



Cisco NCS 5000 シリーズ ルータ IP アドレスおよびサービス コマンド リファレンス

初版：2015年12月23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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



目次

はじめに ix

マニュアルの変更履歴 ix

マニュアルの入手方法およびテクニカル サポート ix

アクセス リスト コマンド 1

clear access-list ipv4 2

copy access-list ipv4 5

deny (IPv4) 7

ipv4 access-group 18

ipv4 access-list 20

ipv4 access-list log-update rate 22

ipv4 access-list log-update threshold 24

permit (IPv4) 26

remark (IPv4) 47

resequence access-list ipv4 49

show access-lists afi-all 51

show access-lists ipv4 52

show pfilter-ea 58

ARP コマンド 61

arp 62

arp dagr 64

arp gratuitous ignore 65

arp purge-delay 66

arp timeout 68

clear arp-cache 70

local-proxy-arp 72

peer (DAGR) 74

priority-timeout 75

proxy-arp	77
route distance	79
route metric	81
show arp	83
show arp dagr	87
show arp traffic	88
timers (DAGR)	91
シスコ エクスプレス フォワーディング コマンド	93
clear cef ipv4 drops	95
clear cef ipv4 exceptions	97
clear cef ipv6 drops	99
clear cef ipv6 exceptions	101
show adjacency	103
show cef	106
show cef ipv4	108
show cef ipv4 adjacency	110
show cef ipv4 drops	113
show cef ipv4 hardware	116
show cef ipv4 exact-route	119
show cef ipv4 exceptions	121
show cef ipv4 resource	123
show cef ipv4 summary	125
show cef ipv4 unresolved	128
show cef ipv6	130
show cef ipv6 adjacency	134
show cef ipv6 adjacency hardware	138
show cef ipv6 drops	141
show cef ipv6 exact-route	144
show cef ipv6 exceptions	147
show cef ipv6 hardware	149
show cef ipv6 interface	151
show cef ipv6 resource	154
show cef ipv6 summary	156
show cef ipv6 unresolved	158
show cef mpls adjacency	160

show cef mpls adjacency hardware	163
show cef mpls interface	165
show cef mpls unresolved	168
show cef summary	170
ホスト サービスおよびアプリケーション コマンド	173
cinetd rate-limit	175
clear host	176
destination address (ipsla)	178
domain ipv4 host	180
domain ipv6 host	182
domain list	184
domain lookup disable	186
domain name (IPAddr)	187
domain name-server	188
ftp client anonymous-password	190
ftp client passive	191
ftp client password	193
ftp client source-interface	195
ftp client username	197
logging source-interface	198
ping (ネットワーク)	200
ping bulk (ネットワーク)	203
scp	205
show cinetd services	207
show hosts	209
telnet	211
telnet client source-interface	215
telnet dscp	217
telnet server	219
telnet transparent	221
tftp client source-interface	222
tftp server	224
traceroute	226
LPTS コマンド	231
clear lpts ifib statistics	232

clear lpts pifib statistics	233
show lpts bindings	234
show lpts clients	239
show lpts flows	241
show lpts ifib	245
show lpts ifib slices	249
show lpts ifib statistics	252
show lpts ifib times	254
show lpts pifib	256
show lpts pifib hardware police	261
show lpts pifib hardware usage	264
show lpts pifib statistics	266
show lpts port-arbitrator statistics	268
ネットワーク スタック IPv4 および IPv6 コマンド	271
clear ipv6 neighbors	273
icmp ipv4 rate-limit unreachable	275
ipv4 address (ネットワーク)	277
ipv4 assembler max-packets	280
ipv4 assembler timeout	281
ipv4 mask-reply	283
ipv4 conflict-policy	284
ipv4 mtu	286
ipv4 unnumbered (point-to-point)	288
ipv6 address	290
ipv6 assembler	292
ipv6 conflict-policy	294
ipv6 address link-local	296
ipv6 enable	298
ipv6 hop-limit	300
ipv6 icmp error-interval	301
ipv6 mtu	303
ipv6 nd dad attempts	305
ipv6 nd managed-config-flag	308
ipv6 nd ns-interval	310
ipv6 nd other-config-flag	312

ipv6 nd prefix	314
ipv6 nd ra-interval	317
ipv6 nd ra-lifetime	319
ipv6 nd reachable-time	321
ipv6 nd redirects	323
ipv6 nd scavenge-timeout	324
ipv6 nd suppress-ra	325
ipv6 neighbor	327
ipv6 path-mtu enable	330
ipv6 path-mtu timeout	331
ipv6 source-route	332
ipv6 tcp-mss-adjust	334
ipv6 virtual address	336
show arm conflicts	338
show arm registrations producers	341
show arm router-ids	343
show arm summary	345
show ipv4 interface	347
show ipv4 traffic	351
show ipv6 interface	354
show ipv6 neighbors	359
show ipv6 neighbors summary	365
show ipv6 path-mtu	366
show ipv6 traffic	368
プレフィックス リスト コマンド	371
clear prefix-list ipv4	372
copy prefix-list ipv4	374
deny (プレフィックス リスト)	376
ipv4 prefix-list	379
permit (プレフィックス リスト)	381
remark (プレフィックス リスト)	384
resequence prefix-list ipv4	386
show prefix-list afi-all	388
show prefix-list	389
show prefix-list ipv4	390

show prefix-list ipv4 standby	392
トランスポート スタック コマンド	395
clear raw statistics pcb	397
clear tcp pcb	399
clear tcp statistics	401
clear udp statistics	403
forward-protocol udp	405
service tcp-small-servers	407
service udp-small-servers	409
show raw brief	411
show raw detail pcb	413
show raw extended-filters	415
show raw statistics pcb	417
show tcp brief	420
show tcp detail	422
show tcp extended-filters	424
show tcp statistics	426
show udp brief	428
show udp detail pcb	430
show udp extended-filters	432
show udp statistics	434
tcp mss	436
tcp path-mtu-discovery	438
tcp selective-ack	440
tcp synwait-time	442
tcp timestamp	443
tcp window-size	444



はじめに

「はじめに」の内容は次のとおりです。

- マニュアルの変更履歴, ix ページ
- マニュアルの入手方法およびテクニカル サポート, ix ページ

マニュアルの変更履歴

表 1 に、初版後、このマニュアルに加えられた技術的な変更の履歴を示します。

表 1: マニュアルの変更履歴

日付	変更点
2015 年 12 月	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html> から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダーアプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。



アクセス リスト コマンド

このモジュールでは、IP バージョン 4 (IPv4) や IP バージョン 6 (IPv6) のアクセス リストを設定する際に使用する Cisco IOS XR ソフトウェアのコマンドについて説明します。

ACL の概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [clear access-list ipv4](#), 2 ページ
- [copy access-list ipv4](#), 5 ページ
- [deny \(IPv4\)](#), 7 ページ
- [ipv4 access-group](#), 18 ページ
- [ipv4 access-list](#), 20 ページ
- [ipv4 access-list log-update rate](#), 22 ページ
- [ipv4 access-list log-update threshold](#), 24 ページ
- [permit \(IPv4\)](#), 26 ページ
- [remark \(IPv4\)](#), 47 ページ
- [resequence access-list ipv4](#), 49 ページ
- [show access-lists afi-all](#), 51 ページ
- [show access-lists ipv4](#), 52 ページ
- [show pfilter-ea](#), 58 ページ

clear access-list ipv4

IPv4 アクセスリストカウンタをクリアするには、XR EXEC モードで **clear access-list ipv4** コマンドを使用します。

```
clear access-list ipv4access-list name[sequence-number] hardware {ingress| egress}] [interface type
interface-path-id][location node-id] sequence number]
```

構文の説明

<i>access-list-name</i>	特定の IPv4 アクセスリストの名前この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
<i>sequence-number</i>	(任意) アクセスリストのカウンタをクリアする特定のシーケンス番号。範囲は 1 ~ 2147483644 です。
hardware	アクセスリストを、インターフェイスのアクセスグループとして識別します。
ingress	着信方向を指定します。
egress	発信方向を指定します。
interface	(任意) インターフェイスの統計情報をクリアします。
<i>type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
location <i>node-id</i>	(任意) 指定したノードからのハードウェアリソースカウンタをクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
sequence <i>number</i>	(任意) 特定のシーケンス番号を持つアクセスリストのカウンタをクリアします。範囲は 1 ~ 2147483644 です。

コマンド デフォルト

デフォルトでは、指定された IPv4 アクセスリストがクリアされます。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

clear access-list ipv4 コマンドを使用すると、特定の設定済みアクセスリストのカウンタをクリアすることができます。シーケンス番号を使用すると、特定のシーケンス番号を持つアクセスリストのカウンタをクリアすることができます。

hardware キーワードを使用すると、**ipv4 access-group** コマンドによりイネーブルにしたアクセスリストのカウンタをクリアすることができます。

access-list-name 引数でアスタリスク (*) を使用すると、すべてのアクセスリストをクリアすることができます。



(注)

アクセスリストは、複数のインターフェイスで共有できます。ハードウェアカウンタをクリアすると、指定されたアクセスリストを指定された方向（入力または出力）で使用しているすべてのインターフェイスの全カウンタがクリアされます。

egress での ACL はリリース 6.0 ではサポートされていません

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
acl	読み取り、書き込み
bgp	読み取り、書き込み、実行

例

次の例では、*marketing* という名前のアクセスリストのカウンタがクリアされます。

```
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
ipv4 access-list marketing
 10 permit ip 192.168.34.0 0.0.0.255 any (51 matches)
 20 permit ip 172.16.0.0 0.0.255.255 any (26 matches)
 30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30 (5 matches)
RP/0/RP0/CPU0:router# clear access-list ipv4 marketing
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
```

clear access-list ipv4

```
ipv4 access-list marketing
 10 permit ip 192.168.34.0 0.0.0.255 any
 20 permit ip 172.16.0.0 0.0.255.255 any
 30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30
```

copy access-list ipv4

既存の IPv4 アクセスリストのコピーを作成するには、XR EXEC モードで **copy access-list ipv4** コマンドを使用します。

copy access-list ipv4 *source-acl destination-acl*

構文の説明

<i>source-acl</i>	コピー元のアクセス リストの名前
<i>destination-acl</i>	<i>source-acl</i> 引数の内容がコピーされる宛先のアクセス リストの名前

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

設定済みのアクセスリストをコピーするには、**copy access-list ipv4** コマンドを使用します。*source-acl* 引数を使用してコピー元のアクセス リストを指定し、*destination-acl* 引数を使用して、ソース アクセスリストの内容のコピー先を指定できます。*destination-acl* 引数は一意の名前でなければなりません。アクセス リストまたはプレフィックス リストを示す *destination-acl* 引数名が存在する場合、そのアクセス リストはコピーされません。**copy access-list ipv4** コマンドは、送信元アクセス リストが存在することをチェックしてから既存のリスト名をチェックし、既存のアクセス リストが上書きされないようにします。

タスク ID

タスク ID	動作
acl	読み取り、書き込み
filesystem	実行

例

次の例では、アクセスリスト list-1 のコピーが作成されます。

```
RP/0/RP0/CPU0:router# show access-lists ipv4 list-1
ipv4 access-list list-1
 10 permit tcp any any log
 20 permit ip any any
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RP0/CPU0:router# show access-lists ipv4 list-2
ipv4 access-list list-2
 10 permit tcp any any log
 20 permit ip any any
```

次の例では、アクセスリストの list-1 から list-3 へのコピーが、list-3 のアクセスリストがすでに存在しているために拒否されています。

```
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-3
list-3 exists in access-list
RP/0/RP0/CPU0:router# show access-lists ipv4 list-3
ipv4 access-list list-3
 10 permit ip any any
 20 deny tcp any any log
```

deny (IPv4)

IPv4 アクセスリストの拒否条件を設定するには、アクセスリストコンフィギュレーションモードで **deny** コマンドを使用します。**deny** コマンドには、**deny** (送信元) および **deny** (プロトコル) の2つのバージョンがあります。アクセスリストから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。

```
[sequence-number] deny source [source-wildcard] counter counter-name[log log-input]
```

```
[sequence-number] denyprotocol source source-wildcard destination
destination-wildcard[precedenceprecedence] [dscpdscp] [fragments] [packet-length operator packet-length
value] [ log | log-input] [ttl value[value1....value2]] [counter counter-name]
```

```
no sequence-number
```

インターネット制御メッセージプロトコル (ICMP)

```
[sequence-number] deny icmp source source-wildcard destination destination-wildcard [ icmp-type ]
[ icmp-code ] [precedence precedence] [dscp dscp] [fragments] [log log-input] [counter
counter-name][icmp-off]
```

インターネットグループ管理プロトコル (IGMP)

```
[sequence-number] deny igmp source source-wildcard destination destination-wildcard [ igmp-type ]
[precedence precedence] [dscp value] [fragments] [log log-input] [counter counter-name]
```

ユーザデータグラムプロトコル (UDP)

```
[sequence-number] deny udp source source-wildcard [operator {port| protocol-port}] destination
destination-wildcard [operator {port| protocol-port}] [precedence precedence] [dscp dscp] [fragments]
[log log-input] [counter counter-name]
```

構文の説明

<i>sequence-number</i>	(任意) アクセスリスト中の deny ステートメントの番号。この番号により、アクセスリスト中のステートメントの順番を識別します。番号は1～2147483644です (デフォルトでは、1番目のステートメントの番号は10で、後続のステートメントの番号は10ずつ増加していきます)。設定されているアクセスリストの最初のステートメントの番号を変更して、以降のステートメントを増分するには、 resequence access-list コマンドを使用します。
------------------------	--

<i>source</i>	<p>パケットの送信元のネットワークまたはホストの番号。送信元を指定する場合、代わりに次の3つの方法を使用できます。</p> <ul style="list-style-type: none">• 32 ビットの4分割ドット付き10進表記を使用する。• any キーワードを、<i>source</i> および <i>source-wildcard</i> (0.0.0.0 255.255.255.255) の短縮形として使用します。• hostsource の組み合わせを、<i>source</i> および <i>source</i> の <i>source-wildcard</i> (0.0.0.0) の短縮形として使用します。
<i>source-wildcard</i>	<p>送信元に適用されるワイルドカードビット。送信元のワイルドカードを指定するには、次の3つの方法から選択します。</p> <ul style="list-style-type: none">• 32 ビットの4分割ドット付き10進表記を使用する。無視するビット位置に1を入れます。• any キーワードを、<i>source</i> および <i>source-wildcard</i> (0.0.0.0 255.255.255.255) の短縮形として使用します。• hostsource の組み合わせを、<i>source</i> および <i>source</i> の <i>source-wildcard</i> (0.0.0.0) 短縮形として使用します。
<i>protocol</i>	<p>IPプロトコルの名前または番号。これには、esp、eigrp、gre、icmp、igmp、igrp、ip、ipinip、nos、ospf、pim、pcp、tcp、udp のいずれかのキーワードを指定するか、IPプロトコル番号を示す0～255の整数を指定できます。任意のインターネットプロトコル (ICMP、TCP、UDP など) と一致させるには、ip キーワードを使用します。ICMP および TCP では、さらに、このテーブルの後半に記載されている修飾子を許可します。</p>
<i>destination</i>	<p>パケットの宛先のネットワークまたはホストの番号。宛先を指定するには、次の3つの方法から選択します。</p> <ul style="list-style-type: none">• 32 ビットの4分割ドット付き10進表記を使用する。• any キーワードを、<i>destination</i> および <i>destination-wildcard</i> (0.0.0.0 255.255.255.255) の短縮形として使用します。• hostdestination の組み合わせを、<i>destination</i> および <i>destination</i> の <i>destination-wildcard</i> (0.0.0.0) の短縮形として使用します。

destination-wildcard 宛先に適用されるワイルドカードビット。宛先のワイルドカードを指定するには、次の3つの方法から選択します。

- 32ビットの4分割ドット付き10進表記を使用する。無視するビット位置に1を入れます。
- **any** キーワードを、*destination* および *destination-wildcard* (0.0.0.0 255.255.255.255) の短縮形として使用します。
- **host***destination* の組み合わせを、*destination* および *destination* の *destination-wildcard* (0.0.0.0) の短縮形として使用します。

precedence*precedence* (任意) パケットは、precedence レベル (0～7の番号で指定) または次の名前でフィルタリングできます。

- **routine** : routine precedence (0) に一致するパケット
 - **priority** : priority precedence (1) に一致するパケット
 - **immediate** : immediate precedence (2) に一致するパケット
 - **flash** : flash precedence (3) に一致するパケット
 - **flash-override** : flash override precedence (4) に一致するパケット
 - **critical** : critical precedence (5) に一致するパケット
 - **internet** : internetwork control precedence (6) に一致するパケット
 - **network** : network control precedence (7) に一致するパケット
-

dscp*dscp*

(任意) DiffServ コードポイント (DSCP) により、Quality of Service のコントロールが提供されます。*dscp* の値は次のとおりです。

- **0–63** : DiffServ コードポイント値
- **af11** : パケットを AF11 dscp (001010) と一致させます。
- **af12** : パケットを AF12 dscp (001100) と一致させます。
- **af13** : パケットを AF13 dscp (001110) と一致させます。
- **af21** : パケットを AF21 dscp (010010) と一致させます。
- **af22** : パケットを AF22 dscp (010100) と一致させます。
- **af23** : パケットを AF23 dscp (010110) と一致させます。
- **af31** : パケットを AF31 dscp (011010) と一致させます。
- **af32** : パケットを AF32 dscp (011100) と一致させます。
- **af33** : パケットを AF33 dscp (011110) と一致させます。
- **af41** : パケットを AF41 dscp (100010) と一致させます。
- **af42** : パケットを AF42 dscp (100100) と一致させます。
- **af43** : パケットを AF43 dscp (100110) と一致させます。
- **cs1** : パケットを CS1 (precedence 1) dscp (001000) と一致させます。
- **cs2** : パケットを CS2 (precedence 2) dscp (010000) と一致させます。
- **cs3** : パケットを CS3 (precedence 3) dscp (011000) と一致させます。
- **cs4** : パケットを CS4 (precedence 4) dscp (100000) と一致させます。
- **cs5** : パケットを CS5 (precedence 5) dscp (101000) と一致させます。
- **cs6** : パケットを CS6 (precedence 6) dscp (110000) と一致させます。
- **cs7** : パケットを CS7 (precedence 7) dscp (111000) と一致させます。
- **default** : デフォルト DSCP (000000)。
- **ef** : パケットを EF dscp (101110) と一致させます。

fragments

(任意) このアクセスリスト エントリーを適用すると、ソフトウェアが IPv4 パケットのフラグメントを検査するようになります。このキーワードを指定すると、フラグメントがアクセス キーリスト エントリーによる制約を受けます。

log	<p>(任意) コンソールに送信されるエントリに一致するパケットに関するロギングメッセージ情報が出力されます。(コンソールに記録されるメッセージのレベルは logging console コマンドで制御します)。</p> <p>このメッセージに含まれるものには、アクセスリスト番号、パケットが許可されたか拒否されたか、プロトコルが TCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。このメッセージは、フローに一致した最初のパケットに対して生成され、5 分間隔で、前の 5 分間に許可または拒否されたパケット数を含みます。</p>
log-input	<p>(任意) ロギングメッセージに入力インターフェイスも含まれることを除き、log キーワードと同じ機能を果たします。</p>
ttl	<p>(任意) Time-To-Life (TTL) 値との一致をオンにします。</p>
ttl value [value1..value2]	<p>(任意) フィルタリングに使用される TTL 値の範囲は 1 ~ 255 です。 <i>value</i> が指定されている場合にのみ、この値と照合されます。 <i>value1</i> と <i>value2</i> の両方が指定されている場合は、<i>value1</i> と <i>value2</i> の間の TTL 範囲とパケット TTL が照合されます。</p>
icmp-off	<p>(任意) 拒否されたパケットに対して ICMP 生成をオフにします。</p>
icmp-type	<p>(任意) ICMP パケットのフィルタリングのための ICMP メッセージタイプ。範囲は 0 ~ 255 です。</p>
icmp-code	<p>(任意) ICMP パケットのフィルタリングのための ICMP メッセージコード。範囲は 0 ~ 255 です。</p>
igmp-type	<p>(任意) IGMP パケットをフィルタリングするための、IGMP メッセージタイプ (0 ~ 15) または次のようなメッセージ名。</p> <ul style="list-style-type: none">• dvmrp• host-query• host-report• mtrace• mtrace-response• pim• precedence• trace• v2-leave• v2-report• v3-report

<i>operator</i>	<p>(任意) 演算子は、送信元ポートまたは宛先ポートを比較するために使用されます。使用可能なオペランドは、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、および range (包含範囲) です。</p> <p>演算子を <i>source</i> と <i>source-wildcard</i> の値の後に置いた場合は、送信元ポートと照合されます。</p> <p>演算子を <i>destination</i> および <i>destination-wildcard</i> の値の後に置く場合、宛先ポートと一致する必要があります。</p> <p>演算子を ttl キーワードの後に置いた場合はと、TTL 値と照合されます。</p> <p>range 演算子には2つのポート番号が必要です。他のすべての演算子は1つのポート番号が必要です。</p>
<i>port</i>	<p>TCP または UDP ポートの 10 進数。ポート番号の範囲は 0 ~ 65535 です。</p> <p>TCP ポートは、TCP をフィルタリングする場合にだけ使用できます。UDP ポートは、UDP をフィルタリングする場合にだけ使用できます。</p>
<i>protocol-port</i>	<p>TCP または UDP ポートの名前。TCP および UDP ポートの名前は、「使用上のガイドライン」に示されています。</p> <p>TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。</p>
established	(任意) TCP プロトコルの場合にだけ、確立された接続を表示します。
match-any	(任意) TCP プロトコルの場合にだけ、TCP フラグの任意の組み合わせをフィルタリングします。
match-all	(任意) TCP プロトコルの場合にだけ、すべての TCP フラグをフィルタリングします。
+/-	(必須) TCP プロトコル match-any 、 match-all の場合 : <i>flag-name</i> の前に + または - を付けます。TCP フラグを設定してパケットと照合するには、+ <i>flag-name</i> 引数を使用します。TCP フラグを設定せずにパケットを照合するには、- <i>flag-name</i> 引数を使用します。
<i>flag-name</i>	(任意) TCP プロトコルが match-any 、 match-all の場合。フラグ名は次のとおりです。 ack 、 fin 、 psh 、 rst 、 syn 。
counter	(任意) SNMP クエリーを使用して ACL カウンタへのアクセスをイネーブルにします。
<i>counter-name</i>	ACL カウンタ名を定義します。

コマンド デフォルト IPv4 アクセス リストの送受信時にパケットが拒否される特定の条件はありません。

ICMP メッセージの生成はデフォルトでイネーブルです。

コマンドモード

IPv4 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

アクセスリストでパケットを拒否する条件を指定するには、**ipv4 access-list** コマンドの後ろに **deny** コマンドを使用します。

デフォルトでは、アクセス リストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力せずに、既存のアクセス リストに **permit**、**deny**、または **remark** ステートメントを追加できます。新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ 番号の間にある適切なエントリ 番号を持つ新しいステートメントを作成します。

番号が連続している 2 つのステートメントの間（たとえば、10 行と 11 行の間）にステートメントを追加する場合は、まず **resequence access-list** コマンドを使用して最初のステートメントの番号を付け直し、後続の各ステートメントの番号を増加させます。*increment* 引数を使用すると、ステートメント間に新しい未使用の行番号が生成されます。次に、アクセス リスト中の所属先を指定する *entry-number* 引数を持つ新しいステートメントを追加します。

次に、*precedence* の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

次に、ICMP メッセージ タイプの名前のリストを示します。

- administratively-prohibited
- alternate-address
- conversion-error

- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation

- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

次に、ポート番号の代わりに使用できる TCP ポート名のリストを示します。これらのプロトコルの参考情報については、現在の *Assigned Numbers RFC* を参照してください。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3

- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

次のUDPポート名は、ポート番号の代わり使用できます。これらのプロトコルの参考情報については、現在の *Assigned Numbers RFC* を参照してください。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk

- tftp
- time
- who
- xdmcp

次のフラグを **match-any** と **match-all** キーワードおよび+ と - 記号とともに使用すると、表示するフラグを選択できます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all+ack+syn** は、ack と syn の両方のフラグが設定されている TCP パケットを表示します。また、**match-any+ack-syn** は、ack が設定されている TCP パケットまたは syn が設定されていないが TCP パケットを表示します。



(注) ACL のいずれかの ACE に ABF 句が含まれている場合、その ACL はゼロ以外の圧縮レベルに適用できません。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次の例は、Internet filter という名前のアクセスリストに拒否条件を設定する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

ipv4 access-group

インターフェイスへのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **ipv4 access-group** コマンドを使用します。指定されたアクセス 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。

ipv4 access-group *access-list-name* {**ingress**|**egress**}

no ipv4 access-group *access-list-name* {**ingress**|**egress**}

構文の説明

access-list-name	ipv4 access-list コマンドで指定された IPv4 アクセス リストの名前。
ingress	インバウンドパケットに対してフィルタリングします。
egress	発信パケットをフィルタリングします。

コマンド デフォルト

インターフェイスには、適用される IPv4 アクセス リストがありません。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 access-group コマンドを使用すると、インターフェイスへのアクセスを制御することができます。指定されたアクセス 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。特定の IPv4 アクセス リストを指定するには、*access-list-name* 引数を使用します。着信パケットをフィルタリングするには **ingress** キーワードを使用し、発信パケットをフィルタリングするには **egress** キーワードを使用します。*hardware-count* 引数を使用すると、アクセス グループのハードウェア カウンタをイネーブルにすることができます。

インターフェイス ACL による MPLS パケットのフィルタリングはサポートされていません。

アクセスリストがアドレスを許可する場合は、ソフトウェア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、インターネット制御メッセージプロトコル (ICMP) ホスト到達不能メッセージを返します。

指定したアクセスリストが存在しない場合は、すべてのパケットが通過します。

タスク ID

タスク ID	動作
acl	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/0/0/2 の着信および発信パケットにフィルタリングを適用する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
```

次に、ハードウェア内のインターフェイス統計情報の適用方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
interface-statistics
```

ipv4 access-list

IPv4 アクセスリストを名前で定義するには、XR コンフィギュレーションモードで **ipv4 access-list** コマンドを使用します。IPv4 アクセスリストのすべての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。

ipv4 access-list name

no ipv4 access-list name

構文の説明

<i>name</i>	アクセスリストの名前。名前にはスペースや疑問符を使用できません。
-------------	----------------------------------

コマンド デフォルト

定義されている IPv4 アクセスリストはありません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 access-list コマンドは、IPv4 アクセスリストを設定するために使用します。このコマンドを指定すると、ルータはアクセスリスト コンフィギュレーションモードになります。このモードでは、アクセスを拒否または許可する条件を **deny** または **permit** コマンドを使用して定義する必要があります。

既存の IPv4 アクセスリストの連続しているエントリの間に **permit**、**deny**、または **remark** ステートメントを追加する場合は、**resequence access-list ipv4** コマンドを使用します。先頭のエントリ番号 (*base*) を指定し、ステートメントのエントリ番号を隔てるための増分を指定します。既存のステートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

アクセスリストをインターフェイスに適用するには、**ipv4 access-group** コマンドを使用します。

タスク ID

タスク ID	動作
acl	読み取り、書き込み

例 次に、Internetfilter という名前の標準アクセス リストを定義する方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter  
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255  
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255  
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255  
RP/0/RP0/CPU0:router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.  
RP/0/RP0/CPU0:router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203  
range 1300 1400
```

ipv4 access-list log-update rate

IPv4 アクセスリストが記録されるレートを指定するには、XR コンフィギュレーションモードで **ipv4 access-list log-update rate** コマンドを使用します。更新レートを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。

ipv4 access-list log-update rate rate-number

no ipv4 access-list log-update rate rate-number

構文の説明

<i>rate-number</i>	ルータ上で IPv4 アクセス ヒット ログが生成される毎秒のレート。範囲は 1 ~ 1000 です。
--------------------	---

コマンド デフォルト

デフォルト値は 1 です。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

rate-number 引数は、インターフェイスに設定されているすべての IPv4 アクセス リストに適用されます。つまり、システムに常に 1 ~ 1000 のログ エントリがあるということです。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次に、システムの IPv4 アクセス ヒット ロギング レートを設定する方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update rate 10
```

ipv4 access-list log-update threshold

IPv4 アクセスリストにロギングされるアップデートの数を指定するには、XR コンフィギュレーションモードで **ipv4 access-list log-update threshold** コマンドを使用します。ロギングの更新数を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。

ipv4 access-list log-update threshold *update-number*

no ipv4 access-list log-update threshold *update-number*

構文の説明

<i>update-number</i>	ルータに設定された IPv4 アクセスリストごとに記録される更新数。範囲は 0 ~ 2147483647 です。
----------------------	--

コマンド デフォルト

IPv4 アクセスリストの場合、2147483647 の更新が記録されます。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv4 アクセスリスト更新は、1 番目のロギング更新に続いて 5 分間隔で記録されます。ロギングをより頻繁に更新する場合は、更新数を小さく（デフォルトよりも小さい数）するほうが有益です。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
acl	読み取り、書き込み

例

次の例は、ルータに設定されている IPv4 アクセス リストごとに 10 のアップデートをロギングしきい値として設定する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

permit (IPv4)

IPv4 アクセスリストの条件を設定するには、アクセスリストコンフィギュレーションモードで **permit** コマンドを使用します。**permit** コマンドには、**permit** (送信元) と **permit** (プロトコル) の2つのバージョンがあります。アクセスリストから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。

```
[sequence-number] permit source [source-wildcard] [log|log-input]
```

```
[sequence-number] permit protocol net-group source-net-object-group-name destination
source-port-object-group-name net-group destination-net-object-group-name port-group
destination-port-object-group-name [capture][precedence precedence] [default nexthop1 [vrf vrf-name]
[ipv4 ipv4-address1 nexthop2 [vrf vrf-name] [ipv4 ipv4-address2 nexthop3 [vrf vrf-name] [ipv4
ipv4-address3]] [dscp dscp] [fragments] [log|log-input] [nexthop [track track-name]] [ttl ttl value [value1
... value2]] [counter counter-name]
```

```
[sequence-number] permit protocol net-group source-net-object-group-name
port-group source-port-object-group-name net-group
destination-net-object-group-name port-group destination-port-object-group-name [capture] [precedence
precedence] [default nexthop1 [vrf vrf-name] [ipv4 ipv4-address1] nexthop2 [vrf vrf-name] [ipv4
ipv4-address2] nexthop3 [vrf vrf-name] [ipv4 ipv4-address3]] [dscp range dscp dscp] [fragments] [log|
log-input] [nexthop [track track-name]] [ttl ttl value [value1 ... value2]] [counter counter-name]
```

```
no sequence-number
```

インターネット制御メッセージプロトコル (ICMP)

```
[ sequence-number ] permit icmp source source-wildcard destination destination-wildcard [ icmp-type ]
[ icmp-code ] [precedence precedence] [dscp dscp] [fragments] [log|log-input] [icmp-off][counter
counter-name]
```

インターネットグループ管理プロトコル (IGMP)

```
[ sequence-number ] permit igmp source source-wildcard destination destination-wildcard [ igmp-type ]
[precedence precedence] [dscp value] [fragments] [log|log-input][counter counter-name]
```

ユーザ データグラム プロトコル (UDP)

```
[ sequence-number ] permit udp source source-wildcard [operator {port|protocol-port}] destination
destination-wildcard [operator {port|protocol-port}] [precedence precedence] [dscp dscp] [fragments]
[log|log-input][counter counter-name]
```

構文の説明

sequence-number

(任意) アクセスリスト中の **permit** ステートメントの番号。この番号により、アクセスリスト中のステートメントの順番を識別します。範囲は 1 ～ 2147483644 です。(デフォルトでは、1 番目のステートメントの番号は 10 で、後続のステートメントの番号は 10 ずつ増加していきます)。設定されているアクセスリストの最初のステートメントの番号を変更して、以降のステートメントを増分するには、**resequence access-list** コマンドを使用します。

source

パケットの送信元のネットワークまたはホストの番号。送信元を指定する場合、代わりに次の 3 つの方法を使用できます。

- 32 ビットの 4 分割ドット付き 10 進表記を使用する。
 - **any** キーワードを、*source* および *source-wildcard* (0.0.0.255.255.255.255) の短縮形として使用します。
 - **hostsource** の組み合わせを、*source* および *source* の *source-wildcard* (0.0.0.0) の短縮形として使用します。
-

source-wildcard

送信元に適用されるワイルドカードビット。送信元のワイルドカードを指定するには、次の3つの方法から選択します。

- 32 ビットの 4 分割ドット付き 10 進表記を使用する。無視するビット位置に 1 を入れます。
- **any** キーワードを、*source* および *source-wildcard* (0.0.0.0 255.255.255.255) の短縮形として使用します。
- **host***source* の組み合わせを、*source* および *source* の *source-wildcard* (0.0.0.0) の短縮形として使用します。

protocol

IP プロトコルの名前または番号。これには、**esp**、**eigrp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pim**、**pcp**、**tcp**、**udp** のいずれかのキーワードを指定するか、IP プロトコル番号を示す 0 ~ 255 の整数を指定できます。任意のインターネットプロトコル (ICMP、TCP、UDP など) と一致させるには、**ip** キーワードを使用します。ICMP および TCP では、さらに、このテーブルの後半に記載されている修飾子を許可します。

destination

パケットの宛先のネットワークまたはホストの番号。宛先を指定するには、次の3つの方法から選択します。

- 32 ビットの 4 分割ドット付き 10 進表記を使用する。
- **any** キーワードを、*destination* および *destination-wildcard* (0.0.0.0 255.255.255.255) の短縮形として使用します。
- **hostdestination** の組み合わせを、*destination* および *destination* の *destination-wildcard* (0.0.0.0) の短縮形として使用します。

destination-wildcard

宛先に適用されるワイルドカードビット。宛先のワイルドカードを指定するには、次の3つの方法から選択します。

- 32 ビットの 4 分割ドット付き 10 進表記を使用する。無視するビット位置に 1 を入れます。
- **any** キーワードを、*destination* および *destination-wildcard* (0.0.0.0 255.255.255.255) の短縮形として使用します。
- **hostdestination** の組み合わせを、*destination* および *destination* の *destination-wildcard* (0.0.0.0) の短縮形として使用します。

precedence*precedence*

(任意) パケットは、**precedence** レベル (0 ~ 7 の番号で指定) または次の名前でフィルタリングできます。

- **Routine** : routine precedence
(0) に一致するパケット
- **priority** : priority precedence
(1) に一致するパケット
- **immediate** : immediate precedence (2) に一致するパケット
- **flash** : flash precedence
(3) に一致するパケット
- **flash-override** : flash override precedence (4) に一致するパケット
- **critical** : critical precedence
(5) に一致するパケット
- **internet** : internetwork control precedence (6) に一致するパケット
- **network** : network control precedence (7) に一致するパケット

default

(任意) このエントリのデフォルトのネクストホップを指定します。

default キーワードを設定すると、ACLベースの転送アクションが実行されるのは、パケットの宛先の PLU ルックアップの結果によってデフォルトルートを決める場合、つまり、パケット宛先のルートが指定されていない場合のみとなります。

capture

一致するトラフィックをキャプチャします。

ミラーリング送信元ポートに **acl** コマンドを設定する際に、ACL コンフィギュレーション コマンドで **capture** キーワードを指定しないと、トラフィックはミラーリングされません。

ACL の設定で **capture** キーワードが使用され、送信元ポートに **acl** コマンドが設定されていない場合は、ポートトラフィック全体がミラーリングされ、**capture** アクションは影響を受けません。

ipv4-address1 ipv4-address2 ipv4-address3

(任意) 1 ~ 3 のネクストホップアドレスを使用します。IP アドレスのタイプの定義は、次のとおりです。

- デフォルトの IP アドレス：ルーティング テーブル内にパケットの宛先アドレスの暗黙ルートがない場合、パケットを転送する必要がある宛先へのパスにあるネクスト ホップ ルータを指定します。現在稼働中の接続されたインターフェイスに関連付けられた最初の IP アドレスは、パケットのルーティングに使用されます。
- 指定された IP アドレス：パケットを転送する必要がある宛先へのパスにあるネクスト ホップ ルータを指定します。現在稼働中の接続されたインターフェイスに関連付けられた最初の IP アドレスは、パケットのルーティングに使用されます。

*dscp**dscp*

(任意) DiffServ コードポイント (DSCP) により、Quality of Service のコントロールが提供されます。dscp の値は次のとおりです。

- 0-63 : デイファレンシエーションサービスコードポイント値。
- af11 : パケットを AF11 dscp (001010) と一致させます。
- af12 : パケットを AF12 dscp (001100) と一致させます。
- af13 : パケットを AF13 dscp (001110) と一致させます。
- af21 : パケットを AF21 dscp (010010) と一致させます。
- af22 : パケットを AF22 dscp (010100) と一致させます。
- af23 : パケットを AF23 dscp (010110) と一致させます。
- af31 : パケットを AF31 dscp (011010) と一致させます。
- af32 : パケットを AF32 dscp (011100) と一致させます。
- af33 : パケットを AF33 dscp (011110) と一致させます。
- af41 : パケットを AF41 dscp (100010) と一致させます。
- af42 : パケットを AF42

dscp (100100) と一致させます。

- af43 : パケットを AF43 dscp (100110) と一致させます。

- cs1 : パケットを CS1 (precedence 1) dscp (001000) と一致させます。

- cs2 : パケットを CS2 (precedence 2) dscp (010000) と一致させます。

- cs3 : パケットを CS3 (precedence 3) dscp (011000) と一致させます。

- cs4 : パケットを CS4 (precedence 4) dscp (100000) と一致させます。

- cs5 : パケットを CS5 (precedence 5) dscp (101000) と一致させます。

- cs6 : パケットを CS6 (precedence 6) dscp (110000) と一致させます。

- cs7 : パケットを CS7 (precedence 7) dscp (111000) と一致させます。

- default : デフォルト DSCP (000000)

- ef : パケットを EF dscp (101110) と一致させます。

```
dscp rangedscp dscp
```

(任意) DiffServ コードポイント (DSCP) により、Quality of Service のコントロールが提供されます。dscp の値は次のとおりです。

- 0-63 : デイファレンシエーションサービスコードポイント値。
- af11 : パケットを AF11 dscp (001010) と一致させます。
- af12 : パケットを AF12 dscp (001100) と一致させます。
- af13 : パケットを AF13 dscp (001110) と一致させます。
- af21 : パケットを AF21 dscp (010010) と一致させます。
- af22 : パケットを AF22 dscp (010100) と一致させます。
- af23 : パケットを AF23 dscp (010110) と一致させます。
- af31 : パケットを AF31 dscp (011010) と一致させます。
- af32 : パケットを AF32 dscp (011100) と一致させます。
- af33 : パケットを AF33 dscp (011110) と一致させます。
- af41 : パケットを AF41 dscp (100010) と一致させます。
- af42 : パケットを AF42

dscp (100100) と一致させます。

- af43 : パケットを AF43 dscp (100110) と一致させます。
- cs1 : パケットを CS1 (precedence 1) dscp (001000) と一致させます。
- cs2 : パケットを CS2 (precedence 2) dscp (010000) と一致させます。
- cs3 : パケットを CS3 (precedence 3) dscp (011000) と一致させます。
- cs4 : パケットを CS4 (precedence 4) dscp (100000) と一致させます。
- cs5 : パケットを CS5 (precedence 5) dscp (101000) と一致させます。
- cs6 : パケットを CS6 (precedence 6) dscp (110000) と一致させます。
- cs7 : パケットを CS7 (precedence 7) dscp (111000) と一致させます。
- default : デフォルト DSCP (000000)
- ef : パケットを EF dscp (101110) と一致させます。

fragments	<p>(任意) このアクセス リスト エントリを適用すると、ソフトウェアが IPv4 パケットの非初期フラグメントを検査するようになります。このキーワードを指定すると、フラグメントがアクセス キーリスト エントリによる制約を受けます。</p>
log	<p>(任意) コンソールに送信される エントリに一致するパケットに関する ロギング メッセージ 情報が出力されます。(コンソールに記録されるメッセージのレベルは logging console コマンドで制御します)。</p> <p>このメッセージに含まれるものには、アクセスリスト番号、パケットが許可されたか拒否されたか、プロトコルが TCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。このメッセージは、フローに一致した最初のパケットに対して生成され、5 分間隔で、前の 5 分間に許可または拒否されたパケット数を含みます。</p>
log-input	<p>(任意) ロギングメッセージに 入力インターフェイスも含まれることを除き、log キーワードと同じ機能を果たします。</p>
ttl	<p>(任意) Time-To-Life (TTL) 値との一致をオンにします。</p>

<i>ttl value[value1 ... value2]</i>	<p>(任意) フィルタリングに使用される TTL 値の範囲は 1 ～ 255 です。</p> <p><i>value</i> が指定されている場合にのみ、この値と照合されます。</p> <p><i>value1</i> と <i>value2</i> の両方が指定されている場合は、<i>value1</i> と <i>value2</i> の間の TTL 範囲とパケット TTL が照合されます。</p>
icmp-off	<p>(任意) 拒否されたパケットに対して ICMP の生成をオフにします。</p>
<i>icmp-type</i>	<p>(任意) ICMP パケットのフィルタリングのための ICMP メッセージタイプ。範囲は 0 ～ 255 です。</p>
<i>icmp-code</i>	<p>(任意) ICMP パケットのフィルタリングのための ICMP メッセージコード。範囲は 0 ～ 255 です。</p>
<i>igmp-type</i>	<p>(任意) IGMP パケットをフィルタリングするための、IGMP メッセージタイプ (0 ～ 15) または次のようなメッセージ名。</p> <ul style="list-style-type: none">• dvmrp• host-query• host-report• mtrace• mtrace-response• pim• precedence• trace• v2-leave• v2-report• v3-report

operator

(任意) 演算子は、送信元ポートまたは宛先ポートを比較するために使用されます。使用可能なオペランドは、**lt** (より小さい)、**gt** (より大きい)、**eq** (等しい)、**neq** (等しくない)、および **range** (包含範囲) です。

