンタサンプリングが有効になっているすべてのインターフェイスの sFlow 設定を表示します。
ステップ 7	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。

sFlow 設定の確認

sFlow 設定を表示し、検証するには、次のコマンドを使用します。

表 7: sFlow Show コマンド

コマンド	目的
show sflow	sFlow エージェントおよび sFlow コレクタに関するグローバル sFlow 設定を表示します。

コマンド	目的
show sflow interface	パケットサンプリングまたはカウンタサンプリングが有効になっているすべてのインターフェイスの sFlow 設定を表示します。
show sflow interface <i>interface name</i>	特定のインターフェイスの設定を表示します。
show platform sflow enables	ハードウェアレベルでのグローバル sFlow ステータスを表示します。

sFlow 統計情報のモニタリングとクリア

表 8: sFlow 統計情報のモニタリングとクリア

コマンド	説明
show sflow statistics	sFlow の統計情報を表示します。
show sflow statistics interface <i>interface name</i>	入力および出力で受信したパケットサンプル数など、特定のインターフェイスのインターフェイスレベルの統計情報を表示します。
clear sflow statistics	sFlow 統計情報をクリアします。
clear sflow statistics interface <i>interface name</i>	インターフェイスレベルの sFlow 統計情報をクリアします。

sFlow の設定例

次に、グローバルレベルで sFlow を設定する例を示します。

```
Device#configure terminal
Device(config)#sflow agent ip 10.1.1.1
Device(config)#sflow collector id 1 ip 10.1.1.2 port 6343 datagram-size 1024
Device(config)#sflow collector id 2 ip 10.1.1.3 port 6343 datagram-size 1024
```

次に、sFlow エージェントおよび sFlow コレクタに関するグローバル sFlow 設定を表示する例を示します。

```
Device#show sflow
Device#show sflow
Agent:
-----
IP : 10.1.1.1
Collector:
-----
```

```

Max number of collectors : 2
Id | Collector IP | Port | Max Datagram size
-----
1 | 10.1.1.2 | 6343 | 1024
2 | 10.1.1.3 | 6343 | 1024
Switch#

```

次に、インターフェイスレベルで sFlow を設定する例を示します。

```

Device#configure terminal
Device(config)#interface gigabitethernet1/0/15
Device(config-if)#sflow flow-sampling input id 1 rate 256 hdr-size 200
Device(config-if)#sflow flow-sampling output id 1 rate 256 hdr-size 200
Device(config-if)#sflow counter-sampling id 1 interval 15

```

次に、パケットサンプリングまたはカウンタサンプリングが有効になっているインターフェイスの sFlow 設定の出力例を示します。

```

Device#show sflow interface
In: Input direction, Out: Output direction, '0' indicates No configuration
-----
| Flow sampling |
|-----|
| Sampling Rate | HdrBytes | Coll Id | Counter Sampling |
|-----|-----|-----|-----|
Interface | In Out | In Out | In Out | Interval | Coll Id
-----
Gi1/0/15 | 1/256, 1/256 | 200, 200 | 1, 1 | 15 Sec | 1

```

sFlow の設定に関する機能情報

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 9: sFlow の設定に関する機能情報

機能名	リリース	機能情報
sFlow の設定	Cisco IOS Release 15.2(7)E1	この機能が導入されました。



第 4 章

システム メッセージ ログの設定

- システム メッセージ ログの設定に関する制約事項 (75 ページ)
- システム メッセージ ログの設定に関する情報 (75 ページ)
- システム メッセージ ログの設定方法 (78 ページ)
- システム メッセージ ログのモニタリングおよびメンテナンス (87 ページ)
- システム メッセージ ログの設定例 (88 ページ)
- システム メッセージ ログに関する追加情報 (88 ページ)
- システム メッセージ ログの機能履歴と情報 (89 ページ)

システム メッセージ ログの設定に関する制約事項

logging discriminator コマンドを設定すると、デバイスにメモリリークまたはクラッシュが発生する可能性があります。通常これは、大量のsyslogまたはデバッグが出力されているときに発生します。メモリリークのレートは、生成されるログの数によって異なります。極端なケースでは、デバイスがクラッシュすることもあります。回避するには、**no logging discriminator** コマンドを使用して、ロギングディスクリミネータを無効にします。

システム メッセージ ログの設定に関する情報

ここでは、システムメッセージログの形式、システムメッセージログのデフォルト設定、および Syslog トラップメッセージをイネーブ爾にする方法について説明します。

システム メッセージ ロギング

スイッチはデフォルトで、システム メッセージおよび **debug** 特権 EXEC コマンドの出力をロギングプロセスに送信します。ロギングプロセスはログメッセージを各宛先（設定に応じて、ログバッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ロギングプロセスは、コンソールにもメッセージを送信します。

ロギングプロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマ

ンドの出力が割り込みます。メッセージがアクティブなコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

メッセージの重大度を設定して、コンソールおよび各宛先に表示されるメッセージのタイプを制御できます。ログメッセージにタイムスタンプを設定したり、Syslog 送信元アドレスを設定したりして、リアルタイムのデバッグ機能および管理機能を強化できます。表示されるメッセージについては、このリリースに対応するシステムメッセージガイドを参照してください。

ロギングされたシステムメッセージにアクセスするには、スイッチのコマンドラインインターフェイス (CLI) を使用するか、または適切に設定された Syslog サーバにこれらのシステムメッセージを保存します。スイッチソフトウェアは Syslog メッセージをスタンドアロンスイッチの内部バッファに保存します。スイッチに障害が発生すると、フラッシュメモリに保存されていないログは失われます。

システムメッセージをリモートで監視するには、Syslog サーバ上でログを表示するか、あるいは Telnet、コンソールポート、またはイーサネット管理ポート経由でスイッチにアクセスします。



(注) Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

システム ログメッセージのフォーマット

システム ログメッセージは最大 80 文字とパーセント記号 (%)、およびその前に配置されるオプションのシーケンス番号やタイムスタンプ情報 (設定されている場合) で構成されています。スイッチに応じて、メッセージは次のいずれかの形式で表示されます。

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

パーセント記号の前にあるメッセージの部分は、次のグローバル コンフィギュレーション コマンドの設定によって異なります。

- **service sequence-numbers**
- **service timestamps log datetime**
- **service timestamps log datetime[localtime] [msec] [show-timezone]**
- **service timestamps log uptime**

表 10: システム ログメッセージの要素

要素	説明
<i>seq no:</i>	service sequence-numbers グローバル コンフィギュレーション コマンドが設定されている場合にのみ、ログメッセージにシーケンス番号をスタンプします。

要素	説明
<i>timestamp formats:</i> <i>mm/dd h h:mm:ss</i> または <i>hh:mm:ss</i> (短時間) または <i>d h</i> (長時間)	メッセージまたはイベントの日時です。この情報が表示されるのは、 service timestamps log[datetime log] グローバル コンフィギュレーション コマンドが設定されている場合のみです。
<i>facility</i>	メッセージが参照する機能 (SNMP、SYS など) です。
<i>severity</i>	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。
<i>MNEMONIC</i>	メッセージを一意に示すテキスト ストリングです。
<i>description</i>	レポートされているイベントの詳細を示すテキスト ストリングです。

デフォルトのシステムメッセージログの設定

表 11: デフォルトのシステムメッセージログの設定

機能	デフォルト設定
コンソールへのシステムメッセージログ	イネーブル
コンソールの重大度	デバッグ
ログファイル設定	ファイル名の指定なし
ログバッファサイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイムスタンプ	ディセーブル
同期ログ	ディセーブル
ログサーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	local7
サーバの重大度	Informational

Syslog トラップメッセージのイネーブリング

Syslog トラップは、**snmp-server enable traps syslog** コマンドを使用してイネーブルにすることができます。

Syslog トラップをイネーブルにしたら、トラップメッセージ重大度を指定する必要があります。**logging snmp-trap** コマンドを使用して、トラップレベルを指定します。デフォルトでは、このコマンドは重大度 0 から 4 をイネーブルにします。すべての重大度レベルをイネーブルにするには、**logging snmp-trap 0 7** コマンドを設定します。

個々のトラップレベルをイネーブルにするには、次のコマンドを設定します。

- **logging snmp-trap emergencies** : 重大度 0 のトラップのみをイネーブルにします。
- **logging snmp-trap alert** 重大度 1 のトラップのみをイネーブルにします。

Syslog トラップと一緒に、Syslog 履歴にも適用されることに注意してください。これが設定されていないと、Syslog トラップは送信されません。

logging history informational コマンドを使用して、Syslog 履歴をイネーブルにします。

システムメッセージログの設定方法

メッセージ表示宛先デバイスの設定

メッセージロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。

このタスクはオプションです。

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	logging buffered [size] 例 : Device(config)# logging buffered 8192	スイッチの内部バッファにメッセージを保存します。指定できる範囲は 4096 ~ 2147483647 バイトです。デフォルトのバッファ サイズは 4096 バイトです。 スタンドアロンスイッチに障害が発生すると、ログファイルをフラッシュメモリに保存していなかった場合、ログファイ

	コマンドまたはアクション	目的
		<p>ルは失われます。ステップ4を参照してください。</p> <p>(注) バッファ サイズを大きすぎる値に設定しないでください。他の作業に使用するメモリが不足することがあります。スイッチ上の空きプロセッサメモリを表示するには、show memory 特権 EXEC コマンドを使用します。ただし、表示される値は使用できる最大値であるため、バッファ サイズをこの値に設定しないでください。</p>
<p>ステップ 3</p>	<p>logging host</p> <p>例 :</p> <pre>Device(config)# logging 125.1.1.100</pre>	<p>UNIX Syslog サーバホストにメッセージを保存します。</p> <p><i>host</i> には、syslog サーバとして使用するホストの名前または IP アドレスを指定します。</p> <p>ログメッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。</p>
<p>ステップ 4</p>	<p>logging file flash: filename [max-file-size [min-file-size]] [severity-level-number type]</p> <p>例 :</p> <pre>Device(config)# logging file flash:log_msg.txt 4096 4096 3</pre>	<p>スタンドアロンスイッチのフラッシュメモリ内のファイルにログメッセージを格納します。</p> <ul style="list-style-type: none"> • <i>filename</i> : ログメッセージのファイル名を入力します。 • (任意) max-file-size — には、ログファイルの最大サイズを指定します。指定できる範囲は 4096 ~ 2147483647 です。デフォルトは 4096 バイトです。 • (任意) <i>min-file-size</i> : ログファイルの最小サイズを指定します。指定できる範囲は 1024 ~ 2147483647 です。デフォルトは 2048 バイトです。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) <i>severity-level-number type</i> : ログの重大度またはログタイプを指定します。重大度に指定できる範囲は0～7です。
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	terminal monitor 例 : Device# terminal monitor	現在のセッション間、非コンソール端末にメッセージを保存します。 端末パラメータ コンフィギュレーションコマンドはローカルに設定され、セッションの終了後は無効になります。デバッグメッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。

ログメッセージの同期化

特定のコンソールポート回線または仮想端末回線に対して、非送信請求メッセージおよび **debug** 特権 EXEC コマンドの出力を送信請求デバイスの出力およびプロンプトと同期させることができます。重大度に応じて非同期に出力されるメッセージのタイプを特定できます。また、端末の非同期メッセージが削除されるまで保存しておくバッファの最大数を設定することもできます。

非送信請求メッセージおよび **debug** コマンド出力の同期ロギングがイネーブルの場合、送信請求デバイス出力がコンソールに表示または印刷された後に、非送信請求デバイスからの出力が表示または印刷されます。非送信請求メッセージおよび **debug** コマンドの出力は、ユーザ入力プロンプトが返された後に、コンソールに表示されます。したがって、非送信請求メッセージおよび **debug** コマンドの出力は、送信請求デバイス出力およびプロンプトに割り込まれることはありません。非送信請求メッセージが表示された後に、コンソールはユーザプロンプトを再表示します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	グローバル 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	<p>line [console vty] line-number [ending-line-number]</p> <p>例 :</p> <pre>Device(config)# line console</pre>	<p>メッセージの同期ロギングに設定する回線を指定します。</p> <ul style="list-style-type: none"> • console : スイッチコンソールポートまたはイーサネット管理ポートでの設定を指定します。 • line vty line-number : どの vty 回線の同期ロギングをイネーブルにするかを指定します。Telnet セッションを介して行われる設定には、vty 接続を使用します。回線番号に指定できる範囲は 0 ~ 15 です。 <p>16 個の vty 回線の設定をすべて一度に変更するには、次のように入力します。</p> <pre>line vty 0 15</pre> <p>また、現在の接続に使用されている 1 つの vty 回線の設定を変更することもできます。たとえば、vty 回線 2 の設定を変更するには、次のように入力します。</p> <pre>line vty 2</pre> <p>このコマンドを入力すると、ライン コンフィギュレーション モードになります。</p>
ステップ 3	<p>logging synchronous [level [severity-level all] limit number-of-buffers]</p> <p>例 :</p> <pre>Device(config)# logging synchronous level 3 limit 1000</pre>	<p>メッセージの同期ロギングをイネーブルにします。</p> <ul style="list-style-type: none"> • (任意) level severity-level : メッセージの重大度レベルを指定します。重大度がこの値以上であるメッセージは、非同期に出力されます。値が小さいほど重大度は大きく、値が大きいほど重大度は小さくなります。デフォルトは 2 です。 • (任意) level all : 重大度に関係なく、すべてのメッセージが非同期に出力されます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> （任意） limit number-of-buffers : キューイングされる端末のバッファ数を指定します。これを超える新しいメッセージは廃棄されます。指定できる範囲は 0 ~ 2147483647 です。デフォルトは 20 です。
ステップ 4	end 例 : Device (config) # end	特権 EXEC モードに戻ります。

メッセージロギングのディセーブル化

メッセージロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージロギングをイネーブルにする必要があります。メッセージロギングがイネーブルの場合、ログメッセージはロギングプロセスに送信されます。ロギングプロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

ロギングプロセスをディセーブルにすると、メッセージがコンソールに書き込まれるまでプロセスは処理続行を待機する必要があるため、スイッチの処理速度が低下することがあります。ロギングプロセスがディセーブルの場合、メッセージは生成後すぐに（通常はコマンド出力に割り込む形で）コンソールに表示されます。

logging synchronous グローバルコンフィギュレーションコマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、**Return**を押さなければメッセージが表示されません。

メッセージロギングをディセーブルにした後に再びイネーブルにするには、**logging on** 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。

このタスクはオプションです。

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。

	コマンドまたはアクション	目的
ステップ 2	no logging console 例： Device(config)# no logging console	メッセージ ロギングをディセーブルにします。
ステップ 3	end 例： Device(config)# end	特権 EXEC モードに戻ります。

ログメッセージのタイムスタンプのイネーブル化およびディセーブル化

デフォルトでは、ログメッセージにはタイムスタンプが適用されません。

このタスクはオプションです。

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	次のいずれかのコマンドを使用します。 <ul style="list-style-type: none"> • service timestamps log uptime • service timestamps log datetime[msec localtime show-timezone] 例： Device (config)# service timestamps log uptime または Device (config)# service timestamps log datetime	ログのタイムスタンプをイネーブルにします。 <ul style="list-style-type: none"> • log uptime : ログメッセージのタイムスタンプをイネーブルにして、システムの再起動以降の経過時間を表示します。 • log datetime : ログメッセージのタイムスタンプをイネーブルにします。選択したオプションに応じて、ローカル タイムゾーンを基準とした日付、時間（ミリ秒）、タイムゾーン名をタイムスタンプとして表示できます。

	コマンドまたはアクション	目的
ステップ 3	end 例： Device (config) # end	特権 EXEC モードに戻ります。

ログメッセージのシーケンス番号のイネーブル化およびディセーブル化

タイムスタンプが同じログメッセージが複数ある場合、これらのメッセージを表示するには、シーケンス番号を使用してメッセージを表示できます。デフォルトでは、ログメッセージにシーケンス番号は表示されません。

このタスクはオプションです。

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	service sequence-numbers 例： Device (config) # service sequence-numbers	シーケンス番号をイネーブルにします。
ステップ 3	end 例： Device (config) # end	特権 EXEC モードに戻ります。

メッセージ重大度の定義

メッセージの重大度を指定して、選択したデバイスに表示されるメッセージを制限します。

このタスクはオプションです。

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	logging console level 例 : Device(config)# logging console 3	コンソールに保存するメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 3	logging monitor level 例 : Device(config)# logging monitor 3	端末回線に出力するメッセージを制限します。 デフォルトで、端末はデバッグメッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 4	logging trap level 例 : Device(config)# logging trap 3	Syslog サーバに保存するメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

