



Cisco IOS リリース 15.2(8)E (Catalyst マイクロスイッチシリーズ) 統合プラットフォーム コマンドリファレンス

初版：2021年4月26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)

© 2021 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

コマンドラインインターフェイスの使用 1

コマンドラインインターフェイスの使用 2

コマンドモードについて 2

ヘルプシステムについて 4

コマンドの省略形 5

コマンドの no 形式および default 形式の概要 5

CLI のエラーメッセージについて 6

コンフィギュレーション ロギングの使用 6

コマンド履歴の使用 7

コマンド履歴バッファ サイズの変更 7

コマンドの呼び出し 7

コマンド履歴機能の無効化 8

編集機能の使用 8

編集機能の有効化および無効化 8

キーストロークによるコマンドの編集 9

画面幅よりも長いコマンドラインの編集 11

show および more コマンド出力の検索およびフィルタリング 12

CLI のアクセス 12

コンソール接続または Telnet による CLI アクセス 13

第 1 部 :

インターフェイスおよびハードウェア 15

第 2 章

インターフェイスおよびハードウェア コマンド 17

debug ilpower 19

debug interface	20
debug lldp packets	21
debug nmsp	22
duplex	23
errdisable detect cause	25
errdisable detect cause small-frame	28
errdisable recovery cause	29
errdisable recovery interval	32
lldp (インターフェイス コンフィギュレーション)	33
mdix auto	35
network-policy	36
network-policy profile (グローバル コンフィギュレーション)	37
nmsp attachment suppress	38
power efficient-ethernet auto	39
power inline	40
power inline consumption	44
power inline police	47
power inline ps watt	50
show eee	51
show env	55
show errdisable detect	58
show errdisable recovery	60
show hardware led	62
show interfaces	66
show interfaces counters	71
show interfaces switchport	74
show interfaces transceiver	77
show ip ports all	80
show network-policy profile	81
show power	82
show power inline	83
speed	87
switchport block	89
voice-signaling vlan (ネットワークポリシー コンフィギュレーション)	91

voice vlan (ネットワークポリシー コンフィギュレーション) 93

第 11 部 :

レイヤ 2 95

第 3 章

レイヤ 2 コマンド 97

channel-group 100
channel-protocol 105
clear lacp 106
clear pagp 107
clear spanning-tree counters 108
clear spanning-tree detected-protocols 109
debug etherchannel 110
debug lacp 112
debug pagp 113
debug platform etherchannel 115
debug platform pm 116
debug spanning-tree 119
interface port-channel 121
lacp port-priority 123
lacp system-priority 125
pagp learn-method 126
pagp port-priority 128
pagp timer 129
rep admin vlan 130
rep block port 132
rep lsl-age-timer 134
rep preempt delay 135
rep preempt segment 137
rep preempt segment 139
rep stcn 141
show etherchannel 142
show interfaces rep detail 146
show lacp 148
show pagp 153

show platform etherchannel	155
show platform pm	156
show platform spanning-tree	158
show rep topology	159
show spanning-tree	161
show udld	165
spanning-tree backbonefast	168
spanning-tree bpduguard	169
spanning-tree bpduguard	171
spanning-tree bridge assurance	172
spanning-tree cost	174
spanning-tree etherchannel guard misconfig	176
spanning-tree extend system-id	177
spanning-tree guard	178
spanning-tree link-type	180
spanning-tree loopguard default	181
spanning-tree mode	182
spanning-tree mst configuration	183
spanning-tree mst cost	185
spanning-tree mst forward-time	186
spanning-tree mst hello-time	187
spanning-tree mst max-age	188
spanning-tree mst max-hops	189
spanning-tree mst port-priority	190
spanning-tree mst pre-standard	191
spanning-tree mst priority	192
spanning-tree mst root	193
spanning-tree mst simulate pvst (グローバル コンフィギュレーション)	195
spanning-tree mst simulate pvst (インターフェイス コンフィギュレーション)	197
spanning-tree pathcost method	199
spanning-tree mst port-priority	200
spanning-tree portfast edge (グローバル コンフィギュレーション)	201
spanning-tree portfast edge (インターフェイス コンフィギュレーション)	204
spanning-tree transmit hold-count	206

spanning-tree uplinkfast 207
spanning-tree vlan 209
switchport access vlan 211
switchport mode 214
switchport nonegotiate 217
udld 219
udld port 221
udld reset 223

第 III 部 : ネットワーク管理 225

第 4 章 ネットワーク管理 227

monitor session destination 228
monitor session source 233
show monitor 236
snmp-server enable traps 239
snmp-server enable traps bridge 242
snmp-server enable traps cpu 243
snmp-server enable traps envmon 244
snmp-server enable traps errdisable 245
snmp-server enable traps flash 246
snmp-server enable traps mac-notification 247
snmp-server enable traps port-security 248
snmp-server enable traps rtr 249
snmp-server enable traps snmp 251
snmp-server enable snmp traps storm-control 252
snmp-server enable traps stpx 253

第 IV 部 : QoS 255

第 5 章 QoS 257

class 258
debug qos 261
mls qos 263

mls qos cos	265
mls qos wrr-queue output cos-map	267
priority-queue out	269
show mls qos	270
show mls qos interface	271
wrr-queue bandwidth limit	274
wrr-queue bandwidth shape	275

第 V 部 :

セキュリティ 277

第 6 章

セキュリティ 279

aaa accounting dot1x	281
aaa accounting identity	283
aaa authentication dot1x	285
aaa authorization network	286
aaa new-model	287
authentication host-mode	289
authentication logging verbose	291
authentication mac-move permit	292
authentication priority	293
authentication violation	296
cisp enable	298
clear errdisable interface vlan	300
clear mac address-table	302
deny (MAC アクセス リスト コンフィギュレーション)	304
dot1x critical (グローバル コンフィギュレーション)	308
dot1x logging verbose	309
dot1x pae	310
dot1x supplicant force-multicast	311
dot1x test eapol-capable	312
dot1x test timeout	313
dot1x timeout	314
epm access-control open	317
ip access-group	318

ip admission	320
ip admission name	321
ip device tracking maximum	324
ip device tracking probe	325
ip dhcp snooping database	326
ip dhcp snooping information option format remote-id	328
ip dhcp snooping verify no-relay-agent-address	329
ip source binding	330
ip ssh source-interface	332
limit address-count	333
mab request format attribute 32	334
mab logging verbose	336
permit (MAC アクセス リスト コンフィギュレーション)	337
radius server	341
show aaa clients	343
show aaa command handler	344
show aaa local	345
show aaa servers	346
show aaa sessions	347
show authentication sessions	348
show auto security	351
show cisp	353
show dot1x	355
show eap pac peer	357
show ip dhcp snooping statistics	358
show ip ssh	361
show radius server-group	363
show vlan group	365
switchport port-security aging	366
switchport port-security mac-address	368
switchport port-security maximum	371
switchport port-security violation	373
vlan group	375

第 VI 部 :	システム管理	377
----------	--------	-----

第 7 章	システム管理コマンド	379
	archive download-sw	381
	archive tar	385
	archive upload-sw	389
	boot	391
	boot buffersize	393
	boot enable-break	394
	boot host dhcp	395
	boot host retry timeout	396
	boot manual	397
	boot system	398
	cat	399
	clear logging onboard	400
	clear mac address-table	401
	clear mac address-table move update	402
	copy	403
	debug matm move update	404
	delete	405
	dir	406
	help	408
	hw-module	409
	ip name-server	411
	logging	413
	logging buffered	414
	logging console	415
	logging file flash	417
	logging history	418
	logging history size	419
	logging monitor	420
	logging trap	421
	mac address-table notification	422

mac address-table static	424
mkdir	425
more	426
nmsp notification interval	427
rename	429
reset	430
rmdir	431
service sequence-numbers	432
set	433
show boot	436
show cable-diagnostics tdr	439
show mac address-table	441
show mac address-table address	442
show mac address-table aging-time	443
show mac address-table count	444
show mac address-table dynamic	445
show mac address-table interface	446
show mac address-table move update	447
show mac address-table multicast	448
show mac address-table notification	449
show mac address-table static	451
show mac address-table vlan	452
show nmsp	453
show logging onboard	455
shutdown	457
test cable-diagnostics tdr	458
traceroute mac	459
traceroute mac ip	462
type	465
unset	466
version	468

第 VII 部 : **VLANs** 469

第 8 章

VLAN 471

- clear vtp counters 472
- debug platform vlan 473
- debug sw-vlan 474
- debug sw-vlan ifs 476
- debug sw-vlan notification 477
- debug sw-vlan vtp 479
- interface vlan 481
- show platform vlan 483
- show vlan 484
- show vtp 487
- switchport priority extend 495
- switchport trunk 497
- switchport voice vlan 500
- vlan 503
- vtp (グローバル コンフィギュレーション) 511
- vtp (インターフェイス コンフィギュレーション) 517
- vtp primary 518



コマンドラインインターフェイスの使用

この章は、次の内容で構成されています。

- [コマンドラインインターフェイスの使用 \(2 ページ\)](#)

コマンドラインインターフェイスの使用

この章では、Cisco IOS コマンドラインインターフェイス (CLI) について説明し、CLI を使用してスイッチを設定する方法について説明します。



- (注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナルリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

コマンドモードについて

Cisco IOS ユーザインターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンドモードで使用できるコマンドのリストを取得するには、システムプロンプトで疑問符 (?) を入力します。

スイッチとのセッションを開始するときは、ユーザモード (別名ユーザ EXEC モード) が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえば、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード (グローバル、インターフェイス、およびライン) を使用して、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

次の表に、主要なコマンドモード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表の例では、ホスト名として *Switch* を使用しています。

表 1: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	Switch>	logout または quit の入力。	このモードを使用して次の作業を行います。 <ul style="list-style-type: none"> • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、 enable コマンドを入力します。	#	終了するには、 disable と入力します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、 configure コマンドを入力します。	(config)#	終了して特権 EXEC モードに戻るには、 exit または end を入力するか、 Ctrl+Z を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
VLAN コンフィギュレーション	グローバル コンフィギュレーションモードで、 vlan <i>vlan-id</i> コマンドを入力します。	(config-vlan)#	グローバル コンフィギュレーションモードに戻る場合は、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	このモードを使用して、VLAN（仮想 LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップ コンフィギュレーションファイルに設定を保存できます。

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、 interface コマンド を入力し、イン ターフェイスを指 定します。	(config-if)#	終了してグローバル コンフィギュレー ションモードに戻る には、 exit を入力しま す。 特権 EXEC モードに 戻るには、 Ctrl+Z を 押すか、 end を入力し ます。	このモードを使用し て、イーサネットポー トのパラメータを設定 します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで回線を 指定するには、 linevt または line console コマンドを 入力します。	(config-line)#	終了してグローバル コンフィギュレー ションモードに戻る には、 exit を入力しま す。 特権 EXEC モードに 戻るには、 Ctrl+Z を 押すか、 end を入力し ます。	このモードを使用し て、端末回線のパラ メータを設定します。

コマンドモー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ガイドを参照してください。

ヘルプシステムについて

システムプロンプトに疑問符 (?) を入力すると、各コマンドモードで使用できるコマンドの一覧が表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

表 2: ヘルプの概要

コマンド	目的
help	コマンドモードのヘルプシステムの簡単な説明を表示します。
<i>abbreviated-command-entry ?</i> # di? dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。

コマンド	目的
<code>abbreviated-command-entry <Tab></code> <pre># sh conf<tab> # show configuration</pre>	特定のコマンド名を補完します。
<code>?</code> <pre>Switch> ?</pre>	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
<code>command ?</code> <pre>Switch> show ?</pre>	コマンドに関連するキーワードを一覧表示します。
<code>command keyword ?</code> <pre>(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</pre>	キーワードに関連する引数を一覧表示します。

コマンドの省略形

コマンドの先頭から、スイッチが特定のコマンドとして認識できる文字数だけを入力し、後は省略できます。

showconfiguration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
# show conf
```

コマンドの **no** 形式および **default** 形式の概要

ほとんどのコンフィギュレーションコマンドには、**no** 形式もあります。**no** 形式は一般に、特定の機能または動作を無効にする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、インターフェイス コンフィギュレーション コマンド **no shutdown** を使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** なしでコマンドを使用すると、無効にされた機能を再度有効にしたり、デフォルトで無効になっている機能を有効にすることができます。

コンフィギュレーションコマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンド設定をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、**default** 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトで有効に設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。

す。このような場合、**default** コマンドはそのコマンドを有効にし、変数とそのデフォルト値に設定します。

CLI のエラーメッセージについて

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラーメッセージの一部を紹介します。

表 3: CLI の代表的なエラーメッセージ

エラーメッセージ	意味	ヘルプの表示方法
% Ambiguous command: "show con"	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Invalid input detected at '^' marker.	コマンドの入力ミスです。間違っている箇所をキャレット (^) 記号で示しています。	疑問符 (?) を入力すると、そのコマンドモードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギングの使用法

スイッチの設定変更を記録して表示させることができます。Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーションコマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターンコードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。Syslog へこの通知を送信することも選択できます。



(注) CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、10のコマンドラインが履歴バッファに保存されます。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。これらの手順は任意です。

現在の端末セッションで保存されるコマンドライン数を変更するには、特権EXECモードで次のコマンドを入力します。

```
# terminal history [size number-of-lines]
```

指定できる範囲は0～256です。

特定の回線に関するすべてのセッションで保存されるコマンドライン数を設定するには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
(config-line)# history [size number-of-lines]
```

指定できる範囲は0～256です。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。



(注) 矢印キーが使用できるのは、VT100などのANSI互換端末に限られます。

表 4: コマンドの呼び出し

アクション	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。

アクション	結果
show history (config)# help	特権 EXEC モードで、直前に入力したいくつかのコマンドを一覧表示します。表示されるコマンドの数は、 terminal history グローバルコンフィギュレーションコマンドおよび history ラインコンフィギュレーションコマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的に有効になっています。現在の端末セッションまたはコマンドラインで無効にできます。これらの手順は任意です。

現在の端末セッションでこの機能を無効にするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴を無効にするには、**no history** ラインコンフィギュレーションコマンドを使用します。

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。

編集機能の有効化および無効化

拡張編集モードは自動的に有効になりますが、無効にする、再び有効にする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

拡張編集モードをグローバルに無効にするには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
Switch (config-line)# no editing
```

現在の端末セッションで拡張編集モードを再び有効にするには、特権 EXEC モードで次のコマンドを入力します。

```
# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ラインコンフィギュレーションモードで次のコマンドを入力します。

```
(config-line)# editing
```

キーストロークによるコマンドの編集

このテーブルに、コマンドラインの編集に必要なキーストロークを示します。これらのキーストロークは任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 5:キーストロークによるコマンドの編集

機能	キーストローク	目的
コマンドライン上を移動して、変更または訂正を行います。	Ctrl+B または左矢印キーを押します。	カーソルを 1 文字後退させます。
	Ctrl+F または右矢印キーを押します。	カーソルを 1 文字前進させます。
	Ctrl+A を押します。	コマンドラインの先頭にカーソルを移動します。
	Ctrl+E を押します。	カーソルをコマンドラインの末尾に移動します。
	Esc+B を押します。	カーソルを 1 単語後退させます。
	Esc+F を押します。	カーソルを 1 単語前進させます。
	Ctrl+T を押します。	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
バッファからコマンドを呼び出し、コマンドラインにペーストします。最後に削除した 10 項目がバッファに保存されています。	Ctrl+Y を押します。	バッファ内の最新のエントリを呼び出します。
	Esc+Y を押します。	次のバッファエントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。Esc+Y を 11 回以上押すと、最初のバッファエントリに戻って表示されます。

機能	キーストローク	目的
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
	Ctrl+U または Ctrl+X を押します。	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
	Ctrl+W を押します。	カーソルの左にある単語を削除します。
	Esc+D を押します。	カーソルの位置から単語の末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソルの場所にある単語を小文字にします。
	Esc+U を押します。	カーソルの位置から単語の末尾までを大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	Ctrl+V または Esc+Q キーを押します。	

機能	キーストローク	目的
1行または1画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 (注) show コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。	Return キーを押します。	1行下にスクロールします。
	Space キーを押します。	1画面分下にスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンドラインを再表示します。	Ctrl+L または Ctrl+R を押します。	現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で1行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは10文字分だけ左へシフトされます。コマンドラインの先頭から10文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、Ctrl+A を押します。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンド エントリが1行分よりも長くなっています。最初にカーソルが行末に達すると、その行は10文字分だけ左へシフトされ、再表示されます。ドル記号 (\$) は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び10文字分だけ左へシフトされます。

```
(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
```

```
(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。行末に表示されるドル記号 (\$) は、その行が右へスクロールされたことを表します。

```
(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号 (|) 、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

```
command | {begin | include | exclude} regular-expression
```

文字列では、大文字と小文字が区別されます。たとえば、**|exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

次の例では、**protocol** が使用されている行だけを出力するように指定する方法を示します。

```
# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

CLI のアクセス

CLIにはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。

スイッチスタックおよびスイッチメンバインターフェイスは、アクティブスイッチを経由して管理します。スイッチごとにスイッチスタックメンバを管理することはできません。1つまたは複数のスイッチメンバのコンソールポートまたはイーサネット管理ポートを経由してアクティブスイッチへ接続できます。アクティブスイッチへの複数の CLI セッションを使用する場合は注意が必要です。1つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。



(注) スイッチスタックを管理する場合は、1つの CLI セッションを使用することを推奨します。

特定のスイッチメンバポートを設定する場合は、CLI コマンドインターフェイス表記にスイッチメンバ番号を含めてください。

特定のスイッチメンバをデバッグする場合は、**session stack-member-number** 特権 EXEC コマンドでアクティブスイッチからアクセスできます。スイッチメンバ番号は、システムプロンプトに追加されます。たとえば、*Switch-2#* はスイッチメンバ 2 の特権 EXEC モードのプロンプトであり、アクティブスイッチのシステムプロンプトは *Switch* です。特定のスタックメンバへの CLI セッションで使用できるのは、**show** コマンドと **debug** コマンドに限ります。

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのハードウェア インストレーション ガイドに記載されている手順で、スイッチのコンソールポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

CLI アクセスはスイッチのセットアップの前に使用できます。スイッチが設定された後は、リモート Telnet セッションまたは SSH クライアントで CLI にアクセスできます。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソールポートに管理ステーションまたはダイヤルアップ モデムを接続するか、イーサネット管理ポートに PC を接続します。コンソールポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュアシェル (SSH) パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブルシークレットパスワードを設定しておくことも必要です。

スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソールポート、イーサネット管理ポート、Telnet セッション、または SSH セッション経由で接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。



第 1 部

インターフェイスおよびハードウェア

- [インターフェイスおよびハードウェア コマンド \(17 ページ\)](#)



インターフェイスおよびハードウェア コマンド

- `debug ilpower` (19 ページ)
- `debug interface` (20 ページ)
- `debug lldp packets` (21 ページ)
- `debug nmsp` (22 ページ)
- `duplex` (23 ページ)
- `errdisable detect cause` (25 ページ)
- `errdisable detect cause small-frame` (28 ページ)
- `errdisable recovery cause` (29 ページ)
- `errdisable recovery interval` (32 ページ)
- `lldp` (インターフェイス コンフィギュレーション) (33 ページ)
- `mdix auto` (35 ページ)
- `network-policy` (36 ページ)
- `network-policy profile` (グローバル コンフィギュレーション) (37 ページ)
- `nmsp attachment suppress` (38 ページ)
- `power efficient-ethernet auto` (39 ページ)
- `power inline` (40 ページ)
- `power inline consumption` (44 ページ)
- `power inline police` (47 ページ)
- `power inline ps watt` (50 ページ)
- `show eec` (51 ページ)
- `show env` (55 ページ)
- `show errdisable detect` (58 ページ)
- `show errdisable recovery` (60 ページ)
- `show hardware led` (62 ページ)
- `show interfaces` (66 ページ)
- `show interfaces counters` (71 ページ)
- `show interfaces switchport` (74 ページ)

- [show interfaces transceiver](#) (77 ページ)
- [show ip ports all](#) (80 ページ)
- [show network-policy profile](#) (81 ページ)
- [show power](#) (82 ページ)
- [show power inline](#) (83 ページ)
- [speed](#) (87 ページ)
- [switchport block](#) (89 ページ)
- [voice-signaling vlan](#) (ネットワークポリシー コンフィギュレーション) (91 ページ)
- [voice vlan](#) (ネットワークポリシー コンフィギュレーション) (93 ページ)

debug ilpower

電源コントローラおよびPoweroverEthernet (PoE) システムのデバッグをイネーブルにするには、特権 EXEC モードで **debug ilpower** コマンドを使用します。デバッグ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。

```
debug ilpower {cdp | event | ha | port | powerman | registries | scp | sense}
no debug ilpower {cdp | event | ha | port | powerman | registries | scp | sense}
```

構文の説明

cdp	PoE Cisco Discovery Protocol (CDP) デバッグ メッセージを表示します。
event	PoE イベント デバッグ メッセージを表示します。
ha	PoE ハイ アベイラビリティ メッセージを表示します。
port	PoE ポート マネージャ デバッグ メッセージを表示します。
powerman	PoE 電力管理デバッグ メッセージを表示します。
registries	PoE レジストリ デバッグ メッセージを表示します。
scp	PoE SCP デバッグ メッセージを表示します。
sense	PoE sense デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PoE 対応スイッチだけでサポートされています。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。メンバスイッチのデバッグを有効にする場合は、**session switch-number EXEC** コマンドを使用して、アクティブスイッチからのセッションを開始できます。次に、メンバスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE EXEC** コマンドを使用します。

debug interface

インターフェイス関連アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug interface** コマンドを使用します。デバッグ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。

no debug interface {*interface-id*|**counters** {**exceptions**|**protocol memory**} | **null** *interface-number* | **port-channel** *port-channel-number* | **states** | **vlan** *vlan-id*}

構文の説明

interface-id	物理インターフェイスの ID です。タイプスイッチ番号/モジュール番号/ポート（例：gigabitethernet 1/0/2）によって識別される指定された物理ポートのデバッグ メッセージを表示します。
counters	カウンタ デバッグ情報を表示します。
exceptions	インターフェイス パケットおよびデータ レート統計情報の計算中に回復可能な例外条件が発生したときにデバッグ メッセージを表示します。
protocol memory	プロトコル カウンタのメモリ操作のデバッグ メッセージを表示します。
states	インターフェイスの状態が移行するときに中間のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

undebug interface コマンドは **no debug interface** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。メンバスイッチのデバッグを有効にする場合は、**session switch-number** EXEC コマンドを使用して、アクティブスイッチからのセッションを開始できます。次に、メンバスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE** EXEC コマンドを使用します。

debug lldp packets

Link Layer Discovery Protocol (LLDP) パケットのデバッグをイネーブルにするには、特権 EXEC モードで **debug lldp packets** コマンドを使用します。デバッグ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。

debug lldp packets
no debug lldp packets

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebug lldp packets コマンドは **no debug lldp packets** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。メンバスイッチのデバッグを有効にする場合は、**session switch-number** 特権 EXEC コマンドを使用して、アクティブスイッチからのセッションを開始できます。

debug nmsp

スイッチの Network Mobility Services Protocol (NMSP) のデバッグをイネーブルにするには、特権 EXEC モードで **debug nmsp** コマンドを使用します。デバッグ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。

debug nmsp {all | connection | error | event | packet | rx | tx}
no debug nmsp

構文の説明

all	すべての NMSP デバッグ メッセージを表示します。
connection	NMSP 接続イベントのデバッグ メッセージを表示します。
error	NMSP エラー メッセージのデバッグ情報を表示します。
event	NMSP イベントのデバッグ メッセージを表示します。
rx	NMSP 受信メッセージのデバッグ情報を表示します。
tx	NMSP 送信メッセージのデバッグ情報を表示します。
packet	NMSP パケットイベントのデバッグメッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン



(注) Cisco IOS XE Denali 16.1.1 以降のリリースでは、アタッチメント情報はサポートされません。

undebug nmsp コマンドは **no debug nmsp** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。メンバスイッチのデバッグを有効にする場合は、**session switch-number** EXEC コマンドを使用して、アクティブスイッチからのセッションを開始できます。次に、メンバスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE** EXEC コマンドを使用します。

duplex

ポートのデュプレックスモードで動作するように指定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto** | **full** | **half**}
no duplex {**auto** | **full** | **half**}

構文の説明

auto 自動によるデュプレックス設定をイネーブルにします。接続されたデバイスモードにより、ポートが自動的に全二重モードか半二重モードで動作すべきかを判断します。

full 全二重モードをイネーブルにします。

half 半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

コマンド デフォルト

ギガビット イーサネット ポートに対するデフォルトは **auto** です。

100BASE-x（-xは -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **half** です。

二重オプションは、1000BASE-x または 10GBASE-x（-xは -BX、-CWDM、-LX、-SX、または -ZX）SFP モジュールではサポートされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ギガビット イーサネット ポートでは、接続デバイスがデュプレックスパラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**full** を指定するのと同じ効果があります。



(注) デュプレックスモードが **auto** で、コネクティッドデバイスが半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエー

ションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。



注意 インターフェイス速度およびデュプレックスモードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# duplex full
```

errdisable detect cause

特定の原因またはすべての原因に対して errdisable 検出をイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable detect cause** コマンドを使用します。errdisable 検出機能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。

```
errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|psp shutdown vlan|security-violation shutdown vlan|sfp-config-mismatch}
no errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|psp shutdown vlan|security-violation shutdown vlan|sfp-config-mismatch}
```

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミックアドレス解決プロトコル (ARP) インспекションのエラー検出をイネーブルにします。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol (DHCP) スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	ダイナミック トランッキング プロトコル (DTP) フラップのエラー検出をイネーブルにします。
gbic-invalid	無効なギガビットインターフェイスコンバータ (GBIC) モジュール用のエラー検出をイネーブルにします。 (注) このエラーは、無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。
inline-power	Power over Ethernet (PoE) の errdisable 原因に対して、エラー検出をイネーブルにします。 (注) このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。
pagp-flap	ポート集約プロトコル (PAgP) フラップの errdisable 原因のエラー検出をイネーブルにします。

pppoe-ia-rate-limit	PPPoE 中継エージェントのレート制限 errdisable 原因に対して、エラー検出をイネーブルにします。
psp shutdown vlan	プロトコルストームプロテクション (PSP) のエラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 IEEE 802.1X セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト 検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 原因 (link-flap、dhcp-rate-limit など) は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、リンクダウンステートに類似した動作ステートとなります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。ブリッジプロトコルデータユニット (BPDU) ガード、音声認識 802.1X セキュリティ、およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN のみをシャットダウンするようにスイッチを設定できます。

errdisable recovery 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、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、インターフェイスを手動で errdisable ステートから回復させる必要があります。

プロトコルストームプロテクションでは、最大 2 個の仮想ポートについて過剰なパケットがドロップされます。**psp** キーワードを使用した仮想ポートの errdisable は、EtherChannel および Flexlink インターフェイスではサポートされません。

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

次の例では、リンクフラップ errdisable 原因に対して errdisable 検出をイネーブルにする方法を示します。

```
Device(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable ステートで BPDU ガードをグローバルに設定する方法を示します。

```
Device(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable ステートで音声認識 802.1X セキュリティをグローバルに設定する方法を示します。

```
Device(config)# errdisable detect cause security-violation shutdown vlan
```

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

errdisable detect cause small-frame

着信 VLAN タグ付きパケットのフレームが小さく（67 バイト以下）、設定された最低速度（しきい値）で到着する場合に、任意のスイッチポートを **error-disabled** にできるようにするには、スイッチスタックまたはスタンドアロンスイッチ上で **errdisable detect cause small-frame** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable detect cause small-frame
no errdisable detect cause small-frame

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

この機能はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、小さいフレームの着信機能をグローバルにイネーブルにします。各ポートのしきい値を設定するには、**small violation-rate** インターフェイス コンフィギュレーション コマンドを使用します。

ポートが自動的に再びイネーブルになるように設定するには、**errdisable recovery cause small-frame** 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。回復時間を設定するには、**errdisable recovery interval interval** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、小さい着信フレームが設定されたしきい値で到着すると **errdisable** モードになるスイッチ ポートをイネーブルにする方法を示します。

```
Device(config)# errdisable detect cause small-frame
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

errdisable recovery cause

特定の原因から回復するように errdisable メカニズムをイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable recovery cause** コマンドを使用します。デフォルト 設定に戻すには、このコマンドの **no** 形式を使用します。

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure | pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control | udld | vmps}
```

```
no errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure | pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control | udld | vmps}
```

構文の説明

all	すべての errdisable の原因から回復するタイマーをイネーブルにします。
arp-inspection	アドレス解決プロトコル (ARP) 検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
bpduguard	ブリッジプロトコルデータユニット (BPDU) ガード errdisable ステートから回復するタイマーをイネーブルにします。
channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
dtp-flap	ダイナミック トランッキングプロトコル (DTP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	ギガビットインターフェイスコンバータ (GBIC) モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 (注) このエラーは無効な Small Form-Factor Pluggable (SFP) の errdisable ステートを意味します。
inline-power	Power over Ethernet (PoE) の errdisable ステートから回復するタイマーをイネーブルにします。 このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。

link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル (PAgP) フラップ errdisable ステートから回復するタイマーをイネーブルにします。
port-mode-failure	ポートモードの変更失敗の errdisable ステートから回復するタイマーをイネーブルにします。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポートセキュリティ違反ディセーブルステートから回復するタイマーをイネーブルにします。
psp	プロトコルストームプロテクション (PSP) の errdisable ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1X 違反ディセーブルステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。
udld	単方向リンク検出 (UDLD) errdisable ステートから回復するタイマーをイネーブルにします。
vmmps	VLAN メンバーシップ ポリシー サーバ (VMPS) errdisable ステートから回復するタイマーをイネーブルにします。

コマンド デフォルト すべての原因に対して回復はディセーブルです。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 原因 (all、BPDU ガードなど) は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート (リンクダウンステートに類似した動作ステート) となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因の回復をイネーブルにしない場合、インターフェイスは、**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 コマンドが入力されるまで errdisable ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でインターフェイスを errdisable ステートから回復させる必要があります。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

例

次の例では、BPDU ガード errdisable 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Device(config)# errdisable recovery cause bpduguard
```

errdisable recovery interval

errdisable ステートから回復する時間を指定するには、グローバルコンフィギュレーションモードで **errdisable recovery interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable recovery interval timer-interval
no errdisable recovery interval timer-interval

構文の説明

timer-interval errdisable ステートから回復する時間。指定できる範囲は 30 ~ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルトの間隔は 300 秒です。

コマンド デフォルト

デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

errdisable recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

例

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Device(config)# errdisable recovery interval 500
```

lldp (インターフェイス コンフィギュレーション)

インターフェイスの Link Layer Discovery Protocol (LLDP) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **lldp** コマンドを使用します。インターフェイスで LLDP 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。

```
lldp {med-tlv-select tlv | receive | tlv-select {power-management} | transmit}
no lldp {med-tlv-select tlv | receive | tlv-select {power-management} | transmit}
```

構文の説明

med-tlv-select	LLDP Media Endpoint Discovery (LLDP-MED) の Time Length Value (TLV) 要素を送信するように選択します。
<i>tlv</i>	TLV 要素を特定するストリング。有効な値は次のとおりです。 <ul style="list-style-type: none"> • inventory-management : LLDP MED インベントリ管理 TLV。 • location : LLDP MED ロケーション TLV。 • network-policy : LLDP MED ネットワーク ポリシー TLV。
receive	LLDP 伝送を受信するようにインターフェイスをイネーブルにします。
tlv-select	送信する LLDP TLV を選択します。
power-management	LLDP 電源管理 TLV を送信します。
transmit	インターフェイスで LLDP 伝送をイネーブルにします。

コマンド デフォルト

LLDP はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、802.1 メディア タイプでサポートされています。

インターフェイスがトンネルポートに設定されていると、LLDP は自動的にディセーブルになります。

インターフェイスの LLDP 伝送をディセーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
```

```
Device(config-if)# no lldp transmit
```

インターフェイスの LLDP 伝送をイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1  
Device(config-if)# lldp transmit
```

mdix auto

インターフェイスで Automatic Medium-Dependent Interface Crossover (Auto MDIX) 機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **mdix auto** コマンドを使用します。Auto MDIX 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。

mdix auto
no mdix auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Auto MDIX は、イネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブルタイプ（ストレートまたはクロス）が不正でもリンクがアップします。

Auto-MDIX は、すべての 10/100 および 10/100/1000 Mbps インターフェイス上および 10/100/1000BASE-T/TX Small Form-Factor Pluggable (SFP) モジュールインターフェイス上でサポートされます。1000BASE-SX または 1000BASE-LX SFP モジュール インターフェイスではサポートされません。

次の例では、ポートの Auto MDIX を有効にする方法を示します。

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

network-policy

インターフェイスにネットワークポリシー プロファイルを適用するには、インターフェイス コンフィギュレーションモードで **network-policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

network-policy *profile-number*
no network-policy

構文の説明	<i>profile-number</i> インターフェイスに適用するネットワークポリシープロファイル番号
-------	-------------------------------------------------------

コマンド デフォルト	ネットワークポリシー プロファイルは適用されません。
------------	----------------------------

コマンド モード	インターフェイス コンフィギュレーション
----------	----------------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン	インターフェイスにプロファイルを適用するには、 network-policy <i>profile number</i> インターフェイス コンフィギュレーション コマンドを使用します。
------------	------------------------------------------------------------------------------------------------------

最初にネットワークポリシー プロファイルを設定する場合、インターフェイスに **switchport voice vlan** コマンドを適用できません。ただし、**switchport voice vlan** *vlan-id* がすでにインターフェイス上に設定されている場合、ネットワークポリシープロファイルをインターフェイス上に適用できます。その後、インターフェイスは、適用された音声または音声シグナリングVLAN ネットワークポリシー プロファイルを使用します。

次の例では、インターフェイスにネットワークポリシー プロファイル 60 を適用する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy 60
```


network-policyprofile (グローバルコンフィギュレーション)

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーションモードを開始するには、グローバルコンフィギュレーションモードで **network-policy profile** コマンドを使用します。ポリシーを削除して、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

network-policy profile *profile-number*
no network-policy profile *profile-number*

構文の説明	<i>profile-number</i> ネットワークポリシー プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。				
コマンド デフォルト	ネットワークポリシー プロファイルは定義されていません。				
コマンド モード	グローバル コンフィギュレーション				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.2(7)E3k</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーションモードを開始するには、**network-policy profile** 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。

ネットワークポリシー プロファイル コンフィギュレーションモードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーションモードの場合、VLAN、Class of Service (CoS)、Diffserv コードポイント (DSCP) の値、およびタギングモードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の network-policy Time Length Value (TLV) に含まれます。

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Device(config)# network-policy profile 60
Device(config-network-policy)#
```

nmosp attachment suppress

特定のインターフェイスからのアタッチメント情報のレポートを抑制するには、インターフェイス コンフィギュレーション モードで **nmosp attachment suppress** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

nmosp attachment suppress
no nmosp attachment suppress

構文の説明

このコマンドには引数やキーワードはありません。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ロケーションおよびアタッチメント通知を Cisco モビリティサービスエンジン (MSE) に送信しないようにインターフェイスを設定するには、**nmosp attachment suppress** インターフェイス コンフィギュレーション コマンドを使用します。



(注) Cisco IOS XE Denali 16.1.1 以降のリリースでは、アタッチメント情報はサポートされません。

次の例では、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# nmosp attachment suppress
```

power efficient-ethernet auto

インターフェイスの Energy Efficient Ethernet (EEE) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **power efficient-ethernet auto** コマンドを使用します。インターフェイスで EEE 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。

power efficient-ethernet auto
no power efficient-ethernet auto

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンド デフォルト	EEE が有効です。	
コマンド モード	インターフェイス コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 低電力アイドル (LPI) モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応している場合のみ、**power efficient-ethernet auto** コマンドを使用できます。インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities EXEC** コマンドを使用します。

EEE がイネーブルの場合、デバイスはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。インターフェイスの現在の EEE ステータスを表示するには、**show eee status EXEC** コマンドを使用します。

このコマンドにライセンスは必要ありません。

次に、インターフェイスで EEE を有効にする例を示します。

```
Device(config-if)# power efficient-ethernet auto
Device(config-if)#
```

次に、インターフェイスで EEE を無効にする例を示します。

```
Device(config-if)# no power efficient-ethernet auto
Device(config-if)#
```

power inline

Power over Ethernet (PoE) ポートで電源管理モードを設定するには、インターフェイス コンフィギュレーション モードで **power inline** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power inline {auto [max max-wattage] | consumption wattage | never | police [action ]{errdisable | log } | port {2-event | poe-ha} | static [max max-wattage]}
power inline {auto | consumption | never | police | port {2-event | poe-ha} | static }
```

構文の説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。割り当ては、検出された順序で行われます。
max <i>max-wattage</i>	(任意) ポートに供給される電力を制限します。指定できる範囲は 4000 ~ 30000 mW です。値を指定しない場合は、最大電力が供給されます。
consumption <i>wattage</i>	インラインデバイスの電力消費を設定します。
never	装置の検出とポートへの電力供給をディセーブルにします。
police	ポート上の使用電力をポリシングします。
action { errdisable log }	(任意) ポートで電力がオーバードローされたときに実行するアクションを指定します。 <ul style="list-style-type: none"> • errdisable : ポートを error-disable します。 • log : メッセージをログに記録します。

port {2-event poe-ha}	<p>ポートの電力レベルを設定します。</p> <ul style="list-style-type: none"> • 2-event : 2 イベント分類をイネーブルにします。 • poe-ha : ポートに poe-ha を適用します。
static	<p>受電装置の検出をイネーブルにします。スイッチが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます (確保します)。このアクションによって、インターフェイスに接続されたデバイスで十分な電力を受け取ることができます。</p>
max max-wattage	<p>(任意) インターフェイスで許容される最大電力を指定します。</p>

コマンドデフォルト デフォルトは **auto** (イネーブル) です。
 最大ワット数は、30,000 mW です。
 デフォルトのポート プライオリティは低です。

コマンドデフォルト インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```

スイッチスタックでは、このコマンドはPoEをサポートしているスタックの全ポートでサポートされます。

max max-wattage オプションを使用して、受電デバイスの電力が制限を超えないようにします。この設定によって、受電デバイスが最大ワット数より多い電力を要求する Cisco Discovery Protocol (CDP) メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル電力バジェットに送られます。



(注) **power inline max max-wattage** コマンドが 30 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電デバイスへの電力供給を拒否する場合（受電デバイスが CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは **power-deny** ステートになります。スイッチはシステムメッセージを生成し、**show power inline** 特権 EXEC コマンド出力の Oper カラムに **power-deny** が表示されます。

ポートに高いプライオリティを与えるには、**power inline static maxmax-wattage** コマンドを使用します。スイッチは、**auto** モードに設定されたポートに電力を割り当てる前に、**static** モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティックポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティックポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの CDP メッセージによって調節されることはありません。電力が事前割り当てられているので、最大ワット数以下の電力を使用する受電デバイスは、スタティックポートに接続されていれば電力が保証されます。ただし、受電デバイスの IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電デバイスが最大ワット数を超えた量を要求していることをスイッチが認識すると、受電デバイスがシャットダウンします。

ポートが **static** モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、電力バジェット全体がすでに別の自動ポートまたはスタティックポートに割り当てられているなど）、次のメッセージが表示されます。Command rejected: power inline static: pwr not available。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** 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すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電デバイスであるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。不正なリンクアップが生じ、ポートが **errdisable** ステートになる可能性があります。

設定を確認するには、**show power inline EXEC** コマンドを入力します。

例

次の例では、スイッチ上で受電デバイスの検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline auto
```

次に、Class 1 または Class2 の受電デバイスを受け入れるように、スイッチ上で PoE ポートを設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、スイッチ上で PoE ポートへの電力供給を停止する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline never
```

power inline consumption

IEEE 分類によって受電デバイスに指定された電力量を上書きするには、グローバルまたはインターフェイス コンフィギュレーションで **power inline consumption** コマンドを使用して、各デバイスで使用されるワット数を指定します。デフォルトの電力設定に戻すには、このコマンドの **no** 形式を使用します。

power inline consumption [default] wattage
no power inline consumption [default]

構文の説明

default default キーワードが表示されるのは、グローバルコンフィギュレーションのみです。コマンドはキーワードの有無にかかわらず、同じ結果が得られます。

wattage スイッチがポート用に確保する電力を指定します。指定できる範囲は 4000 ~ 15400 mW です。

コマンド デフォルト

Power over Ethernet (PoE) ポートのデフォルトの電力は 15400 mW です。

コマンド モード

グローバル コンフィギュレーション

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

シスコの受電デバイスが PoE ポートに接続されている場合、スイッチは Cisco Discovery Protocol (CDP) を使用して装置が消費する CDP 独自の電力量を決定し、CDP メッセージに基づいて電力バジェットを調整します。これに従って、スイッチは電力バジェットを調整します。この機能は、IEEE サードパーティの受電デバイスには適用されません。この装置の場合、スイッチが電力要求を許可したときに、受電装置の IEEE 分類に応じて電力バジェットを調整します。受電デバイスが Class0 (クラスステータスは不明) または Class 3 である場合、CDP 独自に必要な電力量に関係なく、スイッチはポート用に 15400 mW の電力を確保します。

受電デバイスが CDP 固有の消費よりも高いクラスを報告してきたり、または電力分類 (デフォルトはクラス 0) をサポートしていない場合、スイッチは IEEE クラス情報を使用してグローバル電力バジェットを追跡するため、電力供給できるデバイスが少なくなります。

PoE+ では、受電デバイスは、最大 30 W の電力ネゴシエーションのために Media Dependent Interface (MDI) の Type, Length, and Value description (TLV)、Power-via-MDA TLV で IEEE 802.3at および LLDP 電源を使用します。シスコの先行標準デバイスおよび IEEE 受電デバイスでは、CDP または IEEE 802.3at Power-via-MDI 電力ネゴシエーションメカニズムにより最大 30 W の電力レベルを要求できます。



- (注) クラス 0、クラス 3、およびクラス 4 の受電装置の初期割り当ては 15.4 W です。装置が起動し、CDP または LLDP を使用して 15.4 W を超える要求を送信する場合、最大 30 W を割り当てることができます。

power inline consumption wattage コンフィギュレーション コマンドの使用で、IEEE 分類のデフォルトの電力要件を無視することができます。IEEE 分類で指定された電力と実際に装置が必要とする電力の差は、追加の装置が使用するためグローバル電力バジェットに入れられます。したがって、スイッチの電力バジェットを拡張してもっと効率的に使用できます。

power inline consumption wattage コンフィギュレーション コマンドを入力する前に、**power inline police [action log]** 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リアルタイムの電力消費のポリシングをイネーブルにすることを推奨します。



- 注意 慎重にスイッチの電力バジェットを計画し、電源装置がオーバーサブスクライブ状態にならないようにしてください。

power inline consumption default wattage または **no power inline consumption default** グローバル コンフィギュレーション コマンド、または **power inline consumption wattage** または **no power inline consumption** 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、この注意メッセージが表示されます。

```
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the switch and void your warranty. Take precaution not to
oversubscribe the power supply.
It is recommended to enable power policing if the switch supports it.
Refer to documentation.
```



- (注) 手動で電力バジェットを設定する場合、スイッチと受電デバイス間のケーブルでの電力消失を考慮する必要があります。

IEEE 分類に関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

このコマンドは、PoE 対応ポートだけでサポートされています。PoE をサポートしていないスイッチまたはポートでこのコマンドを入力すると、エラーメッセージが表示されます。

スイッチ スタックでは、このコマンドは PoE をサポートしているスタックの全スイッチまたはポートでサポートされます。

設定を確認するには、**show power inline consumption** 特権 EXEC コマンドを入力します。

例

次の例では、グローバル コンフィギュレーション モードでコマンドを使用して、各 PoE ポートに 5000 mW の電力を確保するようスイッチを設定する方法を示します。

```
Device(config)# power inline consumption default 5000  
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'  
command may cause damage to the switch and void your warranty. Take precaution not to  
oversubscribe the power supply.  
It is recommended to enable power policing if the switch supports it.  
Refer to documentation.
```

次の例では、インターフェイス コンフィギュレーション モードでコマンドを使用して、特定の PoE ポートに接続されている受電デバイスに 12000 mW の電力を確保するようスイッチを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline consumption 12000  
%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation'  
command may cause damage to the switch and void your warranty. Take precaution not to  
oversubscribe the power supply.  
It is recommended to enable power policing if the switch supports it.  
Refer to documentation.
```

power inline police

受電デバイスでリアルタイム電力消費のポリシングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **power inline police** コマンドを使用します。この機能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。

power inline police [action {errdisable|log}]
no power inline police

構文の説明	<p>action errdisable (任意) リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにするよう、デバイスを設定します。これがデフォルトのアクションになります。</p>
	<p>action log (任意) リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、接続されているデバイスへの電力を供給しながら、デバイスが syslog メッセージを生成するように設定します。</p>

コマンド デフォルト 受電デバイスのリアルタイムの電力消費のポリシングは、ディセーブルです。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	<table border="1"> <thead> <tr> <th data-bbox="412 1014 1153 1073">リリース</th> <th data-bbox="1153 1014 1523 1073">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="412 1073 1153 1171">Cisco IOS Release 15.2(7)E3k</td> <td data-bbox="1153 1073 1523 1171">このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				

使用上のガイドライン このコマンドは、Power of Ethernet (PoE) 対応ポートのみでサポートされています。PoE をサポートしていないデバイスまたはポートでこのコマンドを入力すると、エラーメッセージが表示されます。

スイッチスタックでは、このコマンドは、PoE およびリアルタイム電力消費モニタリングをサポートしているスタックの全スイッチまたはポートでサポートされます。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電デバイスが割り当てられた最大電力より多くの量を消費すると、デバイスが対処します。

PoE がイネーブルである場合、デバイスは受電デバイスのリアルタイムの電力消費を検知しません。この機能は、パワー モニタリングまたはパワー センシングといわれます。また、デバイスはパワーポリシング機能を使用して消費電力をポリシングします。

パワーポリシングがイネーブルである場合、デバイスは次の順のいずれかの方式で PoE ポートのカットオフ電力として、これらの値の 1 つを使用します。

1. **power inline auto max max-wattage** インターフェイス コンフィギュレーション コマンドまたは **power inline static max max-wattage** インターフェイス コンフィギュレーション コマンドを入力したときにポート上で許可される電力を制限するユーザ定義の電力レベル。

2. デバイスでは、CDP パワーネゴシエーションまたは IEEE 分類および LLDP 電力ネゴシエーションを使用して、装置の消費使用量が自動的に設定されます。

カットオフ電力量の値を手動で設定しない場合、デバイスは、CDP 電力ネゴシエーションまたはデバイスの IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に値を決定します。CDP または LLDP がイネーブルでない場合は、デフォルト値の 30 W が適用されます。ただし、CDP または LLDP がない場合は、15400 ~ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、デバイスで 15.4 W を超える電力の消費がデバイスから許可されません。受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する場合、装置は最大電流 I_{max} の制限に違反し、最大値を超える電流が供給されるという *Icut* 障害が発生する可能性があります。再び電源を入れるまで、ポートは障害状態のままになります。ポートが継続的に 15.4W を超えて給電されると、サイクルが繰り返されません。

PoE+ ポートに接続されている受電デバイスが再起動し、電力 TLV で CDP パケットまたは LLDP パケットが送信される場合、デバイスは最初のパケットの電力ネゴシエーションプロトコルをロックし、その他のプロトコルからの電力要求に応答しません。たとえば、デバイスが CDP にロックされている場合、LLDP 要求を送信するデバイスに電力を供給しません。デバイスが CDP にロックされた後で CDP がディセーブルになった場合、デバイスは LLDP 電源要求に応答せず、アクセサリの電源がオンにならなくなります。この場合、受電デバイスを再起動する必要があります。

パワーポリシングがイネーブルである場合、デバイスはリアルタイムの電力消費を PoE ポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（またはカットオフ電力）を超える電力をポートで使用している場合、スイッチでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながら syslog メッセージが生成されて LED（ポート LED はオレンジ色に点滅）が更新されます。

- ポートへの電力供給をオフにして、ポートを **error-disabled** ステートとするようデバイスを設定するには、**power inline police** インターフェイス コンフィギュレーション コマンドを使用します。
- 装置に電力を供給しながら、syslog メッセージを生成するようデバイスを設定するには、**power inline police action log** コマンドを使用します。

action log キーワードを入力しない場合のデフォルトのアクションは、ポートのシャットダウン、ポートへの電力供給のオフ、およびポートを PoE **error-disabled** ステートに移行になります。PoE ポートを **error-disabled** ステートから自動的に回復するよう設定するには、**errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用して、PoE 原因に対する **error-disabled** 検出をイネーブルにして、**errdisable recovery cause inline-power interval** 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、PoE **error-disabled** 原因の回復タイマーをイネーブルにします。



注意 ポリシングがディセーブルである場合、受電デバイスがポートに割り当てられた最大電力より多くの量を消費しても対処されないため、デバイスに悪影響を与える場合があります。

設定を確認するには、**show power inline police** 特権 EXEC コマンドを入力します。

例

次の例では、電力消費のポリシングをイネーブルにして、デバイスの PoE ポートで **syslog** メッセージを生成するようデバイスを設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# power inline police action log
```

power inline ps watt

電源を 65W に設定するには、グローバル コンフィギュレーション モードで **power inline ps watt** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
power inline ps watt 65
no power inline ps watt 65
```

構文の説明

65 電源を 65W に設定します。

コマンド デフォルト

デフォルトの電源は 80W に設定されています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco Catalyst マイクロスイッチ シリーズの CMICR-4PC および CMICR-4PS モデルでのみサポートされます。

例

次に、電源を 65W に設定する例を示します。