演算子を *source* と *source-wildcard* の値の後に置いた場合は、送信元ポートと照合されます。

演算子を *destination* および *destination-wildcard* の値の後に置く場合、宛先ポートと一致する必要があります。

演算子を **ttd** キーワードの後に置いた場合は、TTL 値と照合されます。

range 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。

port

TCP または UDP ポートの 10 進数。範囲は 0 ~ 65535 です。

TCP ポートは、TCP をフィルタリングする場合にだけ使用できます。UDP ポートは、UDP をフィルタリングする場合にだけ使用できます。

protocol-port

TCP または UDP ポートの名前。TCP および UDP ポートの名前は、「使用上のガイドライン」に示されています。

TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。

established	(任意) TCPプロトコルの場合にだけ、確立された接続を表示します。
match-any	(任意) TCPプロトコルの場合にだけ、TCPフラグの任意の組み合わせをフィルタリングします。
match-all	(任意) TCPプロトコルの場合にだけ、すべてのTCPフラグをフィルタリングします。
+ -	(必須) TCPプロトコル match-any 、 match-all の場合： <i>flag-name</i> の前に+または-を付けます。TCPフラグを設定してパケットと照合するには、+ <i>flag-name</i> 引数を使用します。 TCPフラグを設定せずにパケットを照合するには、- <i>flag-name</i> 引数を使用します。
<i>flag-name</i>	(任意) TCPプロトコルが match-any 、 match-all の場合。 フラグ名は次のとおりです。 ack 、 fin 、 psh 、 rst 、 syn 。
counter	(任意) SNMPクエリーを使用してACLカウンタへのアクセスをイネーブルにします。 countercounter-name キーワードは、Cisco ASR 9000 拡張イーサネットラインカードでのみ使用できます。
<i>counter-name</i>	ACLカウンタ名を定義します。

コマンド デフォルト

IPv4 アクセスリストの送受信時にパケットが拒否される特定の条件はありません。
ICMP メッセージの生成はデフォルトでイネーブルです。

コマンド モード

IPv4 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

アクセスリストでパケットを許可する条件を指定するには、**ipv4 access-list** コマンドの後ろに **permit** コマンドを使用します。

デフォルトでは、アクセスリストの最初のステートメントは 10 で、その次のステートメントからは 10 ずつ増加します。

リスト全体を再入力せずに、既存のアクセスリストに **permit**、**deny**、または **remark** ステートメントを追加できます。新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

番号が連続している 2 つのステートメントの間（たとえば、10 行と 11 行の間）にステートメントを追加する場合は、まず **resequence access-list** コマンドを使用して最初のステートメントの番号を付け直し、後続の各ステートメントの番号を増加させます。**increment** 引数を使用すると、ステートメント間に新しい未使用の行番号が生成されます。次に、アクセスリスト中の所属先を指定する **entry-number** を持つ新しいステートメントを追加します。



(注) ACL のいずれかの ACE に ABF 句が含まれている場合、その ACL はゼロ以外の圧縮レベルに適用できません。

次に、**precedence** の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

次に、ICMP メッセージタイプの名前のリストを示します。

- administratively-prohibited
- alternate-address

- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement

- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

次に、ポート番号の代わりに使用できる TCP ポート名のリストを示します。これらのプロトコルの参考情報については、現在の *Assigned Numbers RFC* を参照してください。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2

- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

次のUDPポート名は、ポート番号の代わり使用できます。これらのプロトコルの参考情報については、現在の *Assigned Numbers RFC* を参照してください。これらのプロトコルに対応するポート番号を検索するには、ポート番号の代わりに「?」を入力します。

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs

- talk
- tftp
- time
- who
- xdmcp

次のフラグを **match-any** と **match-all** キーワードおよび+ と - 記号とともに使用すると、表示するフラグを選択できます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all+ack+syn** は、ack と syn の両方のフラグが設定されている TCP パケットを表示します。また、**match-any+ack-syn** は、ack が設定されている TCP パケットまたは syn が設定されていない TCP パケットを表示します。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
acl	読み取り、書き込み

例

次に、Internetfilter という名前のアクセスリストの許可条件を設定する方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

remark (IPv4)

IPv4 アクセスリストのエントリに有益なコメント（注釈）を記入するには、IPv4 アクセスリスト コンフィギュレーションモードで **remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

```
[ sequence-number ] remark remark
no sequence-number
```

構文の説明

<i>sequence-number</i>	(任意) アクセスリスト内の remark ステートメントの番号。この番号により、アクセスリスト中のステートメントの順番を識別します。範囲は 1 ~ 2147483646 です。(デフォルトでは、1 番目のステートメントの番号は 10 で、後続のステートメントの番号は 10 ずつ増加していきます)。
remark	アクセスリスト中のエントリを記述するコメント (最大 255 文字まで) です。

コマンド デフォルト

IPv4 アクセスリストのエントリには注釈がありません。

コマンド モード

IPv4 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

remark コマンドを使用すると、IPv4 アクセスリストのエントリに有益なコメントを書き込むことができます。コメントを削除するには、このコマンドの **no** 形式を使用します。

注釈は最大 255 文字まで可能で、これより長い文字は切り捨てられます。

削除するコメントのシーケンス番号がわかっている場合は、**no sequence-number** コマンドで削除できます。

既存のアクセスリストにステートメントを追加したいときに、連続エントリにシーケンス番号が付いているためステートメントを追加できない場合は、**resequence access-list ipv4** コマンドを使用します。

タスク ID	タスク ID	動作
	ipv4	読み取り、書き込み
	acl	読み取り、書き込み

例

次の例では、発信 Telnet を使用するための user1 サブネットは許可されません。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RP0/CPU0:router# show ipv4 access-list telnetting

ipv4 access-list telnetting
 0 remark Do not allow user1 to telnet out
 20 deny tcp 172.16.2.88 255.255.0.0 any eq telnet out
 30 permit icmp any any
```

resequence access-list ipv4

既存のステートメントの番号を再設定して以降のステートメントを増分し、新しいIPv4アクセスリストステートメント (**permit**、**deny**、**remark**) を追加できるようにするには、XR EXEC モードで **resequence access-list ipv4** コマンドを使用します。

resequence access-list ipv4 name [base [increment]]

構文の説明

<i>name</i>	IPv4 アクセス リストの名前。
<i>base</i>	(任意) 指定されたアクセスリスト中の 1 番目のステートメントであり、アクセスリスト中の順番を決定します。最大値は 2147483644 です。デフォルト値は 10 です。
<i>increment</i>	(任意) 以降のステートメントでの、ベースシーケンス番号に対する増分。最大値は 2147483644 です。デフォルト値は 10 です。

コマンド デフォルト

base: 10
increment: 10

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

既存の IPv4 アクセスリストの連続しているエントリの間には **permit**、**deny**、または **remark** ステートメントを追加するには、**resequence access-list ipv4** コマンドを使用します。先頭のエントリ番号 (*base*) を指定し、ステートメントのエントリ番号を隔てるための増分を指定します。既存のステートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

タスク ID	タスク ID	動作
	acl	読み取り、書き込み

例

次の例では、既存のアクセスリストがあると想定しています。

```
ipv4 access-list marketing
 1 permit 10.1.1.1
 2 permit 10.2.0.0 0.0.255.255
 3 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

アクセスリストにエントリを追加する場合は次のようにします。最初に、エントリの番号を付け直して（ステートメントの番号を20から始めて5ずつ増加させる）、既存の各ステートメント間に追加ステートメントを挿入できるスペースを設けます。

```
RP/0/RP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
```

```
ipv4 access-list marketing
 20 permit 10.1.1.1
 25 permit 10.2.0.0
 30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

これで、新しいエントリを追加できます。

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
```

```
ipv4 access-list marketing
 3 remark Do not allow user1 to telnet out
 4 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
 20 permit 10.1.1.1
 25 permit 10.2.0.0
 29 remark Allow user2 to telnet out
 30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

show access-lists afi-all

現在のIPv4およびIPv6アクセスリストの内容を表示するには、XR EXEC モードで **show access-lists afi-all** コマンドを使用します。

show access-lists afi-all

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンドモード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
acl	読み取り

例

次の例は、**show access-lists afi-all** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show access-lists afi-all

ipv4 access-list crypto-1
 10 permit ipv4 65.21.21.0 0.0.0.255 65.6.6.0 0.0.0.255
 20 permit ipv4 192.168.241.0 0.0.0.255 192.168.65.0 0.0.0.255
```

show access-lists ipv4

現在の IPv4 アクセスリストの内容を表示するには、XR EXEC モードで **show access-lists ipv4** コマンドを使用します。

```
show access-lists ipv4 [access-list-name hardware {ingress| egress} [interface type] {sequence number|
location node-id} | summary [ access-list-name ] access-list-name [sequence-number] maximum [detail]
[usage pfilter {resource-usage location node-id| all}]
```

構文の説明

<i>access-list-name</i>	(任意) 特定の IPv4 アクセスリストの名前。この名前にスペースや引用符を含めることはできませんが、数値を含めることはできます。
hardware	(任意) アクセスリストを、インターフェイスのアクセスリストとして識別します。
ingress	(任意) 着信インターフェイスを指定します。
egress	(任意) 発信インターフェイスを指定します。
interface	(任意) インターフェイス統計情報を表示します。
<i>type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
sequencenumber	(任意) 特定の IPv4 アクセスリストのシーケンス番号。範囲は 1 ~ 2147483644 です。
resource-usage	圧縮レベルの TCAM リソース使用量を表示します。
location <i>node-id</i>	(任意) 特定の IPv4 アクセスリストの場所。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

summary	(任意) 現在のすべての IPv4 アクセスリストのサマリーを表示します。
<i>sequence-number</i>	(任意) 特定の IPv4 アクセスリストのシーケンス番号。範囲は 1 ~ 2147483644 です。
maximum	(任意) IPv4 アクセス コントロールリスト (ACL) およびアクセス コントロール エントリ (ACE) の現在の設定可能最大数を表示します。
detail	(任意) 完全な out-of-resource (OOR) の詳細を表示します。
usage	(任意) 指定されたラインカード上のアクセスリストの使用方法を表示します。
pfilter	(任意) 指定されたラインカードのパケットフィルタリングの使用方法を表示します。
all	(任意) すべてのラインカードの場所を表示します。

コマンド デフォルト デフォルトでは、すべての IPv4 アクセス リストを表示します。

コマンド モード XR EXEC モード

コマンド履歴	リリース	変更内容
	リリース 6.0	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 access-lists ipv4 コマンドを使用すると、すべての IPv4 アクセスリストの内容を表示することができます。特定の IPv4 アクセスリストの内容を表示するには、*name* 引数を使用します。*sequence-number* 引数を使用すると、アクセスリストのシーケンス番号を指定できます。

特定の方向（入力または出力）で特定のアクセスリストを使用するすべてのインターフェイスについて、アクセスリストのハードウェアコンテンツとカウンタを表示するには、**hardware**、**ingress** または **egress**、および **location** キーワードを使用します。特定のアクセスリストエントリの内容を表示するには、**sequencenumber** キーワードと引数を使用します。インターフェイスのアクセスグループを設定するには、**ipv4 access-group** コマンドを使用してアクセスリストのハードウェアカウンタをイネーブルにする必要があります。

show access-lists ipv4 summary コマンドを使用すると、現在の全 IPv4 アクセスリストのサマリーを表示できます。特定の IPv4 アクセスリストのサマリーを表示するには、*name* 引数を使用します。

show access-lists ipv4 maximum detail コマンドを使用すると、IPv4 アクセスリストの OOR の詳細を表示できます。OOR は、システムに設定可能な ACL および ACE の数を制限します。この制限に達すると、新しい ACL または ACE が拒否されます。

show access-list ipv4 usage コマンドを使用すると、特定のラインカードにプログラミングされているすべてのインターフェイスとアクセスリストのサマリーを表示できます。

egress での ACL はリリース 6.0 ではサポートされていません

タスク ID

タスク ID	動作
acl	読み取り

例

次の例では、すべての IPv4 アクセスリストの内容が表示されています。

```
RP/0/RP0/CPU0:router# show access-lists ipv4

ipv4 access-list 101
 10 deny udp any any eq ntp
 20 permit tcp any any
 30 permit udp any any eq tftp
 40 permit icmp any any
 50 permit udp any any eq domain
ipv4 access-list Internetfilter
 10 permit tcp any 172.16.0.0 0.0.255.255 eq telnet
 20 deny tcp any any
 30 deny udp any 172.18.0.0 0.0.255.255 lt 1024
 40 deny ipv4 any any log
```

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 2: *show access-lists ipv4* の *hardware* フィールドの説明

フィールド	説明
hw matches	ハードウェア一致の数
ACL name	ハードウェアにプログラミングされた ACL の名前。
Sequence Number	各 ACE シーケンス番号は、ACE に設定された値に対応するすべてのフィールドとともにハードウェア内にプログラミングされます。
Grant	ACE ルールによって、grant は拒否、許可、またはその両方に設定されます。
Logging	Logging は、ACE がログ オプションを使用してログをイネーブルにする場合にオンに設定されます。
Per ace icmp	Per ace icmp がハードウェア内でオンに設定されると、ICMP は到達不能で、レートが制限され、生成されます。デフォルトでは、オンに設定されます。
Hits	ACE のハードウェア カウンタ。

次の例では、すべての IPv4 アクセス リストのサマリーが表示されています。

```
RP/0/RP0/CPU0:router# show access-lists ipv4 summary
```

```
ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

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 3: *show access-lists ipv4 summary* のフィールドの説明

フィールド	説明
Total ACLs configured	設定された IPv4 ACL の数
Total ACEs configured	設定された IPV4 ACE の数

次の例では、すべての IPv4 アクセス リストの OOR の詳細が表示されています。

```
RP/0/RP0/CPU0:router# show access-lists ipv4 maximum detail
```

```

Default max configurable acls :5000
Default max configurable aces :200000
Current configured acls      :1
Current configured aces     :2
Current max configurable acls :5000
Current max configurable aces :200000
Max configurable acls       :9000
Max configurable aces       :350000

```

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 4 : *show access-lists ipv4 maximum detail* コマンドのフィールドの説明

フィールド	説明
Default max configurable acls	IPv4 ACL のデフォルトの設定可能最大数
Default max configurable aces	IPv4 ACE のデフォルトの設定可能最大数
Current configured acls	設定された IPv4 ACL の数
Current configured aces	設定された IPv4 ACE の数
Current max configurable acls	IPv4 ACL の設定可能最大数
Current max configurable aces	IPv4 ACE の設定可能最大数
Max configurable acls	IPv4 ACL の設定可能最大数
Max configurable aces	IPv4 ACE の設定可能最大数

次の例は、特定のラインカードに対するパケットフィルタリングの使用を表示します。

```

RP/0/RP0/CPU0:router# show access-lists ipv4 usage pfilter location 0/RP0/CPU0

Interface : tenGigE 0/0/0/1
Input Common-ACL : ipv4_c_acl  ACL : ipv4_i_acl_1
Output ACL : ipv4_i_acl_1

```



(注) バンドルインターフェイスに対するパケットフィルタリングの使用を表示するには、**show access-lists ipv4 usage pfilter location all** コマンドを使用します。

次の例は、TCAM リソースの使用量を表示します。

```

RP/0/RP0/CPU0:router# sh access-lists ipv4 acl-v4 hardware ingress resource-usage location
0/RP0/CPU0

Rules (ACE)          : 2
TCAM Entries used   : 2 ( 2048k total)

```

TCAM Key Width : 160

show pfilter-ea

パケットフィルタ **ea** 情報を表示するには、ASR 9000 拡張イーサネット ラインカードで XR EXEC モードに入って `show pfilter ea` コマンドを入力します。

show pfilter-ea fea {**ipv4 acl** | **ipv6 acl**} *acl-name***locationnode-id**

構文の説明

ipv4 acl	IPv4 アクセス リストを示します。
ipv6 acl	IPv6 アクセス リストを示します。
<i>acl-name</i>	IPv4/IPv6 アクセス リストの名前。
locationnode-id	特定の IPv4/IPv6 アクセス リストの場所。node-id 引数は、rack/slot/module の形式で入力します。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	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、ASR 9000 拡張イーサネット ラインカードでのみ使用できます。

タスク ID

タスク ID	動作
root-system	読み取り、書き込み

例

次の例は、パケットフィルタ `ea` 情報の表示方法を示しています。

```
RP/0/RP0/CPU0:router# show feature-mgr client pfilter-ea feature-info summary location
0/RP0/CPU0
```

```
IFH          NPU DIR Lookup-type  VMR-ID          ACL-ID Refcnt Feature-Name
-----
0x80000048  0   IN  IPV4_ACL (L3)  0x2             3         1   skywarp_acl
0x80000038  0   IN  IPV4_ACL (L3)  0x1             2         1   v4-acl
0x80000040  0   IN  IPV4_ACL (L2)  0x200000001    2         1   v4-acl
```

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 5: `show pfilter-ea` のフィールドの説明

フィールド	説明
IFH	ACLが適用されるインターフェイスのインターフェイスハンドル
DIR	ACLが適用される方向を示します。INは入力、OUTは出力。
Lookup-type	ACLのタイプ (IPv4またはIPv6)。L3/L2はインターフェイスのタイプを示します。
Reference count	特定のACLが適用されるインターフェイスの番号を示します。
Feature name	ハードウェアにプログラミングされたACLの名前。



ARP コマンド

この章では、NCS 5000 ルータでアドレス解決プロトコル（ARP）を設定したりモニタする際に使用するコマンドについて説明します。

ARP の概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [arp, 62 ページ](#)
- [arp dagr, 64 ページ](#)
- [arp gratuitous ignore, 65 ページ](#)
- [arp purge-delay, 66 ページ](#)
- [arp timeout, 68 ページ](#)
- [clear arp-cache, 70 ページ](#)
- [local-proxy-arp, 72 ページ](#)
- [peer \(DAGR\) , 74 ページ](#)
- [priority-timeout, 75 ページ](#)
- [proxy-arp, 77 ページ](#)
- [route distance, 79 ページ](#)
- [route metric, 81 ページ](#)
- [show arp, 83 ページ](#)
- [show arp dagr, 87 ページ](#)
- [show arp traffic, 88 ページ](#)
- [timers \(DAGR\) , 91 ページ](#)

arp

アドレス解決プロトコル (ARP) キャッシュにパーマネント エントリを追加するには、XR コンフィギュレーションモードで **arp** コマンドを使用します。ARP キャッシュからエントリを削除するには、このコマンドの **no** 形式を入力します。

arp [vrf vrf-name] ip-address hardware-address encapsulation-type [alias]

no arp [vrf vrf-name] ip-address hardware-address encapsulation-type [alias]

構文の説明

vrf	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
vrf-name	(任意) VPN を識別する VRF インスタンス。
ip-address	パーマネント エントリが ARP キャッシュに追加される IPv4 (ネットワーク層) アドレス。ローカルデータリンク アドレス (32 ビットアドレス) に対応する 4 分割ドット付き 10 進表記で IPv4 アドレスを入力します。
hardware-address	IPv4 アドレスがリンクされているハードウェア (データリンク層) アドレス 0800.0900.1834 のようなローカルデータリンク アドレス (48 ビットアドレス) を入力します。
encapsulation-type	カプセル化タイプ。カプセル化タイプは次のとおりです。 <ul style="list-style-type: none"> • arpa • srp • srpa • srpb <p>イーサネット インターフェイスの場合、これは通常 arpa キーワードになります。</p>
alias	(任意) プロキシ ARP がイネーブルであるかどうかにかかわらず、ソフトウェアが、指定された IP アドレスおよびハードウェア アドレスの両方の所有者であるかのように ARP 要求に応答するようになります。

コマンド デフォルト

ARP キャッシュに永続的にインストールされるエントリはありません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ソフトウェアは ARP キャッシュ エントリを使用して 32 ビット IP アドレスを 48 ビット ハードウェア アドレスに変換します。

大部分のホストはダイナミック レゾリューションをサポートしているため、通常はスタティック ARP キャッシュ エントリを指定する必要はありません。

スタティック エントリは、ネットワーク層アドレス (IPv4 アドレス) をデータリンク層アドレス (MAC アドレス) にマッピングするパーマネント エントリです。エントリの作成時に **alias** キーワードを指定すると、エントリに関連付けられているインターフェイスが、指定されたアドレスの所有者のように動作します。つまり、インターフェイスは、エントリ内のデータリンク層アドレスを使って、このネットワーク層アドレスに対する ARP 要求パケットに応答します。

ソフトウェアは、ARP 要求を受信したインターフェイス上でプロキシ ARP がイネーブルにされないかぎり、指定された IP アドレスに受信されたどの ARP 要求にも応答しません。プロキシ ARP がイネーブルになると、ソフトウェアは、独自のローカルインターフェイス ハードウェア アドレスを持つ ARP 要求に応答します。

ARP キャッシュからすべての非スタティック エントリを削除するには、XR EXEC モードで **clear arp-cache**、(70 ページ) を入力します。

タスク ID

タスク ID	動作
cef	読み取り、書き込み

例

次に、一般的なイーサネット ホストのスタティック ARP エントリの例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# arp 192.168.7.19 0800.0900.1834 arpa
```

arp dagr

Direct Attached Gateway Redundancy (DAGR) 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 **arp dagr** コマンドを使用します。

arp dagr

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ディセーブル

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例では、DAGR 設定をイネーブルにしています。

```
RP/0/# configure
RP/0/(config)# interface TenGigE 0/0/0/1
RP/0/(config-if)# arp dagr
RP/0/(config-if-dagr)#
```

arp gratuitous ignore

Gratuitous アドレス解決プロトコル (ARP) パケットの受信を無視するには、インターフェイス コンフィギュレーションモードで **arp gratuitous ignore** コマンドを使用します。Gratuitous ARP を受信するには、このコマンドの **no** 形式を使用します。

arp gratuitous ignore

noarp gratuitous ignore

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ディセーブル

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例は、**arp gratuitous ignore** コマンドの設定方法を示しています。

```
RP/0/# configure
RP/0/(config)# interface TenGigE 0/0/0/1
RP/0/(config-if)# arp gratuitous ignore
```

arp purge-delay

インターフェイスがダウンしたときにアドレス解決プロトコル（ARP）のパージングを遅らせるには、インターフェイス コンフィギュレーション モードで **arp purge-delay** コマンドを使用します。パージ遅延機能をオフにするには、このコマンドの **no** 形式を使用します。

arp purge-delay value

no arp purge-delay value

構文の説明

value	パージ遅延時間を秒単位で設定します。有効値の範囲は 1 ～ 65535 です。
-------	---

コマンド デフォルト

デフォルト値はオフです。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

arp purge-delay コマンドを使用すると、インターフェイスがダウンしたときに ARP エントリのパージングを遅らせることができます。インターフェイスが遅延時間以内に起動した場合、ARP エントリが復元され、Equal Cost Multipath（ECMP）を設定してパケット損失を防止します。

タスク ID

タスク ID	動作
cef	読み取り、書き込み

例

次に、パージ遅延を 50 秒に設定する例を示します。

```
RP/0/# configure
RP/0/(config)# interface TenGigE 0/0/0/0
```

```
RP/0/(config-if)# arp purge-delay 50
```

arp timeout

インターフェイスで学習したダイナミックエントリをアドレス解決プロトコル (ARP) キャッシュ内に留める時間を指定するには、インターフェイス コンフィギュレーションモードで **arp timeout** コマンドを入力します。コンフィギュレーション ファイルから **arp timeout** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を入力します。

arp timeout seconds

no arp timeout seconds

構文の説明

seconds	エントリが ARP キャッシュ内に残る時間 (秒単位) を示します。値の範囲は 30 ~ 4294967295 です。
---------	---

コマンド デフォルト

エントリは ARP キャッシュ内に 14,400 秒 (4 時間) 残ります。

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
リリース 6.0	このコマンドがサポートされました。

使用上のガイドライン

このコマンドは、ARP を使用しないインターフェイス上で発行した場合は無視されます。また、ローカル インターフェイスに対応する ARP、またはユーザが静的に設定する ARP はタイムアウトしません。

arp timeout コマンドは、入力されたインターフェイスにのみ適用されます。あるインターフェイスのタイムアウトを変更すると、その変更はそのインターフェイスだけに適用されます。

show interfaces コマンドは、ARP タイムアウト値を次のように「時間:分:秒」で表示します。

```
ARP type: ARPA, ARP Timeout 04:00:00
```

タスク ID

タスク ID	動作
cef	読み取り、書き込み

例

次に、ARP タイムアウトを 3600 秒に設定して、エントリがデフォルトよりも速くタイムアウトできるようにする例を示します。

```
RP/0/#configure
RP/0/(config)#interface TenGigE 0/0/0/0
RP/0/(config-if)# arp timeout 3600
```

clear arp-cache

アドレス解決プロトコル (ARP) キャッシュからすべてのダイナミック エントリを削除して、高速スイッチングキャッシュをクリアし、IP ルートキャッシュをクリアするには、**clear arp-cache** コマンドを使用します。

clear arp-cache {*traffic type interface-path-id*| **location node-id**}

構文の説明

traffic	指定したインターフェイス上のトラフィック統計情報を削除します。
type	インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
interface-path-id	次に示す、物理インターフェイスインスタンスまたは仮想インターフェイスインスタンスのいずれかです。 <ul style="list-style-type: none"> • 物理インターフェイス インスタンス。名前表記は <i>rack/slot/module/port</i> です。値の間に表記の一部としてスラッシュが必要です。 <ul style="list-style-type: none"> ◦ <i>rack</i> : ラックのシャーシ番号。 ◦ <i>slot</i> : モジュラ サービス カードまたはラインカードの物理スロット番号。 ◦ <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ◦ <i>port</i> : インターフェイスの物理ポート番号。 • 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。</p>
location node-id	指定された場所の ARP エントリをクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンドモード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

キーワードや引数を指定せずに **clear arp-cache** コマンドを使用すると、ARP キャッシュ内のすべてのエントリがクリアされます。

タスク ID

タスク ID	動作
cef	実行

例

次に、トラフィック統計情報エントリを、指定されたインターフェイスと一致する ARP キャッシュから削除する方法の例を示します。

```
RP/0/# clear arp-cache traffic TenGigE 0/0/0/1 location 0/1/CPU0
```

次に、エントリを、指定された場所と一致する ARP キャッシュから削除する方法の例を示します。

```
RP/0/# clear arp-cache location 0/1/CPU0
```

local-proxy-arp

インターフェイスでローカルプロキシアドレス解決プロトコル（ARP）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 **local-proxy-arp** コマンドを入力します。インターフェイスでローカルプロキシ ARP をディセーブルにするには、このコマンドの **no** 形式を入力します。

local-proxy-arp

no local-proxy-arp

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

すべてのインターフェイスでローカルプロキシ ARP がディセーブルになります。

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

リリース 6.0

このコマンドが導入されました。

使用上のガイドライン

ローカルプロキシ ARP がイネーブルになっている場合、ネットワークング デバイスは、次の条件をすべて満たす ARP 要求に応答します。

- ARP 要求のターゲット IP アドレス、ARP ソースの IP アドレス、および ARP 要求を受信するインターフェイスの IP アドレスが、同じレイヤ 3 ネットワーク上にある。
- ターゲット IP アドレスのネクストホップが、要求を受信するインターフェイスと同じインターフェイスを使用する。

通常、ローカルプロキシ ARP は、レイヤ 2 で分離されたプライベート VLAN など、同じレイヤ 3 ネットワークで MAC アドレスを IP アドレスに解決するために使用されます。ローカルプロキシ ARP は、ARP でサポートされるあらゆるタイプのインターフェイスに加えて、アンナンバードインターフェイスに対応しています。

コマンドの **no** 形式を使用して、指定されたコマンドを設定ファイルから削除し、システムをコマンドに関してデフォルトの状態に戻します。

タスク ID	タスク ID	動作
	cef	読み取り、書き込み

priority-timeout

優先順位が高い Direct Attached Gateway Redundancy (DAGR) ルートをタイムアウトにして、通常の優先順位に戻るようタイマーを設定するには、DAGR ピア インターフェイス コンフィギュレーション モードで **priority-timeout** コマンドを使用します。

priority-timeout time

構文の説明

time	ハイ プライオリティ ルートから通常のプライオリティ ルートに戻るまでの時間 (秒単位)。値の範囲は 1 ~ 10000 です。
------	--

コマンド デフォルト

time のデフォルトは 20 秒です。

コマンド モード

DAGR ピア 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
リリース 6.0	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には、適切なタスク ID を含むタスク グループに関連付けられているユーザグループに属している必要があります。ユーザグループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

この機能が適用されると、データベース内の DAGR グループ コンフィギュレーションが更新されます。

新しいタイマー値は、次回にタイマーが設定されるときに有効になります。このイベントごとにトリガーされる即時タイマー再起動はありません。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例では、プライオリティ タイムアウトを 25 秒に設定しています。

```
RP/0/ (config-if-dagr-peer) # priority-timeout 25  
RP/0/ (config-if-dagr-peer) #
```

proxy-arp

インターフェイスでプロキシアドレス解決プロトコル（ARP）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 **proxy-arp** コマンドを入力します。インターフェイス上のプロキシ ARP をディセーブルにするには、このコマンドの **no** 形式を入力します。

proxy-arp

no proxy-arp

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

すべてのインターフェイスでプロキシ ARP はディセ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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

プロキシ ARP がディセーブルにされると、ネットワークングデバイスは、次のいずれかの条件が満たされる場合に限り、インターフェイスに受信された ARP 要求に応答します。

- ARP 要求のターゲット IP アドレスは、要求が受信されたインターフェイス IP アドレスと同じです。
- ARP 要求のターゲット IP アドレスには、静的に設定された ARP エイリアスがあります。

プロキシ ARP がイネーブルにされると、ネットワークングデバイスは、次の条件すべてを満たす ARP 要求にも応答します。

- ターゲット IP アドレスが、要求を受信した同一の物理ネットワーク（LAN）上にない。
- ネットワークング デバイスに、ターゲット IP アドレスまでのルートが 1 つ以上存在する。
- ターゲット IP アドレスまでのルートすべてが、要求を受信したインターフェイスとは別のインターフェイスを通過する。

コマンドの **no** 形式を使用して、指定されたコマンドを設定ファイルから削除し、システムをコマンドに関してデフォルトの状態に戻します。

タスク ID	タスク ID	動作
	cef	読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/0/0/0 でプロキシ ARP をイネーブルにする方法を示しています。

```
RP/0/#(config)# interface TenGigE 0/0/0/0  
RP/0/#(config-if)# proxy-arp
```

route distance

特定の Direct Attached Gateway Redundancy (DAGR) グループのルート ディスタンスを設定するには、DAGR ピア インターフェイス コンフィギュレーション モードで **route distance** コマンドを使用します。

route distance normal normal-distance priority priority-distance

構文の説明

normal <i>normal-distance</i>	通常ルート (管理) ディスタンスを設定します。範囲は 0 ~ 256 です。
priority <i>priority-distance</i>	プライオリティルート (管理) ディスタンスを設定します。範囲は 0 ~ 256 です。

コマンド デフォルト

normal-distance のデフォルトは 150、*priority-distance* のデフォルトは 5 です。

コマンド モード

DAGR ピア 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

プライオリティディスタンスのデフォルト設定は、通常の Internet Gateway Protocol (IGP) の設定よりも優先されます。通常ディスタンスの設定は IGP の設定よりも優先されません。

この設定が適用されると、データベース内の DAGR グループが更新されます。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例では、通常ルートディスタンスが 48 でプライオリティルートディスタンスが 5 の DAGR グループピアを設定しています。

```
RP/0/(config-if-dagr-peer)# route distance normal 48 priority 5
RP/0/(config-if-dagr-peer)#
```

route metric

特定の Direct Attached Gateway Redundancy (DAGR) グループの標準ルートメトリックとプライオリティルートメトリックを設定するには、DAGR ピア インターフェイス コンフィギュレーション モードで **route metric** コマンドを使用します。

route metric normal normal-metric priority priority-metric

構文の説明

normal <i>normal-metric</i>	Routing Information Base (RIB) にインストールされたルートの通常値を設定します。値の範囲は 0 ~ 256 です。
priority <i>priority-metric</i>	RIB にインストールされたルートのプライオリティ値を設定します。値の範囲は 0 ~ 256 です。

コマンド デフォルト

normal-metric のデフォルトは 100、*priority-metric* のデフォルトは 90 です。

コマンド モード

DAGR ピア 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ルートメトリックの値は、**route distance** コマンドの値よりも重要ではありません。ルートメトリックを設定すると、RIB にインストールされたルータの値を設定することができます。この設定が適用されると、データベース内の DAGR グループが更新されます。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例では、48 の通常メトリックおよび 5 のプライオリティメトリックを持つ DAGR グループピアを設定しています。

```
RP/0/(config-if-dagr-peer)# route metric normal 48 priority 5  
RP/0/(config-if-dagr-peer)#
```

show arp

アドレス解決プロトコル (ARP) を表示するには、で **show arp** コマンドを入力します。

show arp vrf *vrf-name* [*ip-address*| *hardware-address*]| *interface-path-id* **location***node-id*

構文の説明

vrf	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
vrf-name	(任意) VPN を識別する VRF インスタンス。
ip-address	(任意) 表示する ARP エントリ。
hardware-address	(任意) 48 ビット MAC アドレスと一致する ARP エントリが表示されます。
<i>interface-path-id</i>	<p>(任意) 次のような物理インターフェイスのインスタンスまたは仮想インターフェイスのインスタンスです。</p> <ul style="list-style-type: none"> • 物理インターフェイス インスタンス。名前表記は <i>rack/slot/module/port</i> です。値の間に表記の一部としてスラッシュが必要です。 <ul style="list-style-type: none"> ◦ <i>rack</i> : ラックのシャーシ番号。 ◦ <i>slot</i> : モジュラ サービス カードまたはラインカードの物理スロット番号。 ◦ <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ◦ <i>port</i> : インターフェイスの物理ポート番号。 • 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。</p>
location <i>node-id</i>	(任意) 特定の場所の ARP エントリを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

アクティブ RSP はデフォルトの場所です。

コマンドモード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン ARP は、ネットワーク アドレス (IP アドレスなど) とイーサネット ハードウェア アドレスの間の通信を確立します。各通信の記録は、キャッシュ内に事前定義された期間だけ保持された後、廃棄されます。

show arp*interface-type interface-instance* 形式の場合は、Bundle インターフェイスや VLAN-on-Bundle インターフェイスでバンドルのキャッシュエントリを表示すべき場所を示すために、**locationnode-id** キーワードと引数が必須になります。物理インターフェイスの場合は、インターフェイスが 1 つのノード上にしか存在しないため、**locationnode-id** キーワードと引数の指定は任意です。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、場所を指定しない場合の **show arp** コマンドの出力を示しています。

```
RP/0/# show arp
```

```
-----
0/RP0/CPU0
-----
Address          Age           Hardware Addr  State   Type   Interface
5.28.0.1         03:13:25     0000.0c07.ac1c Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.0.2         00:00:29     d824.bd90.2180 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.0.3         00:00:30     d824.bd90.2100 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.7.111       00:06:11     000c.29e4.c25f Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.10.10      01:19:49     0022.bdd9.0948 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.11.4       02:29:58     d46d.5037.29c0 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.11.12      01:31:08     4055.395f.4408 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.11.66      01:10:34     d46d.5028.9e20 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.12.31      00:40:01     00a0.c900.0000 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.12.58      01:19:37     a80c.0d1f.8278 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.12.59      01:11:06     6c9c.ed75.9f78 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.12.89      00:35:53     10f3.1111.90c8 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.12.100     -            c472.95a6.2a80 Interface ARPA   MgmtEth0/RP0/CPU0/0
5.28.14.52      00:12:36     8478.ac36.08e0 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.14.55      00:19:38     a80c.0d19.0808 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.14.59      01:16:19     d46d.5064.b080 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.17.3       01:20:21     e0ac.f16c.a6d0 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.20.111     00:22:15     000c.2925.d81f Dynamic ARPA   MgmtEth0/RP0/CPU0/0
5.28.21.1       01:47:22     28c7.ce01.f830 Dynamic ARPA   MgmtEth0/RP0/CPU0/0
```

```

5.28.21.6      01:29:30    c472.95a6.2390 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.21.7      01:15:56    c472.95a6.1740 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.1      01:22:32    d867.d955.2888 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.2      01:27:29    c472.95a6.fa20 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.3      01:27:15    001a.6c40.e232 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.4      01:26:11    c472.95a6.f7c0 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.5      01:20:44    6c9c.ed6b.a888 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.6      01:30:06    c472.95a6.e930 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.7      01:21:08    0001.0203.0406 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.8      01:12:40    28c7.ce01.df50 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.9      01:29:06    28c7.ce01.dc20 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.10     01:14:46    c472.95a6.0600 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.22.109    00:30:33    28c7.ce01.dc20 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.100.50    03:43:05    000c.29c2.f21d Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
5.28.201.28    03:12:40    c472.95a6.a161 Dynamic   ARPA    MgmtEth0/RP0/CPU0/0
20.30.1.1      -           c472.95a6.2a86 Interface ARPA    TenGigE0/0/0/1
20.30.1.2      00:01:47    6c9c.ed2c.a060 Dynamic   ARPA    TenGigE0/0/0/1
20.31.1.1      -           c472.95a6.2a87 Interface ARPA    TenGigE0/0/0/2

```

次の例は、*interface-typeinterface-instance* 引数を指定した場合の **show arp** コマンドの出力を示しています。

```
RRP/0/# show arp tenGigE 0/0/0/1
```

```

-----
0/RP0/CPU0
-----
Address      Age      Hardware Addr  State   Type   Interface
20.30.1.1    -        c472.95a6.2a86 Interface ARPA   TenGigE0/0/0/1
20.30.1.2    00:04:58 6c9c.ed2c.a060 Dynamic  ARPA   TenGigE0/0/0/1

```

次の例は、*hardware-address* を指定した場合の **show arp** コマンドの出力を示しています。

```
RP/0/# show arp 0005.5f1d.8100
```

```

Address Age Hardware Addr State Type Interface
172.16.7.2 - 0005.5f1d.8100 Interface ARPA TenGigE0/0/0/2

```

次の例は、**location** キーワードと *node-id* 引数を指定した場合の **show arp** コマンドの出力を示しています。

```
RP/0/# show arp location 0/2/CPU0
```

```

Address Age Hardware Addr State Type Interface
192.168.15.1 - 00dd.00ee.00ff Alias ARPA
192.168.13.1 - 00aa.00bb.00cc Static ARPA
172.16.7.1 00:35:49 0002.fc0e.9600 Dynamic ARPA TenGigE0/0/0/2
172.16.7.2 - 0005.5f1d.8100 Interface ARPA TenGigE0/0/0/2

```

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 6: **show arp** のコマンド フィールドの説明

フィールド	説明
Address	ハードウェアアドレスと通信するネットワークアドレスを表示します。
Age	キャッシュ エントリの経過時間 (時間 : 分 : 秒) を表示します。ハイフン (-) は、アドレスがローカルであることを意味します。

フィールド	説明
Hardware Addr	ネットワークアドレスに対応している MAC アドレスの LAN ハードウェア アドレスを表示します。
State	キャッシュ エントリの現在の状態を表示します。値は次のとおりです。 <ul style="list-style-type: none"> • Dynamic • Interface • Alias • Static • "-" (グローバル スタティック エントリおよびエイリアス エントリを示します)
Type	Cisco IOS XR ソフトウェアがエントリ内のネットワークアドレスに使用しているカプセル化タイプを表示します。値は ARPA です。
Interface	このネットワークアドレスに関連付けられたインターフェイスを表示します。
ARP statistics	ARP パケットおよびエラー統計情報を表示します。
ARP cache	ARP キャッシュ内の IP アドレスおよび MAC アドレス アソシエーション エントリに関する一般情報を表示します。
IP Packet drop count for node */*/*	ARP 応答の受信前にバッファがスペースを使い果たしたためにドロップした IP パケット数を表示します。 <p>(注) */*/* は、ノード ID を rack/slot/module のフォーマットで表します。</p>

show arp dagr

すべての Direct Attached Gateway Redundancy (DAGR) グループの動作状態を表示するには、`show arp dagr` コマンドを使用します。

`show arp dagr [interface [IP-address]]`

構文の説明

`interface[IP-address]` (任意) 特定のインターフェイスおよび仮想 IP アドレスへの出力を制限します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	読み取り、書き込み

例

次に、DAGR グループの現在の動作状態の例を示します。

```
RP/0/# show arp dagr
```

```
-----
0/1/CPU0
-----
```

Interface	Virtual IP	State	Query-pd	Dist	Metr
GigabitEthernet0/1/0/2	192.168.7.19	Active	None	150	100
GigabitEthernet0/1/0/2	193.24.0.45	Query	1	None	None
GigabitEtherget0/1/0/3	192.66.0.45	Init	None	None	None

show arp traffic

アドレス解決プロトコル（ARP）トラフィック統計情報を表示するには、で **show arp traffic** コマンドを入力します。

show arp traffic [*vrf vrf-name*] [*interface-path-id*] [**location** *node-id*]

構文の説明

vrf	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
vrf-name	(任意) VPN を識別する VRF インスタンス。
interface-path-id	(任意) 次のような物理インターフェイスのインスタンスまたは仮想インターフェイスのインスタンスです。 <ul style="list-style-type: none"> • 物理インターフェイス インスタンス。名前表記は <i>rack/slot/module/port</i> です。値の間に表記の一部としてスラッシュが必要です。 <ul style="list-style-type: none"> ◦ <i>rack</i> : ラックのシャーシ番号。 ◦ <i>slot</i> : モジュラサービスカードまたはラインカードの物理スロット番号。 ◦ <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ◦ <i>port</i> : インターフェイスの物理ポート番号。 • 仮想インターフェイス インスタンス。数字の範囲は、インターフェイスタイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。</p>
locationnode-id	(任意) 特定の場所の ARP エントリを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

アクティブ RSP はデフォルトの場所です。

コマンドモード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ARP は、ネットワーク アドレス (IP アドレスなど) とイーサネットハードウェア アドレスの間の通信を確立します。各通信の記録は、キャッシュ内に事前定義された期間だけ保持された後、廃棄されます。

show arp traffic, *interface-instance* の場合は、Bundle インターフェイスや VLAN-on-Bundle インターフェイスでバンドルのキャッシュ エントリを表示すべき場所を示すために、**locationnode-id** キーワードと引数が必須になります。物理インターフェイスの場合は、インターフェイスが1つのノード上にしか存在しないため、**locationnode-id** キーワードと引数の指定は任意です。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show arp traffic** コマンドの出力を示しています。

```
RP/0/# show arp traffic

show arp traffic
Thu Dec 10 09:51:38.761 UTC

-----
0/6/CPU0
-----

ARP statistics:
  Recv: 163 requests, 79 replies
  Sent: 14138 requests, 177 replies (0 proxy, 0 local proxy, 14 gratuitous)
  Resolve requests rcvd: 7204
  Resolve requests dropped: 295
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet

ARP cache:
  Total ARP entries in cache: 22
  Dynamic: 11, Interface: 11, Standby: 0
  Alias: 0,   Static: 0,   DHCP: 0

IP Packet drop count for node 0/6/CPU0: 6909

Total ARP-IDB:19
```

```
-----  
0/2/CPU0  
-----
```

```
ARP statistics:  
  Recv: 162532 requests, 243 replies  
  Sent: 15879 requests, 162561 replies (0 proxy, 0 local proxy, 29 gratuitous)  
  Resolve requests rcvd: 47593  
  Resolve requests dropped: 0  
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet
```

```
ARP cache:  
  Total ARP entries in cache: 125  
  Dynamic: 112, Interface: 13, Standby: 0  
  Alias: 0,   Static: 0,   DHCP: 0
```

```
IP Packet drop count for node 0/2/CPU0: 44804
```

```
Total ARP-IDB:13
```