履歴テーブルおよび SNMP に送信される syslog メッセージの制限

このタスクでは、履歴テーブルおよび SNMP に送信される syslog メッセージを制限する方法について説明します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	グローバル 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	logging history level 例 : Device(config)# logging history 3	履歴ファイルに保存され、SNMPサーバに送信される syslog メッセージのデフォルトレベルを変更します。 デフォルトでは warnings 、 errors 、 critical 、 alerts 、および emergencies メッセージは送信されません。
ステップ 3	logging history size number 例 : Device(config)# logging history size 200	履歴テーブルに保存できる Syslog メッセージの数を指定します。 デフォルトでは1つのメッセージが格納されます。指定できる範囲は0～500です。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

UNIX Syslog デーモンへのメッセージのロギング

このタスクはオプションです。



- (注) 最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。このようなシステムの場合に、Syslog メッセージのリモートロギングをイネーブルにするには、Syslog コマンドラインに追加または削除する必要があるオプションを、UNIX の **man syslogd** コマンドを使用して判別します。

始める前に

- root としてログインします。
- システム ログメッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>/etc/syslog.conf ファイルに次の行を追加します。</p> <p>例 :</p> <pre>local7.debug /usr/adm/logs/cisco.log</pre>	<ul style="list-style-type: none"> • local7 : ログ機能指定します。 • debug : syslog レベルを指定します。このファイルは、syslog デーモンに書き込み権限がある既存ファイルである必要があります。
ステップ 2	<p>UNIX シェルプロンプトに次のコマンドを入力します。</p> <p>例 :</p> <pre>\$ touch /var/log/cisco.log \$ chmod 666 /var/log/cisco.log</pre>	<p>ログファイルを作成します。syslog デーモンは、このレベルまたはこのファイルのより高い重大度レベルでメッセージを送信します。</p>
ステップ 3	<p>Syslog デーモンに新しい設定を認識させます。</p> <p>例 :</p> <pre>\$ kill -HUP `cat /etc/syslog.pid`</pre>	<p>詳細については、ご使用の UNIX システムの man syslog.conf および man syslogd コマンドを参照してください。</p>

システムメッセージログのモニタリングおよびメンテナンス

コンフィギュレーションアーカイブログのモニタリング

コマンド	目的
<pre>show archive log config {all number [end-number] user username [session number] number [end-number] statistics} [provisioning]</pre>	<p>コンフィギュレーションログ全体、または指定されたパラメータのログを表示します。</p>

システムメッセージログの設定例

例：スイッチシステムメッセージ

次に、スイッチ上のスイッチシステムメッセージの一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

例：サービスタイムスタンプログの表示

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のロギング表示（一部）の例を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
(Switch-2)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のロギング表示（一部）の例を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell, changed state to up (Switch-2)
```

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)
```

システムメッセージログに関する追加情報

関連資料

関連項目	マニュアルタイトル
システムメッセージログ コマンド	<i>Catalyst 2960-L</i> スイッチシステム管理コマンドリファレンス
プラットフォームに依存しないコマンドリファレンス	<i>Cisco IOS 15.3M&T</i> コマンドリファレンス

関連項目	マニュアルタイトル
プラットフォームに依存しない設定情報	<i>Cisco IOS 15.3M&T</i> コンフィギュレーションガイド

システムメッセージログの機能履歴と情報

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。

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 12: システムメッセージログの機能履歴と情報

機能	リリース	機能情報
システムメッセージログ	Cisco IOS Release 15.2(7)E1	この機能が導入されました。



第 5 章

オンライン診断の設定

- [オンライン診断の設定に関する情報 \(91 ページ\)](#)
- [オンライン診断の設定方法 \(92 ページ\)](#)
- [オンライン診断のモニタリングおよびメンテナンス \(97 ページ\)](#)
- [オンライン診断テストの設定例 \(97 ページ\)](#)
- [オンライン診断の機能履歴と情報 \(102 ページ\)](#)

オンライン診断の設定に関する情報

オンライン診断

オンライン診断機能を使用すると、デバイスをアクティブネットワークに接続したまま、デバイスのハードウェア機能をテストして確認できます。

オンライン診断には、異なるハードウェアコンポーネントをチェックするパケット交換テストが含まれ、データパスおよび制御信号が確認されます。

オンライン診断では、次の領域の問題が検出されます。

- ハードウェア コンポーネント
- インターフェイス (イーサネットポートなど)
- はんだ接合

オンライン診断は、オンデマンド診断、スケジュール診断、ヘルスマニタリング診断に分類できます。オンデマンド診断は、CLIから実行されます。スケジュールされた診断は、動作中のネットワークにデバイスが接続されているときに、ユーザが指定した間隔または指定した時刻に実行されます。ヘルスマニタリングは、バックグラウンドでユーザが指定した間隔で実行されます。デフォルトでは、30 秒ごとにヘルスマニタリングテストが実行されます。

オンライン診断を設定したあと、手動で診断テストを開始したり、テスト結果を表示したりできます。また、デバイスに設定されているテストの種類、およびすでに実行された診断テスト名を確認できます。



(注) Catalyst 2960L スイッチはスタックできません。そのため、このスイッチでは **switch number** キーワードがサポートされていません。

オンライン診断の設定方法

オンライン診断テストの開始

スイッチで実行する診断テストを設定したあと、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テストプロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	diagnostic start test { <i>name</i> <i>test-id</i> <i>test-id-range</i> all basic non-disruptive } 例 : Device# diagnostic start test basic	診断テストを開始します。 次のいずれかのオプションを使用してテストを指定できます。 <ul style="list-style-type: none"> • name : テストの名前を入力します。 • test-id : テストの ID 番号を入力します。 • test-id-range : カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。 • all : すべてのテストを開始します。 • basic : 基本テストスイートを開始します。 • non-disruptive : ノンディスラプティブテストスイートを開始します。

オンライン診断の設定

診断モニタリングをイネーブルにする前に、障害しきい値およびテストの間隔を設定する必要があります。

オンライン診断のスケジューリング

特定のスイッチについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	<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 2	<p>diagnostic schedule test {<i>name</i> <i>test-id</i> <i>test-id-range</i> all basic non-disruptive } {daily on <i>mm dd yyyy hh:mm</i> weekly <i>day-of-week hh:mm</i>}</p> <p>例 :</p> <pre>Device(config)# diagnostic schedule test 1-5 on July 3 2013 23:10</pre>	<p>特定日時のオンデマンド診断テストをスケジュールします。</p> <p>スケジュールするテストを指定する場合は、次のオプションを使用します。</p> <ul style="list-style-type: none"> • name : show diagnostic content コマンドの出力に表示されるテストの名前です。 • test-id : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • test-id-range : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • all : すべてのテスト ID。 • basic : 基本的なオンデマンドの診断テストを開始します。 • non-disruptive : ノンディスラプティブテストスイートを開始します。 <p>テストは次のようにスケジュールできます。</p> <ul style="list-style-type: none"> • 毎日 : daily <i>hh:mm</i> パラメータを使用します。 • 特定日時 : on <i>mm dd yyyy hh:mm</i> パラメータを使用します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 毎週：weekly day-of-week hh:mm パラメータを使用します。

ヘルス モニタリング診断の設定

デバイスが稼働中のネットワークに接続されている間に、スイッチに対しヘルスモニタリング診断テストを設定できます。各ヘルスモニタリングテストの実行間隔を設定したり、デバイスをイネーブルにし、テスト失敗時の Syslog メッセージを生成したり、特定のテストをイネーブルにできます。

テストをディセーブルにするには、コマンドの **no** 形式を入力します。

デフォルトでは、ヘルスモニタリングはディセーブルですが、デバイスはテストの失敗時に Syslog メッセージを生成します。

ヘルス モニタリング診断テストを設定し、イネーブルにするには、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。 <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	diagnostic monitor interval test {name test-id test-id-range all} hh:mm:ss milliseconds day 例： Device(config)# diagnostic monitor interval test 1 12:30:00 750 5	指定のテストに対し、ヘルス モニタリングの実行間隔を設定します。 テストを指定する場合は、次のいずれかのパラメータを使用します。 <ul style="list-style-type: none"> name：show diagnostic content コマンドの出力に表示されるテストの名前です。 test-id：show diagnostic content コマンドの出力に表示されるテストの ID 番号です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • test-id-range : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • all : すべての診断テスト。 <p>間隔を指定する場合は、次のパラメータを設定します。</p> <ul style="list-style-type: none"> • hh:mm:ss : モニタリング間隔 (時間、分、秒)。指定できる範囲は hh が 0~24、mm および ss が 0~60 です。 • milliseconds : モニタリング間隔 (ミリ秒 (ms))。指定できる範囲は 0~999 です。 • day : モニタリング間隔 (日数)。指定できる範囲は 0~20 です。
<p>ステップ 4</p>	<p>diagnostic monitor syslog</p> <p>例 :</p> <pre>Device(config)# diagnostic monitor syslog</pre>	<p>(任意) ヘルス モニタリング テストの失敗時にスイッチが Syslog メッセージを生成するように設定します。</p>
<p>ステップ 5</p>	<p>diagnostic monitor threshold number test {name test-id test-id-range all} failure count count</p> <p>例 :</p> <pre>Device(config)# diagnostic monitor threshold test 1 failure count 20</pre>	<p>(任意) ヘルス モニタリング テストの失敗しきい値を設定します。</p> <p>テストを指定する場合は、次のいずれかのパラメータを使用します。</p> <ul style="list-style-type: none"> • name : show diagnostic content コマンドの出力に表示されるテストの名前です。 • test-id : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • test-id-range : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • all : すべての診断テスト。 <p>失敗しきい値 count に指定できる範囲は 0~99 です。</p>

	コマンドまたはアクション	目的
ステップ 6	diagnostic monitor test { <i>name</i> <i>test-id</i> <i>test-id-range</i> all } 例 : Device (config) # diagnostic monitor test 1	指定のヘルス モニタリング テストをイネーブルにします。 switch number キーワードは、スタック構成スイッチだけでサポートされます。 テストを指定する場合は、次のいずれかのパラメータを使用します。 <ul style="list-style-type: none"> • name : show diagnostic content コマンドの出力に表示されるテストの名前です。 • test-id : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • test-id-range : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • all : すべての診断テスト。
ステップ 7	end 例 : Device (config) # end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
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。

次のタスク

no diagnostic monitor interval test{*test-id* | *test-id-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、間隔をデフォルトの値またはゼロに変更します。 **no diagnostic monitor syslog** コマンドを使用し、ヘルスマニタリングテストが失敗した場合の Syslog メッセージの生

成をディセーブルにします。**diagnostic monitor threshold test***test-id | test-id-range* }**failure count** コマンドを使用し、失敗しきい値を削除します。

オンライン診断のモニタリングおよびメンテナンス

オンライン診断テストとテスト結果の表示

デバイスに設定されているオンライン診断テストを表示し、この表に示す **show** 特権 EXEC コマンドを使用してテスト結果を確認することができます。

表 13: 診断テストの設定および結果用のコマンド

コマンド	目的
show diagnostic content	スイッチに対して設定されたオンライン診断を表示します。
show diagnostic status	現在実行中の診断テストを表示します。
show diagnostic result switch [<i>number</i> all] [detail test { <i>name</i> <i>test-id</i> <i>test-id-range</i> all } [detail]]	オンライン診断テストの結果を表示します。
show diagnostic detail	オンライン診断テストの結果を表示します。
show diagnostic schedule	オンライン診断テストのスケジュールを表示します。
show diagnostic post	POST 結果を表示します（出力は show post コマンドの出力と同じ）。

オンライン診断テストの設定例

オンライン診断テストの開始

スイッチで実行する診断テストを設定したあと、**diagnostic start** 特権 EXEC コマンドを使用して診断テストを開始します。

テストを開始したら、テストプロセスの停止はできません。

手動でオンライン診断テストを開始するには、次の特権 EXEC コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	diagnostic start test { <i>name</i> <i>test-id</i> <i>test-id-range</i> all basic non-disruptive } 例： Device# diagnostic start test basic	診断テストを開始します。 次のいずれかのオプションを使用してテストを指定できます。 <ul style="list-style-type: none"> • name : テストの名前を入力します。 • test-id : テストの ID 番号を入力します。 • test-id-range : カンマとハイフンで区切ってテスト ID の範囲を整数で入力します。 • all : すべてのテストを開始します。 • basic : 基本テストスイートを開始します。 • non-disruptive : ノンディスラプティブテストスイートを開始します。

例：ヘルス モニタリング テストの設定

次に、ヘルス モニタリング テストを設定する例を示します。

```
Device(config)# diagnostic monitor threshold test 1 failure count 50
Device(config)# diagnostic monitor interval test TestPortAsicLoopback
```



(注) Catalyst 2960L スイッチはスタックできません。そのため、このスイッチでは **switch number** キーワードがサポートされていません。

オンライン診断のスケジューリング

特定のスイッチについて指定した時間、または日、週、月単位でオンライン診断をスケジューリングできます。スケジューリングを削除するには、コマンドの **no** 形式を入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	<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 2	<p>diagnostic schedule test {<i>name</i> <i>test-id</i> <i>test-id-range</i> all basic non-disruptive } {daily on <i>mm dd yyyy hh:mm</i> weekly <i>day-of-week hh:mm</i>}</p> <p>例 :</p> <pre>Device(config)# diagnostic schedule test 1-5 on July 3 2013 23:10</pre>	<p>特定日時のオンデマンド診断テストをスケジューリングします。</p> <p>スケジューリングするテストを指定する場合は、次のオプションを使用します。</p> <ul style="list-style-type: none"> • name : show diagnostic content コマンドの出力に表示されるテストの名前です。 • test-id : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • test-id-range : show diagnostic content コマンドの出力に表示されるテストの ID 番号です。 • all : すべてのテスト ID。 • basic : 基本的なオンデマンドの診断テストを開始します。 • non-disruptive : ノンディスラプティブテストスイートを開始します。 <p>テストは次のようにスケジューリングできます。</p> <ul style="list-style-type: none"> • 毎日 : daily <i>hh:mm</i> パラメータを使用します。 • 特定日時 : on <i>mm dd yyyy hh:mm</i> パラメータを使用します。 • 毎週 : weekly <i>day-of-week hh:mm</i> パラメータを使用します。

オンライン診断の表示 : 例

次の例では、スイッチのオンライン診断の詳細情報を表示する方法を示します。

```
Device# show diagnostic switch detail

:   SerialNo :

Overall Diagnostic Result : UNTESTED

Test results: (. = Pass, F = Fail, U = Untested)

-----

1) TestPortAsicLoopback -----> U

    Error code -----> 3 (DIAG_SKIPPED)
    Total run count -----> 0
    Last test testing type -----> n/a
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0

-----

2) TestPortAsicCam -----> U

    Error code -----> 3 (DIAG_SKIPPED)
    Total run count -----> 0
    Last test testing type -----> n/a
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0

-----

3) TestPortAsicMem -----> U

    Error code -----> 3 (DIAG_SKIPPED)
    Total run count -----> 0
    Last test testing type -----> n/a
    Last test execution time -----> n/a
    First test failure time -----> n/a
    Last test failure time -----> n/a
    Last test pass time -----> n/a
    Total failure count -----> 0
    Consecutive failure count -----> 0

-----
```

次の例では、スイッチに設定されているオンライン診断を表示する方法を示します。

```
Device# show diagnostic content

:

Diagnostics test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
```



```

D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive
R/* - Switch will reload after test list completion / NA
P/* - will partition stack / NA
    
```

ID	Test Name	Attributes	Test Interval day hh:mm:ss.ms	Three- day shold
1)	TestPortAsicLoopback	B*D*X**IR*	not configured	n/a
2)	TestPortAsicCam	B*D*X**IR*	not configured	n/a
3)	TestPortAsicMem	B*D*X**IR*	not configured	n/a

次の例では、スイッチのオンライン診断結果を表示する方法を示します。

```

Device# show diagnostic result

: SerialNo :

Overall Diagnostic Result : UNTESTED

Test results: (. = Pass, F = Fail, U = Untested)

1) TestPortAsicLoopback -----> U
2) TestPortAsicCam -----> U
3) TestPortAsicMem -----> U
    
```

次の例では、オンライン診断テストのステータスを表示する方法を示します。

```

Device# show diagnostic status

<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics

=====
Card   Description                               Current Running Test           Run by
-----
                                             N/A                             N/A
=====

Switch#
    
```