```
Device# enable
Device> configure terminal
Device(config)# power inline ps watt 65
Device(config)# end
```

show eee

インターフェイスの Energy Efficient Ethernet (EEE) 情報を表示するには、EXEC モードで **show eee** コマンドを使用します。

show eee{capabilities | status}**interface** *interface-id*

構文の説明	capabilities	指定インターフェイスの EEE 機能を表示します。
	status	指定したインターフェイスの EEE ステータス情報を表示します。
	interface <i>interface-id</i>	EEE 機能またはステータス情報を表示するためのインターフェイスを指定します。
コマンドデフォルト	なし	
コマンドモード	ユーザ EXEC 特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

低電力アイドル (LPI) モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い電力使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities** コマンドを使用します。**power efficient-ethernet auto** 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、EEE に対応しているインターフェイスで EEE をイネーブルにできます。

インターフェイスの EEE ステータス、LPI ステータス、および wake エラーカウント情報を表示するには、**show eee status** コマンドを使用します。

次の例では、EEE がイネーブルのインターフェイスの **show eee capabilities** コマンドの出力を示します。

```
Device# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
    EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
```

```
Link Partner          : yes (100-Tx and 1000T auto)
```

次の例では、EEE がイネーブルでないインターフェイスの **show eee capabilities** コマンドの出力を示します。

```
Device# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
EEE(efficient-ethernet): not enabled
Link Partner          : not enabled
```

次の例では、EEE がイネーブルで機能しているインターフェイスの **show eee status** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
EEE(efficient-ethernet): Operational
Rx LPI Status          : Received
Tx LPI Status          : Received
```

次の例では、EEE が機能していて、ポートが節電モードであるインターフェイスの **show eee status** コマンドの出力を示します。

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
EEE(efficient-ethernet): Operational
Rx LPI Status          : Low Power
Tx LPI Status          : Low Power
Wake Error Count       : 0
```

次の例では、リモートリンクパートナーが EEE と互換性がないために、EEE がイネーブルでないインターフェイスの **show eee status** コマンドの出力を示します。

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
EEE(efficient-ethernet): Disagreed
Rx LPI Status          : None
Tx LPI Status          : None
Wake Error Count       : 0
```


表 6 : show eee status のフィールドの説明

フィールド	説明
EEE (efficient-ethernet)	<p>インターフェイスの EEE ステータス。このフィールドには、次のいずれかの値を使用できます。</p> <ul style="list-style-type: none"> • N/A : ポートは EEE に対応できません。 • Disabled : ポートの EEE はディセーブルです。 • Disagreed : リモートリンク パートナーが EEE に互換性がない可能性があるため、ポートの EEE は設定されていません。EEE 対応でないか、EEE の設定に互換性はありません。 • Operational : ポートの EEE がイネーブルで機能しています。 <p>インターフェイスの速度が 10Mbps として設定されていると、EEE は内部的にディセーブルになります。インターフェイスの速度が auto、100 Mbps または 1000 Mbps に戻ると、EEE は再びアクティブになります。</p>

フィールド	説明
Rx/Tx LPI Status	<p>リンク パートナーの低電力アイドル (LPI) ステータス。このフィールドには、次のいずれかの値を使用できます。</p> <ul style="list-style-type: none"> • N/A : ポートは EEE に対応できません。 • Interrupted : リンク パートナーは低電力モードへの移行中です。 • Low Power : リンク パートナーは低電力モードにあります。 • None : EEE がディセーブルであるか、リンク パートナー側で対応できません。 • Received : リンク パートナーは低電力モードにあり、トラフィック アクティビティがあります。 <p>インターフェイスが半二重として設定されており、LPI ステータスが「None」の場合、インターフェイスが全二重として設定されるまで、インターフェイスは低電力モードにすることはできないことを意味します。</p>
Wake Error Count	<p>発生した PHY wake-up エラーの数 EEE がイネーブルで、リンク パートナーへの接続が切断された場合に、wake-up エラーが発生します。</p> <p>この情報は、PHY のデバッグに役立ちます。</p>

show env

ファン、温度、および電源の情報を表示するには、EXEC モードで **show env** コマンドを使用します。

show env {**all** | **fan** | **power** [**allswitch** [*stack-member-number*]] | **stack** [*stack-member-number*] | **temperature** [*status*]}

構文の説明		
	all	ファンおよび温度の環境ステータスおよび内部電源装置のステータスを表示します。
	fan	スイッチのファンの状態を表示します。
	power	アクティブスイッチの内部電源の状態を表示します。
	all	(任意) スイッチでコマンドが入力された場合、スタンドアロンスイッチのすべての内部電源の状態が表示されます。アクティブスイッチでコマンドが入力された場合は、すべてのメンバスイッチのすべての内部電源の状態が表示されます。
	switch	(任意) スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
	<i>stack-member-number</i>	(任意) 内部電源または環境ステータスの状態を表示するメンバスイッチの数。 指定できる範囲は 1 ~ 8 です。
	stack	スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
	temperature	スイッチの温度ステータスを表示します。
	status	(任意) スイッチの内部温度 (外部温度ではなく) およびしきい値を表示します。
コマンドデフォルト	なし	
コマンドモード	ユーザ EXEC 特権 EXEC	

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

アクセスされているスイッチ（スタンドアロンスイッチまたはアクティブスイッチ）の情報を表示するには、**show env EXEC** コマンドを使用します。**stack** および **switch** キーワードとともにこのコマンドを使用すると、スタックまたは指定されたメンバスイッチのすべての情報が表示されます。

show env temperature status コマンドを入力すると、コマンド出力にスイッチの温度状態としきい値レベルが表示されます。

show env temperature コマンドを使用して、スイッチの温度状態を表示することもできます。コマンド出力では、GREEN および YELLOW ステートを *OK* と表示し、RED ステートを *FAULTY* と表示します。**show env all** コマンドを入力した場合のコマンド出力は、**show env temperature status** コマンド出力と同じです。

例

次に、**show env all** コマンドの出力例を示します。

```
Device# show env all

SWITCH: 1
SYSTEM FAN SPEED is OK
SYSTEM TEMPERATURE is OK
System Temperature Value: 52 Degree Celsius
PHY Temperature Value: 36 Degree Celsius
DDR Temperature Value: 46 Degree Celsius
System Temperature State: GREEN
Yellow Threshold : 74 Degree Celsius
Red Threshold    : 77 Degree Celsius

SWITCH: 1
PID: Built-in
System Power:(Watts) 36
Max Power Usage:(Watts) 14
Maximum Heat Dissipation: (Watts) 14
PoE Power extract:(Watts) 0.0
Power Supply Status: Good
```

次に、**show env fan** コマンドの出力例を示します。

```
Device# show env fan
SYSTEM FAN SPEED is OK
```

次に、**show env power** コマンドの出力例を示します。

```
Device>show env power
PID: Built-in
System Power:(Watts) 36
Max Power Usage:(Watts) 14
Maximum Heat Dissipation: (Watts) 14
PoE Power extract:(Watts) 0.0
```

Power Supply Status: Good

アクティブスイッチでの **show env power all** コマンドの出力例を示します。

```
Device# show env power allSWITCH: 1
PID: Built-in
System Power:(Watts) 36
Max Power Usage:(Watts) 14
Maximum Heat Dissipation: (Watts) 14
PoE Power extract:(Watts) 0.0
Power Supply Status: Good
```

アクティブスイッチでの **show env stack** コマンドの出力例を示します。

```
Device# show env stack
SWITCH: 1
SYSTEM FAN SPEED is OK
SYSTEM TEMPERATURE is OK
System Temperature Value: 52 Degree Celsius
PHY Temperature Value: 36 Degree Celsius
DDR Temperature Value: 46 Degree Celsius
System Temperature State: GREEN
Yellow Threshold : 74 Degree Celsius
Red Threshold    : 77 Degree Celsius
```

表 7: *show env temperature status* コマンド出力のステート

状態	説明
グリーン	スイッチの温度が正常な動作範囲にあります。
イエロー	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。
レッド	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show errdisable detect

errdisable 検出ステータスを表示するには、EXEC モードで **show errdisable detect** コマンドを使用します。

show errdisable detect

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid エラーの理由は、無効な Small Form-Factor Pluggable (SFP) モジュールを意味します。

コマンド出力内の **errdisable** の理由がアルファベット順に表示されます。Mode 列は、**errdisable** が機能ごとにどのように設定されているかを示します。

errdisable 検出は次のモードで設定できます。

- ポート モード：違反が発生した場合、物理ポート全体が **errdisable** になります。
- VLAN モード：違反が発生した場合、VLAN が **errdisable** になります。
- ポート/VLAN モード：一部のポートでは物理ポート全体が **errdisable** になり、その他のポートでは VLAN ごとに **errdisable** になります。

次に、**show errdisable detect** コマンドの出力例を示します。

```
Device> show errdisable detect
ErrDisable Reason          Detection          Mode
-----
arp-inspection             Enabled           port
bpduguard                  Enabled           port
channel-misconfig (STP)   Enabled           port
community-limit           Enabled           port
dhcp-rate-limit           Enabled           port
dtp-flap                   Enabled           port
gbic-invalid               Enabled           port
iif-reg-failure           Enabled           port
inline-power               Enabled           port
invalid-policy             Enabled           port
link-flap                  Enabled           port
```

```

loopback                Enabled      port
lsgroup                 Enabled      port
mac-limit               Enabled      port
pagp-flap               Enabled      port
port-mode-failure      Enabled      port
pppoe-ia-rate-limit    Enabled      port
psecure-violation      Enabled      port/vlan
security-violation     Enabled      port
sfp-config-mismatch    Enabled      port
sgacl_limitation        Enabled      port
small-frame             Enabled      port
storm-control           Enabled      port
udld                    Enabled      port
vmmps                   Enabled      port
psp                      Enabled      port

```

show errdisable recovery

errdisable 回復タイマー情報を表示するには、EXEC モードで **show errdisable recovery** コマンドを使用します。

show errdisable recovery

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

gbic-invalid error-disable の理由は、無効な Small Form-Factor Pluggable (SFP) インターフェイスを意味します。



(注) unicast-flood フィールドは、出力に表示はされますが無効です。

次に、**show errdisable recovery** コマンドの出力例を示します。

```
Device> show errdisable recovery
ErrDisable Reason          Timer Status
-----
arp-inspection             Disabled
bpduguard                  Disabled
channel-misconfig (STP)   Disabled
dhcp-rate-limit           Disabled
dtp-flap                   Disabled
gbic-invalid               Disabled
inline-power               Disabled
link-flap                  Disabled
mac-limit                  Disabled
loopback                   Disabled
pagg-flap                  Disabled
port-mode-failure         Disabled
ppoe-ia-rate-limit        Disabled
psecure-violation         Disabled
security-violation         Disabled
sfp-config-mismatch       Disabled
small-frame                Disabled
storm-control              Disabled
udld                       Disabled
```



```
vmps                Disabled
psp                 Disabled
```

```
Timer interval: 300 seconds
```

```
Interfaces that will be enabled at the next timeout:
```

show hardware led

デバイスの LED の色を表示するには、特権 EXEC モードで **show hardware led** コマンドを使用します。

show hardware led port [*{interface-number}*]{**duplex** | **power** | **speed** | **stack** | **status**}

構文の説明

port	ポート LED の色を表示します。
<i>interface-number</i>	インターフェイス番号を指定します。
duplex	ポートのデュプレックスモードのポート LED を表示します。
power	PoE ステータスのポート LED を表示します。
speed	ポートの動作速度のポート LED を表示します。
stack	スタックリンクステータスのポート LED を表示します。
status	ポートステータスのポート LED を表示します。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

特権 EXEC モードで **show hardware led** コマンドを実行すると、出力にデバイスの LED 情報が表示されます。次の表では、出力の LED コードについて説明します。

コード	説明
B	黒色
A	オレンジ
G	グリーン
GA	グリーンおよびオレンジ
F	点滅
AL	交互に点滅

コード	説明
BL	点滅
BL2	点滅_2

表 8: 各種モードでの LED カラーの意味

オプション	色	説明
状態	消灯	リンクが確立されていないか、ポートが管理上の理由でシャットダウンされました。
	グリーン	リンクが確立されています。
	グリーンに点滅	アクティブな状態です。ポートがデータを送信または受信しています。
	グリーンとオレンジに交互に点滅	リンク障害が発生しています。エラーフレームが接続に影響を与える可能性があり、リンク障害について、大量のコリジョン、CRCエラー、アライメントエラーなどのエラーがモニタされています。
	オレンジ	ポートがスパンニングツリープロトコル (STP) によってブロックされており、データを転送していません。ポートを再設定した後は、STPによってループが検索されるので、最大 30 秒間 LED がオレンジに点灯します。
	オレンジに点滅	ポートが STP によってブロックされており、データを送信していません。
速度	消灯	ポートは 10 Mb/s で動作しています。
	グリーン	ポートは 100 Mb/s で動作しています。
	緑色に点滅	ポートは 1000 Mb/s で動作しています。

オプション	色	説明
電源	消灯	PoE がオフになっています。受電デバイスの電力が AC 電源から供給されている場合は、受電デバイスがスイッチポートに接続されていても、PoE ポート LED はオフになります。
	グリーン	PoE がオンになっています。LED がグリーンに点灯するのは、スイッチポートが電力を供給している場合だけです。
	グリーンとオレンジに交互に点滅	受電デバイスへの供給電力がスイッチの電力容量を超えるため、PoE が無効になっています。
	オレンジ	ポートの PoE がディセーブルになっていますデフォルトでは、PoE は有効になっています。
	オレンジに点滅	障害により PoE がオフになっています。



(注) 物理的には、デバイスにオレンジ色の LED はありません。 **show hardware led** コマンドの出力に示されているオレンジ色の LED は、ソフトウェアでのみ表示されます。

コンボポートアップリンクの場合、LED コードは「ファイバポート LED - 銅線ポート LED」と表記されます。たとえば、コンボポートのアップリンク LED が B-G と表記されている場合、これはファイバポートの LED が黒で、銅線ポートの LED がグリーンであることを意味します。

次に、**show hardware led port duplex** コマンドの出力例を示します。

```
Device# show hardware led port duplex
SWITCH: 1
-----
SYSTEM: GREEN

LED Codes: B-Black, A-Amber, G-Green, GA-Green Amber, F-Flashing, AL-Alternating,
BL-blinking, BL2-Blinking_2

For Combo port uplinks please read LED Codes as (Fiber-Copper)
PORT : 1      2      3      4      5      6      7      8
-----
DUPLEX: G      G      G      G      G      G      G      G

UPLINK 1G :   9      10

-----
DUPLEX   :   B-G   B-G
```

次に、**show hardware led port stack** コマンドの出力例を示します。

```
Device# show hardware led port stack
SWITCH: 1
-----
SYSTEM: GREEN
```

LED Codes: B-Black, A-Amber, G-Green, GA-Green Amber, F-Flashing, AL-Alternating,
BL-blinking, BL2-Blinking_2

For Combo port uplinks please read LED Codes as (Fiber-Copper)

PORT : 1 2 3 4 5 6 7 8

STACK : B B B B B B B B

UPLINK 1G : 9 10

STACK : B-G B-G

show interfaces

すべてのインターフェイスまたは指定したインターフェイスの管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces** コマンドを使用します。

show interfaces [{*interface-id* | **vlan** *vlan-id*}] [{**accounting** | **capabilities** [**module** *number*] | **debounce** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [{**err-disabled**}] | **trunk**}]

構文の説明

<i>interface-id</i>	(任意) インターフェイスの ID です。有効なインターフェイスには、物理ポート (タイプ、スタック構成可能なスイッチのスタックメンバ、モジュール、およびポート番号を含む) やポートチャンネルが含まれます。指定できるポートチャンネルは 1 ~ 48 です。
vlan <i>vlan-id</i>	(任意) VLAN ID です。指定できる範囲は 1 ~ 4094 です。
accounting	(任意) インターフェイスのアカウント情報 (アクティブプロトコル、入出力のパケット、オクテットを含む) を表示します。 (注) ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。
capabilities	(任意) すべてのインターフェイスまたは指定されたインターフェイスの性能 (機能、インターフェイス上で設定可能なオプションを含む) を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLAN ID に使用できません。
module <i>number</i>	(任意) スイッチまたは指定されたスタックメンバのすべてのインターフェイスの機能を表示します。 指定できる範囲は 1 ~ 8 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
debounce	(任意) インターフェイスのポートデバウンスタイマー情報を表示します。
description	(任意) 特定のインターフェイスに設定された管理ステータスおよび説明を表示します。
etherchannel	(任意) インターフェイス EtherChannel 情報を表示します。

flowcontrol	(任意) インターフェイスのフロー制御情報を表示します。
pruning	(任意) インターフェイスのトランク VTP プルーニング情報を表示します。
stats	(任意) インターフェイスのパスを切り替えることによる入出力パケットを表示します。
status	(任意) インターフェイスのステータスを表示します。Type フィールドの unsupported のステータスは、他社製の Small Form-Factor Pluggable (SFP) モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	(任意) errdisable ステートのインターフェイスを表示します。
trunk	(任意) インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブなトランッキング ポートの情報だけが表示されます。



(注) **crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、および **rate-limit** キーワードはコマンドラインのヘルプストリングに表示されますが、サポートされていません。

コマンドデフォルト	なし	
コマンドモード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **show interfaces capabilities** コマンドに異なるキーワードを指定することで、次のような結果になります。

- **show interface capabilities module number** コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスの機能を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。
- 指定されたインターフェイスの機能を表示するには、**show interfaces interface-id capabilities** を使用します。

- スタック内のすべてのインターフェイスの機能を表示するには、**show interfaces capabilities** を使用します（モジュール番号またはインターフェイス ID の指定なし）。

次の例では、スタック メンバ 3 のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

次に、**show interfaces accounting** コマンドの出力例を示します。

```
Device# show interfaces accounting
Vlan1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
      IP        382021   29073978   41157      20408734
      ARP        981      58860      179        10740
FastEthernet0
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
      Other      4         276        0           0
      Spanning Tree  41       2132      0           0
      CDP        5         2270      10          4318
GigabitEthernet1/0/1
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/3
      Protocol  Pkts In   Chars In   Pkts Out   Chars Out
      Other      0         0          226505     14949330
      Spanning Tree  679120   40747200   0           0
      CDP        22623    10248219   22656      10670858
      DTP        45226    2713560    0           0
```



```
GigabitEthernet1/0/4
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/5
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/6
      Protocol    Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>
```

```
Device# show interfaces gigabitethernet1/0/1 capabilities
GigabitEthernet1/0/1
  Model:                C1000-48P-4G-L
  Type:                 10/100/1000BaseTX
  Speed:                10,100,1000,auto
  Duplex:               half,full,auto
  Trunk encap. type:    802.1Q
  Trunk mode:           on,off,desirable,nonegotiate
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(off,on,desired),tx-(none)
  Fast Start:           yes
  QoS scheduling:       rx-(not configurable on per port basis),
                       tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:          yes
  ToS rewrite:          yes
  UDLD:                 yes
  Inline power:         no
  SPAN:                 source/destination
  PortSecure:           yes
  Dot1x:                yes
```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを *Connects to Marketing* として指定した場合の **show interfaces interface description** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/2 description
Interface              Status          Protocol Description
Gi1/0/2                up              down         Connects to Marketing
```

次の例では、VTP ドメイン内でプルーンングがイネーブルの場合の **show interfaces interface-id pruning** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Device# show interfaces vlan 1 stats
Switching path   Pkts In   Chars In   Pkts Out   Chars Out
  Processor      1165354   136205310   570800     91731594
  Route cache      0         0           0          0
```

```
Total      1165354    136205310    570800    91731594
```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

```
Device# show interfaces status
Port      Name          Status      Vlan      Duplex  Speed  Type
Gi1/0/1   Gi1/0/1       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/2   Gi1/0/2       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/3   Gi1/0/3       connected  1         a-full  a-1000 10/100/1000BaseTX
Gi1/0/4   Gi1/0/4       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/5   Gi1/0/5       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/6   Gi1/0/6       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/7   Gi1/0/7       notconnect  1         auto    auto   10/100/1000BaseTX
Gi1/0/8   Gi1/0/8       notconnect  1         auto    auto   10/100/1000BaseTX
```

<output truncated>

次に、**show interfaces status err-disabled** コマンドの出力例を示します。errdisable ステータスのインターフェイスのステータスを表示します。

```
Device# show interfaces status err-disabled
Port      Name          Status      Reason
Gi1/0/2   Gi1/0/2       err-disabled gbic-invalid
Gi2/0/3   Gi2/0/3       err-disabled dtp-flap
```

次の例では、**show interfaces interface-id pruning** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

show interfaces counters

スイッチまたは特定のインターフェイスのさまざまなカウンタを表示するには、特権 EXEC モードで **show interfaces counters** コマンドを使用します。

show interfaces [*interface-id*] **counters** [{**errors** | **etherchannel** | **module** *stack-member-number* | **protocol status** | **trunk**}]

構文の説明	
<i>interface-id</i>	(任意) 物理インターフェイスの ID (タイプ、スタックメンバ (スタック構成可能なスイッチのみ)、モジュール、ポート番号を含む)。
errors	(任意) エラーカウンタを表示します。
etherchannel	(任意) 送受信されたオクテット、ブロードキャストパケット、マルチキャストパケット、およびユニキャストパケットなど、EtherChannel カウンタを表示します。
module <i>stack-member-number</i>	(任意) 指定されたスタックメンバのカウンタを表示します。 指定できる範囲は 1 ~ 8 です。 (注) このコマンドでは、 module キーワードはスタックメンバ番号を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。
protocol status	(任意) インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	(任意) トランクカウンタを表示します。



(注) **vlan** *vlan-id* キーワードは、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。

コマンド デフォルト	なし	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン キーワードを入力しない場合は、すべてのインターフェイスのすべてのカウンタが表示されます。

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters
Port          InOctets      InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              0              0              0              0
Gi1/0/2              0              0              0              0
Gi1/0/3          95285341      43115          1178430        1950
Gi1/0/4              0              0              0              0

<output truncated>
```

次の例では、スタックメンバ2に対する **show interfaces counters module 2** コマンドの出力の一部を示します。スタック内で指定されたスイッチのすべてのカウンタが表示されます。

```
Device# show interfaces counters module 2
Port          InOctets      InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              520            2              0              0
Gi1/0/2              520            2              0              0
Gi1/0/3              520            2              0              0
Gi1/0/4              520            2              0              0

<output truncated>
```

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

次に、**show interfaces counters trunk** コマンドの出力例を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```

Device# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1      0               0               0
Gi1/0/2      0               0               0
Gi1/0/3      80678           0               0
Gi1/0/4      82320           0               0
Gi1/0/5      0               0               0
    
```

<output truncated>

show interfaces switchport

ポートブロッキング、ポート保護設定など、スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces switchport** コマンドを使用します。

show interfaces [{ *interface-id* }] **switchport** [{ *module number* }]

構文の説明

interface-id (任意) インターフェイスの ID です。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタックメンバ、モジュール、およびポート番号を含む）やポートチャネルが含まれます。指定できるポートチャネルは 1～48 です。

module number (任意) スイッチまたは指定されたスタックメンバのすべてのインターフェイスのスイッチポート設定を表示します。

有効な範囲は 1～8 です。

このオプションは、特定のインターフェイス ID を入力したときは利用できません。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スタックのスイッチ上のすべてのインターフェイスのスイッチポート特性を表示するには、**show interface switchport module number** コマンドを使用します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。

次の例では、ポートの **show interfaces switchport** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。



(注) プライベート VLAN はこのリリースではサポートされないため、フィールドは適用されません。

```
Device# show interfaces gigabitethernet1/0/1 switchport
```

```
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
```

```

Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: disabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
    
```

表 9 : show interfaces switchport のフィールドの説明

フィールド	説明
Name	ポート名を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この出力の場合、ポートはスイッチポートモードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキング ネゴシエーションがイネーブるかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。

フィールド	説明
Protected	インターフェイス上で保護ポートがイネーブル (True) であるかまたはディセーブル (False) であるかを表示します。
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャストトラフィックがインターフェイス上でブロックされているかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Appliance trust	IP Phone のデータパケットのサービスクラス (CoS) 設定を表示します。

show interfaces transceiver

Small Form-Factor Pluggable (SFP) モジュールインターフェイスの物理インターフェイスを表示するには、EXEC モードで **show interfaces transceiver** コマンドを使用します。

show interfaces [*interface-id*] **transceiver** [{**detail** | **module number** | **properties** | **supported-list** | **threshold-table**}]

構文の説明	<p>interface-id (任意) 物理インターフェイスの ID (タイプ、スタックメンバ (スタック構成可能なスイッチのみ)、モジュール、ポート番号を含む)。</p> <p>detail (任意) (スイッチにインストールされている場合) Digital Optical Monitoring (DoM) 対応トランシーバの高低値やアラーム情報などの、調整プロパティを表示します。</p> <p>module number (任意) スイッチのモジュールのインターフェイスへの表示を制限します。指定できる範囲は 1 ~ 8 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。</p> <p>properties (任意) インターフェイスの速度、デュプレックス、およびインラインパワー設定を表示します。</p> <p>supported-list (任意) サポートされるトランシーバをすべて表示します。</p> <p>threshold-table (任意) アラームおよび警告しきい値テーブルを表示します。</p>
-------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

コマンドモード	<p>ユーザ EXEC</p> <p>特権 EXEC</p>
---------	--------------------------------

コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.2(7)E3k</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				

例 次の例では、**show interfaces interface-id transceiver properties** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/0/50 transceiver properties
Diagnostic Monitoring is not implemented.
Name : Gi1/0/50
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
```

show interfaces transceiver

```
Operational Speed: 1000
Operational Duplex: full
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX
```

次の例では、**show interfaces interface-id transceiver detail** コマンドの出力を示します。

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1/1	29.9	74.0	70.0	0.0	-4.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1/1	3.28	3.60	3.50	3.10	3.00

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	1.8	7.9	3.9	0.0	-4.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

次に、**show interfaces transceiver threshold-table** コマンドの出力例を示します。

```
Device# show interfaces transceiver threshold-table
```

	Optical Tx	Optical Rx	Temp	Laser Bias current	Voltage
DWDM GBIC					
Min1	-4.00	-32.00	-4	N/A	4.65
Min2	0.00	-28.00	0	N/A	4.75
Max2	4.00	-9.00	70	N/A	5.25
Max1	7.00	-5.00	74	N/A	5.40
DWDM SFP					
Min1	-4.00	-32.00	-4	N/A	3.00
Min2	0.00	-28.00	0	N/A	3.10
Max2	4.00	-9.00	70	N/A	3.50
Max1	8.00	-5.00	74	N/A	3.60
RX only WDM GBIC					
Min1	N/A	-32.00	-4	N/A	4.65
Min2	N/A	-28.30	0	N/A	4.75
Max2	N/A	-9.00	70	N/A	5.25
Max1	N/A	-5.00	74	N/A	5.40
DWDM XENPAK					

```

Min1          -5.00      -28.00      -4          N/A          N/A
Min2          -1.00      -24.00      0           N/A          N/A
Max2          3.00       -7.00      70          N/A          N/A
Max1          7.00       -3.00      74          N/A          N/A
  DWDM X2
Min1          -5.00      -28.00      -4          N/A          N/A
Min2          -1.00      -24.00      0           N/A          N/A
Max2          3.00       -7.00      70          N/A          N/A
Max1          7.00       -3.00      74          N/A          N/A
  DWDM XFP
Min1          -5.00      -28.00      -4          N/A          N/A
Min2          -1.00      -24.00      0           N/A          N/A
Max2          3.00       -7.00      70          N/A          N/A
Max1          7.00       -3.00      74          N/A          N/A
  CWDM X2
Min1          N/A        N/A         0           N/A          N/A
Min2          N/A        N/A         0           N/A          N/A
Max2          N/A        N/A         0           N/A          N/A
Max1          N/A        N/A         0           N/A          N/A

```

<output truncated>

show ip ports all

デバイスで開いているすべてのポートを表示するには、EXEC モードまたはユーザ EXEC モードで **show ip ports all** コマンドを使用します。

show ip ports all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC、特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show ip ports all** コマンドの出力例を示します。

```
Device# show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *: * LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:443 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:80 *: * LISTEN 286/[IOS]HTTP CORE
tcp *:80 *: * LISTEN 286/[IOS]HTTP CORE
udp *:10002 *: * 0/[IOS] Unknown
udp *:2228 0.0.0.0:0 318/[IOS]L2TRACE SERVER
```

Device#

次の表に、フィールドの説明を示します。

フィールド	説明
Protocol	使用されている転送プロトコル。
Foreign Address	リモートまたはピアアドレス。
State	接続の状態：リッスン/確立/接続
PID/Program Name	プロセス ID/プロセス名
Local Address	デバイスの IP アドレス

関連コマンド

show tcp brief all

show ip sockets

show network-policy profile

ネットワークポリシープロファイルを表示するには、特権 EXEC モードで **show network policy profile** コマンドを使用します。

show network-policy profile [*profile-number*]

構文の説明	<i>profile-number</i> (任意) ネットワークポリシープロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシー プロファイルが表示されます。	
コマンド デフォルト	なし	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show network-policy profile** コマンドの出力例を示します。

```
Device# show network-policy profile
Network Policy Profile 60
  Interface:
    none
```

show power

デバイスの電源装置の定格を表示するには、特権 EXEC モードで **show power** コマンドを使用します。

show power

コマンドモード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show power** コマンドの出力例を示します。

```
Device> show power
W: Watts.
=====
System Power : 15000 mW
PoE Power : 65000 mW
```

show power inline

指定された Powerover Ethernet (PoE) ポート、指定されたスタックメンバ、またはスイッチスタックのすべての PoE ポートの PoE ステータスを表示するには、EXEC モードで **show power inline** コマンドを使用します。

show power inline [**consumptionpolice**] [*interface-id*][**module** *stack-member-number*] [**detail**]

構文の説明

consumption	(任意) インライン電力消費を表示します。
police	(任意) リアルタイムの電力消費に関するパワー ポリシング情報を表示します。
<i>interface-id</i>	(任意) 物理インターフェイスの ID です。
module <i>stack-member-number</i>	(任意) 指定されたスタック メンバのポートだけを表示します。 指定できる範囲は 1 ~ 8 です。 このキーワードは、スタック対応スイッチでのみサポートされています。
detail	(任意) インターフェイスまたはモジュールの詳細な出力を表示します。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show power inline** コマンドの出力例を示します。次の表に、出力フィールドについて説明します。

```
Device> show power inline
Available:65.0(w) Used:21.7(w) Remaining:43.3(w)

Interface Admin Oper      Power  Device           Class Max
-----
Gi1/0/1  auto  on       15.4   Ieee PD          4    30.0
Gi1/0/2  auto  off      0.0   n/a              n/a  30.0
Gi1/0/3  auto  off      0.0   n/a              n/a  30.0
Gi1/0/4  auto  on       6.3   IP Phone 7962   2    30.0
```

次の例では、スイッチポートに対する **show power inline interface-id** コマンドの出力を示します。

```
Device# show power inline police gigabitethernet 1/0/1
Interface Admin Oper      Admin      Oper      Cutoff Oper
           State State      Police     Police     Power  Power
-----
Gi1/0/1   auto  off       none       n/a       n/a    n/a
```

次の例では、スタッキング対応スイッチに対する **show power inline police** コマンドの出力を示します。

```
Device> show power inline police
Available:65.0(w) Used:21.7(w) Remaining:43.3(w)

Interface Admin Oper      Admin      Oper      Cutoff Oper
           State State      Police     Police     Power  Power
-----
Gi1/0/1   auto  on        errdisable ok        15.4   6.3
Gi1/0/2   auto  off       none       n/a       n/a    n/a
Gi1/0/3   auto  off       none       n/a       n/a    n/a
Gi1/0/4   auto  on        none       n/a       n/a    4.5
-----
Totals:                                     10.8
```

上の例では、次のようになっています。

- Gi1/0/1 ポートは起動していて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシングアクションとしてポートをシャットダウンするよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシングアクションは作動しません。
- Gi1/0/2 および Gi1/0/3 ポートは起動していて、ポリシングはディセーブルですが、コネクテッドデバイスに対してスイッチから電力が供給されていません。
- Gi1/0/4 ポートは起動していて、ポリシングはディセーブルですが、コネクテッドデバイスに対してスイッチから電力が供給されていません。

次の例では、スタンドアロンスイッチに対する **show power inline police interface-id** コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Device# show power inline police gigabitethernet 1/0/1
Interface Admin Oper      Admin      Oper      Cutoff Oper
           State State      Police     Police     Power  Power
-----
Gi1/0/1   auto  off       none       n/a       n/a    n/a
```

表 10: show power inline police のフィールドの説明

フィールド	説明
Available	スイッチ上の設定電力 ¹ の合計で、ワット数 (W) です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。

フィールド	説明
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）
Admin State	管理モード： auto、 off、 static
Oper State	<p>動作モード：</p> <ul style="list-style-type: none"> • errdisable： ポリシングはイネーブルです。 • faulty： 受電デバイスでのデバイス検出が障害の状態です。 • off： PoE が適用されていません。 • on： 受電デバイスが検出され、電力が適用されています。 • power-deny： 受電デバイスが検出されていますが、PoEが使用できない状態か、リアルタイム電力消費が最大電力割り当てを超えています。 <p>(注) 動作モードは、指定したPoEポート、指定したスタックメンバ、またはスイッチのすべてのPoEポートの現在のPoEステータスです。</p>
Admin Police	<p>リアルタイム電力消費ポリシング機能のステータス：</p> <ul style="list-style-type: none"> • errdisable： ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 • l og： ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 • none： ポリシングはディセーブルです。
Oper Police	<p>ポリシング ステータス：</p> <ul style="list-style-type: none"> • errdisable： リアルタイム電力消費が最大電力割り当てを超えています。スイッチが PoE ポートをシャットダウンします。 • log： リアルタイム電力消費が最大電力割り当てを超えています。スイッチが Syslog メッセージを生成します。 • n/a： デバイス検出がディセーブルで、電力が PoE ポートに適用されていないか、ポリシングアクションが設定されていません。 • ok： リアルタイム電力消費は最大電力割り当てを下回っています。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシングアクションを実行します。
Oper Power	受電デバイスのリアルタイム電力消費です。

- ¹ 設定電力とは、手動で指定する電力、または CDP 電力ネゴシエーションまたは IEEE 分類を使用してスイッチが指定する電力です（電力検知機能によってモニタされるリアルタイムの電力とは異なります）。

speed

10/100/1000 Mbps ポートの速度を指定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
speed { 10 | 100 | 1000 | auto  [{ 10 | 100 | 1000 }]}
no speed
```

構文の説明

10	ポートが 10 Mbps で稼働することを指定します。
100	ポートが 100 Mbps で稼働することを指定します。
1000	ポートが 1000 Mbps で稼働することを指定します。このオプションは、10/100/1000 Mb/s ポートでだけ有効になって表示されます。
auto	稼働時のポートの速度を、リンクのもう一方の終端のポートを基準にして自動的に検出します。 auto キーワードと一緒に 10 、 100 、または 1000 キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。

コマンド デフォルト

デフォルトは **auto** です。

コマンド モード

インターフェイス コンフィギュレーション (**config-if**)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

10 ギガビットイーサネット ポートでは速度を設定できません。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーション設定を使用することを強く推奨します。一方のインターフェイスでは自動ネゴシエーションをサポートし、もう一方の終端ではサポートしていない場合、サポートしている側には **auto** 設定を使用し、サポートしていない終端にはデュプレックスおよび速度を設定します。



注意

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

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェアコンフィギュレーションガイドの「Configuring Interface Characteristics」の章を参照してください。

設定を確認するには、**show interfaces** 特権 EXEC コマンドを使用します。

例

次に、ポートの速度を 100 Mbps に設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed 100
```

次に、10 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10
```

次に、10 Mbps または 100 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10 100
```

switchport block

不明なマルチキャストまたはユニキャストパケットが転送されないようにするには、インターフェイス コンフィギュレーションモードで **switchport block** コマンドを使用します。不明なマルチキャストまたはユニキャストパケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block {multicast | unicast}
no switchport block {multicast | unicast}

構文の説明

multicast 不明のマルチキャストトラフィックがブロックされるように指定します。

(注) 純粋なレイヤ2マルチキャストトラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。

unicast 不明のユニキャストトラフィックがブロックされるように指定します。

コマンドデフォルト

不明なマルチキャストおよびユニキャストトラフィックはブロックされていません。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、不明な MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャストトラフィックをブロックすることができます。不明なマルチキャストまたはユニキャストトラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャストトラフィックでは、ポートブロッキング機能は純粋なレイヤ2パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャストパケットはブロックされません。

不明なマルチキャストまたはユニキャストトラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェアコンフィギュレーションガイドを参照してください。

次の例では、インターフェイス上で不明なユニキャストトラフィックをブロックする方法を示します。

```
Device(config-if)# switchport block unicast
```

設定を確認するには、**show interfaces *interface-id* switchport** 特権 EXEC コマンドを入力します。

voice-signalingvlan (ネットワークポリシーコンフィギュレーション)

音声シグナリングアプリケーションタイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice-signaling vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice-signaling vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}

構文の説明

vlan-id	(任意) 音声トラフィック用の VLAN。指定できる範囲は 1 ~ 4094 です。
cos cos-value	(任意) 設定された VLAN に対するレイヤ 2 プライオリティ Class of Service (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルト値は 5 です。
dscp dscp-value	(任意) 設定された VLAN に対する Diffserv コードポイント (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 46 です。
dot1p	(任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話を設定します。
none	(任意) 音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	(任意) タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンドデフォルト

音声シグナリングアプリケーションタイプのネットワークポリシー プロファイルは定義されていません。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンドモード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** 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。

voice-signaling アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが **voice policy TLV** にアドバタイズされたポリシーとして適用される場合、このアプリケーションタイプはアドバタイズしないでください。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、Diffserv コード ポイント (DSCP) の値、およびタギング モードを指定することで、音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の **network-policy Time Length Value (TLV)** に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 2 の CoS を持つ VLAN 200 用の音声シグナリングを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 200 cos 2
```

次の例では、DSCP 値 45 を持つ VLAN 400 用の音声シグナリングを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 400 dscp 45
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声シグナリングを設定する方法を示します。

```
Device(config-network-policy)# voice-signaling vlan dot1p cos 4
```


voicevlan (ネットワークポリシーコンフィギュレーション)

音声アプリケーションタイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーションモードで **voice vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

```
voice vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

構文の説明

<i>vlan-id</i>	(任意) 音声トラフィック用の VLAN。指定できる範囲は 1 ~ 4094 です。
cos <i>cos-value</i>	(任意) 設定された VLAN に対するレイヤ 2 プライオリティ Class of Service (CoS) を指定します。指定できる範囲は 0 ~ 7 です。デフォルト値は 5 です。
dscp <i>dscp-value</i>	(任意) 設定された VLAN に対する Diffserv コードポイント (DSCP) 値を指定します。指定できる範囲は 0 ~ 63 です。デフォルト値は 46 です。
dot1p	(任意) IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話を設定します。
none	(任意) 音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	(任意) タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンドデフォルト

音声アプリケーションタイプのネットワークポリシー プロファイルは定義されていません。
 デフォルトの CoS 値は、5 です。
 デフォルトの DSCP 値は、46 です。
 デフォルトのタギングモードは、untagged です。

コマンドモード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーションモードを開始するには、**network-policy profile** 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。

voice アプリケーションタイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データアプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service (CoS)、Diffserv コード ポイント (DSCP) の値、およびタギング モードを指定することで、音声用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) の network-policy Time Length Value (TLV) に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーションタイプを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーションタイプを設定する方法を示します。

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 dscp 34
```

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

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



第 II 部

レイヤ2

- [レイヤ2 コマンド \(97 ページ\)](#)



レイヤ2コマンド

- [channel-group](#) (100 ページ)
- [channel-protocol](#) (105 ページ)
- [clear lacp](#) (106 ページ)
- [clear pagp](#) (107 ページ)
- [clear spanning-tree counters](#) (108 ページ)
- [clear spanning-tree detected-protocols](#) (109 ページ)
- [debug etherchannel](#) (110 ページ)
- [debug lacp](#) (112 ページ)
- [debug pagp](#) (113 ページ)
- [debug platform etherchannel](#) (115 ページ)
- [debug platform pm](#) (116 ページ)
- [debug spanning-tree](#) (119 ページ)
- [interface port-channel](#) (121 ページ)
- [lacp port-priority](#) (123 ページ)
- [lacp system-priority](#) (125 ページ)
- [pagp learn-method](#) (126 ページ)
- [pagp port-priority](#) (128 ページ)
- [pagp timer](#) (129 ページ)
- [rep admin vlan](#) (130 ページ)
- [rep block port](#) (132 ページ)
- [rep lsl-age-timer](#) (134 ページ)
- [rep preempt delay](#) (135 ページ)
- [rep preempt segment](#) (137 ページ)
- [rep preempt segment](#) (139 ページ)
- [rep stcn](#) (141 ページ)
- [show etherchannel](#) (142 ページ)
- [show interfaces rep detail](#) (146 ページ)
- [show lacp](#) (148 ページ)
- [show pagp](#) (153 ページ)

- show platform etherchannel (155 ページ)
- show platform pm (156 ページ)
- show platform spanning-tree (158 ページ)
- show rep topology (159 ページ)
- show spanning-tree (161 ページ)
- show udld (165 ページ)
- spanning-tree backbonefast (168 ページ)
- spanning-tree bpdfilter (169 ページ)
- spanning-tree bpdguard (171 ページ)
- spanning-tree bridge assurance (172 ページ)
- spanning-tree cost (174 ページ)
- spanning-tree etherchannel guard misconfig (176 ページ)
- spanning-tree extend system-id (177 ページ)
- spanning-tree guard (178 ページ)
- spanning-tree link-type (180 ページ)
- spanning-tree loopguard default (181 ページ)
- spanning-tree mode (182 ページ)
- spanning-tree mst configuration (183 ページ)
- spanning-tree mst cost (185 ページ)
- spanning-tree mst forward-time (186 ページ)
- spanning-tree mst hello-time (187 ページ)
- spanning-tree mst max-age (188 ページ)
- spanning-tree mst max-hops (189 ページ)
- spanning-tree mst port-priority (190 ページ)
- spanning-tree mst pre-standard (191 ページ)
- spanning-tree mst priority (192 ページ)
- spanning-tree mst root (193 ページ)
- spanning-tree mst simulate pvst (グローバル コンフィギュレーション) (195 ページ)
- spanning-tree mst simulate pvst (インターフェイス コンフィギュレーション) (197 ページ)
- spanning-tree pathcost method (199 ページ)
- spanning-tree mst port-priority (200 ページ)
- spanning-tree portfast edge (グローバル コンフィギュレーション) (201 ページ)
- spanning-tree portfast edge (インターフェイス コンフィギュレーション) (204 ページ)
- spanning-tree transmit hold-count (206 ページ)
- spanning-tree uplinkfast (207 ページ)
- spanning-tree vlan (209 ページ)
- switchport access vlan (211 ページ)
- switchport mode (214 ページ)
- switchport nonegotiate (217 ページ)
- udld (219 ページ)

- [udld port](#) (221 ページ)
- [udld reset](#) (223 ページ)

channel-group

EtherChannel グループにイーサネットポートを割り当てる、EtherChannel モードをイネーブルにする、またはその両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。EtherChannel グループからイーサネットポートを削除するには、このコマンドの **no** 形式を使用します。

channel-group | *channel-group-number* **mode** {**active** | **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** | **passive**}
no channel-group

構文の説明

auto	個々のポート インターフェイスの auto-LAG 機能をイネーブルにします。 デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
<i>channel-group-number</i>	チャンネルグループ番号。 指定できる範囲は 1 ~ 6 です。
mode	EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol (LACP) をイネーブルにします。
auto	Port Aggregation Protocol (PAgP) 装置が検出された場合に限り、PAgP をイネーブルにします。
non-silent	(任意) PAgP 対応のパートナーに接続されたとき、インターフェイスを非サイレント動作に設定します。他の装置からのトラフィックが予想されている場合に PAgP モードで auto または desirable キーワードとともに使用されません。

desirable	無条件に PAgP をイネーブルにします。
on	on モードをイネーブルにします。
passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。

コマンド デフォルト チャンネルグループは割り当てることができません。
モードは設定されていません。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン レイヤ2の EtherChannel では、チャンネルグループに最初の物理ポートが追加されると、**channel-group** コマンドがポートチャンネルインターフェイスを自動的に作成します。ポートチャンネルインターフェイスを手動で作成するためにグローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用する必要はありません。最初にポートチャンネルインターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは自動的に新しいポートチャンネルを作成します。

チャンネルグループの一部である物理ポートに割り当てられた IP アドレスをディセーブルにする必要はありませんが、これをディセーブルにすることを強く推奨します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーションコマンドを使用して、レイヤ3のポートチャンネルを作成できます。インターフェイスをチャンネルグループに適用する前に、ポートチャンネルの論理インターフェイスを手動で設定してください。

EtherChannel を設定した後、ポートチャンネルインターフェイスに加えられた設定の変更は、そのポートチャンネルインターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャンネルインターフェイスに対してコンフィギュレーションコマンドを適用します。たとえば、**spanning-tree** コマンドを使用して、レイヤ2 EtherChannel をトランクとして設定します。

active モードは、ポートをネゴシエーションステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャンネルは、active モードまたは passive モードの別のポートグループで形成されます。

auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケットネゴシエーションを開始することはありません。チャンネルは、**desirable** モードの別のポートグループでだけ形成されます。**auto** がイネーブルの場合、サイレント動作がデフォルトになります。

desirable モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、**desirable** モードまたは **auto** モードの別のポートグループで形成されます。**desirable** がイネーブルの場合、サイレント動作がデフォルトになります。

auto モードまたは **desirable** モードとともに **non-silent** を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレントモードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にデバイスを接続する場合です。サイレントパートナーの例は、トラフィックを生成しないファイルサーバ、またはパケットアナライザなどです。この場合、物理ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャンネルグループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

on モードでは、使用可能な EtherChannel が存在するのは、両方の接続ポートグループが **on** モードになっている場合だけです。



(注) **on** モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループを正しく設定しないと、パケット損失やスパニングツリーループが発生することがあります。

passive モードは、ポートをネゴシエーションステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。チャンネルは、**active** モードの別のポートグループでだけ形成されます。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック構成ではできません）。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol 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プロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては上書きされません。

アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、IEEE 802.1X ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1X 認証をイネーブルにしようとすると、エラーメッセージが表示され、IEEE 802.1X 認証はイネーブルになりません。

セキュアポートを EtherChannel の一部として、または EtherChannel ポートをセキュアポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。



- (注) 物理 EtherChannel ポート上で、レイヤ3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジグループを割り当てることは、ループが発生する原因になるため、行わないでください。

次に、スタック内の1つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート2つを PAgP モード desirable であるチャンネル5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable
Device(config-if-range)# end
```

次に、スタック内の1つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート2つを LACP モード active であるチャンネル5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/1 - 2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

次の例では、スイッチスタックのクロススタック EtherChannel を設定する方法を示します。LACP パッシブモードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタックメンバ2 のポートを2つ、スタックメンバ3 のポートを1つチャンネル5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range GigabitEthernet 2/0/4 - 5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface GigabitEthernet 3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-protocol	チャネリングを管理するため、ポート上で使用されるプロトコルを制限します。

コマンド	説明
switchport access vlan	ポートをスタティックアクセスポートとして設定します。
switchport mode	ポートの VLAN メンバーシップモードを設定します。

channel-protocol

ポート上で使用されるプロトコルを制限してチャネリングを管理するには、インターフェイス コンフィギュレーションモードで **channel-protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

channel-protocol {lacp | pagp}
no channel-protocol

構文の説明

lacp Link Aggregation Control Protocol (LACP) で EtherChannel を設定します。

pagp Port Aggregation Protocol (PAgP) で EtherChannel を設定します。

コマンド デフォルト

EtherChannel に割り当てられているプロトコルはありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定は **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

channel-group インターフェイス コンフィギュレーション コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

クロススタック構成の PAgP を設定できません。

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
Device(config-if)# channel-protocol lacp
```

設定を確認するには、**show etherchannel [channel-group-number] protocol** 特権 EXEC コマンドを入力します。

clear lacp

Link Aggregation Control Protocol (LACP) チャンネルグループカウンタをクリアするには、特権 EXEC モードで **clear lacp** コマンドを使用します。

clear lacp [*channel-group-number*] **counters**

構文の説明	<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1～6 です。
	counters	トラフィックカウンタをクリアします。
コマンド デフォルト	なし	
コマンド モード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン すべてのカウンタをクリアするには、**clear lacp counters** コマンドを使用します。また、指定のチャンネルグループのカウンタのみをクリアするには、**clear lacp channel-group-number counters** コマンドを使用します。

次の例では、すべてのチャンネルグループ情報をクリアする方法を示します。