次の例は、**location** キーワードと *node-id* 引数を指定した場合の **show arptraffic** コマンドの出力を示しています。

```
RP/0/# show arp traffic location 0/4/CPU0
```

```
Thu Dec 10 09:51:56.209 UTC
```

```
ARP statistics:  
  Recv: 364474 requests, 96 replies  
  Sent: 14131 requests, 364499 replies (0 proxy, 0 local proxy, 25 gratuitous)  
  Resolve requests rcvd: 5699  
  Resolve requests dropped: 94  
  Errors: 0 out of memory, 0 no buffers, 0 out of sunbet
```

```
ARP cache:  
  Total ARP entries in cache: 18  
  Dynamic: 9, Interface: 9, Standby: 0  
  Alias: 0,   Static: 0,   DHCP: 0
```

```
IP Packet drop count for node 0/4/CPU0: 5603
```

```
Total ARP-IDB:18
```

timers (DAGR)

ARP 要求を送信するために Direct Attached Gateway Redundancy (DAGR) タイマーを設定するには、DAGR ピア インターフェイス コンフィギュレーション モードで **timers** コマンドを使用します。

timers query query-time standby standby-time

構文の説明

query <i>query-time</i>	値は、グループがクエリー ステートであるときに仮想 IP アドレスに送出されている連続した ARP 要求間の時間 (秒単位) です。値の範囲は 1 ~ 10000 です。
standby <i>standby-time</i>	値は、グループがスタンバイ ステートであるときに仮想 IP アドレスに送出されている連続した ARP 要求間の時間 (秒単位) です。値の範囲は 1 ~ 10000 です。

コマンド デフォルト

query-time のデフォルトは 1 秒、*standby-time* のデフォルトは 20 秒です。

コマンド モード

DAGR ピア 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

この機能が適用されると、データベース内の DAGR グループ コンフィギュレーションが更新されます。新しいタイマー値は、次回にタイマーが設定されるときに有効になります。このイベントごとにトリガーされる即時タイマー再起動はありません。

タスク ID

タスク ID	動作
cef	書き込み

例

次の例では、query time が 2 で standby time が 40 の DAGR グループ ピア を設定しています。



シスコエクスプレスフォワーディングコマンド

この章では、NCS 5000 ルータでシスコエクスプレス フォワーディング（CEF）を設定したりモニタする際に使用するコマンドについて説明します。

CEF の概念、設定作業、および例の詳細については、『*Cisco IP Addresses and Services Configuration Guide*』を参照してください。

- [clear cef ipv4 drops, 95 ページ](#)
- [clear cef ipv4 exceptions, 97 ページ](#)
- [clear cef ipv6 drops, 99 ページ](#)
- [clear cef ipv6 exceptions, 101 ページ](#)
- [show adjacency, 103 ページ](#)
- [show cef, 106 ページ](#)
- [show cef ipv4, 108 ページ](#)
- [show cef ipv4 adjacency, 110 ページ](#)
- [show cef ipv4 drops, 113 ページ](#)
- [show cef ipv4 hardware, 116 ページ](#)
- [show cef ipv4 exact-route, 119 ページ](#)
- [show cef ipv4 exceptions, 121 ページ](#)
- [show cef ipv4 resource, 123 ページ](#)
- [show cef ipv4 summary, 125 ページ](#)
- [show cef ipv4 unresolved, 128 ページ](#)
- [show cef ipv6, 130 ページ](#)
- [show cef ipv6 adjacency, 134 ページ](#)

- [show cef ipv6 adjacency hardware, 138 ページ](#)
- [show cef ipv6 drops, 141 ページ](#)
- [show cef ipv6 exact-route, 144 ページ](#)
- [show cef ipv6 exceptions, 147 ページ](#)
- [show cef ipv6 hardware, 149 ページ](#)
- [show cef ipv6 interface, 151 ページ](#)
- [show cef ipv6 resource, 154 ページ](#)
- [show cef ipv6 summary, 156 ページ](#)
- [show cef ipv6 unresolved, 158 ページ](#)
- [show cef mpls adjacency, 160 ページ](#)
- [show cef mpls adjacency hardware, 163 ページ](#)
- [show cef mpls interface, 165 ページ](#)
- [show cef mpls unresolved, 168 ページ](#)
- [show cef summary, 170 ページ](#)

clear cef ipv4 drops

シスコ エクスプレス フォワーディング (CEF) IPv4 パケット ドロップ カウンタをクリアするには、`clear cef ipv4 drops` コマンドを使用します。

`clear cef ipv4 drops location node-id`

構文の説明

location <i>node-id</i>	指定されたノードの IPv4 パケット ドロップ カウンタをクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
--------------------------------	---

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードのみ IPv4 CEF ドロップ カウンタがクリアされます。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
cef	読み取り、書き込み

例

次の例は、IPv4 シスコ エクスプレス フォワーディング (CEF) テーブルパケット ドロップ カウンタの出力を表示し、ロケーション 0/RP0/CPU0 の IPv4 CEF ドロップ カウンタをクリアします。

```
RP/0/# show cef ipv4 drops
```

clear cef ipv4 drops

```
CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops    packets :          0
  Unsupported drops   packets :         61
  Null0 drops         packets :          0
  No route drops      packets :       74026
  No Adjacency drops  packets :          0
  Checksum error drops packets :          0
  RPF drops           packets :          0
  RPF suppressed drops packets :          0
  RP destined drops   packets :          0
  Discard drops       packets :          0
  GRE lookup drops    packets :          0
  GRE processing drops packets :          0
  LISP punt drops     packets :          0
  LISP encap err drops packets :          0
  LISP decap err drops packets :          0
```

```
RP/0/# clear cef ipv4 drops location 0/RP0/CPU0
```

```
Node: 0/RP0/CPU0
Clearing CEF Drop Statistics
```

clear cef ipv4 exceptions

IPv4 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタをクリアするには、モードで **clear cef ipv4 exceptions** コマンドを使用します。

clear cef ipv4 exceptions location node-id

構文の説明

location*node-id* 指定されたノードの IPv4 CEF 例外パケット カウンタをクリアします。
node-id 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv4 CEF 例外パケット カウンタがクリアされます。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
cef	読み取り、書き込み

例

次の例は、IPv4 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタの出力を表示し、ノード 0/RP0/CPU0 の IPv4 CEF 例外パケット カウンタをクリアします。

```
RP/0/# show cef ipv4 exceptions
```

clear cef ipv4 exceptions

```
CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap packets :           0
  Unsupported packets :           0
  Redirect packets :             0
  Receive packets :              0
  Broadcast packets :            0
  IP options packets :           0
  TTL expired packets :          0
  Fragmented packets :           0

RP/0/# clear cef ipv4 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
Clearing CEF Exception Statistics
```

clear cef ipv6 drops

シスコ エクスプレス フォワーディング (CEF) IPv6 パケット ドロップ カウンタをクリアするには、`clear cef ipv6 drop` コマンドを使用します。

clear cef ipv6 drops location *node-id*

構文の説明

location <i>node-id</i>	指定されたノードの IPv6 パケット ドロップ カウンタをクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
--------------------------------	---

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv6 CEF ドロップ カウンタがクリアされます。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
cef	読み取り、書き込み

例

次の例は、IPv6 シスコ エクスプレス フォワーディング (CEF) テーブルパケット ドロップ カウンタの出力を表示し、ロケーション 0/RP0/CPU0 の IPv6 CEF ドロップ カウンタをクリアします。

```
RP/0/# show cef ipv6 drops
```

clear cef ipv6 drops

```
CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops      packets :      0
  Unsupported drops     packets :      0
  Null0 drops          packets :      0
  No route drops       packets :      0
  No Adjacency drops   packets :      0
  Checksum error drops packets :      0
  RPF drops            packets :      0
  RPF suppressed drops packets :      0
  RP destined drops    packets :      0
  Discard drops        packets :      0
  GRE lookup drops     packets :      0
  GRE processing drops packets :      0
  LISP punt drops      packets :      0
  LISP encap err drops packets :      0
  LISP decap err drops packets :      0
```

```
RP/0/# clear cef ipv6 drop
```

```
Node: 0/RP0/CPU0
Clearing CEF Drop Statistics
```

clear cef ipv6 exceptions

IPv6 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタをクリアするには、`clear cef ipv6 exceptions` コマンドを使用します。

`clear cef ipv6 exceptions location node-id`

構文の説明

location*node-id* 指定されたノードの IPv6 CEF 例外パケット カウンタをクリアします。
node-id 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv6 CEF 例外パケット カウンタがクリアされます。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み
cef	読み取り、書き込み

例

次に、IPv6 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタの出力例、および次のロケーションの IPv6 CEF 例外パケットをクリアする例を示します。

```
RP/0/# show cef ipv6 exceptions
```

clear cef ipv6 exceptions

```
CEF Exception Statistics
Node: 0/RP0/CPU0
  Slow encap packets :           0
  Unsupported packets :           0
  Redirect packets :             0
  Receive packets :             0
  Broadcast packets :           0
  IP options packets :           0
  TTL expired packets :          0
  Fragmented packets :          0

RP/0/# clear cef ipv6 exceptions location 0/RP0/CPU0

Node: 0/RP0/CPU0
Clearing CEF Exception Statistics
```

show adjacency

シスコ エクスプレス フォワーディング (CEF) 隣接関係テーブル情報を表示するには、**show adjacency** コマンドを使用します。

```
show adjacency [ipv4 [nexthop ipv4-address]] [mpls|ipv6] [interface type interface-instance] [remote] [detail] [location node-id]
```

構文の説明

ipv4	(任意) IPv4 隣接だけを表示します。
nexthop <i>ipv4-address</i>	(任意) 指定された IPv4 ネクストホップに送信される隣接を表示します。
mpls	(任意) MPLS 隣接だけを表示します。
ipv6	(任意) IPv6 隣接だけを表示します。
<i>interface-type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-instance</i>	<p>物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスを指定します。</p> <ul style="list-style-type: none"> • 物理インターフェイス インスタンス。命名規則は、<i>rack/slot/module/port</i> です。値と値の間には、表記の一部としてスラッシュ マークが必須です。 <ul style="list-style-type: none"> ◦ <i>rack</i> : ラックのシャーシ番号。 ◦ <i>slot</i> : ラインカードの物理スロット番号。 ◦ <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ◦ <i>port</i> : インターフェイスの物理ポート番号。 • 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。</p>
remote	(任意) リモート隣接だけを表示します。リモート隣接は、ラインカード間のパケット転送に使用される内部隣接です。
detail	(任意) レイヤ 2 情報など、隣接の詳細情報を表示します。

location*node-id* (任意) 指定したノードの詳細な CEF 情報を表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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、接続デバイスに隣接が存在するかどうか、その隣接が有効かどうか、MACヘッダー書き換えストリングが正しいかどうかの検証に使用されます。

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの CEF 隣接関係テーブルが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**location** キーワードを指定した場合の **show adjacency** コマンドの出力を示しています。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 7: **show adjacency** コマンドのフィールドの説明

フィールド	説明
Interface	隣接に関連付けられている発信インターフェイス。

フィールド	説明
Address	Address は、次のいずれかのアドレスです。 <ul style="list-style-type: none">• ネクストホップ IPv4 または IPv6 アドレス• Point-to-Point アドレス 括弧内の情報は、別のタイプの隣接を示します。
Version	隣接のバージョン番号。隣接が更新されると更新されます。
RefCount	この隣接のリファレンス番号。
Protocol	隣接が関連付けられるプロトコル。
0f000800 および 000c86f33d330800453a21c10800	レイヤ 2 カプセル化ストリング。
mtu	最大伝送ユニット (MTU) の値。
flags	内部フィールド。
packets	隣接を通過するパケット数。
bytes	隣接を通過するバイト数。

show cef

シスコ エクスプレス フォワーディング (CEF) により転送されるパケットの情報を表示するには、`show cef` コマンドを使用します。

`show cef [prefix [mask]] [hardware {egress| ingress}| detail] [location {node-id| all}]`

構文の説明

<code>prefix</code>	(任意) 指定された IPv4 送信先プレフィックスの最長一致 CEF エントリ。
<code>mask</code>	(任意) 指定された IPv4 プレフィックスおよびマスクの正確な CEF エントリ。
<code>hardware</code>	(任意) ハードウェアの詳細情報を表示します。
<code>egress</code>	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
<code>ingress</code>	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
<code>detail</code>	(任意) 詳細情報を表示します。
<code>location node-id</code>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <code>node-id</code> 引数は、 <code>rack/slot/module</code> の形式で入力します。
<code>all</code>	(任意) すべてのロケーションを表示します。

コマンド デフォルト

プレフィックスが明示的に指定されていない場合、このコマンドは、CEF に存在するすべての IPv4 プレフィックスを表示します。指定されていない場合、`location` は、デフォルトでアクティブなルート プロセッサ (RP) ノードになります。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID

動作

cef

読み取り

例

次の例は、**hardware** と **ingress** キーワードの両方を指定した場合の **show cef** コマンドのロード情報フラグの出力を示しています。

```
RP/0/# show cef 101.1.3.0/24 hardware ingress location 0/RP0/CPU0
101.1.3.0/24, version 0, internal 0x40000001 (0x598491e8) [1], 0x0 (0x0),
(0x0)
  local adjacency 10.0.101.2
  Prefix Len 24, traffic index 0, precedence routine (0)
  BGP Attribute: id: 8, Local id: 6, Origin AS: 1003, Next Hop AS: 4

  via 10.0.101.2, 2 dependencies, recursive
    next hop 10.0.101.2 via 10.0.101.2/32

Number of Mnodes: 2
Mnode 0 HW Location: 0x00080404 HW Value
[ 0x00081a600 00000000 00000000 00000000 ]

Leaf Mnode 1 HW Location: 0x040d3030
Hardware Leaf: PLU Leaf Value
[ 0x8000d800 028842c6 00000000 1fff2000 ]

FCR 2 TLU Address 0x00210b19 TI 0 AS 6

VPN Label 1 0

***** IGP LoadInfo *****
Loadinfo HW Max Index 0
Loadinfo SW Max Index 0
PBTS Loadinfo Attached: No
LI Path [ 0] HFA Info: 0x10204028 FCR: 4
*****

-----
HW Rx Adjacency 0 Detail:
-----
Rx Adj HW Address 0x02040280 (ADJ)
packets 0 bytes 0
HFA Bits 0x80 gp 16 mtu 9248 (Fabric MTU) TAG length 0
OI 0x409 (Tx uidb 0 PPindex 1033)
OutputQ 0 Output-port 0x0 local-outputq 0x8000

[ 0x80181040 00002420 00000409 00008000 ]
[ 0x00000000 00000000 00000000 00000000 ]
[ 0x00000000 00000000 00000000 00000000 ]
```

show cef ipv4

IPv4 シスコ エクスプレス フォワーディング (CEF) テーブルの情報を表示するには、**show cef ipv4** コマンドを使用します。

show cef ipv4 [*prefix* [*mask*]] *interface-type interface-instance* [**detail**] [**location node-id**]

構文の説明

<i>prefix</i>	(任意) 指定された IPv4 送信先プレフィックスの最長一致 CEF エントリ。
<i>mask</i>	(任意) 指定された IPv4 プレフィックスおよびマスクの正確な CEF エントリ。
<i>interface-type</i>	(任意) インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-instance</i>	物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスを指定します。 <ul style="list-style-type: none"> 物理インターフェイス インスタンス。命名規則は、<i>rack/slot/module/port</i> です。値と値の間には、表記の一部としてスラッシュ マークが必須です。 <ul style="list-style-type: none"> <i>rack</i> : ラックのシャーシ番号。 <i>slot</i> : ラインカードの物理スロット番号。 <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 <i>port</i> : インターフェイスの物理ポート番号。 (注) ルートプロセッサカード上の管理イーサネットインターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。</p>
detail	(任意) CEF エントリの詳細情報を表示します。
location node-id	(任意) 指定されたノードの IPv4 CEF テーブルを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

location が指定されていない場合、デフォルトで RP ノードが使用されます。

コマンドモード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの CEF テーブルが表示されます。これらが指定されている場合、このコマンドは、**locationnode-id** キーワードおよび引数で指定されたノードで機能します。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**showcefipv4** コマンドの出力を示しています。

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 8 : **show cef ipv4** コマンドのフィールドの説明

フィールド	説明
Prefix	IPv4 CEF テーブルのプレフィックス
Next Hop	プレフィックスのネクスト ホップ
Interface	プレフィックスに関連付けられているインターフェイス

show cef ipv4 adjacency

シスコ エクスプレス フォワーディング (CEF) IPv4 隣接ステータスと設定情報を表示するには、`show cef ipv4 adjacency` コマンドを使用します。

show cef ipv4 adjacency [*interface-type interface-path-id*] [**location node-id**] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**] [**protected**]

構文の説明

<i>interface-type</i>	(任意) インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	(任意) 物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスのいずれかです。 <ul style="list-style-type: none"> 物理インターフェイス インスタンス。命名規則は、<i>rack/slot/module/port</i> です。値と値の間には、表記の一部としてスラッシュ マークが必須です。 <ul style="list-style-type: none"> ° <i>rack</i> : ラックのシャーシ番号。 ° <i>slot</i> : ラインカードの物理スロット番号。 ° <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ° <i>port</i> : インターフェイスの物理ポート番号。 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。</p>
location <i>node-id</i>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
detail	(任意) 隣接の詳細情報を表示します。
discard	(任意) 廃棄された隣接情報だけをフィルタリングして表示します。
glean	(任意) glean 隣接情報だけをフィルタリングして表示します。
null	(任意) 隣接情報だけをフィルタリングして表示します。
punt	(任意) パント隣接情報だけをフィルタリングして表示します。

remote	(任意) リモート隣接情報だけをフィルタリングして表示します。
protected	(任意) IP-Fast Reroute (FRR) 保護された隣接情報だけをフィルタリングして表示します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **location** キーワードと *node-id* 引数でノードを指定しない場合は、**show cef ipv4 adjacency** をコマンドを発行したノードの CEF 隣接関係テーブルが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例 次の例は、**show cef ipv4 adjacency** コマンドの出力を示しています。

```
RP/0/:# show cef ipv4 adjacency tenGigE 0/0/0/0

Display protocol is ipv4
Interface      Address                               Type      Refcount
Mg0/RSP0/CPU0/0Prefix: 10.25.0.3/32          local      2
Adjacency: PT:0x782a2900 12.25.0.3/32
Interface: Mg0/RSP0/CPU0/0
MAC: 00.d0.02.75.ab.fd.00.11.93.ef.e3.50.08.00
Interface Type: 0x8, Base Flags: 0x1
Dependent adj type: remote
Dependent adj intf: Mg0/RSP0/CPU0/0
Mg0/RSP0/CPU0/0Prefix: 10.24.0.32/32          remote     6
Adjacency: PT:0x782a2b58
Interface: Mg0/RSP0/CPU0/0
MAC: 28.4e.4f.4e.45.29
Interface Type: 0x8, Base Flags: 0x0
```

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 9 : *show cef ipv4 adjacency* コマンドのフィールドの説明

フィールド	説明
Interface	プレフィックスに関連付けられているインターフェイス
Address	プレフィックス アドレス情報。
Type	隣接のタイプ。ローカルまたはリモートのいずれかです。
RefCount	他のルータにより隣接が参照される回数。

show cef ipv4 drops

IPv4 シスコ エクスプレス フォワーディング (CEF) テーブル パケット ドロップ カウンタを表示するには、で **show cefipv4 drops** コマンドを使用します。

show cef ipv4 drops [*location node-id*]

構文の説明

location*node-id* (任意) 指定されたノードの IPv4 CEF テーブル パケット ドロップ カウンタを表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

CEF エントリが解決されていない、機能がサポートされていない、ルート情報がない、隣接情報がない、または IP チェックサム エラーが発生したために、パケットが IPv4 CEF テーブルからドロップされた可能性があります。

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv4 CEF パケット ドロップ カウンタが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、ロケーション コマンドの **show cef ipv4drops** の出力を示しています。

```
RP/0/# show cef ipv4 drops
```

show cef ipv4 drops

```

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops    packets :           0
  Unsupported drops   packets :           61
  Null0 drops         packets :           0
  No route drops      packets :       74026
  No Adjacency drops  packets :           0
  Checksum error drops packets :           0
  RPF drops           packets :           0
  RPF suppressed drops packets :           0
  RP destined drops   packets :           0
  Discard drops       packets :           0
  GRE lookup drops    packets :           0
  GRE processing drops packets :           0
  LISP punt drops     packets :           0
  LISP encap err drops packets :           0
  LISP decap err drops packets :           0

```

表 10 : show cef ipv4 drop コマンドのフィールドの説明

フィールド	説明
Unresolved drops	未解決ルートによるドロップ
Unsupported drops	サポートされていない機能によるドロップ
Null0 drops	Null0 インターフェイスへのドロップ
No route drops	宛先へのルートがなかったためにドロップされたパケット数
No Adjacency drops	隣接が確立されていなかったためにドロップされたパケット数
Checksum error drops	IPv4 チェックサム エラーによるドロップ
RPF drops	IPv4 ユニキャスト RPF ¹ に起因するドロップ。
RPF suppressed drops	IPv4 ユニキャスト RPF により抑制されたドロップ
RP destined drops	ルータへのドロップ
Discard drops	破棄されたドロップ
GRE lookup drops	GRE ルックアップ中にドロップされた GRE パケット。
GRE processing drops	GRE の処理中にドロップされた GRE パケット。
LISP punt drops	パケットのソフトウェア処理中にドロップされた LISP パケット。

フィールド	説明
LISP encap err drops	エラーのためにドロップされた LISP カプセル化パケット。
LISP decap err drops	エラーのためにドロップされた LISP カプセル化解除パケット。

¹ RPF = リバース パス フォワーディング

show cef ipv4 hardware

シスコ エクスプレス フォワーディング (CEF) IPv4 ハードウェア ステータスおよび設定情報を表示するには、XR EXEC モードで **show cef ipv4 hardware** コマンドを使用します。

show cef [*vrf vrf-name*] **ipv4 hardware** {*egress*|*ingress* [*detail*|*location node-id*]}

構文の説明

vrf	(任意) VPN ルーティング/転送 (VRF) インスタンス情報を表示します。
vrf-name	(任意) VRF の名前。
egress	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
ingress	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
detail	(任意) 詳細情報を表示します。
location <i>node-id</i>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv4 hardware** コマンドの出力を示しています。

```

RP/0/# sh cef ipv4 hardware egress

Prefix                Next Hop                Interface
-----
0.0.0.0/0             7.35.0.1/32            <recursive>
0.0.0.0/32           broadcast
5.5.5.1/32           receive                Loopback0
7.35.0.0/16         attached              MgmtEth0/RP0/CPU0/0
7.35.0.0/32         broadcast              MgmtEth0/RP0/CPU0/0
7.35.0.1/32         7.35.0.1/32           MgmtEth0/RP0/CPU0/0
7.35.0.2/32         7.35.0.2/32           MgmtEth0/RP0/CPU0/0
7.35.0.3/32         7.35.0.3/32           MgmtEth0/RP0/CPU0/0
7.35.0.5/32         7.35.0.5/32           MgmtEth0/RP0/CPU0/0
7.35.0.6/32         7.35.0.6/32           MgmtEth0/RP0/CPU0/0
7.35.0.56/32        7.35.0.56/32          MgmtEth0/RP0/CPU0/0
7.35.0.245/32       7.35.0.245/32         MgmtEth0/RP0/CPU0/0
7.35.10.38/32       7.35.10.38/32         MgmtEth0/RP0/CPU0/0
7.35.10.44/32       7.35.10.44/32         MgmtEth0/RP0/CPU0/0
7.35.10.47/32       receive                MgmtEth0/RP0/CPU0/0
7.35.10.74/32       7.35.10.74/32         MgmtEth0/RP0/CPU0/0
7.35.10.113/32      7.35.10.113/32        MgmtEth0/RP0/CPU0/0
7.35.11.22/32       7.35.11.22/32         MgmtEth0/RP0/CPU0/0
7.35.11.27/32       7.35.11.27/32         MgmtEth0/RP0/CPU0/0
7.35.11.32/32       7.35.11.32/32         MgmtEth0/RP0/CPU0/0
7.35.11.78/32       7.35.11.78/32         MgmtEth0/RP0/CPU0/0
7.35.11.111/32      7.35.11.111/32        MgmtEth0/RP0/CPU0/0
7.35.11.112/32      7.35.11.112/32        MgmtEth0/RP0/CPU0/0
7.35.12.11/32       7.35.12.11/32         MgmtEth0/RP0/CPU0/0
7.35.12.23/32       7.35.12.23/32         MgmtEth0/RP0/CPU0/0
7.35.12.24/32       7.35.12.24/32         MgmtEth0/RP0/CPU0/0
7.35.12.29/32       7.35.12.29/32         MgmtEth0/RP0/CPU0/0
7.35.12.30/32       7.35.12.30/32         MgmtEth0/RP0/CPU0/0
7.35.12.44/32       7.35.12.44/32         MgmtEth0/RP0/CPU0/0
7.35.15.83/32       7.35.15.83/32         MgmtEth0/RP0/CPU0/0
7.35.15.84/32       7.35.15.84/32         MgmtEth0/RP0/CPU0/0
7.35.15.86/32       7.35.15.86/32         MgmtEth0/RP0/CPU0/0
7.35.15.92/32       7.35.15.92/32         MgmtEth0/RP0/CPU0/0
7.35.15.93/32       7.35.15.93/32         MgmtEth0/RP0/CPU0/0
7.35.15.95/32       7.35.15.95/32         MgmtEth0/RP0/CPU0/0
7.35.15.96/32       7.35.15.96/32         MgmtEth0/RP0/CPU0/0
7.35.15.97/32       7.35.15.97/32         MgmtEth0/RP0/CPU0/0
7.35.15.98/32       7.35.15.98/32         MgmtEth0/RP0/CPU0/0
7.35.15.103/32      7.35.15.103/32        MgmtEth0/RP0/CPU0/0
7.35.15.119/32      7.35.15.119/32        MgmtEth0/RP0/CPU0/0
7.35.15.123/32      7.35.15.123/32        MgmtEth0/RP0/CPU0/0
7.35.15.133/32      7.35.15.133/32        MgmtEth0/RP0/CPU0/0
7.35.15.173/32      7.35.15.173/32        MgmtEth0/RP0/CPU0/0
7.35.15.175/32      7.35.15.175/32        MgmtEth0/RP0/CPU0/0
7.35.15.178/32      7.35.15.178/32        MgmtEth0/RP0/CPU0/0
7.35.15.179/32      7.35.15.179/32        MgmtEth0/RP0/CPU0/0
7.35.15.188/32      7.35.15.188/32        MgmtEth0/RP0/CPU0/0
7.35.19.124/32      7.35.19.124/32        MgmtEth0/RP0/CPU0/0
7.35.19.127/32      7.35.19.127/32        MgmtEth0/RP0/CPU0/0
7.35.19.180/32      7.35.19.180/32        MgmtEth0/RP0/CPU0/0
7.35.19.181/32      7.35.19.181/32        MgmtEth0/RP0/CPU0/0
7.35.19.182/32      7.35.19.182/32        MgmtEth0/RP0/CPU0/0
7.35.19.183/32      7.35.19.183/32        MgmtEth0/RP0/CPU0/0
7.35.19.201/32      7.35.19.201/32        MgmtEth0/RP0/CPU0/0
7.35.19.205/32      7.35.19.205/32        MgmtEth0/RP0/CPU0/0
7.35.20.157/32      7.35.20.157/32        MgmtEth0/RP0/CPU0/0
7.35.21.156/32      7.35.21.156/32        MgmtEth0/RP0/CPU0/0
7.35.21.212/32      7.35.21.212/32        MgmtEth0/RP0/CPU0/0
7.35.23.59/32       7.35.23.59/32         MgmtEth0/RP0/CPU0/0
7.35.25.48/32       7.35.25.48/32         MgmtEth0/RP0/CPU0/0
7.35.25.77/32       7.35.25.77/32         MgmtEth0/RP0/CPU0/0

```

show cef ipv4 hardware

```
7.35.25.100/32      7.35.25.100/32      MgmtEth0/RP0/CPU0/0
7.35.25.101/32      7.35.25.101/32      MgmtEth0/RP0/CPU0/0
7.35.25.102/32      7.35.25.102/32      MgmtEth0/RP0/CPU0/0
7.35.25.107/32      7.35.25.107/32      MgmtEth0/RP0/CPU0/0
7.35.25.148/32      7.35.25.148/32      MgmtEth0/RP0/CPU0/0
7.35.25.198/32      7.35.25.198/32      MgmtEth0/RP0/CPU0/0
7.35.25.210/32      7.35.25.210/32      MgmtEth0/RP0/CPU0/0
7.35.25.223/32      7.35.25.223/32      MgmtEth0/RP0/CPU0/0
7.35.25.232/32      7.35.25.232/32      MgmtEth0/RP0/CPU0/0
7.35.25.233/32      7.35.25.233/32      MgmtEth0/RP0/CPU0/0
7.35.26.107/32      7.35.26.107/32      MgmtEth0/RP0/CPU0/0
7.35.26.188/32      7.35.26.188/32      MgmtEth0/RP0/CPU0/0
7.35.49.94/32       7.35.49.94/32       MgmtEth0/RP0/CPU0/0
7.35.104.155/32     7.35.104.155/32     MgmtEth0/RP0/CPU0/0
7.35.255.255/32     broadcast             MgmtEth0/RP0/CPU0/0
202.153.144.25/32   7.35.0.1/32          MgmtEth0/RP0/CPU0/0
224.0.0.0/4         0.0.0.0/32           MgmtEth0/RP0/CPU0/0
224.0.0.0/24        receive
255.255.255.255/32 broadcast
```

show cef ipv4 exact-route

IPv4 シスコ エクスプレス フォワーディング (CEF) の正確なルートを表示するには、で **show cefipv4 exact-route** コマンドを使用します。

```
show cefipv4 exact-route {source-address destination-address} [protocol protocol-name]
[source-ports source-port] [destination-port destination-port] [ingress-interface type
interface-path-id] [policy-class value] [detail | location node-id]
```

構文の説明

<i>source-address</i>	x.x.x.x フォーマットの IPv4 送信元アドレス。
<i>destination-address</i>	x.x.x.x フォーマットの IPv4 宛先アドレス。
protocol <i>protocol name</i>	(任意) 指定したルートのプロトコルを表示します。
source-ports <i>source-port</i>	(任意) UDP 送信元ポートを設定します。範囲は 0 ~ 65535 です。
destination-port <i>destination-port</i>	(任意) UDP 宛先ポートを設定します。範囲は 0 ~ 65535 です。
ingress-interface	(任意) 入力インターフェイスを設定します。
<i>type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
policy-class <i>value</i>	(任意) ポリシーベースのトンネル選択のクラスを表示します。トンネルポリシー クラスの値の範囲は 1 ~ 7 です。
detail	(任意) CEF エントリの詳細情報を表示します。
location <i>node-id</i>	(任意) 指定されたノードの IPv4 CEF テーブルを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 4 情報がイネーブルの場合、source-port、destination-port、ingress-interface、および protocol フィールドは必須です。これらのフィールドを指定しない場合、**show cef ipv4 exact-route** コマンドは正確な結果を出力しません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv4 exact-route** コマンドの出力を示しています。

```
RP/0/# show cef ipv4 exact-route 10.1.1.1 10.1.1.2 detail
0.0.0.0/0, version 432, proxy default, internal 0x2000201[1]
  Prefix Len 0, traffic index 0, precedence routine (0)
  via tenGigE0/RSP0RP1/CPU0/0
```

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 11 : **show cef ipv4 exact-route** コマンドのフィールドの説明

フィールド	説明
Prefix	IPv4 CEF テーブルのプレフィックス
Next Hop	プレフィックスのネクスト ホップ
Interface	プレフィックスに関連付けられているインターフェイス

show cef ipv4 exceptions

IPv4 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタを表示するには、**show cef ipv4 exceptions** コマンドを使用します。

show cef ipv4 exceptions [location node-id]

構文の説明

location*node-id* (任意) 指定されたノードの CEF 例外パケット カウンタを表示します。
node-id 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

CEF 例外パケットは、追加の処理が必要なためにハードウェアからソフトウェアに送信されたパケットです。IPv4 CEF 例外パケットのタイプは、コマンドの出力に表示され、定義されます。

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv4 CEF 例外パケット カウンタが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv4 exceptions** コマンドの出力を示しています。

```
RP/0/# show cef ipv4 exceptions
CEF Exception Statistics
Node: 0/RP0/CPU0
```

show cef ipv4 exceptions

```

Slow encap packets :          0
Unsupported packets :          0
Redirect packets :            0
Receive packets :            0
Broadcast packets :           0
IP options packets :          0
TTL expired packets :         0
Fragmented packets :          0

```

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 12 : *show cef ipv4 exceptions* コマンドのフィールドの説明

フィールド	説明
Slow encap	カプセル化中に特殊な処理を必要とするパケット数
Redirect	送信された ICMP ² リダイレクトメッセージの数。
Receive	ルータに送信されるパケット数
Broadcast	受信したブロードキャスト数。
IP options	IP オプションパケット数
TTL expired	TTL ³ が期限切れのパケットの数。
Fragmented	フラグメントされたパケット数

² ICMP = インターネット制御メッセージプロトコル

³ TTL = 存続可能時間

show cef ipv4 resource

IPv4 シスコ エクスプレス フォワーディング (CEF) テーブルの IPv4 非再帰的プレフィックス エントリを表示するには、で **show cef ipv4 resource** コマンドを使用します。

show cef ipv4 resource [detail] [hardware {egress| ingress}] [location node-id]

構文の説明

detail	(任意) IPv4 CEF テーブルにリストされているリソースの詳細情報を表示します。
hardware	(任意) ハードウェアの詳細情報を表示します。
egress	(任意) 出力パケット スイッチ交換 (PSE) を表示します。
ingress	(任意) 入力パケット スイッチ交換 (PSE) を表示します。
location node-id	(任意) 指定されたノードの IPv4 CEF テーブルの IPv4 リソース エントリを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの IPv4 CEF 非再帰的ルートが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv4 resource** コマンドの出力を示しています。

```
RP/0/# show cef ipv4 resource detail

CEF resource availability summary state: GREEN
  ipv4 shared memory resource:
    CurrMode GREEN, CurrUtil 0%
    CurrAvail 1874526208 bytes, MaxAvail 1875693568 bytes
  ipv6 shared memory resource:
    CurrMode GREEN, CurrUtil 0%
    CurrAvail 1874591744 bytes, MaxAvail 1875365888 bytes
  mpls shared memory resource:
    CurrMode GREEN, CurrUtil 0%
    CurrAvail 1874407424 bytes, MaxAvail 1875038208 bytes
  common shared memory resource:
    CurrMode GREEN, CurrUtil 0%
    CurrAvail 1873215488 bytes, MaxAvail 1874972672 bytes
  TABLE hardware resource: GREEN
  LEAF hardware resource: GREEN
  LOADINFO hardware resource: GREEN
  NHINFO hardware resource: GREEN
  LABEL_INFO hardware resource: GREEN
  IDB hardware resource: GREEN
  FRR_NHINFO hardware resource: GREEN
  LDSH_ARRAY hardware resource: GREEN
  RSRC_MON hardware resource: GREEN
```

show cef ipv4 summary

IPv4 シスコ エクスプレス フォワーディング (CEF) テーブルのサマリーを表示するには、**show cef ipv4 summary** コマンドを使用します。

show cef ipv4 summary [*location node-id*]

構文の説明

location*node-id* (任意) 指定されたノードの IPv4 CEF テーブルのサマリー情報を表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの IPv4 CEF テーブルのサマリーが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv4 summary** コマンドの出力を示しています。

```
RP/0/# show cef ipv4 summary
Router ID is
10
0
.0.0.0

IP CEF with switching (Table Version 0)
```

show cef ipv4 summary

```

Load balancing: L3
Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
Vrfname default, Refcount 367
193 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 13896 bytes
204 load sharing elements, 51904 bytes, 154 references
17 shared load sharing elements, 5536 bytes
187 exclusive load sharing elements, 46368 bytes
0 CEF route update drops, 175 revisions of existing leaves
Resolution Timer: 15s
0 prefixes modified in place
0 deleted stale prefixes
16 prefixes with label imposition, 51 prefixes with label information
Adjacency Table has 44 adjacencies
1 incomplete adjacency

```

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 13: show cef ipv4 summary コマンドのフィールドの説明

フィールド	説明
Load balancing	現在のロードバランシングモード。デフォルト値は L3 です。
Table Version	CEF テーブルのバージョン。
tableid	テーブル ID 番号。
vrfid	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
vrfname	VRF 名。
vrid	仮想ルータ ID (vrid) 番号。
flags	テーブルのオプション値。
routes	ルートの合計数。
reresolve	再解決されるルートの合計数。
unresolved (x old, x new)	未解決のルートの合計数。
load sharing elements	内部ロードシェアリングデータ構造の合計数。
bytes	内部ロードシェアリングデータ構造で使われる合計メモリ。
references	すべての内部ロードシェアリングデータ構造の合計リファレンスカウント数。
CEF resets	CEF テーブルリセット数。

フィールド	説明
revisions of existing leaves	既存のプレフィックスへの更新数。
Exponential (currently <i>xs</i> , peak <i>xs</i>)	現在使用されていません。
prefixes modified in place	正しく修正されたプレフィックス。
Adjacency Table has <i>x</i> adjacencies	合計隣接数。
<i>x</i> incomplete adjacency	未完了の隣接の合計数。

show cef ipv4 unresolved

IPv4 シスコ エクスプレス フォワーディング (CEF) テーブルの未解決ルートを表示するには、`show cef ipv4 unresolved` コマンドを使用します。

`show cef ipv4 unresolved [detail] [hardware {egress| ingress}] [location node-id]`

構文の説明

detail	(任意) IPv4 CEF テーブルにリストされている未解決ルートの詳細情報を表示します。
hardware	(任意) ハードウェアの詳細情報を表示します。
egress	(任意) 出力パケット スイッチ交換 (PSE) を表示します。
ingress	(任意) 入力パケット スイッチ交換 (PSE) を表示します。
location node-id	(任意) 指定されたノードの IPv4 CEF テーブルの未解決ルートを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの未解決ルートが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、未解決ルートを検出する場合の **show cef ipv4 unresolved** コマンドの出力を示しています。

```
RP/0/# show cef ipv4 unresolved
Prefix           Next Hop           Interface
10.3.3.3         102.2.2.2         ?
```

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 14 : **show cef ipv4 unresolved** コマンドのフィールドの説明

フィールド	説明
Prefix	未解決 CEF のプレフィックス。
Next Hop	未解決 CEF のネクスト ホップ。
Interface	ネクスト ホップ インターフェイス。疑問符 (?) は、インターフェイスが解決されていないことを示します。

show cef ipv6

IPv6 シスコ エクスプレス フォワーディング (CEF) テーブルの情報を表示するには、`show cef ipv6` コマンドを使用します。

show cef]ipv6[*interface-type interface-number* | *ipv6-prefix/ prefix-length*] [**detail**] [**location***node-id*]

構文の説明

<i>interface-type</i> <i>interface-number</i>	(任意) 指定されたネクスト ホップ インターフェイスを通過する IPv6 プレフィックス。
<i>ipv6-prefix/prefix-length</i>	(任意) 指定された IPv6 プレフィックスおよびプレフィックス長と一致する CEF テーブルの最長プレフィックス エントリ。
detail	(任意) IPv6 CEF テーブルの詳細情報を表示します。
location <i>node-id</i>	(任意) 指定されたノードの IPv6 CEF テーブルを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの IPv6 CEF テーブルが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv6** コマンドの出力を示しています。

```
RP/0/# show cef ipv6
::/0
::/128
  drop
::1/128
  loopback
66::4/128
  receive      Loopback0
2222::/64
  connected    tenGigE0/0/0/4
2222::1/128
  receive      tenGigE0/0/0/4
3333::/64
  connected    tenGigE0/0/0/3
3333::2/128
  receive      tenGigE0/0/0/3
5656::2/128
  recursive    fe80::3031:48ff:fe53:5533, tenGigE0/0/0/3
7777::/64
  connected    tenGigE0/0/0/0
7777::2/128
  receive      tenGigE0/0/0/0
9999::1/128
  recursive    fe80::205:5fff:fe1d:7600, tenGigE0/0/0/4
ff00::/8
  drop
ff02::1/128
  receive
ff02::2/128
  receive
ff02::5/128
  receive
ff02::6/128
  receive
ff02::1:ff00:0/104
  receive
```

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 15: **show cef ipv6** コマンドのフィールドの説明

フィールド	説明
drop	送信先プレフィックスに送信されるパケットがドロップされることを示します。
loopback	プレフィックスはループバックアドレスを示します。ループバックアドレスに送信されるパケットはドロップされます。
receive	プレフィックスがルータインターフェイスのいずれかで設定されていることを示します。これらのプレフィックスに送信されるパケットは、ルータにより受信されます。

フィールド	説明
connected	プレフィックスは、直接接続されているネクストホップ インターフェイスを示します。
recursive	プレフィックスが直接接続されていないが、表示されているネクストホッププレフィックスから到達可能であることを示します。

次の例は、**detail** キーワードを指定した場合の **showcefipv6** の出力を示しています。

```
RP/0/# show cef ipv6 detail

::/0
  flags: source_rib
  Loadinfo owner: <this route>
  fast adj: glean
  path 1:
    flags      :
    next hop   : ::
    interface  :
  tenGigE/0/0/0

::/128
  flags: drop, source_fib
  Loadinfo owner: <this route>
  fast adj: drop
  path 1:
    flags      :
    next hop   : ::
    interface  : <not specified>

::1/128
  flags: loopback, source_fib
  Loadinfo owner: <this route>
  fast adj: loopback
  path 1:
    flags      :
    next hop   : ::
    interface  : <not specified>

66::4/128
  flags: receive, source_rib
  Loadinfo owner: <this route>
  fast adj: receive
  path 1:
    flags      : point-to-point
    next hop   : ::
    interface  : Loopback0
```

次の表で、この出力に表示される重要な出力フィールドを説明します。

表 16 : **show cef ipv6 detail** コマンドのフィールドの説明

フィールド	説明
flags:	示されたプレフィックスのプロパティ。

フィールド	説明
Loadinfo owner:	転送のためにプレフィックスにより使用される Loadinfo のオーナー。Loadinfo オーナーは、隣接を示すポインタの配列を所有するプレフィックスです。
fast adj:	転送のために使用される、キャッシュに入った隣接。
path 1:	次の 3 つの項目は、path 1: の下に表示されます。 <ul style="list-style-type: none">• flags : パスのプロパティ。• next hop : ネクストホッププレフィックス (パケットが転送される場合)。• interface : ネクストホップインターフェイス (パケットが転送される場合)。

show cef ipv6 adjacency

シスコ エクスプレス フォワーディング (CEF) IPv6 隣接ステータスと設定情報を表示するには、`show cef ipv6 adjacency` コマンドを使用します。

show cef ipv6 adjacency [*interface-type interface-path-id*] [**location node-id**] [**detail**] [**discard**] [**glean**] [**null**] [**punt**] [**remote**]