次の例では、スイッチのオンライン診断のテストスケジュールを表示する方法を示します。

```

Device# show diagnostic schedule

Current Time = 17:06:07 IST Tue Sep 11 2018

Diagnostic is not scheduled.
    
```

オンライン診断の機能履歴と情報

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。

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 14: オンライン診断の機能履歴と情報

機能	リリース	機能情報
オンライン診断	Cisco IOS Release 15.2(7)E1	この機能が導入されました。



第 6 章

Dying Gasp の設定

このドキュメントでは、Dying Gasp 機能について説明します。この機能は、突然の停電をホストプラットフォームに報告するために、SNMP、Syslog、またはイーサネットの運用、管理、保守（OAM）を介して Dying Gasp メッセージを送信するために使用されます。

- [Dying Gasp の設定に関する制約事項](#)（103 ページ）
- [Dying Gasp の設定について](#)（103 ページ）
- [Dying Gasp の設定方法](#)（104 ページ）
- [Dying Gasp の設定例](#)（105 ページ）
- [Dying Gasp に関するその他の参考資料](#)（106 ページ）
- [Dying Gasp の機能履歴](#)（106 ページ）

Dying Gasp の設定に関する制約事項

- この機能は、ギガビットイーサネットダウンリンクポートを備えたスタンドアロンスイッチでのみサポートされます。
- イーサネットの運用、管理、保守（OAM）は、Catalyst 1000 シリーズスイッチではサポートされていません。

Dying Gasp の設定について

ここでは、Dying Gasp について説明します。

Dying Gasp の概要

Dying Gasp は、リセットまたは電源障害によりデバイスがダウンしようとしているときに生成される信号/アラートです。システムは、電源障害が発生した後、管理者またはユーザに通知する Dying Gasp メッセージを送信するために十分な残存電力を保持します。ネットワークデバイスは、グレースフルシャットダウンと Dying Gasp メッセージの生成を可能にする、コン

デンサでの一時的なバックアップ電源に依存しています。この一時的な電源は、これらのタスクを実行するために、10～20 ミリ秒持続するように設計されています。

Dying Gasp パケットは、**dyling-gasp** コンフィギュレーション コマンドを使用してホストを設定すると作成されます。**show dying-gasp packets** コマンドを実行すると、作成されたパケットに関する詳細情報が表示されます。

SNMP Dying Gasp メッセージの SNMP サーバは、**snmp-server host** コマンドを使用して指定します。Syslog Dying Gasp メッセージを送信する Syslog サーバは、**logging host hostname/ipv6address transport udp** コマンドを使用して指定します。

Dying Gasp パケットは、通知タイプごとに最大 5 台のサーバに送信できます。

Dying Gasp の設定方法

ここでは、Dying Gasp の設定方法について説明します。

Dying Gasp の設定

Dying Gasp 通知をイネーブルにするには、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	dyling-gasp primary {ethernet-oam snmp-trap syslog} secondary {ethernet-oam snmp-trap syslog} 例： Device(config)# dyling-gasp primary syslog secondary snmp-trap	Dying Gasp プライマリ通知をイネーブルにします。 • ethernet-oam : イーサネット OAM 通知をイネーブルにします。 (注) このキーワードは、Catalyst 1000 シリーズ スイッチではサポートされていません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • snmp-trap : SNMP サーバに送信されるトラップ通知をイネーブルにします。 • syslog : システムロガーをイネーブルにします。 • secondary : Dying Gasp セカンダリ通知をイネーブルにします。
ステップ 4	exit 例 : Device(config)# exit	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 5	show dying-gasp status 例 : Device# show dying-gasp status	(任意) Dying Gasp の設定を表示します。

Dying Gasp の設定例

ここでは、Dying Gasp の設定方法の例を示します。

例 : Dying Gasp の設定

次に、SNMP トラップをプライマリ通知として設定し、syslog をセカンダリ通知として設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dying-gasp primary snmp-traps secondary syslog
```

次に、**show dying-gasp status** コマンドの出力例を示します。

```
Device# show dying-gasp status

Dying Gasp Configuration
SNMP Trap Enabled
Syslog Enabled
Ethernet OAM Disabled
```

次に、**show dying-gasp packets snmp-trap** コマンドの出力例を示します。

```
Device# show dying-gasp packets snmp-trap

SNMP Trap packet for server 10.1.1.2, link type IP
Interface, via GigabitEthernet1/0/0, local IP address 10.2.2.9
```

```
Encap type is ARPA, local hardware address 0022.bdd4.2f48
Next hop IP address 10.2.2.8, next hop hardware address 0000.0c07.ac09
SNMP Trap packet for server 10.1.1.4, link type IP
Interface, via GigabitEthernet1/0/1, local IP address 10.2.2.7
Encap type is ARPA, local hardware address 0012.001a.2f08
Next hop IP address 10.2.2.8, next hop hardware address 0cd0.0c02.ac10
```

Dying Gasp に関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
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。	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches)

Dying Gasp 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 リリース 15.2(7)E2	Dying Gasp	Dying Gasp は、リセットまたは電源障害によりデバイスがダウンしようとしているときに生成される信号/アラートです。

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

Cisco IOS ファイルシステム、コンフィギュレーションファイル、およびソフトウェアイメージの操作

- [フラッシュファイルシステムの操作 \(107 ページ\)](#)
- [設定ファイルの取り扱い \(116 ページ\)](#)
- [コンフィギュレーションの交換およびロールバック \(129 ページ\)](#)
- [ソフトウェアイメージの操作 \(134 ページ\)](#)
- [TFTP によるイメージファイルのコピー \(136 ページ\)](#)
- [FTP によるイメージファイルのコピー \(140 ページ\)](#)
- [RCP によるイメージファイルのコピー \(145 ページ\)](#)

フラッシュ ファイル システムの操作

フラッシュ ファイル システムについて

フラッシュファイルシステムは、ファイルを格納できる単一のフラッシュデバイスです。ソフトウェアバンドルおよびコンフィギュレーションファイルの管理に役立つ複数のコマンドも備えています。デバイスのデフォルトのフラッシュファイルシステムは `flash:` です。

アクティブなスイッチから見ると、`flash:` はローカルフラッシュデバイスを指します。これは、ファイルシステムが表示されているのと同じスイッチに接続されているデバイスです。

一度に1人のユーザのみが、ソフトウェアバンドルおよびコンフィギュレーションファイルを管理できます。

使用可能なファイル システムの表示

デバイスで使用可能なファイルシステムを表示するには、`show file systems` 特権 EXEC コマンドを使用します (次のスタンドアロンデバイスの例を参照)。

```

Device# show file systems
File Systems:
      Size(b)   Free(b)      Type   Flags  Prefixes
*    15998976   5135872     flash  rw     flash:
      -         -           opaque rw     bs:
      -         -           opaque rw     vb:
      524288    520138     nvram   rw     nvram:
      -         -           network rw     tftp:
      -         -           opaque rw     null:
      -         -           opaque rw     system:
      -         -           opaque ro     xmodem:
      -         -           opaque ro     ymodem:

```

表 15: *show file systems* のフィールドの説明

フィールド	値
Size(b)	ファイル システムのメモリ サイズ (バイト単位) です。
Free(b)	ファイル システムの空きメモリ サイズ (バイト単位) です。
Type	<p>ファイル システムのタイプです。</p> <p>disk : ファイル システムは、フラッシュ メモリ デバイス、USB フラッシュ、crashinfo ファイル用です。</p> <p>network : ファイル システムは、FTP サーバや HTTP サーバなどのネットワーク デバイス用です。</p> <p>nvram : ファイル システムは NVRAM (不揮発性 RAM) デバイス用です。</p> <p>opaque : ファイル システムは、ローカルに生成された pseudo ファイル システム (system など)、またはダウンロード インターフェイス (brimux など) です。</p> <p>unknown : ファイル システムのタイプは不明です。</p>
Flags	<p>ファイル システムの権限です。</p> <p>ro : 読み取り専用です。</p> <p>rw : 読み取りおよび書き込みです。</p> <p>wo : 書き込み専用です。</p>

フィールド	値
Prefixes	<p>ファイル システムのエイリアスです。</p> <p>crashinfo : crashinfo ファイルです。</p> <p>flash : フラッシュ ファイル システムです。</p> <p>ftp : FTP サーバです。</p> <p>http : HTTP サーバです。</p> <p>https : セキュア HTTP サーバです。</p> <p>nvr : NVRAM です。</p> <p>null : コピーのヌル宛先です。リモート ファイルをヌルへコピーして、サイズを判別できます。</p> <p>rcp : Remote Copy Protocol (RCP) サーバです。</p> <p>scp : Session Control Protocol (SCP) サーバです。</p> <p>system : 実行コンフィギュレーションを含むシステムメモリが格納されています。</p> <p>tftp : TFTP ネットワーク サーバです。</p> <p>usbflash0 : USB フラッシュ メモリです。</p> <p>xmodem : XMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。</p> <p>ymodem : YMODEM プロトコルを使用して、ネットワーク マシンからファイルを取得します。</p>

デフォルト ファイル システムの設定

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd filesystem:** 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに **filesystem:** 引数を省略できます。たとえば、オプションの **filesystem:** 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは **flash:** です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システムのファイルに関する情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同

じ名前のコンフィギュレーションファイルが格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、ファイル名を確認して、その名前を別のコマンドで使用できます。ファイルシステムのファイルに関する情報を表示するには、次の表に記載する特権 EXEC コマンドのいずれかを使用します。

表 16: ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [/all] [filesystem:filename]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information file-url	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子のリストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリを変更し、作業ディレクトリを表示するには、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	dir filesystem: 例： Device# dir flash:	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。 <i>filesystem:</i> には、システム ボードのフラッシュ デバイスの <i>flash:</i> を使用します。
ステップ 3	cd directory_name 例： Device# cd new_configs	指定されたディレクトリへ移動します。 コマンド例では、 <i>new_configs</i> という名前のディレクトリに移動する方法を示します。

	コマンドまたはアクション	目的
ステップ 4	pwd 例 : Device# pwd	作業ディレクトリを表示します。
ステップ 5	cd 例 : Device# cd	デフォルトディレクトリに移動します。

ディレクトリの作成

特権 EXEC モードを開始して、ディレクトリを作成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	dir filesystem: 例 : Device# dir flash:	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。 <i>filesystem:</i> には、システム ボードのフラッシュ デバイスの flash: を使用します。
ステップ 2	mkdir directory_name 例 : Device# mkdir new_configs	新しいディレクトリを作成します。スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、スラッシュ、引用符、セミコロン、またはコロンは使用できません。
ステップ 3	dir filesystem: 例 : Device# dir flash:	入力を確認します。

ディレクトリの削除

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force /recursive filesystem:/file-url** 特権 EXEC コマンドを使用します。

名前指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。

filesystem には、システム ボードのフラッシュ デバイスの **flash:** を使用します。*file-url* には、削除するディレクトリの名前を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意 ディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

送信元から宛先にファイルをコピーするには、**copy source-url destination-url** 特権 EXEC コマンドを使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワードショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドは、現在実行中のコンフィギュレーション ファイルをフラッシュメモリの NVRAM セクションに保存し、システム初期化の際にコンフィギュレーションファイルとして使用されるようにします。

XMODEM または YMODEM プロトコルを使用するネットワーク マシンのファイルに対する送信元として特殊なファイルシステム (**xmodem:**、**ymodem:**) を指定し、そこからコピーすることもできます。

ネットワーク ファイルシステムの URL には、ftp:、rcp:、tftp:、scp:、http:、https: などがあり、構文は次のとおりです。

- FTP : ftp:[[/username [:password]@location]/directory]/filename
- RCP : rcp:[[/username@location]/directory]/filename
- TFTP : tftp:[[/location]/directory]/filename
- SCP : scp:[[/username [:password]@location]/directory]/filename
- HTTP : http:[[/username [:password]@location]/directory]/filename
- HTTPS : https:[[/username [:password]@location]/directory]/filename



(注) パスワードに特殊文字「@」を含めることはできません。文字「@」を使用すると、コピーでサーバの IP アドレスを解析できません。

ローカルにある書き込み可能なファイル システムには **flash:** などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスに (たとえば、**copy flash: flash:** コマンドは無効)

ファイルの削除

フラッシュ メモリ デバイスのファイルが不要になった場合は、そのファイルを永久に削除できます。指定されたフラッシュ デバイスからファイルまたはディレクトリを削除するには、**delete [/force] [/recursive] [filesystem:]/file-url** 特権 EXEC コマンドを使用します。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem: オプションを省略すると、デバイスは **cd** コマンドで指定したデフォルトのデバイスを使用します。*file-url* には、削除するファイルのパス (ディレクトリ) および名前を指定します。

ファイルを削除しようとする時、削除の確認を求めるプロンプトが表示されます。



注意 ファイルが削除された場合、その内容は回復できません。

ここでは、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する例を示します。