```
Device# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
Device# clear lacp 4 counters
```

情報が削除されたことを確認するには、**show lacp counters** または **show lacp channel-group-number counters** 特権 EXEC コマンドを使用します。

関連コマンド	コマンド	説明
	debug lacp	LACP アクティビティのデバッグを有効にします。
	show lacp	LACP チャンネルグループ情報を表示します。

clear pagp

Port Aggregation Protocol (PAgP) チャンネルグループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

clear pagp [*channel-group-number*] **counters**

構文の説明

<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 6 です。
counters	トラフィックカウンタをクリアします。

コマンドデフォルト

なし

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、指定のチャンネルグループのカウンタのみをクリアするには、**clear pagp channel-group-number counters** コマンドを使用します。

次の例では、すべてのチャンネルグループ情報をクリアする方法を示します。

```
Device# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
Device# clear pagp 10 counters
```

情報が削除されたことを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show pagp	PAgP チャンネル グループ情報を表示します。

clear spanning-tree counters

スパニングツリーのカウンタをクリアするには、特権EXECモードで **clear spanning-tree counters** コマンドを使用します。

clear spanning-tree counters [**interface interface-id**]

構文の説明

interface interface-id

(任意) 指定のインターフェイスのスパニングツリーカウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。

指定できる VLAN 範囲は 1 ~ 4094 です。

ポートチャネルの範囲は 1 ~ 6 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC (#)

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

interface-id が指定されていない場合は、すべてのインターフェイスのスパニングツリーカウンタがクリアされます。

次の例では、すべてのインターフェイスのスパニングツリーカウンタをクリアする方法を示します。

```
Device# clear spanning-tree counters
```


clear spanning-tree detected-protocols

デバイスでプロトコル移行プロセスを再開して、強制的にネイバーと再ネゴシエーションするには、特権 EXEC モードで **clear spanning-tree detected-protocols** コマンドを使用します。

clear spanning-tree detected-protocols [*interface interface-id*]

構文の説明	interface interface-id	(任意) 指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。 指定できる VLAN 範囲は 1 ~ 4094 です。 ポートチャネルの範囲は 1 ~ 6 です。
コマンドデフォルト	なし	
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン Rapid Per-VLAN Spanning-Tree Plus (Rapid PVST+) プロトコルまたは Multiple Spanning Tree Protocol (MSTP) が稼働するデバイスは、組み込み済みのプロトコル移行方式をサポートしています。それによって、スイッチはレガシー IEEE 802.1D デバイスと相互に動作できるようになります。Rapid PVST+ または MSTP デバイスが、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーションブリッジプロトコルデータユニット (BPDU) を受信した場合、そのデバイスはそのポートで IEEE 802.1D BPDU だけを送信します。マルチスパンニングツリー (MST) デバイスが、レガシー BPDU、別のリージョンに対応する MST BPDU (バージョン3)、または高速スパンニングツリー (RST) BPDU (バージョン2) を受信したときは、そのポートがリージョンの境界にあることを検知します。

デバイスは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的に Rapid PVST+ モードまたは MSTP モードには戻りません。これは、レガシースイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Device# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

EtherChannel のデバッグをイネーブルにするには、特権 EXEC モードで **debug etherchannel** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug etherchannel [{all | detail | error | event | idb}]
no debug etherchannel [{all | detail | error | event | idb}]
```

構文の説明

all	(任意) EtherChannel デバッグ メッセージをすべて表示します。
detail	(任意) EtherChannel デバッグ メッセージの詳細を表示します。
error	(任意) EtherChannel エラー デバッグ メッセージを表示します。
event	(任意) EtherChannel イベント メッセージを表示します。
idb	(任意) PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebg etherchannel コマンドは **no debug etherchannel** コマンドと同じです。



(注) **linecard** キーワードは、コマンドラインのヘルプに表示されますが、サポートされていません。

あるスタック上でデバッグをイネーブルにした場合、でのみイネーブルになります。でデバッグをイネーブルにするには、特権 EXEC モードで **session switch-number** コマンドを使用してからセッションを開始します。のコマンドラインプロンプトで **debug** コマンドを入力します。

で最初にセッションを開始せずにでデバッグをイネーブルにするには、特権 EXEC モードで **remote command switch-number LINE** コマンドを使用します。

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
Device# debug etherchannel all
```

次の例では、EtherChannel イベント関連のデバッグ メッセージを表示する方法を示します。

```
Device# debug etherchannel event
```

debug lacp

Link Aggregation Control Protocol (LACP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug lacp** コマンドを使用します。LACP のデバッグ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。

```
debug lacp [{all | event | fsm | misc | packet}]
no debug lacp [{all | event | fsm | misc | packet}]
```

構文の説明

all	(任意) LACP デバッグ メッセージをすべて表示します。
event	(任意) LACP イベント デバッグ メッセージを表示します。
fsm	(任意) LACP 有限状態マシン内の変更に関するメッセージを表示します。
misc	(任意) 各種 LACP デバッグ メッセージを表示します。
packet	(任意) 受信および送信 LACP 制御パケットを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebg etherchannel コマンドは **no debug etherchannel** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session switch-number** コマンドを使用してアクティブスイッチからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command switch-number LINE** コマンドを使用します。

次の例では、すべての LACP デバッグ メッセージを表示する方法を示します。

```
Device# debug LACP all
```

次の例では、LACP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
Device# debug LACP event
```

debug pagp

Port Aggregation Protocol (PAgP) アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pagp** コマンドを使用します。PAgP のデバッグ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。

```
debug pagp [{all | dual-active | event | fsm | misc | packet}]
no debug pagp [{all | dual-active | event | fsm | misc | packet}]
```

構文の説明		
	all	(任意) PAgP デバッグ メッセージをすべて表示します。
	dual-active	(任意) デュアル アクティブ検出メッセージを表示します。
	event	(任意) PAgP イベントデバッグメッセージを表示します。
	fsm	(任意) PAgP 有限状態マシン内の変更に関するメッセージを表示します。
	misc	(任意) 各種 PAgP デバッグメッセージを表示します。
	packet	(任意) 送受信 PAgP 制御パケットを表示します。

コマンド デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebug pagp** コマンドは **no debug pagp** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session switch-number** コマンドを使用してアクティブスイッチからセッションを開始します。スタックメンバのコマンドラインプロンプトで **debug** コマンドを入力します。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command switch-number LINE** コマンドを使用します。

次の例では、すべての PAgP デバッグ メッセージを表示する方法を示します。

```
Device# debug pagp all
```

次の例では、PAgP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
Device# debug pagp event
```

debug platform etherchannel

プラットフォームに依存する EtherChannel イベントのデバッグをイネーブルにするには、EXEC モードで **debug platform etherchannel** コマンドを使用します。デバッグ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。

```
debug platform etherchannel {init | link-up | rpc | warnings}
no debug platform etherchannel {init | link-up | rpc | warnings}
```

構文の説明

init	EtherChannel モジュール初期化デバッグ メッセージを表示します。
link-up	EtherChannel リンクアップおよびリンクダウンに関連したデバッグ メッセージを表示します。
rpc	EtherChannel リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。
warnings	EtherChannel 警告デバッグ メッセージを表示します。

コマンドデフォルト

デバッグはディセーブルです。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebg platform etherchannel コマンドは **no debug platform etherchannel** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session switch-number** コマンドを使用してアクティブスイッチからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command switch-number LINE** コマンドを使用します。

次に、EtherChannel 初期化に関連するデバッグ メッセージを表示する例を示します。

```
Device# debug platform etherchannel init
```

debug platform pm

プラットフォーム依存ポートマネージャソフトウェアモジュールのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform pm** コマンドを使用します。デバッグ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。

```
debug platform pm {all | atom | counters | errdisable | etherchnl | exceptions | gvi | hpm-events |
idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span | pm-vectors [detail]
| rpc [{general | oper-info | state | vectors | vp-events}]} | soutput-vectors | stack-manager | sync |
vlans}
no debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events | idb-events
| if-numbers | ios-events | link-status | platform | pm-events | pm-span | pm-vectors [detail] | rpc
[{general | oper-info | state | vectors | vp-events}]} | soutput-vectors | stack-manager | sync | vlans}
```

構文の説明

all	すべてのポートマネージャデバッグメッセージを表示します。
atom	AToM 関連イベントを表示します。
counters	リモートプロシージャコール (RPC) デバッグメッセージのカウンタを表示します。
errdisable	error-disabled 関連イベントデバッグメッセージを表示します。
etherchnl	EtherChannel 関連イベントデバッグメッセージを表示します。
exceptions	システム例外デバッグメッセージを表示します。
gvi	IPe GV 関連メッセージを表示します。
hpm-events	プラットフォームポートマネージャイベントデバッグメッセージを表示します。
idb-events	インターフェイス記述ブロック (IDB) 関連イベントデバッグメッセージを表示します。
if-numbers	インターフェイス番号移動イベントデバッグメッセージを表示します。
ios-events	Cisco IOS ソフトウェアイベントを表示します。
link-status	インターフェイスリンク検出イベントデバッグメッセージを表示します。

platform	ポートマネージャ関数イベントデバッグメッセージを表示します。
pm-events	ポートマネージャイベントデバッグメッセージを表示します。
pm-span	ポートマネージャスイッチドポートアナライザ (SPAN) イベントデバッグメッセージを表示します。
pm-vectors	ポートマネージャベクトル関連イベントデバッグメッセージを表示します。
detail	(任意) ベクトル関数の詳細を表示します。
rpc	RPC 関連メッセージを表示します。
general	(任意) 一般的な RPC 関連メッセージを表示します。
oper-info	(任意) 操作および情報関連 RPC メッセージを表示します。
state	(任意) 管理および操作関連 RPC メッセージを表示します。
vectors	(任意) ベクトル関連 RPC メッセージを表示します。
vp-events	(任意) 仮想ポート関連 RPC メッセージを表示します。
soutput-vectors	IDB 出力ベクトル イベント デバッグ メッセージを表示します。
stack-manager	スタックマネージャ関連イベントデバッグメッセージを表示します。 このキーワードは、スタック対応スイッチでのみサポートされています。
sync	操作同期およびVLANラインステートイベントデバッグメッセージを表示します。
vlans	VLAN 作成および削除イベント デバッグ メッセージを表示します。

コマンドデフォルト デバッグはディセーブルです。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebg platform pm** コマンドは **no debug platform pm** コマンドと同じです。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次に、VLAN の作成および削除に関するデバッグ メッセージを表示する例を示します。

```
Device# debug platform pm vlans
```

debug spanning-tree

スパニングツリーアクティビティのデバッグをイネーブルにするには、EXEC モードで **debug spanning-tree** コマンドを使用します。デバッグ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。

debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | csuf/csrt | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast}

構文の説明

all	スパニングツリーのデバッグメッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニングツリーブリッジプロトコルデータユニット (BPDU) デバッグメッセージを表示します。
bpdu-opt	最適化された BPDU 処理デバッグメッセージを表示します。
config	スパニングツリー設定変更デバッグメッセージを表示します。
csuf/csrt	クロススタック UplinkFast およびクロススタック高速遷移アクティビティ デバッグメッセージを表示します。
etherchannel	EtherChannel サポート デバッグメッセージを表示します。
events	スパニングツリー トポロジ イベント デバッグメッセージを表示します。
exceptions	スパニングツリー例外デバッグメッセージを表示します。
general	一般的なスパニングツリー アクティビティ デバッグメッセージを表示します。
mstp	Multiple Spanning Tree Protocol (MSTP) イベントをデバッグします。
pvst+	Per VLAN Spanning-Tree Plus (PVST+) イベント デバッグメッセージを表示します。

root	スパニングツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニングツリーの Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 処理デバッグ メッセージを表示します。
switch	デバイス シム コマンド デバッグ メッセージを表示します。このシムは、一般的なスパニングツリー プロトコル (STP) コードと、各デバイス プラットフォーム固有コードとの間のインターフェイスとなるソフトウェアモジュールです。
synchronization	スパニングツリー同期 イベント デバッグ メッセージを表示します。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

コマンド デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebg spanning-tree** コマンドは **no debug spanning-tree** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合は、アクティブスイッチでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session switch-number** コマンドを使用してアクティブスイッチからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

アクティブスイッチで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command switch-number LINE** コマンドを使用します。

次の例では、すべてのスパニングツリーデバッグメッセージを表示する方法を示します。

```
Device# debug spanning-tree all
```

interface port-channel

ポートチャンネルにアクセスするか、またはポートチャンネルを作成するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。ポートチャンネルを削除するには、このコマンドの **no** 形式を使用します。

```
interface port-channel port-channel-number
no interface port-channel
```

構文の説明	<i>port-channel-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1～6 です。
コマンド デフォルト	ポートチャンネル論理インターフェイスは定義されません。	
コマンド モード	グローバル コンフィギュレーション (config)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン レイヤ 2 EtherChannel では、物理ポートをチャンネルグループに割り当てる前にポートチャンネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。このコマンドでは、チャンネルグループが最初の物理ポートを獲得すると、ポートチャンネル論理インターフェイスが自動的に作成されます。最初にポートチャンネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャンネルを作成します。

interface port-channel コマンドの次に **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 3 のポートチャンネルを作成できます。インターフェイスをチャンネルグループに適用する前に、ポートチャンネルの論理インターフェイスを手動で設定してください。

チャンネル グループ内の 1 つのポートチャンネルだけが許可されます。



(注) ポートチャンネル インターフェイスをルーテッドポートとして使用する場合、チャンネルグループに割り当てられた物理ポート上のレイヤ 3 に、アドレスを割り当てないようにしてください。



- (注) レイヤ3のポートチャネルインターフェイスとして使用されているチャネルグループの物理ポート上で、ブリッジグループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用するときは、次のガイドラインに従ってください。

- Cisco Discovery Protocolを使用する場合には、これを物理ポートで設定してください。ポートチャネルインターフェイスでは設定できません。
- EtherChannelのアクティブメンバであるポートをIEEE 802.1Xポートとしては設定しないでください。まだアクティブになっていないEtherChannelのポートでIEEE 802.1Xをイネーブルにしても、ポートはEtherChannelに加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーションガイドの「Configuring EtherChannels」の章を参照してください。

次の例では、ポートチャネル番号5でポートチャネルインターフェイスを作成する方法を示します。

```
Device(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel channel-group-number detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
channel-group	EtherChannelグループにイーサネットポートを割り当てる、EtherChannelモードをイネーブルにする、またはこの両方を行います。
show etherchannel	チャネルのEtherChannel情報を表示します。
show pagp	PAgPチャネルグループ情報を表示します。

lacp port-priority

Link Aggregation Control Protocol (LACP) のポートプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp port-priority priority
no lacp port-priority

構文の説明

priority LACP のポートプライオリティ。指定できる範囲は1～65535です。

コマンドデフォルト

デフォルトは 32768 です。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネルグループに9つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイモードに置かれるポートを判別します。

LACP チャネルグループは、同じタイプのイーサネットポートを16個まで保有できます。最大8つのポートを active モードに、最大8つのポートを standby モードにできます。

ポートプライオリティの比較では、数値が小さいほどプライオリティが高くなります。LACP チャネルグループに9つ以上のポートがある場合、LACP ポートプライオリティの数値が小さい（つまり、高いプライオリティ値の）8つのポートがチャネルグループにバンドルされ、それより低いプライオリティのポートはホットスタンバイモードに置かれます。LACP ポートプライオリティが同じポートが2つ以上ある場合（たとえば、そのいずれもデフォルト設定の65535に設定されている場合）、ポート番号の内部値によりプライオリティが決定されます。



- (注) LACP リンクを制御するデバイス上にポートがある場合に限り、LACP ポートプライオリティは有効です。リンクを制御するデバイスの判別については、**lacp system-priority** グローバルコンフィギュレーション コマンドを参照してください。

LACP ポートプライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上でのLACPの設定については、このリリースに対応する構成ガイドを参照してください。

次の例では、ポートで LACP ポートプライオリティを設定する方法を示します。

```
Device# interface gigabitethernet2/0/1  
Device(config-if)# lACP port-priority 1000
```

設定を確認するには、**show lACP [channel-group-number] internal** 特権 EXEC コマンドを入力します。

lACP system-priority

Link Aggregation Control Protocol (LACP) のシステムプライオリティを設定するには、デバイスのグローバルコンフィギュレーションモードで **lACP system-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lACP system-priority priority
no lACP system-priority

構文の説明

priority LACP のシステムプライオリティ。指定できる範囲は 1～65535 です。

コマンドデフォルト

デフォルトは 32768 です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

lACP system-priority コマンドでは、ポートプライオリティを制御する LACP リンクのデバイスが判別されます。

LACP チャネルグループは、同じタイプのイーサネットポートを 16 個まで保有できます。最大 8 つのポートを **active** モードに、最大 8 つのポートを **standby** モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にあるデバイスは、ポートプライオリティを使用して、チャンネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他のデバイス（リンクの非制御側終端）上のポートプライオリティは無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システムプライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのデバイスも同じ LACP システムプライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（デバイスの MAC アドレス）により制御するデバイスが判別されます。

lACP system-priority コマンドは、デバイス上のすべての LACP EtherChannel に適用されます。

ホットスタンバイモード（ポートステータスフラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次の例では、LACP のシステムプライオリティを設定する方法を示します。

```
Device(config)# lACP system-priority 20000
```

設定を確認するには、**show lACP sys-id** 特権 EXEC コマンドを入力します。

pagp learn-method

EtherChannelポートから受信した着信パケットの送信元アドレスを学習するには、インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

構文の説明

aggregation-port 論理ポート チャンネルでのアドレス ラーニングを指定します。デバイスは、EtherChannel のいずれかのポートを使用して送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要ではありません。

physical-port EtherChannel 内の物理ポートでのアドレス ラーニングを指定します。デバイスは、送信元アドレスを学習したのと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャンネルのもう一方の終端では、特定の宛先 MAC または IP アドレスに対してチャンネル内の同じポートが使用されます。

コマンド デフォルト

デフォルトは、aggregation-port（論理ポート チャンネル）です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス (CLI) で **physical-port** キーワードが指定された場合でも、デバイスがサポートするのは集約ポートでのアドレスラーニングのみです。 **pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドはデバイスのハードウェアには影響を及ぼしませんが、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンクパートナーが物理ラーナーである場合、 **pagp learn-method physical-port** 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物理ポートラーナーとしてデバイスを設定することを推奨します。また、 **port-channel load-balance src-mac** 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、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。 **pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、EtherChannel 内の物理ポート上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel 内のポート チャンネル上のアドレスを学習するように学習方式を設定する方法を示します。

```
Device(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp channel-group-number internal** 特権 EXEC コマンドを入力します。

pagp port-priority

EtherChannel を経由してすべての Port Aggregation Protocol (PAgP) トラフィックが送信されるポートを選択するには、インターフェイス コンフィギュレーション モードで **pagp port-priority** コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイモードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼働状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority priority
no pagp port-priority

構文の説明

priority プライオリティ番号。有効な範囲は0～255です。

コマンド デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

コマンドライン インターフェイス (CLI) で **physical-port** キーワードが指定された場合でも、デバイスがサポートするのは集約ポートでのアドレスラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドはデバイスのハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンクパートナーが物理ラーナーである場合、**pagp learn-method physical-port** 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物理ポートラーナーとしてデバイスを設定することを推奨します。また、**port-channel load-balance src-mac** 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、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、ポートプライオリティを 200 に設定する方法を示します。

```
Device(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp channel-group-number internal** 特権 EXEC コマンドを入力します。

pagp timer

PAgP タイマーの有効期限を設定するには、インターフェイス コンフィギュレーション モードで **pagp timer** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp timer *time*

no pagp timer

構文の説明	<i>time</i> PAgP 情報パケットがタイムアウトするまでの経過時間を秒数で指定します。指定できる範囲は 45 ~ 90 です。
-------	-----------------------------------------------------------------------

コマンド デフォルト	なし
------------	----

コマンド モード	インターフェイス コンフィギュレーション
----------	----------------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン	このコマンドは、PAgP ポート チャネルの一部として設定されているすべてのインターフェイスで使用できます。
------------	--------------------------------------------------------

次に、PAgP タイマーの有効期限を 50 秒に設定する例を示します。

```
Device(config-if)# pagp timer 50
```

rep admin vlan

Resilient Ethernet Protocol (REP) の REP 管理 VLAN を設定して、ハードウェアフラッドレイヤ (HFL) メッセージを送信するには、グローバルコンフィギュレーションモードで **rep admin vlan** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
rep admin vlan vlan-id [segment segment-id]
no rep admin vlan vlan-id [segment segment-id]
```

構文の説明	<i>vlan-id</i>	REP 管理 VLAN。これは、48 ビットの静的 MAC アドレスです。管理 VLAN のデフォルト値は VLAN 1 です。
	segment <i>segment-id</i>	指定したセグメントに管理 VLAN を構成します。セグメント ID の範囲は 1 ~ 1024 です。管理 VLAN を設定しない場合、デフォルト VLAN は VLAN 1 です。
コマンド デフォルト	なし	
コマンド モード	グローバル コンフィギュレーション (config)	
コマンド履歴	リリース	変更内容
	Cisco IOS リリース 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン REP は、STANDALONE モードの動作でのみサポートされます。
 REP 管理 VLAN の範囲は 1 ~ 4094 です。
 デバイスとセグメントで 1 つの管理 VLAN だけが可能です。
 設定を確認するには、特権 EXEC モードで **show interfaces rep detail** コマンドを入力します。

例 次に、VLAN 100 を REP 管理 VLAN として設定する例を示します。

```
Device(config)# rep admin vlan 100
```

次に、セグメントごとに管理 VLAN を作成する例を示します。ここでは、VLAN 2 は REP セグメント 2 でのみ管理 VLAN として設定されます。設定されていない残りのすべてのセグメントでは、デフォルトで VLAN 1 が管理 VLAN として設定されます。

```
Device(config)# rep admin vlan 2 segment 2
```

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep block port

Resilient Ethernet Protocol (REP) プライマリエッジポートで REP VLAN ロードバランシングを設定するには、インターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
no rep block port {id port-id | neighbor-offset | preferred}
```

構文の説明

id <i>port-id</i>	REP を有効にすると自動的に生成される一意のポート ID を入力して VLAN ブロッキング代替ポートを指定します。REP ポート ID は、16 文字の 16 進数値です。
<i>neighbor-offset</i>	ネイバーのオフセット番号を入力することによる、VLAN ブロック代替ポート。範囲は -256 ~ +256 です。値 0 は無効です。
preferred	すでに VLAN ロードバランシングの優先代替ポートとして指定されている通常セグメントポートを選択します。
vlan	ブロックされる VLAN を指定します。
<i>vlan-list</i>	表示される VLAN ID または VLAN ID の範囲。ブロックする VLAN ID (1 ~ 4094 の範囲) を入力するか、ブロックする LANID の範囲または連続番号 (1-3、22、41-44 など) を入力します。
all	すべての VLAN をブロックします。

コマンド デフォルト

特権 EXEC モードで **rep preempt segment** コマンドを入力した後のデフォルト動作では (手動プリエンプションの場合)、プライマリエッジポートですべての VLAN をブロックします。この動作は、**rep block port** コマンドを設定するまで継続されます。

プライマリ エッジ ポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンプションなし、および VLAN ロードバランシングなしです。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS リリース 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。

負の番号は、セカンダリ エッジポート（オフセット番号-1）とダウンストリーム ネイバーを識別します。



- (注) 番号 1 はプライマリ エッジポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

インターフェイス コンフィギュレーションモードで、**rep preempt delay seconds** コマンドを入力することでプリエンプション遅延時間を設定しており、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロードバランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメントポートのブロックを解除します。プライマリ エッジポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポートのポート ID を判別するには、特権 EXEC モードで **show interfaces interface-id rep detail** コマンドを入力します。

例

次に、REP VLAN ロードバランシングを設定する例を示します。

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep lsl-age-timer

Resilient Ethernet Protocol (REP) リンクステータスレイヤ (LSL) のエージアウトタイマー値を設定するには、インターフェイス コンフィギュレーションモードで **rep lsl-age-timer** コマンドを使用します。デフォルトのエージアウトタイマー値に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age-timer *milliseconds*
no rep lsl-age-timer *milliseconds*

構文の説明 *milliseconds* ミリ秒単位の REP LSL エージアウト タイマー値。範囲は 120 ~ 10000 の 40 の倍数です。

コマンド デフォルト デフォルトの LSL エージアウト タイマー値は 5 ミリ秒です。

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

例 次に、REP LSL エージアウト タイマー値を設定する例を示します。

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep lsl-age-timer 2000
```

関連コマンド	コマンド	説明
	interface interface-type interface-name	STCNを受信する物理インターフェイスまたはポートチャネルを指定します。
	rep segment	インターフェイス上で REP をイネーブルにし、セグメント ID を割り当てます。

rep preempt delay

セグメントポートの障害およびリカバリの発生後、Resilient Ethernet Protocol (REP) VLAN ロードバランシングがトリガーされるまでの待機時間を設定するには、インターフェイスコンフィギュレーションモードで **rep preempt delay** コマンドを使用します。設定した遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay seconds
no rep preempt delay

構文の説明

seconds REP プリエンプションを遅延する秒数です。範囲は 15 ~ 300 秒です。デフォルトは遅延なしの手動プリエンプションです。

コマンド デフォルト

REP プリエンプション遅延は設定されていません。デフォルトは遅延なしの手動プリエンプションです。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

REP プライマリ エッジ ポート上にこのコマンドを入力します。

リンク障害とリカバリ後に自動的に VLAN ロードバランシングをトリガーする場合は、このコマンドを入力してプリエンプション時間遅延を設定します。

VLAN ロードバランシングが設定されている場合、セグメントポート障害とリカバリの後、VLAN ロードバランシングが発生する前に REP プライマリ エッジポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、(**rep block port** 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設定された) VLAN ロードバランシングを実行するように REP プライマリエッジポートが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジポートでブロックされます。

設定を確認するには、**show interfaces rep** コマンドを入力します。

例

次に、プライマリ エッジポートで REP プリエンプション時間遅延を 100 秒に設定する例を示します。

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep preempt segment

Resilient Ethernet Protocol (REP) VLAN ロードバランシングがセグメントで手動で開始されるようにするには、特権 EXEC モードで **rep preempt segment** コマンドを使用します。

rep preempt segment *segment-id*

構文の説明

segment-id REP セグメントの ID です。有効な範囲は 1 ~ 1024 です。

コマンド デフォルト

デフォルト動作は手動プリエンプションです。

コマンド モード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デバイスのプライマリ エッジポートがあるセグメントで、次のコマンドを入力します。

VLAN ロードバランシングのプリエンプションを設定する前に、他のすべてのセグメントの設定が完了していることを確認してください。VLAN ロードバランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの実行前に確認メッセージが表示されます。

プライマリエッジポートで、インターフェイス コンフィギュレーションモードから **rep preempt delay** *seconds* コマンドを入力せずに、プリエンプション時間遅延を設定する場合、デフォルト設定はセグメントでの VLAN ロードバランシングの手動トリガーです。

特権 EXEC モードで **show rep topology** コマンドを入力して、セグメント内のどのポートがプライマリエッジポートなのかを確認します。

VLAN ロードバランシングを設定しない場合、**rep preempt segment** *segment-id* コマンドを入力すると、デフォルトの動作が実行されます。つまりプライマリエッジポートがすべてのVLANをブロックします。

REP プライマリエッジポートのインターフェイス コンフィギュレーションモードで **rep block port** コマンドを入力して VLAN ロードバランシングを設定してから、手動でプリエンプションを開始できます。

例

次に、セグメント 100 で手動で REP プリエンプションをトリガーする例を示します。

```
Device# rep preempt segment 100
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロードバランシングがトリガーされるまでの待機期間を設定します。
show rep topology	セグメントまたはすべてのセグメントの REP トポロジ情報を表示します。

rep preempt segment

Resilient Ethernet Protocol (REP) VLAN ロードバランシングがセグメントで手動で開始されるようにするには、特権 EXEC モードで **rep preempt segment** コマンドを使用します。

rep preempt segment *segment-id*

構文の説明

segment-id REP セグメントの ID です。有効な範囲は 1 ~ 1024 です。

コマンド デフォルト

デフォルト動作は手動プリエンプションです。

コマンド モード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デバイスのプライマリ エッジポートがあるセグメントで、次のコマンドを入力します。

VLAN ロードバランシングのプリエンプションを設定する前に、他のすべてのセグメントの設定が完了していることを確認してください。VLAN ロードバランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの実行前に確認メッセージが表示されます。

プライマリエッジポートで、インターフェイス コンフィギュレーションモードから **rep preempt delay** *seconds* コマンドを入力せずに、プリエンプション時間遅延を設定する場合、デフォルト設定はセグメントでの VLAN ロードバランシングの手動トリガーです。

特権 EXEC モードで **show rep topology** コマンドを入力して、セグメント内のどのポートがプライマリエッジポートなのかを確認します。

VLAN ロードバランシングを設定しない場合、**rep preempt segment** *segment-id* コマンドを入力すると、デフォルトの動作が実行されます。つまりプライマリエッジポートがすべての VLAN をブロックします。

REP プライマリエッジポートのインターフェイス コンフィギュレーションモードで **rep block port** コマンドを入力して VLAN ロードバランシングを設定してから、手動でプリエンプションを開始できます。

例

次に、セグメント 100 で手動で REP プリエンプションをトリガーする例を示します。

```
Device# rep preempt segment 100
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロードバランシングがトリガーされるまでの待機期間を設定します。
show rep topology	セグメントまたはすべてのセグメントの REP トポロジ情報を表示します。

rep stcn

セグメントトポロジ変更通知 (STCN) を他のインターフェイスまたは他のセグメントに送信するように Resilient Ethernet Protocol (REP) エッジポートを設定するには、インターフェイスコンフィギュレーションモードで **rep stcn** コマンドを使用します。インターフェイスまたはセグメントへの STCN の送信タスクを無効にするには、このコマンドの **no** 形式を使用します。

```
rep stcn {interface interface-id | segment segment-id-list}
no rep stcn {interface | segment}
```

構文の説明

interface interface-id STCN を受信する物理インターフェイスまたはポートチャネルを指定します。

segment segment-id-list STCN を受信する 1 つの REP セグメントまたは REP セグメントの一覧を指定します。セグメントの範囲は 1 ~ 1024 です。また、一連のセグメント (たとえば 3 ~ 5、77、100) を設定することもできます。

コマンドデフォルト

他のインターフェイスおよびセグメントへの STCN 送信は、無効になっています。

コマンドモード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

設定を確認するには、特権 EXEC モードで **show interfaces rep detail** コマンドを入力します。

例

次に、セグメント 25 ~ 50 に STCN を送信するように REP エッジポートを設定する例を示します。

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```

show etherchannel

チャンネルの EtherChannel 情報を表示するには、ユーザ EXEC モードで **show etherchannel** コマンドを使用します。

```
show etherchannel [{channel-group-number | {detail | port | port-channel | protocol | summary
}}] | [{auto | detail | load-balance | port | port-channel | protocol | summary}]
```

構文の説明	<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 6 です。
	auto	(任意) Etherchannel が自動的に作成する情報を表示します。
	detail	(任意) 詳細な EtherChannel 情報を表示します。
	load-balance	(任意) ポート チャンネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
	port	(任意) EtherChannel ポートの情報を表示します。
	port-channel	(任意) ポート チャンネル情報を表示します。
	protocol	(任意) EtherChannel で使用されるプロトコルを表示します。
	summary	(任意) 各チャンネル グループのサマリーを 1 行で表示します。
コマンド デフォルト	なし	
コマンド モード	ユーザ EXEC (>) 特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン チャンネル グループ番号を指定しない場合は、すべてのチャンネル グループが表示されます。

出力では、パッシブ ポート リスト フィールドはレイヤ 3 のポート チャンネルだけで表示されます。このフィールドは、まだ起動していない物理ポートがチャンネルグループ内で設定されていること（および間接的にチャンネル グループ内で唯一のポート チャンネルであること）を意味します。

次に、**show etherchannel auto** コマンドの出力例を示します。

```
Device# show etherchannel auto

Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SUA)        LACP        Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次に、**show etherchannel channel-group-number detail** コマンドの出力例を示します。

```
Device> show etherchannel 1 detail

Group state = L2
Ports: 2  Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:    LACP
              Ports in the group:
              -----
Port: Gi1/0/1
-----
Port state    = Up Mstr In-Bndl
Channel group = 1      Mode = Active          Gcchange = -
Port-channel  =          PolGC = -          Pseudo port-channel = Po1
Port index    =          0Load = 0x00        Protocol = LACP

Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:

Port      Flags  State  LACP port  Admin  Oper  Port  Port
Gi1/0/1  SA    bndl   32768     0x1    0x1   0x101 0x3D
Gi1/0/2  A     bndl   32768     0x0    0x1   0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

              Port-channels in the group:
              -----

Port-channel: Po1  (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1      Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
```

```

-----+-----+-----+-----+-----
0      00    Gi1/0/1    Active      0
0      00    Gi1/0/2    Active      0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

```

次に、**show etherchannel channel-group-number summary** コマンドの出力例を示します。

```

Device> show etherchannel 1 summary

Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)        LACP      Gi1/0/1(P) Gi1/0/2(P)

```

次に、**show etherchannel channel-group-number port-channel** コマンドの出力例を示します。

```

Device> show etherchannel 1 port-channel

Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load  Port  EC state  No of bits
-----+-----+-----+-----+-----
0      00    Gi1/0/1 Active    0
0      00    Gi1/0/2 Active    0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2

```

次に、**show etherchannel protocol** コマンドの出力例を示します。

```

Device# show etherchannel protocol

Channel-group listing:
-----
Group: 1
-----
Protocol: LACP
Group: 2
-----

```

Protocol: PAgP

show interfaces rep detail

管理 VLAN を含む、すべてのインターフェイスまたは指定されたインターフェイスの詳細な Resilient Ethernet Protocol (REP) の設定およびステータスを表示するには、特権 EXEC モードで **show interfaces rep detail** コマンドを使用します。

show interfaces [*interface-id*] **rep detail**

構文の説明	<i>interface-id</i> (任意) ポート ID を表示するために使用される物理インターフェイス。	
コマンド デフォルト	なし	
コマンド モード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、1つ以上のセグメントまたは1つのインターフェイスに STCN を送信先するために、セグメントエッジポートで入力します。

設定を確認するには、特権 EXEC モードで **show interfaces rep detail** コマンドを入力します。

例

次に、指定されたインターフェイスに関する REP 設定とステータスを表示する例を示します。

```
Devices# show interfaces TenGigabitEthernet4/1 rep detail
```

```
TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

関連コマンド

コマンド	説明
rep admin vlan	REPがHFLメッセージを送信するためのREP管理VLANを設定します。

show lacp

Link Aggregation Control Protocol (LACP) チャンネルグループ情報を表示するには、ユーザ EXEC モードで **show lacp** コマンドを使用します。

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}

構文の説明	
<i>channel-group-number</i>	(任意) チャンネルグループ番号。指定できる範囲は 1 ~ 6 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。
sys-id	LACP によって使用されるシステム識別子を表示します。システム識別子は、LACP システムプライオリティとデバイス MAC アドレスで構成されています。

コマンド デフォルト なし

コマンド モード ユーザ EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

show lacp コマンドを入力すると、アクティブなチャンネルグループの情報が表示されます。特定のチャンネル情報を表示するには、チャンネルグループ番号を指定して **show lacp** コマンドを入力します。

チャンネルグループを指定しない場合は、すべてのチャンネルグループが表示されます。

channel-group-number を入力すると、**sys-id** 以外のすべてのキーワードでチャンネルグループを指定できます。

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group:1
Gi2/0/1    19   10         0    0         0    0         0
Gi2/0/2    14    6         0    0         0    0         0
```


表 11: `show lacp counters` のフィールドの説明

フィールド	説明
LACPDUs Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

次に、`show lacp internal` コマンドの出力例を示します。

```
Device> show lacp 1 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State  LACP port  Admin  Oper  Port  Port
Gi2/0/1   SA     bndl   32768      0x3    0x3   0x4   0x3D
Gi2/0/2   SA     bndl   32768      0x3    0x3   0x5   0x3D
```

次の表に、出力されるフィールドの説明を示します。

表 12: show lacp internal のフィールドの説明

フィールド	説明
ステータス	<p>特定のポートの状態。次に使用可能な値を示します。</p> <ul style="list-style-type: none"> • - : ポートの状態は不明です。 • bndl : ポートがアグリゲータに接続され、他のポートとバンドルされています。 • susp : ポートが中断されている状態で、アグリゲータには接続されていません。 • hot-sby : ポートがホットスタンバイの状態です。 • indiv : ポートは他のポートとバンドルできません。 • indep : ポートは独立状態です。バンドルされていませんが、データトラフィックを処理することができます。この場合、LACP は相手側ポートで実行されていません。 • down : ポートがダウンしています。
LACP Port Priority	<p>ポートのプライオリティ設定。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポートプライオリティを使用してポートをスタンバイモードにします。</p>
Admin Key	<p>ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します (16 進数)。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。ポートが他のポートと集約できるかどうかは、ポートの物理特性 (たとえば、データレートやデュプレックス機能) と設定に指定された制限によって決定されます。</p>
Oper Key	<p>ポートで使用される実行時の操作キー。LACP は自動的に値を生成します (16 進数)。</p>
Port Number	<p>ポート番号。</p>

フィールド	説明
Port State	<p>ポートの状態変数。1つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。</p> <ul style="list-style-type: none"> • bit0 : LACP のアクティビティ • bit1 : LACP のタイムアウト • bit2 : 集約 • bit3 : 同期 • bit4 : 収集 • bit5 : 配信 • bit6 : デフォルト • bit7 : 期限切れ <p>(注) 上のリストでは、bit7 が MSB で bit0 は LSB です。</p>

次に、**show lacp neighbor** コマンドの出力例を示します。

```
Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
```

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Partner Age	Partner Flags
Gi2/0/1	32768,0007.eb49.5e80	0xC	19s	SP
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Partner Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

次に、**show lacp sys-id** コマンドの出力例を示します。

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

システムIDは、システムプライオリティおよびシステムMACアドレスで構成されています。最初の2バイトはシステムプライオリティ、最後の6バイトはグローバルに管理されているシステム関連の個々のMACアドレスです。

show pagp

ポート集約プロトコル (PAgP) のチャンネルグループ情報を表示するには、EXEC モードで **show pagp** コマンドを使用します。

show pagp [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**}

構文の説明		
	<i>channel-group-number</i>	(任意) チャンネルグループ番号。 指定できる範囲は 1 ~ 6 です。
	counters	トラフィック情報を表示します。
	dual-active	デュアルアクティブ ステータスが表示されま す。
	internal	内部情報を表示します。
	neighbor	ネイバーの情報を表示します。

コマンド デフォルト なし

コマンド モード ユーザ EXEC (>)
特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されまし た。

使用上のガイドライン **show pagp** コマンドを入力すると、アクティブなチャンネルグループの情報が表示されます。非アクティブポートチャンネルの情報を表示するには、チャンネルグループ番号を指定して **show pagp** コマンドを入力します。

例

次に、**show pagp 1 counters** コマンドの出力例を示します。

```
Device> show pagp 1 counters
```

```

          Information          Flush
Port      Sent   Recv   Sent   Recv
-----
Channel group: 1
  Gi1/0/1   45    42     0     0
  Gi1/0/2   45    41     0     0

```

次に、**show pagp dual-active** コマンドの出力例を示します。

```
Device> show pagp dual-active
```

```
PAGP dual-active detection enabled: Yes
PAGP dual-active version: 1.1
```

```
Channel group 1
      Dual-Active   Partner           Partner   Partner
Port   Detect Capable Name             Port      Version
Gi1/0/1 No              Device          Gi3/0/3   N/A
Gi1/0/2 No              Device          Gi3/0/4   N/A
```

```
<output truncated>
```

次に、**show pagp 1 internal** コマンドの出力例を示します。

```
Device> show pagp 1 internal
```

```
Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
       A - Device is in Auto mode.
Timers: H - Hello timer is running.       Q - Quit timer is running.
       S - Switching timer is running.    I - Interface timer is running.
```

```
Channel group 1
      Hello   Partner   PAGP   Learning   Group
Port   Flags State  Timers  Interval Count  Priority Method  Ifindex
Gi1/0/1 SC   U6/S7  H       30s      1     128    Any    16
Gi1/0/2 SC   U6/S7  H       30s      1     128    Any    16
```

次に、**show pagp 1 neighbor** コマンドの出力例を示します。

```
Device> show pagp 1 neighbor
```

```
Flags: S - Device is sending Slow hello.  C - Device is in Consistent state.
       A - Device is in Auto mode.         P - Device learns on physical port.
```

```
Channel group 1 neighbors
      Partner           Partner           Partner Group
Port   Name                 Device ID         Port              Age  Flags  Cap.
Gi1/0/1 Device-p2             0002.4b29.4600  Gi01//1          9s  SC    10001
Gi1/0/2 Device-p2             0002.4b29.4600  Gi1/0/2          24s SC    10001
```

show platform etherchannel

プラットフォーム依存 EtherChannel 情報を表示するには、特権 EXEC モードで **show platform etherchannel** コマンドを使用します。

show platform etherchannel {**data-structures** | **flags** | **time-stamps**}

構文の説明	data-structures	EtherChannel データ構造を表示します。
	flags	EtherChannel ポート フラグを表示します。
	time-stamps	EtherChannel タイム スタンプを表示します。

コマンド デフォルト なし

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform pm

プラットフォーム依存のポートマネージャ情報を表示するには、特権 EXEC モードで **show platform pm** コマンドを使用します。

show platform pm {**counters** | **group-masks** | **idbs** {**active-idbs** | **deleted-idbs**} | **if-numbers** | **link-status** | **module-info** | **platform-block** | **port-info** *interface-id* | **stack-view** | **vlan** {**info** | **line-state**}}

構文の説明		
	counters	モジュール カウンタ情報を表示します。
	group-masks	EtherChannel グループ マスク情報を表示します。
	idbs { active-idbs deleted-idbs }	Interface Data Block (IDB) 情報を表示します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • active-idbs : アクティブな IDB 情報を表示します。 • deleted-idbs : 削除または漏えいされた IDB 情報を表示します。
	if-numbers	インターフェイス番号情報を表示します。
	link-status	ローカルポートリンクステータス情報を表示します。
	module-info	モジュールのステータス情報を表示します。
	platform-block	プラットフォーム ポートブロック情報を表示します。
	port-info <i>interface-id</i>	指定されたインターフェイスのポート管理フィールドおよび動作フィールドを表示します。
	stack-view	スタックのステータス情報を表示します。 このキーワードは、LAN Lite イメージではサポートされません。

vlan {info | line-state}

プラットフォーム VLAN 情報を表示します。キーワードの意味は次のとおりです。

- **info** : アクティブ VLAN の情報を表示します。
 - **line-state** : 回線状態の情報を表示します。
-

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release
15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

stack-view キーワードは、LAN Lite イメージを実行するスイッチではサポートされません。

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform spanning-tree

プラットフォーム依存スパニングツリー情報を表示するには、**show platform spanning-tree** 特権 EXEC コマンドを使用します。

show platform spanning-tree synchronization [{detail | vlan *vlan-id*}]

構文の説明

synchronization スパニングツリー ステート同期情報を表示します。

detail (任意) スパニングツリーの詳細情報を表示します。

vlan *vlan-id* (任意) 指定した VLAN の VLAN デバイスのスパニングツリー情報を表示します。指定できる範囲は 1 ~ 4094 です。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show rep topology

セグメント、またはセグメント内のプライマリおよびセカンダリエッジポートを含むすべてのセグメントの Resilient Ethernet Protocol (REP) トポロジ情報を表示するには、特権 EXEC モードで **show rep topology** コマンドを使用します。

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

構文の説明

segment <i>segment-id</i>	(任意) REP トポロジ情報を表示するセグメントを指定します。セグメント <i>ID</i> の範囲は 1 ~ 1024 です。
archive	(任意) セグメントの前のトポロジを表示します。このキーワードは、リンク障害のトラブルシューティングに役立ちます。
detail	(任意) REP トポロジの詳細情報を表示します。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show rep topology** コマンドの出力例を示します。

```
Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228  Te3/4         Open
10.64.106.228  Te3/3         Open
10.64.106.67   Te4/3         Open
10.64.106.67   Te4/4         Alt
10.64.106.63   Te4/4         Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68    Gi40/2        Open
10.64.106.68    Gi40/1        Open
10.64.106.63    Gi50/2        Sec  Alt
```

次に、**show rep topology detail** コマンドの出力例を示します。

```
Device# show rep topology detail

REP Segment 1
```

```
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

show spanning-tree

指定されたスパニングツリー インスタンスのスパニングツリー情報を表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show spanning-tree** コマンドを使用します。

```
show spanning-tree [{active | backbonefast | blockedports | bridge | detail | inconsistentports |
interface interface-type interface-number | mst | pathcost | root | summary [totals] | uplinkfast | vlan
vlan-id}]
```

構文の説明

active	(任意) アクティブインターフェイスに関するスパニングツリー情報だけを表示します。
backbonefast	(任意) スパニングツリー BackboneFast ステータスを表示します。
blockedports	(任意) ブロックされたポート情報を表示します。
bridge	(任意) このスイッチのステータスおよび設定を表示します。
detail	(任意) 詳細情報を表示します。
inconsistentports	(任意) 不整合ポートに関する情報を表示します。
interface <i>interface-type</i> <i>interface-number</i>	(任意) インターフェイスのタイプおよび番号を指定します。
mst	(任意) 複数のスパニングツリーを指定します。
pathcost	(任意) スパニングツリーの pathcost オプションを表示します。
root	(任意) ルートスイッチのステータスおよび設定を表示します。
summary	(任意) ポート ステートのサマリーを指定します。
totals	(任意) スパニングツリーステートセクションのすべての行を表示します。
uplinkfast	(任意) スパニングツリー UplinkFast ステータスを表示します。
vlan <i>vlan-id</i>	(任意) VLAN ID を指定します。指定できる範囲は 1 ~ 4094 です。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **vlan** キーワードを使用するときに **vlan-id** 値を指定しないと、コマンドはすべての VLAN の spanning-tree インスタンスに適用されます。

次に、**show spanning-tree active** コマンドの出力例を示します。

```
Device# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost       3038
             Port       24 (GigabitEthernet2/0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153 (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300
  Uplinkfast enabled

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi2/0/1        Root FWD 3019      128.24  P2p
Gi0/1          Root FWD 3019      128.24  P2p
<output truncated>
```

次に、**show spanning-tree detail** コマンドの出力例を示します。

```
Device# show spanning-tree detail
Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.42e2.cdd0
Root port is 1 (GigabitEthernet2/0/1), cost of root path is 3038
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 1d16h ago
Times: hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300
Uplinkfast enabled

Port 1 (GigabitEthernet2/0/1) of VLAN0001 is forwarding
  Port path cost 3019, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 0001.42e2.cdd0
  Designated bridge has priority 32768, address 00d0.bbf5.c680
  Designated port id is 128.25, designated path cost 19
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  BPDU: sent 0, received 72364

<output truncated>
```

次に、**show spanning-tree summary** コマンドの出力例を示します。

```
Device# show spanning-tree interface mst configuration
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is disabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is enabled
BackboneFast is enabled
Pathcost method used is short

Name                Blocking Listening Learning Forwarding STP Active
-----
VLAN0001             1           0           0           11          12
VLAN0002             3           0           0           1           4
VLAN0004             3           0           0           1           4
VLAN0006             3           0           0           1           4
VLAN0031             3           0           0           1           4
VLAN0032             3           0           0           1           4
<output truncated>
-----
37 vlans             109         0           0           47          156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----
Number of transitions via uplinkFast (all VLANs) : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0
```

次に、**show spanning-tree mst configuration** コマンドの出力例を示します。

```
Device# show spanning-tree interface mst configuration
Name [region1]
Revision 1
Instance Vlans Mapped
-----
0       1-9,21-4094
1       10-20
-----
```

次の例では、**show spanning-tree interface mst interface interface-id** コマンドの出力を示します。

```
Device# show spanning-tree interface mst configuration
GigabitEthernet2/0/1 of MST00 is root forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (STP) bpdu guard : disable (default)
Bpdus sent 5, received 74
```

```
Instance role state cost      prio vlans mapped
0          root FWD  200000  128  1,12,14-4094
```

次の例では、**show spanning-tree interface mst *instance-id*** コマンドの出力を示します。

```
Device# show spanning-tree interface mst 0
GigabitEthernet2/0/1 of MST00 is root forwarding
Edge port: no                (default)      port guard : none        (default)
Link type: point-to-point (auto)      bpdu filter: disable    (default)
Boundary : boundary         (STP)        bpdu guard : disable    (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0          root FWD  200000  128  1,12,14-4094
```


show uddl

すべてのポートまたは指定されたポートの単方向リンク検出 (UDLD) の管理ステータスおよび動作ステータスを表示するには、ユーザ EXEC モードで **show uddl** コマンドを使用します。

show uddl [{*interface_id* | **neighbors**}]

構文の説明

interface-id (任意) インターフェイスの ID およびポート番号です。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャンネルなどがあります。

neighbors (任意) ネイバー情報だけを表示します。

コマンドデフォルト

なし

コマンドモード

ユーザ EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

インターフェイス ID を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

次の例では、**show uddl interface-id** コマンドの出力を示します。ここでは、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを UDLD が検出します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device> show uddl gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

表 13: show uddl のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス。
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブルステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼働しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	UDLD ステート マシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステートマシンはアダバタイズ フェーズです。
Message interval	ローカルデバイスからアダバタイズメッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD がネイバー デバイスからのエコーを待機する期間 (秒)。
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間 (秒)。
Device ID	ネイバー デバイスの ID。

フィールド	説明
Current neighbor state	ネイバーの現在の状態。ローカルデバイスおよびネイバー装置の両方で UDLD が通常どおり稼働している場合、ネイバー ステートおよびローカル ステートは双方向です。リンクがダウンしているか、またはネイバーが UDLD 対応でない場合、キャッシュ エントリは表示されません。
デバイス名	装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト (Switch) に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーのネイバー デバイス名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズ メッセージを送信する速度 (秒)。
CDP device name	CDP デバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト (Switch) に設定されている場合、システムのシリアル番号が表示されます。

次に、**show udld neighbors** コマンドの出力例を示します。