構文の説明

interface-type (任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。

interface-path-id (任意) 物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスのいずれかです。

- 物理インターフェイス インスタンス。命名規則は、*rack/slot/module/port* です。値と値の間には、表記の一部としてスラッシュマークが必須です。

- ° *rack* : ラックのシャーシ番号。

- ° *slot* : ラインカードの物理スロット番号。

- ° *module* : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。

- ° *port* : インターフェイスの物理ポート番号。

(注) ルート プロセッサ カード上の管理イーサネット インターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 /CPU0/0

- 仮想インターフェイス インスタンス。数字の範囲は、インターフェイスタイプによって異なります。

ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

locationnode-id (任意) 指定したノードの詳細な CEF 情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

detail (任意) 隣接の詳細情報を表示します。

discard (任意) 廃棄された隣接情報だけをフィルタリングして表示します。

glean (任意) **glean** 隣接情報だけをフィルタリングして表示します。

null (任意) ヌル隣接情報だけをフィルタリングして表示します。

punt	(任意) パント隣接情報だけをフィルタリングして表示します。
remote	(任意) リモート隣接情報だけをフィルタリングして表示します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **location** キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの CEF 隣接関係テーブルが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例 次の例は、**show cef ipv6 adjacency** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 adjacency

Display protocol is ipv6
Interface      Address                                     Type      Refcount
-----
Te0/0/0/9     Interface: Te0/0/0/9 Type: glean
              Interface Type: 0x1e, Base Flags: 0x220 (0x8a796038)
              Nhinfo PT: 0x8a796038, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
              Dependent adj type: remote (0x8c34c238)
              Dependent adj intf: Te0/0/0/9
              Ancestor If Handle: 0x0
Update time   Dec 19 06:43:23.354

Te0/0/0/9     Prefix: 9::2/128                           local    3
              Adjacency: PT:0x88155c18 9::2/128
              Interface: Te0/0/0/9
              NHID: 0x0
              MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
              Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e238)
```

show cef ipv6 adjacency

```

Nhinfo PT: 0x8c39e238, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
Dependent adj type: remote (0x8c34c238)
Dependent adj intf: Te0/0/0/9
Ancestor If Handle: 0x0
Update time Dec 19 06:44:49.548

Te0/0/0/9 Prefix: fe80::12f3:11ff:fe25:395b/128 local 3
Adjacency: PT:0x881559c8 fe80::12f3:11ff:fe25:395b/128
Interface: Te0/0/0/9
NHID: 0x0
MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e568)
Nhinfo PT: 0x8c39e568, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
Dependent adj type: remote (0x8c34c238)
Dependent adj intf: Te0/0/0/9
Ancestor If Handle: 0x0
Update time Dec 19 06:44:59.553

Te0/0/0/8 special 2
Interface: Te0/0/0/8 Type: glean
Interface Type: 0x1e, Base Flags: 0x220 (0x8a795ea8)
Nhinfo PT: 0x8a795ea8, Idb PT: 0x8a3e0920, If Handle: 0x8000080
Dependent adj type: remote (0x8c34c0a0)
Dependent adj intf: Te0/0/0/8
Ancestor If Handle: 0x0
Update time Dec 19 06:43:23.351

Te0/0/0/8 Prefix: 8::2/128 local 3
Adjacency: PT:0x88155e68 8::2/128
Interface: Te0/0/0/8
NHID: 0x0
MAC: 10.f3.11.25.39.5a.28.c7.ce.01.ec.1f.86.dd
Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e0a0)
Nhinfo PT: 0x8c39e0a0, Idb PT: 0x8a3e0920, If Handle: 0x8000080
Dependent adj type: remote (0x8c34c0a0)
Dependent adj intf: Te0/0/0/8
Ancestor If Handle: 0x0
Update time Dec 19 06:44:46.155

Te0/0/0/8 Prefix: fe80::12f3:11ff:fe25:395a/128 local 3
Adjacency: PT:0x88155d40 fe80::12f3:11ff:fe25:395a/128
Interface: Te0/0/0/8
NHID: 0x0
MAC: 10.f3.11.25.39.5a.28.c7.ce.01.ec.1f.86.dd
Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e3d0)
Nhinfo PT: 0x8c39e3d0, Idb PT: 0x8a3e0920, If Handle: 0x8000080
Dependent adj type: remote (0x8c34c0a0)
Dependent adj intf: Te0/0/0/8
Ancestor If Handle: 0x0
Update time Dec 19 06:44:56.154

```

次の例は、**show cef ipv6 adjacency remote detail** コマンドの出力を示しています。

```

RP/0/# show cef ipv6 adjacency remote detail location 0/RP0/CPU0

Display protocol is ipv6
Interface Address Type Refcount
-----
Te0/2/0/3 Ifhandle: 0x8000240 remote 2
Adjacency: PT:0xa1bed9e4
Interface: Te0/2/0/3
Interface Type: 0x0, Base Flags: 0x0 (0xa55f3114)
Nhinfo PT: 0xa55f3114, Idb PT: 0xa2d850d8, If Handle: 0x8000240
Ancestor If Handle: 0x0

tt103 Ifhandle: 0x120 remote 1

```

```
no next-hop adj
Interface: NULLIFHNDL
tunnel adjacency
Interface Type: 0x24, Base Flags: 0x200 (0xa61ddc30)
Nhinfo PT: 0xa61ddc30, Idb PT: 0xa2d851d8, If Handle: 0x120
Ancestor If Handle: 0x0

tt2993      Ifhandle: 0xf9a0                      remote 1
no next-hop adj
Interface: NULLIFHNDL
tunnel adjacency
Interface Type: 0x24, Base Flags: 0x200 (0xa65634f0)
Nhinfo PT: 0xa65634f0, Idb PT: 0xa2d94a58, If Handle: 0xf9a0
Ancestor If Handle: 0x0

tt2994      Ifhandle: 0xf9e0                      remote 1
no next-hop adj
Interface: NULLIFHNDL
tunnel adjacency
Interface Type: 0x24, Base Flags: 0x200 (0xa65641e0)
Nhinfo PT: 0xa65641e0, Idb PT: 0xa2d94a98, If Handle: 0xf9e0
Ancestor If Handle: 0x0

tt2995      Ifhandle: 0xfa20                      remote 1
no next-hop adj
Interface: NULLIFHNDL
tunnel adjacency
Interface Type: 0x24, Base Flags: 0x200 (0xa6564350)
Nhinfo PT: 0xa6564350, Idb PT: 0xa2d94ad8, If Handle: 0xfa20
Ancestor If Handle: 0x0
```

show cef ipv6 adjacency hardware

シスコ エクスプレス フォワーディング (CEF) IPv6 隣接ハードウェア ステータスおよび設定情報を表示するには、XR EXEC モードで **show cef ipv6 adjacency hardware** コマンドを使用します。

show cef ipv6 adjacency hardware {egress| ingress} [detail| discard| drop| glean location *node-id*| null| punt| remote]

構文の説明

egress	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
ingress	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
detail	(任意) 詳細情報を表示します。
discard	(任意) 廃棄隣接情報を表示します。
drop	(任意) ドロップ隣接情報を表示します。
glean	(任意) glean 隣接情報を表示します。
location <i>node-id</i>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
null	(任意) ノル隣接情報を表示します。
punt	(任意) パント隣接情報を表示します。
remote	(任意) リモート隣接情報を表示します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID

動作

cef

読み取り

例

次の例は、**show cef ipv6 adjacency hardware** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 adjacency hardware egress

Display protocol is ipv6
Interface      Address                                     Type      Refcount
-----
Te0/0/0/9                                           special  2
                Interface: Te0/0/0/9 Type: glean
                Interface Type: 0x1e, Base Flags: 0x220 (0x8a796038)
                Nhinfo PT: 0x8a796038, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
                Dependent adj type: remote (0x8c34c238)
                Dependent adj intf: Te0/0/0/9
                Ancestor If Handle: 0x0
Update time Dec 19 06:43:23.354

Show-data Print at RPLC

RX H/W Result on NP:10 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform

TX H/W Result for NP:10 (index: 0x186ac (BE)):
```

```
Next Hop Data
Next Hop Valid:      YES
Next Hop Index:      100012
Egress Next Hop IF:  100012
Hw Next Hop Intf:    0
HW Port:              0
Next Hop Flags:      DISCARD PUNT
Next Hop MAC:        0000.0000.0000
```

```
Te0/0/0/9 Prefix: 9::2/128 local 3
Adjacency: PT:0x88155c18 9::2/128
Interface: Te0/0/0/9
NHID: 0x0
MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e238)
Nhinfo PT: 0x8c39e238, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
Dependent adj type: remote (0x8c34c238)
Dependent adj intf: Te0/0/0/9
Ancestor If Handle: 0x0
Update time Dec 19 06:44:49.548

Show-data Print at RPLC

TX H/W Result for NP:0 (index: 0x186bd (BE)):
```

```
Next Hop Data
Next Hop Valid:      YES
Next Hop Index:      100029
Egress Next Hop IF:  100028
Hw Next Hop Intf:    15
HW Port:              10
```

show cef ipv6 adjacency hardware

```
Next Hop Flags:      COMPLETE
Next Hop MAC:        10f3.1125.395b
```

```
NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform
```

```
NHINDEX STATS: pkts 0, bytes 0 (all NPs combined, no stats)
```

```
RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

```
Te0/0/0/9    Prefix: fe80::12f3:11ff:fe25:395b/128      local  3
Adjacency: PT:0x881559c8 fe80::12f3:11ff:fe25:395b/128
Interface: Te0/0/0/9
NHID: 0x0
MAC: 10.f3.11.25.39.5b.28.c7.ce.01.ec.20.86.dd
Interface Type: 0x1e, Base Flags: 0x1 (0x8c39e568)
Nhinfo PT: 0x8c39e568, Idb PT: 0x8a3e09a0, If Handle: 0x8000088
Dependent adj type: remote (0x8c34c238)
Dependent adj intf: Te0/0/0/9
Ancestor If Handle: 0x0
Update time Dec 19 06:44:59.554
```

```
Show-data Print at RPLC
```

```
TX H/W Result for NP:0 (index: 0x186bf (BE)):
```

```
Next Hop Data
Next Hop Valid:      YES
Next Hop Index:      100031
Egress Next Hop IF:  100030
Hw Next Hop Intf:    15
HW Port:             10
Next Hop Flags:      COMPLETE
Next Hop MAC:        10f3.1125.395b
```

```
NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform
```

```
NHINDEX STATS: pkts 0, bytes 0 (all NPs combined, no stats)
```

```
RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef ipv6 drops

IPv6 シスコ エクスプレス フォワーディング (CEF) テーブル パケット ドロップ カウンタを表示するには、で **show cef ipv6 drops** コマンドを使用します。

show cefipv6 drops [location node-id]

構文の説明

location*node-id* (任意) 指定されたノードの IPv6 CEF テーブル パケット ドロップ カウンタを表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

CEF エントリが解決されていない、機能がサポートされていない、ルート情報がない、隣接情報がない、または IP チェックサム エラーが発生したために、パケットが IPv6 CEF テーブルによりドロップされた可能性があります。

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードのパケットドロップが表示されます。



(注) ハードウェア転送がルート プロセッサ (RP) で発生していないため、そのノードのパケットドロップ情報は表示されません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv6 drops** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 drops location 0/RP0/CPU0

CEF Drop Statistics
Node: 0/RP0/CPU0
  Unresolved drops      packets :      0
  Unsupported drops     packets :      0
  Null0 drops           packets :      0
  No route drops        packets :      0
  No Adjacency drops    packets :      0
  Checksum error drops  packets :      0
  RPF drops             packets :      0
  RPF suppressed drops  packets :      0
  RP destined drops     packets :      0
  Discard drops         packets :      0
  GRE lookup drops      packets :      0
  GRE processing drops  packets :      0
  LISP punt drops       packets :      0
  LISP encap err drops  packets :      0
  LISP decap err drops  packets :      0
```

表 17: **show cef ipv6 drops** コマンドのフィールドの説明

フィールド	説明
Unresolved drops	未解決ルートによるドロップ
Unsupported drops	サポートされていない機能によるドロップ
Null0 drops	Null0 インターフェイスへのドロップ
No route drops	宛先へのルートがなかったためにドロップされたパケット数
No Adjacency drops	隣接が確立されていなかったためにドロップされたパケット数
Checksum error drops	IPv6 チェックサム エラーによるドロップ
RPF drops	IPv6 ユニキャスト RPF ⁴ に起因するドロップ。
RPF suppressed drops	IPv6 ユニキャスト RPF により抑制されたドロップ
RP destined drops	ルータへのドロップ
Discard drops	破棄されたドロップ

フィールド	説明
GRE lookup drops	GRE ルックアップ中にドロップされた GRE パケット。
GRE processing drops	GRE の処理中にドロップされた GRE パケット。
LISP punt drops	パケットのソフトウェア処理中にドロップされた LISP パケット。
LISP encap err drops	エラーのためにドロップされた LISP カプセル化パケット。
LISP decap err drops	エラーのためにドロップされた LISP カプセル化解除パケット。

⁴ RPF = リバース パス フォワーディング

show cef ipv6 exact-route

送信元および宛先アドレスから成る IPv6 フローが通過するパスを表示するには、で **show cefipv6 exact-route** コマンドを使用します。

```
show cefipv6 exact-route {source-address destination-address} [protocol protocol
name] [source-port source-port] [destination-port destination-port] [ingress-interface type
interface-path-id] [policy-class value] [detail | location node-id]
```

構文の説明

<i>source-address</i>	x::x フォーマットの IPv6 送信元アドレス。
<i>destination-address</i>	x::x フォーマットの IPv6 宛先アドレス。
protocol <i>protocolname</i>	(任意) 指定したルートのプロトコルを表示します。
source-port <i>source-port</i>	(任意) UDP 送信元ポートを設定します。範囲は 0 ~ 65535 です。
destination-port <i>destination-port</i>	(任意) UDP 宛先ポートを設定します。範囲は 0 ~ 65535 です。
ingress-interface	(任意) 入力インターフェイスを設定します。
<i>type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。

<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
<i>policy-classvalue</i>	(任意) ポリシーベースのトンネル選択のクラスを表示します。トンネルポリシークラスの値の範囲は 1 ~ 7 です。
detail	(任意) CEF エントリの詳細情報を表示します。
<i>locationnode-id</i>	(任意) 指定されたノードの IPv6 CEF テーブルを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 4 情報がイネーブルの場合、*source-port*、*destination-port*、*protocol* および *ingress-interface* フィールドは必須です。これらのフィールドを指定しない場合、**show cef ipv6 exact-route** コマンドは正確な結果を出力しません。

タスク ID

タスク ID

動作

cef

読み取り

例

次の例は、**show cef ipv6 exact-route** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 exact-route 222::2 9999::6751 location
```

```
0/RP0/CPU0 source address: 222::2 destination address: 9999::6751  
interface : tenGigE 0/0/0/3 non local interface
```

show cef ipv6 exceptions

IPv6 シスコ エクスプレス フォワーディング (CEF) 例外パケット カウンタを表示するには、**show cef ipv6 exceptions** コマンドを使用します。

show cef ipv6 exceptions [location node-id]

構文の説明

location*node-id* (任意) 指定されたノードの IPv6 CEF 例外パケット カウンタを表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

CEF 例外パケットは、追加の処理が必要なためにハードウェアからソフトウェアに送信されたパケットです。IPv6 CEF 例外パケットのタイプは、**show cef ipv6 exceptions** の出力に表示されます。

location キーワードと *node-id* 引数でノードを指定しない場合は、すべてのノードの IPv6 CEF 例外パケット カウンタが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv6 exceptions** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 exceptions location 0/RP0/CPU0
CEF Exception Statistics
Node: 0/RP0/CPU0
```

show cef ipv6 exceptions

```

Slow encap packets :          0
Unsupported packets :          0
Redirect packets :            0
Receive packets :            0
Broadcast packets :          0
IP options packets :          0
TTL expired packets :         0
Fragmented packets :          0

```

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 18 : *show cef ipv6 exceptions* コマンドのフィールドの説明

フィールド	説明
Slow encap	カプセル化中に特殊な処理を必要とするパケット数
Redirect	送信された ICMP ⁵ リダイレクトメッセージの数。
Receive	ルータに送信されるパケット数
Broadcast	受信したブロードキャスト数。
IP options	IP オプションパケット数
TTL expired	TTL ⁶ が期限切れのパケットの数。
Fragmented	フラグメントされたパケット数

⁵ ICMP = インターネット制御メッセージプロトコル

⁶ TTL = 存続可能時間

show cef ipv6 hardware

シスコ エクスプレス フォワーディング (CEF) IPv6 ハードウェア ステータスおよび設定情報を表示するには、で **show cef ipv6 hardware** コマンドを使用します。

show cef ipv6 hardware {egress| ingress [detail| location node-id]}

構文の説明

egress	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
ingress	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
detail	(任意) 詳細情報を表示します。
locationnode-id	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv6 hardware** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 hardware egress detail
```

show cef ipv6 hardware

```
::/0, version 0, proxy default, default route handler, drop adjacency, internal
Prefix Len 0, traffic index 0, precedence routine (0)
gateway array (0x0) reference count 1, flags 0x4000, source 4,
      [0 type 3 flags 0x109000 (0x7895114c) ext 0x0 (0x0)]
LW-LDI[type=3, refc=1, ptr=0x78a7d0dc, sh-ldi=0x7895114c]
via point2point, 0 dependencies, weight 0, class 0
  next hop point2point
  drop adjacency

Load distribution: 0 (refcount 0)

Hash OK Interface Address
0 Y Unknown drop
ff02::/16, version 0, receive
Prefix Len 16
ff02::2/128, version 0, receive
Prefix Len 128
ff02::1:ff00:0/104, version 0, receive
Prefix Len 104
```

show cef ipv6 interface

インターフェイスの IPv6 シスコ エクスプレス フォワーディング (CEF) の関連情報を表示するには、`show cef ipv6 interface` コマンドを使用します。

show cef ipv6 interface *type interface-path-id* [**detail**] [**location node-id**][**rpf-drop**]

構文の説明

<i>type</i>	インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
detail	(任意) コマンドが発行されるノードのすべてのインターフェイスに関する CEF 詳細情報を表示します。
location <i>node-id</i>	(任意) インターフェイスの IPv4 CEF 関連情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
rpf-drop	(任意) IPv6 ユニキャスト RPF によるドロップに関する情報を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合、**show cef ipv6 interface** コマンドは、ルートプロセッサのインターフェイスの CEF 関連情報を表示します。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef ipv6 interface** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 interface

fib_show_interface
created item name: 1000/protocol/1/vrf/default/interface-info/1/
Bundle-Ether5.2 is down if_handle 0x0800002c if_type IFT_VLAN_SUBIF(0x19)
  idb info 0x898ecfa0 flags 0x48001 ext 0x8c38b488 flags 0x10
  Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1 Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
Bundle-Ether5.1 is down if_handle 0x08000024 if_type IFT_VLAN_SUBIF(0x19)
  idb info 0x898ecf20 flags 0x48001 ext 0x8c38b338 flags 0x10
  Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1 Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
Loopback0 is up if_handle 0x0800001c if_type IFT_LOOPBACK(0x10)
  idb info 0x898ecda0 flags 0x8061 ext 0x0
  Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Interface is marked as point to point interface
  Interface is marked as loopback interface
  Reference count 1 Next-Hop Count 0
  Protocol Reference count 0
  Protocol ipv6 not configured or enabled on this card
  Primary IPV6 local address NOT PRESENT
Bundle-Ether5 is down if_handle 0x08000014 if_type IFT_ETHERBUNDLE(0x1c)
  idb info 0x898ecd20 flags 0x48001 ext 0x8c38b1e8 flags 0x10
  Vrf Local Info (0x0)
  Interface last modified Dec 15, 2015 16:15:28, modify
  Reference count 1 Next-Hop Count 0
  Forwarding is disabled
  ICMP redirects are never sent
  ICMP unreachables are enabled
  Protocol MTU 9202, TableId 0xe0800000(0x8a1ce6c8)
  Protocol Reference count 1
  Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/79 is down if_handle 0x080002b8 if_type IFT_TENGETHERNET(0x1e)
  idb info 0x898ecca0 flags 0x8001 ext 0x0
  Vrf Local Info (0x0)
  Interface last modified Dec 14, 2015 17:24:58, modify
  Reference count 1 Next-Hop Count 0
  Protocol Reference count 0
  Protocol ipv6 not configured or enabled on this card
  Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/78 is down if_handle 0x080002b0 if_type IFT_TENGETHERNET(0x1e)
```

```
idb info 0x898ecc20 flags 0x8001 ext 0x0
Vrf Local Info (0x0)
Interface last modified Dec 14, 2015 17:24:58, modify
Reference count 1 Next-Hop Count 0
Protocol Reference count 0
Protocol ipv6 not configured or enabled on this card
Primary IPV6 local address NOT PRESENT
TenGigE0/0/0/77 is down if handle 0x080002a8 if_type IFT_TENGETHERNET(0x1e)
idb info 0x898ecba0 flags 0x8001 ext 0x0
Vrf Local Info (0x0)
Interface last modified Dec 14, 2015 17:24:58, modify
Reference count 1 Next-Hop Count 0
Protocol Reference count 0
Protocol ipv6 not configured or enabled on this card
Primary IPV6 local address NOT PRESENT
```

show cef ipv6 resource

IPv6 シスコ エクスプレス フォワーディング (CEF) テーブルの IPv6 非再帰的プレフィックス エントリを表示するには、`show cef ipv6 resource` コマンドを使用します。

`show cef ipv6 resource [detail] [hardware {egress|ingress}] [location node-id]`

構文の説明

detail	(任意) IPv6 CEF テーブルにリストされているリソースの詳細情報を表示します。
hardware	(任意) シスコ エクスプレス フォワーディング (CEF) IPv6 ハードウェア ステータスおよび設定情報を表示します。
egress	(任意) 出力パケットスイッチ交換 (PSE) ファイルから情報を表示します。
ingress	(任意) 入力パケットスイッチ交換 (PSE) ファイルから情報を表示します。
location node-id	(任意) 指定されたノードの IPv6 CEF テーブルの IPv6 リソース エントリを表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの IPv6 CEF 非再帰的ルートが表示されます。

タスク ID	タスク ID	動作
	cef	読み取り

例 次の例は、**show cef ipv6 resource** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 resource
CEF resource availability summary state: GREEN
  ipv4 shared memory resource: GREEN
  ipv6 shared memory resource: GREEN
  mpls shared memory resource: GREEN
  common shared memory resource: GREEN
  TABLE hardware resource: GREEN
  LEAF hardware resource: GREEN
  LOADINFO hardware resource: GREEN
  NHINFO hardware resource: GREEN
  LABEL_INFO hardware resource: GREEN
  IDB hardware resource: GREEN
  FRR_NHINFO hardware resource: GREEN
  LDSH_ARRAY hardware resource: GREEN
  RSRC_MON hardware resource: GREEN
```

show cef ipv6 summary

IPv6 シスコ エクスプレス フォワーディング (CEF) テーブルのサマリーを表示するには、で **show cef ipv6 summary** コマンドを使用します。

show cef ipv6 summary [location node-id]

構文の説明

location node-id (任意) 指定されたノードの IPv6 CEF テーブルのサマリー情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの IPv6 CEF テーブルのサマリーが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**showcefipv6summary** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 summary
IP CEF with switching (Table Version 0)

Load balancing: L3
Tableid 0xe0800000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
Vrfname default, Refcount 12
4 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 288 bytes
```

```

0 load sharing elements, 0 bytes, 0 references
0 shared load sharing elements, 0 bytes
0 exclusive load sharing elements, 0 bytes
0 CEF route update drops, 0 revisions of existing leaves
Resolution Timer: 15s
0 prefixes modified in place
0 deleted stale prefixes
0 prefixes with label imposition, 0 prefixes with label information
Adjacency Table has 44 adjacencies
  1 incomplete adjacency

```

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 19 : *show cef ipv6 summary* コマンドのフィールドの説明

フィールド	説明
Load balancing	現在のロードバランシングモード。デフォルト値は L3 です。
Table Version	CEF テーブルのバージョン。
routes	ルートの合計数。
unresolved (x old, x new)	未解決のルートの合計数。
load sharing elements	内部ロードシェアリングデータ構造の合計数。
bytes	内部ロードシェアリングデータ構造で使われる合計メモリ。
references	すべての内部ロードシェアリングデータ構造の合計リファレンス カウント数。
CEF resets	CEF テーブル リセット数。
revisions of existing leaves	既存のプレフィックスへの更新数。
Exponential (currently xs, peak xs)	現在使用されていません。
prefixes modified in place	正しく修正されたプレフィックス。
Router ID	ルータ ID
Adjacency Table has x adjacencies	合計隣接数。
x incomplete adjacency	未完了の隣接の合計数。

show cef ipv6 unresolved

IPv6 シスコ エクスプレス フォワーディング (CEF) テーブルの未解決ルートを表示するには、`show cef ipv6 unresolved` コマンドを使用します。

`show cef ipv6 unresolved [detail] [hardware {egress| ingress}] [location node-id]`

構文の説明

detail	(任意) 詳細情報を表示します。
hardware	(任意) シスコ エクスプレス フォワーディング (CEF) IPv6 ハードウェア ステータスおよび設定情報を表示します。
egress	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
ingress	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
location node-id	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合は、コマンドが発行されるノードの未解決ルートが表示されます。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、未解決ルートを検出する場合の **show cef ipv6 unresolved** コマンドの出力を示しています。

```
RP/0/# show cef ipv6 unresolved
```

```
9999::/64  
  unresolved
```

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 20 : **show cef ipv6 unresolved** コマンドのフィールドの説明

フィールド	説明
xxxx::/xx	検出された未解決ルート

show cef mpls adjacency

マルチプロトコル ラベル スイッチング (MPLS) 隣接関係テーブルを表示するには、で **show cef mpls adjacency** コマンドを使用します。

show cef mpls adjacency [*interface-type interface-path-id*] [**detail** | **discard** | **drop** | **glean** | **null** | **punt** | **remote**] [**location** *node-id*]

構文の説明

<i>interface-type</i>	(任意) インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
<i>interface-path-id</i>	(任意) 物理インターフェイスインスタンスまたは仮想インターフェイスインスタンスのいずれかです。 <ul style="list-style-type: none"> 物理インターフェイス インスタンス。命名規則は、<i>rack/slot/module/port</i> です。値と値の間には、表記の一部としてスラッシュ マークが必須です。 <ul style="list-style-type: none"> ° <i>rack</i> : ラックのシャーシ番号。 ° <i>slot</i> : ラインカードの物理スロット番号。 ° <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ° <i>port</i> : インターフェイスの物理ポート番号。 (注) ルートプロセッサカード上の管理イーサネットインターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 /CPU0/0 仮想インターフェイスインスタンス。数字の範囲は、インターフェイスタイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。</p>
detail	(任意) 詳細情報を表示します。
discard	(任意) 廃棄隣接情報を表示します。
drop	(任意) ドロップ隣接情報を表示します。
glean	(任意) glean 隣接情報を表示します。
null	(任意) nul隣接情報を表示します。

punt	(任意) パント隣接情報を表示します。
remote	(任意) リモート隣接情報を表示します。
locationnode-id	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード XR EXEC モード

コマンド履歴	リリース	変更内容
	リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **location** キーワードと *node-id* 引数でノードを指定しない場合は、**show cef mpls adjacency** をコマンドを発行したノードの MPLS 隣接関係テーブルが表示されます。

タスク ID	タスク ID	動作
	cef	読み取り

例 次の例は、**show cef mpls adjacency** コマンドの出力を示しています。

```
RP/0/# show cef mpls adjacency hardware egress

Display protocol is mpls
Interface      Address                                     Type      Refcount
-----
Te0/0/0/11    Prefix: 79.0.0.2/32                        local     5
               Adjacency: PT:0x894d40c0 79.0.0.2/32
               Interface: Te0/0/0/11
               NHID: 0x0
               MAC: 6c.9c.ed.28.8b.71.28.c7.ce.01.f0.4f.88.47
               Interface Type: 0x1e, Base Flags: 0x1 (0x8bec8230)
               Nhinfo PT: 0x8bec8230, Idb PT: 0x899f6a20, If Handle: 0x8000090
               Dependent adj type: remote (0x8be85230)
               Dependent adj intf: Te0/0/0/11
               Ancestor If Handle: 0x0
Update time   Dec 17 09:44:45.779
```

```
Show-data Print at RPLC
```

```
TX H/W Result for NP:0 (index: 0x186bc (BE)):
```

```
Next Hop Data
Next Hop Valid:      YES
Next Hop Index:     100028
Egress Next Hop IF: 100028
Hw Next Hop Intf:   17
HW Port:            12
Next Hop Flags:     COMPLETE
Next Hop MAC:       6c9c.ed28.8b71
```

```
NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform
```

```
NHINDEX STATS: pkts 0, bytes 0 (no stats)
```

```
RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef mpls adjacency hardware

マルチプロトコル ラベル スイッチング (MPLS) 隣接ハードウェア ステータスと設定情報を表示するには、で **show cef mpls adjacency hardware** コマンドを使用します。

show cef mpls adjacency hardware {egress| ingress} [detail| discard| drop| glean| location *node-id*] null| punt| remote]

構文の説明

egress	出力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
ingress	入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
detail	(任意) 詳細情報を表示します。
discard	(任意) 廃棄隣接情報を表示します。
drop	(任意) ドロップ隣接情報を表示します。
glean	(任意) glean 隣接情報を表示します。
location <i>node-id</i>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
null	(任意) ノル隣接情報を表示します。
punt	(任意) パント隣接情報を表示します。
remote	(任意) リモート隣接情報を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID

動作

cef

読み取り

例

次の例は、**show cef mpls adjacency hardware** コマンドの出力を示しています。

```
RP/0/# show cef mpls adjacency hardware egress
```

```
Display protocol is mpls
Interface      Address                                     Type      Refcount
-----
Te0/0/0/11    Prefix: 79.0.0.2/32                         local     5
               Adjacency: PT:0x894d40c0 79.0.0.2/32
               Interface: Te0/0/0/11
               NHID: 0x0
               MAC: 6c.9c.ed.28.8b.71.28.c7.ce.01.f0.4f.88.47
               Interface Type: 0x1e, Base Flags: 0x1 (0x8bec8230)
               Nhinfo PT: 0x8bec8230, Idb PT: 0x899f6a20, If Handle: 0x8000090
               Dependent adj type: remote (0x8be85230)
               Dependent adj intf: Te0/0/0/11
               Ancestor If Handle: 0x0
Update time Dec 17 09:44:45.779
```

```
Show-data Print at RPLC
```

```
TX H/W Result for NP:0 (index: 0x186bc (BE)):
```

```
Next Hop Data
Next Hop Valid:      YES
Next Hop Index:     100028
Egress Next Hop IF: 100028
Hw Next Hop Intf:   17
HW Port:            12
Next Hop Flags:     COMPLETE
Next Hop MAC:       6c9c.ed28.8b71
```

```
NHINDEX H/W Result for NP:0 (index: 0 (BE)):
NhIndex is NOT required on this platform
```

```
NHINDEX STATS: pkts 0, bytes 0 (no stats)
```

```
RX H/W Result on NP:0 [Adj ptr:0x40 (BE)]:
Rx-Adj is NOT required on this platform
```

show cef mpls interface

インターフェイスのマルチプロトコル ラベル スイッチング (MPLS) シスコ エクスプレス フォワーディング (CEF) の関連情報を表示するには、`show cef mpls interface` コマンドを使用します。

`show cef mpls interface type interface-path-id [detail] [location node-id]`

構文の説明

type インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用します。

interface-path-id 次に示す、物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスのいずれかです。

- 物理インターフェイス インスタンス。名前表記は *rack/slot/module/port* です。値の間に表記の一部としてスラッシュが必要です。

- *rack* : ラックのシャーシ番号。

- *slot* : モジュラ サービス カードまたはラインカードの物理スロット番号。

- *module* : モジュール番号。物理層インターフェイスモジュール (PLIM) は、常に 0 です。

- *port* : インターフェイスの物理ポート番号。

(注) ルートプロセッサ カード上の管理イーサネット インターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0

- 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。

ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。

detail (任意) コマンドが発行されるノードのすべてのインターフェイスに関する CEF 詳細情報を表示します。

location node-id (任意) インターフェイスの IPv4 CEF 関連情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location キーワードと *node-id* 引数でノードを指定しない場合、**show cef mpls interface** コマンドは、ルートプロセッサのインターフェイスの CEF 関連情報を表示します。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef mpls interface** コマンドの出力を示しています。

```
RP/0/# show cef mpls interface

fib_show_interface
Loopback0 is up if_handle 0x08000014 if_type IFT_LOOPBACK(0x10)
  idb info 0x899f78a0 flags 0x8061 ext 0x0
  Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:15, create
  Interface is marked as point to point interface
  Interface is marked as loopback interface
  Reference count 1      Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
mpls v6 item name: 1000/protocol/1/vrf/default/interface-info/2/8000090
TenGigE0/0/0/11 is up if_handle 0x08000090 if_type IFT_TENGETHERNET(0x1e)
  idb info 0x899f6a20 flags 0x8001 ext 0x8bf0b098 flags 0x50
  Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:12, create
  Reference count 1      Next-Hop Count 2
  Forwarding is enabled
  Protocol MTU 1500, TableId 0(0x8a287098)
  Protocol Reference count 2
TenGigE0/0/0/1 is up if_handle 0x08000040 if_type IFT_TENGETHERNET(0x1e)
  idb info 0x899f6520 flags 0x8001 ext 0x0
  Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:42:12, create
  Reference count 1      Next-Hop Count 0
  Protocol Reference count 0
  Protocol mpls not configured or enabled on this card
Null0 is up if_handle 0x0800000c if_type IFT_NULL(0x11)
  idb info 0x899f61a0 flags 0x8061 ext 0x0
  Vrf Local Info (0x0)
  Interface last modified Dec 17, 2015 09:41:51, create
  Interface is marked as point to point interface
  Interface is marked as nullidb
```

```
Reference count 1      Next-Hop Count 0
Protocol Reference count 0
Protocol mpls not configured or enabled on this card
FINT0/RP0/CPU0 is up if_handle 0x08000010 if_type IFT_FINT_INTF(0x1b)
  idb info 0x899f6120 flags 0x8021 ext 0x0
  Vrf Local Info (0x0)
Interface last modified Dec 17, 2015 09:41:51, create
Interface is marked as point to point interface
Reference count 1      Next-Hop Count 0
Protocol Reference count 0
Protocol mpls not configured or enabled on this card
```

show cef mpls unresolved

マルチプロトコル ラベル スイッチング (MPLS) 未解決ルートを表示するには、で **show cef mpls unresolved** コマンドを使用します。

show cef mpls unresolved [detail] [location node-id]

構文の説明

detail	(任意) レイヤ 2 情報など、隣接の詳細情報を表示します。
location node-id	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef mpls unresolved** コマンドの出力を示しています。

```
RP/0/# show cef mpls unresolved
```

```
Label/EOS           Next Hop           Interface
20001/0
20001/1
```

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 cef mpls unresolved* コマンドのフィールドの説明

フィールド	説明
Label/EOS	MPLS 転送ラベル/End of Stack (EOS) ビット
Next Hop	プレフィックスのネクスト ホップ
Interface	プレフィックスに関連付けられているインターフェイス

show cef summary

シスコ エクスプレス フォワーディング (CEF) テーブルのサマリー情報を表示するには、**show cef summary** コマンドを使用します。

show cef summary [**location** {*node-id*} **all**]

構文の説明

location <i>node-id</i>	(任意) 指定したノードの詳細な CEF 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
all	(任意) すべてのロケーションを表示します。

コマンド デフォルト

show cef summary コマンドでは、IPv4 CEF テーブルとアクティブな RP ノードはロケーションと見なされます。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
cef	読み取り

例

次の例は、**show cef summary** コマンドの出力を示しています。

```
RP/0/# show cef summary location 0/RP0/CPU0
Router ID is 10.1.1.1
IP CEF with switching (Table Version 0) for node0_1_CPU0
```

```

Load balancing: L3
Tableid 0xe0000000, Vrfid 0x60000000, Vrid 0x20000000, Flags 0x301
Vrfname default, Refcount 318
170 routes, 0 reresolve, 0 unresolved (0 old, 0 new), 12240 bytes
183 load sharing elements, 57292 bytes, 184 references
19 shared load sharing elements, 7036 bytes
164 exclusive load sharing elements, 50256 bytes
0 CEF route update drops, 10 revisions of existing leaves
Resolution Timer: 15s
0 prefixes modified in place
0 deleted stale prefixes
21 prefixes with label imposition, 60 prefixes with label information
Adjacency Table has 49 adjacencies
25 incomplete adjacencies

```

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 22: *show cef summary* コマンドのフィールドの説明

フィールド	説明
Load balancing	現在のロードバランシングモード。デフォルト値は L3 です。
Table Version	CEF テーブルのバージョン。
tableid	テーブル ID 番号。
vrfname	VRF 名。
flags	テーブルのオプション値。
ルート	ルートの合計数。
reresolve	再解決されるルートの合計数。
unresolved (x old, x new)	未解決のルートの合計数。
load sharing elements	内部ロードシェアリングデータ構造の合計数。
bytes	内部ロードシェアリングデータ構造で使 用される合計メモリ。
references	すべての内部ロードシェアリングデータ構造 の合計リファレンス カウント数。
CEF resets	CEF テーブル リセット数。
revisions of existing leaves	既存のプレフィックスへの更新数。
Exponential (currently xs, peak xs)	現在使用されていません。
prefixes modified in place	正しく修正されたプレフィックス。

フィールド	説明
Adjacency Table has x adjacencies	合計隣接数。
x incomplete adjacency	未完了の隣接の合計数。



ホストサービスおよびアプリケーションコマンド

この章では、ドメインネームシステム (DNS)、Telnet、ファイル転送プロトコル (FTP)、簡易ファイル転送プロトコル (TFTP)、リモートコピープロトコル (RCP) など、ホストサービスやアプリケーションを設定したりモニタする際に使用するコマンドについて説明します。

ホストサービスおよびアプリケーションの概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [cinetd rate-limit](#), 175 ページ
- [clear host](#), 176 ページ
- [destination address \(ipsla\)](#) , 178 ページ
- [domain ipv4 host](#), 180 ページ
- [domain ipv6 host](#), 182 ページ
- [domain list](#), 184 ページ
- [domain lookup disable](#), 186 ページ
- [domain name \(IPAddr\)](#) , 187 ページ
- [domain name-server](#), 188 ページ
- [ftp client anonymous-password](#), 190 ページ
- [ftp client passive](#), 191 ページ
- [ftp client password](#), 193 ページ
- [ftp client source-interface](#), 195 ページ
- [ftp client username](#), 197 ページ
- [logging source-interface](#) , 198 ページ
- [ping \(ネットワーク\)](#) , 200 ページ

- ping bulk (ネットワーク) , 203 ページ
- scp, 205 ページ
- show cinetd services, 207 ページ
- show hosts, 209 ページ
- telnet, 211 ページ
- telnet client source-interface, 215 ページ
- telnet dscp, 217 ページ
- telnet server, 219 ページ
- telnet transparent, 221 ページ
- tftp client source-interface, 222 ページ
- tftp server, 224 ページ
- traceroute, 226 ページ

cinetd rate-limit

Cisco inetd (Cinetd) で許容されるサービス要求のレート制限を設定するには、XR コンフィギュレーションモードで **cinetd rate-limit** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

cinetd rate-limit *value*

no cinetd rate-limit *value*

構文の説明

value	1 秒あたりに許可されるサービス リクエストの総数です。範囲は 1 ~ 100 です。デフォルト値は 1 です。
-------	--

コマンド デフォルト

1 秒あたりに 1 回のサービス リクエストが許可されます。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

レート制限を超過したサービス リクエストは拒否されます。レート制限はアプリケーションごとに適用されます。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次の例では、**cinetd rate-limit** に 10 が設定されています。

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# cinetd rate-limit 10
```

clear host

hostname-to-address キャッシュから一時エントリを削除するには、XR EXEC モードで **clear host** コマンドを使用します。

clear host {*host-name* | *}

構文の説明

host-name	削除するホストの名前。
*	ローカルキャッシュのすべてのエントリを削除するように指定します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

キャッシュ内のダイナミック ホスト エントリがクリアされます。

キャッシュ内の一時エントリがクリアされます。 [domain ipv4 host, \(180 ページ\)](#) コマンドまたは [domain ipv6 host, \(182 ページ\)](#) コマンドで入力された永続エントリはクリアされません。

デフォルトでは、スタティック マッピングは設定されません。

タスク ID

タスク ID	動作
ip-services	実行

例

次に、hostname-and-address キャッシュからすべての一時エントリをクリアする方法の例を示します。

```
RP/0/RP0/CPU0:router# clear host *
```

destination address (ipsla)

宛先デバイスのアドレスを設定するには、IP SLA エコー コンフィギュレーション モードで **destination address** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を入力します。

destination address*address*

no destination address*address*

構文の説明

address 宛先デバイスの IPv4/IPv6 アドレスを指定します。

コマンド デフォルト

なし

コマンド モード

IP SLA エコー 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
monitor	読み取り、書き込み

例

次の例は、デバイスの宛先アドレスとして 10.10.10.20 を設定する方法を示しています。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# ipsla
RP/0/RP0/CPU0:router (config-ipsla)# operation 500
RP/0/RP0/CPU0:router (config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router (config-ipsla-echo)# timeout 5000
```

```
RP/0/RP0/CPU0:router(config-ipsla-echo)# destination address 10.10.10.20
```

domain ipv4 host

IPv4 を使用するホスト キャッシュにスタティックな `hostname-to-address` マッピングを定義するには、XR コンフィギュレーションモードで **domain ipv4 host** コマンドを使用します。コンフィギュレーション ファイルから **domain ipv4 host** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

domain ipv4 host *host-name* *v4address2*.....*v4address8*

no domain ipv4 host *host-name* *v4address1*

構文の説明

host-name	ホストの名前。名前の冒頭は、文字と数字のいずれも使用できません。
v4address1	対応付けられる IP アドレス。
v4address2...v4address8	(任意) 対応付けられる追加の IP アドレス。ホスト名 1 つに最大 8 つのアドレスをバインドできます。

コマンド デフォルト

スタティック マッピングは設定されません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

名前の冒頭は、文字と数字のいずれも使用できます。数字を使用すると、実行可能な操作 (**ping** など) が制限されます。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み
basic-services	読み取り、書き込み