```
Device# delete myconfig
```

ファイルの作成、表示、および抽出

ファイルを作成してそこにファイルを書き込んだり、ファイル内のファイルをリスト表示したり、ファイルからファイルを抽出したりできます (次の項を参照)。

ファイルの作成、内容の表示、およびファイルの抽出を行うには、特権 EXEC コマン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	archive tar /create destination-url flash: /file-url 例 : <pre>Device# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</pre>	ファイルを作成し、そこにファイルを追加します。 <i>destination-url</i> には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成するファイルの名前を指定します。 <ul style="list-style-type: none"> ローカルフラッシュファイルシステム構文

	コマンドまたはアクション	目的
		<p>flash:</p> <ul style="list-style-type: none"> • FTP 構文 <code>ftp://username[:password]@location/directory/-filename.</code> • RCP 構文 <code>rnp://username@location/directory/-filename.</code> • TFTP 構文 <code>tftp://location/directory/-filename.</code> <p>flash:/file-urlには、ローカルフラッシュファイルシステム上の、新しいファイルが作成される場所を指定します。送信元ディレクトリ内に格納されている任意のファイルまたはディレクトリの一覧を指定して、新しいファイルに追加することもできます。何も指定しないと、このレベルにおけるすべてのファイルおよびディレクトリが、新規に作成されたファイルに書き込まれます。</p>
ステップ 2	<p>archive tar /table source-url</p> <p>例 :</p> <pre>Device# archive tar /table flash: /new_configs</pre>	<p>ファイルの内容を表示します。</p> <p><i>source-url</i>には、ローカルファイルシステムまたはネットワーク ファイルシステムの送信元 URL エイリアスを指定します。<i>-filename.</i> は、表示するファイルです。次のオプションがサポートされています。</p> <ul style="list-style-type: none"> • ローカルフラッシュファイルシステム構文 <p>flash:</p> <ul style="list-style-type: none"> • FTP 構文 <code>ftp://username[:password]@location/directory/-filename.</code> • RCP 構文 <code>rnp://username@location/directory/-filename.</code> • TFTP 構文 <code>tftp://location/directory/-filename.</code> <p>ファイルのあとにファイルまたはディレクトリのリストを指定して、ファイルの表示を制限することもできます。指定したファイルだけが表示されます。何も指</p>

	コマンドまたはアクション	目的
		定しないと、すべてのファイルおよびディレクトリが表示されます。
ステップ 3	archive tar /xtract source-url flash:/file-url [dir/file...] 例 : <pre>Device# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs</pre>	<p>ファイルをフラッシュ ファイル システム上のディレクトリに抽出します。</p> <p><i>source-url</i> には、ローカルファイルシステムの送信元 URL のエイリアスを指定します。-<i>filename.</i> は、ファイルの抽出元のファイルです。次のオプションがサポートされています。</p> <ul style="list-style-type: none"> ローカルフラッシュファイルシステム構文 <p>flash:</p> <ul style="list-style-type: none"> FTP 構文 ftp:[//<i>username</i>[<i>password</i>]@<i>location</i>]/<i>directory</i>]-<i>filename.</i> RCP 構文 rtp:[//<i>username</i>@<i>location</i>]/<i>directory</i>]-<i>filename.</i> TFTP 構文 tftp:[//<i>location</i>]/<i>directory</i>]-<i>filename.</i> <p>flash:/file-url [dir/file...] には、ファイルの抽出元にするローカルフラッシュファイルシステム上の場所を指定します。抽出対象のファイル内のファイルまたはディレクトリのリストを指定するには、<i>dir/file...</i> オプションを使用します。何も指定されないと、すべてのファイルとディレクトリが抽出されます。</p>
ステップ 4	more [/ascii /binary /ebcdic] /file-url 例 : <pre>Device# more flash:/new-configs</pre>	<p>リモートファイルシステム上のファイルを含めて、読み取り可能なファイルの内容を表示します。</p>

設定ファイルの取り扱い

コンフィギュレーション ファイルに関する情報

コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。基本的なコンフィギュレーション ファイルを作成するには、`setup` プログラムを使用するか、または `setup` 特権 EXEC コマンドを使用します。

TFTP、FTP、または RCP サーバから、スイッチの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコンフィギュレーション ファイルをコピー（ダウンロード）できます。次のいずれかの目的でこの操作が必要になります。

- バックアップ コンフィギュレーション ファイルを復元するため。
- コンフィギュレーション ファイルを別のスイッチに使用するため。たとえば、ネットワークに別のスイッチを追加して、元のスイッチと同じ設定にできます。ファイルを新しいスイッチにコピーすると、ファイル全体を再作成しないで、関連部分を変更できます。
- すべてのスイッチのコンフィギュレーションが同じになるように、ネットワーク内のすべてのスイッチに同じコンフィギュレーション コマンドをロードするため。

スイッチからファイル サーバにコンフィギュレーション ファイルをコピー（アップロード）するには、TFTP、FTP、または RCP を使用します。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておく、後でサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成すると、スイッチを設定するときに役立ちます。コンフィギュレーション ファイルには、1 台または複数のスイッチを設定する場合に必要なコマンドの一部、またはすべてを格納できます。たとえば、同じハードウェア構成の複数のスイッチに、同じコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- スイッチを最初に設定する場合、コンソールポートまたはイーサネット管理ポートから接続することを推奨します。コンソールポートまたはイーサネット管理ポートとの直接接続ではなく、ネットワーク接続を介してスイッチにアクセスする場合は、設定の変更（スイッチの IP アドレスの変更やポートのディセーブル化など）によっては、スイッチとの接続が切断される可能性があることにご注意ください。

- スイッチにパスワードが設定されていない場合は、**enable secret secret-password** 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、パスワードを設定することを推奨します。



(注) **copy {ftp: | rcp: | tftp:} system:running-config** 特権 EXEC コマンドを実行すると、コマンドラインにコマンドを入力した場合と同様に、スイッチにコンフィギュレーション ファイルがロードされます。コマンドを追加するまで、既存の実行コンフィギュレーションは消去されません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わせられた (コピーされたコンフィギュレーション ファイルが優先する) コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルを復元して、サーバに保存されたファイルの正確なコピーを作成するには、コンフィギュレーション ファイルを直接スタートアップコンフィギュレーションにコピーして (**copy {ftp: | rcp: | tftp:} nvram:startup-config** 特権 EXEC コマンドを使用)、スイッチをリロードします。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップコンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2つのコンフィギュレーション ファイルは別々の設定にできません。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した後、**copy running-config startup-config** 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存されますが、スタートアップコンフィギュレーションはフラッシュメモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

手順

-
- ステップ 1** スイッチからサーバに既存のコンフィギュレーションをコピーします。
- ステップ 2** UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。
- ステップ 3** 目的のコマンドが格納されたコンフィギュレーションファイルの一部を抽出して、新しいファイルに保存します。
- ステップ 4** コンフィギュレーションファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ (UNIX ワークステーションの場合は、通常 /tftpboot) にコピーします。
- ステップ 5** ファイルに関する権限が world-read に設定されていることを確認します。
-

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーションファイルを使用してスイッチを設定したり、別のスイッチからダウンロードしたり、TFTP サーバからダウンロードしたりすることが可能です。また、コンフィギュレーション ファイルを TFTP サーバにコピー (アップロード) して、格納できます。

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、/etc/inetd.conf ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

/etc/services ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



-
- (注) /etc/inetd.conf および /etc/services ファイルを変更した後に、inetd デーモンを再起動する必要があります。このデーモンを再起動するには、inetd プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) もしくは **reboot** コマンド (Solaris 2.x もしくは SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。
-

- スイッチに TFTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーションファイルが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 /tftpboot)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、touch filename コマンドを入力します。filename の部分には、サーバにアップロードする際に使用するファイル名を指定します。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

手順

- ステップ 1** コンフィギュレーションファイルをワークステーションの適切な TFTP ディレクトリにコピーします。
- ステップ 2** TFTP サーバが適切に設定されていることを確認します。
- ステップ 3** コンソール ポート、イーサネット管理ポート、または Telnet セッションを介して、スイッチにログインします。
- ステップ 4** TFTP サーバからコンフィギュレーション ファイルをダウンロードして、スイッチを設定します。

TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

```
copy tftp:[[//location]/directory]/filename] system:running-config
```

```
copy tftp:[[//location]/directory]/filename] nvram:startup-config
```

```
copy tftp:[[//location]/directory]/filename] flash[n]:/directory/startup-config
```

このコンフィギュレーションファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

例

次に、IP アドレス 172.16.2.155 にあるファイル `tokyo-config` からソフトウェアを設定する例を示します。

```
Device# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして格納するには、次の手順を実行します。

手順

-
- ステップ 1** TFTP サーバが適切に設定されていることを確認します。
 - ステップ 2** コンソール ポート、イーサネット管理ポート、または Telnet セッションを介して、スイッチにログインします
 - ステップ 3** スwitchのコンフィギュレーションを TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- `copy system:running-config tftp:[[/location]/directory]/filename]`
- `copy nvram:startup-config tftp:[[/location]/directory]/filename]`
- `copy flash[n]:/directory/startup-config tftp:[[/location]/directory]/filename]`

TFTP サーバにファイルがアップロードされます。

例

次に、スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードする例を示します。

```
Device# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```

デバイスから FTP サーバへのコンフィギュレーション ファイルのコピー

デバイスから FTP サーバにコンフィギュレーション ファイルをコピーできます。

FTP ユーザ名およびパスワードの概要



(注) パスワードに特殊文字「@」を含めることはできません。文字「@」を使用すると、コピーでサーバの IP アドレスを解析できません。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してデバイスからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy EXEC** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. Anonymous

デバイスは、次の順番で最初に発見した有効なパスワードを送信します。

1. **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. デバイスは、*username@devicename.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*devicename* は設定済みのホスト名、*domain* はデバイスのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、デバイス上のユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** 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。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy EXEC** コマンド内でユーザ名を指定します。

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip ftp username *username* 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、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定します。
- コンフィギュレーション ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、FTP サーバを適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、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	スイッチ上で、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。 このステップが必要になるのは、デフォルトのリモートユーザ名またはパスワードを上書きする場合のみです（ステップ 2、3、および 4 を参照）。
ステップ 2	ip ftp username <i>username</i>	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 3	ip ftp password <i>password</i>	（任意）デフォルトのパスワードを変更します。
ステップ 4	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 5	次のいずれかを実行します。 <ul style="list-style-type: none"> • copy system:running-config ftp: [[[/[username [:password]@]location]/directory]/filename] • copy nvram:startup-config ftp: [[[/[username [:password]@]location]/directory]/filename] 	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップコンフィギュレーション ファイルにコピーします。

例

次に、`host1-config` という名前のコンフィギュレーション ファイルを、IP アドレスが `172.16.101.101` であるリモートサーバ上のディレクトリ `netadmin1` からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Device# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
Device#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、`netadmin1` というリモートユーザ名を指定する例を示します。コンフィギュレーション ファイル `host2-config` が、IP アドレス `172.16.101.101` のリモートサーバ上のディレクトリ `netadmin1` から、スイッチのスタートアップコンフィギュレーションにコピーされます。

```
Device# configure terminal
Device(config)# ip ftp username netadmin1
Device(config)# ip ftp password mypass
Device(config)# end
Device# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
[OK]
Device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、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	スイッチ上で、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。 このステップが必要になるのは、デフォルトのリモートユーザ名またはパスワードを上書きする場合のみです（ステップ 2、3、および 4 を参照）。
ステップ 2	ip ftp username <i>username</i>	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 3	ip ftp password <i>password</i>	（任意）デフォルトのパスワードを変更します。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 <ul style="list-style-type: none"> • copy system:running-config ftp: [[[/<i>username</i> [<i>:password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] または • copy nvram:startup-config ftp: [[[/<i>username</i> [<i>:password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] 	FTP を使用して、スイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定場所に格納します。

例

次に、実行コンフィギュレーション ファイル `switch2-config` を、IP アドレスが `172.16.101.101` であるリモート ホスト上のディレクトリ `netadmin1` にコピーする例を示します。

```
Device# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Device#
```

次に、FTP を使用してスタートアップコンフィギュレーションファイルをサーバに格納して、ファイルをコピーする例を示します。

```
Device# configure terminal
Device(config)# ip ftp username netadmin2
Device(config)# ip ftp password mypass
Device(config)# end
Device# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```


RCP によるコンフィギュレーション ファイルのコピー

リモートホストとスイッチ間でコンフィギュレーションファイルをダウンロード、アップロード、およびコピーするための別の方法は、RCP を使用することです。コネクションレス プロトコルであるユーザ データグラム プロトコル (UDP) を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の `copy` コマンドは、リモートシステム上の `rsh` サーバ (またはデーモン) を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは `rsh` をサポートするサーバにアクセスするだけですみます (ほとんどの UNIX システムが `rsh` をサポートしています)。ある場所から別の場所にファイルをコピーするため、コピー元のファイルに対する読み取り権限とコピー先のファイルに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- `copy` コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)
- `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- 現在の TTY (端末) プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、`username` コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチソフトウェアによって送信されます。
- スイッチのホスト名。

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- スイッチに RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと

サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、RCP サーバへの接続を確認します。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip rcmd remote-username username 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、すべてのコピー処理中に使用する新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、そのユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定します。
- ファイルを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモートユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを Switch1.company.com に変換する場合は、RCP サーバ上の User0 用の .rhosts ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、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	スイッチ上で、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。 この手順は、デフォルトのリモートユーザ名を上書きにする場合にだけ必要です (ステップ 2 および 3 を参照)。
ステップ 2	ip rcmd remote-username <i>username</i>	(任意) デフォルトのリモートユーザ名を変更します。
ステップ 3	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 4	次のいずれかを実行します。 <ul style="list-style-type: none"> • <code>copy rcp://<remote-host>/<remote-system>/<running-config></code> • <code>copy rcp://<remote-host>/<remote-host>/<startup-config></code> 	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップコンフィギュレーション ファイルにコピーします。

例

次に、`host1-config` という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 であるリモートサーバ上のディレクトリ `netadmin1` からコピーして、スイッチ上でこれらのコマンドをロードおよび実行する例を示します。

```
Device# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Device#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、`netadmin1` というリモートユーザ名を指定する例を示します。次いで、コンフィギュレーション ファイル `host2-config` が、IP アドレス 172.16.101.101 のリモートサーバ上の `netadmin1` ディレクトリから、スタートアップ コンフィギュレーション にコピーされます。

```
Device# configure terminal
Device(config)# ip rcmd remote-username netadmin1
Device(config)# end
Device# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
Device#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、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	<code>configure terminal</code>	スイッチ上で、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
		この手順は、デフォルトのリモートユーザ名を上書きにする場合にだけ必要です (ステップ 2 および 3 を参照)。
ステップ 2	ip rcmd remote-username <i>username</i>	(任意) リモート ユーザ名を指定します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを実行します。 <ul style="list-style-type: none"> • copy system:running-config rcp:[[/useame@]location/]directory/]filename] • copy nvram:startup-config rcp:[[/useame@]location/]directory/]filename] 	RCPを使用して、コンフィギュレーション ファイルをスイッチの実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコピーします。

例

次に、実行コンフィギュレーション ファイル `switch2-config` を、IP アドレスが `172.16.101.101` であるリモート ホスト上のディレクトリ `netadmin1` にコピーする例を示します。