```
Device# show udld neighbors
Port      Device Name      Device ID  Port-ID  OperState
-----
Gi2/0/1   Switch-A         1          Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A         2          Gi3/0/1  Bidirectional
```

spanning-tree backbonefast

BackboneFast をイネーブルにして、デバイス上のブロックされたポートを即座にリスニングモードに切り替えられるようにするには、グローバル コンフィギュレーション モードで **spanning-tree backbonefast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree backbonefast
no spanning-tree backbonefast

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

BackboneFast はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

BackboneFast をイネーブルにすることで、デバイスは間接リンク障害を検出し、通常のスパニングツリールールを使用している場合よりも早く、スパニングツリーの再設定を開始できるようになります。

BackboneFast は、Rapid PVST+ またはマルチ スパニングツリー (MST) モード用に設定できますが、スパニングツリーモードを PVST+ に変更するまでこの機能はディセーブルのままです。

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを使用します。

例

次に、デバイスで BackboneFast をイネーブルにする例を示します。

```
Device(config)# spanning-tree backbonefast
```

spanning-tree bpdudfilter

インターフェイス上でブリッジプロトコルデータユニット (BPDU) フィルタリングをイネーブルにするには、インターフェイス コンフィギュレーションモードで **spanning-tree bpdudfilter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpdudfilter {enable | disable}
no spanning-tree bpdudfilter

構文の説明

enable インターフェイスでの BPDU フィルタリングをイネーブルにします。

disable インターフェイスでの BPDU フィルタリングをディセーブルにします。

コマンド デフォルト

spanning-tree portfast bpdudfilter default コマンドの入力時点ですでに設定されている設定

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdudfilter enable** : インターフェイス上の BPDU フィルタリングを無条件にイネーブルにします。
- **spanning-tree bpdudfilter disable** : インターフェイス上の BPDU フィルタリングを無条件にディセーブルにします。
- **no spanning-tree bpdudfilter** : 動作中の PortFast インターフェイスに **spanning-tree portfast bpdudfilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。



注意

spanning-tree bpdudfilter enable コマンドを入力するときは注意してください。インターフェイス上で BPDU フィルタリングをイネーブルにすることは、このインターフェイスのスパニングツリーをディセーブルにすることと類似しています。このコマンドを正しく使用しない場合、ブリッジング ループが発生する可能性があります。

デバイスが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST モード、またはマルチ スパニング ツリー (MST) モードで動作している場合は、BPDU フィルタリングをイネーブルにできます。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdudfilter default** コマンドを使用します。

spanning-tree bpdudfilter enable コマンドは、PortFast の設定に優先します。

例

次に、現在のインターフェイス上で BPDU フィルタリングをイネーブルにする例を示します。

```
Device(config-if) # spanning-tree bpdudfilter enable  
Device(config-if) #
```

spanning-tree bpduguard

インターフェイス上で Bridge protocol data unit (BPDU) Guard をイネーブルにするには、インターフェイス コンフィギュレーション モードで **spanning-tree bpduguard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree bpduguard {enable | disable}
no spanning-tree bpduguard
```

構文の説明

enable インターフェイス上での BPDU ガードをイネーブルにします。

disable インターフェイス上での BPDU ガードをディセーブルにします。

コマンド デフォルト

spanning-tree portfast bpduguard default コマンドの入力時点ですでに設定されている設定

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

サービスプロバイダー環境内で任意のアクセスポートがスパンニングツリーに参加しないようにするには、BPDU ガード機能を使用します。ポートが引き続き BPDU を受信する場合は、保護対策としてポートが **error-disabled** ステートに置かれます。このコマンドには次の3つの状態があります。

- **spanning-tree bpduguard enable** : インターフェイスで BPDU ガードを無条件でイネーブルにします。
- **spanning-tree bpduguard disable** : インターフェイスで BPDU ガードを無条件でディセーブルにします。
- **no spanning-tree bpduguard** : 動作中の PortFast インターフェイスに **spanning-tree portfast bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

例

次の例では、インターフェイス上で BPDU ガードをイネーブルにする方法を示します。

```
Device(config-if)# spanning-tree bpduguard enable
Device(config-if)#
```

spanning-tree bridge assurance

ネットワークで Bridge Assurance をイネーブルにするには、**spanning-tree bridge assurance** コマンドを使用します。この機能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。

spanning-tree bridge assurance
no spanning-tree bridge assurance

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Bridge Assurance はイネーブルにされています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドがサポートされるようになりました。

使用上のガイドライン

この機能により、ネットワークがブリッジンググループから保護されます。この機能では、すべてのネットワークポートでのポイントツーポイントリンクのBPDUの受信がモニタされます。ポートが割り当てられた hello タイム期間内に BPDU を受信しない場合、ポートはブロック状態（フレームの転送が停止するポート不整合状態と同じ）になります。ポートがBPDUの受信を再開すると、ポートは通常のスパニングツリー動作を再開します。

デフォルトでは、Bridge Assurance は動作中のすべてのネットワークポート（代替ポートとバックアップポートを含む）でイネーブルになっています。接続されたレイヤ2スイッチまたはブリッジであるすべての必須ポートで **spanning-tree portfast network** コマンドを設定した場合、Bridge Assurance はこれらすべてのネットワークポートで自動的に有効になります。

Bridge Assurance をサポートするのは、Rapid PVST+ および MST スパニングツリープロトコルのみです。PVST+ は Bridge Assurance をサポートしません。

Bridge Assurance が正しく動作するには、ポイントツーポイントリンクの両端で Bridge Assurance がサポートおよび設定されている必要があります。リンクの一端のデバイスで Bridge Assurance がイネーブルであっても、他端のデバイスでイネーブルになっていない場合、接続ポートはブロックされます（Bridge Assurance 不整合状態）。Bridge Assurance は、ネットワーク全体でイネーブルにすることを推奨します。

ポート上で Bridge Assurance をイネーブルにするには、BPDU フィルタリングと BPDU Guard をディセーブルにする必要があります。

Bridge Assurance は、Loop Guard とともにイネーブルにできます。

Bridge Assurance は、ルートガードとともにイネーブルにできます。後者は、ネットワークでのルートブリッジの配置を強制する方法を提供するように設計されています。

ブリッジ保証をディセーブルにすると、すべての設定済みネットワークポートが標準のスパニングツリーポートとして動作します。

この機能がポートでイネーブルになっているかどうかを確認するには、**show spanning-tree summary** コマンドを使用します。

例

次の例では、スイッチのすべてのネットワークポートで Bridge Assurance をイネーブルにし、ネットワークポートを設定する方法を示します。

```
Device(config)# spanning-tree bridge assurance
Device(config)# interface gigabitethernet 5/8
Device(config-if)# spanning-tree portfast network
Device(config-if)# exit
```

次に、スパニングツリー情報を表示し、Bridge Assurance がイネーブルになっているかどうかを確認する例を示します。出力で、次の情報を調べます。

- Portfast Default : ネットワーク
- Bridge Assurance : イネーブル

```
Device# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0199-VLAN0200, VLAN0128
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is network
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default is enabled
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active
-----
VLAN0199 0 0 0 5 5
VLAN0200 0 0 0 4 4
VLAN0128 0 0 0 4 4
-----
3 vlans 0 0 0 13 13
```

spanning-tree cost

スパニングツリープロトコル（STP）計算に使用するインターフェイスのパスコストを設定するには、インターフェイス コンフィギュレーション モードで **spanning-tree cost** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree [vlan vlan-id] cost cost
no spanning-tree cost
```

構文の説明

vlan *vlan-id* （任意）スパニングツリー インスタンスに対応させる VLAN 範囲を指定します。VLAN ID の範囲は 1 ～ 4094 です。

cost パス コスト。有効値は 1 ～ 200,000,000 です。

コマンド デフォルト

デフォルトパス コストは、インターフェイスの帯域幅設定から計算されます。デフォルトパス コストは次のとおりです。

- 1 Gb/s : 4
- 100 Mb/s : 19
- 10 Mb/s : 100

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スパニングツリー インスタンスに対応させる VLAN を指定する場合、VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN の範囲、またはカンマで区切られた一連の VLAN ID を指定できます。

引数 **cost** の値を指定する場合、値が大きいほどコストは高くなります。指定されたプロトコルタイプに関係なく、この値が適用されます。

例

次の例では、インターフェイスのパス コストの値を 250 に設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ～ 15、20 にパス コストとして 300 を設定する方法を示します。

```
Device(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

spanning-tree etherchannel guard misconfig

デバイスが EtherChannel の不良構成を検出したときにエラーメッセージを表示するには、グローバル コンフィギュレーション モードで **spanning-tree etherchannel guard misconfig** コマンドを使用します。エラーメッセージ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。

spanning-tree etherchannel guard misconfig
no spanning-tree etherchannel guard misconfig

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

エラー メッセージが表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デバイスが EtherChannel の不良構成を検出すると、次のエラーメッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.
```

不良構成に関与しているローカルポートを特定するには、**show interfaces status err-disabled** コマンドを入力します。リモート装置の EtherChannel 設定を調べるには、リモート装置上で **show etherchannel summary** コマンドを入力します。

設定を修正したら、対応するポートチャネル インターフェイス上で **shutdown** コマンドと **no shutdown** コマンドを入力します。

例

次に、EtherChannel ガードの設定ミス機能をイネーブルにする例を示します。

```
Device(config)# spanning-tree etherchannel guard misconfig
```

spanning-tree extend system-id

拡張システム ID をイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree extend system-id** コマンドを使用します。拡張システム ID 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。

spanning-tree extend system-id
no spanning-tree extend system-id

構文の説明 このコマンドには引数またはキーワードはありません。

コマンド デフォルト 拡張システム ID はイネーブルです。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スパニングツリーは、ブリッジ ID が VLAN またはマルチ スパニングツリー インスタンスごとに一意となるように、拡張システム ID、デバイスプライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用します。スイッチスタックは他のネットワークからは単一のスイッチとして認識されるため、スタック内のすべてのスイッチは、指定のスパニングツリーに対して同一のブリッジ ID を使用します。アクティブスイッチに障害が発生した場合、スタックメンバは、アクティブスイッチの新しい MAC アドレスに基づいて、実行しているスパニングツリーすべてのブリッジ ID を再計算します。

拡張システム ID のサポートにより、ルートスイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティの手動での設定方法に影響が生じます。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルートスイッチになることはほぼありません。拡張システム ID によって、接続されたスイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチプライオリティ値が増大します。

例

次に、拡張システム ID をイネーブルにする例を示します。

```
Device(config)# spanning-tree extend system-id
```

spanning-tree guard

インターフェイスに対応する VLAN でルートガードモードまたはループガードモードをイネーブルまたはディセーブルにするには、インターフェイス コンフィギュレーション モードで **spanning-tree guard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree guard {loop|root|none}
no spanning-tree guard
```

構文の説明

loop インターフェイスでループガードモードをイネーブルにします。

root インターフェイスでルートガードモードをイネーブルにします。

none ガードモードを None に設定します。

コマンド デフォルト

ルートガードモードはディセーブルです。

ループガードモードは、グローバル コンフィギュレーション モードの **spanning-tree loopguard default** コマンドによって設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デバイスが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、またはマルチスパンニングツリー (MST) モードで動作している場合は、ルートガードまたはループガードをイネーブルにできます。

ルートガードとループガードの両方を同時にイネーブルにすることはできません。

スパンニングツリーループガードのデフォルト設定を上書きするには、**spanning-tree guard loop** コマンドを使用します。

ルートガードがイネーブルの場合に、スパンニングツリーを計算すると、インターフェイスがルートポートとして選択され、**root-inconsistent** (ブロック) ステートに移行します。これにより、デバイスがルートスイッチになったり、ルートへのパスになったりすることはなくなります。ルートポートは、スイッチからルートスイッチまでの最適パスを提供します。

no spanning-tree guard または **no spanning-tree guard none** コマンドを入力すると、ルートガードは選択されたインターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが **root-inconsistent** (ブロック) ステートの場合、インターフェイスはリスニングステートに自動的に移行します。

UplinkFast 機能で使用するインターフェイスでは、ルートガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロック状態の）バックアップインターフェイスがルートポートになります。ただし、同時にルートガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップインターフェイスが **root-inconsistent**（ブロック）状態になり、フォワーディング状態に移行できなくなります。デバイスが Rapid-PVST+ モードまたは MST モードで動作している場合、UplinkFast 機能は使用できません。

例

次の例では、指定されたインターフェイスに対応するすべての VLAN で、ルートガードをイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/1  
Device(config-if)# spanning-tree guard root
```

spanning-tree link-type

ポートにリンクタイプを設定するには、インターフェイス コンフィギュレーション モードで **spanning-tree link-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree link-type {point-to-point | shared}
no spanning-tree link-type
```

構文の説明

point-to-point インターフェイスがポイントツーポイントリンクになるように指定します。

shared インターフェイスが共有メディアになるように指定します。

コマンド デフォルト

リンクタイプは、明示的に設定しなければ、デュプレックス設定から自動的に生成されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

Rapid Spanning Tree Protocol Plus (RSTP+) 高速トランジションが機能するのは、2つのブリッジ間のポイントツーポイントリンク上だけです。

デフォルトでは、デバイスはポートのリンクタイプをデュプレックスモードから取得します。つまり、全二重ポートはポイントツーポイントリンクと見なされ、半二重設定は共有リンク上にあると見なされます。

ポートを共有リンクとして指定した場合は、デュプレックス設定に関係なく、RSTP+高速トランジションは禁止されます。

例

次に、ポートを共有リンクとして設定する例を示します。

```
Device(config-if)# spanning-tree link-type shared
```


spanning-tree loopguard default

指定されたブリッジのすべてのポート上でループガードをデフォルトでイネーブルにするには、グローバル コンフィギュレーション モードで **spanning-tree loopguard default** コマンドを使用します。ループガード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。

spanning-tree loopguard default
no spanning-tree loopguard default

構文の説明 このコマンドには引数またはキーワードはありません。

コマンド デフォルト ループ ガードはディセーブルです。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン ループガードを使用すると、ブリッジネットワークのセキュリティを高めることができます。また、単方向リンクの原因となる障害によって代替ポートまたはルートポートが指定ポートとして使用されることがなくなります。

ループガードは、スパニングツリーがポイントツーポイントであると見なすポート上でのみ動作します。

ループガード ポートを個別に設定すると、このコマンドが上書きされます。

例

次に、ループ ガードをイネーブルにする例を示します。

```
Device(config)# spanning-tree loopguard default
```

spanning-tree mode

Per-VLAN Spanning Tree+ (PVST+)、Rapid-PVST+、およびマルチスパンニングツリー (MST) モードの間で切り替えるには、グローバル コンフィギュレーション モードで **spanning-tree mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree mode {pvst | mst | rapid-pvst}
no spanning-tree mode
```

構文の説明	pvst	PVST+ モードをイネーブルにします。
	mst	MST モードをイネーブルにします。
	rapid-pvst	Rapid-PVST+ モードをイネーブルにします。

コマンド デフォルト デフォルトモードは Rapid-PVST+ です。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 一度にアクティブにできるのは1つのモードだけです。

すべてのスタック メンバは、同一のスパンニングツリー モードを実行します。



注意 **spanning-tree mode** コマンドを使用して PVST+、Rapid-PVST+、および MST モードを切り替える場合は、慎重に行ってください。このコマンドを入力すると、以前のモードのスパンニングツリーインスタンスはすべて停止し、新しいモードで再開されます。このコマンドを使用すると、ユーザ トラフィックが中断されることがあります。

例

次に、MST モードをイネーブルにする例を示します。

```
Device(config)# spanning-tree mode mst
```

次に、デフォルト モード (PVST+) に戻す例を示します。

```
Device(config)# no spanning-tree mode
```

spanning-tree mst configuration

MST コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **spanning-tree mst configuration** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst configuration
no spanning-tree mst configuration

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、マルチ スパニングツリー (MST) の設定値がすべてのパラメータのデフォルト値になります。

- VLAN はどの MST インスタンスにもマッピングされません (すべての VLAN は Common and Internal Spanning Tree [CIST] インスタンスにマッピングされます)。
- 領域名は空の文字列になります。
- リビジョン番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

MST コンフィギュレーションには、次のコマンドを使用できます。

- **abort** 設定変更を適用しないで、MST リージョン コンフィギュレーション モードを終了します。
- **exit** MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用します。
- **instance** *instance_id* **vlan** *vlan_id* : VLAN を MST インスタンスにマッピングします。インスタンス ID の範囲は、1 ~ 4094 です。VLAN の範囲は 1 ~ 4094 です。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。
- **name** *name* : コンフィギュレーション名を設定します。 *name* 文字列では大文字と小文字が区別され、最大 32 文字です。
- **no** *instance*、*name*、および *revision* コマンドを無効にするか、またはデフォルト設定に戻します。
- **revision** *version* : コンフィギュレーション リビジョン番号を設定します。指定できる範囲は 0 ~ 65535 です。

- **show [current | pending** 現在のまたは保留中の MST リージョンの設定を表示します。

MST モードでは、1つのスイッチスタックは最大 65 個の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

2 台以上のスイッチが同一 MST リージョン内に存在する場合、同じ VLAN マッピング、同じコンフィギュレーション名、および同じコンフィギュレーションリビジョン番号が設定されている必要があります。

VLAN を MST インスタンスにマッピングすると、マッピングは増分で実行されます。コマンドで指定された VLAN は、すでにマッピング済みの VLAN に対して追加または削除されます。範囲を指定する場合はハイフンを使用します。たとえば、**instance 1 vlan 1-63** を指定した場合、VLAN 1 ~ 63 を MST インスタンス 1 にマッピングされます。列挙して指定する場合は、カンマを使用します。たとえば **instance 1 vlan 10, 20, 30** と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、Common and Internal Spanning Tree (CIST) インスタンス (インスタンス 0) にマッピングされます。このマッピングは、このコマンドの **no** 形式では CIST から解除できません。

MST コンフィギュレーションモードパラメータを変更すると、接続が失われることがあります。サービスの中断を最小限に抑えるために、MST コンフィギュレーションモードを開始したら、現在の MST コンフィギュレーションのコピーに変更を行ってください。コンフィギュレーションの編集が終了したら、**exit** キーワードを使用してすべての変更内容を一度に適用するか、または **abort** キーワードを使用して変更をコンフィギュレーションにコミットせずにモードを終了します。

例

次の例は、MST コンフィギュレーションモードを開始し、VLAN 10 ~ 20 を MSTI 1 にマッピングし、リージョンに **region1** という名前を付けて、コンフィギュレーションリビジョンを 1 に設定し、保留中の設定を表示する方法を示しています。

```
Device(config)# spanning-tree mst configuration
Device(config-mst)# instance 1 vlan 10-20
Device(config-mst)# name region1
Device(config-mst)# revision 1
Device(config-mst)# show pending
Pending MST configuration
Name          [region1]
Revision     1
Instance     Vlans  Mapped
-----
0            1-9,21-4094
1            10-20
-----
```

次の例では、MST コンフィギュレーションをデフォルト設定にリセットする方法を示します。

```
Device(config)# no spanning-tree mst configuration
```

spanning-tree mst cost

マルチスパンニングツリー（MST）計算に使用するインターフェイスのパスコストを設定するには、インターフェイス コンフィギュレーション モードで **spanning-tree mst cost** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst instance-id cost cost
no spanning-tree mst instance-id cost

構文の説明

instance-id スパンニングツリーインスタンス範囲。指定できる範囲は1～4094です。

cost パス コスト。指定できる範囲は1～200000000です。

コマンド デフォルト

デフォルトパス コストは、インターフェイスの帯域幅設定から計算されます。デフォルトパス コストは次のとおりです。

- 1 Gb/s : 20000
- 100 Mb/s : 200000
- 10 Mb/s : 2000000

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

引数 *cost* の値を指定する場合、値が大きいほどコストは高くなります。

例

次の例では、MST インスタンス 2 および 4 に対応するインターフェイスのパス コストを 50 に設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree mst 2,4 cost 250
```

spanning-tree mst forward-time

転送遅延タイマーを MST インスタンスに設定するには、グローバル コンフィギュレーション モードで **spanning-tree mst forward-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst forward-time seconds
no spanning-tree mst forward-time

構文の説明

seconds すべての MST インスタンスに設定される転送遅延タイマーの秒数。範囲は 4 ～ 30 です。

コマンド デフォルト

デフォルトは 15 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、すべての MST インスタンスに転送遅延タイマーを設定する方法を示します。

```
Device(config)# spanning-tree mst forward-time 20
```

spanning-tree mst hello-time

hello タイム遅延タイマーを設定するには、グローバル コンフィギュレーション モードで **spanning-tree mst hello-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst hello-time seconds
no spanning-tree mst hello-time

構文の説明

seconds hello BPDUの間隔 (秒数)。指定できる範囲は1～10です。

コマンド デフォルト

デフォルトは2です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

hello-time 値を指定しない場合は、ネットワーク直径から値が計算されます。

このコマンドの使用には注意してください。多くの場合、**spanning-tree vlan *vlan-id* root primary** および **spanning-tree vlan *vlan-id* root secondary** 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、Hello タイムを変更することを推奨します。

例

次に、hello タイム遅延タイマーを3秒に設定する例を示します。

```
Device(config)# spanning-tree mst hello-time 3
```

spanning-tree mst max-age

スパニングツリーがルートスイッチからメッセージを受信する間隔を設定するには、グローバルコンフィギュレーションモードで **spanning-tree mst max-age** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-age seconds
no spanning-tree mst max-age

構文の説明

seconds スパニングツリーがルートスイッチからメッセージを受信する間隔（秒単位）です。指定できる範囲は 6 ~ 40 です。

コマンド デフォルト

デフォルトは 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、**max-age** タイマーを 40 秒に設定する方法を示します。

```
Device(config)# spanning-tree mst max-age 40
```


spanning-tree mst max-hops

ブリッジプロトコルデータユニット（BPDU）が廃棄されるまでの領域内の最大ホップ数を指定するには、グローバルコンフィギュレーションモードで **spanning-tree mst max-hops** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-hops *hop-count*
no spanning-tree mst max-hops

構文の説明	<i>hop-count</i> BPDU が廃棄されるまでに領域内で可能なホップ数。指定できる範囲は 1 ～ 255 です。
-------	-----------------------------------------------------------------

コマンドデフォルト	デフォルトは 20 です。
-----------	---------------

コマンドモード	グローバル コンフィギュレーション
---------	-------------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、許容されるホップ数を 25 に設定する例を示します。

```
Device(config)# spanning-tree mst max-hops 25
```

spanning-tree mst port-priority

インターフェイスのプライオリティを設定するには、インターフェイスコンフィギュレーションモードで **spanning-tree mst port-priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree mst instance-id port-priority priority
no spanning-tree mst instance-id port-priority
```

構文の説明

instance-id スパニングツリーインスタンス範囲。指定できる範囲は1～4094です。

priority プライオリティ。指定できる範囲は0～240で、16ずつ増加します。

コマンド デフォルト

デフォルト値は128です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てるができます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、Multiple Spanning-Tree (MST) はインターフェイス番号が最小のインターフェイスをフォワーディングステートにし、他のインターフェイスをブロックします。

スイッチがスイッチスタックのメンバである場合、**spanning-tree mst *instance_id* cost *cost*** コマンドを使用して、フォワーディングステートにするインターフェイスを選択する必要があります。

例

次の例では、ループが発生した場合に、スパニングツリー インスタンス 20 および 22 に対応するインターフェイスがフォワーディングステートになる可能性を高める方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree mst 20,24 port-priority 0
```

spanning-tree mst pre-standard

先行標準のブリッジプロトコルデータユニット（BPDU）だけを送信するようにポートを設定するには、インターフェイスコンフィギュレーションモードで **spanning-tree mst pre-standard** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst pre-standard
no spanning-tree mst pre-standard

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトでは、先行標準ネイバーを自動的に検出します。

コマンドモード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ポートでは、先行標準と標準の両方の BPDU を受け入れることができます。ネイバータイプが不一致の場合、Common and Internal Spanning Tree（CIST）だけがこのインターフェイスで実行されます。



- (注) スイッチポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** インターフェイスコンフィギュレーションコマンドを使用する必要があります。先行標準 BPDU だけを送信するようにポートを設定していない場合、Multiple STP（MSTP）のパフォーマンスが低下することがあります。

自動的に先行標準ネイバーを検出するようにポートが設定されている場合、**show spanning-tree mst** コマンドに **prestandard** フラグが常に表示されます。

例

次に、先行標準 BPDU だけを送信するようにポートを設定する例を示します。

```
Device(config-if)# spanning-tree mst pre-standard
```

spanning-tree mst priority

インスタンスのブリッジプライオリティを設定するには、グローバルコンフィギュレーションモードで **spanning-tree mst priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance* priority *priority*
no spanning-tree mst priority

構文の説明

instance インスタンス ID 番号。指定できる範囲は 0 ~ 4094 です。

priority *priority* ブリッジプライオリティを指定します。指定できる範囲は 0 ~ 614440 で、4096 ずつ増加します。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ブリッジプライオリティは、4096 ずつ増分して設定できます。有効な値は 0、4096、8192、12288、16384、20480、24576、28672、32768、40960、45056、49152、53248、57344 および 61440 です。

instance は、単一インスタンスまたはインスタンス範囲 (0 ~ 3、5、7 ~ 9 など) として入力できます。

例

次に、MST インスタンスのスパニングツリー プライオリティを 0 から 4096 に設定する例を示します。

```
Device(config)# spanning-tree mst 0 priority 4096
```

spanning-tree mst root

インスタンスのプライマリルートスイッチおよびセカンダリルートスイッチを指定し、タイマー値を設定するには、グローバル コンフィギュレーション モードで **spanning-tree mst root** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst instance root {primary | secondary}

no spanning-tree mst instance root

構文の説明	
<i>instance</i>	インスタンス ID 番号。指定できる範囲は 0 ~ 4094 です。
primary	このスイッチを強制的にルートスイッチに設定します。
secondary	プライマリ ルートに障害が発生した場合に、このスイッチがルートスイッチとして機能するように指定します。

コマンドデフォルト なし

コマンドモード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、バックボーンスイッチ上だけで使用します。*instance-id* は、単一インスタンスまたはインスタンス範囲 (0 ~ 3、5、7 ~ 9 など) として入力できます。

spanning-tree mst instance-id root コマンドを入力すると、ソフトウェアはこのスイッチをスパンニングツリーインスタンスのルートに設定するのに十分なプライオリティを設定しようとし、拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチプライオリティを 24576 に設定します (この値によってこのスイッチが指定されたインスタンスのルートになる場合)。指定されたインスタンスのルートスイッチに、24576 に満たないスイッチプライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチプライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビットスイッチプライオリティの最下位ビットの値です)。

spanning-tree mst instance-id root secondary コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアはスイッチプライオリティをデフォルト値 (32768) から 28672 に変更します。ルートスイッチに障害が発生した場合は、このスイッチが次のルートスイッチになります (ネットワーク内の他のスイッチがデフォルトのスイッチプライオリティである 32768 を使用しているため、ルートスイッチになる可能性が低い場合)。

例

次の例は、インスタンス 10 のルートスイッチとしてスイッチを設定する方法を示しています。

```
Device(config)# spanning-tree mst 10 root primary
```

spanning-tree mst simulate pvst (グローバル コンフィギュレーション)

PVST+ シミュレーションをグローバルにイネーブルにするには、**spanning-tree mst simulate pvst global** コマンドを使用します。この設定はデフォルトでイネーブルになっています。PVST+ シミュレーション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。

spanning-tree mst simulate pvst global
no spanning-tree mst simulate pvst global

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

PVST+ シミュレーションは、デフォルトでイネーブルになっています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドがサポートされるようになりました。

使用上のガイドライン

この機能は、(同一リージョン内の) MST スイッチが PVST+ スイッチとシームレスに対話するように設定します。この機能がイネーブルになっているかどうかを確認するには、**show spanning-tree summary** コマンドを使用します。

ポート上で PVST+ シミュレーションをイネーブルにするには、**spanning-tree mst simulate pvst (interface configuration)** を参照してください。

例

次に、MSTP モードで PVST+ シミュレーションがイネーブルな場合のスパニングツリーの概要の例を示します。

```
Device# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled
Name Blocking Listening Learning Forwarding STP Active
-----
MST0 2 0 0 0 2
```

```
-----  
1 mst 2 0 0 0 2
```

次に、スイッチが MSTP モードでない、つまりスイッチが PVST または Rapid PVST モードの場合のスパニングツリーの概要の例を示します。出力文字列は現在の STP モードを表示します。

```
Device# show spanning-tree summary  
Switch is in rapid-pvst mode  
Root bridge for: VLAN0001, VLAN2001-VLAN2002  
EtherChannel misconfig guard is enabled  
Extended system ID is enabled  
Portfast Default is disabled  
PortFast BPDU Guard Default is disabled  
Portfast BPDU Filter Default is disabled  
Loopguard Default is disabled  
UplinkFast is disabled  
BackboneFast is disabled  
Pathcost method used is short  
PVST Simulation Default is enabled but inactive in rapid-pvst mode  
Name Blocking Listening Learning Forwarding STP Active  
-----  
VLAN0001 2 0 0 0 2  
VLAN2001 2 0 0 0 2  
VLAN2002 2 0 0 0 2  
-----  
3 vlans 6 0 0 0 6
```


spanning-tree mst simulate pvst (インターフェイス コンフィギュレーション)

任意のポートでPVST+シミュレーションをイネーブルにするには、インターフェイスコンフィギュレーションモードで **spanning-tree mst simulate pvst** コマンドを使用します。この設定はデフォルトでイネーブルになっています。PVST+シミュレーションをディセーブルにするには、このコマンドの **no** 形式を使用するか、または **spanning-tree mst simulate pvst disable** コマンドを入力します。

spanning-tree mst simulate pvst [disable]
no spanning-tree mst simulate pvst

構文の説明	disable PVST+シミュレーション機能をディセーブルにします。このコマンドを実行すると、ポートは Rapid PVST+ を実行している接続先デバイスと自動的に相互運用できなくなります。				
コマンドデフォルト	PVST+シミュレーションは、デフォルトでイネーブルになっています。				
コマンドモード	インターフェイス コンフィギュレーションモード				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.2(7)E3k</td> <td>このコマンドがサポートされるようになりました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドがサポートされるようになりました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドがサポートされるようになりました。				
使用上のガイドライン	<p>この機能は、(同一リージョン内の) MST スイッチが PVST+ スイッチとシームレスに対話するように設定します。この機能がイネーブルになっているかどうかを確認するには、show spanning-tree interface interface-id detail コマンドを使用します。</p> <p>PVST+シミュレーションをグローバルにイネーブルにするには、spanning-tree mst simulate pvst global を参照してください。</p>				

例

次の例に、PVST+シミュレーションがポートで明示的にイネーブルになっている場合のインターフェイスの詳細情報を示します。

```
Device# show spanning-tree interface gi3/13 detail
Port 269 (GigabitEthernet3/13) of VLAN0002 is forwarding
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
```

```
PVST Simulation is enabled  
BPDU: sent 132, received 1
```

次の例に、PVST+シミュレーション機能がポートでディセーブルになっており、PVSTピアが不整合になっている場合のインターフェイスの詳細情報を示します。

```
Device# show spanning-tree interface gi3/13 detail  
Port 269 (GigabitEthernet3/13) of VLAN0002 is broken (PVST Peer Inconsistent)  
Port path cost 4, Port priority 128, Port Identifier 128.297.  
Designated root has priority 32769, address 0013.5f20.01c0  
Designated bridge has priority 32769, address 0013.5f20.01c0  
Designated port id is 128.297, designated path cost 0  
Timers: message age 0, forward delay 0, hold 0  
Number of transitions to forwarding state: 1  
Link type is point-to-point by default  
PVST Simulation is disabled  
BPDU: sent 132, received 1
```

spanning-tree pathcost method

デフォルトのパスコスト計算方式を設定するには、グローバル コンフィギュレーション モードで **spanning-tree pathcost method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree pathcost method {long | short}
no spanning-tree pathcost method

構文の説明

long デフォルト ポート パス コスト用の 32 ビット ベース値を指定します。

short デフォルト ポート パス コスト用の 16 ビット ベース値を指定します。

コマンド デフォルト

short

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

long パスコスト計算方式では、パスコスト計算に 32 ビットをすべて利用して、1 ~ 200000000 の値を生成します。

short パスコスト計算方式 (16 ビット) では、1 ~ 65535 の値を生成します。

例

次に、デフォルトのパス コスト計算方式を **long** に設定する例を示します。

```
Device(config)#spanning-tree pathcost method long
```

次に、デフォルトのパス コスト計算方式を **short** に設定する例を示します。

```
Device(config)#spanning-tree pathcost method short
```

spanning-tree mst port-priority

インターフェイスのプライオリティを設定するには、インターフェイスコンフィギュレーションモードで **spanning-tree mst port-priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* port-priority *priority*
no spanning-tree mst *instance-id* port-priority

構文の説明

instance-id スパニングツリーインスタンス範囲。指定できる範囲は1～4094です。

priority プライオリティ。指定できる範囲は0～240で、16ずつ増加します。

コマンド デフォルト

デフォルト値は128です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てるができます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、Multiple Spanning-Tree (MST) はインターフェイス番号が最小のインターフェイスをフォワーディングステートにし、他のインターフェイスをブロックします。

スイッチがスイッチスタックのメンバである場合、**spanning-tree mst *instance-id* cost *cost*** コマンドを使用して、フォワーディングステートにするインターフェイスを選択する必要があります。

例

次の例では、ループが発生した場合に、スパニングツリーインスタンス 20 および 22 に対応するインターフェイスがフォワーディングステートになる可能性を高める方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# spanning-tree mst 20,24 port-priority 0
```

spanning-tree portfast edge (グローバル コンフィギュレーション)

PortFast エッジ対応インターフェイスでブリッジプロトコルデータユニット (BPDU) フィルタリングをイネーブルにする場合、PortFast エッジ対応インターフェイスで BPDU ガード機能をイネーブルにする場合、またはすべての非トランキングインターフェイス上で PortFast エッジ機能をイネーブルにする場合は、グローバルコンフィギュレーションモードで **spanning-tree portfast edge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree portfast edge {bpdupfilter default | bpduguard default | default}
no portfast edge {bpdupfilter default | bpduguard default | default}
```

構文の説明

bpdupfilter default	PortFast エッジ対応インターフェイス上で BPDU フィルタリングをイネーブルにし、エンドステーションに接続されたスイッチインターフェイスでの BPDU の送受信を禁止します。
bpduguard default	PortFast エッジ対応インターフェイス上で BPDU ガード機能をイネーブルにし、BPDU を受信する PortFast エッジ対応インターフェイスを error-disabled ステートにします。
default	すべての非トランキング インターフェイス上で PortFast エッジ機能をグローバルにイネーブルにします。

コマンドデフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid-PVST+ モード、または Multiple Spanning-Tree (MST) モードで稼働している場合は、これらの機能をイネーブルにできません。

PortFast エッジ対応インターフェイス (PortFast エッジ動作ステートのインターフェイス) 上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast edge bpdupfilter default** 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。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。PortFast エッジ対応インターフェイスでは、BPDU

を受信すると、PortFast エッジ動作ステートが解除され、BPDU フィルタリングがディセーブルになります。

spanning-tree portfast edge bpdudfilter default コマンドは、**spanning-tree portfast edge bpdudfilter** インターフェイスコマンドを使用して上書きできます。



注意

このコマンドを使用するときは注意してください。BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

PortFast エッジ動作ステートのインターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast edge bpduguard default** 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。有効な設定では、PortFast エッジ対応インターフェイスは BPDU を受信しません。PortFast エッジ対応インターフェイスが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは **error-disabled** ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

spanning-tree portfast edge bpduguard default コマンドは、**spanning-tree portfast edge bpduguard** インターフェイスコマンドを使用して上書きできます。

すべての非トランクインターフェイス上で PortFast エッジ機能をグローバルにイネーブルにするには、**spanning-tree portfast edge default** コマンドを使用します。PortFast エッジは、エンドステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポロジループが原因でデータの packets ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。リンクが確立すると、PortFast エッジ対応インターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディングステートに移行します。

spanning-tree portfast edge default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast edge** インターフェイス コンフィギュレーション コマンドを使用します。**no spanning-tree portfast edge default** グローバル コンフィギュレーション コマンドを使用すると、**spanning-tree portfast edge** 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個別に設定した場合を除き、すべてのインターフェイス上で PortFast エッジをディセーブルにできます。

グローバル コンフィギュレーション モードで **spanning-tree portfast [trunk]** コマンドを入力すると、システムは自動的に **spanning-tree portfast edge [trunk]** として保存します。

次の例では、BPDU フィルタリングをデフォルトでグローバルにイネーブルにする方法を示します。

```
Device(config)# spanning-tree portfast edge bpdudfilter default
```

次の例では、BPDU ガード機能をデフォルトでグローバルにイネーブルにする方法を示します。

```
Device(config)# spanning-tree portfast edge bpduguard default
```

次の例では、すべての非ランキング インターフェイス上で PortFast 機能をグローバルにイネーブルにする方法を示します。

```
Device(config)# spanning-tree portfast edge default
```

spanning-tree portfast edge (インターフェイス コンフィギュレーション)

リンクがアップした時点で、インターフェイスがタイマーの経過を待たずにただちにフォワーディングステートに移行した場合に、PortFast エッジモードをイネーブルにするには、インターフェイス コンフィギュレーションモードで **spanning-tree portfast edge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast edge [{disable | trunk}]
no spanning-tree portfast edge

構文の説明

disable (任意) インターフェイス上で PortFast エッジをディセーブルにします。

trunk (任意) インターフェイス上で PortFast エッジモードをイネーブルにします。

コマンド デフォルト

spanning-tree portfast edge default コマンドによって設定される設定値

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus (PVST+) モード、Rapid PVST+ モード、またはマルチ スパニングツリー (MST) モードで稼働している場合は、その機能をイネーブルにできません。

この機能はインターフェイス上のすべての VLAN に影響します。

このコマンドは、端末に接続されているインターフェイスでのみ使用してください。そうでない場合、予想外のトポジグループが原因でデータパケット ループが発生し、スイッチおよびネットワークの動作が中断する可能性があります。

トランクポートで PortFast エッジをイネーブルにするには、**spanning-tree portfast edge trunk** インターフェイス コンフィギュレーションコマンドを使用する必要があります。**spanning-tree portfast edge** コマンドは、トランクポートではサポートされません。

PortFast エッジ機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行します。

spanning-tree portfast edge default グローバルコンフィギュレーションコマンドを使用すると、すべての非トランクインターフェイス上で PortFast エッジ機能をグローバルにイネーブルにできます。**spanning-tree portfast edge** インターフェイス コンフィギュレーション コマンドは、グローバル設定を上書きするために使用します。

spanning-tree portfast edge default グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast edge disable** 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、トランクインターフェイス以外のインターフェイス上で PortFast エッジ機能をディセーブルにできます。

グローバル コンフィギュレーション モードで **spanning-tree portfast [trunk]** コマンドを入力すると、システムは自動的に **spanning-tree portfast edge [trunk]** として保存します。

例

次の例では、ポート上で PortFast エッジ機能をイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)#spanning-tree portfast edge
```

spanning-tree transmit hold-count

送信ホールドカウントを指定するには、グローバル コンフィギュレーション モードで **spanning-tree transmit hold-count** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count

構文の説明

value 毎秒送信されるブリッジプロトコルデータユニット (BPDU) の数。範囲は 1 ~ 20 です。

コマンド デフォルト

デフォルト値は 6 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべてのスパンニングツリー モードでサポートされています。送信ホールド カウントは、一時停止するまで 1 秒間に送信される BPDU の数を決定します。



- (注) 特に Rapid Per-VLAN Spanning Tree (PVST+) モードの場合、送信ホールド カウント値を増やすと、CPU 使用率に重大な影響を与える可能性があります。この値を減らすと、コンバージェンスの速度が低下します。デフォルト設定を使用することを推奨します。

例

次の例では、送信ホールド カウントを 8 に指定する方法を示します。

```
Device(config)# spanning-tree transmit hold-count 8
```

spanning-tree uplinkfast

UplinkFast をイネーブルにするには、グローバルコンフィギュレーションモードで **spanning-tree uplinkfast** コマンドを使用します。UplinkFast 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。

spanning-tree uplinkfast [**max-update-rate** *packets-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

構文の説明

max-update-rate (任意) 更新パケット送信時の送信速度 (1秒あたりのパケット数) を指定します。指定できる範囲は 0 ~ 320000 です。
デフォルト値は 150 です。

コマンド デフォルト

UplinkFast はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、アクセス スイッチ上だけで使用します。

UplinkFast 機能は、Rapid PVST+ モードまたは Multiple Spanning-Tree (MST) モードで設定できますが、Spanning Tree モードを PVST+ に変更するまでこの機能はディセーブル (非アクティブ) のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになります。VLAN 単位でイネーブルにすることはできません。

UplinkFast をイネーブルまたはディセーブルにすると、すべての非スタック ポートのインターフェイス上で、Cross-Stack UplinkFast (CSUF) も自動的にイネーブルまたはディセーブルになります。CSUF は、リンクやスイッチに障害が発生した場合、または Spanning Tree が自動的に再設定された場合に、新しいルート ポートを短時間で選択できるようにします。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチプライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上の値に変更した場合、パス コストは変更されません)。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

ルートポートに障害が発生していることがスパンニングツリーで検出されると、UplinkFastはスイッチをただちに代替ルートポートに変更して、新しいルートポートを直接フォワーディングステートに移行させます。この間、トポロジ変更通知が送信されます。

UplinkFast機能で使用するインターフェイスでは、ルートガードをイネーブルにしないでください。UplinkFastを使用すると、障害発生時に（ブロックステートの）バックアップインターフェイスがルートポートになります。しかし、同時にルートガードもイネーブルになっていた場合は、UplinkFast機能で使用するすべてのバックアップインターフェイスがroot-inconsistent（ブロック）ステートになり、フォワーディングステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパンニングツリー トポロジのコンバージェンスに要する時間が長くなります。

例

次の例では、UplinkFast をイネーブルにして、最大速度を 200 パケット/秒に設定する方法を示します。

```
Device(config)# spanning-tree uplinkfast max-update-rate 200
```

spanning-tree vlan

仮想LAN (VLAN) 単位でスパニングツリープロトコル (STP) を設定するには、グローバルコンフィギュレーションモードで **spanning-tree vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
spanning-tree vlan vlan-id [{forward-time seconds | hello-time seconds | max-age seconds |
priority priority | [root {primary | secondary} [diameter net-diameter]}]
no spanning-tree vlan vlan-id [{forward-time | hello-time | max-age | priority | root}]
```

構文の説明

<i>vlan-id</i>	スパニングツリーインスタンスに対応するVLAN範囲です。範囲は1～4094です。
forward-time <i>seconds</i>	(任意) STP 転送遅延時間を秒単位で設定します。指定できる範囲は4～30です。 デフォルトは15です。
hello-time <i>seconds</i>	(任意) ルートスイッチが設定メッセージを生成する間隔を秒単位で指定します。指定できる範囲は1～10です。 デフォルトは2です。
max-age <i>seconds</i>	(任意) ブリッジパケットデータユニット (BPDU) で情報が有効な最大秒数を指定します。指定できる範囲は6～40です。 デフォルトは20です。
priority <i>priority</i>	(任意) STP ブリッジプライオリティを設定します。指定できる範囲は0～61440で、4096ずつ増加します。 プライマリ ルートスイッチのデフォルトは24576です。 セカンダリ ルートスイッチのデフォルトは28672です。
root primary	(任意) このスイッチを強制的にルートスイッチに設定します。
root secondary	(任意) プライマリ ルートに障害が発生した場合に、このスイッチがルートスイッチとして機能するように指定します。
diameter <i>net -diameter</i>	(任意) 端末の2つの接続ポイントの間に存在するスイッチの最大数を指定します。指定できる範囲は2～7です。

コマンド デフォルト

すべてのVLANでスパニングツリーがイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スイッチが **max-age seconds- value** で指定された時間内に BPDU を受信しなかった場合、スパニングツリートポロジが再計算されます。

spanning-tree vlan vlan-id root は、バックボーンスイッチのみで使用してください。

spanning-tree vlan vlan-id root secondary コマンドを使用すると、このスイッチのプライオリティが 32768 から 28672 に変更されます。ルートスイッチに障害が発生した場合は、このスイッチが次のルートスイッチになります。



注意 物理的なループの存在しないトポロジーであっても、スパニングツリーをディセーブルにすることは推奨しません。スパニングツリーは誤設定やケーブル障害を防ぐ役割を果たします。VLAN に物理ループが存在しないことを確認せずに、VLAN でスパニングツリーをディセーブルにしないでください。

例

次に、VLAN 200 でスパニングツリーをイネーブルにする例を示します。

```
Device(config)# spanning-tree vlan 200
```

次に、スイッチを VLAN 10 のルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Device(config)# spanning-tree vlan 10 root primary diameter 4
```

次に、スイッチを VLAN 10 のセカンダリルートスイッチとして設定し、ネットワーク直径を 4 に設定する例を示します。

```
Device(config)# spanning-tree vlan 10 root secondary diameter 4
```

switchport access vlan

ポートをスタティック アクセス ポートとして設定するには、インターフェイス コンフィギュレーションモードで **switchport access vlan** コマンドを使用します。アクセスモードをデフォルトの VLAN モードにリセットするには、このコマンドの **no** 形式を使用します。

```
switchport access vlan {vlan-id }
no switchport access vlan
```

構文の説明	<i>vlan-id</i> (任意) アクセスモードにあるインターフェイス上の VLAN の番号。有効な値は 1 ~ 4094 です。
コマンド デフォルト	デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。 ダイナミック アクセス ポートは、最初は何の VLAN のメンバにも属さず、受信したパケットに基づいて割り当てを受信します。
コマンド モード	インターフェイス コンフィギュレーションモード
コマンド履歴	リリース 変更内容 Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

使用上のガイドライン **switchport access vlan** コマンドを有効にするには、事前にポートをアクセスモードにする必要があります。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。**access vlan dynamic** として設定されている場合、ポートは受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

no switchport access コマンドを使用すると、アクセスモード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

例

次の例では、最初に VLANID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセスモードにあるインターフェイス上の VLAN を設定します (名前を使用)。設定を確認するには、特権 EXEC コマンドで **show interfaces interface-id switchport** を入力して、Access Mode VLAN : 行の情報を調べます。

手順 1 : VLAN データベースでのエントリの作成

```
Device# configure terminal
Device(config)# vlan 33
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

手順 2 : VLAN データベースの確認

```

Device # show vlan id 33
VLAN Name      Status Ports
-----
33    test       active
-----

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
33    enet    100033   1500   -     -     -     -     -     0     0

Remote SPAN VLAN
-----
Disabled

Primary  Secondary Type          Ports
-----

```

手順 3 : インターフェイス上の VLAN の設定 (vlan_name 「test」 を使用)

```

Device # configure terminal
Device(config)# interface GigabitEthernet5/1
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan name test
Device(config-if)# end
Device#

```

手順 4 : 実行コンフィギュレーションの確認

```

Device # show running-config interface GigabitEthernet5/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet5/1
switchport access vlan 33
switchport mode access
Switch#

```

手順 5 : インターフェイスのスイッチ ポートで設定を確認

```

Device # show interface GigabitEthernet5/1 switchport
Name: Gi5/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: None
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled

```



```
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

switchport mode

ポートの VLAN メンバーシップモードを設定するには、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用します。モードをデバイスに適したデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

```
switchport mode {access | dynamic | {auto | desirable} | trunk}
noswitchport mode {access | dynamic | {auto | desirable} | trunk}
```

構文の説明

access	ポートをアクセス モードに設定します (switchport access vlan インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか)。ポートは無条件にアクセスするように設定され、非カプセル化 (タグなし) フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。
dynamic auto	ポート トランキング モードのダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	ポート トランキング モードのダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
trunk	ポートを無条件にトランクに設定します。ポートはトランキング VLAN レイヤ 2 インターフェイスです。ポートは、送信元の VLAN を識別するカプセル化 (タグ付き) フレームを送受信します。トランクは、2 つのスイッチ間、またはスイッチとルータ間のポイントツーポイント リンクです。

コマンド デフォルト デフォルト モードは **dynamic auto** です。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して適切なモードでポートを設定した場合のみです。スタティック アクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定だけです。

access モードを開始すると、インターフェイスは永続的な非トランキングモードになり、隣接インターフェイスがリンクから非トランクリンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始すると、インターフェイスは永続的なトランキングモードになり、接続先のインターフェイスがリンクからトランクリンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを開始すると、隣接インターフェイスが **trunk** または **desirable** モードに設定された場合に、インターフェイスはリンクをトランクリンクに変換します。

dynamic desirable モードを開始すると、隣接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定された場合に、インターフェイスはトランクインターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキングプロトコル (VTP) ドメインに存在する必要があります。トランクネゴシエーションは、ポイントツーポイントプロトコルである **Dynamic Trunking Protocol (DTP)** によって管理されます。ただし、一部のインターネットワーキングデバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この問題を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定し、DTP をオフにします。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** 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、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセスポートとトランクポートは、互いに排他的な関係にあります。

IEEE 802.1X 機能は、次の方法でスイッチポートモードに作用します。

- トランクポートで IEEE 802.1X をイネーブルにしようとする、エラーメッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードをトランクに変更しようとしても、ポートモードは変更されません。
- ポート設定で IEEE 802.1X を **dynamic auto** または **dynamic desirable** にイネーブルにしようとする、エラーメッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポートモードは変更されません。
- ダイナミックアクセス (VLAN Query Protocol (VQP)) ポートで IEEE 802.1X をイネーブルにしようとする、エラーメッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラーメッセージが表示され、VLAN 設定は変更されません。

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力して、*Administrative Mode* 行と *Operational Mode* 行の情報を調べます。

例

次の例では、ポートをアクセスモードに設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1  
Device(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1  
Device(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1  
Device(config-if)# switchport mode trunk
```

switchport nonegotiate

ダイナミック トランキング プロトコル (DTP) ネゴシエーション パケットがレイヤ2 インターフェイス上で送信されないように指定するには、インターフェイス コンフィギュレーション モードで **switchport nonegotiate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate
no switchport nonegotiate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

no switchport nonegotiate コマンドは **nonegotiate** ステータスを解除します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセスまたはトランク (**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定) の場合だけです。dynamic (auto または desirable) モードでこのコマンドを実行しようとする、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスがトランキングを実行するかどうかは、**mode** パラメータ (**access** または **trunk.**) によって決まります。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** 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、トランキングをディセーブルにします。
- DTP をサポートしていないデバイス上のトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