例 次に、2種類の IPv4 スタティック マッピングの定義方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# domain ipv4 host host1 192.168.7.18
RP/0/RP0/CPU0:router(config)# domain ipv4 host host2 10.2.0.2 192.168.7.33
```

domain ipv6 host

IPv6 を使用するホスト キャッシュにスタティックな `hostname-to-address` マッピングを定義するには、XR コンフィギュレーションモードで **domain ipv6 host** コマンドを使用します。コンフィギュレーション ファイルから **domain ipv6 host** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

domain ipv6 host *host-name* *v6address1* [*v6address2**v6address4*]

no domain ipv6 host *host-name* *v6address1*

構文の説明

host-name	ホストの名前。名前の冒頭は、文字と数字のいずれも使用できません。
v6address1	対応付けられる IP アドレス。
v6address2...v6address4	(任意) 対応付けられる追加の IP アドレス。ホスト名 1 つに最大 4 つのアドレスをバインドできます。

コマンド デフォルト

スタティック マッピングは設定されません。IPv6 アドレスプレフィックスはイネーブルではありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

名前の冒頭は、文字と数字のいずれも使用できます。数字を使用すると、実行可能な操作 (**ping** など) が制限されます。

タスク ID

タスク ID	動作
ip services	読み取り、書き込み

例 次に、2種類のIPv6スタティックマッピングの定義方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# domain ipv6 host host1 ff02::2  
RP/0/RP0/CPU0:router(config)# domain ipv6 host host2 ff02::1
```

domain list

修飾子がないホスト名を補完するためのデフォルトドメイン名のリストを定義するには、XR コンフィギュレーションモードで **domain list** コマンドを使用します。リストから名前を削除するには、このコマンドの **no** 形式を使用します。

domain list *domain-name*

no domain list *domain-name*

構文の説明

domain-name	ドメイン名。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。
-------------	---

コマンド デフォルト

ドメイン名は定義されません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ドメインリストがない場合、[domain name \(IPAddr\)](#)、[\(187 ページ\)](#) コマンドで指定したドメイン名が使用され、未修飾のホスト名が完成します。ドメインリストがある場合、デフォルトのドメイン名は使用されません。**domain list** コマンドは [domain name \(IPAddr\)](#)、[\(187 ページ\)](#) コマンドとほぼ同じですが、相違点として、**domain list** コマンドでは順番に試行されるドメインのリストを定義できます。

タスク ID

タスク ID	動作
ip-service	読み取り、書き込み

例

次に、複数のドメイン名を 1 つのリストに追加する方法について例を示します。

```
RP/0/RP0/CPU0:router(config)# domain list domain1.com  
RP/0/RP0/CPU0:router(config)# domain list domain2.edu
```

次の例では、リストに名前を追加し、その後、名前を削除する方法を示します。

```
RP/0/RP0/CPU0:router(config)# domain list domain3.edu  
RP/0/RP0/CPU0:router(config)# no domain list domain2.edu
```

domain lookup disable

IP ドメイン ネーム システム (DNS) に基づいた `hostname-to-address` の変換をディセーブルにするには、XR コンフィギュレーション モードで **domain lookup disable** コマンドを使用します。指定したコマンドをコンフィギュレーション ファイルから削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

domain lookup disable

no domain lookup disable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IP DNS に基づいた `host-to-address` 変換はイネーブルです。

コマンド モード

XR 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
リリース 6.0	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 コマンドを使用すると、コンフィギュレーション ファイルから指定のコマンドが削除され、システムはデフォルトの状態に戻ります。このコマンドの **no** 形式はコンフィギュレーション ファイルに保存されません。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、IP DNS に基づいた `hostname-to-address` 変換をイネーブルにする例を示します。

```
RP/0/RP0/CPU0:router(config)# domain lookup disable
```

domain name (IPAddr)

修飾子がないホスト名を補完するために使用されるデフォルトのドメイン名を定義するには、適切なモードで **domain name** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。

domain name *domain-name*

no domain name *domain-name*

構文の説明

domain-name	未修飾のホスト名を完成するためのデフォルトのドメイン名。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。
-------------	---

コマンド デフォルト

デフォルトのドメイン名はありません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ホスト名にドメイン名が含まれていない場合は、ドットと **domain name** コマンドで設定されたドメイン名がホスト名に付加され、その後ホスト名がホスト テーブルに追加されます。

domain name コマンドでドメイン名が設定されていない場合にホスト名のみを入力すると、要求は検索されません。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

domain name-server

名前とアドレスの解決に使用する 1 つ以上のネーム サーバのアドレスを指定するには、XR コンフィギュレーションモードで **domain name-server** コマンドを使用します。指定した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。

domain name-server *server-address*

no domain name-server *server-address*

構文の説明

server-address	ネーム サーバの IP アドレス
----------------	------------------

コマンド デフォルト

ネーム サーバのアドレスが指定されていない場合、デフォルトのネーム サーバのアドレスは 255.255.255.255 になります。IPv4 および IPv6 のアドレス プレフィックスはイネーブルになりません。

コマンド モード

XR 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
リリース 6.0	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 つのアドレスを入力できますが、各コマンドでは 1 つずつしか指定できません。

ネーム サーバのアドレスが指定されていない場合にデフォルトのネーム サーバのアドレスが 255.255.255.255 になるため、DNS ルックアップをローカルネットワークセグメントにブロードキャストできます。ローカルネットワーク上に DNS サーバがあれば、それが応答します。DNS サーバがなくても、DNS 要求を正しい DNS サーバに転送する方法を知っているサーバが置かれている場合もあります。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、ホスト 192.168.1.111 をプライマリ ネーム サーバとして指定し、ホスト 192.168.1.2 をセカンダリ サーバとして指定する方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.111  
RP/0/RP0/CPU0:router(config)# domain name-server 192.168.1.2
```

ftp client anonymous-password

匿名ユーザにパスワードを割り当てるには、XR コンフィギュレーション モードで **ftp client anonymous-password** コマンドを使用します。コンフィギュレーション ファイルから **ftp client anonymous-password** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

ftp client anonymous-password *password*

no ftp client anonymous-password

構文の説明

password 匿名ユーザにパスワードを割り当てます。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ftp client anonymous-password コマンドはファイル転送プロトコル (FTP) サーバに応じて異なります。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、xxxx への匿名パスワードの設定方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# ftp client anonymous-password xxxx
```

ftp client passive

パッシブ ファイル転送プロトコル (FTP) 接続だけを使用するようにソフトウェアを設定するには、XR コンフィギュレーションモードで **ftp client passive** コマンドを使用します。コンフィギュレーション ファイルから **ftp client passive** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

ftp client passive

no ftp client passive

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

FTP のデータ接続はアクティブです。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ftp client passive コマンドを使用すると、パッシブ モードの FTP 接続だけを確立できます。FTP 接続の送信元 IP アドレスを指定するには、**ftp client source-interface** コマンドを指定します。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、ネットワーキングデバイスでパッシブ FTP 接続だけを使用するように設定する例を示します。

```
RP/0/RP0/CPU0:router(config)# ftp client passive
1d:3h:54:47: ftp_fs[16437]: FTP: verifying tuple passive (SET).
```

```
1d:3h:54:47: ftp_fs[16437]: FTP: applying tuple passive (SET).  
1d:3h:54:47: ftp_fs[16437]: FTP: passive mode has been enabled.
```

ftp client password

ファイル転送プロトコル (FTP) 接続のパスワードを指定するには、XR コンフィギュレーションモードで **ftp client password** 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。

```
ftp client password {clear-text-password| clear clear-text password| encrypted encrypted-text password}
no ftp client password {clear-text-password| clear clear-text password| encrypted encrypted-text password}
```

構文の説明

<code>clear-text-password</code>	暗号化していない (クリアテキスト) ユーザパスワードを指定します。
<code>clear</code> <i>clear-text password</i>	暗号化していない (クリアテキスト) 共有パスワードを指定します。
<code>encrypted</code> <i>encrypted-text password</i>	暗号化された共有パスワードを指定します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、ファイル転送プロトコル (FTP) 接続にパスワードを指定する例を示します。

```
RP/0/RP0/CPU0:router(config)# ftp client password lab
```

ftp client source-interface

ファイル転送プロトコル (FTP) 接続の送信元 IP アドレスを指定するには、XR コンフィギュレーション モードで **ftp client source-interface** コマンドを使用します。コンフィギュレーション ファイルから **ftp client source-interface** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

ftp client source-interface *type interface-path-id*

no ftp client source-interface *type interface-path-id*

構文の説明

<i>type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

コマンド デフォルト

FTP の送信元アドレスは、ネットワーキング デバイスから脱退するために FTP パケットで使用されたインターフェイスの IP アドレスです。

コマンド モード

XR 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
リリース 6.0	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 FTP 接続に同一の送信元アドレスを設定するにはこのコマンドを使用します。パッシブ FTP 接続だけを使用するようにソフトウェアを設定するには、**ftp client passive** コマンドを使用します。

タスク ID

タスク ID

動作

ip-services

読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/1/2/1 に関連付けられている IP アドレスを、すべての FTP パケットの送信元アドレスとして設定する方法を示しています。実際のパケット送信にどのインターフェイスが使用されるかは問いません。

```
RP/0/RP0/CPU0:router(config)# ftp client source-interface tenGigE0/1/2/1
```

ftp client username

ファイル転送プロトコル (FTP) 接続のユーザ名を指定するには、XR コンフィギュレーションモードで **ftp client username** 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、コマンドの **no** 形式を使用します。

ftp client username *username*

no ftp client username *username*

構文の説明

username	FTP ユーザの名前
----------	------------

コマンドモード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次に、FTP 接続のユーザ名を指定する方法の例を示します。

```
RP/0/RP0/CPU0:router(config)# ftp client username brownfox
```

logging source-interface

特定のルータから発信される syslog トラフィックを単一のデバイスからの着信として識別できるように、ロギング送信元インターフェイスを設定するには、XR コンフィギュレーション モードで **logging source-interface** コマンドを使用します。送信元インターフェイス ロギング設定を削除するには、このコマンドの **no** 形式を使用します。

logging source-interface *interface*

no logging source-interface *interface*

構文の説明

interface 送信元のインターフェイス番号

コマンド デフォルト

vrf-name が指定されていない場合は、デフォルトの VRF に対して送信元インターフェイスが設定されます。

コマンド モード

XR 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
リリース 6.0	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、syslog メッセージには、ルータから出るために使用されるインターフェイスの IPv4 または IPv6 アドレスが含まれています。**logging source-interface** コマンドは、パケットがどのインターフェイスを使用してルータから出るかに関係なく、特定のインターフェイスの IPv4 または IPv6 アドレスを含むように syslog パケットを設定します。

タスク ID

タスク ID	動作
logging	読み取り、書き込み

例

次の例は、VRF vrf1 のロギング送信元インターフェイスとしてインターフェイス ループバック 0 を設定する方法を示しています。

```
RP/0/RP0/CPU0:router#logging source-interface loopback 0 vrf vrf1
RP/0/RP0/CPU0:router#logging source-interface loopback 1 vrf default
```

次の例は、VRF に対して適切に設定されているロギング送信元インターフェイスを示しています。

```
RP/0/RP0/CPU0:router#show running configuration logging
```

```
logging trap debugging
logging 223.255.254.249 vrf vrf1
logging 223.255.254.248 vrf default
logging source-interface Loopback0 vrf vrf1
logging source-interface Loopback1
```

ping (ネットワーク)

IP ネットワーク上のホストへの到達可能性とネットワーク接続をチェックするには、XR EXEC モードで **ping** コマンドを使用します。

ping [**ipv4** | **ipv6**] [*host-name* | *ip-address*] [**count** *number*] [**size** *number*] [**source** {*ip-address* | **type** *number*}] [**timeout** *seconds*] [**pattern** *number*] [**type** *number*] [**priority** *number*][**verbose**] [**donnotfrag**] [**validate**] [**sweep**]

構文の説明

ipv4	(任意) IPv4 アドレスのプレフィックスを指定します。
A.B.C.D	擬似回線のターゲット終了アドレス。
<i>host-name</i>	(任意) ping を実行するためのシステムのホスト名。
<i>ip-address</i>	(任意) ping を実行するためのシステムの IP アドレス。
count <i>number</i>	(任意) 繰り返しのカウントを設定します。範囲は 0 ~ 2147483647 です。
size <i>number</i>	(任意) データグラムのサイズを設定します。範囲は 36 ~ 18024 です。
<i>source</i>	(任意) 送信元アドレスまたは送信元インターフェイスを識別します。
type <i>number</i>	(任意) サービスタイプを設定します。範囲は 0 ~ 255 です。 ipv4 キーワードが指定されている場合に使用できます。
timeout <i>seconds</i>	(任意) タイムアウトを設定します (秒数)。範囲は 0 ~ 3600 です。
priority <i>number</i>	(任意) パケットの優先順位を設定します。範囲は 0 ~ 15 です。 ipv6 キーワードが指定されている場合に使用できます。
pattern <i>number</i>	(任意) データパターンを設定します。範囲は 0 ~ 65535 です。
<i>verbose</i>	(任意) 詳細な出力を設定します。
donnotfrag	(任意) IP ヘッダーに Don't Fragment (DF) ビットを設定します。
validate	(任意) 戻りパケットを検証します。
sweep	(任意) ping スイープを設定します。

コマンド モデル

XR EXEC の動作または値はありません。

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ping コマンドのデフォルト値は、ターゲット IP アドレスだけを参照します。ターゲット IP アドレスで利用可能なデフォルト値はありません。

ping プログラムはエコー要求パケットをあるアドレスに送信して応答を待ちます。ping 出力により、パス/ホスト間の信頼性やパス上の遅延を評価したり、ホストが到達可能かどうか、または機能しているかどうかを確認したりできます。



(注) **ping** (EXEC) コマンドは IP ネットワークでのみサポートされます。

ホスト名または IP アドレスを指定せずにコマンドを入力すると、ターゲットの IP アドレスおよび他の複数のコマンドパラメータを指定するようにシステムから要求されます。ターゲットの IP アドレスを指定すると、残りのパラメータに対する代替値を指定できます。あるいは表示された各パラメータのデフォルト値を受け入れることも可能です。

システムでホストのアドレスをマッピングできない場合は、「%Unrecognized host or address, or protocol not running」というエラーメッセージが返されます。

ping セッションを異常終了させるには、エスケープシーケンス (デフォルトでは Ctrl-C) を入力します。デフォルトのエスケープシーケンスは、Ctrl キーと C キーを同時に押してから離します。

次の表に、ping 機能で送信されるテスト文字の説明を示します。

表 23: ping テスト文字

文字	説明
!	感嘆符は応答の受信を意味します。
.	ピリオドはネットワークサーバの応答待機中にタイムアウトしたことを意味します。
?	パケットタイプが不明です。
U	「destination unreachable」エラーを示すプロトコルデータユニット (PDU) を受信しました。
C	「輻輳に遭遇した」パケットを受信したことを示します。

文字	説明
M	フラグメンテーションが必要ですが、IP ヘッダーに「don't fragment」ビットが設定されています。このビットが設定されていると、IP レイヤはパケットをフラグメント化せず、パケットのサイズが最大伝送サイズを超過した送信元にインターネット制御メッセージプロトコル (ICMP) エラーメッセージを返します。このビットが設定されていない場合は、IP レイヤはこのパケットをフラグメント化してネクストホップに転送します。
Q	ソースクエンチパケットを受信しました。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み、実行

例

IPv4 と IPv6 では正確なダイアログは多少異なりますが、次の出力例に示すように、デフォルト値を使用する ping セッションでは両者はほぼ同一です。

```
RP/0/RP0/CPU0:router# ping

Protocol [ipv4]:
Target IP address: 10.0.0.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface: 10.0.0.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.25.58.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/49 ms
```

ping コマンドと同じ行にホスト名またはアドレスを入力すると、そのホスト名またはアドレスのプロトコルタイプに適したデフォルトのアクションが実行されます (次の出力例を参照)。

```
RP/0/RP0/CPU0:router# ping server01

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
```

ping bulk (ネットワーク)

IP ネットワーク上の複数のホストへの到達可能性とネットワーク接続をチェックするには、XR EXEC モードで **ping bulk** コマンドを使用します。

ping bulk ipv4 [input cli [batch| inline]]

構文の説明

ipv4	IPv4 アドレス プレフィックスを指定します。
input	入力モードを指定します。
cli	CLI によって入力を指定します。
batch	すべての宛先の後の ping は入力です。
inline	各宛先の後の ping は入力です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

[Enter] ボタンを押し、宛先アドレスを 1 行に 1 つずつ指定する必要があります。
CLI モードまたはバッチ モードで指定できる宛先の最大数は 2000 です。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み、実行

例

次に、CLI 方式で入力して、多くのホストに ping を実行する例を示します。

```
RP/0/RP0/CPU0:router# ping bulk ipv4 input cli batch

Please enter input via CLI with one destination per line and when done Ctrl-D/(exit)
to initiate pings:
1: vrf myvrf1 10.2.1.16
2:
Starting pings...
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.1.16, vrf is myvrf1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/9 ms

RP/0/RP0/CPU0:router# ping bulk ipv4 input cli

Please enter input via CLI with one destination per line:
vrf myvrf1 1.1.1.1
vrf myvrf2 2.2.2.2
vrf myvrf1 myvrf1.cisco.com
vrf myvrf2 myvrf2.cisco.com

Starting pings...
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/1/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
Sending 1, 100-byte ICMP Echos to 1.1.1.1, vrf is myvrf1:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 1/4/1 ms
Sending 2, 100-byte ICMP Echos to 2.2.2.2, vrf is myvrf2:
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/3/1 ms
```

scp

ローカルディレクトリからリモートディレクトリに、またはリモートディレクトリからローカルディレクトリに安全にファイルを転送するには、XR EXEC モードで **scp** コマンドを使用します。

```
scp {local-directory|username@location/directory}/filename {username@location/directory|local-directory}/filename
```

構文の説明

<i>local-directory</i>	デバイス上のローカルディレクトリを指定します。
<i>username@location /directory</i>	<i>location</i> がリモートデバイスの IP アドレスであるリモートディレクトリを指定します。
<i>filename</i>	転送するファイルの名前を指定します。

コマンドデフォルト

なし

コマンドモード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

セキュアコピープロトコル (SCP) は、ファイルを転送するための認証されたセキュアな方式を提供するファイル転送プロトコルです。SCP は SSHv2 に依存して、リモートロケーションからローカルロケーションに、またはローカルロケーションからリモートロケーションにファイルを転送します。

ローカルデバイスから宛先デバイスに、または宛先デバイスからローカルデバイスにファイルをコピーするには、**scp** コマンドを使用します。

SCP では、個々のファイルの転送のみを実行できます。リモートデバイスから別のリモートデバイスにファイルを転送することはできません。

リモートデバイスで SSH サーバプロセスを実行している必要があります。

タスク ID	タスク ID	動作
	ip-services	読み取り、書き込み

例

次の例は、**scp** コマンドを使用して、ローカルディレクトリからリモートディレクトリにファイルをコピーする方法を示しています。

```
RP/0/RP0/CPU0:router# scp /usr/file1.txt root@209.165.200.1:/root/file3.txt
```

```
Connecting to 209.165.200.1...
```

```
Password:
```

```
Transferred 553065 Bytes
```

```
553065 bytes copied in 0 sec (7576232)bytes/sec
```

次の例は、**scp** コマンドを使用して、リモートディレクトリからローカルディレクトリにファイルをコピーする方法を示しています。

```
RP/0/RP0/CPU0:router# scp root@209.165.200.1:/root/file4.txt /usr/file.txt
```

```
Connecting to 209.165.200.1...
```

```
Password:
```

```
Transferred 553065 Bytes
```

```
553065 bytes copied in 0 sec (7576232)bytes/sec
```

show cinetd services

要求の受信時に Cinetd によってプロセスが生成されたサービスを表示するには、XREXEC モードで **show cinetd services** コマンドを使用します。

show cinetd services

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ip-services	読み取り

例

次の例は、**show cinetd services** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show cinetd services
Vrf Name          Family Service Proto Port ACL max_cnt curr_cnt wait Program Client Option
context-management v4 telnet tcp 23 100 0 nowait telnetd sysdb
default           v4 telnet tcp 23 100 2 nowait telnetd sysdb
```

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 24 : show cinetd services コマンドのフィールドの説明

フィールド	説明
Family	ネットワーク層のバージョン (IPv4 または IPv6)。
Service	ネットワーク サービス (FTP、Telnet など)。
Proto	サービスで使用する転送プロトコル (tcp または udp)。
Port	サービスで使用するポート番号。
ACL	一部のホストに対するサービスを制限するために使用するアクセス リスト。
max_cnt	1 つのサービスに許可される並列サーバの最大数。
curr_cnt	1 つのサービスに許可される並列サーバの現在の数。
wait	次の要求を処理するまでに Cinetd がサービスを待機する必要があるかどうかを示すステータス。
Program	サービスのプログラムの名前。
Option	サービスに固有のオプション。

show hosts

デフォルトのドメイン名、ネームルックアップサービスのスタイル、ネームサーバホストのリスト、ホスト名とアドレスのキャッシュリストを表示するには、XR EXEC モードで **show hosts** コマンドを使用します。

show hosts [*host-name*]

構文の説明

host-name (任意) 情報を表示するホストの名前。省略すると、ローカルキャッシュ内のすべてのエントリが表示されます。

コマンド デフォルト

IPv4 アドレス プレフィックスが設定されている場合は、ユニキャスト アドレス プレフィックスがデフォルトです。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ip-services	読み取り

例

次の例は、**show hosts** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host                Flags          Age (hr)   Type          Address(es)
```

```
host1.cisco.com (temp, OK) 1 IP 192.168.4.10
abc (perm, OK) 0 IP 10.0.0.0 10.0.0.2 10.0.0.3
```

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 25: *show hosts* コマンドのフィールドの説明

フィールド	説明
Default domain	未修飾のホスト名を完成するためのデフォルトのドメイン。
Name/address lookup	ルックアップがディセーブルに指定されている、または、ドメインサービスを使用していると表示されます。
Name servers	設定されているネーム サーバのリスト。
Host	ホスト名。
Flags	<p>エントリのステータスを示します。</p> <ul style="list-style-type: none"> • temp : ネーム サーバで入力される一時エントリ。72 時間以上非アクティブなエントリは削除されます。 • perm : コンフィギュレーション コマンドで入力される永続エントリ。このエントリはタイムアウトしません。 • OK : エントリは有効と見なされます。 • ?? : エントリは問題があると疑われ、再検証の対象となります。 • EX : エントリは期限切れです。
Age(hr)	ソフトウェアによる最新のキャッシュエントリ参照からの経過時間。
Type	アドレス タイプ (IPv4 または IPv6) 。
Address(es)	ホストのアドレス1 ホストあたり最大 8 つのアドレスを指定できます。

telnet

Telnet をサポートしているホストにログインするには、XR EXEC モードで **telnet** コマンドを使用します。

telnet {*ip-address*|*host-name*} [*options*]

構文の説明

ip-address	ネットワークにある特定のホストの IP アドレス。
	<ul style="list-style-type: none"> • IPv4 アドレス形式： (<i>x.x.x.x</i>) 形式で入力する必要があります。 • IPv6 アドレス形式：アドレスは、RFC 2373 に記載されている、コロンを区切り文字に使用し、16 進数表記の 16 ビット値で指定した形式で入力する必要があります。
host-name	ネットワークにある特定のホストの名前。
options	(任意) Telnet 接続オプション。サポート対象のオプションのリストについては、 表 26 : Telnet 接続オプション , (212 ページ) を参照してください。

コマンド デフォルト

Telnet クライアントは Telnet 接続オプションが `nostream` モードです。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン Telnet サーバがイネーブルの場合は、有効なユーザ名およびパスワードがある限り、Telnet セッションを開始することができます。

次の表に、サポート対象の Telnet 接続オプションを示します。

表 26 : Telnet 接続オプション

オプション	説明
/stream	ストリーム処理をオンにします。これにより、Telnet の制御シーケンスなしの raw TCP ストリームがイネーブルになります。ストリーム接続は Telnet オプションを処理せず、UNIX 間コピー プログラム (UUCP) や他の非 Telnet プロトコルを実行するポート接続に適している場合があります。
/nostream	ストリーム処理をオフにします。
port number	ポート番号。範囲は 0 ~ 65535 です。
/source-interface	送信元インターフェイスを指定します。

利用可能なホストのリストを表示するには、**show hosts** コマンドを使用します。すべての TCP 接続のステータスを表示するには、**show tcp** コマンドを使用します。

ソフトウェアから各接続に論理名が割り当てられ、これらの名前を使用する複数のコマンドによって接続が識別されます。名前がすでに使用されている場合と **name-connection EXEC** コマンドで接続名が変更された場合を除き、論理名はホスト名と同じになります。この名前が使用中の場合、ソフトウェアによりヌル名が接続に割り当てられます。

Telnet ソフトウェアは Telnet シーケンス形式の特殊な Telnet コマンドをサポートします。このシーケンスは、一般的な端末制御機能をオペレーティング システム固有の機能にマッピングします。特殊な Telnet コマンドを発行するには、エスケープ シーケンスを入力してからコマンド文字を入力します。デフォルトのエスケープ シーケンスは、Ctrl-^ (Control キーと Shift キーを押しながら数字の 6 キーを押す) です。大文字のコマンド文字は Ctrl キーを押しながら、小文字のコマンド文字は Ctrl キーを離して入力するとそれぞれ入力できます。表 27 : 特殊な Telnet のエスケープ シーケンス、(212 ページ) に、特殊な Telnet のエスケープ シーケンスの一覧を示します。

表 27 : 特殊な Telnet のエスケープ シーケンス

エスケープ シーケンス ¹	目的
Ctrl-^ c	プロセスの割り込み (IP)

エスケープシーケンス ⁷	目的
Ctrl-^ o	出力の中断 (AO)
Ctrl-^ u	行の消去 (EL)

⁷ キャレット (^) 記号はキーボードの Shift+6 で入力します。

アクティブな Telnet セッション中の任意の時点で、システムプロンプトでエスケープシーケンスキーを押してから疑問符を入力すると、Telnet コマンドを一覧表示できます。

ctrl-^?

次に、この一覧の例を示します。この出力例では、最初のキャレット (^) 記号は Control キーを表し、2 番目のキャレット記号はキーボードの Shift+6 を表しています。

```
RP/0/RP0/CPU0:router# ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

複数の並列 Telnet セッションを開き、セッション間を切り替えることができます。以降のセッションを開くには、最初に、エスケープシーケンスで (デフォルトでは Ctrl-Shift-6、x [Ctrl^x] の順に押す) 現在の接続を一時停止してシステムコマンドプロンプトに戻ります。その後、telnet コマンドで新しい接続を開きます。

アクティブな Telnet セッションを終了するには、接続しているデバイスのプロンプトから次のいずれかのコマンドを発行します。

- close
- disconnect
- exit
- logout
- quit

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み、実行

例

次の例は、リモートホスト host1 との Telnet セッションを確立する方法を示します。

```
RP/0/RP0/CPU0:router# telnet host1
```

telnet client source-interface

Telnet 接続の送信元 IP アドレスを指定するには、XR コンフィギュレーション モードで **telnet client source-interface** コマンドを使用します。コンフィギュレーション ファイルから **telnet client source-interface** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

telnet {ipv4|ipv6} client source-interface type interface-path-id

no telnet client source-interface type interface-path-id

構文の説明

ipv4	IPv4 アドレス プレフィックスを指定します。
ipv6	IPv6 アドレス プレフィックスを指定します。
<i>type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプ を参照してください。

コマンド デフォルト

送信元の IP アドレスとして、宛先までの最善ルートの IP アドレスが使用されます。

コマンド モード

XR 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
リリース 6.0	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 Telnet 接続の送信元としてインターフェイスの IP アドレスを設定するには、**telnet client source-interface** コマンドを使用します。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
ip-services	読み取り、書き込み

例

次の例は、Telnet 接続の送信元アドレスとして tenGigE インターフェイス 1/0/2/1 の IP アドレスを設定する方法を示しています。

```
RP/0/RP0/CPU0:router (config)# telnet ipv4 client source-interface tengige1/0/2/1
```

telnet dscp

Telnet トラフィックの QoS (Quality of Service) マーキングをネットワークデバイスに特別に設定するために、DiffServ コードポイント (DSCP) の値と IPv4 の優先度を定義するには、XR コンフィギュレーションモードで **telnet dscp** コマンドを使用します。DSCP 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。

telnet ipv4 dscp dscp-value

no telnet ipv4 dscp dscp-value

構文の説明

ipv4	IPv4 アドレス プレフィックスを指定します。
dscp-value	DSCP の値。範囲は 0 ~ 63 です。デフォルト値は 0 です

コマンド デフォルト

DSCP がディセーブルになっているか設定されていない場合、次のデフォルト値が示されます。

- サーバのデフォルト値は 16 です。
- クライアントのデフォルト値は 0 です。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv4 は、ローカルに発信される Telnet トラフィックのために DSCP 値を定義する場合にサポートされるプロトコルです。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
ip-services	読み取り、書き込み

例

次に、DSCP 値と IPv4 の優先度を定義する例を示します。

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 dscp 40  
RP/0/RP0/CPU0:router(config)# telnet ipv4 dscp 10
```

telnet server

ネットワークデバイスでの Telnet サービスをイネーブルにするには、XR コンフィギュレーションモードで **telnet server** コマンドを使用します。Telnet サービス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。

```
telnet [vrf {vrf-name| default}] {ipv4| ipv6} server max-servers {no-limit| limit} [access-list list-name]
no telnet [vrf {vrf-name| default}] {ipv4| ipv6} server max-servers {no-limit| limit} [access-list list-name]
```

構文の説明

vrf	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
vrf-name	(任意) ping を実行するためのシステムの VRF 名。
default	(任意) デフォルトの VRF インスタンスを指定します。
ipv4	IPv4 アドレス プレフィックスを指定します。
ipv6	IPv6 アドレス プレフィックスを指定します。
max-servers	許容可能な Telnet サーバの数を設定します。
no-limit	許容可能な Telnet サーバの最大数を設定しないように指定します。
limit	許容可能な Telnet サーバの最大数を指定します。範囲は 1 ~ 200 です。
access-list	(任意) アクセス リストを指定します。
list-name	(任意) アクセス リストの名前。

コマンド デフォルト

Telnet サービスはディセーブルです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

telnet コマンドによって着信 Telnet 接続がネットワーク デバイスに受け入れられるのを阻止するには、Telnet サービスをディセーブルにします。Telnet サービスがディセーブルにされると、その後は新規の着信接続が受け入れられなくなり、Cisco インターネット サービス デーモン (Cinetd) は Telnet ポートのリスニングを停止します。

Telnet サービスをイネーブルにするには、**max-servers** キーワードに 1 以上の値を設定します。このように設定すると、着信 Telnet 接続がネットワーク デバイスで許可されます。

このコマンドは、ネットワーク デバイスへの着信 Telnet 接続にだけ影響します。発信 Telnet 接続は、Telnet サービスがイネーブルであるかどうかにかかわらず確立できます。

このコマンドの **no** 形式を使用すると、Telnet 接続がディセーブルになり、システムはデフォルトの状態に戻ります。



(注)

Telnet セッションを介してルータとの接続を確立する前に、telnet サーバと vty-pool 機能を設定します (『Cisco ASR 9000 Series Aggregation Services RouterSystem Management Command Reference』、『Cisco ASR 9000 Series Aggregation Services RouterSystem Management Configuration Guide』、『Cisco ASR 9000 Series Aggregation Services RouterIP Addresses and Services Configuration Guide』を参照してください)。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
ip-services	読み取り、書き込み

例

次に、1 台のサーバに対する Telnet サービスをイネーブルにする例を示します。

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 1
```

telnet transparent

仮想ターミナルセッションの復帰 (CR) を、復帰-改行 (CR-LF) ではなく、CR-NULL として送信するには、行テンプレートサブモードで **telnet transparent** コマンドを使用します。コンフィギュレーションファイルから **telnet transparent** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

telnet transparent

no telnet transparent

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

ライン コンソール

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

telnet transparent コマンドは、Telnet プロトコルの仕様で行末処理の解釈が異なる場合の対処に役立ちます。

タスク ID

タスク ID	動作
tty-access	読み取り、書き込み

例

次の例で、Telnet トランスペアレントモードで vty 行を操作するための設定方法を示します。これにより、復帰キーを押すと、システムからの信号はCR-LFキーの組み合わせではなく、CR-NULLキーの組み合わせで送信されます。

```
RP/0/RP0/CPU0:router(config)# line console
RP/0/RP0/CPU0:router(config-line)# telnet transparent
```

tftp client source-interface

TFTP 接続の送信元 IP アドレスを指定するには、XR コンフィギュレーション モードで **tftp client source-interface** コマンドを指定します。コンフィギュレーション ファイルから **tftp client source-interface** コマンドを削除してシステムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

tftp client source-interface *type interface-path-id*

no tftp client source-interface *type interface-path-id*

構文の説明

<i>type</i>	インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

コマンド デフォルト

送信元の IP アドレスとして、宛先までの最善ルートの IP アドレスが使用されます。

コマンド モード

XR 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
リリース 6.0	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 TFTP 接続の送信元としてインターフェイスの IP アドレスを設定するには、**tftp client source-interface** コマンドを使用します。

タスク ID

タスク ID	動作
ip-services	読み取り、書き込み

例

次の例は、TFTP 接続の送信元アドレスとして tenGigE インターフェイス 1/0/2/1 の IP アドレスを設定する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# tftp client source-interface tengig1/0/2/1
```

tftp server

TFTPサーバまたはTFTPサーバで実行中の機能をイネーブルまたはディセーブルにするには、XR コンフィギュレーション モードで **tftp server** コマンドを使用します。システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

```
tftp {ipv4|ipv6} server homedir tftp-home-directory [max-servers [number|no-limit]] [access-list name]
no tftp {ipv4|ipv6} server homedir tftp-home-directory [max-servers [number|no-limit]] [access-list
name]
```

構文の説明

ipv4	IPv4 アドレス プレフィックスを指定します。
ipv6	IPv6 アドレス プレフィックスを指定します。
homedir <i>tftp-home-directory</i>	ホーム ディレクトリを指定します。
max-servers <i>number</i>	(任意) 並列 TFTP サーバの最大数を設定します。範囲は、1 ～ 2147483647 です。
max-servers no-limit	(任意) 処理が可能な TFTP サーバの数に上限がないことを設定します。
access-list <i>name</i>	(任意) TFTP サーバに関連付けるアクセスリストの名前を指定します。

コマンド デフォルト

デフォルトでは TFTP サーバはディセーブルになっています。指定しない場合は、**max-servers** キーワードのデフォルト値は無制限になります。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **tftp server** コマンドの **no** 形式を使用すると、指定したコマンドがコンフィギュレーションファイルから削除され、システムはデフォルトの状態に戻ります。コマンドの **no** 形式はコンフィギュレーションファイルに保存されません。

タスク ID	タスク ID	動作
	ipv4	読み取り、書き込み
	ip-services	読み取り、書き込み

例 次に、アクセスリスト名のテストを実行するために TFTP サーバをイネーブルにする例を示します。

```
RP/0/RP0/CPU0:router(config)# tftp ipv4 server homedir disk0 access-list test
```

tracertoute

IP ネットワークを介して宛先に到達するためにパケットが実際に使用するルートを検出するには、XR EXEC モードで **tracertoute** コマンドを使用します。

tracertoute [**ipv4**|**ipv6**] [*host-name*|*ip-address*] [**source** *ip-address-name*] [**numeric**] [**timeout** *seconds*] [**probe** *count*] [**minttl** *seconds*] [**maxttl** *seconds*] [**port** *number*] [**priority** *number*] [**verbose**]

構文の説明

ipv4	(任意) IPv4 アドレスのプレフィックスを指定します。
ipv6	(任意) IPv6 アドレスのプレフィックスを指定します。
host-name	(任意) トレース試行の宛先としてシステムで使用されるホスト名。
ip-address	(任意) トレース試行の宛先としてシステムで使用されるアドレス。
source	(任意) 送信元アドレスです。
ip-address-name	(任意) IP アドレス A.B.C.D またはホスト名。
numeric	(任意) 数字だけを表示。
timeoutseconds	(任意) タイムアウト値。範囲は 0 ~ 3600 です。
probecount	(任意) プロブ カウント。範囲は 0 ~ 65535 です。
minttlseconds	(任意) 最小存続可能時間。範囲は 0 ~ 255 です。
maxttlseconds	(任意) 最大存続可能時間。範囲は 0 ~ 255 です。
portnumber	(任意) ポート番号です。範囲は 0 ~ 65535 です。
prioritynumber	(任意) パケットのプライオリティ。範囲は 0 ~ 15 です。 ipv6 キーワードが指定されている場合に使用できます。
verbose	(任意) 詳細な出力。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

traceroute コマンドのデフォルト値は、宛先だけを参照します。宛先のアドレスで利用可能なデフォルト値はありません。

traceroute コマンドは、データグラムが存続可能時間 (TTL) の値を超過したときにネットワークング デバイスで生成されるエラー メッセージを利用して動作します。

traceroute コマンドは、最初に TTL 値が 1 のプローブ データグラムを送信します。すると、1 番目のネットワークング デバイスはそのプローブ データグラムを破棄し、エラー メッセージを送り返します。**traceroute** コマンドは TTL レベルごとに複数のプローブを送信し、それぞれのラウンドトリップ時間を表示します。

traceroute コマンドは一度に 1 つのプローブを送信します。各発信パケットから 1 つまたは 2 つのエラー メッセージが生成される可能性があります。「time-exceeded」というエラー メッセージは、中間ネットワークング デバイスで検出されたプローブが破棄されたことを意味します。

「destination unreachable」エラー メッセージは、宛先ノードがプローブを受信して、パケットを配信できないためにそれを破棄したことを示します。応答が着信する前にタイマーがオフになった場合、**traceroute** コマンドはアスタリスク (*) を出力します。

traceroute コマンドが終了するのは、宛先が応答したとき、最大 TTL を超過したとき、または、ユーザがエスケープ シーケンス (デフォルトでは Ctrl-C) を押してトレースを中断したときです (デフォルトのエスケープ シーケンスは、Ctrl キーと C キーを同時に押してから離します)。

デフォルト以外のパラメータを使用して拡張 **traceroute** テストを呼び出すには、*host-name* や *ip-address* 引数を指定せずにコマンドを入力します。ダイアログの手順に従って **traceroute** テストに必要なパラメータ値を選択します。

多様なネットワークング デバイスに応じて IP の実装方法も異なっているので、IP **traceroute** コマンドが予期しない動作をする場合があります。

宛先によっては、メッセージ「ICMP port unreachable」を送り返してプローブメッセージに正しく応答できない場合があります。最大 TTL を超過した場合に限り終了する、アスタリスクだけが付加された TTL レベルの長いシーケンスがこの問題の原因となっている可能性があります。

一部のホストが「ICMP TTL exceeded」というメッセージを処理する方法について、既知の問題があります。一部のホストでは「ICMP」メッセージを生成しますが、着信パケットの TTL を再利用します。この値はゼロのため、ICMP パケットの返信は失敗します。このようなホストへのパスをトレースすると、アスタリスク (*) の付いた TTL 値のセットが表示される場合があります。最終的には、この TTL は「ICMP」メッセージを返信できるまでの値に増加します。たとえば、ホストが 6 ホップ離れた位置にある場合、**traceroute** コマンドは、6 ~ 11 回の応答でタイムアウトします。

タスク ID

タスク ID	動作
basic-services	読み取り、書き込み、実行

例

次の例は、宛先のホスト名が指定されている場合の **traceroute** セッションの出力を示しています。

```
RP/0/RP0/CPU0:router# traceroute host8-sun

Type escape sequence to abort.
Tracing the route to 192.168.0.73
 1 192.168.1.6 (192.168.1.6) 10 msec 0 msec 10 msec
 2 gateway01-gw.gateway.cisco.com (192.168.16.2) 0 msec 10 msec 0 msec
 3 host8-sun.cisco.com (192.168.0.73) 10 msec * 0 msec
```

次の例は、宛先が指定されていない場合の拡張 **traceroute** セッションの出力を示しています。

```
traceroute# traceroute

Protocol [ipv4]:
Target IP address: ena-view3
Source address: 10.0.58.29
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.
Tracing the route to 171.71.164.199
 1 sjc-jpxlnock-vpn.cisco.com (10.25.0.1) 30 msec 4 msec 4 msec
 2 15lab-vlan725-gx1.cisco.com (173.19.72.2) 7 msec 5 msec 5 msec
 3 stc15-00lab-gw1.cisco.com (173.24.114.33) 5 msec 6 msec 6 msec
 4 stc5-lab4-gw1.cisco.com (173.24.114.89) 5 msec 5 msec 5 msec
 5 stc5-sbb4-gw1.cisco.com (172.71.241.162) 5 msec 6 msec 6 msec
 6 stc5-dc5-gw1.cisco.com (172.71.241.10) 6 msec 6 msec 5 msec
 7 stc5-dc1-gw1.cisco.com (172.71.243.2) 7 msec 8 msec 8 msec
 8 ena-view3.cisco.com (172.71.164.199) 6 msec * 8 msec
```

次の表に、**traceroute** の出力に表示される文字について説明します。

表 28: **traceroute** テキスト文字

文字	説明
xx msec	指定された数のプローブに対する各ノードのラウンドトリップ時間（ミリ秒）。
*	プローブのタイムアウト。
?	パケットタイプが不明です。

文字	説明
A	管理上、到達不能です。通常、この出力はアクセスリストがトラフィックをブロックしていることを示します。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。



LPTS コマンド

この章では、NCS 5000 ルータで Local Packet Transport Services (LPTS) をモニタする際に使用する Cisco IOS XR ソフトウェアのコマンドについて説明します。

LPTS の概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [clear lpts ifib statistics, 232 ページ](#)
- [clear lpts pifib statistics, 233 ページ](#)
- [show lpts bindings, 234 ページ](#)
- [show lpts clients, 239 ページ](#)
- [show lpts flows, 241 ページ](#)
- [show lpts ifib, 245 ページ](#)
- [show lpts ifib slices, 249 ページ](#)
- [show lpts ifib statistics, 252 ページ](#)
- [show lpts ifib times, 254 ページ](#)
- [show lpts pifib, 256 ページ](#)
- [show lpts pifib hardware police, 261 ページ](#)
- [show lpts pifib hardware usage, 264 ページ](#)
- [show lpts pifib statistics, 266 ページ](#)
- [show lpts port-arbitrator statistics, 268 ページ](#)

clear lpts ifib statistics

Internal Forwarding Information Base (IFIB) 統計情報をクリアするには、で **clear lpts ifib statistics** コマンドを使用します。

clear lpts ifib statistics [*location node-id*]

構文の説明

location*node-id* 指定されたノードの IFIB 統計情報をクリアします。*node-id* 引数は、標準の *rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	実行

例

次に、RP の IFIB 統計情報をクリアする例を示します。

```
RP/0/# clear lpts ifib statistics
```

clear lpts pifib statistics

Pre-Internal Forwarding Information Base (Pre-IFIB) 統計情報をクリアするには、で **clear lpts pifib statistics** コマンドを使用します。

clear lpts pifib statistics [**location** *node-id*]