```
Device# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Device#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
Device# configure terminal
Device(config)# ip rcmd remote-username netadmin2
Device(config)# end
Device# copy nvram:startup-config rcp:
Remote host[ ]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
![OK]
```

設定情報の消去

スタートアップ コンフィギュレーション から設定情報を消去できます。スタートアップ コンフィギュレーション を使用しないでスイッチを再起動すると、スイッチはセットアップ プログラムを開始し、新しい設定でスイッチを再設定できます。

スタートアップ コンフィギュレーション ファイルの消去

スタートアップ コンフィギュレーションの内容を消去するには、**erase nvram**: または **erase startup-config** 特権 EXEC コマンドを使用します。



(注) 削除されたスタートアップ コンフィギュレーション ファイルは復元できません。

格納されたコンフィギュレーション ファイルの削除

保存された設定をフラッシュ メモリから削除するには、**delete flash:filename** 特権 EXEC コマンドを使用します。file prompt グローバルコンフィギュレーション コマンドの設定によっては、ファイルを削除する前に確認を求めるプロンプトが表示されることがあります。デフォルトでは、スイッチは、破壊的なファイル操作に関する確認をプロンプトで要求します。file prompt コマンドの詳細については、『Cisco IOS Command Reference for Release 12.4』を参照してください。



(注) 削除されたファイルは復元できません。

コンフィギュレーションの交換およびロールバック

コンフィギュレーション交換およびロールバック機能を使用すると、実行コンフィギュレーションが、保存されている任意の Cisco IOS コンフィギュレーション ファイルに置き換えられます。ロールバック機能を使用すると以前のコンフィギュレーションに戻すことができます。

コンフィギュレーションの置換とロールバックに関する情報

コンフィギュレーション アーカイブ

Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドにより提供されるコンフィギュレーションのロールバック機能を強化するために、Cisco IOS コンフィギュレーション ファイルのアーカイブの保存、整理、管理を行うことを目的としたメカニズムです。この機能の導入前にも、実行コンフィギュレーションのコピーを **copy running-config destination-url** コマンドを使用して保存し、ローカルやリモートに置換ファイルを保管できました。ただし、この方法ではファイルの自動管理を行うことはできませんでした。一方、コンフィギュレーションの置換とロールバック機能では、実行コンフィギュレーション ファイルを自動的に Cisco IOS コンフィギュレーション アーカイブに保存できます。アーカイブされたファイルはコンフィギュレーションのチェックポイントとして参照することができ、**configure replace** コマンドを使用して以前のコンフィギュレーション状態に戻すために利用できます。

archive config コマンドを使用すると、Cisco IOS コンフィギュレーションをコンフィギュレーション アーカイブに保存できます。その場合、標準のディレクトリとファイル名のプレフィク

スが使用され、バージョン番号（およびオプションでタイムスタンプ）が自動的に付加されます。バージョン番号は連続したファイルを保存するごとに、1 つずつ大きくなります。この機能により、保存した Cisco IOS コンフィギュレーション ファイルを一貫して識別できます。アーカイブに保存する実行コンフィギュレーションの数は指定することができます。アーカイブ内のファイル数が上限値に達すると、次に最新のファイルが保存されるときに、最も古いファイルが自動的に消去されます。**show archive** コマンドを使用すると、Cisco IOS コンフィギュレーション アーカイブに保存されているすべてのコンフィギュレーション ファイルに関する情報が表示されます。

コンフィギュレーション ファイルを保存する Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドで使用することによって、FTP、HTTP、RCP、TFTP のファイルシステム上に配置できます。

コンフィギュレーションの置換

configure replace 特権 EXEC コマンドを使用すると、実行コンフィギュレーションと保存されている任意のコンフィギュレーション ファイルを交換できます。**configure replace** コマンドを入力すると実行コンフィギュレーションと指定した交換コンフィギュレーションが比較され、コンフィギュレーションの差分が生成されます。生成された差分がコンフィギュレーションの交換に使用されます。コンフィギュレーション交換は、通常 3 回以下のパスで完了します。ループを防ぐために 6 回以上のパスが実行されることはありません。

copy source-url running-config 特権 EXEC コマンドを使用すると、保存されているコンフィギュレーション ファイルを実行コンフィギュレーションにコピーできます。このコマンドを **configure replace target-url** 特権コマンドの代わりに使用する場合は、次のような違いがあることに注意してください。

- **copysource-urlrunning-config** コマンドはマージ動作であり、ソース ファイルと実行コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、コピー元ファイルに実行コンフィギュレーションのコマンドがない場合でも実行コンフィギュレーションのコマンドを削除しません。**configure replace** コマンドは、交換ファイルにならないコマンドは実行コンフィギュレーションから削除し、実行コンフィギュレーションにならないコマンドがある場合はそのコマンドを追加します。
- **copysource-urlrunning-config** コマンドのコピー元ファイルとして、部分コンフィギュレーションファイルを使用できます。**configure replacetarget-url** コマンドの交換ファイルには、完全なコンフィギュレーション ファイルを使用する必要があります。

設定のロールバック

configure replace コマンドを使用して、前回コンフィギュレーションを保存した後で行った変更をロールバックさせることもできます。コンフィギュレーション ロールバック機能では、コンフィギュレーションを特定の変更時点に戻すのではなく、保存されているコンフィギュレーション ファイルに基づいて特定のコンフィギュレーションに戻します。

コンフィギュレーションロールバック機能を利用する場合は、コンフィギュレーションを変更する前に実行コンフィギュレーションを保存する必要があります。その後、コンフィギュレー

ションを変更した後で **configure replacetarget-url** コマンドを使用し、保存したコンフィギュレーション ファイルを使って変更をロールバックします。

保存されている任意のファイルをロールバック コンフィギュレーションとして指定できます。一部のロールバック モデルと同様、ロールバック回数は無制限です。

設定時の注意事項

コンフィギュレーション交換およびロールバックを設定し実行する場合は、次の注意事項に従ってください。

- スイッチのメモリの空き容量が、2つのコンフィギュレーションファイル（実行コンフィギュレーションと保存されている交換コンフィギュレーション）の合計容量よりも大きいことを確認します。スイッチのメモリ容量の方が小さい場合、コンフィギュレーション交換は実行されません。
- また、スイッチにコンフィギュレーション交換やロールバック コンフィギュレーション コマンドが実行できるほどの空き容量があることも確認してください。
- ネットワークデバイスの物理コンポーネント（物理インターフェイスなど）に関連するコンフィギュレーションコマンドを実行コンフィギュレーションに追加または削除することはできません。
 - インターフェイスがデバイス上に物理的に存在する場合、コンフィギュレーション交換を行っても実行コンフィギュレーションから **interface interface-id** コマンド行を削除することはできません。
 - インターフェイスがデバイス上に物理的に存在しない場合、**interface interface-id** コマンド行を実行コンフィギュレーションに追加することはできません。
- **configure replace** コマンドを使用する場合、保存されているコンフィギュレーションを実行コンフィギュレーションの交換コンフィギュレーションファイルとして指定する必要があります。交換ファイルはCisco IOS デバイスによって生成された完全なコンフィギュレーションであることが必要です（たとえば **copy running-configdestination-url** コマンドで生成したコンフィギュレーション）。



(注) 交換コンフィギュレーション ファイルを外部に生成する場合、Cisco IOS デバイスで生成したファイルのフォーマットと一致する必要があります。

コンフィギュレーション アーカイブの設定

configure terminal コマンドをコンフィギュレーション アーカイブおよび **archive config** コマンドとともに使用することは任意ですが、コンフィギュレーションロールバックを行うときに大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブを設定するには、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	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	archive	アーカイブ 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	pathurl	コンフィギュレーションアーカイブに、ファイルのディレクトリとファイル名プレフィックスを指定します。
ステップ 4	maximumnumber	<p>(任意) コンフィギュレーション アーカイブに保存する実行コンフィギュレーションのアーカイブ ファイルの最大数を設定します。</p> <p><i>number</i> : コンフィギュレーション アーカイブでの実行コンフィギュレーション ファイルの最大数。有効な値は 1 ~ 14 で、デフォルトは 10 です。</p> <p>(注) このコマンドを使用する前に path アーカイブ コンフィギュレーション コマンドを入力して、コンフィギュレーション アーカイブのファイルのディレクトリとファイル名プレフィックスを指定しておく必要があります。</p>
ステップ 5	time-period minutes	<p>(任意) コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。</p> <p><i>minutes</i> : コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を、分単位で指定します。</p>
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show running-config	設定を確認します。
ステップ 8	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。

コンフィギュレーション置換またはロールバック動作の実行

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換するには、特権 EXEC モードで次の手順を実行します。

手順

ステップ 1 archive config

(任意) 実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。

(注) **path** アーカイブ コンフィギュレーション コマンドを入力してから、このコマンドを実行します。

ステップ 2 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 実行コンフィギュレーションに必要な変更を行います。

—

ステップ 4 exit

特権 EXEC モードに戻ります。

ステップ 5 configure replace *target-url* [**list**] [**force**] [**time seconds**] [**nolock**]

実行コンフィギュレーション ファイルを保存されているコンフィギュレーション ファイルと交換します。

target-url : 保存されているコンフィギュレーション ファイルの URL (ファイル システムからアクセス可能)。実行コンフィギュレーションと置換されるファイル。ステップ 2 で **archive config** 特権 EXEC コマンドを使用して作成したコンフィギュレーション ファイルなど。

list : コンフィギュレーション置換動作のパスごとにソフトウェア パーサーによって適用されるコマンド エントリのリストを表示します。パスの合計数も表示されます。

force : 実行コンフィギュレーション ファイルと指定した保存済みコンフィギュレーション ファイルの置換を、確認なしで実行します。

timeseconds : 実行コンフィギュレーション ファイルの置換を確認する **configure confirm** コマンドの入力時間制限を、秒単位で指定します。指定時間内に **configure confirm** コマンドを入力しない場合、コンフィギュレーション交換動作が自動的に停止します (つまり、実行コンフィギュレーション ファイルは **configure replace** コマンドを入力する以前に存在していたコンフィギュレーションに保存されます)。

(注) **time seconds** コマンドライン オプションを使用する前に、コンフィギュレーション アーカイブを有効にしておく必要があります。

nolock : コンフィギュレーション 置換動作時に他のユーザが実行コンフィギュレーションを変更できないようにする実行コンフィギュレーションファイルのロックを無効にします。

ステップ 6 **configure confirm**

(任意) 実行コンフィギュレーションと保存されているコンフィギュレーションファイルとの交換を確認します。

(注) このコマンドは、**time seconds** キーワードと **configure replace** コマンドの引数が指定されている場合にだけ使用します。

ステップ 7 **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。

ソフトウェア イメージの操作

ソフトウェア イメージの操作に関する情報

ここでは、システム ソフトウェア、Cisco IOS コード、および組み込みのデバイス マネージャ ソフトウェアを格納するソフトウェア イメージ ファイルをアーカイブ (ダウンロードおよびアップロード) する方法を示します。



(注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

スイッチ ソフトウェア をアップグレードするには、TFTP、FTP、または RCP サーバ からスイッチ イメージ ファイル をダウンロード します。TFTP サーバ にアクセス できない場合、Web ブラウザ (HTTP) を使用 し、次にデバイス マネージャ または Cisco Network Assistant を使用 してスイッチ をアップグレード することにより、PC またはワークステーション に直接ソフトウェア イメージ ファイル をダウンロード できます。TFTP サーバ または Web ブラウザ (HTTP) を使用 したスイッチ のアップグレード については、リリース ノート を参照 してください。

現在のイメージを新しいイメージで置き換えたり、ダウンロード後に現在のイメージをフラッシュ メモリに保存したりできます。

バックアップのために、スイッチ イメージ ファイル を TFTP、FTP、または RCP サーバ にアップロード します。アップロード されたこのイメージは、今後同じスイッチ や、同じタイプの別のスイッチ にダウンロード する場合に使用 できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。これらの機能を実現するために、FTP および RCP はコネクション型の TCP/IP スタックに基づいて構築され、このスタックが使用されています。



(注) ソフトウェア イメージ、およびサポートされているアップグレード パスの一覧については、スイッチに付属のリリース ノートを参照してください。

スイッチ上のイメージの場所

Cisco IOS イメージは、バージョン番号を表すディレクトリ内に .bin ファイルとして格納されます。サブディレクトリには、Web 管理に必要なファイルが格納されます。イメージはシステム ボードのフラッシュ メモリ (flash:) に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで現在稼働しているソフトウェア バージョンを参照できます。画面上で、**System image file is...** で始まる行を調べます。。この行は、イメージが格納されているフラッシュ メモリ内のディレクトリ名を示します。

また、**dir filesystem:** 特権 EXEC コマンドを使用して、フラッシュ メモリに格納された可能性のあるその他のソフトウェア イメージのディレクトリ名を表示することもできます。

サーバまたは Cisco.com 上のイメージのファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- tar ファイルの内容を表形式で示す info ファイル
- Cisco IOS イメージや Web 管理用ファイルなど、他のイメージおよびファイルが格納された 1 つまたは複数のサブディレクトリ

次に、info ファイルに格納された情報の一部の例を示します。表には、この情報に関する詳細を示しています。

```
system_type:0x00000000:image-name
  image_family:xxxx
  info_end:

version_suffix:xxxx
  version_directory:image-name
  image_system_type_id:0x00000000
  image_name:image-nameB.bin
  ios_image_file_size:6398464
  total_image_file_size:8133632
  image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
  image_family:xxxx
  board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002

0x40110000
  info_end
```

表 17: info ファイルの説明

フィールド	説明
version_suffix	Cisco IOS イメージバージョン スtring のサフィックスを指定します。
version_directory	Cisco IOS イメージおよび HTML サブディレクトリがインストールされているディレクトリを指定します。
image_name	tar ファイル内の Cisco IOS イメージの名前を指定します。
ios_image_file_size	tar ファイル内の Cisco IOS イメージのサイズを指定します。このサイズは、Cisco IOS イメージのみを保持するために必要なフラッシュメモリ サイズの概算値です。
total_image_file_size	tar ファイル内のすべてのイメージ (Cisco IOS イメージおよび Web 管理ファイル) のサイズを指定します。このサイズは、これらのファイルを保持するために必要なフラッシュメモリ サイズの概算値です。
image_feature	イメージの主な機能に関する説明です。
image_min_dram	このイメージを実行するために必要な DRAM の最小サイズを指定します。
image_family	ソフトウェアをインストールできる製品ファミリーに関する説明です。

ソフトウェアイメージのアップグレード履歴の表示

リリース 15.2(7)E3 以降では、**show archive sw-upgrade history** コマンドを使用してデバイスのソフトウェアイメージアップグレードの履歴を表示できます。このコマンドは、各アップグレードのイメージ名、バージョン、アップグレード方法、タイムラインなどのアップグレードの詳細を表示します。

TFTP によるイメージファイルのコピー

TFTP サーバからスイッチイメージをダウンロードしたり、スイッチから TFTP サーバにスイッチイメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後、同じスイッチまたは同じタイプの別のスイッチへのダウンロードに使用できます。



- (注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

`/etc/services` ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



- (注) `/etc/inetd.conf` および `/etc/services` ファイルを変更した後に、`inetd` デーモンを再起動する必要があります。このデーモンを再起動するには、`inetd` プロセスを終了して再起動するか、または `fastboot` コマンド (SunOS 4.x の場合) もしくは `reboot` コマンド (Solaris 2.x もしくは SunOS 5.x の場合) を入力します。TFTP デーモンの詳細については、ワークステーションのマニュアルを参照してください。

- スwitch に TFTP サーバへのルートが設定されているかどうかを確認します。サブネットワーク間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと TFTP サーバは同じサブネットワークに置かれていなければなりません。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 `/tftpboot`) 。

- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は **world-read** でなければなりません。
- イメージ ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch filename** コマンドを入力します。**filename** は、イメージをサーバにアップロードする際に使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル（空のファイルを作成する必要があった場合は、空のファイルを含む）を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は **world-write** でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～3 を実行します。現在のイメージを保存するには、ステップ 3 へ進みます。

手順

ステップ 1 イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。TFTP サーバが適切に設定されていることを確認します。

—

ステップ 2 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

—

ステップ 3 **archive download-sw/overwrite/reload tftp:** [[//location] /directory] /image-name.tar

TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。

- **/overwrite** オプションを指定すると、フラッシュメモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **// location** には、TFTP サーバの IP アドレスを指定します。
- **/directory/image-name.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ステップ 4 **archive download-sw/leave-old-sw/reload tftp:** [[//location] /directory] /image-name.tar

TFTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。

- **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェアバージョンが保持されます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **//location** には、TFTP サーバの IP アドレスを指定します。
- **/directory/image-name.tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロードアルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかが検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、ダウンロードアルゴリズムによって、新しいイメージと同じであるかどうかに関係なくフラッシュデバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注) フラッシュデバイスに2つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に稼働中のイメージを保存しようとする、ダウンロードプロセスが停止して、エラーメッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (**flash:**) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロードプロセス中に古いイメージを保持した場合 (**/leave-old-sw** キーワードを指定した場合) は、**delete /force /recursive filesystem :/ file-url** 特権 EXEC コマンドを入力すると、そのイメージを削除できます。**filesystem** には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。**file-url** には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

(注) ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

TFTP によるイメージ ファイルのアップロード

スイッチから TFTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

手順

ステップ 1 TFTP サーバが適切に設定されていることを確認します。

—

ステップ 2 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

—

ステップ 3 `archive upload-sw tftp:[[/ location]/directory]/image-name .tar`

現在稼働中のスイッチ イメージを TFTP サーバにアップロードします。

- `/location` には、TFTP サーバの IP アドレスを指定します。
- `directory/image-name.tar` には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。`image-name.tar` は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw 特権 EXEC コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージ ファイルが構築されます。これらのファイルがアップロードされた後に、アップロードアルゴリズムによって tar ファイル形式が作成されます。

(注) ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのコピー

FTP サーバからスイッチ イメージをダウンロードしたり、スイッチから FTP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



- (注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)。
- **ip ftp username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- Anonymous

スイッチは、次のリスト内の最初の有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password password** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- スイッチが作成した `username@switchname.domain` パスワード。変数 `username` は現在のセッションに関連付けられているユーザ名、`switchname` は設定されているホスト名、`domain` はスイッチのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定しません。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- スイッチに FTP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スイッチと FTP サーバは同じサブネットに置かれていなければなりません。ping コマンドを使用して、FTP サーバへの接続をチェックします。
- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の FTP ユーザ名が FTP ダウンロードに使用するユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip ftp username username 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、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、FTP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、archive download-sw または archive upload-sw 特権 EXEC コマンドでユーザ名を指定します。
- イメージ ファイルを FTP サーバにアップロードする場合は、スイッチ上のユーザからの書き込み要求が許可されるように、適切に設定する必要があります。

詳細については、FTP サーバのマニュアルを参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～7 の手順を実行します。現在のイメージを保存するには、ステップ 7 へ進みます。

手順

ステップ 1 FTP サーバが適切に設定されていることを確認します。

—

ステップ 2 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

—

ステップ 3 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。

このステップが必要になるのは、デフォルトのリモートユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。

ステップ 4 ip ftp username *username*

(任意) デフォルトのリモート ユーザ名を変更します。

ステップ 5 **ip ftp password***password*

(任意) デフォルトのパスワードを変更します。

ステップ 6 **end**

特権 EXEC モードに戻ります。

ステップ 7 **archive download-sw /overwrite/reload**

ftp: [[/ / *username* [:*password*] @*location*] / *directory*] / *image-name.tar*

FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。

- **/overwrite** オプションを指定すると、フラッシュメモリ内のソフトウェア イメージが、ダウンロードされたイメージによって上書きされます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **//username [:password]** には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。
- **@ location** には、FTP サーバの IP アドレスを指定します。
- **directory/image-name.tar** には、ディレクトリ (任意) とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ステップ 8 **archive download-sw /leave-old-sw/reload**

ftp: [[/ / *username* [:*password*] @*location*] / *directory*] / *image-name.tar*

FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。

- **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェアバージョンが保持されます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **//username [:password]** には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。
- **@ location** には、FTP サーバの IP アドレスを指定します。
- **directory/image-name.tar** には、ディレクトリ (任意) とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによってフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注) フラッシュ デバイスに2つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に稼働中のイメージを保存しようとする、ダウンロードプロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (**flash:**) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロードプロセス中に古いイメージを保持した場合 (**/leave-old-sw** キーワードを指定した場合) は、**delete/force/recursivefilesystem :/file-url** 特権 EXEC コマンドを入力すると、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

(注) ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

FTP によるイメージ ファイルのアップロード

スイッチから FTP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが、既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

手順

ステップ 1 **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。

このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 2、3、および 4 を参照)。

ステップ 2 **ip ftp usernameusername**

(任意) デフォルトのリモート ユーザ名を変更します。

ステップ 3 **ip ftp passwordpassword**

(任意) デフォルトのパスワードを変更します。

ステップ 4 end

特権 EXEC モードに戻ります。

ステップ 5 archive upload-sw ftp: [[// [username [:password] @] location] /directory] /image-name.tar

現在稼働中のスイッチ イメージを FTP サーバにアップロードします。

- **username:password** には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。
- **@location** には、FTP サーバの IP アドレスを指定します。
- **directory/image-name.tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。**image-name.tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージファイルが構築されます。これらのファイルがアップロードされた後に、アップロードアルゴリズムによって tar ファイル形式が作成されます。

(注) ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのコピー

RCP サーバからスイッチ イメージをダウンロードしたり、スイッチから RCP サーバにスイッチ イメージをアップロードしたりできます。

スイッチ ソフトウェアをアップグレードするには、サーバからスイッチ イメージ ファイルをダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。バックアップのために、スイッチ イメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じスイッチや、同じタイプの別のスイッチにダウンロードする場合に使用できます。



(注) ソフトウェア イメージ ファイルをダウンロードおよびアップロードするには、**copy** 特権 EXEC コマンドまたは **archive tar** 特権 EXEC コマンドではなく、**archive download-sw** および **archive upload-sw** 特権 EXEC コマンドを使用することを推奨します。

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

リモート ホストとスイッチの間でイメージ ファイルをダウンロードおよびアップロードするための別の方法は、RCP を使用することです。コネクションレス プロトコルであるユーザデータグラム プロトコル (UDP) を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の `copy` コマンドは、リモート システム上の `rsh` サーバ (またはデーモン) を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは `rsh` をサポートするサーバにアクセスするだけですみます (ほとんどの UNIX システムが `rsh` をサポートしています)。ある場所から別の場所にファイルをコピーするため、コピー元のファイルに対する読み取り権限とコピー先のファイルに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージ ファイルをスイッチからサーバにコピーすると、Cisco IOS ソフトウェアは次のリスト内の最初の有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)。
- **ip rcmd remote-username *username*** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが入力されている場合)。
- 現在の TTY (端末) プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がスイッチ ソフトウェアによって送信されます。
- スwitch のホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- スwitch に RCP サーバへのルートが設定されているかどうかを確認します。サブネット間でトラフィックをルーティングするようにルータを設定していない場合、スウィッチとサーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバへの接続を確認します。

- コンソールまたは Telnet セッションを介してスイッチにアクセスしていて有効なユーザ名がない場合は、現在の RCP ユーザ名が RCP ダウンロードに使用するユーザ名であることを確認します。 **show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username username** 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、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを介してスイッチにアクセスしていて、有効なユーザ名がある場合は、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- イメージを RCP サーバにアップロードする場合は、スイッチ上のユーザからの RCP 書き込み要求が許可されるように、適切に設定する必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の **.rhosts** ファイルにエントリを追加する必要があります。

たとえば、スイッチに次のコンフィギュレーション行が含まれているとします。