次の例では、ポートに対してトランキングモードのネゴシエートを制限し、（モードの設定に応じて）トランクポートまたはアクセスポートとして動作させる方法を示します。

```
Device(config)# interface gigabitethernet2/0/1  
Device(config-if)# switchport nonegotiate
```

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力します。

udld

単方向リンク検出 (UDLD) で、アグレッシブモードまたは通常モードをイネーブルにし、設定可能なメッセージタイマーの時間を設定するには、グローバルコンフィギュレーションモードで **udld** コマンドを使用します。すべての光ファイバポート上でアグレッシブモード UDLD または通常モード UDLD 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。

```
udld {aggressive|enable|message time message-timer-interval}
no udld {aggressive|enable|message}
```

構文の説明

aggressive	すべての光ファイバインターフェイスにおいて、アグレッシブモードで UDLD をイネーブルにします。
enable	すべての光ファイバインターフェイスにおいて、通常モードで UDLD をイネーブルにします。
message time <i>message-timer-interval</i>	アダプタイズメントフェーズにあり、双方向と判別されたポートにおける UDLD プローブメッセージ間の時間間隔を設定します。指定できる範囲は 1 ~ 90 秒です。デフォルトは 15 秒です。

コマンドデフォルト

すべてのインターフェイスで UDLD はディセーブルです。
メッセージタイマーは 15 秒に設定されます。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

UDLD は、2 つの動作モードをサポートしています。通常 (デフォルト) とアグレッシブです。ノーマルモードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブモードでは、UDLD はまた、光ファイバおよびツイストペアリンクの単一方向トラフィックによる単一方向リンク、および光ファイバリンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。プローブパケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷との折り返いをつけることとなります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバインターフェイスだけです。他のインターフェイスタイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーションコマンドを使用します。

次のコマンドを使用して、UDLD によってシャットダウンされたインターフェイスをリセットできます。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **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 モード コマンド。
- **no udld enable** グローバルコンフィギュレーションコマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** 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：指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval interval** グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

次の例では、すべての光ファイバインターフェイスでUDLDをイネーブルにする方法を示します。

```
Device(config)# udld enable
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

udld port

個々のインターフェイスで単方向リンク検出 (UDLD) をイネーブルにするか、または光ファイバインターフェイスが **udld** グローバルコンフィギュレーション コマンドによってイネーブルになるのを防ぐには、インターフェイス コンフィギュレーション モードで **udld port** コマンドを使用します。 **udld** グローバル コンフィギュレーション コマンド設定に戻すか、または非光ファイバポートで入力された場合に UDLD 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。

udld port [aggressive]

no udld port [aggressive]

構文の説明

aggressive (任意) 指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

コマンド デフォルト

光ファイバインターフェイスでは、UDLD はディセーブルになっていますが、光ファイバインターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに応じて UDLD をイネーブルにします。

非光ファイバインターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

UDLD 対応ポートが別のデバイスの UDLD 非対応ポートに接続されている場合、このポートは単方向リンクを検出できません。

UDLD は、2つの動作モードをサポートしています。通常 (デフォルト) とアグレッシブです。ノーマルモードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペアリンクの単方向トラフィックによる単方向リンク、および光ファイバリンクにおいて誤って接続されたインターフェイスによる単方向リンクを検出します。

UDLD を通常モードでイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。UDLD をアグレッシブモードでイネーブルにするには、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を上書きする場合は、光ファイバポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no** 形式を使用します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **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 モード コマンド。
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** 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：指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval interval** グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定に関係なく、光ファイバインターフェイス上で UDLD をディセーブルにする方法を示します。

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld interface** 特権 EXEC コマンドを入力します。

udld reset

単方向リンク検出 (UDLD) によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、特権 EXEC モードで **udld reset** コマンドを使用します (イネーブルの場合には、スパニングツリー、ポート集約プロトコル (PAgP)、ダイナミック トランッキング プロトコル (DTP) などの他の機能を介することで有効になります)。

udld reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

なし

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの設定で、UDLD がまだイネーブルである場合、これらのポートは再び UDLD の稼働を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

次の例では、UDLD によってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
Device# udld reset
1 ports shutdown by UDLD were reset.
```




第 III 部

ネットワーク管理

- [ネットワーク管理](#) (227 ページ)



ネットワーク管理

- [monitor session destination](#) (228 ページ)
- [monitor session source](#) (233 ページ)
- [show monitor](#) (236 ページ)
- [snmp-server enable traps](#) (239 ページ)
- [snmp-server enable traps bridge](#) (242 ページ)
- [snmp-server enable traps cpu](#) (243 ページ)
- [snmp-server enable traps envmon](#) (244 ページ)
- [snmp-server enable traps errdisable](#) (245 ページ)
- [snmp-server enable traps flash](#) (246 ページ)
- [snmp-server enable traps mac-notification](#) (247 ページ)
- [snmp-server enable traps port-security](#) (248 ページ)
- [snmp-server enable traps rtr](#) (249 ページ)
- [snmp-server enable traps snmp](#) (251 ページ)
- [snmp-server enable snmp traps storm-control](#) (252 ページ)
- [snmp-server enable traps stpx](#) (253 ページ)

monitor session destination

新規にスイッチドポートアナライザ (SPAN) セッションまたはリモート SPAN (RSPAN) 宛先セッションを開始し、ネットワークセキュリティ デバイス (Cisco IDS Sensor アプライアンスなど) の宛先ポート上の入力トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session destination** 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。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session-number destination { interface interface-id [, | -] [
encapsulation { replicate | dot1q } ] { ingress [ dot1q | untagged ] } | { remote
} vlan vlan-id
no monitor session session-number destination { interface interface-id [, | -] [
encapsulation { replicate | dot1q } ] { ingress [ dot1q | untagged ] } | { remote
} vlan vlan-id
```

構文の説明

<i>session-number</i>	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 68 です。
interface <i>interface-id</i>	SPAN または RSPAN セッションの宛先または送信元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 (タイプ、スタック メンバ、モジュール、ポート番号を含む) です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイスタイプであり、指定できる範囲は 1 ～ 128 です。
,	(任意) 複数のインターフェイスまたは VLAN を指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	(任意) インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。

encapsulation replicate	<p>(任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。</p> <p>次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。encapsulation オプションは、no 形式では無視されます。</p>
encapsulation dot1q	<p>(任意) 宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。</p> <p>次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。encapsulation オプションは、no 形式では無視されます。</p>
ingress	入力トラフィック転送をイネーブルにします。
dot1q	(任意) 指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。
untagged	(任意) 指定された VLAN をデフォルト VLAN として、タグなしカプセル化された着信パケットを受け入れます。
isl	ISL カプセル化を使用して入力トラフィックを転送するように指定します。
remote	<p>RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ~ 1001 または 1006 ~ 4094 です。</p> <p>RSPAN VLAN は VLAN 1 (デフォルトの VLAN)、または VLAN ID 1002 ~ 1005 (トークンリングおよび FDDI VLAN に予約済) になることはできません。</p>
vlan <i>vlan-id</i>	ingress キーワードとのみ使用された場合、入力トラフィックに対するデフォルトの VLAN を設定します。

コマンド デフォルト モニタセッションは設定されていません。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

all、**local**、**range session-range**、または **remote** を **no monitor session** コマンドに指定することで、すべての SPAN および RSPAN、すべてのローカル SPAN、範囲または、すべての RSPAN セッションをクリアできます。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 4つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチスタック上で、合計 68 の SPAN および RSPAN セッションを保有できます。

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチスタック上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN (VSPAN) を使用して、VLAN または一連の VLAN 内のネットワークトラフィックを解析する場合、送信元 VLAN のすべてのアクティブポートが SPAN または RSPAN セッションの送信元ポートになります。トランクポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1つのポート、1つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,]- オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ (,) の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン (-) の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1X 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1X 認証はディセーブルです。IEEE 802.1X 認証がポート上で使用できない場合、スイッチはエラーメッセージを返しません。SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができません。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- **monitor session session_number destination interface interface-id** を他のキーワードなしで入力すると、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session session_number destination interface interface-id ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります。
- **monitor session session_number destination interface interface-id encapsulation replicate** を他のキーワードなしで入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力転送はイネーブルになりません（これはローカル SPAN だけに適用しません。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session session_number destination interface interface-id encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet2/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

monitor session source

スイッチドポートアナライザ (SPAN) セッションまたはリモート SPAN (RSPAN) 送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスまたは VLAN を追加または削除するには、**monitor session source** 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。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

```
monitor session session_number source { interface interface-id [, | -] [ both | rx | tx ] | [ remote ] vlan vlan-id [, | -] [ both | rx | tx ] }
no monitor session session_number source { interface interface-id [, | -] [ both | rx | tx ] | [ remote ] vlan vlan-id [, | -] [ both | rx | tx ] }
```

構文の説明

<i>session_number</i>	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1～68 です。
interface <i>interface-id</i>	SPAN または RSPAN セッションの送信元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 (タイプ、スタックメンバ、モジュール、ポート番号を含む) です。送信元インターフェイスの場合は、ポートチャネルも有効なインターフェイスタイプであり、指定できる範囲は 1～128 です。
,	(任意) 複数のインターフェイスまたは VLAN を指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	(任意) インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
both rx tx	(任意) モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。

remote	(任意) RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1 (デフォルトの VLAN)、または VLAN ID 1002 ～ 1005 (トークンリングおよび FDDI VLAN に予約済) になることはできません。
vlan <i>vlan-id</i>	ingress キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。

コマンド デフォルト

モニタセッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

4 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチスタック上で、合計 68 の SPAN および RSPAN セッションを保有できます。

物理ポート、ポートチャネル、VLAN が送信元になることができます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN (VSPAN) を使用して、VLAN または一連の VLAN 内のネットワークトラフィックを解析する場合、送信元 VLAN のすべてのアクティブポートが SPAN または RSPAN セッションの送信元ポートになります。トランクポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ (,) の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン (-) の前後にスペースが必要です。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet2/0/2
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 source interface port-channel 2 tx
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

show monitor

すべてのスイッチドポートアナライザ (SPAN) およびリモート SPAN (RSPAN) セッションに関する情報を表示するには、EXEC モードで **show monitor** コマンドを使用します。

show monitor [**session** {*session_number* | **all** | **local** | **range list** | **remote**} [**detail**]]

構文の説明

session	(任意) 指定された SPAN セッションの情報を表示します。
<i>session_number</i>	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ~ 68 です。
all	(任意) すべての SPAN セッションを表示します。
local	(任意) ローカル SPAN セッションだけを表示します。
range list	(任意) 一定範囲の SPAN セッションを表示します。 <i>list</i> は有効なセッションの範囲です。 range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 (注) このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	(任意) リモート SPAN セッションだけを表示します。
detail	(任意) 指定されたセッションの詳細情報を表示します。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **show monitor** コマンドと **show monitor session all** コマンドの出力は同じです。

SPAN 送信元セッションの最大数 : 4 (送信元およびローカルセッションに適用)

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Device# show monitor
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Device# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encaps : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
```

```
Encapsulation : Replicate  
Ingress : Enabled, default VLAN = 4  
Ingress encap : Untagged
```

snmp-server enable traps

デバイスでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップの Simple Network Management Protocol（SNMP）通知を送信可能にするには、グローバルコンフィギュレーションモードで **snmp-server enable traps** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps [bridge | cluster | config | copy-config | cpu threshold |
entity | envmon | errdisable | flash | fru-ctrl | hsrp | ipmulticast | mac-notification
| msdp | ospf | pim | port-security | rtr | snmp | storm-control | stpx | syslog |
tty | vlan-membership | vlancreate | vlandelete | vtp ]
no snmp-server enable traps [bridge | cluster | config | copy-config | cpu threshold |
entity | envmon | errdisable | flash | fru-ctrl | hsrp | ipmulticast | mac-notification
| msdp | ospf | pim | port-security | rtr | snmp | storm-control | stpx | syslog |
tty | vlan-membership | vlancreate | vlandelete | vtp ]
```

構文の説明

bridge	(任意) SNMP STPブリッジMIBトラップをイネーブルにします。*
cluster	(任意) SNMP クラスタトラップをイネーブルにします。
config	(任意) SNMP 設定トラップをイネーブルにします。
copy-config	(任意) SNMP コピー設定トラップをイネーブルにします。
cpu threshold	(任意) CPU 関連のトラップをイネーブルにします。*
entity	(任意) SNMP エンティティトラップをイネーブルにします。
envmon	(任意) SNMP 環境モニタトラップをイネーブルにします。*
errdisable	(任意) SNMP エラーディセーブルトラップをイネーブルにします。*
flash	(任意) SNMP フラッシュ通知トラップをイネーブルにします。*
fru-ctrl	(任意) エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。デバイススタックでは、このトラップはスタックにおけるデバイスの挿入/取り外しを意味します。
hsrp	(任意) Hot Standby Router Protocol（HSRP）トラップをイネーブルにします。

ipmulticast	(任意) IP マルチキャストルーティングトラップをイネーブルにします。
mac-notification	(任意) SNMP MAC 通知トラップをイネーブルにします。 *
msdp	(任意) Multicast Source Discovery Protocol (MSDP) トラップをイネーブルにします。
ospf	(任意) Open Shortest Path First (OSPF) トラップをイネーブルにします。
pim	(任意) Protocol-Independent Multicast (PIM) トラップをイネーブルにします。
port-security	(任意) SNMP ポートセキュリティトラップをイネーブルにします。*
rtr	(任意) SNMP Response Time Reporter (RTR) トラップをイネーブルにします。
snmp	(任意) SNMP トラップをイネーブルにします。*
storm-control	(任意) SNMP ストーム制御トラップパラメータをイネーブルにします。
stpx	(任意) SNMP STPX MIB トラップをイネーブルにします。 *
syslog	(任意) SNMP syslog トラップをイネーブルにします。
tty	(任意) TCP 接続トラップを送信します。この設定はデフォルトでイネーブルになっています。
vlan-membership	(任意) SNMP VLAN メンバーシップトラップをイネーブルにします。
vlancreate	(任意) SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	(任意) SNMP VLAN 削除トラップをイネーブルにします。
vtp	(任意) VLAN トランキンングプロトコル (VTP) トラップをイネーブルにします。

コマンド デフォルト SNMP トラップの送信をディセーブルにします。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 上記の表のアスタリスクが付いているコマンド オプションにはサブ コマンドがあります。これらのサブ コマンドの詳細については、関連コマンドの項を参照してください。

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。



(注) **fru-ctrl, insertion** および **removal** キーワードは、コマンドラインのヘルプストリングに表示されますが、デバイスでサポートされていません。**snmp-server enable informs** グローバル コンフィギュレーションコマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host host-addr informs** グローバル コンフィギュレーション コマンドを組み合わせで使用します。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps cluster
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

STPブリッジMIBトラップを生成するには、グローバルコンフィギュレーションモードで **snmp-server enable traps bridge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps bridge [newroot] [topologychange]
no snmp-server enable traps bridge [newroot] [topologychange]
```

構文の説明

newroot	(任意) SNMP STPブリッジMIB新規ルートトラップをイネーブルにします。
topologychange	(任意) SNMP STPブリッジMIBトポロジ変更トラップをイネーブルにします。

コマンドデフォルト

ブリッジSNMPトラップの送信はディセーブルになります。

コマンドモード

グローバルコンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト(NMS)を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次の例では、NMSにブリッジ新規ルートトラップを送信する方法を示します。

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps cpu

CPU通知をイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps cpu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cpu [threshold]
no snmp-server enable traps cpu [threshold]

構文の説明

threshold (任意) CPUしきい値通知をイネーブルにします。

コマンドデフォルト

CPU通知の送信はディセーブルになります。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、CPU しきい値通知を生成する例を示します。

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

SNMP 環境トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps envmon** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
no snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
```

構文の説明

fan	(任意) ファン トラップをイネーブルにします。
shutdown	(任意) 環境シャットダウンモニタ トラップをイネーブルにします。
status	(任意) SNMP 環境ステータス変更トラップをイネーブルにします。
supply	(任意) 環境電源モニタ トラップをイネーブルにします。
temperature	(任意) 環境温度モニタ トラップをイネーブルにします。

コマンド デフォルト

環境 SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

次に、ファン トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps envmon fan
```

例

snmp-server enable traps errdisable

エラーディセーブルの SNMP 通知をイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps errdisable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

構文の説明	notification-rate <i>number-of-notifications</i>	(任意) 通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ~ 10000 です。
コマンド デフォルト	エラー ディセーブルの SNMP 通知送信はディセーブルになります。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **snmp-server host** 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

SNMP フラッシュ通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps flash** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps flash [insertion] [removal]
no snmp-server enable traps flash [insertion] [removal]

構文の説明

insertion (任意) SNMP フラッシュ挿入通知をイネーブルにします。

removal (任意) SNMP フラッシュ取り出し通知をイネーブルにします。

コマンド デフォルト

SNMP フラッシュ通知の送信はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps mac-notification

SNMP MAC 通知トラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps mac-notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]
no snmp-server enable traps mac-notification [**change**] [**move**] [**threshold**]

構文の説明

change (任意) SNMP MAC 変更トラップをイネーブルにします。

move (任意) SNMP MAC 移動トラップをイネーブルにします。

threshold (任意) SNMP MAC しきい値トラップをイネーブルにします。

コマンド デフォルト

SNMP MAC 通知トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps port-security

SNMP ポートセキュリティトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps port-security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps port-security [*trap-rate value*]
no snmp-server enable traps port-security [*trap-rate value*]

構文の説明

trap-rate value (任意) 1 秒間に送信するポートセキュリティトラップの最大数を設定します。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 です (制限はなく、トラップは発生するたびに送信されます)。

コマンド デフォルト

ポートセキュリティ SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、1 秒当たり 200 の速度でポートセキュリティトラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps rtr

Cisco IOS IP サービスレベル契約 (SLA) の Simple Network Management Protocol (SNMP) トラップ通知の送信をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps rtr** コマンドを使用します。IP SLAs SNMP 通知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。

snmp-server enable traps rtr
no snmp-server enable traps rtr

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SNMP 通知はデフォルトで無効に設定されています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、応答時間モニタ MIB (CISCO-RTTMON-MIB) で定義されているように、Cisco IOS IP SLA 通知を制御 (有効化または無効化) します。

snmp-server enable traps rtr コマンドは **snmp-server host** コマンドと組み合わせて使用します。**snmp-server host** コマンドを使用して、SNMP 通知を受信するホスト (1 つ以上) を指定します。SNMP 通知を送信するには、少なくとも 1 つの **snmp-server host** コマンドを設定する必要があります。

例

次に、パブリックとして定義されているコミュニティストリングを使用して、ルータがアドレス `myhost.cisco.com` にあるホストに IP SLA SNMP トラップを送信するように設定する方法の例を示します。

```
snmp-server enable traps rtr
snmp-server host myhost.cisco.com informs version 2c public rtr
```

関連コマンド

Command	Description
ip sla monitor	IP SLA 動作の設定を開始し、IP SLA モニタ コンフィギュレーション モードに移行します。
ip sla	IP SLA 動作の設定を開始し、IP SLA コンフィギュレーション モードに移行します。
snmp-server host	SNMP 通知の宛先 NMS および転送パラメータを指定します。

Command	Description
snmp-server trap-source	SNMP トラップの送信元とするインターフェイスを指定します。

snmp-server enable traps snmp

SNMP トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps snmp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup]
] [warmstart]
no snmp-server enable traps snmp [authentication] [coldstart] [linkdown] [linkup]
] [warmstart]
```

構文の説明

authentication	(任意) 認証トラップをイネーブルにします。
coldstart	(任意) コールドスタートトラップをイネーブルにします。
linkdown	(任意) リンクダウントラップをイネーブルにします。
linkup	(任意) リンクアップトラップをイネーブルにします。
warmstart	(任意) ウォームスタートトラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップ タイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable snmp traps storm-control

ストーム制御 SNMP トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps storm-control [trap-rate value]
no snmp-server enable traps storm-control

構文の説明

trap-rate value (任意) 1 分ごとに送信されるストーム制御トラップの最大数を設定します。指定できる範囲は 0 ~ 1000 です。(デフォルト値は 0 です。発生するたびにトラップが送信されます。)

コマンド デフォルト

ストーム制御 SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次の例は、発生するたびにストーム制御トラップをイネーブルにする方法を示しています。

```
Device(config)# snmp-server enable traps
```


snmp-server enable traps stpx

SNMP STPX MIB トラップをイネーブルにするには、グローバルコンフィギュレーションモードで **snmp-server enable traps stpx** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
no snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

構文の説明

inconsistency (任意) SNMP STPX MIB 矛盾更新トラップをイネーブルにします。

loop-inconsistency (任意) SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。

root-inconsistency (任意) SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。

コマンド デフォルト

SNMP STPX MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

snmp-server host 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、トラップを受信するホスト (NMS) を指定します。トラップタイプを指定しない場合は、すべてのトラップタイプが送信されます。



(注) SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
Device(config)# snmp-server enable traps stpx inconsistency
```

```
snmp-server enable traps stpx
```



第 **IV** 部

QoS

- [QoS \(257 ページ\)](#)



QoS

この章では、次の QoS コマンドについて説明します。

- [class](#) (258 ページ)
- [debug qos](#) (261 ページ)
- [mls qos](#) (263 ページ)
- [mls qos cos](#) (265 ページ)
- [mls qos wrr-queue output cos-map](#) (267 ページ)
- [priority-queue out](#) (269 ページ)
- [show mls qos](#) (270 ページ)
- [show mls qos interface](#) (271 ページ)
- [wrr-queue bandwidth limit](#) (274 ページ)
- [wrr-queue bandwidth shape](#) (275 ページ)

class

指定されたクラスマップ名のトラフィックを分類する一致基準を定義するには、ポリシーマップコンフィギュレーションモードで **class** コマンドを使用します。既存のクラスマップを削除する場合は、このコマンドの **no** 形式を使用します。

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

構文の説明

class-map-name クラス マップに名前を割り当てます。

class-default 分類されていないパケットに一致するシステムのデフォルトクラスを参照します。

コマンド デフォルト

ポリシーマップクラスマップは定義されていません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用する前に、**policy-map** 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リシー マップを識別し、ポリシーマップ コンフィギュレーション モードを開始する必要があります。ポリシーマップを指定すると、ポリシーマップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** 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、ポリシーマップをポートへ添付することができます。

class コマンドを入力すると、ポリシーマップクラス コンフィギュレーション モードが開始されます。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **exit** : ポリシーマップクラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードに戻ります。
- **no** : コマンドをデフォルト設定に戻します。
- **police** : 分類したトラフィックにポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。詳細については、**police** を参照してください。
- **set** : 分類したトラフィックに割り当てる値を指定します。詳細については、**set** を参照してください。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバルコンフィギュレーションコマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

class class-default ポリシーマップ コンフィギュレーション コマンドを使用して、デフォルトクラスを設定できます。分類されていないトラフィック（トラフィッククラスで指定された一致基準を満たさないトラフィック）は、デフォルトトラフィックとして処理されます。

例

次の例では、ポリシーマップにデフォルトのトラフィッククラスを設定する方法を示します。

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit
Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit
Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
Device(config-pmap)# class cm-4
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

次の例では、**class-default** が最初に設定された場合でも、デフォルトのトラフィッククラスをポリシー マップ pm3 の終わりに自動的に配置する方法を示します。

```
Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class class-default
    set dscp 10
Device#
```

関連コマンド

コマンド	説明
class	名前を指定したクラスとパケットとの照合に使用されるクラス マップを作成します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに接続可能なポリシーマップを作成または変更して、サービス ポリシーを指定します。

コマンド	説明
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy map	Quality of Service (QoS) ポリシーマップを表示します。

debug qos

Quality of Service (QoS) ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug qos** コマンドを使用します。QoS デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

```
debug qos {capability | command-installation-time | events | index | pre-classify | provision |
service-policy | set | snmp | tunnel_marking}
no debug qos {capability | command-installation-time | events | index | pre-classify | provision |
service-policy | set | snmp | tunnel_marking}
```

構文の説明

capability	すべての QoS 機能のデバッグ メッセージを表示します。
command-installation-time	QoS コマンドが有効になるまでの時間を表示します。
events	QoS MQC イベントを表示します。
index	クラスベース QoS MIB インデックス永続性を表示します。
pre-classify	VPN の QoS 事前分類イベントを表示します。
provision	QoS プロビジョンを表示します。
service-policy	QoS サービス ポリシーを表示します。
set	QoS パケット マーキングを表示します。
snmp	クラスベース QoS の設定および統計情報を表示します。
tunnel_marking	QoS パケットのトンネル マーキングを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebg qos コマンドは **no debug qos** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。メンバスイッチのデバッグをイネーブルにする場合は、**session switch-number** 特権 EXEC コマンドでアクティブスイッチからセッションを開始して、メンバスイッチのコマンドラインプロンプトで **debug** コマンドを入力できます。また、最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE** 特権 EXEC コマンドを使用できます。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグタイプに関する情報を表示します。

mls qos

スイッチ全体に対して Quality of Service (QoS) をイネーブルにするには、グローバルコンフィギュレーションモードで **mls qos** コマンドを使用します。スイッチ全体のすべての QoS 関連の統計をリセットし、QoS 機能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。

mls qos
no mls qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

QoS はディセーブルです。パケットが変更されない (パケット内の CoS 値は変更されない) ため、信頼できるポートまたは信頼できないポートといった概念は存在しません。トラフィックは Pass-Through モードでスイッチングされます (パケットは書き換えられることなくスイッチングされ、ポリシングなしのベストエフォートに分類されます)。

mls qos 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 QoS をイネーブルにし、その他のすべての QoS 設定はデフォルトに設定されている場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます (CoS 値は 0 に設定されます)。ポリシーマップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし (untrusted) の状態です。デフォルトの出力キューの設定値が有効となります。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

mls qos コマンドを入力すると、システム内のすべてのポートでデフォルトパラメータが使用されて QoS がイネーブルになります。

QoS 分類、ポリシング、マーキングまたは廃棄 (ドロップ)、キューイング、トラフィックシェーピング機能を使用するには、QoS をグローバルにイネーブルにする必要があります。

mls qos コマンドを入力する前に、ポリシーマップを作成し、それをポートに適用できます。QoS 処理は、**mls qos** コマンドを入力するまでは、ディセーブルになっています。

no mls qos コマンドを入力しても、QoS を設定するために使用されるポリシーマップとクラスマップは設定から削除されません。ただし、システムリソースを節約するため、ポリシーマップに対応するエントリはスイッチハードウェアから削除されます。以前の設定で QoS を再度イネーブルにする場合、**mls qos** コマンドを入力します。

このコマンドでスイッチの QoS 状態を切り替えることで、キューのサイズが修正 (再割り当て) されます。キューサイズの変更時には、ハードウェアを再設定する期間中キューは一時的にシャットダウンされ、スイッチはこのキューに新たに到着したパケットをドロップします。

例

次の例では、スイッチ上で QoS をイネーブルにする方法を示します。

```
Device(config)# mls qos
```

設定を確認するには、**show mls qos** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos	QoS 情報を表示します。

mls qos cos

デフォルトのポートサービスクラス (CoS) 値を定義するか、あるいはポートのすべての着信パケットにデフォルトの CoS 値を割り当てるには、インターフェイス コンフィギュレーション モードで **mls qos cos** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos cos {default-cos | override}
no qos mls cos {default-cos | override}
```

構文の説明

default-cos ポートに割り当てられるデフォルトの CoS 値。パケットがタグ付けされていない場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0～7 です。

override 着信パケットの CoS 値を無効にし、すべての着信パケットにデフォルトのポート CoS 値を適用します。

コマンド デフォルト

デフォルトのポート CoS 値は 0 です。
CoS 無効化はディセーブルに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デフォルト値を使用して、タグなし (着信パケットが CoS 値を持たない場合) で着信したすべてのパケットに CoS 値と値を割り当てることができます。また、**override** キーワードを使用すると、デフォルトの CoS 値と値をすべての着信パケットに割り当てることができます。

特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、**override** キーワードを使用します。たとえポートがすでに CoS を信頼するように設定されていても、このコマンドは以前に設定済みの信頼状態を無効にし、すべての着信 CoS 値に **mls qos cos** コマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、パケットの CoS 値は、入力ポートで、ポートのデフォルト CoS を使用して変更されます。

例

次の例では、ポートのデフォルト ポート CoS 値を 4 に設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos trust cos
Device(config-if)# mls qos cos 4
```

次の例では、ポートで、ポートに着信するすべてのパケットにデフォルトのポート CoS 値 4 を割り当てる方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# mls qos cos 4
Device(config-if)# mls qos cos override
```

設定を確認するには、**show mls qos interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos interface	Quality of Service (QoS) 情報を表示します。

mls qos wrr-queue output cos-map

サービスクラス (CoS) 値を出力キューにマッピングするか、または CoS 値をキューおよびしきい値 ID にマッピングするには、グローバル コンフィギュレーション モードで **mls qos wrr-queue output cos-map** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
mls qos wrr-queue output cos-map queue queue-id { cos1 ... cos8 | threshold threshold-id
cos1 ... cos8 }
no mls qos wrr-queue output cos-map
```

構文の説明

queue <i>queue-id</i>	キュー番号を指定します。 <i>queue-id</i> で指定できる範囲は 1 ~ 4 です。
<i>cos1 ... cos8</i>	出力キューにマッピングする CoS 値。 <i>cos1...cos8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 7 です。
threshold <i>threshold-id</i> <i>cos1...cos8</i>	CoS 値をキューのしきい値 ID にマッピングします。 <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。 <i>cos1...cos8</i> には、各値をスペースで区切って、最大 8 の値を入力します。指定できる範囲は 0 ~ 7 です。

コマンド デフォルト

デフォルトの CoS 出力キューしきい値については、「デフォルトの CoS 出力キューしきい値マップ」を参照してください。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが追加されました。

使用上のガイドライン

しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。



(注) 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの Quality of Service (QoS) ソリューションを満たさない場合にのみ、設定を変更してください。

各 CoS 値を、異なるキューおよびしきい値の組み合わせに対してマッピングできます。これによりフレームを異なる動作に従わせることができます。

表 14: デフォルトの CoS 出力キューしきい値マップ

CoS 値	0	1	2	3	4	5	6	7
キュー ID-しきい値 ID	2 - 1	2 - 1	3 - 1	3 - 1	4 - 1	1 - 1	4 - 1	4 - 1

例 :

次の例では、ポートをキューセット 1 にマッピングする方法を示します。CoS 値 0 ~ 3 を出力キュー 1 としきい値 ID 1 にマッピングします。

```
Device(config)# mls qos wrr-queue output cos-map queue 1 threshold 1 0 1 2 3
```

関連コマンド

コマンド	説明
show mls qos maps	QoS のマッピング情報を表示します。

priority-queue out

出力プライオリティキューをイネーブルにするには、インターフェイスコンフィギュレーションモードで **priority-queue out** コマンドを使用します。優先キューを無効にするには、このコマンドの **no** 形式を使用します。

priority-queue out

no priority-queue out

コマンドモード	インターフェイス コンフィギュレーションモード (config-if)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例：

次に、出力プライオリティキューをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth shape 3 0 0 0
Device(config-if)# priority-queue out
```

show mls qos

グローバルの Quality of Service (QoS) 設定情報を表示するには、EXEC モードで **show mls qos** コマンドを使用します。

show mls qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

例

次の例では、QoS がイネーブルの場合の **show mls qos** コマンドの出力を示します。

```
Device# show mls qos
QoS is enabled
```

関連コマンド

コマンド	説明
mls qos	スイッチ全体で QoS をイネーブルにします。

show mls qos interface

ポート レベルのサービス品質 (QoS) 情報を表示するには、EXEC モードで **show mls qos interface** コマンドを使用します。

show mls qos interface [*interface-id* [**policers** | **queueing** | **statistics**]] **stack-port statistics**

構文の説明

<i>interface-id</i>	(任意) 指定されたポートのQoS情報を表示します。有効なインターフェイスには、物理ポートが含まれます。
policers	(任意) インターフェイスのポリサーを表示します。
queueing	(任意) キューイングの指針およびキューに対応したウェイトを表示します。
statistics	(任意) 送受信されたサービスクラス (CoS) 値、キューに入れられたかまたは出力キュー単位で削除されたパケット数、各ポリサーのプロファイル内外のパケット数を表示します。
stack-port statistics	(任意) スタッキングポートのQoS統計情報を表示します。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

policers キーワードは、コマンドラインのヘルプストリングには表示されますが、サポートされていません。

例

次の例では、ポートベース QoS がイネーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```
Device# show mls qos interface gigabitethernet2/0/1
GigabitEthernet1/0/1
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
Trust device: none
```

```
qos mode: port-based
```

次の例では、ポートベース QoS がディセーブルの場合の **show mls qos interface interface-id** コマンドの出力を示します。

```
Device# show mls qos interface interface gigabitethernet2/0/1
GigabitEthernet1/0/1
QoS is disabled. When QoS is enabled, following settings will be applied
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
Trust device: none
qos mode: port-based
```

次の例では、**show mls qos interface interface-id queueing** コマンドの出力を示します。出力緊急キューは、設定されたシェイプド ラウンドロビン (SRR) の重みを無効にします。

```
Device# show mls qos interface gigabitethernet2/0/1 queueing
GigabitEthernet1/0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

次の表に、この出力で表示されるフィールドの説明を示します。

表 15: **show mls qos interface statistics** のフィールドの説明

フィールド		説明
CoS	incoming	CoS 値ごとに受信したパケット数
	outgoing	CoS 値ごとに送信したパケット数
Output queues	enqueued	出力キュー内のパケット数
	dropped	ドロップされた出力キュー内のパケット数
Policer	Inprofile	ポリサーごとのプロファイル内パケット数
	OutofProfile	ポリサーごとのプロファイル外パケット数

関連コマンド

コマンド	説明
mls qos wrr-queue output cos-map	CoS 値を出力キューにマッピング、または CoS 値をキューおよびしきい値 ID にマッピングします。
wrr-queue bandwidth limit	ポートでの最大出力を制限します。

コマンド	説明
wrr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。

wrr-queue bandwidth limit

ポートの最大出力を制限するには、インターフェイス コンフィギュレーション モードで **wrr-queue bandwidth limit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue bandwidth limit weight1
no wrr-queue bandwidth limit
```

構文の説明

weight1 ポート速度の制限をパーセント値で指定します。指定できる範囲は10～90です。

コマンド デフォルト

ポートはレート制限されておらず、100% に設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ただし、ハードウェアはライン レートを 6%単位で調整しているため、この値は厳密ではありません。

例

次の例では、ポートを 800 Mb/s に制限する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# wrr-queue bandwidth limit 80
```

設定を確認するには、**show mls qos interface [interface-id] queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
wrr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた4つの出力キュー上で帯域幅シェーピングをイネーブルにします。

wrr-queue bandwidth shape

シェーピングされた重みを割り当て、ポートにマッピングされた4つの出力キュー上で帯域幅シェーピングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **wrr-queue bandwidth shape** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
wrr-queue bandwidth shape weight1 weight2 weight3 weight4
no wrr-queue bandwidth shape
```

構文の説明

weight1 weight2 weight3 weight4 シェーピングされるポートのパーセンテージを判別する重みを指定します。インバース比 ($1/\text{weight}$) は、このキューのシェーピング帯域幅を指定します。各値はスペースで区切ります。指定できる範囲は 0 ~ 65535 です。

コマンド デフォルト

weight1 は 25 に設定されています。weight2、weight3、および weight4 は 0 に設定されており、これらのキューは共有モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

シェーピングモードでは、キューには帯域幅が割合で保証され、この総量までにレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。バースト性のあるトラフィックをスムーズにする、または長期間にわたって出力をスムーズにする場合に、シェーピングを使用します。

同じポートのキューを両方ともシェーピングに設定する場合、最小番号のキューをシェーピングに設定します。



- (注) 出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

例

次の例では、ポートのキューをシェーピングに設定する方法を示します。

```
Device(config)#interface gigabitethernet2/0/1
Device(config-if)# srr-queue bandwidth shape 8 0 0 0
```

設定を確認するには、**show mls qos interface [interface-id] queueing** 特権 EXEC コマンドを入力します。



第 **V** 部

セキュリティ

・セキュリティ (279 ページ)



セキュリティ

- [aaa accounting dot1x \(281 ページ\)](#)
- [aaa accounting identity \(283 ページ\)](#)
- [aaa authentication dot1x \(285 ページ\)](#)
- [aaa authorization network \(286 ページ\)](#)
- [aaa new-model \(287 ページ\)](#)
- [authentication host-mode \(289 ページ\)](#)
- [authentication logging verbose \(291 ページ\)](#)
- [authentication mac-move permit \(292 ページ\)](#)
- [authentication priority \(293 ページ\)](#)
- [authentication violation \(296 ページ\)](#)
- [cisp enable \(298 ページ\)](#)
- [clear errdisable interface vlan \(300 ページ\)](#)
- [clear mac address-table \(302 ページ\)](#)
- [deny \(MAC アクセス リスト コンフィギュレーション\) \(304 ページ\)](#)
- [dot1x critical \(グローバル コンフィギュレーション\) \(308 ページ\)](#)
- [dot1x logging verbose \(309 ページ\)](#)
- [dot1x pae \(310 ページ\)](#)
- [dot1x supplicant force-multicast \(311 ページ\)](#)
- [dot1x test eapol-capable \(312 ページ\)](#)
- [dot1x test timeout \(313 ページ\)](#)
- [dot1x timeout \(314 ページ\)](#)
- [epm access-control open \(317 ページ\)](#)
- [ip access-group \(318 ページ\)](#)
- [ip admission \(320 ページ\)](#)
- [ip admission name \(321 ページ\)](#)
- [ip device tracking maximum \(324 ページ\)](#)
- [ip device tracking probe \(325 ページ\)](#)
- [ip dhcp snooping database \(326 ページ\)](#)
- [ip dhcp snooping information option format remote-id \(328 ページ\)](#)

- ip dhcp snooping verify no-relay-agent-address (329 ページ)
- ip source binding (330 ページ)
- ip ssh source-interface (332 ページ)
- limit address-count (333 ページ)
- mab request format attribute 32 (334 ページ)
- mab logging verbose (336 ページ)
- permit (MAC アクセス リスト コンフィギュレーション) (337 ページ)
- radius server (341 ページ)
- show aaa clients (343 ページ)
- show aaa command handler (344 ページ)
- **show aaa local** (345 ページ)
- show aaa servers (346 ページ)
- show aaa sessions (347 ページ)
- show authentication sessions (348 ページ)
- show auto security (351 ページ)
- show cisp (353 ページ)
- show dot1x (355 ページ)
- show eap pac peer (357 ページ)
- show ip dhcp snooping statistics (358 ページ)
- show ip ssh (361 ページ)
- show radius server-group (363 ページ)
- show vlan group (365 ページ)
- switchport port-security aging (366 ページ)
- switchport port-security mac-address (368 ページ)
- switchport port-security maximum (371 ページ)
- switchport port-security violation (373 ページ)
- vlan group (375 ページ)

aaa accounting dot1x

認証、認可、およびアカウントティング (AAA) アカウントティングをイネーブルにして、IEEE 802.1Xセッションの特定のアカウントティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** 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。IEEE 802.1X アカウントティング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。

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group {name | radius | tacacs+}... ]}
no aaa accounting dot1x {name | default}
```

構文の説明

name	サーバグループ名。これは、 broadcast group および group キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウントティング方式を、アカウントティングサービス用に指定します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウントティングレコードはバックグラウンドで送信されます。アカウントティングサーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウントティングレコードをイネーブルにして、アカウントティングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
group	アカウントティングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 <ul style="list-style-type: none"> • name : サーバグループの名前。 • radius : すべての RADIUS ホストのリスト。 • tacacs+ : すべての TACACS+ ホストのリスト。 broadcast group および group キーワードの後に入力する場合、 group キーワードはオプションです。オプションの group キーワードより多くの値を入力できます。
radius	(任意) RADIUS アカウントティングをイネーブルにします。
tacacs+	(任意) TACACS+ アカウントティングをイネーブルにします。

コマンドデフォルト AAA アカウントティングはディセーブルです。

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、RADIUS サーバへのアクセスが必要です。
 インターフェイスに IEEE 802.1X RADIUS アカウンティングを設定する前に、**dot1x reauthentication** 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ことを推奨します。

次の例では、IEEE 802.1X アカウンティングを設定する方法を示します。

```
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

IEEE 802.1X、MAC 認証バイパス (MAB)、および Web 認証セッションの認証、認可、およびアカウントリング (AAA) アカウントリングをイネーブルにするには、グローバルコンフィギュレーションモードで、**aaa accounting identity** コマンドを使用します。IEEE 802.1X アカウントリング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。

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group {name | radius | tacacs+} ... ]}
no aaa accounting identity {name | default}
```

構文の説明

name	サーバグループ名。これは、 broadcast group および group キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウントリング方式を、アカウントリングサービス用に使用します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。 start アカウントリングレコードはバックグラウンドで送信されます。アカウントリングサーバが start アカウントリング通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウントリングレコードをイネーブルにして、アカウントリングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
group	アカウントリングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 <ul style="list-style-type: none"> • name : サーバグループの名前。 • radius : すべての RADIUS ホストのリスト。 • tacacs+ : すべての TACACS+ ホストのリスト。 broadcast group および group キーワードの後に入力する場合、 group キーワードはオプションです。オプションの group キーワードより多くの値を入力できます。
radius	(任意) RADIUS 認証をイネーブルにします。
tacacs+	(任意) TACACS+ アカウントリングをイネーブルにします。

コマンドデフォルト AAA アカウントリングはディセーブルです。

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン AAA アカウンティングアイデンティティをイネーブルにするには、ポリシーモードをイネーブルにする必要があります。ポリシーモードを有効にするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

次の例では、IEEE 802.1X アカウンティングアイデンティティを設定する方法を示します。

```
Device# authentication display new-style
```

```
Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.
```

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```


aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで使用する認証、認可、およびアカウントティング (AAA) 方式を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上のグローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

構文の説明

default	ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。
method1	サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、 group radius キーワードを入力します。 (注) コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは default および group radius キーワードのみです。

コマンド デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。IEEE 802.1X に準拠している唯一の方式は、クライアントデータが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** 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 RADIUS サーバを設定する必要があります。

設定された認証方式の一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

次の例では AAA をイネーブルにして IEEE 802.1X 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authorization network

IEEE 802.1x VLAN 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、グローバルコンフィギュレーションモードで **aaa authorization network** コマンドを使用します。RADIUS ユーザ認証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。

aaa authorization network default group radius
no aaa authorization network default

構文の説明	default group radius デフォルトの認証リストとして、サーバグループ内のすべての RADIUS ホストのリストを使用します。	
コマンド デフォルト	認証はディセーブルです。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** 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。認証パラメータは、VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

```
Device(config)# aaa authorization network default group radius
```

aaa new-model

認証、認可、およびアカウントिंग（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーションモードで **aaa new-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

aaa new-model
no aaa new-model

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

AAA が有効になっていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合、**aaa new-model** コマンドを削除するときは、スイッチをリロードしてデフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。



(注) **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

```
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
 login local !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

例

次に、AAA を初期化する例を示します。

```
Device(config)# aaa new-model
```

Device (config) #

関連コマンド

Command	Description
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
aaa authentication arap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaa authentication enable default	ユーザが特権コマンドレベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

authentication host-mode

ポートで認証マネージャモードを設定するには、インターフェイス コンフィギュレーション モードで **authentication host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication host-mode {multi-auth | multi-domain | multi-host | single-host}
no authentication host-mode

構文の説明		
	multi-auth	ポートのマルチ認証モード (multi-auth モード) をイネーブルにします。
	multi-domain	ポートのマルチドメインモードをイネーブルにします。
	multi-host	ポートのマルチホストモードをイネーブルにします。
	single-host	ポートのシングルホストモードをイネーブルにします。

コマンド デフォルト シングルホストモードがイネーブルにされています。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 接続されているデータホストが1つだけの場合は、シングルホストモードを設定する必要があります。シングルホストポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データホストが IP フォン経由でポートに接続されている場合は、マルチドメインモードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメインモードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポートアクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは1つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホストモードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-auth
```

次の例では、ポートのマルチドメインモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-domain
```

次の例では、ポートのマルチホストモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode multi-host
```

次の例では、ポートのシングルホストモードをイネーブルにする方法を示します。

```
Device(config-if)# authentication host-mode single-host
```

設定を確認するには、**show authentication sessions interface *interface* details** 特権 EXEC コマンドを入力します。

authentication logging verbose

認証システムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **authentication logging verbose** コマンドをグローバルコンフィギュレーション モードで使用します。

authentication logging verbose
no authentication logging verbose

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンド デフォルト	システムメッセージの詳細ログは有効になっていません。	
コマンド モード	グローバル コンフィギュレーション (config)	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドにより、認証システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システムメッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# authentication logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
	dot1x logging verbose	802.1X システムメッセージから詳細情報をフィルタリングします。
	mab logging verbose	MAC 認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

authentication mac-move permit

デバイス上でのMAC移動をイネーブルにするには、グローバルコンフィギュレーションモードで **authentication mac-move permit** コマンドを使用します。MAC 移動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。

authentication mac-move permit
no authentication mac-move permit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

MAC 移動は無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、デバイスの 802.1x 対応ポート間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

MAC 移動は、ポートセキュリティ対応の 802.1x ポートではサポートされません。MAC 移動がスイッチ上でグローバルに設定され、ポートセキュリティ対応ホストが 802.1x 対応ポートに移動した場合、違反エラーが発生します。

次の例では、デバイス上で MAC 移動をイネーブルにする方法を示します。

```
Device(config)# authentication mac-move permit
```


authentication priority

プライオリティリストに認証方式を追加するには、インターフェイスコンフィギュレーションモードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

構文の説明	dot1x	(任意) 認証方式の順序に 802.1X を追加します。
	mab	(任意) 認証方式の順序に MAC 認証バイパス (MAB) を追加します。
	webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト デフォルトのプライオリティは、802.1X 認証、MAC 認証バイパス、Web 認証の順です。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証 (webauth) を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。



(注) クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1X 認証、MAC 認証バイパス (MAB)、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

次の例では、802.1X を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority dotx webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番目の認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority mab webauth
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザクレデンシャルの結果として処理する方法を指定します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウントिंगサーバが使用可能になったときに認証マネージャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウントिंगサーバが到達不能になったときに認証マネージャセッションを許可します。
authentication fallback	Web 認証のフォールバック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープンアクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャセッションを強制終了するまでの時間を設定します。

コマンド	説明
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
mab	ポートのMAC認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャセッションに関する情報を表示します。
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報を表示します。

authentication violation

新しいデバイスがポートに接続されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーションモードで **authentication violation** コマンドを使用します。

authentication violation { **protect** | **replace** | **restrict** | **shutdown** }

no authentication violation { **protect** | **replace** | **restrict** | **shutdown** }

構文の説明

protect	予期しない着信 MAC アドレスをドロップします。syslog エラーは生成されません。
replace	現在のセッションを削除し、新しいホストによる認証を開始します。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

コマンド デフォルト

Authentication violation shutdown モードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システムエラーメッセージを生成して、ポートを制限モードに変更するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1X 対応ポートを設定する方法を示します。

```
Device(config-if)# authentication violation replace
```

cisp enable

スイッチ上で Client Information Signalling Protocol (CISP) を有効にして、サブリカントスイッチのオーセンティケータとして機能し、オーセンティケータスイッチのサブリカントとして機能するようにするには、**cisp enable** 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。

cisp enable
no cisp enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

オーセンティケータとサブリカントスイッチの間のリンクはトランクです。両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTP モードを設定する場合に MD5 チェックサムの一一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

次の例では、CISP をイネーブルにする方法を示します。

```
Device(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials プロファイル	プロファイルをサブリカントスイッチに設定します。
dot1x supplicant force-multicast	802.1X サブリカントがマルチキャストパケットを送信するように強制します。

コマンド	説明
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを設定します。
show cisp	指定されたインターフェイスのCISP情報を表示します。

clear errdisable interface vlan

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

構文の説明	<i>interface-id</i>	インターフェイスを指定します。
	<i>vlan list</i>	(任意) 再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **shutdown** および **no shutdown** のインターフェイス 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びイネーブルにするか、**clear errdisable** インターフェイスコマンドを使用して VLAN の error-disabled をクリアできます。