構文の説明

location <i>node-id</i>	指定したノードの Pre-IFIB 統計情報をクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
--------------------------------	---

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	実行

例

次の例は、RP の Pre-IFIB 統計情報をクリアする方法を示します。

```
RP/0/# clear lpts pifib statistics location 0/RP0/CPU0
```

show lpts bindings

Port Arbitrator でのバインディング情報を表示するには、で **show lpts bindings** コマンドを使用します。

```
show lpts bindings [location node-id] [client-id {clnl| ipsec| ipv4-io| ipv6-io| mpa| tcp| test| udp| raw}]
[brief] [vrf vrf-name]
```

構文の説明

location <i>node-id</i>	(任意) 指定したノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
client-id	(任意) クライアントの種類。次のいずれかの値を指定できます。 <ul style="list-style-type: none"> • clnl : ISO コネクションレス プロトコル (IS-IS で使用) • ipsec : セキュア IP • ipv4-io : IPv4 スタックによって処理されるトラフィック • ipv6-io : IPv6 スタックによって処理されるトラフィック • mpa : Multicast Port Arbitrator (マルチキャストグループ加入) • tcp : トランスミッションコントロールプロトコル • test : テストアプリケーション • udp : ユーザデータグラムプロトコル • raw : Raw IP
brief	(任意) 要約出力を表示します。
vrf <i>vrf-name</i>	(任意) 割り当てられている VRF の名前。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 lpts bindings コマンドは、Local Packet Transport Services (LPTS) バインディング (特定のタイプのトラフィックを受信するための要求) を表示します。バインディングは、LPTS Port Arbitrator によってフローに集約されます。パケットをアプリケーションに渡すため、フローは Internal Forwarding Information Base (IFIB) および Pre-IFIB にプログラムされます。

オプションの **client-id** キーワードとクライアントのタイプを指定した場合は、そのクライアントからのバインディングだけが表示されます。オプションの **location** キーワードと **node-id** 引数を指定した場合は、そのノード上のクライアントからのバインディングだけが表示されます。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の **show lpts bindings** コマンドの出力例は、すべてのクライアント ID タイプのバインディングを表示します。

```
RP/0/# show lpts bindings

@ - Indirect binding; Sc - Scope

-----
Location      :0/1/CPU0
Client ID     :IPV4_IO
Cookie        :0x00000001
Clnt Flags   :
Layer 3       :IPV4
Layer 4       :ICMP
Local Addr    :any
Remote Addr   :any
Local Port    :any
Remote Port   :any
Filters       :Type / Intf or Pkt Type / Source Addr / Location
               INCLUDE_TYPE / type 8
               INCLUDE_TYPE / type 13
               INCLUDE_TYPE / type 17
-----

Location      :0/2/CPU0
Client ID     :IPV4_IO
Cookie        :0x00000001
Clnt Flags   :
Layer 3       :IPV4
Layer 4       :ICMP
Local Addr    :any
Remote Addr   :any
Local Port    :any
Remote Port   :any
Filters       :Type / Intf or Pkt Type / Source Addr / Location
               INCLUDE_TYPE / type 8
               INCLUDE_TYPE / type 13
               INCLUDE_TYPE / type 17
-----

Location      :0/RP1/CPU0
Client ID     :TCP
```

show lpts bindings

```

Cookie      :0x4826f1f8
Clnt Flags :REUSEPORT
Layer 3     :IPV4
Layer 4     :TCP
Local Addr  :any
Remote Addr:any
Local Port  :7
Remote Port:any
-----
Location    :0/RP1/CPU0
Client ID   :TCP
Cookie      :0x4826fa0c
Clnt Flags :REUSEPORT
Layer 3     :IPV4
Layer 4     :TCP
Local Addr  :any
Remote Addr:any
Local Port  :9
Remote Port:any
-----
Location    :0/RP1/CPU0
Client ID   :TCP
Cookie      :0x482700d0
Clnt Flags :REUSEPORT
Layer 3     :IPV4
Layer 4     :TCP
Local Addr  :any
Remote Addr:any
Local Port  :19
Remote Port:any
-----
Location    :0/RP1/CPU0
Client ID   :IPV4_IO
Cookie      :0x00000001
Clnt Flags :
Layer 3     :IPV4
Layer 4     :ICMP
Local Addr  :any
Remote Addr:any
Local Port  :any
Remote Port:any
Filters     :Type / Intf or Pkt Type / Source Addr / Location
INCLUDE_TYPE / type 8
INCLUDE_TYPE / type 13
INCLUDE_TYPE / type 17

```

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 29 : show lpts bindings コマンドのフィールドの説明

フィールド	説明
Location	rack/slot/module 形式のノードの場所
Client ID	LPTS クライアント タイプ
Cookie	バインディングに対するクライアントの一意のタグ。
Clnt Flags	REUSEPORT : クライアントがソケット オプション SO_REUSEPORT または SO_REUSEADDR を設定
Layer 3	レイヤ 3 プロトコル (IPv4、IPv6、CLNL)

フィールド	説明
Layer 4	レイヤ 4 プロトコル (TCP、UDP)
Local Addr	ローカル (宛先) アドレス
Remote Addr	リモート (送信元) アドレス
Local Port	ローカル (宛先) TCP または UDP ポート、または ICMP/IGMP パケットタイプ、または IPsec Security Parameter Index (SPI)
Remote Port	リモート (送信元) TCP または UDP ポート

次の例は、**show lpts bindings brief** コマンドの出力を示しています。

```
RP/0/# show lpts bindings brief
@ - Indirect binding; Sc - Scope
```

```

Location  Clnt Sc L3  L4  VRF-ID  Local,Remote Address.Port  Interface
-----
0/1/CPU0  IPV4 LO IPV4 ICMP *      any.ECHO any                    any
0/1/CPU0  IPV4 LO IPV4 ICMP *      any.TSTAMP any                   any
0/1/CPU0  IPV4 LO IPV4 ICMP *      any.MASKREQ any                   any
0/1/CPU0  IPV6 LO IPV6 ICMP6 *     any.ECHOREQ any                   any
0/3/CPU0  IPV4 LO IPV4 ICMP *      any.ECHO any                    any
0/3/CPU0  IPV4 LO IPV4 ICMP *      any.TSTAMP any                   any

```

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 30: **show lpts bindings brief** コマンドのフィールドの説明

フィールド	説明
Location	<i>rack/slot/module</i> 形式のノードの場所
Clnt ID	LPTS クライアントタイプ
Sc	スコープ (LR = 論理ルータ、LO = ローカル)
Layer 3	レイヤ 3 プロトコル
Layer 4	レイヤ 4 プロトコル
VRF-ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Local,Remote Address.Port	ローカル (宛先) およびリモート (送信元) アドレスとポートまたはパケットタイプ

フィールド	説明
Interface	インバウンド インターフェイス

show lpts clients

Port Arbitrator でのクライアント情報を表示するには、で **show lpts clients** コマンドを使用します。

show lpts clients [times]

構文の説明

times (任意) バインディング要求レートとサービス時間に関する情報を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 lpts clients コマンドは、Local Packet Transport Services (LPTS) Port Arbitrator (PA) に接続されているクライアントを表示します。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts clients** コマンドの出力を示しています。

```
RP/0/# show lpts clients
o_flg - open flags ; clid - client id
clid      loc      flags  o_flg
RAW (3)   0/RP1/CPU0  0x1   0x2
TCP (1)   0/RP1/CPU0  0x1   0x2
IPV4_IO (5) 0/1/CPU0    0x3   0x2
IPV4_IO (5) 0/2/CPU0    0x3   0x2
```

```
IPV4_IO(5)      0/RP1/CPU0      0x3      0x2
MFA(7)          0/RP1/CPU0      0x3      0x0
```

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 31 : **show lpts clients** コマンドのフィールドの説明

フィールド	説明
Clid	LPTS クライアント ID。
Loc	<i>rack/slot/module</i> 形式のノードの場所
Flags	クライアントフラグ。 (注) クライアントフラグは、デバッグ目的でだけ使用されます。
o_flags	オープンフラグ。 (注) オープンフラグは、デバッグ目的でだけ使用されます。

次の例は、**show lpts clients times** コマンドの出力を示しています。出力には、最後の 30 秒間、1 分間、5 分間、10 分間、合計のサンプルが表示されます（ゼロでない場合）。トランザクション数、更新回数、各トランザクションの処理に要した最小/平均/最大時間（ミリ秒単位）が表示されます。

```
RP/0/# show lpts clients times

o_flg - open flags ; clid - client id
clid   loc      flags  o_flg
RAW(3) 0/RP1/CPU0 0x1   0x2
 30s:2 tx 2 upd 2/2/3ms/tx
  1m:2 tx 2 upd 2/2/3ms/tx
  5m:2 tx 2 upd 2/2/3ms/tx
 10m:2 tx 2 upd 2/2/3ms/tx
total:2 tx 2 upd 2/-/3ms/tx
TCP(1) 0/RP1/CPU0 0x1   0x2
total:3 tx 3 upd 1/-/1ms/tx
IPV4_IO(5) 0/1/CPU0 0x3   0x2
total:1 tx 1 upd 0/-/0ms/tx
IPV4_IO(5) 0/2/CPU0 0x3   0x2
total:1 tx 1 upd 1/-/1ms/tx
IPV4_IO(5) 0/RP1/CPU0 0x3   0x2
total:1 tx 1 upd 3/-/3ms/tx
MFA(7) 0/RP1/CPU0 0x3   0x0
```

show lpts flows

Local Packet Transport Services (LPTS) フローに関する情報を表示するには、で **show lpts flows** コマンドを使用します。

show lpts flows [brief]

構文の説明

brief (任意) 要約出力を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 lpts flows コマンドは、LPTS フローを表示するために使用します。これは、複数のクライアントからの同じバインディング要求を集約したものであり、LPTS Internal Forwarding Information Base (IFIB) と Pre-IFIB をプログラムするために使用されます。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts flows** コマンドの出力を示しています。

```
RP/0/# show lpts flows
-----
L3-proto      : IPV4 (2)
L4-proto      : ICMP (1)
VRF-ID        : * (000000000)
Local-IP      : any
Remote-IP     : any
```

show lpts flows

```

Pkt-Type      : 8
Remote-Port   : any
Interface     : any (0x0)
Flow-type     : ICMP-local
Min-TTL       : 0
Slice         : RAWIP4_FM
Flags         : 0x20 (in Pre-IFIB)
Location      : (drop)
Element References
location / count / scope
* / 3 / LOCAL

```

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 32 : show lpts flows コマンドのフィールドの説明

フィールド	説明
L3-proto	レイヤ 3 プロトコル (IPv4、IPv6、CLNL)
L4-proto	レイヤ 4 プロトコル (TCP、UDP など)
VRF-ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Local-IP	ローカル (宛先) IP アドレス
Remote-IP	リモート (送信元) IP アドレス
Pkt-Type	ICMP または IGMP パケット タイプ
Remote-Port	リモート (送信元) TCP または UDP ポート
Interface	入力インターフェイス
Flow-type	ハードウェア パケット ポリシングのためのフロー分類
Min-TTL	受信パケットで期待される最小 Time-to-Live 値 これよりも小さい TTL 値を持つ受信パケットはすべてドロップされます。
Slice	IFIB スライス

フィールド	説明
Flags	<ul style="list-style-type: none"> • Has FGID : 複数の宛先に配信 • No IFIB entry : IFIB エントリを抑制 • Retrying FGID allocation • In Pre-IFIB : エントリは Pre-IFIB にも存在 • Deliver to one : 複数バインディングの場合、1 つだけに配信
Location	配信先の <i>rack/slot/module</i>
Element References	<ul style="list-style-type: none"> • location : クライアントの <i>rack/slot/module</i>。 • count : その場所にあるクライアントの数。 • scope : バインディングスコープ (LR : 論理ルータ、LOCAL : ローカル)。

次の例は、**show lpts flows brief** コマンドの出力を示しています。

```
RP/0/# show lpts flows brief
```

```
+ - Additional delivery destination; L - Local interest; P - In Pre-IFIB
```

```

L3   L4   VRF-ID   Local, Remote Address.Port   Interface   Location   LP
-----
IPV4 ICMP *       any.ECHO any                       any        (drop)    LP
IPV4 ICMP *       any.TSTAMP any                       any        (drop)    LP
IPV4 ICMP *       any.MASKREQ any                       any        (drop)    LP
IPV6 ICMP6 *      any.ECHOREQ any                       any        (drop)    LP
IPV4 any  default 224.0.0.2 any                       Gi0/1/0/1  0/5/CPU0  P

```

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 33 : **show lpts flows brief** コマンドのフィールドの説明

フィールド	説明
L3	レイヤ 3 プロトコル (IPv4、IPv6、CLNL)
L4	レイヤ 4 プロトコル
VRF-ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。

フィールド	説明
Local, Remote Address.Port	ローカル (宛先) およびリモート (送信元) IP アドレスおよび TCP または UDP ポート、または ICMP/IGMP パケット タイプ、または IPSec SPI
Interface	入力インターフェイス
Location	配信場所 <ul style="list-style-type: none"> • <i>rack/slot/module</i> : 個別の場所 • <i>[0xNNNNN]</i> : 複数の場所 (プラットフォーム依存の値) • <i>(drop)</i> : どのアプリケーションにも配信しない
LP	ローカル関係 (IPv4 または IPv6 スタックで直接処理される) またはエントリが Pre-IFIB に常駐

show lpts ifib

Internal Forwarding Information Base (IFIB) 内のエントリーを表示するには、で **show lpts ifib** コマンドを使用します。

```
show lpts ifib [entry] [type {bgp4| bgp6| isis| mcast4| mcast6| ospf-mc4| ospf-mc6| ospf4| ospf6| raw4| raw6| tcp4| tcp6| udp4| udp6}| all] [brief [statistics]] [slices] [times] [location node-id]
```

構文の説明

entry	(任意) IFIB エントリーを表示します。
type	(任意) 次のプロトコル タイプを表示します。 <ul style="list-style-type: none"> • bgp4 : IPv4 ボーダー ゲートウェイ プロトコル (BGP) スライス • bgp6 : IPv6 BGP スライス • isis : Intermediate System-to-Intermediate System (IS-IS) スライス • mcast4 : IPv4 マルチキャスト スライス • mcast6 : IPv6 マルチキャスト スライス • ospf-mc4 : IPv4 オープン ショーテストパス ファースト (OSPF) マルチキャスト スライス • ospf-mc6 : IPv6 OSPF マルチキャスト スライス • ospf4 : IPv4 OSPF スライス • ospf6 : IPv6 OSPF スライス • raw4 : IPv4 raw IP • raw6 : IPv6 raw IP • tcp4 : IPv4 伝送制御プロトコル (TCP) スライス • tcp6 : IPv6 TCP スライス • udp4 : IPv4 UDP スライス • udp6 : IPv6 UDP スライス
all	すべての IFIB タイプを表示します。
brief	(任意) IFIB エントリーを簡潔な形式で表示します。
statistics	(任意) IFIB テーブルと統計情報を表示します。
slices	(任意) IFIB スライスを表示します。

times	(任意) IFIB 更新トランザクション時間を表示します。
locationnode-id	(任意) フローマネージャの場所を指定します。node-id 引数は、rack/slot/module の形式で入力します。

コマンド デフォルト デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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、IFIB スライス内のエントリーに関する詳細情報を表示するために使用します。このコマンドは、アプリケーションへのパケットの配信に関する問題をデバッグする場合に有効です。

statistics キーワードを使用すると、パケット数、各スライス内のエントリー数、合計エントリー数の詳細な統計情報が表示されます。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts ifib** コマンドの出力を示しています。

```
RP/0/# show lpts ifib
O - Opcode; A - Accept Counter; D - Drop Counter; F - Flow Type; L - Listener Tag;
I - Local Flag; Y - SYN; T - Min TTL; DV - Deliver; DP - Drop; RE - Reassemble; na - Not
Applicable
-----
VRF-ID           : default (0x60000000)
Port/Type        : any
Source Port      : any
Dest IP          : any
Source IP        : any
Layer 4          : 88 (88)
Interface        : any (0x0)
O/A/D/F/L/I/Y/T : DELIVER/0/0/EIGRP/IPv4_STACK/0/0/0
```

```
Deliver List      : 0/5/CPU0
```

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 34 : `show lpts ifib entries` コマンドのフィールドの説明

フィールド	説明
VRF-ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Port/Type	宛先 (ローカル) TCP または UDP ポート番号、または ICMP/IGMP パケットタイプ、または IPsec SPI t2222
Source Port	ソース (リモート) TCP または UDP ポート
Dest IP	宛先 (ローカル) IP アドレス
Source IP	ソース (リモート) IP アドレス
Layer 4	レイヤ 4 プロトコル番号 (6 = TCP) (注) 一般的なレイヤ 4 プロトコル名だけが表示されます。
Interface	入力インターフェイス名
O/S/P/R/L/I/Y	<ul style="list-style-type: none"> • O : Opcode (DELIVER、DROP、REASSEMBLE のいずれか) • S : 統計カウンタ • P : パケットフォワーディングプライオリティ (LO、MED、HIGH のいずれか) • R : レート制限 (LO、MED、HIGH のいずれか) • L : リスナー タグ (IPv4_STACK、IPv6_STACK、CLNL_STACK のいずれか) • I : ローカル関係フラグ (0 または 1) • Y : TCP SYN フラグ (0 または 1)

フィールド	説明
Deliver List	<ul style="list-style-type: none"> • (drop) : パケットをドロップ • rack/slot/module : 単一の宛先に配信 • [0xNNNN] : 複数の宛先に配信 (プラットフォーム依存の形式)

次の例は、**show lpts ifib brief** コマンドの出力を示しています。

```
RP/0/# show lpts ifib brief
```

```

Slice      Local, Remote Address.Port      L4      Interface      Dlv
-----
TCP4       any.7 any                        TCP     any            0/RP1/CPU0
TCP4       any.9 any                        TCP     any            0/RP1/CPU0

```

次の例は、**show lpts ifib brief statistics** コマンドの出力を示しています。

```
RP/0/# show lpts ifib brief statistics
```

```

Slice      Local, Remote Address.Port      L4      Interface      Accept/Drop
-----
TCP4       any.7 any                        TCP     any            0/0
TCP4       any.9 any                        TCP     any            0/0
TCP4       any.19 any                       TCP     any            0/0

Slice      Num. Entries Accepts/Drops
-----
TCP4       3              0/0
Total     3              0/0

```

show lpts ifib slices

Internal Forwarding Information Base (IFIB) スライス情報を表示するには、`show lpts ifib slices` コマンドを使用します。

```
show lpts ifib slices [type {bgp4|bgp6|isis|mc4|mc6|ospf-mc4|ospf-mc6|ospf4|ospf6|raw4|raw6|tcp4|tcp6|udp4|udp6}] [all] [statistics] [times]
```

構文の説明

type	(任意) プロトコル タイプを入力します。 <ul style="list-style-type: none"> • bgp4 : IPv4 ボーダー ゲートウェイ プロトコル (BGP) スライス • bgp6 : IPv6 BGP スライス • isis : Intermediate System-to-Intermediate System (IS-IS) スライス • mc4 : IPv4 マルチキャスト スライス • mc6 : IPv6 マルチキャスト スライス • ospf-mc4 : IPv4 オープン ショーテスト パス ファースト (OSPF) マルチキャスト スライス • ospf-mc6 : IPv6 OSPF マルチキャスト スライス • ospf4 : IPv4 OSPF スライス • ospf6 : IPv6 OSPF スライス • raw4 : IPv4 raw IP • raw6 : IPv6 raw IP • tcp4 : IPv4 伝送制御プロトコル (TCP) スライス • tcp6 : IPv6 TCP スライス • udp4 : IPv4 UDP スライス • udp6 : IPv6 UDP スライス
all	(任意) すべてのエントリを表示します。
statistics	(任意) スライス ルックアップの統計情報を表示します。
times	(任意) IFIB 更新トランザクション時間を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンドモード

コマンド履歴

リリース	変更内容
リリース 6.0	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 lpts ifib slices** コマンドは、IFIB エントリとスライス割り当てをトラブルシューティングする場合に使用します。このコマンドは、アプリケーションへのパケットの配信に関する問題をトラブルシューティングする場合に特に便利です。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts ifib slices** コマンドの出力を示しています。

```
RP/0/# show lpts ifib slices

Slice      L3    L4      Port  Location
-----
RAWIP4     IPV4  any     any    0/RP0/CPU0
RAWIP6     IPV6  any     any    0/RP0/CPU0
OSPF4      IPV4  OSPF    any    0/RP0/CPU0
OSPF6      IPV6  OSPF    any    0/RP0/CPU0
OSPF_MC4   IPV4  any     any    0/RP0/CPU0
OSPF_MC6   IPV6  any     any    0/RP0/CPU0
BGP4       IPV4  TCP     179    0/RP0/CPU0
BGP6       IPV6  TCP     179    0/RP0/CPU0

UDP4       IPV4  UDP     any    0/RP0/CPU0
UDP6       IPV6  UDP     any    0/RP0/CPU0
TCP4       IPV4  TCP     any    0/RP0/CPU0
TCP6       IPV6  TCP     any    0/RP0/CPU0
ISIS       CLNS  -       any    0/RP0/CPU0
MCAST4     IPV4  any     any    0/RP0/CPU0
MCAST6     IPV6  any     any    0/RP0/CPU0
```

次の例は、**show lpts ifib slices times** コマンドの出力を示しています。

```
RP/0/# show lpts ifib slices times

Slice      L3    L4      Port  Location
-----
RAWIP4     IPV4  any     any    0/RP0/CPU0
RAWIP6     IPV6  any     any    0/RP0/CPU0
OSPF4      IPV4  OSPF    any    0/RP0/CPU0
OSPF6      IPV6  OSPF    any    0/RP0/CPU0
```

```

OSPF_MC4 IPV4 any any 0/RP0/CPU0
OSPF_MC6 IPV6 any any 0/RP0/CPU0
BGP4 IPV4 TCP 179 0/RP0/CPU0
BGP6 IPV6 TCP 179 0/RP0/CPU0

UDP4 IPV4 UDP any 0/RP0/CPU0
UDP6 IPV6 UDP any 0/RP0/CPU0
TCP4 IPV4 TCP any 0/RP0/CPU0
TCP6 IPV6 TCP any 0/RP0/CPU0
ISIS CLNS - any 0/RP0/CPU0
MCAST4 IPV4 any any 0/RP0/CPU0
MCAST6 IPV6 any any 0/RP0/CPU0
Flow Manager 0/RP0/CPU0:
total:5 tx 13 upd 1/-/1ms/tx

```

次の例は、**show lpts ifib slices statistics** コマンドの出力を示しています。

```
RP/0/# show lpts ifib slices all statistics
```

Slice	L3	L4	Port	Location	Lookups	RmtDlvr	Rejects	RLDrops	NoEntry
RAWIP4	IPV4	any	any	0/0/CPU0	5	0	0	0	0
RAWIP6	IPV6	any	any	0/0/CPU0	0	0	0	0	0
OSPF4	IPV4	OSPF	any	0/0/CPU0	0	0	0	0	0
OSPF6	IPV6	OSPF	any	0/0/CPU0	0	0	0	0	0
OSPF_MC4	IPV4	any	any	0/0/CPU0	0	0	0	0	0
OSPF_MC6	IPV6	any	any	0/0/CPU0	0	0	0	0	0
BGP4	IPV4	TCP	179	0/0/CPU0	0	0	0	0	0
BGP6	IPV6	TCP	179	0/0/CPU0	0	0	0	0	0
UDP4	IPV4	UDP	any	0/0/CPU0	3704	0	979	0	0
UDP6	IPV6	UDP	any	0/0/CPU0	0	0	0	0	0
TCP4	IPV4	TCP	any	0/0/CPU0	0	0	0	0	0
TCP6	IPV6	TCP	any	0/0/CPU0	0	0	0	0	0
ISIS	CLNS	-	any	0/0/CPU0	0	0	0	0	0
MCAST4	IPV4	any	any	0/0/CPU0	0	0	0	0	0
MCAST6	IPV6	any	any	0/0/CPU0	0	0	0	0	0

```

Flow Manager 0/0/CPU0:
Packets in: 3792
Packets delivered locally without lookups: 83
Slice lookups: 3709
Rejects: 979

```

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 35 : **show lpts ifib slices statistics** コマンドのフィールドの説明

フィールド	説明
Slice	スライス番号
L3-proto	レイヤ 3 プロトコル (IPv4、IPv6、CLNL)
L4-proto	レイヤ 4 プロトコル (TCP、UDP など)
Port	ローカル (宛先) TCP または UDP ポート
Location	rack/slot/module 形式のノードの場所

show lpts ifib statistics

Internal Forwarding Information Base (IFIB) 統計情報を表示するには、で **show lpts ifib statistics** コマンドを使用します。

show lpts ifib statistics [location node-id]

構文の説明

location*node-id* (任意) 指定したノードの IFIB 統計情報を表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts ifib statistics** コマンドの出力を示しています。

```
RP/0/# show lpts ifib statistics

Flow Manager 0/RP0/CPU0:
  Packets in:254
  Packets delivered locally without lookups:0
  Slice lookups:254
    Post-lookup error drops:
      Failed ipv4_netio_input:1
  Rejects:254
```

```
Packets delivered locally:0
Packets delivered remotely:0
```

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 36 : *show lpts ifib statistics* コマンドのフィールドの説明

フィールド	説明
Packets in	netio で LPTS decaps ノードに渡されたパケット
Packets delivered locally without lookups	LC 上で以前解決され直接 L3 に配信されたパケット
Slice lookups	スライス ルックアップが必要なパケット
Post-lookup error drops	スライス ルックアップ後にドロップされたパケット
Rejects	TCP RST または ICMP ポート/プロトコル Unreachable となったパケット
Packets delivered locally	スライスルックアップ後にローカルアプリケーションに配信されたパケット
Packets delivered remotely	リモート RP 上のアプリケーションに配信されたパケット



(注) この出力例はあくまで例であり、値があるフィールドだけが表示されています。ゼロ以外の値に対しては表示が存在しません。ルータの設定によっては、これ以外の値が表示される場合があります。

show lpts ifib times

Internal Forwarding Information Base (IFIB) 更新トランザクション時間を表示するには、XR EXEC モードで **show lpts ifib times** コマンドを使用します。

show lpts ifib times [location node-id]

構文の説明

location*node-id* (任意) 指定したノードの IFIB 更新トランザクション時間を表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンドモード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts ifib times** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show lpts ifib times
```

Slice	L3	L4	Port	Location
RAWIP4	IPV4	any	any	0/RP1/CPU0
RAWIP6	IPV6	any	any	0/RP1/CPU0
OSPF4	IPV4	OSPF	any	0/RP1/CPU0
OSPF6	IPV6	OSPF	any	0/RP1/CPU0
OSPF_MC4	IPV4	any	any	0/RP1/CPU0
OSPF_MC6	IPV6	any	any	0/RP1/CPU0
BGP4	IPV4	TCP	179	0/RP1/CPU0
BGP6	IPV6	TCP	179	0/RP1/CPU0
UDP4	IPV4	UDP	any	0/RP1/CPU0
UDP6	IPV6	UDP	any	0/RP1/CPU0

```

TCP4    IPV4 TCP    any    0/RP1/CPU0
TCP6    IPV6 TCP    any    0/RP1/CPU0
ISIS    CLNS  -        any    0/RP1/CPU0
MCAST4  IPV4 any     any    0/RP1/CPU0
MCAST6  IPV6 any     any    0/RP1/CPU0
Flow Manager 0/RP0/CPU0:
  total:5 tx 13 upd 1/-/1ms/tx

```

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 37 : *show lpts ifib times* コマンドのフィールドの説明

フィールド	説明
Slice	スライス番号
L3 Protocol	レイヤ 3 プロトコル (IPv4、IPV6、CLNL)
L4 Protocol	レイヤ 4 プロトコル (TCP、UDP など)
Port	ローカル (宛先) TCP または UDP ポート
Location	<i>rack/slot/module</i> 形式のノードの場所

show lpts pifib

Pre-Internal Forwarding Information Base (Pre-IFIB) エントリを表示するには、で **show lpts pifib** コマンドを使用します。

show lpts pifib[entry] [hardware {entry | police}] [type {isis | ipv4 | ipv6} {any}] [brief] [statistics] [location *node-id*]

構文の説明

entry	(任意) Pre-IFIB エントリ。
hardware	(任意) Pre-IFIB のハードウェアを表示します。
entry	(任意) Pre-IFIB のエントリを表示します。
police	(任意) 使用されているポリサー値を表示します。
type	(任意) プロトコルタイプ。
isis	(任意) Intermediate System-to-Intermediate System (IS-IS) サブ Pre-IFIB タイプ。
ipv4	(任意) IPv4 サブ Pre-IFIB タイプ。可能な値は次のとおりです。 frag 、 ixmp 、 mcast 、 tcp 、 udp 、 ipsec 、 raw 。
ipv6	(任意) IPv6 サブ Pre-IFIB タイプ。可能な値は次のとおりです。 frag 、 icmp 、 ixmp 、 mcast 、 tcp 、 udp 、 ipsec 、 raw 。
any	IPv4 または IPv6 プロトコル。
brief	(任意) 簡潔な形式の Pre-IFIB エントリ。
statistics	(任意) Pre-IFIB テーブルと統計情報。
location <i>node-id</i>	(任意) <i>node-id</i> 引数は、 <i>rack/slot/module</i> 表記で入力します (例 : 0/7/CPU0) 。

コマンド デフォルト

デフォルトでは、すべてのエントリが表示されます。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

次の機能を実行するには、**show lpts pifib** コマンドを **brief** キーワードとともに使用します。

- Pre-IFIB のすべてまたは一部のエントリを表示する。
- LPTS Pre-IFIB 内の各エントリの簡単な説明を表示し、必要に応じて各エントリのパケットカウントを表示する。



(注) これらの統計情報は、ラインカード、ルートプロセッサ、分散ルートプロセッサで処理されるパケットだけに使用されます。

ラインカードハードウェアで処理されるパケットの Pre-IFIB 統計情報は個別にカウントされます。

デフォルトでは、すべてのデフォルトが表示されます。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts pifib** コマンドの出力を示しています。

```
RP/0/# show lpts pifib

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
-----
L3 Protocol      : CLNS
L4 Protocol      : -
VRF-ID           : default (0x60000000)
Destination IP   : any
Source IP        : any
Port/Type        : any
Source Port      : any
Is Fragment      : 0
Is SYN           : 0
Interface        : any (0x0)
O/F/L/I/T       : DELIVER/ISIS-default/CLNS_STACK/0/0
Deliver List     : FGID 11935
Accepts/Drops    : 0/0
Is Stale         : 0
```

次の例は、**ipv4** と **tcp** キーワードを指定した場合の **show lpts pifib type** コマンドの出力を示しています。

```
RP/0/# show lpts pifib type ipv4 tcp

O - Opcode; F - Flow Type; L - Listener Tag; I - Local Flag; T - Min TTL;
na - Not Applicable
-----
L3 Protocol      : IPV4
L4 Protocol      : TCP
VRF-ID          : default (0x60000000)
Destination IP   : any
Source IP        : any
Port/Type        : Port:23
Source Port      : any
Is Fragment      : 0
Is SYN           : 0
Interface        : any (0x0)
O/F/L/I/T       : DELIVER/TELNET-default/IPv4_LISTENER/0/0
Deliver List     : 0/RP0

/CPU0
Accepts/Drops    : 0/0
Is Stale         : 0
-----
```

次の例は、**entry** と **brief** キーワードを追加した場合の **show lpts pifib** コマンドの出力を示しています。

```
RP/0/# show lpts pifib entry brief

* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;

Type          VRF-ID   Local, Remote Address.Port L4   Interface   Deliver
-----
ISIS          *        - -                          -    any        0/0/CPU0
IPv4_frag     *        any any                      any   any        R
IPv4_IXMP     *        any.ECHO any                    ICMP  any        XI
IPv4_IXMP     *        any.TSTAMP any                  ICMP  any        XI
IPv4_IXMP     *        any.MASKREQ any                ICMP  any        XI
IPv4_IXMP     *        any any                      ICMP  any        0/0/CPU0
IPv4_IXMP     *        any any                      IGMP   any        0/0/CPU0
IPv4_mcast    *        224.0.0.5 any                any   any        0/0/CPU0
IPv4_mcast    *        224.0.0.6 any                any   any        0/0/CPU0
IPv4_mcast    *        224.0.0.0/4 any                any   any        0/0/CPU0

IPv4_TCP      *        any.179 any                    TCP   any        0/0/CPU0
IPv4_TCP      *        any any.179                  TCP   any        0/0/CPU0
IPv4_TCP      *        any any                      TCP   any        0/0/CPU0
IPv4_UDP      *        any any                      UDP   any        0/0/CPU0
IPv4_IPsec    *        any any                      ESP   any        0/0/CPU0
IPv4_IPsec    *        any any                      AH    any        0/0/CPU0
IPv4_rawIP    *        any any                      OSPF  any        0/0/CPU0
IPv4_rawIP    *        any any                      any   any        0/0/CPU0
IPv6_frag     *        any any                      any   any        R
IPv6_ICMP     *        any.na any                    ICMP6 any        XI
IPv6_ICMP     *        any any                      ICMP6 any        0/0/CPU0
IPv6_mcast    *        ff02::5 any                    any   any        0/0/CPU0
IPv6_mcast    *        ff02::6 any                    any   any        0/0/CPU0
IPv6_mcast    *        ff00::/8 any                    any   any        0/0/CPU0
IPv6_TCP      *        any.179 any                    TCP   any        0/0/CPU0
IPv6_TCP      *        any any.179                  TCP   any        0/0/CPU0
IPv6_TCP      *        any any                      TCP   any        0/0/CPU0
IPv6_UDP      *        any any                      UDP   any        0/0/CPU0
IPv6_IPsec    *        any any                      ESP   any        0/0/CPU0
IPv6_IPsec    *        any any                      AH    any        0/0/CPU0
IPv6_rawIP    *        any any                      OSPF  any        0/0/CPU0
```

```
IPv6_rawIP *          any any          any any          0/0/CPU0
```

次の例は、**entry**、**brief** と **entry briefstatistics** キーワードを追加した場合の **show lpts pifib** コマンドの出力を示しています。

```
RP/0/# show lpts pifib entry brief statistics
```

```
* - Critical Flow; I - Local Interest;
X - Drop; R - Reassemble;
```

Type	VRF-ID	Local, Remote Address.Port	L4	Interface	Accepts/Drops
ISIS	*	- -	-	any	0/0
IPv4_frag	*	any any	any	any	0/0
IPv4_IXMP	*	any.ECHO any	ICMP	any	0/0
IPv4_IXMP	*	any.TSTAMP any	ICMP	any	0/0
IPv4_IXMP	*	any.MASKREQ any	ICMP	any	0/0
IPv4_IXMP	*	any any	ICMP	any	5/0
IPv4_IXMP	*	any any	IGMP	any	0/0
IPv4_mcast	*	224.0.0.5 any	any	any	0/0
IPv4_mcast	*	224.0.0.6 any	any	any	0/0
IPv4_mcast	*	224.0.0.0/4 any	any	any	0/0
IPv4_TCP	*	any.179 any	TCP	any	0/0
IPv4_TCP	*	any any.179	TCP	any	0/0
IPv4_TCP	*	any any	TCP	any	0/0
IPv4_UDP	*	any any	UDP	any	4152/0
IPv4_IPsec	*	any any	ESP	any	0/0
IPv4_IPsec	*	any any	AH	any	0/0
IPv4_rawIP	*	any any	OSPF	any	0/0

```
statistics:
```

Type	Num. Entries	Accepts/Drops
ISIS	1	0/0
IPv4_frag	1	0/0
IPv4_IXMP	5	5/0
IPv4_mcast	3	0/0
IPv4_TCP	3	0/0
IPv4_UDP	1	4175/0
IPv4_IPsec	2	0/0
IPv4_rawIP	2	0/0
IPv6_frag	1	0/0
IPv6_ICMP	2	0/0
IPv6_mcast	3	0/0
IPv6_TCP	3	0/0
IPv6_UDP	1	0/0
IPv6_IPsec	2	0/0
IPv6_rawIP	2	0/0
Total	32	

```
Packets into Pre-IFIB: 4263
```

```
Lookups: 4263
```

```
Packets delivered locally: 4263
```

```
Packets delivered remotely: 0
```

次の表には、**show lpts pifib** コマンドで **brief** と **statistics** キーワードを指定した場合に表示される重要なフィールドが記載されています。

表 38 : show lpts pifib コマンドのフィールドの説明

フィールド	説明
Type	ハードウェア エントリ タイプ
VRF ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Local, Remote Address.Port	ローカル アドレス (ローカル ポートとタイプの形式) とリモート アドレス (リモート ポート)
L4	エントリのレイヤ 4 プロトコル
Interface	このエントリのインターフェイス
Accepts/Drops	DestAddr に送信されたパケット数/ポリシングによりドロップされたパケット数
Num.Entries	リストされたタイプの pre-ifib エントリ数
Packets into Pre-IFIB	pre-IFIB ルックアップに渡されたパケット数
Lookups	ルックアップされたパケット数
Packets delivered locally	ローカルアプリケーションに配信されたパケット数、またはアプリケーションおよびローカルスタックへの配信用に複製されたローカルスタック (n 個複製) のパケット数
Packets delivered remotely	アプリケーションまたは他の RP 上でのルックアップのために配信されたパケット数

show lpts pifib hardware police

ポリサー設定値セットを表示するには、XR EXEC モードで **show lpts pifib hardware police** コマンドを使用します。

show lpts pifib hardware police [**location** {**all**|*node-id*}]

構文の説明

location <i>node-id</i>	(任意) 指定したノードの pre-Internal Forwarding Information Base (IFIB) 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
all	すべての場所を指定します。

コマンド デフォルト

ポリサーが設定されていない場合、デフォルト値は設定レートです。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、0/RP0/CPU0 に対して **location** キーワードを指定した場合の **show lpts pifib hardware police** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router#show lpts pifib hardware police location 0/RP0/CPU0
```

show lpts pifib hardware police

```

-----
Node 0/RP0/CPU0:
-----
Burst = 100ms for all flow types
-----

```

FlowType	Policer	Type	Cur. Rate	Def. Rate	Accepted	Dropped
unconfigured-default	100	Static	500	500	0	0
Fragment	106	Static	1000	1000	0	0
OSPF-mc-known	107	Static	20000	20000	0	0
OSPF-mc-default	111	Static	5000	5000	0	0
OSPF-uc-known	161	Static	5000	5000	0	0
OSPF-uc-default	162	Static	1000	1000	0	0
ISIS-known	108	Static	20000	20000	0	0
ISIS-default	112	Static	5000	5000	0	0
BFD-known	170	Static	8500	8500	0	0
BFD-default	171	Static	8500	8500	0	0
BFD-MP-known	177	Static	8400	8400	0	0
BFD-MP-0	178	Static	128	128	0	0
BGP-known	113	Static	25000	25000	0	0
BGP-cfg-peer	114	Static	10000	10000	0	0
BGP-default	115	Static	1500	1500	0	0
PIM-mcast-default	116	Static	23000	23000	0	0
PIM-mcast-known	176	Static	23000	23000	0	0
PIM-ucast	117	Static	10000	10000	0	0
IGMP	118	Static	3500	3500	0	0
ICMP-local	119	Static	2500	2500	0	0
ICMP-app	120	Static	2500	2500	0	0
ICMP-control	164	Static	2500	2500	0	0
ICMP-default	121	Static	2500	2500	0	0
LDP-TCP-known	122	Static	25000	25000	0	0
LDP-TCP-cfg-peer	152	Static	10000	10000	0	0
LDP-TCP-default	154	Static	10000	10000	0	0
LDP-UDP	158	Static	2500	2500	0	0
All-routers	160	Static	10000	10000	0	0
LMP-TCP-known	123	Static	25000	25000	0	0
LMP-TCP-cfg-peer	153	Static	10000	10000	0	0
LMP-TCP-default	155	Static	10000	10000	0	0
LMP-UDP	159	Static	2500	2500	0	0
RSVP-UDP	124	Static	7000	7000	0	0
RSVP-default	125	Static	500	500	0	0
RSVP-known	126	Static	7000	7000	0	0
IKE	127	Static	1000	1000	0	0
IPSEC-known	129	Static	3000	3000	0	0
IPSEC-default	128	Static	1000	1000	0	0
MSDP-known	130	Static	1000	1000	0	0
MSDP-cfg-peer	131	Static	1000	1000	0	0
MSDP-default	132	Static	1000	1000	0	0
SNMP	133	Static	2000	2000	0	0
SSH-known	135	Static	1000	1000	0	0
SSH-default	136	Static	1000	1000	0	0
HTTP-known	137	Static	1000	1000	0	0
HTTP-default	138	Static	1000	1000	0	0
SHTTP-known	139	Static	1000	1000	0	0
IFIB_FT_SHTTP_DEFAULT	140	Static	1000	1000	0	0
TELNET-known	141	Static	1000	1000	0	0
TELNET-default	142	Static	1000	1000	0	0
CSS-known	143	Static	1000	1000	0	0
CSS-default	144	Static	1000	1000	0	0
RSH-known	145	Static	1000	1000	0	0
RSH-default	146	Static	1000	1000	0	0
UDP-known	147	Static	25000	25000	0	0
UDP-listen	156	Static	4000	4000	0	0
UDP-cfg-peer	157	Static	4000	4000	0	0
UDP-default	101	Static	500	500	0	0
TCP-known	148	Static	25000	25000	0	0
TCP-listen	149	Static	25000	25000	0	0
TCP-cfg-peer	150	Static	25000	25000	0	0
TCP-default	102	Static	500	500	0	0
Mcast-known	151	Static	25000	25000	0	0
Mcast-default	103	Static	500	500	0	0
Raw-listen	104	Static	500	500	0	0
Raw-default	105	Static	500	500	0	0

```

Ip-Sla          163      Static  10000   10000   0        0
EIGRP          109      Static  20000   20000   0        0
RIP            110      Static  20000   20000   0        0
L2TPv3        165      Static  25000   25000   0        0
PCEP          166      Static  100     100     0        0
GRE           167      Static  1000    1000    0        0
VRRP          168      Static  1000    1000    0        0
HSRP          169      Static  400     400     0        0
MPLS-oam      172      Static  100     100     0        0
L2TPv2        179      Static  25000   25000   0        0
DNS           173      Static  500     500     0        0
RADIUS        174      Static  7000    7000    0        0
TACACS        175      Static  500     500     0        0
NTP-default   134      Static  500     500     0        0
NTP-known     180      Static  500     500     0        0

```

```

-----
statistics:
Packets accepted by deleted entries: 0
Packets dropped by deleted entries: 0
Run out of statistics counter errors: 0

```

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 39 : show lpts pifib hardware police コマンドのフィールドの説明