```
hostname Switch1
ip rcmd remote-username User0
```

このスイッチの IP アドレスを *Switch1.company.com* に変換する場合は、RCP サーバ上の User0 用の **.rhosts** ファイルに次の行が含まれている必要があります。

```
Switch1.company.com Switch1
```

詳細については、RCP サーバのマニュアルを参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～6 の手順を実行します。現在のイメージを保存するには、ステップ 6 へ進みます。

手順

ステップ 1 RCP サーバが適切に設定されていることを確認します。

—

ステップ 2 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

—

ステップ 3 **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。

このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。

ステップ 4 ip rcmd remote-username username

（任意）リモート ユーザ名を指定します。

ステップ 5 end

特権 EXEC モードに戻ります。

ステップ 6 archive download-sw /overwrite/reload

rcp: [[[/username@]/location]/directory]/image-name.tar

RCP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを上書きします。

- **/overwrite** オプションを指定すると、フラッシュメモリ内のソフトウェア イメージが、ダウンロードされたイメージによって上書きされます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **//username** には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。
- **@location** には、RCP サーバの IP アドレスを指定します。
- **directory/image-name.tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ステップ 7 archive download-sw /leave-old-sw/reload

rcp: [[[/[username@]location]/directory]/image-name.tar

FTP サーバからスイッチにイメージ ファイルをダウンロードして、現在のイメージを保存します。

- **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保持されます。
- **/reload** オプションを指定すると、設定が変更されて保存されなかった場合を除いて、イメージのダウンロード後にシステムがリロードされます。
- **//username** には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。
- **@location** には、RCP サーバの IP アドレスを指定します。
- **directory/image-name.tar** には、ディレクトリ（任意）とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

ダウンロード アルゴリズムによって、イメージがスイッチ モデルに対して適切であるかどうか、および DRAM サイズが十分であるかどうかを検証されます。問題がある場合、プロセスは中断され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによってフラッシュ デバイスの既存のイメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注) フラッシュ デバイスに2つのイメージを保持する十分なスペースがあり、これらのイメージのいずれかを同じバージョンで上書きする場合は、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に稼働中のイメージを保存しようとする、ダウンロードプロセスが停止して、エラー メッセージが表示されます。

ダウンロードされたイメージは、システム ボードのフラッシュ デバイス (**flash:**) にアルゴリズムによってインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロードプロセス中に古いイメージを保持した場合 (**/leave-old-sw** キーワードを指定した場合) は、**delete/force/recursivefilesystem :/file-url** 特権 EXEC コマンドを入力すると、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスを指定する場合は **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

(注) ダウンロードおよびアップロード アルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。

RCP によるイメージ ファイルのアップロード

スイッチから RCP サーバにイメージをアップロードできます。後でこのイメージをこのスイッチや、同じタイプの別のスイッチにダウンロードできます。

組み込みのデバイス マネージャと連携する Web 管理ページが既存のイメージでインストールされている場合に限って、アップロード機能を使用します。

イメージを RCP サーバにアップロードするには、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	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。 この手順は、デフォルトのリモートユーザ名またはパスワードを上書きする場合にだけ必要です (ステップ 2 および 3 を参照)。
ステップ 2	ip rcmd remote-username <i>username</i>	(任意) リモート ユーザ名を指定します。
ステップ 3	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 4	archive upload-sw rpx [[[/[/[<i>username</i> @] <i>location</i>]/ <i>directory</i>]/ <i>image-name.tar</i>	<p>現在稼働中のスイッチ イメージを RCP サーバにアップロードします。</p> <ul style="list-style-type: none"> • <i>//username</i> には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。 • <i>@location</i> には、RCP サーバの IP アドレスを指定します。 • <i>directory/image-name.tar</i> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • <i>image-name.tar</i> は、サーバに保存するソフトウェア イメージの名前です。 <p>archive upload-sw コマンドを実行すると、これらのファイルが info、Cisco IOS イメージ、Web 管理ファイルの順にアップロードされて、サーバにイメージファイルが構築されます。これらのファイルがアップロードされた後に、アップロードアルゴリズムによって tar ファイル形式が作成されます。</p> <p>(注) ダウンロードおよびアップロードアルゴリズムを適切に動作させるために、イメージの名前は変更しないでください。</p>



第 8 章

ソフトウェア設定のトラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。問題の性質に応じて、コマンドラインインターフェイス (CLI)、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

LEDの説明など、トラブルシューティングの詳細については、ハードウェアインストールガイドを参照してください。

- [ソフトウェア設定のトラブルシューティングに関する情報 \(151 ページ\)](#)
- [ソフトウェア設定のトラブルシューティング方法 \(158 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングの確認 \(174 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングのシナリオ \(177 ページ\)](#)
- [ソフトウェアのトラブルシューティングの設定例 \(182 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングに関する追加情報 \(184 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングの機能履歴と情報 \(185 ページ\)](#)

ソフトウェア設定のトラブルシューティングに関する情報

スイッチのソフトウェア障害

スイッチソフトウェアがアップグレード中に破損する原因として、誤ったファイルがスイッチにダウンロードされた場合やイメージファイルが削除された場合があります。いずれの場合にも、スイッチは電源投入時自己診断テスト (POST) に失敗し、接続できなくなります。

デバイスのパスワードを紛失したか忘れた場合

デバイスのデフォルト設定では、デバイスを直接操作するエンドユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失し

た状態から回復できます。ここで紹介する回復手順を実行するには、デバイスを直接操作してください。



- (注) これらのデバイスでは、システム管理者はデフォルト設定に戻す場合に限りエンドユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできません。パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとする、ステータスメッセージで回復プロセスの間はデフォルトの設定に戻すように指示されます。

Power over Ethernet (PoE) ポート

Power over Ethernet (PoE) 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スイッチが検知した場合、接続している次のデバイスに電力が自動的に供給されます。

- シスコ先行標準受電デバイス (Cisco IP Phone や Cisco Aironet アクセス ポイントなど)
- IEEE 802.3af 準拠の受電装置
- IEEE 802.3at 準拠の受電装置

受電デバイスが PoE スイッチ 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。受電装置が PoE ポートにだけ接続されている場合、受電装置には冗長電力は供給されません。

受電デバイスを検出すると、スイッチは受電デバイスの電力要件を判断し、受電デバイスへの電力供給を許可または拒否します。また、スイッチは消費電力をモニタリングおよびポリシングすることで、装置の電力の消費をリアルタイムに検知できます。

詳細については、『*Catalyst 1000 Series Switches Interface and Hardware Component Configuration Guide*』の「Configuring PoE」の章を参照してください。

電力消失によるポートの障害

PoE デバイスポートに接続され、AC 電源から電力が供給されている受電デバイス (Cisco IP Phone 7910 など) に AC 電源から電力が供給されない場合、そのデバイスは **errdisable** ステートになることがあります。errdisable ステートから回復するには、**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入力してから、**no shutdown** インターフェイスコマンドを入力します。デバイスで自動回復を設定し、errdisable ステートから回復することもできます。

デバイスの場合、**errdisable recovery cause loopback** および **errdisable recovery interval seconds** グローバル コンフィギュレーション コマンドは、指定した期間が経過したあと自動的にインターフェイスを errdisable ステートから復帰させます。

PoE ポート ステータスのモニタリング

- **show controllers power inline** 特権 EXEC コマンド

- **show power inline EXEC** コマンド
- **debug ilpower** 特権 EXEC コマンドを使用します。

不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** 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を設定した場合は、不正リンクアップが発生し、ポートが **errdisable** ステートになることがあります。ポートを **errdisable** ステートから回復するには、**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 コマンドを入力します。

power inline never コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

ping

デバイスは IP の **ping** をサポートしており、これを使用してリモートホストへの接続をテストできます。**ping** はアドレスにエコー要求パケットを送信し、応答を待ちます。**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* が存在する) は、ネットワーク トラフィックにもよりますが、1 ~ 10 秒以内で発生します。
- 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。
- 不明なホスト：ホストが存在しない場合、*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への到達不能：ルートテーブルにホストまたはネットワークのエントリがない場合、*network or host unreachable* メッセージが返されます。

レイヤ 2 traceroute

レイヤ 2 **traceroute** 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への物理パスを識別できます。レイヤ 2 **traceroute** 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。**transroute** は、パス内にあるデバイスの MAC アドレステーブルを使用してパスを識別します。デバイスがパス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。

デバイスは、送信元デバイスから宛先デバイスへのパスのみを識別できます。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の traceroute のガイドライン

- ネットワーク内のすべてのデバイスで、Cisco Discovery Protocol (CDP) をイネーブルにする必要があります。レイヤ2 traceroute が適切に動作するために、CDP をディセーブル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。
- ping 特権 EXEC コマンドを使用して接続をテストできれば、このデバイスは別のデバイスから到達可能であると定義できます。物理パス内のすべてのデバイスは、他のスイッチから相互に到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスと宛先デバイスの間の物理パス内にないデバイスで、**traceroute mac** または **traceroute mac ip** の特権 EXEC コマンドを実行できます。パス内のすべてのデバイスは、このスイッチから到達可能でなければなりません。
- 指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ2 パスを表示します。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。
- 指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ2 パスを表示します。IP アドレスを指定した場合、デバイスは Address Resolution Protocol (ARP) を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を対応させます。
 - 指定の IP アドレスの ARP のエントリが存在している場合、デバイスは関連付けられた 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、デバイスは ARP クエリを送信し、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 トレースルートは、ユーザデータグラム プロトコル (UDP) ポート 2228 でリスニングソケットを開きます。このポートは、任意の IPv4 アドレスを使用してリモートからアクセスでき、認証は必要ありません。この UDP ソケットにより、VLAN 情報、リンク、特定の MAC アドレスの存在、および CDP ネイバー情報をデバイスから読み取ることができます。この情報を使用することにより、最終的にレイヤ2 ネットワークトポロジの全体像を構築できます。
- レイヤ2 トレースルートはデフォルトで有効になっており、グローバル コンフィギュレーション モードで **no l2 traceroute** コマンドを実行することによって無効にできます。レイヤ2 トレースルートを再度有効にするには、グローバル コンフィギュレーション モードで **l2 traceroute** コマンドを使用します。

IP トレースルート

IP **traceroute** を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。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。

デバイスは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、**traceroute** コマンドの出力でホップとして表示される場合があります。デバイスを **traceroute** の宛先とすると、スイッチは、**traceroute** の出力で最終の宛先として表示されます。中間デバイスが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、**traceroute** の出力に中間スイッチは表示されません。ただし、中間デバイスが特定の packets をルーティングするマルチレイヤデバイスの場合、このデバイスは **traceroute** の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間 (TTL) フィールドを使用して、ルータおよび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。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージプロトコル (ICMP) **time-to-live-exceeded** メッセージを送信元に送信します。**traceroute** は、ICMP **time-to-live-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別します。

ネクスト ホップを識別するために、**traceroute** 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 値が 1 であることを確認すると、このデータグラムを廃棄し、**time-to-live-exceeded** メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで (または TTL の最大値に達するまで) TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、**traceroute** は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛てのデータグラムを受信すると、送信元に ICMP ポート到達不能エラーを送信します。ポート到達不能エラーを除くすべてのエラーは中間ホップから送信されるため、ポート到達不能エラーを受信するという事は、このメッセージが宛先ポートから送信されたことを意味します。

Time Domain Reflector ガイドライン

Time Domain Reflector (TDR) 機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR 稼働時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は 10/100/1000 の銅線イーサネットポート上でだけサポートされます。10 ギガビットイーサネットポートまたは SFP モジュールポートではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイストペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- デバイスの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2 つのデバイス間の接続のトラブルシューティング

TDR の実行時、次の場合にデバイスは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にデバイスは正確な情報をレポートしません。

- ギガビット リンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル
- リンク パートナーが Cisco IP Phone
- リンク パートナーが IEEE 802.3 に準拠していない

debug コマンド



注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。

スイッチのオンボード障害ロギング

オンボード障害ロギング (OBFL) 機能を使用すれば、デバイスに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、シスコのテクニカルサポート担当者がデバイスの問題をトラブルシューティングする際に役立ちます。OBFL はイネーブルにしておき、フラッシュメモリに保存されたデータは消さないようにすることを推奨します。

OBFL は、デフォルトでイネーブルになっています。デバイスおよび Small Form-Factor Pluggable (SFP) モジュールに関する情報が収集されます。デバイスは、次の情報をフラッシュメモリに保存します。

- CLI コマンド：スタンドアロンデバイスで入力された OBFL CLI コマンドの記録。
- 環境データ：スタンドアロンデバイスおよび接続されているすべての FRU デバイスの一意のデバイス ID (UDI) 情報、製品 ID (PID)、バージョン ID (VID)、およびシリアル番号。
- メッセージ：スタンドアロンデバイスにより生成されたハードウェア関連のシステムメッセージの記録。
- Power over Ethernet (PoE)：スタンドアロンデバイスの PoE ポートの消費電力の記録。
- 温度：スタンドアロンデバイスの温度。
- 稼働時間：スタンドアロンデバイスが起動された際の時刻、再起動された理由、およびデバイスが最後に再起動されて以来の稼働時間。
- 電圧：スタンドアロンデバイスのシステム電圧。

システム時計は、手動で時刻を設定するか、またはネットワーク タイム プロトコル (NTP) を使用するように設定します。

デバイスの稼働中には、**show logging onboard** 特権 EXEC コマンドを使用することにより、OBFL データを取得できます。デバイスに障害が発生した場合のデータの取得方法については、お客様担当のシスコテクニカルサポート担当者にお問い合わせください。

OBFL がイネーブルになっているデバイスが再起動された場合、新しいデータの記録が開始するまでに 10 分間の遅延があります。

CPU 使用率が高い場合に起こりうる症状

CPU 使用率が高すぎることで次の症状が発生する可能性があります。他の原因で発生する場合もあります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求 (ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション) に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- スイッチが要求を転送しない、または要求に応答しない場合の DHCP または IEEE 802.1x の処理の失敗

レイヤ 3 スイッチの場合：

- ソフトウェアでルーティングされるパケットのドロップまたは遅延の増加

ソフトウェア設定のトラブルシューティング方法

ソフトウェア障害からの回復

アップグレード中にスイッチソフトウェアが破損する状況としては、スイッチに誤ったファイルをダウンロードした場合や、イメージファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは電源投入時自己診断テスト (POST) に失敗し、接続できなくなります。

次の手順では、XMODEM プロトコルを使用して、破損したイメージファイルまたは間違ったイメージファイルを回復します。XMODEM プロトコルをサポートするソフトウェアパッケージは多数あり、使用するエミュレーション ソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

手順

ステップ 1 PC 上で、Cisco.com から tar 形式のソフトウェア イメージファイル (*image_filename.tar*) をダウンロードします。Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージファイルの検索方法については、リリース ノートを参照してください。

ステップ 2 tar ファイルから bin ファイルを抽出します。Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して移動します。Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して移動します。UNIX を使用している場合は、次の手順に従ってください。

a) **tar -tvf** <image_filename.tar> UNIX コマンドを使用して、tar ファイルの内容を表示します。

例 :