次の例では、ギガビットイーサネットポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド	コマンド	説明
	errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
	errdisable recovery	回復メカニズム変数を設定します。
	show errdisable detect	errdisable 検出ステータスを表示します。
	show errdisable recovery	errdisable 回復タイマーの情報を表示します。

コマンド	説明
show interfaces status err-disabled	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

clear mac address-table

特定のダイナミックアドレス、特定のインターフェイス上のすべてのダイナミックアドレス、スタックメンバ上のすべてのダイナミックアドレス、または特定の VLAN 上のすべてのダイナミックアドレスを MAC アドレステーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。このコマンドはまた MAC アドレス通知グローバルカウンタもクリアします。

clear mac address-table { **dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification** }

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address <i>mac-addr</i>	(任意) 指定されたダイナミック MAC アドレスを削除します。
interface <i>interface-id</i>	(任意) 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ダイナミック MAC アドレスを削除します。
vlan <i>vlan-id</i>	(任意) 指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ~ 4094 です。
move update	MAC アドレステーブルの move-update カウンタをクリアします。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

情報が削除されたことを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
mac address-table move update {receive transmit}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。
show mac address-table notification	interface キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

deny (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックが転送されるのを防止するには、スイッチスタックまたはスタンドアロンスイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。名前付き MAC アクセスリストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

```
deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [cos cos]
no deny {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [cos cos]
```

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host src-MAC-addr src-MAC-addr mask	ホスト MAC アドレスと任意のサブネットマスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host dst-MAC-addr dst-MAC-addr mask	宛先 MAC アドレスと任意のサブネットマスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
<i>type mask</i>	(任意) パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 type には、0 ~ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。
aarp	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。

amber	(任意) EtherType DEC-Amber を指定します。
appletalk	(任意) EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	(任意) EtherType DEC-Diagnostic を指定します。
dsm	(任意) EtherType DEC-DSM を指定します。
etype-6000	(任意) EtherType 0x6000 を指定します。
etype-8042	(任意) EtherType 0x8042 を指定します。
lat	(任意) EtherType DEC-LAT を指定します。
lavec-sca	(任意) EtherType DEC-LAVC-SCA を指定します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 <i>mask</i> は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	(任意) EtherType DEC-MOP Remote Console を指定します。
mop-dump	(任意) EtherType DEC-MOP Dump を指定します。
msdos	(任意) EtherType DEC-MSDOS を指定します。
mumps	(任意) EtherType DEC-MUMPS を指定します。
netbios	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
vines-echo	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。

vines-ip	(任意) EtherType VINES IP を指定します。
xns-idp	(任意) 10 進数、16 進数、または 8 進数の任意の EtherType である EtherType Xerox Network Systems (XNS) プロトコルスイート (0 ~ 65535) を指定します。
cos cos	(任意) プライオリティを設定するため、0 ~ 7 までのサービスクラス (CoS) 値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。 cos オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

コマンド モード MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

mac access-list extended 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、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレスマスクは入力できません。**host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、**type mask** または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

表 16: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
Device(config-ext-macl)# deny any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit	MAC アクセスリスト コンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

dot1x critical (グローバル コンフィギュレーション)

IEEE 802.1X クリティカル認証パラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical eapol

構文の説明

eapol スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

コマンド デフォルト

eapol はディセーブルです

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するよう指定する例を示します。

```
Device(config)# dot1x critical eapol
```


dot1x logging verbose

802.1xシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **dot1x logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

dot1x logging verbose
no dot1x logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システムメッセージの詳細ログは有効になっていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、802.1Xシステムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# dot1x logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
dot1x logging verbose	802.1Xシステムメッセージから詳細情報をフィルタリングします。
mab logging verbose	MAC認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

dot1x pae

Port Access Entity (PAE) タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。設定された PAE タイプ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。

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

構文の説明

supplicant インターフェイスはサブリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。

authenticator インターフェイスはオーセンティケータとしてだけ動作し、サブリカント向けのメッセージに応答しません。

コマンド デフォルト

PAE タイプは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

IEEE 802.1X 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x port-control 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などしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

次に、インターフェイスがサブリカントとして動作するように設定されている例を示します。

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x pae supplicant
```

dot1x supplicant force-multicast

サブリカントスイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN (EAPOL) パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバルコンフィギュレーションモードで **dot1x supplicant force-multicast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

サブリカントスイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

Network Edge Access Topology (NEAT) がすべてのホストモードで機能するようにするには、サブリカントスイッチ上でこのコマンドをイネーブルにします。

次の例では、サブリカントスイッチがオーセンティケータスイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Device(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol (CISP) をイネーブルにすることで、スイッチがサブリカントスイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サブリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサブリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、スイッチスタックまたはスタンドアロンスイッチ上で特権 EXEC モードで **dot1x test eapol-capable** コマンドを使用します。

dot1x test eapol-capable [*interface interface-id*]

構文の説明	interface <i>interface-id</i>	(任意) クエリー対象のポートです。
コマンド デフォルト	デフォルト設定はありません。	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1X 機能をテストするには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、スイッチ上で IEEE 802.1X の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1X 対応であることを示します。

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

関連コマンド	コマンド	説明
	dot1x test timeout <i>timeout</i>	IEEE 802.1X 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

IEEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチスタックまたはスタンドアロン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で **dot1x test timeout** コマンドを使用します。

dot1x test timeout *timeout*

構文の説明	<i>timeout</i>	EAPOL 応答を待機する時間 (秒)。指定できる範囲は 1 ~ 65535 秒です。
-------	----------------	---------------------------------------------

コマンド デフォルト デフォルト設定は 10 秒です。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Device# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド	コマンド	説明
	dot1x test eapol-capable [interface interface-id]	すべての、または指定された IEEE 802.1X 対応ポートに接続するデバイスで IEEE 802.1X の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバル コンフィギュレーション モードまたは インターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウトをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout { **auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

構文の説明

auth-period <i>seconds</i>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。</p>
held-period <i>seconds</i>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
quiet-period <i>seconds</i>	<p>認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
ratelimit-period <i>seconds</i>	<p>動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。</p> <ul style="list-style-type: none"> オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 有効な範囲は 1 ～ 65535 です。デフォルトでは、レート制限はディセーブルになっています。
server-timeout <i>seconds</i>	<p>連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。</p> <ul style="list-style-type: none"> 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 <p>サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。</p>

start-period <i>seconds</i>	連続して送信される 2 つの EAPOL-Start フレーム間の間隔 (秒単位) を設定します。 有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。
supp-timeout <i>seconds</i>	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。
tx-period <i>seconds</i>	クライアントに EAP 要求 ID パケットを再送信する間隔を (応答が受信されないものと仮定して) 秒数で設定します。 <ul style="list-style-type: none"> 有効な範囲は 1 ~ 65535 です。デフォルトは 30 です。 802.1X パケットがサブリカントに送信され、そのサブリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

コマンド デフォルト 定期的な再認証と定期的なレート制限が行われます。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication 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定期的な再認証をイネーブルにただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0 (デフォルト) に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

次に、さまざまな 802.1X 再送信およびタイムアウト時間が設定されている例を示します。

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
```

```
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```


epm access-control open

アクセスコントロールリスト（ACL）が設定されていないポートにオープンディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを使用します。オープンディレクティブ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。

epm access-control open
no epm access-control open

構文の説明 このコマンドには、引数またはキーワードはありません。

コマンド デフォルト デフォルトのディレクティブが適用されます。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スタティック ACL が設定されたアクセスポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープン両方のディレクティブがポートへのアクセスを許可します。

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

次の例では、オープンディレクティブを設定する方法を示します。

```
Device(config)# epm access-control open
```

関連コマンド

コマンド	説明
show running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します

ip access-group

IP アクセスグループを適用するには、インターフェイス コンフィギュレーション モードで **ip access-group** コマンドを使用します。IP アクセスグループを削除するには、このコマンドの **no** 形式を使用します。

ip access-group { *access-list-name* | *standard-access-list* | *expanded-access-list* } **in**

no ip access-group { *access-list-name* | *standard-access-list* | *expanded-access-list* } **in**

構文の説明

access-list-name 既存の IP アクセスリスト名。

standard-access-list 標準アクセスリスト番号。

- 標準または拡張 IP アクセスリストの有効値は、1～199 です。

expanded-access-list 拡張アクセスリスト番号。

- 標準または拡張 IP アクセスリストの有効値は、1300～2699 です。

in インバウンドパケットをフィルタリングします。

コマンド デフォルト

アクセスグループは適用されません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS リリース 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

指定したアクセスリストが使用できない場合、すべてのパケットが渡されます（警告メッセージは発行されません）。

インターフェイスへのアクセスリストの適用

標準の受信アクセスリストの場合、インターフェイスがパケットを受信すると、Cisco IOS ソフトウェアがこのアクセスリストに照らし合わせてパケットの送信元アドレスをチェックします。拡張アクセスリストの場合、ネットワークデバイスが宛先アクセスリストもチェックします。アクセスリストがアドレスを許可している場合は、パケットの処理を継続します。アクセスリストでアドレスが拒否されている場合、ソフトウェアはパケットを廃棄し、Internet Control Management Protocol (ICMP) ホスト到達不能メッセージを返します。

例

次に、ギガビットイーサネット インターフェイス 1/0/1 から受信するパケットにリスト 101 を適用する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# end
```

ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、フォールバック プロファイル コンフィギュレーション モードでも使用できます。Web 認証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。

ip admission rule
no ip admission rule

構文の説明

rule IP アドミッション ルール の名前。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション
 フォールバック プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ip admission コマンドはスイッチポートに web 認証ルールを適用します。

次の例では、スイッチポートに Web 認証ルールを適用する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

次の例では、IEEE 802.1X 対応のスイッチポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

Web 認証をイネーブルにするには、グローバルコンフィギュレーションモードで **ip admission name** コマンドを使用します。Web 認証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。

```
ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
no ip admission name name {consent | proxy http} [absolute timer minutes | inactivity-time
minutes | list {acl | acl-name} | service-policy type tag service-policy-name]
```

構文の説明

name	ネットワークアドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを <i>admission-name</i> 引数で指定された IP アドミッションルールに対応させます。
proxy http	Web 認証のカスタムページを設定します。
absolute-timer 分	(任意) 外部サーバがタイムアウトするまでの経過時間 (分)。
inactivity-time 分	(任意) 外部ファイルサーバが到達不能であると見なされるまでの経過時間 (分)。
list	(任意) 指定されたルールをアクセス コントロールリスト (ACL) に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1~199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
service-policy type tag	(任意) コントロールプレーン サービス ポリシーを設定できます。
service-policy-name	policy-map type control tag <i>policyname</i> コマンド、キーワード、および引数を使用して設定されたコントロールプレーンタグのサービスポリシー。このポリシーマップは、タグを受信したときのホストでの処理を適用するために使用されます。

コマンド デフォルト Web 認証はディセーブルです。

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **ip admission name** コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証をイネーブルにしてから、**ip access-group in** および **ip admission web-rule** 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、特定のインターフェイス上で Web 認証をイネーブルにします。

例 次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

次の例では、スイッチポートでのフォールバックメカニズムとして、Web 認証とともに IEEE 802.1X 認証を設定する方法を示します。

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE802.1x 認証をサポートしていないクライアント用のフォールバック方式として Web 認証を使用するようにポートを設定します。
fallback profile	Web 認証のフォールバックプロファイルを作成します。

コマンド	説明
ip admission	ポートで Web 認証をイネーブ ルにします。
show authentication sessions interface <i>interface</i> detail	Web 認証セッションのステ ータスに関する情報を表示しま す。
show ip admission	NAC のキャッシュされたエン トリーまたは NAC 設定につい ての情報を表示します。

ip device tracking maximum

レイヤ2アクセスポートでIPデバイストラッキングパラメータを設定するには、インターフェイスコンフィギュレーションモードで **ip device tracking maximum** コマンドを使用します。最大値を削除するには、このコマンドの **no** 形式を使用します。

ip device tracking maximum *number*
no ip device tracking maximum

構文の説明

number ポートのIPデバイストラッキングテーブルに作成するバインディングの数。範囲は0（ディセーブル）～65535です。

コマンドデフォルト

なし

コマンドモード

インターフェイスコンフィギュレーションモード

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

最大値を削除するには、**no ip device tracking maximum** コマンドを使用します。

IPデバイストラッキングを無効にするには、**ip device tracking maximum 0** コマンドを使用します。



(注) このコマンドは、設定されている場合は常にIPDTを有効にします。

例

次の例では、レイヤ2アクセスポートでIPデバイストラッキングパラメータを設定する方法を示します。

```
Device# configure terminal
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```


ip device tracking probe

Address Resolution Protocol (ARP) プロブの IP デバイス トラッキング テーブルを設定するには、グローバル コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。ARP インспекション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。

ip device tracking probe {count number|delay seconds|interval seconds|use-svi address}
no ip device tracking probe {count number|delay seconds|interval seconds|use-svi address}

構文の説明

count number	スイッチが ARP プロブを送信する回数を設定します。範囲は 1 ~ 255 です。
delay seconds	スイッチが ARP プロブを送信するまで待機する秒数を設定します。指定できる範囲は 1 ~ 120 です。
interval seconds	スイッチが応答を待ち、ARP プロブを再送信するまでの秒数を設定します。指定できる範囲は 30 ~ 1814400 秒です。
use-svi	スイッチ仮想インターフェイス (SVI) IP アドレスを ARP プロブのソースとして使用します。

コマンドデフォルト

カウント番号は 3 です。

遅延はありません。

30 秒間隔です。

ARP プロブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 です。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スイッチポートのデフォルトソース IP アドレス 0.0.0.0 が使用され、ARP プロブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プロブに使用するように設定するには、**use-svi** キーワードを使用します。

例

次の例では、SVI を ARP プロブのソースとして設定する方法を示します。

```
Device(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

Dynamic Host Configuration Protocol (DHCP) のスヌーピングデータベースを設定するには、グローバルコンフィギュレーションモードで **ip dhcp snooping database** コマンドを使用します。DHCP スヌーピングサーバ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。

no ip dhcp snooping database [**timeout** | **write-delay**]

構文の説明	flash:url	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
	ftp:url	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	http:url	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	https:url	セキュア HTTP (HTTPS) を使用して、エントリを格納するためのデータベースの URL を指定します。
	rnp:url	リモートコピー (RCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
	scp:url	セキュアコピー (SCP) を使用して、エントリを格納するためのデータベースの URL を指定します。
	tftp:url	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
	timeout <i>seconds</i>	タイムアウトインターバルを指定します。有効値は 0 ～ 86,400 秒です。

write-delay <i>seconds</i>	ローカル DHCP スヌーピングデータベースにデータが追加されてから、DHCP スヌーピングエントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。
-----------------------------------	--------------------------------------------------------------------------------------------------

コマンド デフォルト DHCP スヌーピングデータベースは設定されていません。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドを入力する前に、インターフェイス上で DHCP スヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピングエントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Device(config)# ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、スイッチのグローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

構文の説明

hostname スイッチのホスト名をリモート ID として指定します。

string string 1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

コマンド デフォルト

スイッチの MAC アドレスは、リモート ID です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** 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 DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。



(注) ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアントメッセージのリレーエージェントアドレス (giaddr) が信頼できないポート上のクライアント ハードウェア アドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバルコンフィギュレーションモードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェント IP アドレス (giaddr) フィールドが 0 であることを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアントメッセージのリレーエージェントの IP アドレス (giaddr) フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

次に、DHCP クライアントメッセージの giaddr 検証をイネーブルにする例を示します。

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング エントリを削除するには、このコマンドの **no** 形式を使用します。

ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*
no ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*

構文の説明	<i>mac-address</i>	バインディング対象MACアドレスです。
	vlan <i>vlan-id</i>	レイヤ 2 VLAN ID を指定します。有効な値は 1~4094 です。
	<i>ip-address</i>	バインディング対象 IP アドレスです。
	interface <i>interface-id</i>	物理インターフェイスの ID です。
コマンド デフォルト	IP 送信元バインディングは設定されていません。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディング エントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Device# configure terminal
```

```
Device (config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface  
gigabitethernet1/0/1
```

ip ssh source-interface

インターフェイスのIPアドレスをセキュアシェル（SSH）クライアントデバイスの送信元アドレスとして指定するには、グローバルコンフィギュレーションモードで **ip ssh source-interface** コマンドを使用します。送信元アドレスとして指定した IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip ssh source-interface *interface*

no ip ssh source-interface *interface*

構文の説明

<i>interface</i>	アドレスをSSHクライアントの送信元アドレスとして使用するインターフェイス。
------------------	----------------------------------------

コマンド デフォルト

宛先に最も近いインターフェイスのアドレスが送信元アドレスとして使用されます（最も近いインターフェイスはSSHパケットが送信される出力インターフェイスです）。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドを指定することにより、SSHクライアントの送信元アドレスとして送信元インターフェイスのIPアドレスを使用するように強制できます。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 に割り当てられた IP アドレスがSSHクライアントの送信元アドレスとして使用されます。

```
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
```


limit address-count

ポートで使用できる IPv6 アドレスの数を制限するには、Neighbor Discovery Protocol (NDP) インスペクション ポリシー コンフィギュレーション モードまたは IPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

limit address-count *maximum*
no limit address-count

構文の説明

maximum ポートで許可されているアドレスの数。範囲は 1 ～ 10000 です。

コマンド デフォルト

デフォルト設定は無制限です。

コマンド モード

ND インスペクション ポリシーの設定
 IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

limit address-count コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ～ 10000 です。

次に、NDP ポリシー名を **policy1** と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を **policy1** と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

スイッチ上でVLANIDベースのMAC認証をイネーブルにするには、グローバルコンフィギュレーションモードで **mab request format attribute 32 vlan access-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

VLAN-ID ベースの MAC 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

次の例では、スイッチで VLAN-ID ベースの MAC 認証をイネーブルにする方法を示します。

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープンアクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブ爾またはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブ爾にします。
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1X 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブ爾にします。
mab eap	Extensible Authentication Protocol (EAP) を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

mab logging verbose

MAC 認証バイパス (MAB) のシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **mab logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

mab logging verbose
no mab logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システムメッセージの詳細ログは有効になっていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、MAC 認証バイパス (MAB) システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Device(config)# mab logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
dot1x logging verbose	802.1X システムメッセージから詳細情報をフィルタリングします。
mab logging verbose	MAC 認証バイパス (MAB) システムメッセージから詳細情報をフィルタリングします。

permit (MAC アクセス リスト コンフィギュレーション)

条件が一致した場合に非 IP トラフィックの転送を許可するには、スイッチスタックまたはスタンドアロンスイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

```
{permit {any | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsaplsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [coscos]
nopermit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv
| diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap lsap mask |
mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip |
xns-idp] [coscos]
```

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	ホスト MAC アドレスと任意のサブネットマスクを指定します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	宛先 MAC アドレスと任意のサブネットマスクを指定します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
<i>type mask</i>	(任意) パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 <ul style="list-style-type: none"> • <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。 • <i>mask</i> は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。

aarp	(任意) データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
amber	(任意) EtherType DEC-Amber を指定します。
appletalk	(任意) EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
decnet-iv	(任意) EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	(任意) EtherType DEC-Diagnostic を指定します。
dsm	(任意) EtherType DEC-DSM を指定します。
etype-6000	(任意) EtherType 0x6000 を指定します。
etype-8042	(任意) EtherType 0x8042 を指定します。
lat	(任意) EtherType DEC-LAT を指定します。
lavc-sca	(任意) EtherType DEC-LAVC-SCA を指定します。
lsap <i>lsap-number mask</i>	(任意) パケットの LSAP 番号 (0 ~ 65535) と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 <i>mask</i> は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	(任意) EtherType DEC-MOP Remote Console を指定します。
mop-dump	(任意) EtherType DEC-MOP Dump を指定します。
msdos	(任意) EtherType DEC-MSDOS を指定します。
mumps	(任意) EtherType DEC-MUMPS を指定します。

netbios	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
vines-echo	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。
vines-ip	(任意) EtherType VINES IP を指定します。
xns-idp	(任意) EtherType Xerox Network Systems (XNS) プロトコルスイートを指定します。
cos cos	(任意) プライオリティを設定するため、0～7までの任意の Class of Service (CoS) 値を指定します。CoSに基づくフィルタリングは、ハードウェアでだけ実行可能です。 cos オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルトアクションは拒否です。

コマンド モード MAC アクセス リスト コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **appletalk** は、コマンドラインのヘルプストリングには表示されますが、一致条件としてはサポートされていません。

mac access-list extended 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、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレスマスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ (ACE) がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap lsap mask** キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

表 17: IPX フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novell 名	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NetBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
Device(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny	MAC アクセスリストコンフィギュレーションを拒否します。条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレスベースのアクセスリストを作成します。
show access-lists	スイッチに設定されたアクセスコントロールリストを表示します。

radius server

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、スイッチスタックまたはスタンドアロンスイッチで **radiusserver** コンフィギュレーションサブモードコマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

構文の説明

address {<i>ipv4</i> <i>ipv6</i>} <i>ip{address / hostname}</i>	RADIUS サーバの IP アドレスを指定します。
auth-port <i>udp-port</i>	(任意) RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。
acct-port <i>udp-port</i>	(任意) RADIUS アカウンティングサーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。
key <i>string</i>	(任意) スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。 (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキストストリングでなければなりません。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 key にスペースが含まれる場合は、引用符が key の一部でない限り、 key を引用符で囲まないでください。
automate tester <i>name</i>	(任意) RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定します。
retransmit <i>value</i>	(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ~ 100 です。この設定は、 radius-server retransmit グローバルコンフィギュレーションコマンドによる設定を上書きします。
timeout <i>seconds</i>	(任意) スイッチが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、 radius-server timeout グローバルコンフィギュレーションコマンドによる設定を上書きします。
no radius server <i>name</i>	デフォルト設定に戻します。

コマンド デフォルト

- RADIUS アカウンティング サーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバテストはディセーブルです。
- タイムアウトは 60 分（1 時間）です。
- 自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー（string）は設定されていません。

コマンド モード

RADIUS サーバ サブモード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが追加されました。

使用上のガイドライン

- RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。
- **key string** サブモード コンフィギュレーション コマンドを使用すると、認証および暗号キーを設定できます。必ずこのコマンドの最終項目として **key** を設定してください。
- RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定するには、**automate-tester name** キーワードを使用します。

次の例では、認証サーバの UDP ポートを 1645、アカウンティングサーバの UDP ポートを 1646 に設定し、文字列を設定する例を示します。

```
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
```

show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients [detailed]

構文の説明	detailed (任意) 詳細なAAAクライアントの統計情報を示します。				
コマンドモード	ユーザ EXEC				
コマンド履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS Release 15.2(7)E3k</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				

次に、**show aaa clients** コマンドの出力例を示します。

```
Device# show aaa clients
Dropped request packets: 0
```

show aaa command handler

AAA コマンドハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show aaa command handler** コマンドの出力例を示します。

```
Device# show aaa command handler
```

```
AAA Command Handler Statistics:
  account-logon: 0, account-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```

show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

構文の説明

user AAA ローカルのロックアウトされたユーザを指定します。
lockout

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers [**private** | **public** | [**detailed**]]

構文の説明	detailed	(任意) AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
	public	(任意) AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
	detailed	(任意) 詳細な AAA サーバの統計情報を表示します。
コマンドモード	ユーザ EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show aaa servers** コマンドの出力例を示します。

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show aaa sessions** コマンドの出力例を示します。

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

show authentication sessions

現在の認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

show authentication sessions [**database**] [**handle** *handle-id* [**details**]] [**interface** *type number* [**details**]] [**mac** *mac-address* [**interface** *type number*]] [**method** *method-name* [**interface** *type number* [**details**]]] [**session-id** *session-id* [**details**]]

構文の説明

handle <i>handle-id</i>	(任意) 認証マネージャ情報を表示する特定のハンドルを指定します。
interface <i>type number</i>	(任意) 認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac <i>mac-address</i>	(任意) 情報を表示する特定の MAC アドレスを指定します。
method <i>method-name</i>	(任意) 認証マネージャ情報を表示する特定の認証方法を指定します。方式を指定する場合 (dot1x 、 mab 、または webauth)、インターフェイスも指定できます。
session-id <i>session-id</i>	(任意) 認証マネージャ情報を表示する特定のセッションを指定します。

コマンドモード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

現在のすべての認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャセッションに関する情報を表示するには、1つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 18: 認証方式の状態

状態	説明
Not run	このセッションの方式は実行されていません。
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。

状態	説明
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

表 19: 認証方式の状態

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Gi1/0/48   0015.63b0.f676   dot1x   DATA   Authz Success 0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401   mab     DATA   Authz Success 0A3462B10000000D24F80B58
Gi1/0/5    0014.bf5d.d26d   dot1x   DATA   Authz Success 0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions interface gigabitethernet2/0/47
      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A3462C80000000000002763C
      Acct Session ID: 0x00000002
      Handle: 0x25000000

Runnable methods list:
      Method  State
      mab     Failed over
      dot1x   Failed over
-----
      Interface: GigabitEthernet2/0/47
      MAC Address: 0005.5e7c.da05
      IP Address: Unknown
      User-Name: 00055e7cda05
      Status: Authz Success
```

```
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A3462C8000000010002A238
Acct Session ID: 0x00000003
Handle: 0x91000001
Runnable methods list:
Method State
mab Authc Success
dot1x Not run
```

show auto security

自動セキュリティステータスを表示するには、特権 EXEC モードで **show auto security** コマンドを使用します。

show auto-security

このコマンドには引数またはキーワードはありません。

コマンドモード	特権 EXEC (#)
---------	-------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **auto security** コマンドを設定すると、グローバルに自動セキュリティが設定されます（すべてのインターフェイスを含む）。自動セキュリティを無効にすると、すべてのインターフェイスで無効になります。

特定のインターフェイスで自動セキュリティを有効にするには、**auto security-port** コマンドを使用します。

自動セキュリティがグローバルに有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Device# show auto security

Auto Security is Enabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/10
GigabitEthernet1/0/12
GigabitEthernet1/0/23
```

自動セキュリティが特定のインターフェイスで有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Device# show auto security

Auto Security is Disabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
```

関連コマンド

コマンド	説明
auto security	グローバルな自動セキュリティを設定します。
auto security-port	インターフェイス上で自動セキュリティを設定します。

show cisp

指定されたインターフェイスの CISP 情報を表示するには、特権 EXEC モードで **show cisp** コマンドを使用します。

show cisp {[clients | interface *interface-id*] | registrations | summary}

構文の説明	clients	(任意) CISP クライアントの詳細を表示します。
	interface <i>interface-id</i>	(任意) 指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
	registrations	CISP の登録情報を表示します。
	summary	(任意) CISP のサマリー情報を表示します。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show cisp interface** コマンドの出力例を示します。

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

次に、**show cisp registration** コマンドの出力例を示します。

```
Device# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
```

```
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol (CISP) をイネーブルにします。
dot1x credentials <i>profile</i>	サブリカント スイッチでプロファイルを設定します。

show dot1x

スイッチまたは指定されたポートの IEEE 802.1x 統計情報、管理ステータス、および動作ステータスを表示するには、ユーザ EXEC モードで **show dot1x** コマンドを使用します。

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface type number** [**details** | **statistics**]] [**statistics**]

構文の説明	all	(任意) すべてのインターフェイスの IEEE 802.1X 情報を表示します。
	count	(任意) 許可されたクライアントと無許可のクライアントの総数を表示します。
	details	(任意) IEEE 802.1X インターフェイスの詳細を表示します。
	statistics	(任意) すべてのインターフェイスの IEEE 802.1X 統計情報を表示します。
	summary	(任意) すべてのインターフェイスの IEEE 802.1X サマリー情報を表示します。
	interface type number	(任意) 指定したポートの IEEE 802.1X ステータスを表示します。
コマンドモード	ユーザ EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show dot1x all** コマンドの出力例を示します。

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

次に、**show dot1x all count** コマンドの出力例を示します。

```
Device# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients       = 0
Unauthorized Clients     = 0
```

```
Total No of Client          = 0
```

次に、**show dot1x all statistics** コマンドの出力例を示します。

```
Device# show dot1x statistics
Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 0

TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0       ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0    ReTxReqIDFail = 0
TxTotal = 0
```


show eap pac peer

拡張可能認証プロトコル (EAP) のセキュアトンネリングを介したフレキシブル認証 (FAST) ピアの格納済み Protected Access Credential (PAC) を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

show eap pac peer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show eap pac peers** 特権 EXEC コマンドの出力例を示します。

```
Device > show eap pac peers
No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザ EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics [detail]

構文の説明	detail (任意) 詳細な統計情報を表示します。
-------	-----------------------------------

コマンドモード	ユーザ EXEC
---------	----------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スイッチスタックでは、すべての統計情報がプライマリスタックで生成されます。新しいアクティブスイッチが選定された場合、統計カウンタはリセットされます。

次に、**show ip dhcp snooping statistics** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics

Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

次に、**show ip dhcp snooping statistics detail** コマンドの出力例を示します。

```
Device> show ip dhcp snooping statistics detail

Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                       = 0
  Interface is in errdisabled      = 0
  Rate limit exceeded              = 0
  Received on untrusted ports      = 0
  Nonzero giaddr                   = 0
  Source mac not equal to chaddr   = 0
  Binding mismatch                 = 0
  Insertion of opt82 fail          = 0
  Interface Down                   = 0
  Unknown output interface         = 0
  Reply output port equal to input port = 0
  Packet denied by platform        = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 20: DHCP スヌーピング統計情報

DHCP スヌーピング統計情報	説明
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートでDHCPパケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバパケット (OFFER、ACK、NAK、LEASEQUERY のいずれか) を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレーエージェントアドレスフィールド (giaddr) がゼロ以外だった回数。または no ip dhcp snooping information option allow-untrusted 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おらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレスフィールド (chaddr) がパケットの送信元 MAC アドレスと一致せず、 ip dhcp snooping verify mac-address 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回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MACアドレスとVLANのペアのバインディングになっているポートとは異なるポートで、RELEASEパケットまたはDECLINEパケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動してRELEASEまたはDECLINEを実行したことを表すこともあります。MACアドレスは、イーサネットヘッダーの送信元MACアドレスではなく、DHCPパケットのchaddrフィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション82挿入がエラーになった回数。オプション82データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットがDHCPリレーエージェントへの応答であるが、リレーエージェントのSVIインターフェイスがダウンしている回数。DHCPサーバへのクライアント要求の送信と応答の受信の間でSVIがダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション82データまたはMACアドレステーブルのルックアップのいずれかで、DHCP応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション82が使用されておらず、クライアントMACアドレスが期限切れになった場合に発生することがあります。ポートセキュリティオプションでIPSGがイネーブルであり、オプション82がイネーブルでない場合、クライアントのMACアドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

show ip ssh

セキュアシェル（SSH）のバージョンおよび設定データを表示するには、**show ip ssh** 特権 EXEC コマンドを使用します。

show ip ssh

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 再試行やタイムアウトなどの設定済みオプションのステータスを表示するには、**show ip ssh** を使用します。このコマンドを使用すると、SSH がイネーブルかディセーブルかを確認できます。

例

次に、SSH をイネーブルにした場合の **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

次に、SSH をディセーブルにした場合の **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
%SSH has not been enabled
```

次に、設定された RSA キーサイズを表示する **show ip ssh** コマンドの出力例を示します。

```
Device# show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
```

```
Minimum expected Diffie Hellman key size : 1024 bits  
IOS Keys in SECSH format(ssh-rsa, base64 encoded): NONE
```

show radius server-group

RADIUS サーバグループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

show radius server-group {*name* | **all**}

構文の説明

name サーバグループの名前。サーバグループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。

all すべてのサーバグループのプロパティを表示します。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k

このコマンドが導入されました。

使用上のガイドライン

aaa group server radius コマンドで定義したサーバグループを表示するには、**show radius server-group** コマンドを使用します。

次に、**show radius server-group all** コマンドの出力例を示します。

```
Device# show radius server-group all
Server group radius
  Sharecount = 1   sg_unconfigured = FALSE
  Type = standard Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 21 : **show radius server-groups** コマンドのフィールドの説明

フィールド	説明
Server group	サーバグループの名前。
Sharecount	このサーバグループを共有している方式リストの数。たとえば、1つの方式リストが特定のサーバグループを使用する場合、sharecountは1です。2つの方式リストが同じサーバグループを使用する場合、sharecountは2です。
sg_unconfigured	サーバグループが設定解除されました。

フィールド	説明
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバグループ構造の内部参照の数。この数は、このサーバグループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocks はメモリ管理のために内部的に使用されます。

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

```
show vlan group [{group-name vlan-group-name [user_count]}]
```

構文の説明	group-name <i>vlan-group-name</i> (任意) 指定した VLAN グループにマッピングされている VLAN を表示します。
	user_count (任意) 特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。
コマンドデフォルト	なし
コマンドモード	特権 EXEC
コマンド履歴	リリース
	変更内容
	Cisco IOS Release 15.2(7)E3k
	このコマンドが導入されました。
使用上のガイドライン	show vlan group コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。 group-name キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

switchport port-security aging

セキュアアドレスエントリのエージングタイムおよびタイプを設定する、または特定のポートのセキュアアドレスのエージング動作を変更するには、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポートセキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

構文の説明

static	このポートに静的に設定されたセキュアアドレスのエージングをイネーブルにします。
time <i>time</i>	このポートのエージングタイムを指定します。指定できる範囲は0～1440分です。 <i>time</i> が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュアアドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュアアドレス リストから削除されます。
inactivity	inactivity エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュアアドレスが期限切れになります。

コマンド デフォルト

ポートセキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。デフォルトのエージング タイプは **absolute** です。デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

特定のポートのセキュアアドレス エージングをイネーブルにするには、ポートエージングタイムを 0 以外の値に設定します。

特定のセキュアアドレスに時間を限定してアクセスできるようにするには、エージングタイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュアアドレスが削除されます。

継続的にアクセスできるセキュアアドレス数を制限するには、エージングタイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュアアドレスが削除され、他のアドレスがセキュアになることができます。

セキュアアドレスへのアクセス制限を解除するには、セキュアアドレスとして設定し、**no switchport port-security aging static** 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、静的に設定されたセキュアアドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュアアドレスに対して、エージングタイプを **absolute**、エージングタイムを2時間に設定します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュアアドレスに対して、エージングタイプを **inactivity**、エージングタイムを2分に設定します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュアアドレスのエージングをディセーブルにする方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

セキュア MAC アドレスまたはスティッキ MAC アドレスラーニングを設定するには、**switchport port-security mac-address** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} |
sticky [{mac-address | vlan {vlan-id {access | voice}}]}]
```

構文の説明

mac-address	48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できません。
vlan vlan-id	(任意) トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。
vlan access	(任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
vlan voice	(任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 (注) voice キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。
sticky	スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。
mac-address	(任意) スティッキ セキュア MAC アドレスを指定する MAC アドレス。

コマンド デフォルト

セキュア MAC アドレスは設定されていません。
スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。
- 音声 VLAN では、スタティックセキュアまたはスティッキセキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。
- 音声 VLAN はアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

スティッキセキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミックセキュア MAC アドレス (スティッキラーニングがイネーブルになる前に動的に学習されたアドレスを含む) を、スティッキセキュア MAC アドレスに変換し、すべてのスティッキセキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** 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、スティッキラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキセキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレステーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミックアドレスとしてアドレステーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** 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、スティッキセキュア MAC アドレスを設定する場合、これらのアドレスはアドレステーブルおよび実行コンフィギュレーションに追加されます。ポートセキュリティがディセーブルの場合、スティッキセキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキセキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくて済みます。スティッキセキュアアドレスを保存しない場合、アドレスは失われます。スティッキラーニングがディセーブルの場合

合、スティッキセキュア MAC アドレスはダイナミックセキュアアドレスに変換され、実行コンフィギュレーションから削除されます。

- スティックラーニングをディセーブルにして、**switchport port-security mac-address sticky mac-address** インターフェイス コンフィギュレーション コマンドを入力した場合、エラーメッセージが表示され、スティッキセキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキラーニングをイネーブルにして、ポート上で2つのスティッキセキュア MAC アドレスを入力する方法を示します。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

セキュア MAC アドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]
no switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]
```

構文の説明

value インターフェイスのセキュア MAC アドレスの最大数を設定します。
デフォルトの設定は 1 秒です。

vlan (任意) トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。

vlan-list (任意) カンマで区切られた VLAN の範囲またはハイフンで区切られた一連の VLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。

access (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

voice (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

(注) **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

コマンド デフォルト

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

スイッチまたはスイッチスタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができます。

- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

音声 VLAN はアクセスポート上でだけサポートされます。トランクポート上ではサポートされません。

- インターフェイスのセキュアアドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュアアドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```


switchport port-security violation

セキュア MAC アドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
no switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
```

構文の説明

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。
shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

コマンド デフォルト

デフォルトの違反モードは **shutdown** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。



- (注) トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが **errdisable** になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュアポートが **errdisable** ステートの場合、**errdisable recovery cause psecure-violation** 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このステートを解除するか、**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て手動で再びイネーブルにできます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが **errdisable** になります。

セキュアポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができます。
- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。

セキュア MAC アドレスの最大値がアドレステーブルに存在し、アドレステーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュアポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

セキュアポートが **errdisable** ステートの場合は、**errdisable recovery cause psecure-violation** 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、このステートから回復させることができます。**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するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

vlan group

VLAN グループを作成または変更するには、グローバルコンフィギュレーションモードで **vlan group** コマンドを使用します。VLAN グループから VLAN リストを削除するには、このコマンドの **no** 形式を使用します。

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

構文の説明	<i>group-name</i>	VLAN グループの名前。名前は最大 32 文字で、文字から始める必要があります。
	vlan-list <i>vlan-list</i>	VLAN グループに追加される 1 つ以上の VLAN を指定します。 <i>vlan-list</i> 回数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。複数のエントリはハイフン (-) またはカンマ (,) で区切ります。
コマンドデフォルト	なし	
コマンドモード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 指定された VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

vlan group コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

次に、VLAN 7～9 と 11 を VLAN グループにマッピングする例を示します。

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Device(config)# no vlan group group1 vlan-list 7
```




第 **VI** 部

システム管理

- [システム管理コマンド \(379 ページ\)](#)



システム管理コマンド

- [archive download-sw](#) (381 ページ)
- [archive tar](#) (385 ページ)
- [archive upload-sw](#) (389 ページ)
- [boot](#) (391 ページ)
- [boot buffersize](#) (393 ページ)
- [boot enable-break](#) (394 ページ)
- [boot host dhcp](#) (395 ページ)
- [boot host retry timeout](#) (396 ページ)
- [boot manual](#) (397 ページ)
- [boot system](#) (398 ページ)
- [cat](#) (399 ページ)
- [clear logging onboard](#) (400 ページ)
- [clear mac address-table](#) (401 ページ)
- [clear mac address-table move update](#) (402 ページ)
- [copy](#) (403 ページ)
- [debug matm move update](#) (404 ページ)
- [delete](#) (405 ページ)
- [dir](#) (406 ページ)
- [help](#) (408 ページ)
- [hw-module](#) (409 ページ)
- [ip name-server](#) (411 ページ)
- [logging](#) (413 ページ)
- [logging buffered](#) (414 ページ)
- [logging console](#) (415 ページ)
- [logging file flash](#) (417 ページ)
- [logging history](#) (418 ページ)
- [logging history size](#) (419 ページ)
- [logging monitor](#) (420 ページ)
- [logging trap](#) (421 ページ)

- mac address-table notification (422 ページ)
- mac address-table static (424 ページ)
- mkdir (425 ページ)
- more (426 ページ)
- nmsp notification interval (427 ページ)
- rename (429 ページ)
- reset (430 ページ)
- rmdir (431 ページ)
- service sequence-numbers (432 ページ)
- set (433 ページ)
- show boot (436 ページ)
- show cable-diagnostics tdr (439 ページ)
- show mac address-table (441 ページ)
- show mac address-table address (442 ページ)
- show mac address-table aging-time (443 ページ)
- show mac address-table count (444 ページ)
- show mac address-table dynamic (445 ページ)
- show mac address-table interface (446 ページ)
- show mac address-table move update (447 ページ)
- show mac address-table multicast (448 ページ)
- show mac address-table notification (449 ページ)
- show mac address-table static (451 ページ)
- show mac address-table vlan (452 ページ)
- show nmsp (453 ページ)
- show logging onboard (455 ページ)
- shutdown (457 ページ)
- test cable-diagnostics tdr (458 ページ)
- traceroute mac (459 ページ)
- traceroute mac ip (462 ページ)
- type (465 ページ)
- unset (466 ページ)
- version (468 ページ)

archive download-sw

TFTP サーバからスイッチまたはスイッチスタックに新しいイメージをダウンロードし、既存のイメージを上書きするか、または保持するには、特権 EXEC モードで **archive download-sw** コマンドを使用します。

archive download-sw {/directory | /force-reload | /imageonly | /leave-old-sw | /no-set-boot | /no-version-check | /overwrite | /reload | /safe} *source-url*

構文の説明

/directory	イメージのディレクトリを指定します。
/force-reload	ソフトウェアイメージのダウンロードが成功した後で無条件にシステムのリロードを強制します。
/imageonly	ソフトウェアイメージのみをダウンロードし、組み込みデバイスマネージャに関連する HTML ファイルはダウンロードしません。既存のバージョンの HTML ファイルは、既存のバージョンが上書きまたは削除されている場合にだけ削除されます。
/leave-old-sw	ダウンロードに成功した後で古いソフトウェアバージョンを保持します。
/no-set-boot	新しいソフトウェアイメージが正常にダウンロードされた後に、そのイメージをポイントするように BOOT 環境変数の設定が変更されることを防ぎます。
/no-version-check	ソフトウェアイメージをダウンロードする際に、スイッチ上で動作中のイメージとのバージョンの互換性を確認しません。スイッチスタックでは、イメージ上およびスタック上のスタックプロトコルバージョンの互換性を確認せずに、ソフトウェアイメージがダウンロードされます。
/overwrite	ダウンロードされたイメージで、フラッシュメモリのソフトウェアイメージに優先します。
/reload	設定が変更され保存されていない場合を除き、イメージのダウンロードに成功した後でシステムをリロードします。
/safe	現在のソフトウェアイメージを保持します。新しいイメージがダウンロードされるまでは、新しいソフトウェアイメージ用の領域を確保する目的で現在のソフトウェアイメージが削除されることはありません。ダウンロード終了後に現在のイメージが削除されます。

source-url ローカルまたはネットワーク ファイルシステム用の送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- セカンダリ ブート ロータ (BS1) :

bsl:

- ローカル フラッシュ : スタンドアロン スイッチまたはアクティブ スイッチ上のファイル システム :

flash:

- メンバ上のローカルな **flash:** ファイルシステム :

flash メンバ数 :

- FTP :

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

- HTTP サーバ :

http: `[[[username:password]@]{hostname | host-ip} [/directory]/image-name.tar`

- セキュア HTTP サーバ :

https: `[[[username:password]@]{hostname | host-ip} [/directory]/image-name.tar`

- Remote Copy Protocol (RCP) :

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

- TFTP :

tftp: `[[/location]/directory]/image-name.tar`

image-name.tar は、スイッチにダウンロードし、インストールするソフトウェアイメージです。

コマンド デフォルト

現行のソフトウェア イメージは、ダウンロードされたイメージで上書きされません。ソフトウェア イメージと HTML ファイルの両方がダウンロードされます。新しいイメージは **flash:** ファイル システムにダウンロードされます。

BOOT 環境変数は、**flash:** ファイル システムの新しいソフトウェア イメージを示すよう変更されます。イメージ ファイルでは大文字と小文字が区別されます。イメージ ファイルは TAR フォーマットで提供されます。

ダウンロードするイメージのスタック プロトコル バージョンの互換性は、スタック上のバージョンと検査されます。

コマンド モード

特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

/imageonly オプションは、既存のイメージが削除されているか置き換えられている場合に、既存のイメージの HTML ファイルを削除します。


(HTML ファイルのない) Cisco IOS イメージだけがダウンロードされます。

/safe または **/leave-old-sw** オプションを指定すると、十分なフラッシュメモリがない場合に、新しいイメージのダウンロードが失敗することがあります。

ソフトウェアを残すことで、領域の制約により新しいイメージ用に十分なフラッシュメモリがない場合は、エラーメッセージが表示されます。

/leave-old-sw オプションを使用し、新しいイメージをダウンロードしたときに古いイメージが上書きされなかった場合、**delete** 特権 EXEC コマンドを使用して古いイメージを削除することができます。

スタックに存在しているバージョンとは異なるスタック プロトコルバージョンのイメージをダウンロードする場合は、**/no-version-check** オプションを使用します。



(注) **/no-version-check** オプションの使用には注意が必要です。同一のスタックにするためには、アクティブスイッチを含め、すべてのメンバでスタック プロトコルバージョンが同一である必要があります。

このオプションを指定すると、最初にスタック プロトコルのバージョンと、スタックのバージョンの互換性を確認することなく、イメージをダウンロードできます。

フラッシュデバイス上のイメージを、ダウンロードしたイメージで上書きする場合は、**/overwrite** オプションを使用します。

/overwrite オプションなしでこのコマンドを指定する場合、ダウンロードアルゴリズムは、新しいイメージが、スイッチフラッシュデバイスのイメージやスタックメンバで実行中のイメージと同じであるかどうかを確認します。

イメージが同じである場合は、ダウンロードは行われません。イメージが異なっている場合、古いイメージは削除され、新しいイメージがダウンロードされます。

新しいイメージをダウンロードした後で、**/reload** 特権 EXEC コマンドを入力して新しいイメージの使用を開始するか、または **archive download-sw** コマンドの **/reload** または **/force-reload** オプションを指定してください。

例

次の例では、172.20.129.10 の TFTP サーバから新しいイメージをダウンロードし、スイッチでイメージを上書きする方法を示します。

```
Device# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

次の例では、172.20.129.10 の TFTP サーバからソフトウェア イメージだけをスイッチにダウンロードする方法を示します。

```
Device# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

次の例では、ダウンロードに成功した後で古いソフトウェアバージョンを保存する方法を示します。

```
Device# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

archive tar

TAR ファイルを作成する、TAR ファイル内のファイルを一覧表示する、または TAR ファイルからファイルを抽出するには、特権 EXEC モードで **archive tar** コマンドを使用します。

```
archive tar {/create destination-url flash:/file-url} | /table source-url | {/xtract source-url  
flash:/file-url [dir/file...]}
```

構文の説明

/create ローカルまたはネットワーク ファイルシステムに新しい TAR ファイルを作成
destination-url します。

flash:/file-url

destination-url : 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 TAR ファイルの名前を指定します。次のオプションがサポートされています。

- ローカルフラッシュファイルシステム :

flash:

- FTP :

ftp: [[/username [:password] @location] /directory] /itar-filename.tar

- HTTP サーバ :

http: [[/username:password] @] {hostname | host-ip} [/directory] /image-name.tar

- セキュア HTTP サーバ :

https: [[/username:password] @] {hostname | host-ip} [/directory] /image-name.tar

- Remote Copy Protocol (RCP) :

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

- TFTP :

tftp: [[/location] /directory] /image-name.tar

tar-filename.tar は、作成する TAR ファイルです。

flash:/file-url : 新しい TAR ファイルが作成されるローカルフラッシュファイルシステムの場所を指定します。

必要に応じて、送信元ディレクトリ内に格納されているファイルまたはディレクトリのリストを指定して、新しい TAR ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された TAR ファイルに書き込まれます。

table*source-url*

既存の TAR ファイルの内容を画面に表示します。

source-url : 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。次のオプションがサポートされています。

- ローカルフラッシュ : ファイルシステム :

flash:

- FTP :

ftp: `[[/username [:password]@location]/directory]/tar-filename.tar`

- HTTP サーバ :

http: `[[[username:password]@] {hostname | host-ip} [/directory]/image-name.tar`

- セキュア HTTP サーバ :

https: `[[[username:password]@] {hostname | host-ip} [/directory]/image-name.tar`

- Remote Copy Protocol (RCP) :

rcp: `[[/username@location]/directory]/tar-filename.tar`

- TFTP :

tftp: `[[/location]/directory]/image-name.tar`

tar-filename.tar は、表示する TAR ファイルです。

/xtract TAR ファイルからローカル ファイル システムにファイルを抽出します。
source-url
flash:/file-url *source-url* : ローカル ファイル システムの送信元 URL エイリアスを指定しま
 [す。次のオプションがサポートされています。
dir/file...]

- ローカル フラッシュ : ファイル システム :
flash:
- FTP :
ftp: [[/username [:password] @location] /directory] /itar-filename.tar
- HTTP サーバ :
http: [[/username:password] @] {hostname | host-ip} [/directory] /image-name.tar
- セキュア HTTP サーバ :
https: [[/username:password] @] {hostname | host-ip} [/directory] /image-name.tar
- Remote Copy Protocol (RCP) :
rcp: [[/username@location] /directory] /tar-filename.tar
- TFTP :
tftp: [[/location] /directory] /image-name.tar

tar-filename.tar は、ファイルの抽出元の TAR ファイルです。

flash:/file-url [*dir/file...*] : 新しい TAR ファイルの抽出元のローカル 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 TAR 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、*dir/file...* 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。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 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。イメージ名では、大文字と小文字が区別されます。

例

次の例では、TAR ファイルを作成する方法を示します。このコマンドは、ローカルフラッシュ ファイル デバイスの *new-configs* ディレクトリの内容を、TFTP サーバの 172.20.10.30 にある *saved.tar* というファイルに書き込みます。

```
Device# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

次の例では、フラッシュ メモリに含まれるファイルの内容を表示する方法を示します。TAR ファイルの内容が画面に表示されます。

```
Device# archive tar /table flash:c2960-lanbase-tar.12-25.FX.tar
info (219 bytes)
info.ver (219 bytes)
```

次の例では、/html ディレクトリおよびその内容だけを表示する方法を示します。

```
flash:2960-lanbase-mz.12-25.FX.tar 2960-lanbase-mz.12-25.FX/html
<output truncated>
```

次の例では、172.20.10.30 のサーバにある TAR ファイルの内容を抽出する方法を示します。ここでは、ローカルフラッシュ ファイル システムのルート ディレクトリに *new-configs* ディレクトリだけを抽出します。saved.tar ファイルの残りのファイルは抽出されません。

```
Device# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new_configs
```


archive upload-sw

サーバに既存のイメージをアップロードするには、**archive upload-sw** 特権 EXEC コマンドを使用します。

```
archive upload-sw [ /version version_string ] destination-url
```

構文の説明

/version (任意) アップロードするイメージの特定バージョン文字列を指定します。
version_string

destination-url 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 エイリアスです。次のオプションがサポートされています。

- ローカルフラッシュ：スタンドアロンスイッチまたはアクティブスイッチ上のファイルシステム：

flash:

- メンバ上のローカルな **flash:** ファイルシステム：

flash メンバ数：

- FTP：

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

- HTTP サーバ：

http: `[[username:password]@]{hostname | host-ip} [/directory]/image-name.tar`

- セキュア HTTP サーバ：

https: `[[username:password]@]{hostname | host-ip} [/directory]/image-name.tar`

- Secure Copy Protocol (SCP)：

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

- Remote Copy Protocol (RCP)：

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

- TFTP：

tftp: `[[/location]/directory]/image-name.tar`

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。

コマンド デフォルト

flash: ファイル システムから現在稼働中のイメージをアップロードします。

コマンド モード

特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

組み込みデバイス マネージャと対応している HTML ファイルが既存のイメージとともにインストールされている場合にだけ、アップロード機能を使用します。

ファイルは、Cisco IOS イメージ、HTML ファイル、info の順序でアップロードされます。これらのファイルがアップロードされると、ソフトウェアによって TAR ファイルが作成されます。

イメージ名では、大文字と小文字が区別されます。

例

次の例では、スタック メンバ 3 で現在実行中のイメージを、172.20.140.2 の TFTP サーバへアップロードする方法を示します。

```
Device# archive upload-sw /source-system-num 3tftp://172.20.140.2/test-image.tar
```

boot

実行可能イメージをロードおよびブートして、コマンドラインインターフェイス (CLI) を表示するには、ブートローダモードで **boot** コマンドを使用します。

boot [-post | -n | -p | flag] filesystem:/file-url...