フィールド	説明
FlowType	タプルと宛先の間でバインドしているフローのタイプ
Policer	PPS のポリサー値
Rate (PPS)	ポリサー レート (パケット/秒、PPS 単位)
Accept	このポリサーによって許可されたパケット数
Drop	このポリサーによってドロップされたパケット数

show lpts pifib hardware usage

ハードウェア テーブルの使用状況を表示するには、XR EXEC モードで **show lpts pifib hardware usage** コマンドを使用します。

show lpts pifib hardware usage [**type** {**ipv4**|**ipv6**|**isis**}] [**location** {*node-id*|**all**}]

構文の説明

type	(任意) ハードウェア エントリ タイプを指定します。次のいずれかのタイプを入力します。 <ul style="list-style-type: none"> • ipv4 : IPv4 エントリを指定します。 • ipv6 : IPv6 エントリを指定します。 • isis : ISIS エントリを指定します。
location <i>node-id</i>	(任意) 指定したノードの pre-Internal Forwarding Information Base (IFIB) 情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
all	(任意) すべての場所を指定します。

コマンド デフォルト

オプションパラメータを指定しない場合、**show lpts pifib hardware usage** コマンドは、ハードウェア エントリ情報の簡潔なサマリーを表示します。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**location** キーワードを指定した場合の **show lpts pifib hardware usage** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show lpts pifib hardware usage location 0/RP0/cpu0
```

Type	Size	Used	Used(%)
ipv4	6000	21	0.35
ipv6	4000	15	0.38
isis	4000	1	0.03

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 40 : **show lpts pifib hardware usage** コマンドのフィールドの説明

フィールド	説明
Type	pre-IFIB エントリのタイプ
Size	このタイプに許可される最大エントリ数 (72 ビット)
Used	使用中のエントリ数
Used(%)	使用中の合計エントリのパーセンテージ

show lpts pifib statistics

Pre-Internal Forwarding Information Base (Pre-IFIB) 統計情報を表示するには、で **show lpts ifib statistics** コマンドを使用します。

show lpts pifib statistics [*location node-id*]

構文の説明

location*node-id* (任意) 指定したノードの Pre-IFIB 統計情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts pifib statistics** コマンドの出力を示しています。

```
RP/0/# show lpts pifib statistics
```

```
Packets into Pre-IFIB:80
Lookups:80
Packets delivered locally:80
Packets delivered remotely:0
```

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 41 : show lpts pifib statistics コマンドのフィールドの説明

フィールド	説明
Packets into Pre-IFIB	pre-IFIB ルックアップに渡されたパケット数
Lookups	ルックアップされたパケット数
Packets delivered locally	ローカルアプリケーションに配信されたパケット数、またはアプリケーションおよびローカルスタックへの配信用に複製されたローカルスタック (n 個複製) のパケット数
Packets delivered remotely	アプリケーションまたは他の RP 上でのルックアップのために配信されたパケット数

show lpts port-arbitrator statistics

Local Packet Transport Services (LPTS) ポートアービトラータ統計情報を表示するには、XR EXEC モードで **show lpts port-arbitrator statistics** コマンドを使用します。

show lpts port-arbitrator statistics

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
lpts	読み取り

例

次の例は、**show lpts port-arbitrator statistics** コマンドの出力を示しています。

```
RP/0/RP0/CPU0:router# show lpts port-arbitrator statistics

LPTS Port Arbitrator statistics:
PA FGID-DB library statistics:
 0 FGIDs in use, 512 cached, 0 pending retries
 0 free allocation slots, 0 internal errors, 0 retry attempts
 1 FGID-DB notify callback, 0 FGID-DB errors returned
FGID-DB permit mask: 0x7 (alloc mark rack0)
PA API calls:
   1 init                1 realloc_done
   8 alloc                8 free
  16 join                16 leave
   8 detach
```

```
FGID-DB API calls:
  1 register          1 clear_old
  1 alloc             0 free
 16 join              16 leave
  0 mark              1 mark_done
```

```
show lpts port-arbitrator statistics
```



ネットワークスタック IPv4 および IPv6 コマンド

この章では、IP バージョン 4 (IPv4) や IP バージョン 6 (IPv6) に関連する機能を設定したりモニタする場合に、NCS 5000 ルータで使用可能な Cisco IOS XR ソフトウェアのコマンドについて説明します。

ネットワークスタックの概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [clear ipv6 neighbors, 273 ページ](#)
- [icmp ipv4 rate-limit unreachable, 275 ページ](#)
- [ipv4 address \(ネットワーク\), 277 ページ](#)
- [ipv4 assembler max-packets, 280 ページ](#)
- [ipv4 assembler timeout, 281 ページ](#)
- [ipv4 mask-reply, 283 ページ](#)
- [ipv4 conflict-policy, 284 ページ](#)
- [ipv4 mtu, 286 ページ](#)
- [ipv4 unnumbered \(point-to-point\), 288 ページ](#)
- [ipv6 address, 290 ページ](#)
- [ipv6 assembler, 292 ページ](#)
- [ipv6 conflict-policy, 294 ページ](#)
- [ipv6 address link-local, 296 ページ](#)
- [ipv6 enable, 298 ページ](#)
- [ipv6 hop-limit, 300 ページ](#)
- [ipv6 icmp error-interval, 301 ページ](#)

- [ipv6 mtu, 303 ページ](#)
- [ipv6 nd dad attempts, 305 ページ](#)
- [ipv6 nd managed-config-flag, 308 ページ](#)
- [ipv6 nd ns-interval, 310 ページ](#)
- [ipv6 nd other-config-flag, 312 ページ](#)
- [ipv6 nd prefix, 314 ページ](#)
- [ipv6 nd ra-interval, 317 ページ](#)
- [ipv6 nd ra-lifetime, 319 ページ](#)
- [ipv6 nd reachable-time, 321 ページ](#)
- [ipv6 nd redirects, 323 ページ](#)
- [ipv6 nd scavenge-timeout, 324 ページ](#)
- [ipv6 nd suppress-ra, 325 ページ](#)
- [ipv6 neighbor, 327 ページ](#)
- [ipv6 path-mtu enable, 330 ページ](#)
- [ipv6 path-mtu timeout, 331 ページ](#)
- [ipv6 source-route, 332 ページ](#)
- [ipv6 tcp-mss-adjust, 334 ページ](#)
- [ipv6 virtual address, 336 ページ](#)
- [show arm conflicts, 338 ページ](#)
- [show arm registrations producers, 341 ページ](#)
- [show arm router-ids, 343 ページ](#)
- [show arm summary, 345 ページ](#)
- [show ipv4 interface, 347 ページ](#)
- [show ipv4 traffic, 351 ページ](#)
- [show ipv6 interface, 354 ページ](#)
- [show ipv6 neighbors, 359 ページ](#)
- [show ipv6 neighbors summary, 365 ページ](#)
- [show ipv6 path-mtu, 366 ページ](#)
- [show ipv6 traffic, 368 ページ](#)

clear ipv6 neighbors

スタティック エントリ以外のIPv6 ネイバー探索キャッシュのすべてのエントリを削除するには、**clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors [*location node-id*]

構文の説明

location*node-id* (任意) 指定されたノード。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location オプションを指定した場合は、**location***node-id* キーワードと引数で指定されているネイバー エントリだけがクリアされます。

タスク ID

タスク ID	動作
network	読み取り、書き込み
IPv6	実行

例

次の例では、ハイライトされたエントリだけが削除されます。

```
RP/0/# clear ipv6 neighbors ?
location specify a node name

RP/0/# show ipv6 neighbor
```

clear ipv6 neighbors

```
IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH tenGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH tenGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE tenGigE0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE tenGigE0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE tenGigE0/0/0/2
```

```
RP/0/# clear ipv6 neighbors location 0/2/0
RP/0/# show ipv6 neighbor
```

```
IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH tenGigE0/0/0/0
8888::8 - 1234.2345.9877 REACH tenGigE0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE tenGigE0/0/0/0
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE tenGigE0/0/0/0
```

icmp ipv4 rate-limit unreachable

IPv4 インターネット制御メッセージプロトコル (ICMP) 宛先到達不能メッセージが生成されるレートを制限するには、で **icmp ipv4 rate-limit unreachable** コマンドを使用します。レート制限を削除するには、このコマンドの **no** 形式を使用します。

icmp ipv4 rate-limit unreachable [DF] milliseconds

no icmp ipv4 rate-limit unreachable [DF] milliseconds

構文の説明

DF	(任意) コード 4 フラグメンテーションが必要で、データフラグメンテーション (DF) が設定されているときに、ICMP 宛先到達不能メッセージの IP ヘッダーに指定されているように、ICMP 宛先到達不能メッセージが送信されるレートを制限します。
<i>milliseconds</i>	ICMP 宛先到達不能メッセージの送信間隔 (ミリ秒)。範囲は 1 ~ 4294967295 です。

コマンド デフォルト

デフォルトでは、500 ミリ秒ごとに 1 件の ICMP 宛先到達不能メッセージが送信されます。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XR ソフトウェアは、通常の宛先到達不能メッセージ用と DF 宛先到達不能メッセージ用の 2 つのタイマーを保持します。これらは同じ時間制限およびデフォルトを共有します。DF オプションが設定されていない場合、**icmp ipv4 rate-limit unreachable** コマンドは、DF 宛先到達不能メッセージの時間値を設定します。DF オプションが設定されている場合、その時間値は、通常の宛先到達不能メッセージの時間値とは別に維持されます。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み

タスク ID	動作
network	読み取り、書き込み

例

次の例は、ICMP 宛先到達不能メッセージを生成する最小間隔を10 ミリ秒に設定する方法を示しています。

```
RP/0/(config)# icmp ipv4 rate-limit unreachable 10
```

ipv4 address (ネットワーク)

インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを設定するには、インターフェイス コンフィギュレーションモードで **ipv4 address** コマンドを使用します。IPv4 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。

ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]

no ipv4 address *ipv4-address mask* [**secondary**] [**route-tag** *route-tag value*]

構文の説明

ipv4-address	IPv4 アドレス。
<i>mask</i>	<p>関連する IP サブネットのマスク。ネットワーク マスクは、次のいずれかの方法で指定できます。</p> <ul style="list-style-type: none"> 4 分割ドット付き 10 進表記のアドレスでネットワーク マスクを指定します。たとえば、255.0.0.0 は、1 に等しい各ビットが、ネットワーク アドレスに属した対応するアドレス ビットを意味することを示します。 ネットワーク マスクは、スラッシュ (/) と数字で示すことができます。たとえば、/8 は、マスクの最初の 8 ビットが 1 で、対応するアドレスのビットがネットワーク アドレスであることを示します。
secondary	(任意) 設定されているアドレスが、セカンダリ IPv4 アドレスであることを指定します。このキーワードが省略されている場合、設定されているアドレスは、プライマリ IPv4 アドレスです。
route-tag	(任意) 設定されたアドレスに関連付けられるルート タグがあることを指定します。
<i>route-tag value</i>	(任意) ルート タグの値。範囲は 1 ~ 4294967295 です。

コマンド デフォルト

IPv4 アドレスはインターフェイスに定義されません。

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
リリース 6.0	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は、1つのプライマリ IPv4 アドレスと複数のセカンダリ IPv4 アドレスを定義できます。ソフトウェアにより生成されるパケットは、必ずプライマリ IPv4 アドレスを使用します。そのため、セグメントのすべてのネットワーキングデバイスは、同じプライマリネットワーク番号を共有する必要があります。



- (注) 2つの異なるインターフェイスに同じ IPv4 アドレスが設定されている場合、競合していることを示すエラーメッセージが表示されます。最も高いラック、スロット、モジュール、インスタンスおよびポートにあるインターフェイスはディセーブルになります。

ホストは、IPv4 インターネット制御メッセージプロトコル (ICMP) マスク要求メッセージを使用して、サブネットマスクを判別できます。ネットワーキングデバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

特定のインターフェイスで IPv4 処理をディセーブルにするには、**noipv4address** コマンドを使用してその IPv4 アドレスを削除します。ソフトウェアが、その IPv4 アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラーメッセージを表示します。

オプションの **secondary** キーワードを使用すると、セカンダリアドレスを無制限に指定できます。システムがセカンダリ送信元アドレスによるルート更新以外のデータグラムを生成しないという点を除き、セカンダリアドレスは、プライマリアドレスのように扱われます。IPv4 ブロードキャストおよびアドレス解決プロトコル (ARP) 要求は、IP ルーティングテーブルのインターフェイスルートのように、正しく処理されます。

セカンダリ IPv4 アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホストアドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1つの物理サブネットでは、300 のホストアドレスが必要になります。ここで、ネットワーキングデバイスでセカンダリ IPv4 アドレスを使用すると、2つの論理サブネットで1つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリアドレスは、慎重に使用することで、サブネット化されたルータベースネットワークへの移行に役立ちます。旧式のブリッジセグメントのルータでは、そのセグメントにサブネットがたくさんあることを簡単に認識させることができます。

route-tag 機能はすべての IPv4 アドレスにタグを付加します。タグは、Address Repository Manager (RPM) への管理エージェント (MA) からルーティングプロトコルに伝播されるため、RPL スクリプトによってルートタグを確認して、接続されたルートの再配布を制御するユーザをイネーブルにします。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/0/0/1 に、プライマリアドレスとして 192.168.1.27、セカンダリアドレスとして 192.168.7.17 および 192.168.8.17 を設定する方法を示しています。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv4 address 192.168.1.27 255.255.255.0
RP/0/(config-if)# ipv4 address 192.168.7.17 255.255.255.0 secondary
RP/0/(config-if)# ipv4 address 192.168.8.17 255.255.255.0 secondary
```

ipv4 assembler max-packets

アセンブリ キューで許可されるパケットの最大数を設定するには、で **ipv4 assembler max-packets** 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。

ipv4 assembler max-packets *percentage value*

no ipv4 assembler max-packets *percentage value*

構文の説明

percentage value システムで使用できるパケット合計数の割合。範囲は 1 ~ 50 です。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み

例

次に、アセンブリ キューのパケット最大数を設定する例を示します。

```
RP/0/(config)# ipv4 assembler max-packets 35
```

ipv4 assembler timeout

タイムアウトが発生するまでにアセンブリ キューを保持できる秒数を設定するには、で **ipv4 assembler timeout** 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。

ipv4 assembler timeout *seconds*

no ipv4 assembler timeout *seconds*

構文の説明

<i>seconds</i>	タイムアウトが発生する前にアセンブリ キューが保持できる秒数。指定できる範囲は 1 ~ 120 です。
----------------	---

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み

例

次に、タイムアウトが発生する前にアセンブリ キューが保持できる時間を設定する例を示します。

```
RP/0/(config)# ipv4 assembler timeout 88
```

ipv4 mask-reply

Cisco IOS XR ソフトウェアが ICMP マスク応答メッセージを送信して、IPv4 インターネット制御メッセージプロトコル (ICMP) マスク要求に応答できるようにするには、インターフェイス コンフィギュレーションモードで **ipv4mask-reply** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を入力します。

ipv4 mask-reply

no ipv4 mask-reply

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IPv4 マスク応答は送信されません。

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
リリース 6.0	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 IOS XR ソフトウェアが ICMP マスク応答メッセージを送信して IPv4 ICMP マスク要求に応答できるようにします。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、HundredGigE インターフェイス 0/1/0/0 で ICMP マスク応答メッセージの送信をイネーブルにします。

```
RP/0/(config)# interface HundredGigE0/1/0/0
RP/0/(config-if)# ipv4 mask-reply
```

ipv4 conflict-policy

IP Address Repository Manager (IPARM) 競合解決をイネーブルにするには、で **ipv4 conflict-policy** コマンドを使用します。IPARM 競合解決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。

ipv4 conflict-policy {highest-ip| longest-prefix| static}

no ipv4 conflict-policy {highest-ip| longest-prefix| static}

構文の説明

highest-ip	競合セットの最も高い IP アドレスを保持します。
longest-prefix	競合セットの最長プレフィックス マッチを保持します。
static	新しいアドレス設定で稼働する既存のインターフェイスを保持します。

コマンド デフォルト

採用される優先順位規則は、ループバック > 物理 > その他の仮想インターフェイスの順です。仮想インターフェイス内では、たとえば、loopback1 > loopback2 > tunnel のように、アルファベット順が採用されます。物理インターフェイスでは、低い方のラックまたはスロットが制御を取得します。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 conflict-policy コマンドは、設定されているアドレスでの競合を解決する IPARM ポリシーを設定するために使用します。このポリシーは、競合しているアドレスからどのアドレスを選択するかを IPARM に通知します。その後、競合しているアドレスを強制的に非アクティブにします。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み

タスク ID	動作
ip-services	読み取り、書き込み

例 次に、競合解決のスタティック ポリシーをイネーブルにする例を示します。

```
RP/0/(config)# ipv4 conflict-policy static
```

ipv4 mtu

インターフェイスで送信される IPv4 パケットの最大伝送ユニット (MTU) サイズを設定するには、インターフェイスコンフィギュレーションモードで **ipv4 mtu** コマンドを使用します。デフォルトの MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ipv4 mtu bytes

no ipv4 mtu

構文の説明

bytes バイト単位の MTU。範囲は、IPv4 パケットで 68 ~ 65535 バイトです。インターフェイスで設定できる最大 MTU サイズは、インターフェイス メディアにより異なります。

コマンド デフォルト

MTU サイズが、インターフェイスで送信される IPv4 パケットに設定されていない場合、そのインターフェイスは、レイヤ 2 MTU から MTU を取得します。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ルータはフラグメンテーションが必要なパケットをパントします。これに対して、ソフトウェアパスはフラグメンテーションが必要な加入者トラフィックをドロップします。

インターフェイスで設定できる最大 MTU サイズは、インターフェイス メディアにより異なります。レイヤ 2 MTU がレイヤ 3 MTU より小さい場合、Cisco IOS XR ソフトウェアは、レイヤ 3 MTU にレイヤ 2 MTU 値を使用します。逆に、レイヤ 3 MTU がレイヤ 2 MTU より小さい場合、ソフトウェアは、レイヤ 3 MTU 値を使用します。つまり、Cisco IOS XR ソフトウェアは、MTU の 2 つの値のうち小さい方を使用します。

物理メディアのすべてのデバイスは、同じプロトコル MTU を使用しなければなりません。



(注) (mtu 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) MTU 値を変更すると、IPv4 MTU 値が影響を受けます。現在の IPv4 MTU 値が、MTU 値と同じ場合、MTU 値を変更すると、IPv4 MTU 値は、新しい MTU に合わせて自動的に修正されます。ただし、この逆の影響はなく、IPv4 MTU 値を変更しても、mtu コマンドの値には影響しません。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/0/0/1 の最大 IPv4 パケット サイズを 1500 バイトに設定する方法を示しています。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv4 mtu 1500
```

ipv4 unnumbered (point-to-point)

明示的な IPv4 アドレスをポイントツーポイントインターフェイスに割り当てることなく、そのインターフェイスでの IPv4 処理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 **ipv4unnumbered** 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。

ipv4 unnumbered *interface-type interface-instance*

no ipv4 unnumbered *interface-type interface-instance*

構文の説明

interface-type インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。

interface-instance 次に示す、物理インターフェイスインスタンスまたは仮想インターフェイスインスタンスのいずれかです。

- 物理インターフェイス インスタンス。名前表記は *rack/slot/module/port* です。値の間に表記の一部としてスラッシュが必要です。
 - *rack* : ラックのシャーシ番号。
 - *slot* : モジュラ サービス カードまたはラインカードの物理スロット番号。
 - *module* : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。
 - *port* : インターフェイスの物理ポート番号。

(注) ルートプロセッサカード上の管理イーサネットインターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0

- 仮想インターフェイスインスタンス。数字の範囲は、インターフェイスタイプによって異なります。

ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

コマンド デフォルト

ポイントツーポイント インターフェイスでの IPv4 処理は、IPv4 アドレスがそのインターフェイスに明示的に割り当てられない限りディセーブルです。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

リリース R 4.2.0 以降の場合、ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。

unnumbered インターフェイスがパケットを生成する場合（たとえば、ルーティングアップデートのため）、必ず、IPv4 パケットの送信元アドレスとして指定されているインターフェイスのアドレスが使用されます。また、unnumbered インターフェイスを介してアップデートを送信するルーティング プロセスを判別する場合、指定されたインターフェイスの IPv4 アドレスが使用されます。制約事項は次のとおりです。

- インターフェイスにはアドレスがないため、**ping EXEC** コマンドを使用してインターフェイスがアップ状態かどうかを確認することはできません。簡易ネットワーク管理プロトコル (SNMP) は、インターフェイス ステータスのリモート監視に使用できます。

interface-type および *interface-number* 引数で指定されたインターフェイスが、イネーブルになっている必要があります (**show interfaces** コマンドの出力に「up」と表示)。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例は、tenGigE インターフェイス 0/0/0/1 にループバック インターフェイス アドレス 5 を割り当てる方法を示しています。

```
RP/0/(config)# interface loopback 5
RP/0/(config-if)# ipv4 address 192.168.6.6 255.255.255.0
RP/0/(config)# interface tenGigE 0/0/0/1
RP/0/(config-if)# ipv4 unnumbered loopback 5
```

ipv6 address

インターフェイスに IPv6 アドレスを設定し、そのアドレスの下位 64 ビットに EUI-64 インターフェイス ID を指定してインターフェイスでの IPv6 処理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 **ipv6 address** コマンドを使用します。インターフェイスから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。

ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]

no ipv6 address *ipv6-prefix/prefix-length* [**eui-64**] [**route-tag** *route-tag value*]

構文の説明

<i>ipv6-prefix</i>	インターフェイスに割り当てられた IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>/prefix-length</i>	IPv6 プレフィックスの長さ。これは、プレフィックス（アドレスのネットワーク部）を構成するアドレスの上位隣接ビット数を示す 10 進数値です。10 進数値の前にスラッシュ記号 (/) を付ける必要があります。
eui-64	(任意) IPv6 アドレスの下位 64 ビットにインターフェイス ID を指定します。
route-tag	(任意) 設定されたアドレスに関連付けられるルートタグがあることを指定します。
<i>route-tag value</i>	(任意) ルートタグの値。範囲は 1 ~ 4294967295 です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン `/prefix-length` 引数で指定された値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。

引数を指定せずに `no ipv6 address` コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

Cisco IOS XR ソフトウェアはその IPv6 アドレスのいずれかを使用している別のホストを検出すると、コンソールにエラー メッセージを表示します。

`route-tag` 機能はすべての IPv6 アドレスにタグを付加します。タグは、Address Repository Manager (RPM) への管理エージェント (MA) からルーティング プロトコルに伝播されるため、RPL スクリプトによってルート タグを確認して、接続されたルートの再配布を制御するユーザをイネーブルにします。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例では、IPv6 アドレス `2001:0DB8:0:1::/64` を `tenGigE` インターフェイス `0/0/0/1` に割り当て、アドレスの下位 64 ビットに `EUI-64` インターフェイス ID を指定します。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

ipv6 assembler

アセンブリ キューで許可されるパケットの最大数を設定したり、タイムアウトまでのアセンブリ キューを保持する秒数を設定するには、適切なコンフィギュレーション モードで **ipv6 assembler** 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。

ipv6 assembler {*max-packetsvalue*|*timeoutseconds*}

no ipv6 assembler {*max-packetsvalue*|*timeoutseconds*}

構文の説明

max-packets	アセンブリ キューで許可されるパケットの最大数。
timeout	タイムアウトの前にアセンブリ キューが保持する秒数。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み

例

次に、アセンブリ キューで許可されるパケットの最大数を設定する例を示します。

```
RP/0/# config
```

```
RP/0/(config)# ipv6 assembler max-packets 100
```

ipv6 conflict-policy

IP Address Repository Manager (IPARM) 競合解決をイネーブルにするには、で **ipv6 conflict-policy** コマンドを使用します。IPARM 競合解決をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 conflict-policy {highest-ip| longest-prefix| static}

no ipv6 conflict-policy {highest-ip| longest-prefix| static}

構文の説明

highest-ip	競合セットの最も高い IP アドレスを保持します。
longest-prefix	競合セットの最長プレフィックス マッチを保持します。
static	新しいアドレス設定で稼働する既存のインターフェイスを保持します。

コマンド デフォルト

競合ポリシーが設定されていない場合、最も低いラック/スロットがデフォルトです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
ip-services	読み取り、書き込み

例 次に、競合解決の最長プレフィックス ポリシーをイネーブルにする例を示します。

```
RP/0/(config)# ipv6 conflict-policy longest-prefix
```

ipv6 address link-local

インターフェイスに IPv6 リンクローカルアドレスを設定し、インターフェイスでの IPv6 処理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 **ipv6 address link-local** コマンドを使用します。このコマンドで指定した *ipv6-address* 値は、インターフェイスに対して自動的に生成されるリンクローカルアドレスよりも優先されます。インターフェイスから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。

ipv6 address *ipv6-address* link-local [route-tag *route-tag value*]

no ipv6 address *ipv6-address* link-local [route-tag *route-tag value*]

構文の説明

<i>ipv6-address</i>	インターフェイスに割り当てられた IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
link-local	リンクローカルアドレスを指定します。このコマンドで指定した <i>ipv6-address</i> 値は、インターフェイスに対して自動的に生成されるリンクローカルアドレスよりも優先されます。
route-tag	(任意) 設定されたアドレスに関連付けられるルートタグがあることを指定します。
<i>route-tag value</i>	(任意) ルートタグ値を表示します。範囲は 1 ~ 4294967295 です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XR ソフトウェアはその IPv6 アドレスのいずれかを使用している別のホストを検出すると、コンソールにエラーメッセージを表示します。

IPv6 処理がインターフェイスでイネーブルにされていて、通常、IPv6 アドレスがインターフェイスで設定されている場合、インターフェイスのリンクローカルアドレスが自動的に生成されます。インターフェイスで使用されるリンクローカルアドレスを手動で指定するには、**ipv6 address link-local** コマンドを使用します。

連続する 16 ビット値がゼロとして指定されている場合は、2 つのコロンを *ipv6-address* 引数の一部として使用できます。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカルアドレスは 1 つだけです。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、FE80::260:3EFF:FE11:6770 を tenGigE インターフェイス 0/0/0/1 のリンクローカルアドレスとして割り当てる方法を示しています。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイスでの IPv6 処理をイネーブルにするには、適切なコンフィギュレーションモードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスが設定されていないインターフェイスでの IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable

no ipv6 enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IPv6 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 (BNG 以外に適用)

ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイスに IPv6 リンクローカルユニキャストアドレスを自動的に設定し、さらにインターフェイスでの IPv6 処理をイネーブルにします。 **no ipv6 enable** コマンドを使用しても、明示的な IPv6 アドレスが設定されているインターフェイスでの IPv6 処理はディセーブルになりません。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、**dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

タスク ID	動作
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、tenGigE インターフェイス 0/0/0/1 で IPv6 処理をイネーブルにする方法を示しています。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv6 enable
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 処理をイネーブルにする方法を示しています。

```
RP/0/(config)# dynamic-template type ppp foo
RP/0/(config-dynamic-template-type)# ipv6 enable
```

ipv6 hop-limit

ルータアドバタイズメントで使用されるホップと、ルータから発信されるすべてのIPv6パケットで使用されるホップの最大数を設定するには、`ipv6 hop-limit` コマンドを使用します。ホップの制限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。

ipv6 hop-limit hops

no ipv6 hop-limit hops

構文の説明

hops ホップの最大数。値の範囲は 1 ~ 255 です。

コマンド デフォルト

hops : 64 ホップ

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次に、ルータから発信されるルータアドバタイズメントおよびすべてのIPv6パケットの最大数を 15 ホップに設定する例を示します。

```
RP/0/(config)# ipv6 hop-limit 15
```

ipv6 icmp error-interval

IPv6 インターネット制御メッセージプロトコル (ICMP) エラーメッセージの間隔とバケットサイズをすべてのノードに設定するには、で **ipv6 icmp error-interval** コマンドを使用します。間隔を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。

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

構文の説明

milliseconds バケットに保存されるトークンの間隔 (ミリ秒)。範囲は0～2147483647です。

bucketsize (任意) バケットに保存されるトークンの最大数。許容範囲は1～200です。デフォルトは10 トークンです。

コマンド デフォルト

デフォルトでは、ICMP レート制限はイネーブルです。ICMP レート制限をディセーブルにするには、間隔をゼロに設定します。

milliseconds : 100 ミリ秒

bucketsize : 10 トークン

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

モードで **ipv6 icmp error-interval** コマンドを使用すると、IPv6 ICMP エラーメッセージが各ノードに送信されるレートを制限できます。トークンバケットアルゴリズムは、1件のIPv6 ICMP エラーメッセージを表す1つのトークンで使用されます。トークンは、バケットで許可されているトークンの最大数に達するまで、指定された間隔で、仮想バケットに保存されます。

milliseconds 引数は、トークンがバケットに保存される間隔を指定します。オプションの *bucketsize* 引数は、バケットに保存されるトークンの最大数の定義に使用されます。トークンは、IPv6 ICMP エラーメッセージが送信されるとバケットから削除されます。たとえば、*bucketsize* 引数を20に設定すると、20のIPv6 ICMP エラーメッセージを連続して送信することができます。トークンの

バケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラーメッセージは送信されません。

show ipv6 traffic EXEC コマンドを使用すると、IPv6 ICMP レート制限カウンタを表示できます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラーメッセージに対して設定されていることを示します。

```
RP/0/(config)# ipv6 icmp error-interval 50 20
```

ipv6 mtu

インターフェイスで送信される IPv6 パケットの最大伝送ユニット (MTU) サイズを設定するには、適切なコンフィギュレーションモードで **ipv6 mtu** コマンドを使用します。デフォルトの MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ipv6 mtu bytes

no ipv6 mtu

構文の説明

bytes バイト単位の MTU。範囲は、IPv6 パケットで 1280 ~ 65535 バイトです。インターフェイスで設定できる最大 MTU サイズは、インターフェイスメディアにより異なります。

コマンド デフォルト

MTU サイズが、インターフェイスで送信される IPv6 パケットに設定されていない場合、そのインターフェイスは、レイヤ 2 MTU から MTU を取得します。

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 (BNG 以外に適用)
ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv6 パケットが、インターフェイスで設定されている MTU を超える場合、パケットの発信元ルータだけがこれをフラグメントできます。

インターフェイスで設定できる最大 MTU サイズは、インターフェイスメディアにより異なります。レイヤ 2 MTU がレイヤ 3 MTU より小さい場合、Cisco IOS XR ソフトウェアは、レイヤ 3 MTU にレイヤ 2 MTU 値を使用します。逆に、レイヤ 3 MTU がレイヤ 2 MTU より小さい場合、ソフトウェアは、レイヤ 3 MTU 値を使用します。つまり、Cisco IOS XR ソフトウェアは、MTU の 2 つの値のうち小さい方を使用します。

物理メディアのすべてのデバイスは、同じプロトコル MTU を使用しなければなりません。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。



- (注) (mtu 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) MTU 値を変更すると、IPv6 MTU 値が影響を受けます。現在の IPv6 MTU 値が、MTU 値と同じ場合、MTU 値を変更すると、IPv6 MTU 値は、新しい MTU に合わせて自動的に修正されます。ただし、この逆の影響はなく、IPv6 MTU 値を変更しても、**mtu** コマンドの値には影響しません。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例 (BNG 以外に該当) は、tenGigE インターフェイス 0/0/0/1 の最大 IPv6 パケット サイズを 1350 バイトに設定する方法を示しています。

```
RP/0/(config)# interface tenGigE0/0/0/1
RP/0/(config-if)# ipv6 mtu 1350
```

次の例 (BNG に該当) は、ダイナミック テンプレート コンフィギュレーション モードで最大 IPv6 パケット サイズを 1350 バイトに設定する方法を示しています。

```
RP/0/(config)# dynamic-template type ppp foo
RP/0/(config-dynamic-template-type)# ipv6 mtu 1350
```

ipv6 nd dad attempts

インターフェイスのユニキャスト IPv6 アドレスに対して重複アドレスの検出が実行されているときに、そのインターフェイスから送信される連続ネイバー送信要求メッセージの数を設定するには、適切なコンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。メッセージ数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。

ipv6 nd dad attempts value

no ipv6 nd dad attempts value

構文の説明

value ネイバー送信要求メッセージ数。範囲は 0 ～ 600 です。値 0 を設定すると、指定されたインターフェイスでの重複アドレス検出処理がディセーブルになります。値 1 を設定すると、追加送信のない単一送信が行われます。

コマンド デフォルト

1 件のネイバー送信要求メッセージが送信される、ユニキャスト IPv6 アドレスの重複アドレス検出がイネーブルにされています。デフォルトは 1 メッセージです。

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 (BNG 以外に適用)

ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます (重複アドレス検出の実行中、新しいアドレスは一時的な状態になります)。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。

DupAddrDetectTransmits ノード設定変数 (『IPv6 Stateless Address Autoconfiguration』の RFC 2462 で指定されています) は、tentative ユニキャスト IPv6 アドレスで重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数を自動的に判別するときに使用されます。

重複アドレス検出のネイバー送信要求メッセージの送信間隔 (重複アドレス検出タイムアウト間隔) は、ネイバー探索に関連する変数 **RetransTimer** (『Neighbor Discovery for IP Version 6 [IPv6]』

の RFC 2461 で指定されています) により指定されます。この変数は、アドレスが解決されるとき、または隣接の到達可能性がプローブされるときに、ネイバー送信要求メッセージが再隣接に転送される間隔を決定するために使用されます。これは、アドレス解決およびネイバー到達不能検出中のネイバー送信要求メッセージの間隔を指定するときに使用される管理変数と同じです。

ipv6 nd ns-interval コマンドを使用すると、重複アドレスの検出中に送信されるネイバー送信要求メッセージの間隔を設定できます。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。インターフェイスが管理上アップ状態に戻ると、そのインターフェイスで重複アドレス検出が自動的に再起動されます。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。



(注)

管理上アップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスを対象に重複アドレス検出が再起動されます。インターフェイスのリンクローカルアドレスで重複アドレス検出が実行されている間、他の IPv6 アドレスの状態は仮承諾に設定されたままとなります。リンクローカルアドレスで重複アドレス検出が完了すると、残りの IPv6 アドレスで重複アドレス検出が実行されます。

重複アドレス検出が、重複アドレスを確認すると、アドレスの状態は、**duplicate** に設定され、そのアドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカルアドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラーメッセージが発行されます。

```
ipv6_nd[145]: %IPV6_ND-3-ADDRESS_DUPLICATE : Duplicate address 111::1 has been detected
```

重複アドレスがインターフェイスのグローバルアドレスである場合、そのアドレスは使用されず、次のようなエラーメッセージが発行されます。

```
%IPV6-4-DUPLICATE: Duplicate address 3000::4 on tenGigE&;
```

重複アドレスに関連付けられているすべてのコンフィギュレーション コマンドは、アドレスの状態が **duplicate** に設定されている間、設定された状態のままになります。

インターフェイスのリンクローカルアドレスが変更された場合、新しいリンクローカルアドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます (重複アドレス検出は新規のリンクローカルアドレスでのみ実行されます)。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例 (BNG 以外に該当) は、インターフェイス 0/2/0/1 で送信される連続ネイバー送信要求メッセージの数を 1 に設定し、インターフェイスに設定されているユニキャスト IPv6 アドレスのステータス (tentative または duplicate) を表示する方法を示しています。

```
RP/0/# configure
RP/0/(config)# interface HundredGigE0/2/0/1
RP/0/(config-if)# ipv6 nd dad attempts 1
RP/0/(config-if)# Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:y

RP/0/# show ipv6 interface
HundredGigE/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
HundredGigE/2/0/1 is Up, line protocol is Up
  IPv6 is enabled, link-local address is fe80::203:fdff:fe1b:4501
  Global unicast address(es):
    1:4::1, subnet is 1:4::/64 [DUPLICATE]
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
HundredGigE/2/0/2 is Shutdown, line protocol is Down
  IPv6 is enabled, link-local address is fe80::200:11ff:fe11:1111 [TENTATIVE]
  Global unicast address(es):
    111::2, subnet is 111::/64 [TENTATIVE]
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

次の例 (BNG に該当) は、ダイナミック テンプレート コンフィギュレーション モードでユニキャスト IPv6 アドレスのステータス (tentative または duplicate) を表示する方法を示しています。

```
RP/0/(config)# dynamic-template type ppp p1
RP/0/(config-dynamic-template-type)# ipv6 nd dad attempts 1
```

ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定するには、適切なコンフィギュレーション モードで **ipv6 nd managed-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

managed address configuration フラグは、IPv6 ルータ アドバタイズメントで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 (BNG 以外に適用)

ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

managed address configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレスの取得にステートフル オートコンフィギュレーションを使用するかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用します。このフラグが設定されていない場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用しません。

ホストは、ステートフルおよびステートレス オートコンフィギュレーションを同時に使用できません。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み

タスク ID	動作
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 で IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定する方法を示しています。

```
RP/0/(config)# interface HundredGigE0/1/0/1  
RP/0/(config-if)# ipv6 nd managed-config-flag
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定する方法を示しています。

```
RP/0/(config)# dynamic-template type ppp p1  
RP/0/(config-dynamic-template-type)# ipv6 nd managed-config-flag
```

ipv6 nd ns-interval

インターフェイスで IPv6 ネイバー送信要求メッセージを再送信する間隔を設定するには、適切なコンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

構文の説明

<i>milliseconds</i>	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒）。値の範囲は 1000 ～ 3600000 です。
---------------------	--

コマンド デフォルト

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 1000 は、ルータ自体のネイバー探索アクティビティに使用されます。

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（BNG 以外に適用）
ダイナミック テンプレート コンフィギュレーション（BNG 向け）

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

この値は、このインターフェイスから送信されるすべての IPv6 ルータアドバタイズメントに含まれます。通常の IPv6 操作には、短すぎる間隔はお勧めできません。デフォルト以外の値が設定されている場合、設定時間は、ルータ自体により、アドバタイズおよび使用されます。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み

タスク ID	動作
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、tenGigE インターフェイス 0/1/0/1 に IPv6 ネイバー送信要求の送信間隔として 9000 ミリ秒を設定します。

```
RP/0/(config)# interface tenGigE0/1/0/1
RP/0/(config-if)# ipv6 nd ns-interval 9000
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ネイバー送信要求の送信間隔を 9000 ミリ秒に設定します。

```
RP/0/(config)# dynamic-template type ppp p1
RP/0/(config-dynamic-template-type)# ipv6 nd ns-interval 9000
```

ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメントに **other stateful configuration** フラグを設定するには、適切なコンフィギュレーションモードで **ipv6 nd other-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

other stateful configuration フラグは、IPv6 ルータ アドバタイズメントで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 (BNG 以外に適用)

ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

other stateful configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレス以外のオートコンフィギュレーション情報を取得できるかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、その他 (アドレス以外) の情報の取得にステートフル オートコンフィギュレーションを使用します。



(注) **ipv6 nd managed-config-flag** コマンドを使用して **managed address configuration** フラグを設定すると、接続ホストは、**other stateful configuration** フラグの設定に関係なく、ステートフル オートコンフィギュレーションを使用してその他の情報 (アドレス以外の情報) を取得できます。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、**dynamic-template** コマンドを実行します。

タスク ID	タスク ID	動作
	ipv6	読み取り、書き込み
	network	読み取り、書き込み
	config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 で IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを設定します。

```
RP/0/(config)# interface HundredGigE0/1/0/1
RP/0/(config-if)# ipv6 nd other-config-flag
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを設定します。

```
RP/0/(config)# dynamic-template type ppp p1
RP/0/(config-dynamic-template-type)# ipv6 nd other-config-flag
```

ipv6 nd prefix

IPv6 ルータ アドバタイズメントで IPv6 プレフィックスがアドバタイズされる方法を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。デフォルトのパラメータ値でプレフィックスをアドバタイズするには、このコマンドの **no** 形式を使用します。1 つのプレフィックス（または複数のプレフィックス）がアドバタイズされないようにするには、**no-adv** キーワードを使用します。

```
ipv6 nd prefix {ipv6prefix/prefix-length} default [valid-lifetime | at| infinite| no-adv| no-autoconfig| off-link]}
no ipv6 nd prefix {ipv6prefix/prefix-length} default [valid-lifetime | at| infinite| no-adv| no-autoconfig| off-link]}
```

構文の説明

ipv6-prefix	ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。 このキーワードは、コロンの中で 16 ビット値を使用する 16 進数でアドレスが指定される、RFC 2373 で定義された形式でなければなりません。
/prefix-length	IPv6 プレフィックスの長さ。これは、プレフィックス（アドレスのネットワーク部）を構成するアドレスの上位隣接ビット数を示す 10 進数値です。10 進数値の前にスラッシュ記号 (/) を付ける必要があります。
default	(任意) すべてのプレフィックスを指定します。
valid-lifetime	(任意) 指定した IPv6 プレフィックスが有効なものとしてアドバタイズされる時間数 (秒)。値の範囲は 0 ~ 4294967295 秒です。
at	(任意) 有効期間および推奨期間が無効になる日時。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は、 <i>date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire</i> の形式で表記されます。
infinite	(任意) 有効なライフタイムは期限切れになりません。
no-adv	(任意) プレフィックスはアドバタイズされません。
no-autoconfig	(オプション) 指定されたプレフィックスを IPv6 自動設定に使用できないことを、ローカルリンク上のホストに示します。
off-link	(任意) 指定されたプレフィックスがリンクに割り当てられることを示します。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、 <i>onlink</i> 決定では使用されません。

コマンド デフォルト IPv6 ルータ アドバタイズメントを発信するインターフェイスに設定されているすべてのプレフィックスが、有効ライフタイム 2592000 秒（30 日）および優先ライフタイム 604800 秒（7 日）でアドバタイズされます。どちらのライフタイムにも「onlink」フラグと「autoconfig」フラグが設定されます。

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
リリース 6.0	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、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに個々のパラメータを制御できます。

プレフィックスのアドバタイズ方法を制御するには、**ipv6 nd prefix** コマンドを使用します。デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されたプレフィックスは、デフォルト値でアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメントのプレフィックスを設定した場合は、そのプレフィックスのみが設定した値でアドバタイズされます。他のすべてのプレフィックスはデフォルト値でアドバタイズされます。

デフォルトキーワードは、すべてのプレフィックスのデフォルトパラメータを設定するときに使用できます。

プレフィックスの有効期限を指定するための日付を設定できます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。失効日に達すると、プレフィックスはアドバタイズされなくなります。

onlink が「on」（デフォルト）である場合、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

autoconfig が「on」（デフォルト）である場合、ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用できることを示します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、HundredGigE インターフェイス 0/1/0/0 から送信されるルータ アドバタイズメントに、IPv6 プレフィックス 2001:0DB8::/35 を含めて、有効期間 1000 秒と推奨期間 900 秒を指定します。

```
RP/0/(config)# interface HundredGigE0/1/0/0
RP/0/(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

ipv6 nd ra-interval

インターフェイスでの IPv6 ルータ アドバタイズメントの送信間隔を設定するには、適切なコンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval *seconds*

構文の説明

<i>seconds</i>	IPv6 ルータ アドバタイズメント送信間隔 (秒)
----------------	----------------------------