```
unix-1% tar -tvf image_filename.tar
```

b) **tar -xvf** <image_filename.tar> <image_filename.bin> UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

例 :

```
unix-1% tar -xvf image_filename.tar image_filename.bin
x c1000-universalk9-mz.152-7.2.18.E1/c1000-universalk9-mz.152-7.2.18.E1.bin, 2928176
  bytes, 5720
tape blocks
```

c) **ls -l** <image_filename.bin> UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

例 :

```
unix-1% ls -l image_filename.bin
-rw-r--r--  1 boba      2928176 Apr 21 12:01
c1000-universalk9-mz.152-7.2.18.UCP/c1000-universalk9-mz.152-7.2.18.UCP.bin
```

ステップ 3 XMODEM プロトコルをサポートする端末エミュレーションソフトウェアを備えた PC を、スイッチのコンソールポートに接続します。

ステップ 4 エミュレーションソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 5 スイッチの電源コードを取り外します。

ステップ 6 [Mode] ボタンを押しながら、電源コードを再度スイッチに接続します。ソフトウェアに関する次の行の情報が説明とともに表示されるまで、[Mode] ボタンを押し続けます。

例 :

```
The system has been interrupted. The following commands will finish loading the operating
system software:
```

```
boot
```

```
switch:
```

- ステップ 7** コンソールポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーションソフトウェアの回線速度をスイッチのコンソールポートに合わせて変更します。
- ステップ 8** XMODEM プロトコルを使用して、ファイル転送を開始します。
- 例：
- ```
switch: copy xmodem: flash:image_filename.bin
```
- ステップ 9** XMODEM 要求が表示されたら、端末エミュレーションソフトウェアに適切なコマンドを使用して、転送を開始し、ソフトウェアイメージをフラッシュメモリにコピーします。
- ステップ 10** 新規にダウンロードされた Cisco IOS イメージを起動します。
- 例：
- ```
switch: boot flash:image_filename.bin
```
- ステップ 11** **archive download-sw** 特権 EXEC コマンドを使用して、スイッチにソフトウェアイメージをダウンロードします。
- ステップ 12** **reload** 特権 EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェアイメージが適切に動作していることを確認します。
- ステップ 13** スイッチから、**flash:image_filename.bin** ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンドユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。



- (注) これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンドユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできません。パスワード回復がディセーブルになっている場合に、エンドユーザがパスワードをリセットしようとする、回復プロセスの間、ステータスメッセージにその旨が表示されます。

パスワードの回復をイネーブルまたはディセーブルにするには、**service password-recovery** 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。

手順

- ステップ 1** 端末または PC をスイッチに接続します。
- 端末または端末エミュレーションソフトウェアが稼働している PC をスイッチのコンソールポートに接続します。

または

- PC をイーサネット管理ポートに接続します。

ステップ 2 エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スイッチの電源を切断します。

ステップ 4 スイッチに電源コードを再接続します。15 秒以内に **Mode** ボタンを押します。このときシステム LED はグリーンに点滅しています。すべてのシステム LED が点灯した状態になるまで、**Mode** ボタンを押し続けます。その後、**Mode** ボタンを放します。

ソフトウェアについての情報および指示が数行表示され、パスワード回復手順がディセーブルであるかどうかを示されます。

- 次のステートメントで始まるメッセージが表示された場合

```
The system has been interrupted. The following commands will finish loading the
operating system software:
```

「パスワード回復がイネーブルになっている場合の手順」セクションに記載されている手順を実行します。

- 次のステートメントで始まるメッセージが表示された場合

```
The password-recovery mechanism has been triggered, but is currently disabled.
```

「パスワード回復がディセーブルになっている場合の手順」に記載されている手順を実行します。

ステップ 5 パスワードが回復したら、スイッチをリロードします。

スイッチの場合

```
Switch> reload
Proceed with reload? [confirm] y
```

パスワード回復がイネーブルになっている場合の手順

パスワード回復動作がイネーブルになっている場合は、次のメッセージが表示されます。

```
The system has been interrupted. The following commands will finish loading the
operating system software:
```

```
boot
```

手順

ステップ 1 コンソールポートの速度を 9600 以外の値に設定していた場合、9600 にリセットされます。エミュレーションソフトウェアの回線速度をスイッチのコンソールポートに合わせて変更します。

ステップ 2 フラッシュメモリの内容を表示します。

```
Device: dir: flash:
Directory of flash:
  13  drwx          192  Mar 01 2013 22:30:48
c1000-universalk9-mz.152-7.2.18.E1/c1000-universalk9-mz.152-7.2.18.E1.bin
  11  -rwx          5825  Mar 01 2013 22:31:59  config.text

16128000 bytes total (10003456 bytes free)
```

ステップ 3 コンフィギュレーションファイルの名前を `config.text.old` に変更します。
このファイルには、パスワード定義が収められています。

```
Device: rename flash:config.text flash:config.text.old
```

ステップ 4 システムを起動します。

```
Device: boot
```

セットアッププログラムを起動するように求められます。プロンプトに **N** を入力します。

```
Continue with the configuration dialog?? [yes/no]: No
```

ステップ 5 スイッチプロンプトで、特権 EXEC モードを開始します。

```
Device> enable
Switch#
```

ステップ 6 コンフィギュレーションファイルを元の名前に戻します。

```
Device# rename flash:config.text.old flash:config.text
```

ステップ 7 コンフィギュレーションファイルをメモリにコピーします。

```
Device# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

確認を求めるプロンプトに、**Return** を押して応答します。これで、コンフィギュレーションファイルがリロードされ、パスワードを変更できるようになります。

ステップ 8 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。

```
Device# configure terminal
```

ステップ 9 パスワードを変更します。

```
Device(config)# enable secret password
```

シークレットパスワードは1～25文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 10 特権 EXEC モードに戻ります。

```
Device(config)# exit
Device#
```

ステップ 11 実行コンフィギュレーションをスタートアップコンフィギュレーションファイルに書き込みます。

```
Device# copy running-config startup-config
```

新しいパスワードがスタートアップコンフィギュレーションに組み込まれました。

(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウンステートになることがあります。このステートになっているインターフェイスを調べるには、**show running-config** 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan vlan-id** グローバルコンフィギュレーションコマンドを入力して、シャットダウンインターフェイスのVLAN IDを指定します。スイッチがインターフェイスコンフィギュレーションモードの状態では、**no shutdown** コマンドを入力します。

ステップ 12 フラッシュのファイルを使用して、デバイスを起動します。

```
Device: boot flash:image_filename.bin
```

ステップ 13 スイッチをリロードします。

```
Device# reload
```

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルの場合、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```



注意 デバイスをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせ、バックアップデバイスと VLAN（仮想 LAN）コンフィギュレーションファイルがあるかどうかを確認してください。

- **n (no)** を入力すると、**Mode** ボタンを押さなかった場合と同様に、通常のブートプロセスが継続されます。ブートルoader プロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。次のメッセージが表示されます。

```
Press Enter to continue.....
```

- **y (yes)** を入力すると、フラッシュメモリ内のコンフィギュレーションファイルおよび VLAN データベースファイルが削除されます。デフォルト設定がロードされる時に、パスワードをリセットできます。

手順

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2 フラッシュメモリの内容を表示します。

```
Device: dir flash:
```

デバイスのファイルシステムが表示されます。

```
Directory of flash:
 13  drwx          192  Mar 01 2013 22:30:48  c1000-universalk9-mz.152-7.2.18.UCP.bin
16128000 bytes total (10003456 bytes free)
```

ステップ 3 システムを起動します。

```
Device: boot
```

セットアッププログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 4 デバイスプロンプトで、特権 EXEC モードを開始します。

```
Device> enable
```


ステップ5 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。

```
Device# configure terminal
```

ステップ6 パスワードを変更します。

```
Device(config)# enable secret password
```

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ7 特権 EXEC モードに戻ります。

```
Device(config)# exit  
Device#
```

ステップ8 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Device# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。

ステップ9 ここで、デバイスを再設定する必要があります。システム管理者によって、バックアップデバイスと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

コマンドスイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。

スタンバイ コマンドスイッチが未設定で、かつコマンドスイッチで電源故障などの障害が発生した場合には、メンバスイッチとの管理接続が失われるので、新しいコマンドスイッチに交換する必要があります。ただし、接続されているスイッチ間の接続は影響を受けません。また、メンバスイッチも通常どおりにパケットを転送します。メンバスイッチは、コンソールポートを介してスタンドアロンのスイッチとして管理できます。また、IP アドレスが与えられている場合は、他の管理インターフェイスを使用して管理できます。

コマンド対応メンバスイッチまたは他のスイッチに IP アドレスを割り当て、コマンドスイッチのパスワードを書き留め、メンバスイッチと交換用コマンドスイッチ間の冗長接続が得られるようにクラスタを配置することにより、コマンドスイッチ障害に備えます。ここでは、故障したコマンドスイッチの交換方法を 2 通り紹介します。

- 故障したコマンドスイッチをクラスタ メンバーと交換する場合
- 故障したコマンドスイッチを他のスイッチと交換する場合

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。コマンド対応スイッチについては、リリースノートを参照してください。

故障したコマンドスイッチをクラスタメンバーと交換する場合

故障したコマンドスイッチを同じクラスタ内のコマンド対応メンバスイッチに交換するには、次の手順に従ってください。

手順

-
- ステップ 1** メンバスイッチからコマンドスイッチを外し、クラスタからコマンドスイッチを物理的に取り外します。
- ステップ 2** 故障したコマンドスイッチの代わりに新しいメンバスイッチを取り付け、コマンドスイッチとクラスタメンバー間の接続を復元します。
- ステップ 3** 新しいコマンドスイッチで CLI セッションを開始します。
- CLI にはコンソールポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。コンソールポートの使用の詳細については、『*Catalyst 1000 Series Switches Hardware Installation Guide*』を参照してください。
- ステップ 4** スイッチプロンプトで、特権 EXEC モードを開始します。
- 例：
- ```
Device> enable
Switch#
```
- ステップ 5** 故障したコマンドスイッチのパスワードを入力します。
- ステップ 6** 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。
- 例：
- ```
Device# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
```
- ステップ 7** クラスタからメンバスイッチを削除します。
- 例：
- ```
Device(config)# no cluster commander-address
```
- ステップ 8** 特権 EXEC モードに戻ります。
- 例：
- ```
Device(config)# end
Switch#
```
- ステップ 9** セットアッププログラムを使用して、スイッチの IP 情報を設定します。IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードで **setup** と入力し、[Return] キーを押します。

例：

```
Device# setup

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

ステップ 10 最初のプロンプトに **Y** を入力します。

例：

```
The prompts in the setup program vary depending on the member switch that you selected
to be the command switch:
Continue with configuration dialog? [yes/no]: y

or

Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

ステップ 11 セットアッププログラムの質問に応答します。

ホスト名を入力するように要求された場合、メンバスイッチで入力できる文字数は 28～31 文字に制限されます。どのスイッチでも、ホスト名の最終文字として **-n** (*n* は数字) を使用しないでください。**Telnet** (仮想端末) パスワードを入力するように要求された場合、パスワードには 1～25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力します。

ステップ 13 要求された場合は、スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** を押します。

ステップ 14 要求された場合は、クラスタに名前を指定し、**Return** を押します。

クラスタ名には 1～31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 16 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。

情報に誤りがある場合には、**N** を入力し、**[Return]** キーを押して、ステップ 9 からやり直します。

ステップ 17 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

- ステップ 18** クラスタメニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンドスイッチを他のスイッチと交換する場合

故障したコマンドスイッチを、クラスタに組み込まれていないコマンド対応スイッチと交換する場合、次の手順に従ってください。

手順

- ステップ 1** 故障したコマンドスイッチの代わりに新しいスイッチを取り付け、コマンドスイッチとクラスタメンバー間の接続を復元します。
- ステップ 2** CLIにはコンソールポートを使用してアクセスできます。また、スイッチにIPアドレスが割り当てられている場合は、Telnetを使用してアクセスできます。コンソールポートの詳しい使用方法については、スイッチ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。
- ステップ 3** スイッチプロンプトで、特権 EXEC モードを開始します。

例：

```
Switch> enable
Switch#
```

- ステップ 4** 故障したコマンドスイッチのパスワードを入力します。
- ステップ 5** セットアッププログラムを使用して、スイッチのIP情報を設定します。IPアドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードで **setup** と入力し、[Return] キーを押します。

例：

```
Switch# setup

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]:
```

- ステップ 6** 最初のプロンプトに **Y** を入力します。

例：

```
The prompts in the setup program vary depending on the member switch that you selected
to be the command switch:
Continue with configuration dialog? [yes/no]: y

or

Configuring global parameters:
```

このプロンプトが表示されなければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

ステップ 7 セットアッププログラムの質問に応答します。

ホスト名を入力するように要求された場合、メンバスイッチで入力できる文字数は 28～31 文字に制限されます。どのスイッチでも、ホスト名の最終文字として **-n** (*n* は数字) を使用しないでください。**Telnet** (仮想端末) パスワードを入力するように要求された場合、パスワードには 1～25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できませんが、先行スペースは無視されます。

ステップ 8 **enable secret** および **enable** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力します。

ステップ 9 要求された場合は、スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、**Return** を押します。

ステップ 10 要求された場合は、クラスタに名前を指定し、**Return** を押します。

クラスタ名には 1～31 文字の英数字、ダッシュ、または下線を使用できます。

ステップ 11 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 12 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。

情報に誤りがある場合には、**N** を入力し、**[Return]** キーを押して、ステップ 9 からやり直します。

ステップ 13 ブラウザを起動し、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 14 クラスタメニューから、**[Add to Cluster]** を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは速度 (10 Mbps、100 Mbps、および SFP モジュールポート以外の 1000 Mbps) およびデュプレックス (半二重または全二重) に関するデバイスの設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

デバイスのパフォーマンスを最大限に引き出してリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。



- (注) 接続先装置が自動ネゴシエーションを実行しない場合は、2つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別に関するトラブルシューティング

シスコの Small Form-Factor Pluggable (SFP) モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティコード、および巡回冗長検査 (CRC) が格納されたシリアルEEPROM (電氣的に消去可能でプログラミング可能なROM) を備えています。デバイスに SFP モジュールを装着すると、デバイスソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティコードと CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティコード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを **errdisable** ステータスにします。



- (注) セキュリティ エラー メッセージは、**GBIC_SECURITY** 機能を参照します。デバイスは、SFP モジュールをサポートしていますが、**GBIC** (ギガビット インターフェイス コンバータ) モジュールはサポートしていません。エラーメッセージテキストは、**GBIC** インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。

他社の SFP モジュールを使用している場合、デバイスから SFP モジュールを取り外し、シスコのモジュールに交換します。シスコの SFP モジュールを装着したら、**errdisable recovery cause gbic-invalid** 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ポートのステータスを確認し、**error-disabled** 状態から回復する時間間隔を入力します。この時間間隔が経過すると、デバイスは **error-disabled** 状態からインターフェイスを回復させ、操作を再実行します。**errdisable recovery** コマンドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダーデータ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラーメッセージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