構文の説明

-post	(任意) 拡張および総合 POST によってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	(任意) 起動後すぐに、Cisco IOS デバッガが休止します。
-p	(任意) イメージのロード後すぐに、JTAG デバッガが休止します。
filesystem:	ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには flash: を使用します。USB メモリスティックには usbflash0: を使用します。
/file-url	ブート可能なイメージのパス (ディレクトリ) および名前。各イメージ名はセミコロンで区切ります。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、デバイスは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

file-url 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブートローダ **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブートローダセッションだけに適用されます。

これらの設定が保存されて次のブート処理に使用されることはありません。

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。

例

次の例では、*new-image.bin* イメージを使用してデバイスをブートする方法を示します。

```
Device: set BOOT flash:/new-images/new-image.bin  
Device: boot
```

このコマンドを入力すると、セットアッププログラムを開始するように求められます。

boot buffersize

NVRAM バッファ サイズを設定するには、**boot buffersize** 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。

boot buffersize *size*

構文の説明

size NVRAM バッファ サイズ (KB) 有効な範囲は 4096 ~ 1048576 です。

コマンド デフォルト

デフォルトの NVRAM バッファ サイズは 512 KB です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

NVRAM バッファ サイズを設定後、スイッチまたはスイッチ スタックをリロードします。スイッチをスタックに追加し、NVRAM サイズが異なる場合、新しいスイッチはスタックと同期し、自動的にリロードされます。

例

次の例では、バッファ サイズを 524288 KB に設定します。

```
Device(config)# boot buffersize 524288
```

boot enable-break

スタンドアロンスイッチで自動起動プロセスの割り込みをイネーブルにするには、**boot enable-break** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot enable-break
no boot enable-break

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブルコンソール上で **Break** キーを押しても自動起動プロセスへの割り込みはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタンドアロンスイッチからだけ正常に動作します。このコマンドを入力すると、**flash:** ファイルシステムが初期化された後に **Break** キーを押して、自動起動プロセスに割り込むことができます。



- (注) このコマンドの設定に関係なく、スイッチ前面パネルの **MODE** ボタンを押すと、いつでも自動起動プロセスを中断することができます。

このコマンドは、ENABLE_BREAK 環境変数の設定を変更します。

boot host dhcp

DHCPサーバからファイルをダウンロードするようにスイッチを設定するには、**boot host dhcp** 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。

boot host dhcp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

なし

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**boot host dhcp** コマンドを使用して、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する方法を示します。

```
Device(config)# boot host dhcp
```

boot host retry timeout

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するには、**boot host retry timeout** 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。

boot host retry timeout *timeout-value*

構文の説明

timeout-value 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した後にタイムアウトになるまでの時間。

コマンド デフォルト

デフォルトはありません。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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、タイムアウトを 300 秒に設定する例を示します。

```
Device(config)# boot host retry timeout 300
```


boot manual

次回のブートサイクル時のスタンドアロンスイッチの手動ブートをイネーブルにするには**boot manual** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

boot manual
no boot manual

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

手動による起動はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタンドアロン スイッチからだけ正常に動作します。

システムを次回再起動すると、スイッチはブートローダ モードで起動します。これは *switch:* プロンプトによってわかります。システムを起動するには、**boot** 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。

このコマンドは、MANUAL_BOOT 環境変数の設定を変更します。

boot system

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するには、**boot system** 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。

boot system *filename* [**switch** {*switch number* | **all**}]

構文の説明

<i>filename</i>	ブート イメージ コンフィギュレーション ファイルの名前。
switch	(任意) スタック内のスイッチのシステムイメージを設定します。
<i>switch number</i>	スイッチ番号。
all	スタック内のすべてのスイッチのシステムイメージを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、ブートイメージコンフィギュレーションファイルの名前を *config-boot.text* と指定します。

```
Device(config)# boot system config-boot.text
```

cat

1つ以上のファイルの内容を表示するには、ブートローダモードで **cat** コマンドを使用します。

cat *filesystem:/file-url...*

構文の説明

filesystem: ファイルシステムを指定します。

/file-url 表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、イメージファイルの内容を表示する方法を示します。

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x000000068 0x000000069 0x00000006a 0x00000006b
info_end:
```

clear logging onboard

すべてのオンボード障害ロギング（OBFL）データをクリアするには、スイッチスタックまたはスタンドアロンスイッチで **clear logging onboard** 特権 EXEC コマンドを使用します。このコマンドを実行すると、フラッシュメモリに保存されている稼働時間と CLI コマンドに関する情報以外の OBFL データがすべてクリアされます。

clear logging onboard [**module** {*switch-number* | **all**}]



(注) このコマンドは、LAN Base イメージのみでサポートされています。

構文の説明

module (任意) スタック内の指定したスイッチの OBFL データをクリアします。

switch-number 指定されたスイッチの ID。指定できる範囲は 1～4 です。

all (任意) スタック内のすべてのスイッチの OBFL データをクリアします。

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

例

次の例では、動作時間と CLI コマンド情報以外のすべての OBFL 情報をクリアする方法を示します。

```
Device# clear logging onboard
Clear logging onboard buffer [confirm]
```

情報が削除されていることを確認するには、**show logging onboard** 特権 EXEC コマンドを入力します。

clear mac address-table

特定のダイナミックアドレス、特定のインターフェイス上のすべてのダイナミックアドレス、スタックメンバのすべてのダイナミックアドレス、

または、MAC アドレステーブルから特定の VLAN 上のすべてのダイナミックアドレスを削除するには、**clear mac address-table** 特権 EXEC コマンドを使用します。

このコマンドはまた MAC アドレス通知グローバルカウンタもクリアします。

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id ]
| notification }
```



(注) このコマンドは、LAN Base イメージのみでサポートされています。

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address mac-addr	(任意) 指定されたダイナミック MAC アドレスを削除します。
interface interface-id	(任意) 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ダイナミック MAC アドレスを削除します。
vlan vlan-id	(任意) 指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ~ 4094 です。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

情報が削除されていることを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

clear mac address-table move update

MAC アドレステーブル移行更新関連カウンタをクリアするには、**clear mac address-table move update** 特権 EXEC コマンドを使用します。

clear mac address-table move update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、**mac address-table move** 更新関連カウンタをクリアする方法を示します。

```
Device# clear mac address-table move update
```

情報がクリアされていることを確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

copy

ファイルをコピー元からコピー先にコピーするには、ブートローダモードで **copy** コマンドを使用します。

copy *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/source-file-url コピー元のパス（ディレクトリ）およびファイル名です。

/destination-file-url コピー先のパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

例

次の例では、ルートにあるファイルをコピーする方法を示します。

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

debug matm move update

MAC アドレステーブル移行更新メッセージ処理のデバッグをイネーブルにするには、**debug matm move update** 特権 EXEC コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
debug matm move update
no debug matm move update
```

コマンド デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebug matm move update** コマンドは、**no debug matm move update** コマンドと同じように機能します。



(注) このコマンドは、LAN Base イメージのみでサポートされています。

デバッグをイネーブルにすると、アクティブスイッチでのみイネーブルになります。メンバスイッチのデバッグを有効にする場合は、**session switch-number** 特権 EXEC コマンドを使用して、アクティブスイッチからのセッションを開始できます。

次に、メンバスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

また、最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、アクティブスイッチ上で **remote command stack-member-number LINE** 特権 EXEC コマンドを使用できます。

delete

指定されたファイルシステムから1つ以上のファイルを削除するには、ブートローダモードで **delete** コマンドを使用します。

delete *filesystem:/file-url...*

構文の説明

filesystem: ファイルシステムのエイリアス。USBメモリスティックの場合は、**usbflash0:**を使用します。

/file-url... 削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

各ファイルを削除する前に確認を求めるプロンプトがデバイスによって表示されます。

例

次の例では、2つのファイルを削除します。

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0:** ブートローダコマンドを入力します。

dir

指定されたファイルシステムのファイルおよびディレクトリのリストを表示するには、ブートローダモードで **dir** コマンドを使用します。

dir filesystem:/file-url

構文の説明

filesystem: ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

/file-url (任意) 表示するコンテンツが格納されているパス (ディレクトリ) およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

例

次の例では、フラッシュメモリ内のファイルを表示する方法を示します。

```
Device: dir flash:
Directory of flash:/
 2  -rwx      561  Mar 01 2013 00:48:15  express_setup.debug
 3  -rwx    2160256  Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
 4  -rwx      1048  Mar 01 2013 00:01:39  multiple-fs
 6  drwx      512  Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx      512  Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx     4316  Mar 01 2013 01:14:05  config.text
648 -rwx        5  Mar 01 2013 00:01:39  private-config.text
```

96453632 bytes available (25732096 bytes used)

表 22: **dir** のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号

フィールド	説明
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） <ul style="list-style-type: none">• d : ディレクトリ• r : 読み取り可能• w : 書き込み可能• x : 実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名

help

利用可能なコマンドを表示するには、ブートローダモードで **help** コマンドを使用します。

help

構文の説明	このコマンドには引数またはキーワードはありません。
コマンド デフォルト	デフォルトの動作や値はありません。
コマンド モード	ブートローダ
コマンド履歴	リリース

変更内容

Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

例

次に、利用可能なブートローダコマンドのリストを表示する例を示します。

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

hw-module

オンボード障害ロギング (OBFL) をイネーブルにするには、スイッチスタックまたはスタンダードアロンスイッチ上で、**hw-module** 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。この機能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。

hw-module module [*switch-number*] **logging onboard** [**message level** *level*]
no hw-module module [*switch-number*] **logging onboard** [**message level** *level*]



(注) このコマンドは、LAN Base イメージのみでサポートされています。

構文の説明

module	モジュール番号を指定します。
<i>switch-number</i>	(任意) スイッチ番号を入力します。これは、メンバスイッチ番号です。スイッチがスタンダードアロンスイッチの場合、スイッチ番号は1です。スイッチがスタック内にある場合は、スタック内のメンバスイッチ番号に応じて、1～4の範囲内の値を指定できます。
logging-onboard	オンボード障害ロギングを指定します。
message level <i>level</i>	(任意) フラッシュメモリに保存されるハードウェア関連のメッセージの重大度を指定します。指定できる範囲は1～7です。

コマンドデフォルト

OBFL はイネーブルになっており、すべてのメッセージが表示されます。

コマンドモード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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 データ ログ内のタイムスタンプを正確にするには、システムクロックを手動で設定するか、または Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用して設定します。

message level *level* パラメータを入力しなければ、スイッチによって生成されたハードウェア関連のすべてのメッセージが、フラッシュメモリに保存されます。

スタンドアロンスイッチで **hw-module module [switch-number] logging onboard [message level level]** コマンドを入力することは、**hw-module module logging onboard [message level level]** コマンドを入力することと同じです。

アクティブスイッチで **hw-module module logging onboard [message level level]** コマンドを入力すると、OBFL をサポートするすべてのスタックメンバで OBFL がイネーブルになります。

例

次の例では、スイッチスタック上で OBFL をイネーブルにし、アクティブスイッチ上でこのコマンドが入力されたときにスタックメンバ 4 でのハードウェア関連のすべてのメッセージがフラッシュメモリに保存されるように指定する方法を示します。

```
Device(config)# hw-module module 4 logging onboard
```

次の例では、スタンドアロンスイッチ上で OBFL をイネーブルにし、ハードウェア関連の重大度 1 のメッセージだけがスイッチのフラッシュメモリに保存されるように指定する方法を示します。

```
Device(config)# hw-module module 1 logging onboard message level 1
```

設定を確認するには、**show logging onboard** 特権 EXEC コマンドを入力します。

ip name-server

ドメインネームサーバ (DNS) の IP アドレスを設定するには、**ip name-server** コマンドを使用します。ネームサーバを削除するには、このコマンドの **no** 形式を使用します。

ip name-server [*ip-server-address* | *ipv6-server-address* | *vrf*]
no ip name-server [*ip-server-address* | *ipv6-server-address* | *vrf*]

構文の説明		
	<i>ip-server-address</i>	名前とアドレスの解決に使用するネームサーバの IPv4 アドレス。
	<i>ipv6-server-address</i>	名前とアドレスの解決に使用するネームサーバの IPv6 アドレス。
	<i>vrf</i>	VRF 名

コマンド デフォルト ネームサーバのアドレスが未設定。

コマンド モード グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 最大 6 つのネームサーバ (IPv4 ネームサーバおよび IPv6 ネームサーバを含む) を設定できます。

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。スイッチは、最初にプライマリサーバに DNS クエリーを送信します。そのクエリーが失敗した場合は、バックアップサーバにクエリーが送信されます。

維持されているすべてのネームサーバの IP アドレスを表示するには、**show ip name-server** コマンドを入力します。

信頼できるソースとしてのドメインネームシステム (DNS-AS) 機能を使用した Application Visibility Control (AVC) の仕様 :

IPv4 アドレスのみがサポートされています。シーケンス内の最初の 2 つ以上の IP アドレスを IPv4 アドレスにします。これは、DNS-AS 機能を使用した AVC がこれらのみを使用するためです。次の例では、最初の 2 つのアドレスは IPv4 (192.0.2.1 および 192.0.2.2)、3 番目のアドレス (2001:DB8::1) は IPv6 アドレスです。DNS-AS を使用した AVC は最初の 2 つを使用します。

```
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

例

次の例は、ネームサーバとして IPv4 ホスト 192.0.2.1 および 192.0.2.2 を指定する方法を示します。

```
Device# configure terminal  
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

次の例は、ネームサーバとして IPv6 ホスト 3FFE:C00::250:8BFF:FEE8:F800 および 2001:0DB8::3 を指定する方法を示します。

```
Device# configure terminal  
Device(config)# ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```


logging

UNIX syslog サーバホストへのメッセージを記録するには、**logging** 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。

logging host

構文の説明	<i>host</i> 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。				
コマンド デフォルト	なし				
コマンド モード	グローバル コンフィギュレーション				
コマンド履歴	<table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>Cisco IOS Release 15.2(7)E3k</td><td>このコマンドが導入されました。</td></tr></tbody></table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				
使用上のガイドライン	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。				

例

次に、125.1.1.100 としてロギング ホスト IP を指定する例を示します。

```
Device(config)# logging 125.1.1.100
```

logging buffered

内部バッファにメッセージを記録するには、**logging buffered** 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。スイッチまたはスタンドアロンスイッチ上か、または、スイッチスタックの場合はアクティブスイッチ上で使用します。

logging buffered [*size*]

構文の説明	<i>size</i> (任意) 作成されるバッファのサイズです (バイト単位)。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。	
コマンド デフォルト	デフォルトのバッファ サイズは 4096 バイトです。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン スタンドアロンスイッチまたはアクティブスイッチに障害が発生した場合、事前に **logging file flash** 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、フラッシュメモリに保存していない限り、ログファイルは失われます。

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バイト数であるため、バッファ サイズをこの値に設定しないでください。

例

次に、ロギング バッファを 8192 バイトに設定する例を示します。

```
Device(config)# logging buffered 8192
```

logging console

重大度に応じてコンソールに保存するメッセージを制限するには、**logging console** コマンドを使用します。メッセージの保存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。

logging console level
no logging console

構文の説明

level コンソールに保存されるメッセージの重大度。重大度は次のとおりです。

- Emergencies : システムは使用不可 (重大度 0)
- Alerts : 早急な対応が必要 (重大度 1)
- Critical : 危険な状態 (重大度 2)
- Errors : エラーが発生している状態 (重大度 3)
- Warnings : 警告状態 (重大度 4)
- Notifications : 通常の状態だが、重要な状態 (重大度 5)
- Informational : 情報メッセージ (重大度 6)
- Debugging : デバッグ メッセージ (重大度 7)
- Discriminator : MD コンソール アソシエーションを確立します
- Filtered : フィルタ処理を伴うロギングをイネーブルにします
- Guaranteed : コンソール メッセージを保証します
- XML : XML でのロギングをイネーブルにします

コマンド デフォルト

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、受信したコンソールメッセージのレベルを重大度 3 (Errors) 以上に設定する例を示します。

```
Device(config)# logging console 3
```

logging file flash

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するには、**logging file flash** コマンドを使用します。スタンドアロンスイッチ上か、または、スイッチスタックの場合はアクティブスイッチ上で使用します。

logging file flash *:filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

構文の説明	<i>:filename</i>	ログメッセージファイルの名前。
	<i>max-file-size</i>	(任意) ログファイルの最大サイズ。指定できる範囲は4096～2147483647です。デフォルトは4096バイトです。
	<i>min-file-size</i>	(任意) ログファイルの最小サイズ。指定できる範囲は1024～2147483647です。デフォルトは2048バイトです。
	<i>max-file-size</i> <i>type</i>	(任意) ログの重大度またはログタイプ。重大度に指定できる範囲は0～7です。
コマンドデフォルト	デフォルトの最大ファイルサイズは4096バイト、デフォルトの最小ファイルサイズは1024バイトです。	
コマンドモード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、`logging flash: filename` を `log_msg.txt`、最大ファイルサイズを40960、最小ファイルサイズを4096、メッセージの重大度を3に設定する例を示します。

```
Device(config)# logging file flash:log_msg.txt 40960 4096 3
```

logging history

履歴ファイルに格納され、SNMP サーバに送信される syslog メッセージのデフォルトのレベルを変更するには、**logging history** コマンドを使用します。

logging history level

構文の説明	<i>level</i> 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のレベル。				
コマンド デフォルト	デフォルトでは、warning、error、critical、alert、および emergency のメッセージが送信されません。				
コマンド モード	グローバル コンフィギュレーション				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS Release 15.2(7)E3k</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。				

例

次の例では、履歴ファイルに保存され、SNMP サーバに送信される syslog メッセージのレベルを 3 に設定します。

```
Device(config)# logging history 3
```

logging history size

履歴テーブルに保存できる Syslog メッセージの数を指定するには、**logging history size** 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。



(注) 履歴テーブルに指定した最大メッセージエントリ数が格納されている場合は、新しいメッセージエントリを格納できるように、最も古いエントリがテーブルから削除されます。

logging history size *number*

構文の説明

number 履歴テーブルに格納できる Syslog メッセージ数。

コマンド デフォルト

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、履歴テーブルに格納できる Syslog メッセージ数を 200 に設定する例を示します。

```
Device(config)# logging history size 200
```

logging monitor

重大度に従って端末回線に記録されるメッセージを制限するには、**logging monitor** コマンドを使用します。

logging monitor *level*

構文の説明

level 端末回線に記録されるメッセージの重大度。重大度は次のとおりです。

- **Emergencies** : システムは使用不可 (重大度 0)
- **Alerts** : 早急な対応が必要 (重大度 1)
- **Critical** : 危険な状態 (重大度 2)
- **Errors** : エラーが発生している状態 (重大度 3)
- **Warnings** : 警告状態 (重大度 4)
- **Notifications** : 通常の状態だが、重要な状態 (重大度 5)
- **Informational** : 情報メッセージ (重大度 6)
- **Debugging** : デバッグメッセージ (重大度 7)

コマンド デフォルト

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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、受信した端末メッセージのレベルを重大度 3 (エラー) 以上に設定する例を示します。

```
Device(config)# logging monitor 3
```


logging trap

syslog サーバに記録されるメッセージを重大度に基づいて制限するには、**logging trap** コマンドを使用します。

logging trap level

構文の説明

level syslog サーバに記録されるメッセージの重大度レベル。重大度は次のとおりです。

- **Emergencies** : システムは使用不可 (重大度 0)
- **Alerts** : 早急な対応が必要 (重大度 1)
- **Critical** : 危険な状態 (重大度 2)
- **Errors** : エラーが発生している状態 (重大度 3)
- **Warnings** : 警告状態 (重大度 4)
- **Notifications** : 通常の状態だが、重要な状態 (重大度 5)
- **Informational** : 情報メッセージ (重大度 6)
- **Debugging** : デバッグ メッセージ (重大度 7)

コマンド デフォルト

デフォルトで、syslog サーバはデバッグ 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。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、syslog サーバのメッセージ受信レベルを重大度 3 (エラー) 以上に設定します。

```
Device(config)# logging trap 3
```

mac address-table notification

スイッチスタックで MAC アドレス通知機能をイネーブルにするには、**mac address-table notification** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table notification [**mac-move** | **threshold** [[**limit percentage**] **interval time**]]
no mac address-table notification [**mac-move** | **threshold** [[**limit percentage**] **interval time**]]

構文の説明

mac-move	(任意) MAC 移動通知をイネーブルにします。
threshold	(任意) MAC しきい値通知をイネーブルにします。
limit percentage	(任意) MAC 使用率しきい値を入力します。指定できる範囲は 1 ~ 100% です。デフォルト値は 50% です。
interval time	(任意) MAC しきい値通知の時間間隔を設定します。指定できる範囲は 120 ~ 1000000 秒です。デフォルトは 120 秒です。

コマンド デフォルト

デフォルトでは、MAC アドレス通知、MAC 移動、および MAC しきい値モニタリングがディセーブルです。

デフォルトの MAC 利用率しきい値は 50% です。

MAC しきい値通知間のデフォルトの時間は 120 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

また、**mac address-table notification mac-move** コマンドおよび **snmp-server enable traps mac-notification move global configuration** コマンドを入力することにより、MAC アドレスが 1 つのポートから同じ VLAN の別のポートに移動した場合に、常にトラップをイネーブルにできます

MAC アドレステーブルのしきい値制限に達するかそれを超えた場合に常にトラップを生成するには、**mac address-table notification threshold** [**limit percentage**] | [**interval time**] コマンドおよび **snmp-server enable traps mac-notification threshold** グローバル コンフィギュレーション コマンドを入力します。

例

次の例に、しきい値制限を 10 に設定し、時間間隔を 120 秒に設定する方法を示します。

```
Device(config)# mac address-table notification threshold limit 10 interval 120
```

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

mac address-table static

MAC アドレステーブルにスタティックアドレスを追加するには、**mac address-table static** 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。スタティックエントリをテーブルから削除するには、このコマンドの **no** 形式を使用します。

mac address-table static mac-addr vlan vlan-id interface interface-id
no mac address-table static mac-addr vlan vlan-id interface interface-id

構文の説明	<i>mac-addr</i>	アドレス テーブルに追加する宛先 MAC アドレス (ユニキャストまたはマルチキャスト)。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 <i>vlan-id</i>	指定した MAC アドレスを持つパケットを受信する VLAN を指定します。指定できる範囲は 1 ~ 4094 です。
	interface <i>interface-id</i>	受信したパケットの転送先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には、物理ポートとポート チャネルが含まれます。

コマンド デフォルト スタティック アドレスは設定されていません。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

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。VLAN 4 でこの MAC アドレスを宛先としてパケットを受信すると、パケットは指定されたインターフェイスに転送されます。

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet6/0/1
```

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

mkdir

指定されたファイルシステムに1つ以上のディレクトリを作成するには、ブートローダモードで **mkdir** コマンドを使用します。

mkdir *filesystem:/directory-url...*

構文の説明

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/directory-url... 作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ディレクトリ **Saved_Configs** を作成する方法を示します。

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

1 つ以上のファイルの内容を表示するには、ブートローダモードで **more** コマンドを使用します。

more *filesystem:/file-url...*

構文の説明

filesystem: ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。

/file-url... 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

nmosp notification interval

コントローラの Network Mobility Services Protocol (NMSP) 通知間隔値をネットワークの遅延に対応するように変更するには、グローバルコンフィギュレーションモードで **nmosp notification interval** コマンドを使用します。

```
nmosp notification interval { attachment | location | rssi { clients | rfid | rogues { ap | client } } }
```

構文の説明	パラメータ	説明
	attachment	アタッチメント情報の集約に使用する時間を指定します。
	location	ロケーション情報の集約に使用する時間を指定します。
	rssi	RSSI 情報の集約に使用する時間を指定します。
	clients	クライアントの時間間隔を指定します。
	rfid	RFID タグの時間間隔を指定します。
	rogues	不正 AP および不正クライアントの時間間隔を指定します。
	ap	不正 AP の集約に使用する時間を指定します。
	client	不正なクライアントの集約に使用する時間を指定します。

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に設定する例を示します。

```
Device# configure terminal
Device(config)# nmosp notification-interval rfid 25
Device(config)# end
```

次に、デバイスアタッチメント（ネットワークへの接続またはネットワークからの切断）の NMSP 通知間隔を 10 秒に変更する例を示します。

```
Device# configure terminal  
Device(config)# nmsp notification-interval attachment 10  
Device(config)# end
```

次に、ロケーションパラメータ（ロケーション変更）のNMSP通知間隔を20秒に設定する例を示します。

```
Device# configure terminal  
Device(config)# nmsp notification-interval location 20  
Device(config)# end
```


rename

ファイルの名前を変更するには、ブートコンフィギュレーションモードで **rename** コマンドを使用します。

rename *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem: ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

/source-file-url 元のパス（ディレクトリ）およびファイル名です。

/destination-file-url 新しいパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

ファイルの名前が変更されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

reset

システムでハードリセットを実行するには、ブートローダモードで **reset** コマンドを実行します。ハードリセットを行うと、デバイスの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	ブートローダ	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、システムをリセットする方法を示します。

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

指定されたファイルシステムから1つ以上の空のディレクトリを削除するには、ブートローダモードで **rmdir** コマンドを使用します。

rmdir *filesystem:/directory-url...*

構文の説明

filesystem: ファイルシステムのエイリアス。USB メモリスティックの場合は、**usbflash0:** を使用します。

/directory-url... 削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。

デバイスは、各ディレクトリを削除する前に、確認を求めるプロンプトを出します。

例

次の例では、ディレクトリを 1 つ削除する方法を示します。

```
Device: rmdir usbflash0:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

service sequence-numbers

タイムスタンプが同じログメッセージが複数ある場合に、シーケンス番号を使用してこれらのメッセージを表示するには、**service sequence-numbers** 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。

service sequence-numbers

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンド デフォルト	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。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、タイムスタンプが同じログメッセージが複数ある場合に、シーケンス番号を使用してこれらのメッセージを表示する方法を示します。

```
Device(config)# service sequence-numbers
```

set

環境変数を設定または表示するには、ブートローダモードで **set** コマンドを使用します。環境変数は、ブートローダまたはデバイスで稼働している他のソフトウェアを制御するために使用できます。

set *variable value*

構文の説明

変数 値 *variable* および *value* の適切な値には、次のいずれかのキーワードを使用します。

MANUAL_BOOT : デバイスの起動を自動で行うか手動で行うかどうかを決定します。

有効な値は 1/Yes と 0/No です。0 または No 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ます。他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デバイスを起動する必要があります。

BOOT filesystem:/file-url : 自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストを識別します。

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。

ENABLE_BREAK : ユーザがコンソールの **Break** キーを押すと自動起動プロセスを中断できるようになります。

有効な値は 1、Yes、On、0、No、および Off です。1、Yes、または On に設定されている場合は、フラッシュファイルシステムの初期化後にコンソール上で Break キーを押すことで、自動起動プロセスを中断できます。

HELPER filesystem:/file-url : ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。

PS1 prompt : ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。

CONFIG_FILE flash:/file-url : 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。

BAUD rate : コンソールのボーレートに使用するビット数/秒 (b/s) を指定します。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。指定できる範囲は0～128000 b/s です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。

SWITCH_NUMBER *stack-member-number* : スタックメンバのメンバ番号を変更します。

SWITCH_PRIORITY *priority-number* : スタックメンバのプライオリティ値を変更します。

コマンド デフォルト

環境変数のデフォルト値は、次のとおりです。

MANUAL_BOOT: No (0)

BOOT : ヌルストリング

ENABLE_BREAK : No (Off または 0) (コンソール上で Break キーを押して自動起動プロセスを中断することはできません)。

HELPER: デフォルト値はありません (ヘルパーファイルは自動的にロードされません)。

PS1 デバイス :

CONFIG_FILE: config.text

BAUD : 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1



(注) 値が設定された環境変数は、各ファイルのフラッシュファイルシステムに保管されます。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。

このファイルに表示されていない変数には値がありません。表示されていればヌルストリングであっても値があります。Null 文字列 (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。

コマンド モード

ブートローダ

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

使用上のガイドライン 環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

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 メモリに保管されます。

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。

MANUAL_BOOT 環境変数は、**boot manual** 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設定することもできます。

BOOT 環境変数は、**boot system filesystem:/file-url** 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設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** 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設定することもできます。

HELPER 環境変数は、**boot helper filesystem: /file-url** 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設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:/file-url** 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設定することもできます。

SWITCH_NUMBER 環境変数は、**switch current-stack-member-number renumber new-stack-member-number** 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設定することもできます。

SWITCH_PRIORITY 環境変数は、**device stack-member-number priority priority-number** 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設定することもできます。

ブート ロードのプロンプト文字列 (PS1) には、等号 (=) を除く、出力可能な文字列を 120 文字まで指定できます。

例

次に、SWITCH_PRIORITY 環境変数を設定する例を示します。

```
Device: set SWITCH_PRIORITY 2
```

設定を確認するには、**set** ブートローダコマンドを使用します。

show boot

BOOT 環境変数の設定を表示するには、**show boot** 特権 EXEC コマンドを使用します。

show boot

構文の説明	このコマンドには引数またはキーワードはありません。
コマンド デフォルト	なし
コマンド モード	特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例は、**show boot** コマンドの出力を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device# show boot
BOOT path-list      :flash:/image
Config file         :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break        :no
Manual Boot         :yes
HELPER path-list   :
Auto upgrade        :yes
-----
```

スイッチ スタックでは、情報はスタック内の各スイッチに対して表示されます。

この機能は、LAN Base イメージのみでサポートされています。

表 23: show boot のフィールドの説明

フィールド	説明
BOOT path-list	<p>自動起動時にロードおよび実行しようとする実行可能ファイルのセミコロン区切りリストを表示します。</p> <p>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。ディレクトリの縦型検索では、検出した各サブディレクトリを完全に検索してから元のディレクトリでの検索を続けます。</p> <p>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>
Config file	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表示します。
Private config file	Cisco IOS がシステム設定のプライベートの不揮発性コピーの読み書きに使用するファイル名を表示します。
Enable break	起動中のブレイクの許可がイネーブルか、またはディセーブルかを表示します。yes、on、または 1 に設定されている場合は、フラッシュファイルシステムの初期化後にコンソール上で Break キーを押すと、自動起動プロセスを中断できます。
Manual boot	スイッチが自動で起動するか、または手動で起動するかを表示します。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。
Helper path-list	ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを表示します。ヘルパー ファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。

フィールド	説明
Auto upgrade	<p>スイッチ スタックが、互換性のないスイッチがスタックに加入できるように、ソフトウェアバージョンの自動コピーが設定されているかどうかを表示します。</p> <p>Version-Mismatch モードにあるスイッチは、スタックとは異なるバージョンのスタック プロトコルが適用されています。</p> <p>Version-Mismatch モードのスイッチはスタックに加入できません。スタックが Version-Mismatch モードのスイッチにコピーできるイメージを保有し、boot auto-copy-sw 機能がイネーブルの場合、他のスタック メンバからのイメージを Version-Mismatch モードのスイッチに自動的にコピーします。その場合、スイッチは Version-Mismatch モードを終了し、再起動後にスタックに加入します。</p>
NVRAM/Config file buffer size	<p>Cisco IOS がメモリ内のコンフィギュレーションファイルのコピーを保持するために使用するバッファ サイズを表示します。コンフィギュレーションファイルは、バッファ サイズ割り当てを超えてはできません。</p>

show cable-diagnostics tdr

タイムドメイン反射率計（TDR）の結果を表示するには、特権 EXEC モードで **show cable-diagnostics tdr** コマンドを使用します。

show cable-diagnostics tdr interface interface-id

構文の説明

interface-id TDRが実行されているインターフェイスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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、および Small Form-Factor Pluggable（SFP）モジュールポートではサポートされません。

例

次に、デバイスに対する **show cable-diagnostics tdr interface interface-id** コマンドの出力例を示します。

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface Speed Local pair Pair length Remote pair Pair status
-----
Gi1/0/23 1000M Pair A 1 +/- 1 meters Pair A Normal
Pair B 1 +/- 1 meters Pair B Normal
Pair C 1 +/- 1 meters Pair C Normal
Pair D 1 +/- 1 meters Pair D Normal
```

表 24: show cable-diagnostics tdr コマンドで出力されるフィールドの説明

フィールド	説明
Interface	TDR が実行されているインターフェイス。
Speed	接続速度。
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名。

フィールド	説明
Pair length	<p>デバイスに関するケーブルの問題の場所。次のいずれかの場合に限り、TDR は場所を特定できます。</p> <ul style="list-style-type: none"> • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が1000 Mb/s である場合。 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合だけ、TDR はリモート ペアについて確認します。
Pair status	<p>TDR が実行されているワイヤ ペアのステータス</p> <ul style="list-style-type: none"> • Normal : ワイヤ ペアが正しく接続されています。 • Not completed : テストは実行中で、完了していません。 • Not supported : インターフェイスは TDR をサポートしません。 • Open : ワイヤペアが断線しています。 • Shorted : ワイヤ ペアがショートしています。 • ImpedanceMis : インピーダンスが一致しません。 • Short/Impedance Mismatched : インピーダンスが一致しないかケーブルがショートしています。 • InProgress : 診断テストが進行中です。

次の例では、TDR が実行されているときの **show interface interface-id** コマンドの出力を示します。

```
Device# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されていないときの **show cable-diagnostics tdr interface interface-id** コマンドの出力を示します。

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
  % TDR test was never issued on gigabitethernet1/0/2
```

インターフェイスでTDRがサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on Device 1
```

show mac address-table

特定の MAC アドレステーブルのエントリを表示するには、EXEC モードで **show mac address-table** コマンドを使用します。

show mac-address-table

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン



(注) この機能は、LAN Base イメージのみでサポートされています。

このコマンドは、特定のインターフェイスやVLAN上のMACアドレステーブルのダイナミック/スタティック エントリを表示します。

例

次に、**show mac address-table** コマンドの出力例を示します。

```
Device# show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
  All    0000.0000.0001   STATIC  CPU
  All    0000.0000.0002   STATIC  CPU
  All    0000.0000.0003   STATIC  CPU
  All    0000.0000.0009   STATIC  CPU
  All    0000.0000.0012   STATIC  CPU
  All    0180.c200.000b   STATIC  CPU
  All    0180.c200.000c   STATIC  CPU
  All    0180.c200.000d   STATIC  CPU
  All    0180.c200.000e   STATIC  CPU
  All    0180.c200.000f   STATIC  CPU
  All    0180.c200.0010   STATIC  CPU
  1      0030.9441.6327   DYNAMIC Gi0/4
Total Mac Addresses for this criterion: 12
```

show mac address-table address

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するには、EXECモードで **show mac address-table address** コマンドを使用します。

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*]

構文の説明

<i>mac-address</i>	48 ビットの MAC アドレスです。有効な形式は H.H.H です。
interface <i>interface-id</i>	(任意) 特定のインターフェイスの情報を表示します。有効なインターフェイスには、物理ポートとポートチャネルが含まれます。
vlan <i>vlan-id</i>	(任意) 特定の VLAN だけのエントリを表示します。指定できる範囲は 1 ~ 4094 です。

コマンドモード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table address** コマンドの出力例を示します。

```
Device# show mac address-table address 0002.4b28.c482
          Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0002.4b28.c482  STATIC CPU
Total Mac Addresses for this criterion: 1
```

show mac address-table aging-time

アドレステーブルエントリのエージングタイムを表示するには、EXEC モードで **show mac address-table aging-time** コマンドを使用します。

show mac address-table aging-time [vlan vlan-id]

構文の説明	vlan (任意) 特定の VLAN のエージングタイム情報を表示します。指定できる範囲は vlan-id 1 ~ 4094 です。
-------	----------------------------------------------------------------------------------

コマンドモード	ユーザ EXEC 特権 EXEC
---------	---------------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン	VLAN 番号が指定されない場合、すべての VLAN に対するエージングタイムが表示されます。このコマンドを使用すると、特定のアドレス テーブル インスタンスのエージングタイム、指定された VLAN 上または指定がない場合はすべての VLAN 上のすべてのアドレス テーブル インスタンスのエージングタイムが表示されます。
------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

例

次に、**show mac address-table aging-time** コマンドの出力例を示します。

```
Device# show mac address-table aging-time
```

```
Vlan   Aging Time
----   -
  1     300
```

次に、**show mac address-table aging-time vlan 10** コマンドの出力例を示します。

```
Device# show mac address-table aging-time vlan 10
```

```
Vlan   Aging Time
----   -
  10    300
```

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するには、EXEC モードで **show mac address-table count** コマンドを使用します。

show mac address-table count [**vlan** *vlan-id*]

構文の説明	vlan (任意) 特定の VLAN のアドレス数を表示します。指定できる範囲は 1 ~ 4094 <i>vlan-id</i> です。
コマンドモード	ユーザ EXEC 特権 EXEC
コマンド履歴	リリース 変更内容 Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。
使用上のガイドライン	VLAN 番号が指定されない場合、すべての VLAN に対するアドレスカウントが表示されます。

例

次に、**show mac address-table count** コマンドの出力例を示します。

```
Device# show mac address-table count

Mac Entries for Vlan : 1
-----
Dynamic Address Count : 2
Static Address Count : 0
Total Mac Addresses : 2
```


show mac address-table dynamic

ダイナミック MAC アドレステーブルのエントリのみを表示するには、EXEC モードで **show mac address-table dynamic** コマンドを使用します。

show mac address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

構文の説明

address <i>mac-address</i>	(任意) 48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です (特権 EXEC モードの場合だけ利用可能)。
interface <i>interface-id</i>	(任意) 照合を行う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には、物理ポートとポート チャネルが含まれます。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ~ 4094 です。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table dynamic** コマンドの出力例を示します。

```
Device# show mac address-table dynamic
Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
1     0030.b635.7862    DYNAMIC   Gi0/2
1     00b0.6496.2741    DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2
```

show mac address-table interface

指定された VLAN の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するには、**show mac address-table interface EXEC** コマンドを使用します。

show mac address-table interface *interface-id* [**vlan** *vlan-id*]

構文の説明

interface-id インターフェイス タイプを指定します。有効なインターフェイスには、物理ポートとポートチャネルが含まれます。

vlan (任意) 特定の VLAN のエントリを表示します。指定できる範囲は 1 ~ 4094 で *vlan-id* す。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table interface** コマンドの出力例を示します。

```
Device# show mac address-table interface gigabitethernet0/2
```

```

                Mac Address Table
-----
Vlan Mac Address      Type      Ports
----  -
1     0030.b635.7862    DYNAMIC   Gi0/2
1     00b0.6496.2741    DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2

```

show mac address-table move update

デバイス上の MAC アドレステーブル移動更新情報を表示するには、EXEC モードで **show mac address-table move update** コマンドを使用します。

show mac address-table move update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table move update** コマンドの出力例を示します。

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show mac address-table multicast

マルチキャスト MAC アドレステーブルに関する情報を表示するには、**show mac-address-table multicast** コマンドを使用します。

```
show mac-address-table multicast [count | {igmp-snooping [count]} | {user [count]} | {vlan vlan_num}]
```

構文の説明	count	(任意) マルチキャスト エントリの数を表示します。
	igmp-snooping	(任意) IGMP スヌーピングによって学習されたアドレスだけを表示します。
	user	(任意) ユーザが入力したスタティック アドレスだけを表示します。
	vlan vlan_num	(任意) 特定の VLAN だけの情報を表示します。有効値の範囲は 1 ~ 4094 です。

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン ルーテッドポートで使用される MAC アドレステーブル エントリの場合、「vlan」列には内部 VLAN 番号ではなくルーテッドポート名が表示されます。

例

次の例では、特定の VLAN のマルチキャスト MAC アドレス テーブル情報を表示する方法を示します。

```
Device# show mac-address-table multicast vlan 1

Multicast Entries
vlan   mac address      type      ports
-----+-----+-----+-----
    1   ffff.ffff.ffff   system   Switch,Fa6/15
Device#
```

次の例では、すべての VLAN のマルチキャスト MAC エントリ数を表示する方法を示します。

```
Device# show mac-address-table multicast count

MAC Entries for all vlans:
Multicast MAC Address Count:           141
Total Multicast MAC Addresses Available: 16384
Device#
```

show mac address-table notification

すべてのインターフェイスまたは指定したインターフェイスの MAC アドレス通知設定を表示するには、EXEC モードで **show mac address-table notification** コマンドを使用します。

```
show mac address-table notification {change [interface[interface-id]] |
mac-move | threshold}
```

構文の説明		
<i>change</i>		MAC 変更通知機能パラメータおよび履歴テーブル。
interface		(任意) すべてのインターフェイスの情報を表示します。有効なインターフェイスには、物理ポートとポートチャンネルが含まれます。
<i>interface-id</i>		(任意) 指定したインターフェイス。有効なインターフェイスには、物理ポートとポートチャンネルが含まれます。
mac-move		MAC アドレス移動通知のステータスを表示します。
threshold		MAC アドレステーブルのしきい値モニタリングのステータスを表示します。

コマンドデフォルト デフォルトでは、MAC アドレス通知、MAC 移動、および MAC しきい値モニタリングがディセーブルです。

デフォルトの MAC 利用率しきい値は 50% です。

MAC しきい値通知間のデフォルトの時間は 120 秒です。

コマンドモード ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン キーワードを指定せずに **show mac address-table notification change** コマンドを使用すると、MAC アドレス変更通知機能がイネーブルかディセーブルか、MAC 通知間隔 (秒数)、

履歴テーブルの最大許容エントリ数、および履歴テーブルの内容を表示します。

すべてのインターフェイスの通知を表示するには、**interface** キーワードを使用します。interface-id が含まれる場合、そのインターフェイスのフラグだけが表示されます。

例

次の例では、**show mac address-table notification change** コマンドの出力を示します。

```
Device# show mac address-table notification change

MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled

History Table contents
-----
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0000 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1
```

show mac address-table static

スタティック MAC アドレステーブルのエントリだけを表示するには、EXEC モードで **show mac address-table static** コマンドを使用します。

show mac address-table static [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

構文の説明

address <i>mac-address</i>	(任意) 48 ビットの MAC アドレスを指定します。有効なフォーマットは H.H.H です (特権 EXEC モードの場合だけ利用可能)。
interface <i>interface-id</i>	(任意) 照合を行う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には、物理ポートとポート チャネルが含まれます。
vlan <i>vlan-id</i>	(任意) 特定の VLAN のアドレスを指定します。指定できる範囲は 1 ~ 4094 です。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table static** コマンドの出力例を示します。

```
Device# show mac address-table static

                Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
4       0001.0002.0004   STATIC  Drop
6       0001.0002.0007   STATIC  Drop
Total Mac Addresses for this criterion: 8
```

show mac address-table vlan

指定された VLAN の MAC アドレステーブル情報を表示するには、EXEC モードで **show mac address-table vlan** コマンドを使用します。

show mac address-table vlan *vlan-id*

構文の説明

vlan-id 特定の VLAN のアドレス。指定できる範囲は 1～4094 です。

コマンドモード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、**show mac address-table vlan 1** コマンドの出力例を示します。

```
Device# show mac address-table vlan 1

                Mac Address Table
-----
Vlan  Mac Address      Type    Ports
----  -
  1    0100.0ccc.cccc    STATIC  CPU
  1    0180.c200.0000    STATIC  CPU
  1    0100.0ccc.cccd    STATIC  CPU
  1    0180.c200.0001    STATIC  CPU
  1    0180.c200.0002    STATIC  CPU
  1    0180.c200.0003    STATIC  CPU
  1    0180.c200.0005    STATIC  CPU
  1    0180.c200.0006    STATIC  CPU
  1    0180.c200.0007    STATIC  CPU
Total Mac Addresses for this criterion: 9
```


show nmosp

Network Mobility Services Protocol (NMSP) 構成の設定を表示するには、**show nmosp** コマンドを使用します。

```
show nmosp {attachment | {suppress interfaces} | capability | notification interval | statistics
{connection | summary} | status | subscription detail [ip-addr ] | summary}
```

構文の説明		
	attachment suppress interfaces	アタッチメント抑制インターフェイスを表示します。
	capability	NMSP 機能を表示します。
	notification interval	NMSP 通知間隔を表示します。
	statistics connection	すべての接続別カウンタを表示します。
	statistics summary	NMSP カウンタを表示します。
	status	アクティブな NMSP 接続のステータスを表示します。
	subscription detail ip-addr	特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。
	subscription summary	コントローラがサブスクライブされているすべての NMSP サービスの詳細を表示します。特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次に、**show nmosp notification interval** コマンドの出力例を示します。

```
Device# show nmosp notification interval
NMSP Notification Intervals
-----

RSSI Interval:
Client          : 2 sec
RFID            : 2 sec
Rogue AP       : 2 sec
```

```
Rogue Client      : 2 sec  
Attachment Interval : 30 sec  
Location Interval  : 30 sec
```

show logging onboard

OBFL 情報を表示するには、**show logging onboard** 特権 EXEC コマンドを使用します。

```
show logging onboard switch-number{clilog | continuous | end | environment | message | module | poe | raw | start | status | summary | temperature | uptime | voltage}
```

構文の説明

<i>switch-number</i>	スイッチまたはスタック メンバ番号を指定します。
clilog	スタンダアロンスイッチまたは指定されたスタック メンバで入力された OBFL CLI コマンドを表示します。
continuous	オンボードロギングの継続情報を表示します。
detail	詳細なオンボードロギング情報を表示します。
end	終了日時の詳細を表示します。
environment	スタンダアロン スイッチまたは指定されたスタック メンバの UDI 情報を表示します。接続されているすべての FRU デバイスについては、PID、VID、およびシリアル番号を表示します。
message	スタンダアロンスイッチまたは指定されたスタック メンバによって生成されたハードウェア関連のメッセージを表示します。
module	システム内の個々のモジュールを指定します。
poe	スタンダアロンスイッチまたは指定されたスイッチスタックメンバの POE の詳細を表示します。
raw	オンボードロギングの raw 情報を表示します。
start	開始日時の詳細を指定します。
status	スタンダアロンスイッチまたは指定されたスタック メンバの状態を表示します。
summary	オンボードロギングのステータス情報を表示します。
temperature	スタンダアロン スイッチまたは指定されたスイッチ スタック メンバの温度を表示します。
uptime	スタンダアロンスイッチまたは指定されたスタック メンバが起動した時刻、スタンダアロンスイッチまたは指定されたスタック メンバが再起動された理由、およびスタンダアロンスイッチまたは指定されたスタック メンバが最後に再起動されて以来の稼働時間を表示します。
voltage	スタンダアロンスイッチまたは指定されたスタック メンバのシステム電圧を表示します。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次の例では、スタンダロンスイッチまたは指定されたスタックメンバで入力された OBFL CLI コマンドを表示します。

```
Device# show logging onboard cliilog
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバの UDI 情報を表示します。接続されているすべての FRU デバイスについては、PID、VID、およびシリアル番号を表示します。

```
Device# show logging onboard environment
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバによって生成されたハードウェア関連のメッセージを表示します。