SFP モジュール ステータスのモニタリング

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラームステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースに対応するコマンドリファレンスにある **show interfaces transceiver** コマンドを参照してください。

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティックルートを定義するか、またはこれらのサブネットワーク間でルーティングされるように IP ルーティングを設定する必要があります。

IP ルーティングは、デフォルトではすべてのデバイスでディセーブルになります。



(注) **ping** コマンドでは、他のプロトコルキーワードも使用可能ですが、このリリースではサポートされていません。

このコマンドは、デバイスからネットワーク上の他のデバイスに ping を実行する目的で使用します。

コマンド	目的
ping ip host address Device# ping 172.20.52.3	IP またはホスト名やネットワーク アドレスを指定してリモート ホストに ping を実行します。

温度のモニタリング

デバイスは温度条件をモニタし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature status** 特権 EXEC コマンドを使用します。温度の値は、デバイス内の温度です（外部温度ではありません）。

物理パスのモニタリング

次のいずれかの特権 EXEC コマンドを使用して、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスをモニタできます。

表 18: 物理パスのモニタリング

コマンド	目的
tracetroute mac [interface <i>interface-id</i>] { <i>source-mac-address</i> } [interface <i>interface-id</i>] { <i>destination-mac-address</i> } [vlan <i>vlan-id</i>] [detail]	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。
tracetroute mac ip { <i>source-ip-address</i> <i>source-hostname</i> } { <i>destination-ip-address</i> <i>destination-hostname</i> } [detail]	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

IP traceroute の実行



- (注) **tracetroute** 特権 EXEC コマンドでは、他のプロトコルキーワードも使用可能ですが、このリリースではサポートされていません。

コマンド	目的
tracetroute ip <i>host</i> Device# tracetroute ip 192.51.100.1	ネットワーク上でパケットが通過するパスを追跡します。

TDR の実行および結果の表示

TDR を実行するには、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを実行します。

デバッグおよびエラー メッセージ出力のリダイレクト

デフォルトでは、ネットワークサーバが **debug** コマンドからの出力とシステムエラーメッセージをコンソールに送信します。このデフォルトの設定を使用する場合は、コンソールポートまたはイーサネット管理ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、およびsyslogサーバを実行している UNIX ホストがあります。Syslog フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。



(注) デバッグの出力先がシステムのオーバーヘッドに影響を与えることがないように注意してください。メッセージをコンソールに記録すると、非常に高いオーバーヘッドが発生します。仮想端末にメッセージを記録すると、発生するオーバーヘッドは低くなります。Syslog サーバでメッセージロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージのロギングに関する詳細については、「システム メッセージ ロギングの設定」を参照してください。

show platform forward コマンドの使用

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに着信するパケットがシステムを介して送信された場合の転送結果に関する有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるポート マップ、ビットマップ、および出力側の情報が表示されます。

このコマンドで出力される情報のほとんどは、主に、デバイスの特定用途向け集積回路 (ASIC) に関する詳細情報を使用するテクニカルサポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

OBFL の設定



注意 OBFLはディセーブルにせず、フラッシュメモリに保存されたデータは削除しないことを推奨します。

- OBFL をイネーブルにするには、**hw-switch switch [switch-number] logging onboard [message level level]** 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。スイッチでは、*switch-number* に指定できる範囲は1～9です。スイッチが生成してフラッシュメモリに保存するハードウェア関連のメッセージの重大度を指定するには、**message level level** パラメータを使用します。
- OBFL データをローカルネットワークまたは特定のファイルシステムにコピーするには、**copy onboard switch switch-number url url-destination** 特権 EXEC コマンドを使用します。
- OBFL をイネーブルにするには、**no hw-switch switch [switch-number] logging onboard [message level level]** 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。
- フラッシュメモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear onboard switch switch-number** 特権 EXEC コマンドを使用します。
- デバイスのメンバースイッチの OBFL をイネーブルまたはディセーブルにできます。

ここで説明した各コマンドの詳細については、このリリースのコマンドリファレンスを参照してください。

ソフトウェア設定のトラブルシューティングの確認

OBFL 情報の表示

表 19: OBFL 情報を表示するためのコマンド

コマンド	目的
show logging onboard [module[switch-number]] clilog Device# show logging onboard 1 clilog	スタンドアロンスイッチ上に入力された OBFL CLI コマンドを表示します。
show logging onboard [module[switch-number]] environment Device# show logging onboard 1 environment	PID、VID、シリアル番号など、スタンドアロンのスイッチおよび接続されているすべての FRU デバイスの UDI 情報を表示します。
show logging onboard [module[switch-number]] message Device# show logging onboard 1 message	スタンドアロンスイッチによって生成されたハードウェア関連メッセージが表示されます。
show logging onboard [module[switch-number]] poe Device# show logging onboard 1 poe	スタンドアロンスイッチの PoE ポートの消費電力を表示します。
show logging onboard [module[switch-number]] temperature Device# show logging onboard 1 temperature	スタンドアロンスイッチの温度を表示します。
show logging onboard [module[switch-number]] uptime Device# show logging onboard 1 uptime	スタンドアロンスイッチまたは指定されたスタックメンバーが起動した時刻、スタンドアロンスイッチまたは指定されたスタックメンバーが再起動された理由、およびスタンドアロンスイッチが最後に再起動されて以来の稼働時間を表示します。

コマンド	目的
show logging onboard [module[switch-number]] voltage Device# show logging onboard 1 voltage	スタンダアロンスイッチのシステム電圧を表示します。
show logging onboard [module[switch-number]] continuous Device# show logging onboard 1 continuous	連続ファイルのデータを表示します。
show logging onboard [module[switch-number]] detail Device# show logging onboard 1 detail	連続データおよびサマリーデータの両方を表示します。
show logging onboard [module[switch-number]] endhh:mm:ss Device# show logging onboard 1 end 13:00:15 jul 2013	スタンダアロンスイッチの終了日時を表示します。
show logging onboard [module[switch-number]] Device# show logging onboard 1	システム内で指定されているスイッチに関する OBFL 情報を表示します。
show logging onboard [module[switch-number]] raw Device# show logging onboard 1 raw	スタンダアロンスイッチの raw 情報を表示します。
show logging onboard [module[switch-number]] start Device# show logging onboard 1 start 13:00:10 jul 2013	スタンダアロンスイッチの開始日時を表示します。
show logging onboard [module[switch-number]] status Device# show logging onboard 1 status	スタンダアロンスイッチのステータス情報を表示します。
show logging onboard [module[switch-number]] summary Device# show logging onboard 1 summary	サマリーファイルの両方のデータを表示します。

例：高い CPU 使用率に関する問題と原因の確認

CPU 使用率が高いことが問題となっているかどうか判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
Device# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
```

例：高い CPU 使用率に関する問題と原因の確認

```

PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>

```

この例は、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 20: CPU 使用率に関する問題のトラブルシューティング

問題のタイプ	原因	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。 「Analyzing Network Traffic (ネットワークトラフィックの解析)」の項を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。「Debugging Active Processes (アクティブなプロセスのデバッグ)」のセクションを参照してください。

ソフトウェア設定のトラブルシューティングのシナリオ

Power over Ethernet (PoE) に関するトラブルシューティングのシナリオ

表 21 : *Power over Ethernet* に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決法
<p>PoE がないポートは1つに限られません。</p> <p>1つのスイッチポートに限り問題が発生する。このポートではPoE装置と PoE 非対応の装置のいずれも動作しないが、他のポートでは動作します。</p>	

症状または問題	考えられる原因と解決法
	<p>この受電デバイスが他の PoE ポートで動作するかを確認する。</p> <p>show run または show interface status ユーザ EXEC コマンドを使用して、ポートがシャットダウンしていないか、または error-disabled になっていないかを確認します。</p> <p>(注) ほとんどのスイッチはポートがシャットダウンしているときはポートの電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指定されている場合も同様です。</p> <p>該当するインターフェイスまたはポートに power inline never が設定されていないことを確認します。</p> <p>受電デバイスからスイッチポートまでのイーサネットケーブルの動作が正常であることを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置とイーサネットケーブルを接続して、受電デバイスがリンクを確立し他のホストとトラフィックを交換することを確認します。</p> <p>(注) シスコ受電装置は、ストレートケーブルでのみ機能します。クロスオーバーケーブルでは機能しません。</p> <p>スイッチのフロントパネルから受電デバイスまでのケーブル長の合計が 100 メートル以下であることを確認します。</p> <p>スイッチポートからイーサネットケーブルを外します。短いイーサネットケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロントパネルの（パッチパネルではない）このポートに直接接続します。これによってイーサネットリンクが確立され他のホストとトラフィックを交換できることを確認します。あるいは、ポートの VLAN SVI で ping を実行してください。次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。</p> <p>パッチコードをスイッチポートに接続しても受電デバイスの電源がオンにならない場合、接続する受電デバイスの合計数とスイッチの電力バジェット（使用可能な PoE）とを比較してください。 show inline power コマンドを使用して、利用可能な電力量を確認します。</p>

症状または問題	考えられる原因と解決法
<p>すべてのポートまたは1つのポートグループで PoE が機能しない。</p> <p>すべてのスイッチポートで問題が発生する。電力が供給されていないイーサネット装置がどのポートでもイーサネットリンクを確立できず、PoE装置の電源がオンになりません。</p>	

症状または問題	考えられる原因と解決法
	<p>電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。そうでない場合はスイッチを交換してください。</p> <p>連続する複数のポートで問題があるものの、すべてのポートで問題が発生するわけではない場合、電源の故障ではないと考えられ、スイッチのPoEレギュレータに関連した異常の可能性がります。</p> <p>PoE の状況やステータスの変更について過去に報告されているアラームまたはシステムメッセージがないか、show log 特権 EXEC コマンドを使用して調べます。</p> <p>アラームがない場合は、show interface status コマンドを使用して、ポートがシャットダウンしていないか、または error-disabled になっていないかを確認します。ポートが error-disabled の場合、shut および no shut 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、ポートを再度有効にします。</p> <p>show env power および show power inline 特権 EXEC コマンドを使用して、PoEのステータスおよび電力バジェット（使用可能な PoE）を調べます。</p> <p>実行コンフィギュレーションを調べて、power inline never がこのポートに設定されていないことを確認します。</p> <p>受電していないイーサネット装置をスイッチポートに直接接続します。接続には短いパッチ コードだけを使用します。既存の配線ケーブルは使用しないでください。shut および no shut 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、イーサネットリンクが確立されていることを確認します。正しく接続している場合、短いパッチコードを使用して受電デバイスをこのポートに接続し、電源がオンになることを確認します。装置の電源がオンになったら、すべての中間パッチパネルが正しく接続されているか確認してください。</p> <p>1本を除くすべてのイーサネットケーブルをスイッチポートから抜きます。短いパッチコードを使用して、1つのPoEポートにだけ受電デバイスを接続します。スイッチポートからの受電に比較して、受電デバイスが多くの電力を必要としないことを確認してください。</p> <p>show power inline 特権 EXEC コマンドを使用して、ポートがシャットダウンされていない場合に、受電デバイスに電力が供給されることを確認します。あるいは、受電デバイ</p>

症状または問題	考えられる原因と解決法
	<p>スを観察して電源がオンになることを確認してください。</p> <p>1 台の受電デバイスだけがスイッチに接続している際に電力が供給される場合、残りのポートで shut および no shut インターフェイス コンフィギュレーション コマンドを入力してから、イーサネットケーブルをスイッチの PoE ポートに 1 本ずつ再接続してください。 show interface status および show power inline 特権 EXEC コマンドを使用して、インラインパワーの統計情報とポートのステータスをモニタします。</p> <p>すべてのポートで、まだ PoE が機能しない場合は、電源装置の PoE セクションでヒューズを開くことができる場合があります。この場合、アラームが生成されるのが一般的です。過去にシステムメッセージでアラームが報告されていないか、ログをもう一度チェックしてください。</p>
<p>シスコ先行標準受電装置は、切断またはリセットされます。</p> <p>正常に動作した後で、シスコ電話機が断続的にリロードしたり、PoE から切断されたりします。</p>	<p>スイッチから受電デバイスまでのすべての電気系統を確認してください。信頼性の低い接続は、電力供給の中断や受電デバイスの機能が不安定になる原因となり、受電デバイスの断続的な切断やリロードが発生します。</p> <p>スイッチ ポートから受電デバイスまでのケーブル長が 100 メートル以下であることを確認してください。</p> <p>スイッチが配置されている場所で電気環境にどのような変化があるか、切断時に、受電デバイスに何が起きるかについて注意してください。</p> <p>切断と同時にエラー メッセージが表示されたか注意します。 show log 特権 EXEC コマンドを使用して、エラーメッセージを確認します。</p> <p>リロードの発生直前に IP Phone から Call Manager へのアクセスが失われていないか確認してください (PoE の障害ではなくネットワークに問題が発生している場合があります)。</p> <p>受電デバイスを PoE 非対応の装置に交換し、装置が正しく動作することを確認します。PoE 非対応の装置にリンク障害または高いエラー率がある場合、スイッチポートと受電デバイスを接続する信頼性の低いケーブル接続が問題の可能性もあります。</p>

症状または問題	考えられる原因と解決法
IEEE 802.3af 準拠または IEEE 802.3at 準拠の受電装置は、Cisco PoE スイッチでは機能しません。 シスコ PoE スイッチに接続するシスコ以外の受電デバイスに電源が供給されないか、電源投入後すぐに電源が切れます。PoE 非対応装置は正常に動作します。	<p>show power inline コマンドを使用して、受電デバイスの接続前後に、スイッチの電力バジェット（使用可能な PoE）が枯渇していないか確認します。受電デバイスを接続する前に、このタイプの装置に十分な電力が使用可能であることを確認します。</p> <p>show interface status コマンドを使用して、接続されている受電デバイスがスイッチに検出されることを確認します。</p> <p>show log コマンドを使用して、ポートの過電流状態を報告したシステムメッセージがないか確認します。症状を正確に特定してください。最初に電力が受電デバイスに供給され、その後、切断される状態ですか。その場合は、問題は最初のサージ電流（突入電流）が原因で、ポートの電流上限しきい値が超過した可能性があります。</p>

ソフトウェアのトラブルシューティングの設定例

例：IP ホストの ping

次に、IP ホストに ping を実行する例を示します。

```
Device# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Device#
```

表 22: ping の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。

文字	説明
?	パケットタイプが不明です。
&	パケットの存続時間を超過したことを示します。

pingセッションを終了するには、エスケープシーケンス（デフォルトではCtrl+^X）を入力してください。Ctrlキー、Shiftキー、および6キーを同時に押してから放し、その後Xキーを押します。

例：IP ホストに対する traceroute の実行

次に、IP ホストに **traceroute** を実行する例を示します。

```
Device# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  0 192.0.2.1 0 msec 0 msec 4 msec
  1 192.0.2.203 12 msec 8 msec 0 msec
  2 192.0.2.100 4 msec 0 msec 0 msec
  3 192.0.2.10 0 msec 4 msec 0 msec
```

ディスプレイには、送信される3つのプローブごとに、ホップカウント、ルータのIPアドレス、およびラウンドトリップタイム（ミリ秒単位）が表示されます。

表 23: traceroute の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケットタイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセスリストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

例：すべてのシステム診断をイネーブルにする

実行中の追跡を終了するには、エスケープシーケンス（デフォルトではCtrl+^X）を入力してください。Ctrl キー、Shift キー、および6 キーを同時に押してから放し、その後 X キーを押します。

例：すべてのシステム診断をイネーブルにする



注意 デバッグ出力は他のネットワークトラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

このコマンドは、すべてのシステム診断をディセーブルにします。

```
Device# debug all
```

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

ソフトウェア設定のトラブルシューティングに関する追加情報

関連資料

関連項目	マニュアル タイトル
トラブルシューティング コマンド	<i>Catalyst 1000 Series Switches System Management Command Reference</i>
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	<i>Catalyst 1000 Series Switches Interface and Hardware Component Configuration Guide</i>
プラットフォームに依存しないコマンド リファレンス	<i>Cisco IOS 15.3M&T</i> コマンド リファレンス
プラットフォームに依存しない設定情報	<i>Cisco IOS 15.3M&T</i> コンフィギュレーション ガイド

ソフトウェア設定のトラブルシューティングの機能履歴と情報

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。

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 24: ソフトウェア設定のトラブルシューティングの機能履歴と情報

機能	リリース	機能情報
ソフトウェア設定のトラブルシューティング	Cisco IOS Release 15.2(7)E1	この機能が導入されました。