```
Device# show logging onboard message
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバの温度を表示します。

```
Device# show logging onboard temperature
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバが起動した時刻、スタンダロンスイッチまたは指定されたスタックメンバが再起動した理由、およびスタンダロンスイッチまたは指定されたスタックメンバが最後に再起動してからの稼働時間を表示します。

```
Device# show logging onboard uptime
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバのシステム電圧を表示します。

```
Device# show logging onboard voltage
```

次の例では、スタンダロンスイッチまたは指定されたスタックメンバの状態を表示します。

```
Device# show onboard switch 1 status
```

shutdown

VLAN スイッチングをシャットダウンするには、グローバル コンフィギュレーション モードで **shutdown** コマンドを使用します。設定セットを無効にするには、このコマンドの **no** 形式を使用します。

```
shutdown [ vlanvlan-id ]  
no shutdown
```

構文の説明

vlan <i>vlan-id</i>	シャットダウンする VLAN の VLAN ID。
----------------------------	---------------------------

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、VLAN をシャットダウンする方法の例を示します。

```
Device(config)# vlan open1  
Device(config-wlan)# shutdown
```

次に、アクセス ポイントがシャットダウンされない例を示します。

```
Device# configure terminal  
Device(config)# ap name 3602a no shutdown
```

test cable-diagnostics tdr

インターフェイス上でタイムドメイン反射率計（TDR）機能を実行するには、特権 EXEC モードで **test cable-diagnostics tdr** コマンドを使用します。

test cable-diagnostics tdr interface interface-id

構文の説明

interface-id TDRを実行するインターフェイス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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Small Form-Factor Pluggable（SFP）モジュールポートではサポートされません。

test cable-diagnostics tdr interface interface-id コマンドを使用して TDR を実行した後、**show cable-diagnostics tdr interface interface-id** 特権 EXEC コマンドを使用して結果を表示します。

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

インターフェイスのリンクステータスがアップ状態で速度が10 Mb/s または100 Mb/s である場合、**test cable-diagnostics tdr interface interface-id** コマンドを入力すると、次のメッセージが表示されます。

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

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 パスを表示するには、特権 EXEC モードで **traceroute mac** コマンドを使用します。

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] [**detail**]

構文の説明	interface <i>interface-id</i> (任意) 送信元または宛先デバイス上のインターフェイスを指定します。
	<i>source-mac-address</i> 送信元デバイスの 16 進形式の MAC アドレス。
	<i>destination-mac-address</i> 宛先デバイスの 16 進形式の MAC アドレス。
	vlan <i>vlan-id</i> (任意) 送信元デバイスから宛先デバイスまでをパケットが通過するレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。
	detail (任意) 詳細情報を表示するよう指定します。

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのデバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

デバイスがレイヤ 2 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。

パス内で識別可能な最大ホップ数は 10 です。

レイヤ 2 **traceroute** はユニキャストトラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、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。

異なる VLAN にある送信元および宛先アドレスを指定した場合、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。

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。

複数の装置がハブを介して 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るなど）、レイヤ 2 **tracert** 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。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) : Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) : Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
    Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先デバイスのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) : Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) : Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) : Gi0/0/2 => Gi0/0/1
```



```
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、デバイスが送信元デバイスに接続されていない場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、デバイスが送信元 MAC アドレスの宛先ポートを検出できない場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先デバイスが複数の VLAN にある場合のレイヤ 2 のパスを示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

tracert mac ip

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 パスを表示するには、特権 EXEC モードで **tracert mac ip** コマンドを使用します。

tracert mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*}
[**detail**]

構文の説明	<i>source-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された送信元デバイスの IP アドレス。
	<i>source-hostname</i>	送信元デバイスの IP ホスト名。
	<i>destination-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された宛先デバイスの IP アドレス。
	<i>destination-hostname</i>	宛先デバイスの IP ホスト名。
	detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークの各デバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

デバイスがレイヤ 2 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。

パス内で識別可能な最大ホップ数は 10 です。

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、**tracert 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 アドレスは同一のサブネットにある必要があります。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。

複数の装置がハブを介して 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るなど）、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。

例

次の例では、**detail** キーワードを使用して、送信元と宛先の IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) : Gi0/0/3 => Gi0/1
con1          (2.2.1.1      ) : Gi0/0/1 => Gi0/2
con2          (2.2.2.2      ) : Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Device# tracert mac ip 2.2.66.66 2.2.77.77  
Arp failed for destination 2.2.77.77.  
Layer2 trace aborted.
```

type

1つ以上のファイルの内容を表示するには、ブートローダモードで **type** コマンドを使用します。

type *filesystem:/file-url...*

構文の説明

filesystem: ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

/file-url... 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

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。

ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

1つ以上の環境変数をリセットするには、ブートローダモードで**unset** コマンドを使用します。

unset variable...

構文の説明

<i>variable</i>	<i>variable</i> には、次に示すキーワードのいずれかを使用します。 MANUAL_BOOT : デバイスの起動を自動で行うか手動で行うかどうかを指定します。
	BOOT : 自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。 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。
	ENABLE_BREAK : フラッシュファイルシステムの初期化後に、コンソール上の Break キーを使用して自動ブートプロセスを中断できるかどうかを指定します。
	HELPER : ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。
	PS1 : ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。
	CONFIG_FILE : 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リセットします。
	BAUD : コンソールで使用される速度（ビット/秒 (b/s) 単位）をリセットします。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン 通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** 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リセットすることもできます。

BOOT 環境変数は、**no boot system** 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リセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** 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リセットすることもできます。

HELPER 環境変数は、**no boot helper** 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リセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** 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リセットすることもできます。

例

次に、SWITCH_PRIORITY 環境変数をリセットする例を示します。

```
Device: unset SWITCH_PRIORITY
```

version

ブートローダのバージョンを表示するには、ブートローダモードで **version** コマンドを使用します。

version

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

例

次に、デバイスのブートローダのバージョンを表示する例を示します。

```
Device:version
C1000 Boot Loader (C1000-HBOOT-M) Version 15.2(7r)E, RELEASE SOFTWARE (fc1)
Compiled
```




第 **VII** 部

VLANs

- [VLAN \(471 ページ\)](#)



VLAN

- [clear vtp counters](#) (472 ページ)
- [debug platform vlan](#) (473 ページ)
- [debug sw-vlan](#) (474 ページ)
- [debug sw-vlan ifs](#) (476 ページ)
- [debug sw-vlan notification](#) (477 ページ)
- [debug sw-vlan vtp](#) (479 ページ)
- [interface vlan](#) (481 ページ)
- [show platform vlan](#) (483 ページ)
- [show vlan](#) (484 ページ)
- [show vtp](#) (487 ページ)
- [switchport priority extend](#) (495 ページ)
- [switchport trunk](#) (497 ページ)
- [switchport voice vlan](#) (500 ページ)
- [vlan](#) (503 ページ)
- [vtp \(グローバル コンフィギュレーション\)](#) (511 ページ)
- [vtp \(インターフェイス コンフィギュレーション\)](#) (517 ページ)
- [vtp primary](#) (518 ページ)

clear vtp counters

VLAN Trunking Protocol (VTP) およびプルーニングカウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

clear vtp counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

次の例では、VTP カウンタをクリアする方法を示します。

```
Device# clear vtp counters
```

情報が削除されたことを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

debug platform vlan

VLAN マネージャソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform vlan** コマンドを使用します。デバッグ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。

構文の説明

error VLAN エラー デバッグ メッセージを表示します。

mvid マッピングされた VLAN ID の割り当ておよびフリー デバッグ メッセージを表示します。

rpc リモート プロシージャ コール (RPC) デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

使用上のガイドライン

undebg platform vlan コマンドは **no debug platform vlan** コマンドと同じです。

次の例では、VLAN エラー デバッグ メッセージを表示する方法を示します。

```
Device# debug platform vlan error
```

debug sw-vlan

VLAN マネージャアクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan** コマンドを使用します。デバッグ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。

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification | packets
| redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | mapping | notification |
packets | redundancy | registries | vtp}
```

構文の説明

badpmcookies	不良ポート マネージャクッキーの VLAN マネージャ インシデントに関するデバッグ メッセージを表示します。
cfg-vlan	VLAN 設定デバッグ メッセージを表示します。
bootup	スイッチが起動すると、メッセージが表示されます。
cli	コマンドライン インターフェイス (CLI) が VLAN コンフィギュレーション モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグ メッセージを表示します。
ifs	VLAN マネージャ IOS ファイルシステム (IFS) のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	VLAN マネージャ通知のデバッグ メッセージを表示します。
packets	パケット処理およびカプセル化プロセスのデバッグ メッセージを表示します。
redundancy	VTP VLAN 冗長性のデバッグ メッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグ メッセージを表示します。
vtp	VLAN Trunking Protocol (VTP) コードのデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan コマンドは **no debug sw-vlan** コマンドと同じです。

次に、VLAN マネージャ イベントのデバッグ メッセージを表示する例を示します。

```
Device# debug sw-vlan events
```

debug sw-vlan ifs

VLAN マネージャ IOS File System (IFS) エラーテストのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan ifs** コマンドを使用します。デバッグ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。

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

構文の説明

open read	VLAN マネージャ IFS ファイル読み取り動作のデバッグメッセージを表示します。
open write	VLAN マネージャ IFS ファイル書き込み動作のデバッグメッセージを表示します。
read	指定されたエラーテスト (1 、 2 、 3 、または 4) に関するファイル読み取り動作のデバッグメッセージを表示します。
write	ファイル書き込み動作のデバッグメッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan ifs コマンドは **no debug sw-vlan ifs** コマンドと同じです。

ファイルの読み取り処理に処理 **1** を選択すると、ヘッダー検証ワードおよびファイルバージョン番号が格納されたファイルヘッダーが読み込まれます。処理 **2** を指定すると、ドメインおよび VLAN 情報の大部分が格納されたファイル本体が読み取られます。処理 **3** を指定すると、Type Length Version (TLV) 記述子構造が読み取られます。処理 **4** を指定すると、TLV データが読み取られます。

次の例では、ファイル書き込み動作のデバッグメッセージを表示する方法を示します。

```
Device# debug sw-vlan ifs write
```


debug sw-vlan notification

VLAN マネージャ通知のデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan notification** コマンドを使用します。デバッグ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。

```
debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange |
modechange | pruningcfgchange | statechange}
no debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange |
modechange | pruningcfgchange | statechange}
```

構文の説明

accfwdchange	集約アクセス インターフェイス スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
allowedvlanfgchange	許可 VLAN の設定変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
fwdchange	スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
linkchange	インターフェイスリンクステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
modechange	インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
pruningcfgchange	プルーニング設定変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
statechange	インターフェイス ステート変更の VLAN マネージャ通知のデバッグ メッセージを表示します。

コマンド デフォルト デバッグはディセーブルです。

コマンド モード 特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebug sw-vlan notification** コマンドは **no debug sw-vlan notification** コマンドと同じです。

次に、インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示する例を示します。

```
Device# debug sw-vlan notification
```

debug sw-vlan vtp

VLAN Trunking Protocol (VTP) コードのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan vtp** コマンドを使用します。デバッグ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。

```
debug sw-vlan vtp {events | packets | pruning [{packets | xmit}] | redundancy | xmit}
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

構文の説明

events	汎用の論理フローのデバッグメッセージおよびVTPコード内のVTP_LOG_RUNTIME マクロによって生成されたVTPメッセージの詳細を表示します。
packets	Cisco IOS VTP プラットフォーム依存層からVTPコードに渡されたすべての着信VTPパケット（プルーニングパケットを除く）の内容のデバッグメッセージを表示します。
pruning	VTPコードのプルーニングセグメントによって生成されるデバッグメッセージを表示します。
packets	（任意）Cisco IOS VTP プラットフォーム依存層からVTPコードに渡されたすべての着信VTPプルーニングパケットの内容のデバッグメッセージを表示します。
xmit	（任意）VTPコードがCisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信VTPパケットの内容のデバッグメッセージを表示します。
redundancy	VTP冗長性のデバッグメッセージを表示します。
xmit	VTPコードがCisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信VTPパケット（プルーニングパケットを除く）の内容のデバッグメッセージを表示します。

コマンドデフォルト デバッグはディセーブルです。

コマンドモード 特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン **undebug sw-vlan vtp** コマンドは **no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードの後に追加のパラメータを入力しない場合は、VTPプルーニングデバッグメッセージが表示されます。これらのメッセージは、VTPプルーニングコード内の

VTP_PRUNING_LOG_NOTICE、VTP_PRUNING_LOG_INFO、VTP_PRUNING_LOG_DEBUG、VTP_PRUNING_LOG_ALERT、および VTP_PRUNING_LOG_WARNING マクロによって生成されます。

次に、VTP 冗長性のデバッグ メッセージを表示する例を示します。

```
Device# debug sw-vlan vtp redundancy
```

interface vlan

ダイナミック スイッチ仮想インターフェイス (SVI) を作成するか、既存のダイナミック SVI にアクセスし、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*
no interface vlan *vlan-id*

構文の説明	<i>vlan-id</i>	VLAN 番号。指定できる範囲は 1 ~ 4094 です。
コマンド デフォルト	デフォルトの VLAN インターフェイスは VLAN 1 です。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、ISL または IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、あるいはアクセス ポート用に設定された VLAN ID に対応します。

SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、またはアクセス ポート用に設定された VLAN ID に対応します。



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

no interface vlan *vlan-id* コマンドを使用して削除した SVI は、**show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。



(注) VLAN 1 インターフェイスを削除することはできません。

削除されたインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力すると、削除された SVI を元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチまたはスイッチ スタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。

sdm prefer 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、システムのハードウェアリソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。

設定を確認するには、**show interfaces** および **show interfaces vlan *vlan-id*** 特権 EXEC コマンドを入力します。

次の例では、VLANID23の新しいSVIを作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Device(config)# interface vlan 23  
Device(config-if)#
```

show platform vlan

プラットフォーム依存 VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

show platform vlan {**misc** | **mvid** | **prune** | **refcount** | **rpc** {**receive** | **transmit**}}

構文の説明

misc	各種 VLAN モジュール情報を表示します。
mvid	Mapped VLAN ID (MVID) 割り当て情報を表示します。
prune	スタックまたはプラットフォームで維持されるプルーニング データベースを表示します。
refcount	VLAN ロック モジュールについてのリファレンス カウントを表示します。
rpc	リモート プロシージャ コール (RPC) メッセージを表示します。
receive	受信された情報を表示します。
transmit	送信された情報を表示します。

コマンドデフォルト

なし

コマンドモード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

次の例では、リモートプロシージャコール (RPC) メッセージを表示する方法を示します。

```
Device# show platform vlan rpc
```

show vlan

設定されたすべての VLAN またはスイッチ上の 1 つの VLAN (VLAN ID または名前を指定した場合) のパラメータを表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [{**brief** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**}]

構文の説明

brief	(任意) VLAN ごとに VLAN 名、ステータス、およびポートを 1 行で表示します。
group	(任意) VLAN グループについての情報を表示します。
id <i>vlan-id</i>	(任意) VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。 <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。
mtu	(任意) VLAN のリストと、VLAN のポートに設定されている最小および最大伝送単位 (MTU) サイズを表示します。
name <i>vlan-name</i>	(任意) VLAN 名で特定された 1 つの VLAN に関する情報を表示します。 VLAN 名は、1 ~ 32 文字の ASCII 文字列です。
remote-span	(任意) Remote SPAN (RSPAN) VLAN に関する情報を表示します。
summary	(任意) VLAN サマリー情報を表示します。



(注) **ifindex** キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。

コマンドデフォルト

なし

コマンドモード

ユーザ EXEC

コマンド履歴

リリース

変更内容

Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

使用上のガイドライン

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に **yes** が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッ

チングされると、ドロップされることがあります。VLANにSVIがない場合、ハイフン (-) 記号がSVI_MTU列に表示されます。MTU-Mismatch列にyesが表示されている場合、MiniMTUとMaxMTUを持つポート名が表示されます。

次に、**show vlan** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Device > show vlan
VLAN Name                               Status      Ports
-----
1    default                               active     Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48

2    VLAN0002                               active
40   vlan-40                                 active
300  VLAN0300                                active
1002 fddi-default                           act/unsup
1003 token-ring-default                   act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001  1500 -     -     -     -   -       0      0
2    enet  100002  1500 -     -     -     -   -       0      0
40   enet  100040  1500 -     -     -     -   -       0      0
300  enet  100300  1500 -     -     -     -   -       0      0
1002 fddi  101002  1500 -     -     -     -   -       0      0
1003 tr   101003  1500 -     -     -     -   -       0      0
1004 fdnet 101004  1500 -     -     -     -   ieee -    0      0
1005 trnet 101005  1500 -     -     -     -   ibm  -    0      0
2000 enet  102000  1500 -     -     -     -   -       0      0
3000 enet  103000  1500 -     -     -     -   -       0      0

Remote SPAN VLANs
-----
2000,3000

Primary Secondary Type           Ports
-----
```

表 25: **show vlan** コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号。

フィールド	説明
Name	VLAN の名前 (設定されている場合)。
Status	VLAN のステータス (active または suspend)。
Ports	VLAN に属するポート。
Type	VLAN のメディア タイプ。
SAID	VLAN のセキュリティ アソシエーション ID 値。
MTU	VLAN の最大伝送単位サイズ。
Parent	親 VLAN (存在する場合)。
RingNo	VLAN のリング番号 (該当する場合)。
BrdgNo	VLAN のブリッジ番号 (該当する場合)。
Stp	VLAN で使用されるスパニングツリープロトコル タイプ。
BrdgMode	この VLAN のブリッジングモード: 可能な値はソースルートブリッジング (SRB) およびソースルートトランスペアレント (SRT) で、デフォルトは SRB です。
Trans1	トランスレーションブリッジ 1。
Trans2	トランスレーションブリッジ 2。
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。

次に、**show vlan summary** コマンドの出力例を示します。

```
Device > show vlan summary
Number of existing VLANs           : 45
Number of existing VTP VLANs      : 45
Number of existing extended VLANs : 0
```

次に、**show vlan id** コマンドの出力例を示します。

```
Device# show vlan id 2
VLAN Name                               Status    Ports
-----
2    VLAN0200                               active   Gi1/0/7, Gi1/0/8
2    VLAN0200                               active   Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
2    enet  100002   1500  -      -      -    -    -      0      0

Remote SPAN VLANs
-----
Disabled
```

show vtp

VLAN Trunking Protocol (VTP) 管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、EXEC モードで **show vtp** コマンドを使用します。

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**}

構文の説明	counters	devices	conflicts	interface	interface-id	password	status
	デバイスの VTP 統計情報を表示します。	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、デバイスが VTP バージョン 3 を実行していない場合だけ適用されます。	(任意) 競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。デバイスが VTP トランスポートモードまたは VTP オフモードにある場合、このコマンドは無視されます。	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。	(任意) VTP ステータスおよび設定を表示するインターフェイス。ここには物理インターフェイスまたはポートチャネルを指定できます。	設定された VTP パスワードを表示します (特権 EXEC モードでのみ使用可能)。	VTP 管理ドメインのステータスに関する一般情報を表示します。

コマンド デフォルト なし

コマンド モード ユーザ EXEC
特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン デバイスが VTP バージョン 3 を実行中に **show vtp password** コマンドを入力すると、表示は次のルールに従います。

- **password** *password* グローバル コンフィギュレーション コマンドで **hidden** キーワードを指定せず、デバイス上で暗号化がイネーブルでない場合、パスワードはクリアテキストで表示されます。

- **password password** コマンドで **hidden** キーワードを指定せず、デバイス上で暗号化がイネーブルの場合、暗号化されたパスワードが表示されます。
- **password password** コマンドに **hidden** キーワードが含まれていた場合、16進数の秘密キーが表示されます。

次に、**show vtp devices** コマンドの出力例を示します。**Conflict** 列の **Yes** は、応答するサーバがその機能のローカルサーバと競合していることを示します。つまり、同じドメイン内の2つのデバイスは、データベースに対して同じプライマリサーバを持ちません。

```
Device# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf Device ID      Primary Server Revision  System Name
-----
VLAN      Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST       No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次に、**show vtp counters** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device> show vtp counters
VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received      : 0
Summary advertisements transmitted  : 0
Subset advertisements transmitted    : 0
Request advertisements transmitted    : 0
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received      Summary advts received from
-----
Gi1/0/47       0                0                0
Gi1/0/48       0                0                0
Gi2/0/1        0                0                0
Gi3/0/2        0                0                0
```

表 26 : show vtp counters のフィールドの説明

フィールド	説明
Summary advertisements received	トランクポート上でこのデバイスが受信するサマリーアドバタイズメントの数。サマリーアドバタイズには、管理ドメイン名、コンフィギュレーションリビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセットアドバタイズメントの数が含まれます。
Subset advertisements received	トランクポート上でこのデバイスが受信するサブセットアドバタイズメントの数。サブセットアドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements received	トランクポート上でこのデバイスが受信するアドバタイズメント要求の数。アドバタイズメント要求は、通常、すべての VLAN に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Summary advertisements transmitted	トランクポート上でこのデバイスが送信するサマリーアドバタイズメントの数。サマリーアドバタイズには、管理ドメイン名、コンフィギュレーションリビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセットアドバタイズメントの数が含まれます。
Subset advertisements transmitted	トランクポート上でこのデバイスが送信するサブセットアドバタイズメントの数。サブセットアドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements transmitted	トランクポート上でこのデバイスが送信するアドバタイズメント要求の数。アドバタイズメント要求は、通常、すべての VLAN に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。

フィールド	説明
Number of configuration revision errors	<p>リビジョン エラーの数。</p> <p>新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、デバイスのコンフィギュレーション リビジョン番号が増加します。</p> <p>リビジョン番号がデバイスのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズメントをデバイスが受信すると、リビジョンエラーが増加します。このエラーは、2つのデバイスの VTP パスワードが異なるか、またはデバイスの設定が異なることを意味します。</p> <p>これらのエラーは、デバイスが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。</p>
Number of configuration digest errors	<p>MD5 ダイジェスト エラーの数。</p> <p>サマリーパケット内の MD5 ダイジェストと、デバイスによって計算された受信済みアドバタイズメントの MD5 ダイジェストが一致しない場合は、ダイジェストエラーが増加します。このエラーは、通常、2つのデバイスの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのデバイスで VTP パスワードが同じになるようにします。</p> <p>これらのエラーは、デバイスが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。</p>

フィールド	説明
Number of V1 summary errors	バージョン 1 エラーの数。 VTP V2 モードのデバイスが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリーエラーが増加します。これらのエラーは、少なくとも 1 つの近接デバイスで、V2 モードがディセーブルにされた VTP バージョン 1、または VTP バージョン 2 が実行されていることを示しています。この問題を解決するには、VTP V2 モードのデバイスの設定をディセーブルに変更します。
Join Transmitted	トランク上で送信された VTP プルーニングメッセージの数。
Join Received	トランク上で受信された VTP プルーニングメッセージの数。
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリーメッセージの数。

次に、**show vtp status** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Device> show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 1
VTP Domain Name         :
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIINO (first layer3 interface found
)

Feature VLAN:
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 7
Configuration Revision  : 2
MD5 digest              : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                        : 0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

表 27: **show vtp status** のフィールドの説明

フィールド	説明
VTP Version capable	デバイス上で動作できる VTP バージョンを表示します。

フィールド	説明
VTP Version running	デバイス上で動作中の VTP バージョンを表示します。デフォルトでは、デバイスはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
VTP Domain Name	デバイスの管理ドメインを特定する名前。
VTP Pruning Mode	プルニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルニングをイネーブルにすると、管理ドメイン全体でプルニングが有効になります。プルニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラグディングトラフィックが制限されます。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
Device ID	ローカル デバイスの MAC アドレスを表示します。
Configuration last modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったデバイスの IP アドレスを表示します。

フィールド	説明
VTP Operating Mode	<p>VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。</p> <p>Server : VTP サーバモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信します。スイッチで VLAN を設定できます。このデバイスを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべてのデバイスが VTP サーバです。</p> <p>（注） デバイスが設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバモードに戻ることができない場合、スイッチは VTP サーバモードから VTP クライアントモードに自動的に変わります。</p> <p>Client : VTP クライアントモードのデバイスは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。</p> <p>Transparent : VTP トランスペアレントモードのデバイスは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定にも影響しません。デバイスは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランクポートを除くすべてのトランクポートにこれを転送します。</p>
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数。
Number of Existing VLANs	既存の VLAN 数。

フィールド	説明
Configuration Revision	このデバイスの現在のコンフィギュレーションリビジョン番号。
MD5 Digest	VTP 設定の 16 バイト チェックサム。

次の例では、VTP バージョン 3 を実行するデバイスに対する **show vtp status** コマンドの出力を示します。

```

Device# show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Cisco
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0cd9.9624.dd80

Feature VLAN:
-----
VTP Operating Mode      : Off
Number of existing VLANs : 11
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 1005

Feature MST:
-----
VTP Operating Mode      : Transparent

Feature UNKNOWN:
-----
VTP Operating Mode      : Transparent

```

switchport priority extend

着信したタグなしフレームのポートプライオリティ、または指定されたポートに接続された IP フォンが受信するフレームのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **switchport priority extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {cos value | trust}
no switchport priority extend

構文の説明

cos value	PC から受信したか、または指定した Class of Service (CoS) 値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ~ 7 です。7 が最も高いプライオリティです。デフォルトは 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

コマンド デフォルト

ポートで受信したタグなしフレームには、デフォルト ポート プライオリティは、CoS 値 0 で設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、デバイスを設定して、Cisco Discovery Protocol (CDP) パケットを送信し、Cisco IP 電話のアクセスポートに接続される装置からデータパケットを送信する方法を IP 電話に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続しているスイッチ ポートの CDP をイネーブルにする必要があります (デフォルトでは、CDP はすべてのデバイスインターフェイスでグローバルにイネーブルです)。

スイッチアクセスポート上で音声 VLAN を設定する必要があります。

音声 VLAN をイネーブルにする前に、**mls qos** 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デバイス上で Quality of Service (QoS) をイネーブルに設定し、さらに **mls qos trust cos** 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ポートの信頼状態を **trust** に設定しておくことを推奨します。

次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport priority extend trust
```

設定を確認するには、**show interfaces *interface-id* switchport** 特権 EXEC コマンドを入力します。

switchport trunk

インターフェイスがトランキングモードの場合、トランクの特性を設定するには、インターフェイス コンフィギュレーションモードで **switchport trunk** コマンドを使用します。トランキング特性をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

```
switchport trunk {allowed vlan vlan-list | native vlan vlan-id | pruning vlan vlan-list }
no switchport trunk {allowed vlan | native vlan | pruning vlan }
```

構文の説明

allowed vlan *vlan-list* トランキングモードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可 VLAN のリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。

native vlan *vlan-id* インターフェイスが IEEE 802.1Q トランキングモードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ~ 4094 です。

pruning vlan *vlan-list* トランキングモードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。
すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

vlan-list の形式は、**all | none | [add | remove | except] *vlan-atom* [,*vlan-atom*...]** です。:

- **all** 1 ~ 4094 のすべての VLAN を指定します。これはデフォルトです。このキーワードは、リストのすべての VLAN を同時に設定することを許可しないコマンド上では使用できません。
- **none** 空のリストを指定します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** リストを置き換えるのではなく、現在設定されている VLAN に VLAN の定義済みリストを追加します。有効な ID は 1 ~ 1005 です。場合によっては、拡張範囲 VLAN (VLAN ID が 1005 より上) を使用できます。



-
- (注) 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。
-

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **remove** リストを置き換えるのではなく、現在設定されている VLAN から VLAN の定義済みリストを削除します。有効な ID は 1 ~ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。



-
- (注) 許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。
-

- **except** 定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定されている VLAN 以外の VLAN が追加されます）。有効な ID の範囲は 1 ~ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **vlan-atom** は、1 ~ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

ネイティブ VLAN :

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブモード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN :

- スパニングツリーループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol (CDP)、ポート集約プロトコル (PAgP)、Link Aggregation Control Protocol (LACP)、ダイナミック トランッキング プロトコル (DTP)、および VLAN 1 の VLAN トランッキング プロトコル (VTP)) を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルトリスト（すべての VLAN を許可）にリセットします。

トランク プルーニング :

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLANをプルーニングしない場合は、プルーニング適格リストから VLANを削除します。プルーニング不適格の VLAN は、フラッドイング トラフィックを受信します。
- VLAN 1、VLAN 1002 ~ 1005、および拡張範囲 VLAN (VLAN 1006 ~ 4094) は、プルーニングできません。

次の例では、すべてのタグなしトラフィックを送信するポートのデフォルトとして、VLAN 3 を設定する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ~ 15 を削除する方法を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces interface-id switchport** 特権 EXEC コマンドを入力します。

switchport voice vlan

ポートに音声 VLAN を設定するには、インターフェイス コンフィギュレーション モードで **switchport voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
switchport voice vlan {vlan-id | dot1p | none | untagged | name vlan_name}
no switchport voice vlan
```

構文の説明	
vlan-id	音声トラフィックに使用する VLAN。指定できる範囲は 1～4094 です。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0 (ネイティブ VLAN) を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキーパッドから入力された設定を使用します。
untagged	タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
name vlan_name	(任意) 音声トラフィックに使用する VLAN 名を指定します。最大 128 文字を入力できます。

コマンド デフォルト デフォルトでは、IP Phone を自動設定しません (**none**)。
デフォルトでは、IP Phone はフレームにタグを付けません。

コマンド モード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

デバイスの Cisco IP 電話に接続しているスイッチポート上の Cisco Discovery Protocol (CDP) をイネーブルにし、Cisco IP 電話に設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** 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スイッチ上で Quality of Service (QoS) をイネーブルに設定し、さらに **mls qos trust cos** 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ポートの信頼状態を **trust** に設定しておくことを推奨します。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。デバイスは IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1p、**none**、または **untagged** を選択した場合、デバイスは指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポートセキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

アクセス VLAN で任意のポートセキュリティタイプがイネーブルにされた場合、音声 VLAN でダイナミックポートセキュリティは自動的にイネーブルになります。

音声 VLAN には、スタティックセキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

次の例では、最初に VLANID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセスモードにあるインターフェイス上の VLAN を設定します（名前を使用）。設定を確認するには、特権 EXEC コマンドで **show interfaces interface-id switchport** を入力して、Voice VLAN: 行の情報を調べます。

パート 1 - VLAN データベースに入力する

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

パート 2 - VLAN データベースを確認する

```
Device# show vlan id 55
VLAN Name Status Ports
-----
55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----
```

パート 3 - VLAN 名を使用して VLAN をインターフェイスに割り当てる

```

Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#

```

パート 4 - 設定を確認する

```

Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#

```

パート 5 - インターフェイス スイッチポートでも確認できる

```

Device# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#

```

vlan

VLAN を追加して、VLAN コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan *vlan-id*
no vlan *vlan-id*

構文の説明	<i>vlan-id</i> 追加および設定する VLAN の ID。指定できる範囲は 1 ~ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。
コマンド デフォルト	なし
コマンド モード	グローバル コンフィギュレーション
コマンド履歴	リリース 変更内容 Cisco IOS Release 15.2(7)E3k このコマンドが導入されました。

使用上のガイドライン 最大 256 の VLAN がサポートされます。

通常範囲の VLAN (VLAN ID 1 ~ 1005) や拡張範囲 VLAN (VLAN ID 1006 ~ 4094) を追加するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。通常範囲の VLAN の設定情報は常に VLAN データベースに保存されます。この情報を表示するには、**show vlan** 特権 EXEC コマンドを入力します。VTP バージョン 1 および 2 を使用する場合、拡張範囲 VLAN は VTP によって認識されず、VLAN データベースに追加されません。VTP バージョン 1 およびバージョン 2 を使用する場合は、拡張範囲 VLAN を追加する前に、**vtp transparent** 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デバイスを VTP トランスペアレントモードにする必要があります。VTP モードがトランスペアレントである場合、VTP モードとドメイン名およびすべての VLAN 設定は実行コンフィギュレーションに保存されますが、この情報をデバイスのスタートアップ コンフィギュレーション ファイルに保存することもできます。

VTP バージョン 3 は拡張範囲 VLAN の伝播をサポートしているため、それらを VTP サーバまたはクライアント モードで作成できます。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ~ 1005 だけです。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存してデバイスをリブートすると、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ)、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定

が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。

- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1～1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

VTP バージョン 1 およびバージョン 2 では、デバイスが VTP トランスペアレントモードではない場合に拡張範囲 VLAN を作成しようとする、VLAN は拒否され、エラーメッセージが表示されます。

無効な VLAN ID を入力すると、エラーメッセージが表示され、VLAN コンフィギュレーションモードを開始できません。

VLAN ID を指定して **vlan** コマンドを入力すると、VLAN コンフィギュレーションモードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーションモードを終了したときに追加または変更されます。(VLAN 1～1005 の) **shutdown** コマンドだけがただちに有効になります。



- (注) すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされる VLAN コンフィギュレーション コマンドは **remote-span** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。

次のコンフィギュレーション コマンドを VLAN コンフィギュレーションモードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

- **are are-number** : この VLAN の全ルートエクスプローラ (ARE) ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0～13 です。デフォルト値は 7 です。値が入力されない場合、最大数は 0 であると見なされます。
- **backupcrf** : バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
 - **enable** : この VLAN のバックアップ CRF モード。
 - **disable** : この VLAN のバックアップ CRF モード (デフォルト)。
- **bridge {bridge-number | type}** : 論理分散ソース ルーティングブリッジ、つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0～15 です。FDDI-NET、TrBRF、およびトークンリング NET VLAN については、デフォルトのブリッジ番号は 0 (ソースルーティングブリッジなし) です。 **type** キーワードは、TrCRF VLAN だけに適用され、次のうちのいずれかです。
 - **srb** : ソースルートブリッジング。

- **srt** : (ソースルート トランスペアレント) ブリッジング VLAN
- **exit** : 変更を適用し、VLAN データベース リビジョン番号 (VLAN 1 ~ 1005) を増加させ、VLAN コンフィギュレーション モードを終了します。
- **media** : VLAN メディア タイプを定義します。タイプは次のいずれかになります。



(注) デバイスがサポートするのは、イーサネットポートだけです。FDDI およびトークンリングメディア固有の特性は、別のデバイスに対する VLAN Trunking Protocol (VTP) グローバルアドバタイズメントに限って設定します。これらの VLAN はローカルに停止されます。

- **ethernet** : イーサネット メディア タイプ (デフォルト)。
- **fd-net** : FDDI ネットワーク エンティティ タイトル (NET) メディア タイプ。
- **fddi** : FDDI メディア タイプ。
- **tokenring** : VTP v2 モードがディセーブルの場合は、トークンリング メディア タイプ。VTP バージョン 2 (v) モードがイネーブルの場合は、TrCRF。
- **tr-net** : VTP v2 モードがディセーブルの場合は、トークンリング ネットワーク エンティティ タイトル (NET) メディア タイプ。VTP v2 モードがイネーブルの場合は、TrBRF メディア タイプ。

さまざまなメディアタイプで有効なコマンドおよび構文については、下の表を参照してください。

- **mtu** *mtu-size* : 最大伝送単位 (MTU) (バイト単位のパケットサイズ) を指定します。指定できる範囲は 576 ~ 18190 です。デフォルトは 1500 バイトです。
- **name** *vlan-name* : 管理ドメイン内で一意である 1 ~ 32 文字の ASCII 文字列で VLAN に名前を付けます。デフォルトは VLANxxxx です。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字 (先行ゼロを含む) です。
- **no** : コマンドを無効にするか、またはデフォルト設定に戻します。
- **parent** *parent-vlan-id* : 既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定しますこのパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときが必要です。指定できる範囲は 0 ~ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0 (親 VLAN なし) です。トークンリングおよび TrCRF VLAN の両方で、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
- **ring** *ring-number* : FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ~ 4095 です。トークンリング VLAN のデフォルト値は 0 です。FDDI VLAN には、デフォルト設定はありません。

- **said** *said-value* : IEEE 802.10に記載されているセキュリティアソシエーションID (SAID) を指定します。指定できるIDは、1～4294967294です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000にVLAN ID番号を加算した値です。
- **shutdown** : VLAN上でVLANスイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLANコンフィギュレーションモードを終了したときに有効になります。
- **state** : VLANの状態を指定します。
 - **active** VLANが稼働中であることを意味します（デフォルト）。
 - **suspend** VLANが停止していることを意味します。停止しているVLANはパケットを通過させません。
- **ste** *ste-number* : スパニングツリーエクスプローラ (STE) ホップの最大数を定義します。このキーワードは、TrCRF VLANだけに適用されます。指定できる範囲は0～13です。デフォルト値は7です。
- **stp type** : FDDI-NET、トークンリングNET、またはTrBRF VLANのスパニングツリータイプを定義します。FDDI-NET VLANの場合、デフォルトのSTPタイプはieeeeです。トークンリングNET VLANの場合、デフォルトのSTPタイプはibmです。FDDIおよびトークンリングVLANの場合、デフォルトのタイプは指定されていません。
 - **ieeee** : ソースルートトランスペアレント (SRT) ブリッジングを実行しているIEEEイーサネットSTP。
 - **ibm** : ソースルートブリッジング (SRB) を実行しているIBM STP。
 - **auto** : ソースルートトランスペアレント (SRT) ブリッジング (IEEE) およびソースルートブリッジング (IBM) の組み合わせを実行しているSTP。
- **tb-vlan1** *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id* : このVLANにトランスレーショナルブリッジングが行われている1番めおよび2番めのVLANを指定します。トランスレーショナルVLANは、たとえばFDDIまたはトークンリングをイーサネットに変換します。指定できる範囲は0～1005です。値が指定されないと、0 (トランスレーショナルブリッジングなし) と見なされます。

表 28: さまざまなメディアタイプで指定できるコマンドと構文

メディアタイプ	指定できる構文
イーサネット	name <i>vlan-name</i> , media ethernet , state { suspend active }, said <i>said-value</i> , mtu <i>mtu-size</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

メディア タイプ	指定できる構文
FDDI	name <i>vlan-name</i> , media <i>fddi</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> , media <i>fd-net</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> VTP v2 モードがディセーブルの場合は、 stp type を <i>auto</i> . に設定しないでください
Token Ring	VTP v1 モードはイネーブルです。 name <i>vlan-name</i> , media <i>tokenring</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
トークンリング コンセントレータ リレー機能 (TrCRF)	VTP v2 モードはイネーブルです。 name <i>vlan-name</i> , media <i>tokenring</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , bridge type { <i>srb</i> <i>srt</i> }, are <i>are-number</i> , ste <i>ste-number</i> , backupcrf { <i>enable</i> <i>disable</i> }, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
トークンリング NET	VTP v1 モードはイネーブルです。 name <i>vlan-name</i> , media <i>tr-net</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type { <i>ieee</i> <i>ibm</i> }, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
トークンリング ブリッジ リレー機能 (TrBRF)	VTP v2 モードはイネーブルです。 name <i>vlan-name</i> , media <i>tr-net</i> , state { <i>suspend</i> <i>active</i> }, said <i>said-value</i> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type { <i>ieee</i> <i>ibm</i> <i>auto</i> }, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

次の表に、VLAN の設定ルールを示します。

表 29: VLAN 設定ルール

設定	ルール
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	<p>すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。</p> <p>リング番号を指定します。このフィールドを空白のままにしないでください。</p> <p>TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1つのバックアップ コンセントレータ リレー機能 (CRF) だけをイネーブルにすることができます。</p>
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードがイネーブルの場合	<p>VLAN の STP タイプを auto に設定しないでください。</p> <p>このルールは、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。</p>

設定	ルール
<p>トランスレーショナルブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）</p>	<p>使用されるトランスレーショナルブリッジング VLAN ID は、すでにデータベースに存在している必要があります。</p> <p>（たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナルブリッジング VLAN ID にも、トランスレーショナルブリッジングパラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。</p> <p>コンフィギュレーションがポイントするトランスレーショナルブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なるメディアタイプである必要があります。</p> <p>両方のトランスレーショナルブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なるメディアタイプである必要があります。</p>

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには VLAN xxxx の *vlan-name* が含まれています。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの *media* は **ethernet** です。state は **active** です。デフォルトの *said-value* は、100000 に VLAN ID を加算した値です。mtu-size 変数は 1500、stp-type は **ieee** です。**exit** VLAN コンフィギュレーションコマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

次に、新しい VLAN をすべてデフォルトの特性で作成し、VLAN コンフィギュレーションモードを開始する例を示します。

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```

次に、新しい拡張範囲 VLAN をすべてデフォルトの特性で作成して、VLAN コンフィギュレーションモードを開始し、新しい VLAN をデバイスのスタートアップコンフィギュレーションファイルに保存する例を示します。

```
Device(config)# vtp mode transparent
Device(config)# vlan 2000
Device(config-vlan)# end
```

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

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

vtp (グローバル コンフィギュレーション)

VLAN トランッキングプロトコル (VTP) 設定の特性を設定するか、または変更するには、グローバル コンフィギュレーション モードで **vtp** コマンドを使用します。この設定を削除したりデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
vtp {domain domain-name | file filename | interface interface-name [only] | mode {client | off | server | transparent} [{mst | unknown | vlan}] | password password [{hidden | secret}] | pruning | version number}
no vtp {file | interface | mode [{client | off | server | transparent}] [{mst | unknown | vlan}] | password | pruning | version}
```

構文の説明

domain <i>domain-name</i>	VTP ドメイン名をスイッチの VTP 管理ドメインを識別する 1 ~ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file <i>filename</i>	VTP VLAN 設定が保存されている Cisco IOS ファイルシステム ファイルを指定します。
interface <i>interface-name</i>	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	(任意) VTP IP アップデータとしてこのインターフェイスの IP アドレスだけを使用します。
mode	VTP デバイス モードをクライアント、サーバ、またはトランスペアレントに指定します。
client	スイッチを VTP クライアントモードにします。VTP クライアントモードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信できますが、VLAN 設定を格納するために必要な不揮発性メモリがありません。VTP クライアントでは、VLAN を設定できません。VLAN は、ドメインに含まれる、他のサーバモードのスイッチで設定します。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	スイッチを VTP オフモードにします。VTP オフモードのスイッチは、トランクポート上で VTP アドバタイズメントを転送しないことを除いて、VTP トランスペアレントデバイスと同様に機能します。
server	スイッチを VTP サーバモードにします。VTP サーバモードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチでは VLAN を設定できます。スイッチは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。

transparent	<p>スイッチを VTP トランスペアレントモードにします。VTP トランスペアレントモードのスイッチは、VTP に対してディセーブルであり、アドバタイズを送信や、他のデバイスから送信されたアドバタイズからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。</p> <p>VTP モードがトランスペアレントである場合、モードおよびドメイン名はデバイスの実行コンフィギュレーションファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーションファイルに保存するには、copy running-config startup config 特権 EXEC コマンドを入力します。</p>
mst	(任意) マルチスパンニングツリー (MST) VTP データベース (VTP バージョン 3 に限る) にモードを設定します。
unknown	(任意) 未知の VTP データベース (VTP バージョン 3 に限る) にモードを設定します。
vlan	(任意) VLAN VTP データベースにモードを設定します。これがデフォルトです (VTP バージョン 3 に限る)。
password password	VTP アドバタイズメントで送信され、受信 VTP アドバタイズメントを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメインパスワードを設定します。パスワードは、1 ~ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	(任意) パスワード文字列から生成されたキーが VLAN データベース ファイルに保存されることを指定します。 hidden キーワードを指定しない場合、パスワード文字列はクリアテキストに保存されます。 hidden パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを実行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	(任意) ユーザがパスワードの秘密キーを直接設定できるようにします (VTP バージョン 3 に限る)。
pruning	デバイス上で VTP プルーニングをイネーブルにします。
version number	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

コマンド デフォルト

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードはトランスペアレントです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。
 プルーニングはディセーブルです。
 デフォルトのバージョンはバージョン 1 です。

コマンドモード	グローバル コンフィギュレーション
---------	-------------------

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン VTP バージョン 3 がサポートされるのは、スイッチで LAN Base イメージが実行されている場合のみです。

VTP モード、ドメイン名、および VLAN 設定をデバイスのスタートアップ コンフィギュレーションファイルに保存して、デバイスを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーションファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され (クリアされ)、スタートアップ コンフィギュレーションファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ~ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

新規データベースをロードするのに **vtp file filename** を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、デバイスは非管理ドメインステートの状態です。非管理ドメインステートの間は、ローカル VLAN 設定に変更が生じて、デバイスは VTP アドバタイズメントを送信しません。デバイスは、トランッキングを行っているポートで最初の VTP サマリーパケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメインステートから抜け出します。装置がサマリーパケットからドメインを受け取る場合は、コンフィギュレーションリビジョン番号が 0 にリセットされます。デバイスが非管理ドメインステートから抜け出したあと、NVRAM をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てることがありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、デバイスを VTP サーバモードに戻すことができません。
- **vtp mode server** コマンドは、デバイスがクライアントモードまたはトランスペアレントモードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。
- 受信デバイスがクライアントモードである場合、クライアントデバイスはその設定を変更して、サーバの設定をコピーします。クライアントモードのデバイスがある場合には、必ずサーバモードのデバイスですべての VTP または VLAN 設定変更を行ってください。サーバモードのデバイスの方が、保持している VTP コンフィギュレーションリビジョン番号が大きいためです。受信デバイスがサーバモードまたはトランスペアレントモードである場合、そのデバイスの設定は変更されません。
- トランスペアレントモードのデバイスは、VTP に参加しません。トランスペアレントモードのデバイスで VTP または VLAN 設定の変更を行った場合、その変更はネットワーク内の他のデバイスには伝播されません。
- サーバモードのデバイスで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのデバイスに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、デバイスからドメインを削除しません。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーションファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。VTP は拡張範囲 VLAN をクライアントおよびサーバモードでサポートし、VLAN データベースに保存します。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN がデバイスで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラーメッセージが表示され、その設定は許可されません。VTP モードは、VTP バージョン 3 で拡張 VLAN を使用することにより変更できます。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーションファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバモードまたはクライアントモードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスを VTP サーバモードにリセットします。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードは大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのデバイスで一致している必要があります。

- デバイスをパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。
- **hidden** および **secret** キーワードは、VTP バージョン 3 だけでサポートされています。VTP バージョン 2 から VTP バージョン 3 に変換する場合、変換前に **hidden** または **secret** キーワードを削除する必要があります。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ~ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2 (v2) モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP デバイスは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP デバイスでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するように設定する必要があります。
- ドメイン内のすべてのデバイスが VTP バージョン 2 対応である場合、1 つのデバイスでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応デバイスに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function (TrBRF) または Token Ring Concentrator Relay Function (TrCRF) VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報がその VTP ドメイン全体に伝播します。
- VTP バージョン 3 の 2 つのリージョンが、VTP バージョン 1 または VTP バージョン 2 のリージョン経由で通信できるのは、トランスペアレントモードの場合に限られます。

デバイス コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

次の例では、VTP コンフィギュレーションストレージのファイル名を `vtpfilename` に変更する方法を示します。

```
Device(config)# vtp file vtpfilename
```

次の例では、デバイスストレージのファイル名をクリアする方法を示します。

```
Device(config)# no vtp file vtpconfig  
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Device(config)# vtp interface gigabitethernet
```

次の例では、デバイスの管理ドメインを設定する方法を示します。

```
Device(config)# vtp domain OurDomainName
```

次の例では、デバイスを VTP トランスペアレントモードにする方法を示します。

```
Device(config)# vtp mode transparent
```

次の例では、VTP ドメインパスワードを設定する方法を示します。

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

次の例では、VLAN データベースでのプルーンングをイネーブルにする方法を示します。

```
Device(config)# vtp pruning  
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Device(config)# vtp version 2
```

設定を確認するには、`show vtp status` 特権 EXEC コマンドを入力します。

vtp (インターフェイス コンフィギュレーション)

ポート単位で VLAN Trunking Protocol (VTP) をイネーブルにするには、インターフェイス コンフィギュレーション モードで **vtp** コマンドを使用します。インターフェイスで VTP 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。

vtp
no vtp

構文の説明 このコマンドには引数またはキーワードはありません。

コマンドデフォルト なし

コマンドモード インターフェイス コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン このコマンドは、トランキング モードのインターフェイスでのみ入力してください。このコマンドは、デバイスが LAN Base イメージ および VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

```
Device(config-if)# vtp
```

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

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

vtp primary

デバイスを VLAN Trunking Protocol (VTP) プライマリサーバとして設定するには、特権 EXEC モードで **vtp primary** コマンドを使用します。

vtp primary [{mst | vlan}] [force]

構文の説明

mst	(任意) デバイスをマルチスパンニングツリー (MST) 機能のプライマリ VTP サーバとして設定します。
vlan	(任意) デバイスを VLAN のプライマリ VTP サーバとして設定します。
force	(任意) プライマリサーバを設定するときにデバイスが競合するデバイスをチェックしないように設定します。

コマンド デフォルト

デバイスは VTP セカンダリサーバです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	このコマンドが導入されました。

使用上のガイドライン

VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバは、プライマリ サーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることだけができます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバのステータスは、管理者がドメイン内のテイクオーバーメッセージを発行する場合のデータベースアップデートのためだけに必要です。プライマリ サーバなしで実用 VTP ドメインを持つことができます。

デバイスがリロードするかドメインパラメータが変更された場合、プライマリ サーバのステータスは失われます。



(注) このコマンドは、デバイスが VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、デバイスを VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
Device# vtp primary vlan  
Setting device to VTP TRANSPARENT mode.
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