コマンド デフォルト

seconds : 200 秒

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 (BNG 以外に適用)
ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv6 nd ra-lifetime コマンドによりルータがデフォルトルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントの有効期間以下でなければなりません。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20% 以内でランダムに調整します。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

タスク ID	動作
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 に IPv6 ルータのアドバタイズメント間隔として 201 秒を設定します。

```
RP/0/(config)# interface HundredGigE0/1/0/1  
RP/0/(config-if)# ipv6 nd ra-interval 201
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ルータのアドバタイズメント間隔を 201 秒に設定します。

```
RP/0/(config)# dynamic-template type ppp p1  
RP/0/(config-dynamic-template-type)# ipv6 nd ra-interval 201
```

ipv6 nd ra-lifetime

インターフェイスでの IPv6 ルータ アドバタイズメントのルータ有効期間値を設定するには、適切なコンフィギュレーションモードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルトの有効期間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime seconds

no ipv6 nd ra-lifetime

構文の説明

<i>seconds</i>	このインターフェイスでのデフォルト ルータとしてのルータの有効期間 (秒)
----------------	---------------------------------------

コマンド デフォルト

seconds : 1800 秒

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 (BNG 以外に適用)
ダイナミック テンプレート コンフィギュレーション (BNG 向け)

使用上のガイドライン

ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイスでのデフォルトルータとしてルータの有用性を示します。値を 0 に設定すると、ルータは、このインターフェイスでデフォルトルータとは見なされません。ルータがこのインターフェイスでデフォルトルータと見なされるようにするには、ルータの有効期間の値にゼロ以外の値を設定します。ルータの有効期間の値として設定するゼロ以外の値は、ルータ アドバタイズメント間隔以上でなければなりません。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーションモードで実行してください。ダイナミック テンプレート コンフィギュレーションモードを開始するには、で **dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 に IPv6 ルータのアドバタイズメント有効期間として 1801 秒を定めます。

```
RP/0/(config)# interface HundredGigE0/1/0/1
RP/0/(config-if)# ipv6 nd ra-lifetime 1801
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ルータのアドバタイズメント有効期間を 1801 秒に設定します。

```
RP/0/(config)# dynamic-template type ppp p1
RP/0/(config-dynamic-template-type)# ipv6 nd ra-lifetime 1801
```

ipv6 nd reachable-time

何らかの到達可能性確認イベントが発生してからリモート IPv6 ノードが到達可能と見なされるまでの時間を設定するには、適切なコンフィギュレーションモードで **ipv6 nd reachable-time** コマンドを使用します。デフォルト値に戻す場合は、このコマンドの **no** 形式を入力します。

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

構文の説明

milliseconds リモート IPv6 ノードが到達可能と見なされる時間（ミリ秒）。範囲は 0 ～ 3600000 です。

コマンド デフォルト

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 30000（30 秒）は、ルータ自体のネイバー探索アクティビティに使用されます。

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（BNG 以外に適用）

ダイナミック テンプレート コンフィギュレーション（BNG 向け）

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

設定時間により、ルータは、利用不可隣接を検出できます。設定時間を短くすると、ルータは、より速く利用不可隣接を検出できます。ただし、設定時間を短くすると、すべての IPv6 ネットワーク デバイスで消費される IPv6 ネットワーク 帯域幅および処理リソースが多くなります。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

設定時間は、インターフェイスから送信されるすべてのルータ アドバタイズメントに含まれるため、同じリンクのノードは同じ時間値を共有します。値に 0 を設定すると、設定時間がこのルータで指定されていないことを示します。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、で **dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 に IPv6 到達可能時間として 1,700,000 ミリ秒を設定します。

```
RP/0/(config)# interface HundredGigE0/1/0/1
RP/0/(config-if)# ipv6 nd reachable-time 1700000
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 到達可能時間を 1,700,000 ミリ秒に設定します。

```
RP/0/(config)# dynamic-template type ppp p1
RP/0/(config-dynamic-template-type)# ipv6 nd reachable-time 1700000
```

ipv6 nd redirects

インターネット制御メッセージプロトコル (ICMP) リダイレクトメッセージを送信するには、インターフェイス コンフィギュレーション モードで **ipv6 nd redirects** コマンドを使用します。システム デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd redirects

no ipv6 nd redirects

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルト値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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、HundredGigE インターフェイス 0/2/0/2 に IPv6 nd ダイレクトブロードキャストをリダイレクトする方法を示しています。

```
RP/0/(config)# interface HundredGigE0/2/0/2
RP/0/(config-if)# ipv6 nd redirects
```

ipv6 nd scavenge-timeout

ネイバー エントリの有効期間を `stale` 状態に設定するには、で `ipv6 nd scavenge-timeout` 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。

ipv6 nd scavenge-timeout *seconds*

no ipv6 nd scavenge-timeout *seconds*

構文の説明

`seconds` RA の有効期間（秒単位）。範囲は 0 ～ 43200 です。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

隣接エントリの廃棄タイマーの有効期間が切れると、そのエントリはクリアされます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次に、隣接エントリの有効期間を設定する例を示します。

```
RP/0/(config)# ipv6 nd scavenge-timeout 3000
```

ipv6 nd suppress-ra

LAN インターフェイスでの IPv6 ルータ アドバタイズメントの送信を抑制するには、適切なコンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスでの IPv6 ルータ アドバタイズメントの送信を再び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。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IPv6 ルータ アドバタイズメントは、IPv6 ユニキャストルーティングが他のタイプのインターフェイスでイネーブルになっている場合、そのインターフェイスで自動的に送信されます。IPv6 ルータ アドバタイズメントは、他のタイプのインターフェイスで送信されません。

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 (BNG 以外に適用)

ダイナミック テンプレート コンフィギュレーション (BNG 向け)

コマンド履歴

リリース	変更内容
リリース 6.0	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 ipv6 nd suppress-ra コマンドを使用すると、LAN 以外のインターフェイス タイプ (シリアル インターフェイス、トンネル インターフェイスなど) における IPv6 ルータ アドバタイズメントの送信をイネーブルにできます。

BNG の場合は、このコマンドを必ずダイナミック テンプレート コンフィギュレーション モードで実行してください。ダイナミック テンプレート コンフィギュレーション モードを開始するには、**dynamic-template** コマンドを実行します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

タスク ID	動作
config-services	読み取り、書き込み

例

次の例（BNG 以外に該当）は、HundredGigE インターフェイス 0/1/0/1 での IPv6 ルータ アドバタイズメントを抑制する方法を示しています。

```
RP/0/(config)# interface HundredGigE0/1/0/1  
RP/0/(config-if)# ipv6 nd suppress-ra
```

次の例（BNG に該当）は、ダイナミック テンプレート コンフィギュレーション モードで IPv6 ルータ アドバタイズメントを抑制する方法を示しています。

```
RP/0/(config)# dynamic-template type ppp p1  
RP/0/(config-dynamic-template-type)# ipv6 nd suppress-ra
```

ipv6 neighbor

IPv6 ネイバー探索キャッシュにスタティック エントリを設定するには、で **ipv6 neighbor** コマンドを使用します。IPv6 ネイバー探索キャッシュからスタティック IPv6 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。

ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-instance hardware-address*

構文の説明

<i>ipv6-address</i>	ローカル データリンク アドレスに対応する IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<i>interface-type</i>	インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。
<i>interface-instance</i>	次に示す、物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスのいずれかです。 <ul style="list-style-type: none"> • 物理インターフェイス インスタンス。名前表記は <i>rack/slot/module/port</i> です。値の間に表記の一部としてスラッシュが必要です。 <ul style="list-style-type: none"> ◦ <i>rack</i> : ラックのシャーシ番号。 ◦ <i>slot</i> : モジュラ サービスカードまたはラインカードの物理スロット番号。 ◦ <i>module</i> : モジュール番号。物理層インターフェイス モジュール (PLIM) は、常に 0 です。 ◦ <i>port</i> : インターフェイスの物理ポート番号。 (注) ルートプロセッサカード上の管理イーサネットインターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0 • 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。 <p>ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。</p>
<i>hardware-address</i>	ローカル データリンク アドレス (48 ビット アドレス) 。
コマンド デフォルト	スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **ipv6 neighbor** コマンドは、**arp** (グローバル) コマンドに似ています。

IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されません。

show ipv6 neighbors コマンドを使用すると、IPv6 ネイバー探索キャッシュのスタティック エントリを表示できます。IPv6 ネイバー探索キャッシュのスタティック エントリの状態は、**reach (reachable)** です。このエントリのインターフェイスはアップ状態です。エントリのインターフェイスがダウンしている場合は、**show ipv6 neighbors** コマンドを使用しても、このエントリは表示されません。



(注) 到達可能性検出は、IPv6 ネイバー探索キャッシュのスタティック エントリには適用されません。そのため、**reach (reachable)** 状態の説明は、ダイナミックおよびスタティック キャッシュ エントリで異なります。ダイナミック キャッシュ エントリの **reach (reachable)** ステータスについては、**show ipv6 neighbors** コマンドを参照してください。

clear ipv6 neighbors コマンドは、スタティック エントリを除き、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定されたスタティック エントリをネイバー探索キャッシュから削除します。IPv6 ネイバー探索プロセスで学習されたダイナミック エントリはキャッシュから削除されません。**no ipv6 enable** または **no ipv6 unnumbered** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除き、そのインターフェイスに設定されているすべての IPv6 ネイバー探索キャッシュ エントリが削除されます (エントリのステータスは **reach [reachable]** に変化します)。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。



(注) IPv6 隣接のスタティック エントリは、IPv6 がイネーブルにされている LAN および ATM LAN Emulation インターフェイスだけで設定できます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、イーサネット インターフェイス 0/RSP0/CPU0 上に IPv6 アドレス 2001:0DB8::45A とリンク層アドレス 0002.7D1A.9472 を持つネイバーに対して、IPv6 ネイバー探索キャッシュにスタティック エントリを設定する方法を示しています。

```
RP/0/(config)# ipv6 neighbor 2001:0DB8::45A 0002.7D1A.9472
```

ipv6 path-mtu enable

IPv6 パケットのパス最大伝送ユニット (MTU) ディスカバリを設定するコマンドをイネーブルにするには、XR コンフィギュレーション モードで **ipv6 path-mtu enable** コマンドを使用します。

ipv6 path-mtu enable

コマンド デフォルト

なし。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv6 パケットのパス MTU ディスカバリは、TCP と Ping プロトコルを使用しているアプリケーションでのみサポートされます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例は、IPv6 パケットのパス MTU ディスカバリ コマンドをイネーブルにする方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv6 path-mtu enable
```

ipv6 path-mtu timeout

IPv6 パケットの最大伝送ユニット (MTU) タイムアウト値を設定するには、XR コンフィギュレーション モードで **ipv6 path-mtu timeout** コマンドを使用します。

ipv6 path-mtu timeout *minutes*

構文の説明

minutes MTU タイムアウト (分単位)。範囲は 1 ~ 15 分です。デフォルトのタイムアウト値は 10 分です。

コマンド デフォルト

なし。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv6 パケットのパス MTU ディスカバリーは、TCP と Ping プロトコルを使用しているアプリケーションでのみサポートされます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例

次の例は、IPv6 パケットのパス MTU タイムアウトをイネーブルにする方法を示しています。

```
RP/0/RP0/CPU0:router(config)# ipv6 path-mtu timeout 15
```

ipv6 source-route

IPv6 タイプ (タイプ 0) の送信元ルーティングヘッダーの処理をイネーブルにするには、で **ipv6 source-route** コマンドを使用します。IPv6 拡張ヘッダーの処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 source-route

no ipv6 source-route

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトは、**ipv6 source-route** コマンドの **no** バージョンです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 ipv6 source-route コマンド (デフォルト) は、ホストがルータを使用して送信元ルーティングを実行しないようにします。**no ipv6 source-route** コマンドが設定されている場合に、ルータがタイプ 0 の送信元ルーティングヘッダーを持つパケットを受信すると、ルータはそのパケットをドロップして、送信元に IPv6 ICMP エラーメッセージを返信し、適切なデバッグメッセージを記録します。

タスク ID

タスク ID	動作
network	読み取り、書き込み
ipv6	読み取り、書き込み

例

次に、source-route ヘッダー オプションを含むすべての IPv6 データグラムの処理を可能にする例を示します。

```
RP/0/# config
RP/0/(config)# ipv6 source-route
RP/0/(config)#
```

ipv6 tcp-mss-adjust

IPv6 パケットに対してセッションを確立するときにトラフィックのフラグメント化を回避するために、TCPフローの中継トラフィックの最大セグメントサイズ (MSS) を GRE トンネルインターフェイスまたは VLAN サブインターフェイスの MTU 未満に調整できるようにするには、インターフェイス コンフィギュレーション モードで **ipv6 tcp-mss-adjust** コマンドを使用します。TCP フローの中継トラフィックの最大セグメントサイズ (MSS) を GRE トンネルインターフェイスまたは VLAN サブインターフェイスの MTU 未満に調整できないようにするには、このコマンドの **no** 形式を使用します。

ipv6 tcp-mss-adjust enable

no ipv6 tcp-mss-adjust enable

構文の説明

enable	インターフェイスでTCPフローの最大セグメントサイズ (MSS) を調整できるようにします。
---------------	--

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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
mpls-te	読み取り、書き込み
ipv6	読み取り、書き込み

例

次の例は、**ipv6 tcp-mss-adjust** コマンドを使用して、IPv6 パケットの TCP フローの中継トラフィックをイネーブルにする方法を示しています。

```
RP/0/# configure
RP/0/(config)# interface HundredEthernet 0/0/0/4.20
RP/0/(config-if)# ipv6 tcp-mss-adjust enable
```

ipv6 virtual address

管理イーサネットインターフェイスのネットワークに対して IPv6 仮想アドレスを定義するには、**ipv6 virtual address** コマンドを使用します。設定から IPv6 仮想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。

ipv6 virtual address {[vrf vrf-name]ipv6-address/prefix-length| use-as-src-addr}

no ipv6 virtual address {[vrf vrf-name]ipv6-address/prefix-length| use-as-src-addr}

構文の説明

vrf vrf-name	(任意) 管理インターフェイスの VPN ルーティングおよび転送 (VRF) ごとに仮想アドレスを設定します。vrf-name 引数には VRF の名前を指定します。
ipv6 address	使用する仮想 IPv6 アドレス。
prefix-length	IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
use-as-src-addr	送信されたパケットのデフォルト SRC アドレスとして使用される仮想アドレスをイネーブルにします。

コマンド デフォルト

コンフィギュレーションに対して IPv6 仮想アドレスは定義されません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

IPv6 仮想アドレスを設定すると、管理ネットワークで単一の仮想アドレスからルータにアクセスできるようになります。IPv6 仮想アドレスは、ルートプロセッサ (RP) のフェールオーバーが発生しても維持されます。

IPv6 仮想アドレスを設定すると、アクティブな RP を事前に認識せずに、単一アドレスからデュアル RP ルータにアクセスできるようになります。IPv6 仮想アドレスは、RP フェールオーバー間

で維持されます。そのためには、仮想 IPv6 アドレスが共通 IPv6 サブネットを両方の RP の管理イーサネット インターフェイスと共有している必要があります。

vrf キーワードを指定して **ipv6 virtual address** コマンドをディセーブルにした場合は、対応する VRF またはデフォルト（VRF が指定されていない場合）に対して仮想 IP アドレスは設定されません。この結果、VRF テーブルおよび ARP キャッシュの仮想 IP アドレスのエントリが削除されます。

デフォルト VRF は、VRF が指定されていない場合に選択されます。仮想 IP アドレスは、デフォルト VRF に接続される管理インターフェイスでアクティブです。

use-as-src-addr キーワードを使用すると、管理アプリケーションの送信元インターフェイス（つまり、更新の送信元）として、ループバック インターフェイスを設定する必要がなくなります。更新送信元が設定されていない場合、管理アプリケーションによって転送プロセス（TCP、UDP、raw_ip）による適切な送信元アドレスの選択が許可されます。また、転送プロセスはこのために FIB を参照します。管理イーサネット IP アドレスが送信元アドレスとして指定されており、**use-as-src-addr keyword** が設定されている場合、転送プロセスは、関連する仮想 IP アドレスで管理イーサネット IP アドレスを置き換えます。この機能は、RP スイッチオーバー全体で機能します。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次の例は、IPv6 仮想アドレスの定義方法を示しています。

```
RP/0/(config)# ipv6 virtual address 0:0:0:7272::72/64
```

次の例は、VRF ごとに管理インターフェイスの仮想 IP アドレスを設定する方法を示しています。

```
RP/0/(config)# ipv6 virtual address vrf ppp 0:0:0:7272::72/64
```

show arm conflicts

Address Repository Manager (ARM) により識別される IPv4 または IPv6 のアドレス競合情報を表示するには、で **show arm conflicts** コマンドを使用します。

show arm {ipv4|ipv6} [vrf vrf-name] conflicts [address|override|unnumbered]

構文の説明

ipv4	IPv4 アドレス競合を表示します。
ipv6	IPv6 アドレス競合を表示します。
vrf	(任意) VPN ルーティング/転送 (VRF) インスタンス情報を表示します。IPv4 だけで使用できます。
<i>vrf-name</i>	(任意) VRF の名前。
address	(任意) アドレス競合情報を表示します。
override	(任意) アドレス競合上書き情報を表示します。
unnumbered	(任意) unnumbered インターフェイス競合情報を表示します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 arm conflicts コマンドを使用すると、IPv4 または IPv6 アドレス競合に関する情報を表示できます。アドレス競合情報を使用すると、誤って設定されている IPv4 または IPv6 アドレスを特定できます。

競合情報は、強制的にダウン状態にされているインターフェイス、およびアップ状態にあるインターフェイスに関して表示されます。

オプション キーワードを指定せずに **showarmconflicts** コマンドを発行すると、**address** と **unnumbered** の両方のキーワードから生成された出力が表示されます。

タスク ID

タスク ID	動作
network	読み取り

例

次の例は、**show arm ipv4 conflicts** コマンドの出力を示しています。

```
RP/0/# show arm ipv4 conflicts
F Forced down
| Down interface & addr
F Lo2 10.1.1.2/24
Forced down interface
tu2->tu1
Up interface & addr
Up interface
tu1->Lo1
Lo1 10.1.1.1/24
```

次の例は、**address** キーワードを指定した場合の **showarm ipv4conflicts** コマンドの出力を示しています。

```
RP/0/# show arm ipv4 conflicts address
F Forced down
| Down interface & addr
F Lo2 10.1.1.2/24
Up interface & addr
Up interface
Lo1 10.1.1.1/24
```

次の例は、**unnumbered** キーワードを指定した場合の **showarm ipv4conflicts** コマンドの出力を示しています。

```
RP/0/# show arm ipv4 conflicts unnumbered
Forced down interface
tu2->tu1
Up interface
tu1->Lo1
VRF
```

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 42 : **show arm conflicts** コマンドのフィールドの説明

フィールド	説明
Forced down	このコマンドの出力に表示される可能性のある記号を定義する凡例。
Down interface & addr	強制的にダウン状態にされているインターフェイスの名前、タイプ、アドレス。
Up interface & addr	アップ状態にあるインターフェイスのリスト。

フィールド	説明
Forced down interface	競合していて、強制的にダウン状態にされている unnumbered インターフェイス。
Up interface	競合していて、アップ状態にある unnumbered インターフェイス。

show arm registrations producers

Address Repository Manager (ARM) のプロデューサ登録情報を表示するには、で **show arm registrations producers** コマンドを使用します。

show arm {ipv4| ipv6} registrations producers

構文の説明

ipv4	IPv4 プロデューサ登録情報を表示します。
ipv6	IPv6 プロデューサ登録情報を表示します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 arm registrations producers コマンドを使用すると、IP ARM 登録のプロデューサに関する情報を表示できます。登録情報は、ID で表示されます。

タスク ID

タスク ID	動作
network	読み取り

例

次の例は、**show arm registrations producers** コマンドの出力を示しています。

```
RP/0/# show arm ipv4 registrations producers
Id      Node          Producer Id  IPC Version Connected?
0       0/0/0         ipv4_io      1.1         Y
4       0/1/0         ipv4_io      1.1         Y
3       0/2/0         ipv4_io      1.1         Y
```

show arm registrations producers

```

2      0/4/0      ipv4_io      1.1      Y
1      0/6/0      ipv4_io      1.1      Y

```

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 43 : show arm registrations producers コマンドのフィールドの説明

フィールド	説明
Id	IP アドレスのプロデューサを追跡するために IP アドレス ARM (IP ARM) により使用される ID。
Node	プロデューサが稼働する物理ノード (RP/LC CPU)。
Producer Id	IP ARM での登録時にプロデューサにより使用されるストリング。
IPC Version	IP ARM との通信のためにプロデューサにより使用される apis のバージョン。
Connected?	プロデューサが接続されているかどうかを示すステータス。

show arm router-ids

ルータ ID 情報と Address Repository Manager (ARM) の仮想ルーティングおよびフォワーディング テーブル情報を表示するには、で **show arm router-ids** コマンドを使用します。

show arm [ipv4] router-ids

構文の説明

ipv4 (任意) IPv4 ルータ情報を表示します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 キーワードを指定して **show arm router-ids** コマンドを使用すると、ルータの特定のルータ ID 情報を表示できます。

タスク ID

タスク ID	動作
network	読み取り

例

次の例は、**show arm router-ids** コマンドの出力を示しています。

```
RP/0/# show arm router-ids
Router-ID      Interface
10.10.10.10    Loopback0
```

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 44 : *show arm router-ids* コマンドのフィールドの説明

フィールド	説明
Router-ID	ルータ ID
Interface	インターフェイス ID

show arm summary

IP Address Repository Manager (ARM) のサマリー情報を表示するには、で **show arm summary** コマンドを使用します。

show arm {ipv4| ipv6} summary

構文の説明

ipv4	IPv4 サマリー情報を表示します。
ipv6	IPv6 サマリー情報を表示します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 arm summary コマンドを使用すると、ルータにおけるプロデューサ、アドレス競合、アンナバード インターフェイス競合の数がサマリー情報に表示されます。

タスク ID

タスク ID	動作
network	読み取り

例

次の例は、**show arm summary** コマンドの出力を示しています。

```
RP/0/# show arm ipv4 summary
```

```
IPv4 Producers           :    5
IPv4 Router id consumers :    7
IPv4 address conflicts   :    2
```

```
IPv4 unnumbered interface conflicts      :      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 45: *show arm summary* コマンドのフィールドの説明

フィールド	説明
IPv4 Producers	ルータの IPv4 プロデューサの数
IPv4 address conflicts	ルータの IPv4 アドレス競合の数
IPv4 unnumbered interface conflicts	unnumbered インターフェイスの IPv4 競合の数
Pv4 DB Master version	IPv4 DB のマスター バージョン

show ipv4 interface

IPv4 用に設定されたインターフェイスの使用可能性ステータスを表示するには、で **show ipv4 interface** コマンドを使用します。

show ipv4 interface [*type interface-path-id*] **brief** | **summary**]

構文の説明

type インターフェイス タイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用します。

interface-path-id 次に示す、物理インターフェイス インスタンスまたは仮想インターフェイス インスタンスのいずれかです。

- 物理インターフェイス インスタンス。名前表記は *rack/slot/module/port* です。値の間に表記の一部としてスラッシュが必要です。

- *rack* : ラックのシャーシ番号。

- *slot* : モジュール サービス カードまたはラインカードの物理スロット番号。

- *module* : モジュール番号。物理層インターフェイスモジュール (PLIM) は、常に 0 です。

- *port* : インターフェイスの物理ポート番号。

(注) ルート プロセッサ カード上の管理イーサネット インターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0

- 仮想インターフェイス インスタンス。数字の範囲は、インターフェイス タイプによって異なります。

ルータの構文の詳細については、疑問符 (?) を使用してオンライン ヘルプを参照してください。

brief (任意) ルータのインターフェイス、およびそのプロトコルとラインステートで設定されているプライマリ IPv4 アドレスを表示します。

summary (任意) ルータの割り当て済み、未割り当てまたは **unnumbered** のインターフェイス数。

コマンド デフォルト

VRF が指定されない場合、デフォルトの VRF が表示されます。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 ipv4 interface コマンドの出力は、IPv4 に固有である点を除き、**show ipv6 interface** コマンドの出力と似ています。

インターフェイスの名前は、名前が VRF インスタンスに属する場合だけ表示されます。*vrf-name* を指定しない場合、インターフェイスインスタンスは、インターフェイスがデフォルト VRF に属している場合にのみ表示されます。

タスク ID

タスク ID	動作
ipv4	読み取り
network	読み取り

例

次の例は、**show ipv4 interface** コマンドの出力を示しています。

```
RP/0/# show ipv4 interface

Loopback0 is Up, line protocol is Up
Internet address is 10.0.0.1/8

Secondary address 10.0.0.2/8
MTU is 1514 (1514 is available to IP)
Multicast reserved groups joined: 10.0.0.1
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
tenGigE/0/0/0/0 is Up, line protocol is Up
Internet address is 10.25.58.1/16
MTU is 1514 (1500 is available to IP)
Multicast reserved groups joined: 10.0.224.1
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
tenGigE/0/0/0/0 is Shutdown, line protocol is Down
Vrf is default (vrfid 0x60000000)
```

```
Internet protocol processing disabled
```

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 46 : `show ipv4 interface` コマンドのフィールドの説明

フィールド	説明
Loopback0 is Up	インターフェイスハードウェアが使用可能な場合は、インターフェイスのステータスが「Up」と表示されます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
line protocol is Up	インターフェイスが双方向通信を提供できる場合は、回線プロトコルのステータスが「Up」と表示されます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
Internet address	インターフェイスの IPv4 インターネットアドレスおよびサブネットマスク。
Secondary address	セカンダリアドレス（設定されている場合）を表示します。
MTU	インターフェイスに設定されている IPv4 MTU ⁸ の値が表示されます。
Multicast reserved groups joined	このインターフェイスが属するマルチキャストグループを示します。
Directed broadcast forwarding	ダイレクトブロードキャスト転送がイネーブルまたはディセーブルかを示します。
Outgoing access list	インターフェイスに発信アクセスリストが設定されているかどうかを示します。
Inbound access list	インターフェイスに着信アクセスリストが設定されているかどうかを示します。
Proxy ARP	プロキシ ARP ⁹ がインターフェイスでイネーブルかディセーブルかを示します。

show ipv4 interface

フィールド	説明
ICMP redirects	ICMPv4 ¹⁰ リダイレクトをこのインターフェイスに送信するかどうかを指定します。
ICMP unreachable	このインターフェイスで到達不能メッセージが送信されるかどうかを指定します。
Internet protocol processing disabled	インターフェイスで IPv4 アドレスが設定されていないことを示します。

⁸ MTU = 最大伝送ユニット

⁹ ARP = アドレス解決プロトコル

¹⁰ ICMPv4 = インターネット制御メッセージプロトコルバージョン 4

show ipv4 traffic

IPv4 トラフィックの統計情報を表示するには、で **show ipv4 traffic** コマンドを使用します。

show ipv4 traffic [brief]

構文の説明

brief (任意) IPv4 およびインターネット制御メッセージプロトコルバージョン 4 (ICMPv4) トラフィックだけを表示します。

コマンド デフォルト

なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

showipv4traffic コマンドの出力は、IPv4 に固有である点を除き、**showipv6traffic** コマンドの出力と似ています。

タスク ID

タスク ID	動作
ipv4	読み取り
network	読み取り

例

次の例は、**show ipv4 traffic** コマンドの出力を示しています。

```
RP/0/# show ipv4 traffic
IP statistics:
  Rcvd: 16372 total, 16372 local destination
        0 format errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
```

show ipv4 traffic

```

    0 security failures, 0 bad source, 0 bad header
    0 with options, 0 bad, 0 unknown
Opts: 0 end, 0 nop, 0 basic security, 0 extended security
      0 strict source rt, 0 loose source rt, 0 record rt
      0 stream ID, 0 timestamp, 0 alert, 0 cipso
Frgs: 0 reassembled, 0 timeouts, 0 couldn't reassemble
      0 fragmented, 0 fragment count
Bcast: 0 sent, 0 received
Mcast: 0 sent, 0 received
Drop: 0 encapsulation failed, 0 no route, 0 too big, 0 sanity address check
Sent: 16372 total

ICMP statistics:
Sent: 0 admin unreachable, 0 network unreachable
      0 host unreachable, 0 protocol unreachable
      0 port unreachable, 0 fragment unreachable
      0 time to live exceeded, 0 reassembly ttl exceeded
      5 echo request, 0 echo reply
      0 mask request, 0 mask reply
      0 parameter error, 0 redirects
      5 total
Rcvd: 0 admin unreachable, 0 network unreachable
      2 host unreachable, 0 protocol unreachable
      0 port unreachable, 0 fragment unreachable
      0 time to live exceeded, 0 reassembly ttl exceeded
      0 echo request, 5 echo reply
      0 mask request, 0 mask reply
      0 redirect, 0 parameter error
      0 source quench, 0 timestamp, 0 timestamp reply
      0 router advertisement, 0 router solicitation
      7 total, 0 checksum errors, 0 unknown

UDP statistics:
    16365 packets input, 16367 packets output
    0 checksum errors, 0 no port
    0 forwarded broadcasts

TCP statistics:
    0 packets input, 0 packets output
    0 checksum errors, 0 no port

```

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 47: show ipv4 traffic コマンドのフィールドの説明

フィールド	説明
bad hop count	TTL ¹¹ フィールドがゼロになったため、パケットが破棄されるときに発生します。
encapsulation failed	通常、ルータに ARP 要求エントリがないため、データグラムを送信しなかったことを示します。
format errors	不可能なインターネット ヘッダー長など、パケットフォーマットでの大きな間違いを示します。

フィールド	説明
IP statistics Rcvd total	ソフトウェアプレーンで受信されるローカル宛先およびその他のパケットの合計数を示します。ハードウェアで転送または廃棄される IP パケットは考慮されません。
no route	ルーティング方法が不明なデータグラムを Cisco IOS XR ソフトウェアが破棄するときにカウントされます。

¹¹ TTL = 存続可能時間

show ipv6 interface

IPv6 用に設定されたインターフェイスの使用可能性ステータスを表示するには、で **show ipv6 interface** コマンドを使用します。

show ipv6 interface [**summary**] [*type interface-path-id*][**brief**][**link-local** **global**]]]

構文の説明

type (任意) インターフェイスタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。

interface-path-id (任意) 次のような物理インターフェイスインスタンスまたは仮想インターフェイスインスタンスです。

- 物理インターフェイス インスタンス。名前表記は *rack/slot/module/port* です。値の間に表記の一部としてスラッシュが必要です。
 - *rack* : ラックのシャーシ番号。
 - *slot* : モジュラ サービス カードまたはラインカードの物理スロット番号。
 - *module* : モジュール番号。物理層インターフェイスモジュール (PLIM) は、常に 0 です。
 - *port* : インターフェイスの物理ポート番号。

(注) ルートプロセッサカード上の管理イーサネットインターフェイスを参照する場合、物理スロット番号は英数字 (RSP0) であり、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0

- 仮想インターフェイス インスタンス。数字の範囲は、インターフェイスタイプによって異なります。

ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

brief (任意) ルータ インターフェイス、およびそのプロトコルとラインステートで設定されているプライマリ IPv6 アドレスを表示します。

link-local (任意) リンク ローカル IPv6 アドレスを表示します。

global (任意) グローバル IPv6 アドレスを表示します。

summary (任意) ルータの割り当て済み、未割り当てまたは unnumbered のインターフェイス数。

コマンド デフォルト なし

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 ipv6 interface` コマンドの出力は、IPv6 に固有である点を除き、`show ipv4 interface` コマンドの出力と似ています。

リンク ローカルまたはグローバル IPv6 アドレスを表示するには、`brief` キーワードとともに `link-local` または `global` キーワードを使用します。

タスク ID

タスク ID	動作
ipv6	読み取り

例

次の例は、`show ipv6 interface` コマンドの出力を示しています。

```
RP/0/# show ipv6 interface

TenGigE0/0/0/0 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:9324
Global unicast address(es):
  200::1, subnet is 200::/64
Joined group address(es): ff02::1:ff00:1 ff02::1:ffa6:9324 ff02::2
  ff02::1
MTU is 1514 (1500 is available to IPv6)
ICMP redirects are disabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND cache entry limit is 1000000000
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 160 to 240 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Outgoing access list is not set
Inbound common access list is not set, access list is not set
Table Id is 0xe0800000
Complete protocol adjacency: 2
Complete glean adjacency: 0
Incomplete protocol adjacency: 0
```

show ipv6 interface

```
Incomplete glean adjacency: 0
Dropped protocol request: 0
```

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 48 : *show ipv6 interface* コマンドのフィールドの説明

フィールド	説明
tenGigE0/0/0/2 is Up	インターフェイスハードウェアが現在アクティブかどうか（回線信号が存在するかどうか）、およびそれが管理者によりダウン状態にされているかどうかを示します。インターフェイスハードウェアが使用可能な場合は、インターフェイスのステータスが「Up」と表示されます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
line protocol is Up (または down)	回線プロトコルを扱うソフトウェアプロセスが回線を使用可能と見なしているかどうか（つまり、キープアライブが成功しているかどうか）を示します。インターフェイスが双方向通信を提供できる場合は、回線プロトコルのステータスが「Up」と表示されます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
IPv6 is enabled, stalled, disabled (出力例には stalled と disabled は表示されていません)	IPv6 がインターフェイスでイネーブル、ストールまたはディセーブルかを示します。IPv6 がイネーブルになっている場合は、インターフェイスのステータスが「enabled」と表示されます。重複アドレス検出でインターフェイスのリンクローカルアドレスが重複していると特定された場合は、そのインターフェイスでの IPv6 パケットの処理がディセーブルになり、インターフェイスのステータスが「stalled」になります。IPv6 がイネーブルになっていない場合は、インターフェイスのステータスが「disabled」と表示されます。
link-local address	インターフェイスに割り当てられているリンクローカルアドレスを表示します。

フィールド	説明
TENTATIVE	<p>重複アドレス検出に関連するアドレスの状態。状態は次のいずれかです。</p> <ul style="list-style-type: none"> • duplicate : アドレスが一意ではなく、使用されていません。重複アドレスが、インターフェイスのリンクローカルアドレスの場合、IPv6 パケットの処理は、そのインターフェイスでディセーブルになります。 • tentative : 重複アドレス検出が、このインターフェイスで保留中か実行中です。 <p>(注) アドレスがこれらのいずれの状態でもない (アドレスの状態がブランク) 場合、アドレスは一意で、使用中です。</p>
Global unicast addresses	インターフェイスに割り当てられているグローバルユニキャストアドレスを表示します。
ICMP redirects	インターフェイスでのインターネット制御メッセージプロトコル (ICMP) IPv6 リダイレクトメッセージの状態 (メッセージの送信かイネーブルかディセーブルか)。
ND DAD	インターフェイスでの重複アドレス検出の状態 (イネーブルまたはディセーブル)。
number of DAD attempts	重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数。
ND reachable time	このインターフェイスに割り当てられているネイバー探索到達可能時間 (ミリ秒) を表示します。

例 次の例は、**show ipv6 interface brief link-local** コマンドの出力を示しています。

```
RP/0/#show ipv6 interface brief link-local
```

```
Interface                IPv6-Address                Status      Protocol
tenGigE0/0/0/0          fe80::fe:8ff:feeb:26c5      Up          Up
tenGigE0/0/0/1          fe80::4f:88ff:fea0:8c9d      Up          Up
tenGigE0/0/0/3          unassigned                  Shutdown    Down
tenGigE0/0/0/4          unassigned                  Shutdown    Down
```

show ipv6 interface

次の例は、**show ipv6 interface brief global** コマンドの出力を示しています。

```
RP/0/#show ipv6 interface brief global
```

Interface	IPv6-Address	Status	Protocol
tenGigE0/0/0/0	2001:db8::1	Up	Up
tenGigE0/0/0/1	2001:db8::2	Up	Up
tenGigE0/0/0/3	unassigned	Shutdown	Down
tenGigE0/0/0/4	unassigned	Shutdown	Down

次の例は、**show ipv6 interface type interface-path-id brief link-local** コマンドの出力を示しています。

```
RP/0/#show ipv6 interface tenGigE 0/0/0/0 brief link-local
```

Interface	IPv6-Address	Status	Protocol
tenGigE0/0/0/0	fe80::fe:8ff:feeb:26c5	Up	Up

次の例は、**show ipv6 interface type interface-path-id brief global** コマンドの出力を示しています。

```
RP/0/#show ipv6 interface tenGigE 0/0/0/0 brief global
```

Interface	IPv6-Address	Status	Protocol
tenGigE0/0/0/0	2001:db8::1	Up	Up

show ipv6 neighbors

IPv6 ネイバー探索キャッシュ情報を表示するには、で **show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbors [*type interface-path-id*] **location node-id**

構文の説明

<i>type</i>	(任意) インターフェイス タイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用します。
<i>interface-path-id</i>	(任意) 物理インターフェイスインスタンスまたは仮想インターフェイス。 (注) ルータに現在設定されているすべてのインターフェイスのリストを表示するには、 show interfaces コマンドを使用します。 ルータの構文の詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。
location <i>node-id</i>	(任意) ノードを指定します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

すべての IPv6 ネイバー探索キャッシュ情報が表示されます。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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-type と *interface-number* 引数が指定されていない場合は、すべての IPv6 ネイバーのキャッシュ情報が表示されます。*interface-type* と *interface-number* 引数を指定すると、特定のインターフェイスのキャッシュ情報だけが表示されます。

タスク ID

タスク ID	動作
ipv6	読み取り

例

次の例は、IPv6 アドレスを指定した場合の **show ipv6 neighbors** コマンドの出力を示しています。

```
RP/0/# show ipv6 neighbors 2000:0:0:4::2

IPv6 Address          Age Link-layer Addr State Interface
Location
2000::2                166 6c9c.ed28.8b74 REACH Te0/0/0/0
0/RP0/CPU0
fe80::6e9c:edff:fe28:8b74 164 6c9c.ed28.8b74 REACH Te0/0/0/0
0/RP0/CPU0
[Mcast adjacency]      - 0000.0000.0000 REACH Te0/0/0/0
0/RP0/CPU0
[Mcast adjacency]      - 0000.0000.0000 REACH Te0/0/0/4
0/RP0/CPU0
```

次の例は、ロケーションを指定した場合の **show ipv6 neighbors** コマンドの出力を示しています。

```
RP/0/# show ipv6 neighbors location 0/2/CPU0

IPv6 Address      Age Link-layer Addr State Interface      Location
2001:3::2         119 0013.9400.0002 REACH BE3             0/2/CPU0
2001:3::3         179 0013.9400.0003 DELAY BE3             0/2/CPU0
2001:3::4         166 0013.9400.0004 REACH BE3             0/2/CPU0
2001:3::5         78  0013.9400.0005 REACH BE3             0/2/CPU0
2001:3::6         19  0013.9400.0006 REACH BE3             0/2/CPU0
2001:3::7         173 0013.9400.0007 REACH BE3             0/2/CPU0
2001:3::8         140 0013.9400.0008 REACH BE3             0/2/CPU0
2001:3::9         163 0013.9400.0009 REACH BE3             0/2/CPU0
2001:3::a         40  0013.9400.000a REACH BE3             0/2/CPU0
2001:3::b         90  0013.9400.000b REACH BE3             0/2/CPU0
2001:3::c         35  0013.9400.000c REACH BE3             0/2/CPU0
2001:3::d         114 0013.9400.000d REACH BE3             0/2/CPU0
2001:3::e         117 0013.9400.000e REACH BE3             0/2/CPU0
2001:3::f         157 0013.9400.000f REACH BE3             0/2/CPU0
2001:3::10        9   0013.9400.0010 REACH BE3             0/2/CPU0
2001:3::11        120 0013.9400.0011 REACH BE3             0/2/CPU0
2001:3::12        87  0013.9400.0012 REACH BE3             0/2/CPU0
2001:3::13        180 0013.9400.0013 DELAY BE3             0/2/CPU0
2001:3::14        103 0013.9400.0014 REACH BE3             0/2/CPU0
2001:3::15        132 0013.9400.0015 REACH BE3             0/2/CPU0
2001:3::16        33  0013.9400.0016 REACH BE3             0/2/CPU0
2001:3::17        150 0013.9400.0017 REACH BE3             0/2/CPU0
2001:3::18        117 0013.9400.0018 REACH BE3             0/2/CPU0
2001:3::19        48  0013.9400.0019 REACH BE3             0/2/CPU0
2001:3::1a        67  0013.9400.001a REACH BE3             0/2/CPU0
2001:3::1b        91  0013.9400.001b REACH BE3             0/2/CPU0
2001:3::1c        33  0013.9400.001c REACH BE3             0/2/CPU0
2001:3::1d        174 0013.9400.001d DELAY BE3             0/2/CPU0
2001:3::1e        144 0013.9400.001e REACH BE3             0/2/CPU0
2001:3::1f        121 0013.9400.001f REACH BE3             0/2/CPU0
2001:3::20        53  0013.9400.0020 REACH BE3             0/2/CPU0
```

次の表に、この出力で表示される重要フィールドの説明を示します。

表 49 : **show ipv6 neighbors** コマンドのフィールドの説明

フィールド	説明
IPv6 Address	隣接またはインターフェイスの IPv6 アドレス。

フィールド	説明
Age	アドレスが到達可能と確認されてから経過した時間 (分)。ハイフン (-) はスタティック エントリを示します。
Link-layer Addr	MAC アドレス。アドレスが不明の場合、ハイフン (-) が表示されます。

show ipv6 neighbors

フィールド	説明
State	

フィールド	説明
	<p>隣接キャッシュエントリの状態。IPv6 ネイバー探索キャッシュのダイナミック エントリのステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • INCMP (incomplete) : アドレス解決がエントリで実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノードマルチキャストアドレスに送信されましたが、対応するネイバーアドバタイズメントメッセージが受信されていません。 • reach (reachable) : 隣接への転送パスが正しく機能していたことを示す確認が、最後の ReachableTime ミリ秒内に受信されました。reach 状態の場合、デバイスは、パケット送信時に特別な処理を行いません。 • stale : 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。stale 状態にある場合、デバイスは、パケットが送信されるまで処理は行いません。 • delay : 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。到達可能性確認が、delay 状態になってから DELAY_FIRST_PROBE_TIME 秒以内に受信されない場合、ネイバー送信要求メッセージを送信して、状態を probe に変更します。 • probe : 到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとに、ネイバー送信要求メッセージを再送信することで、到達可能性確認が積極的に求められます。 <p>IPv6 ネイバー探索キャッシュのスタティック エントリの可能なステータスは、次のとおりです。</p> <ul style="list-style-type: none"> • reach (reachable) : このエントリのインター

フィールド	説明
	<p>フェイスはアップ状態です。</p> <ul style="list-style-type: none">• INCMP (incomplete) : このエントリのインターフェイスはダウン状態です。 <p>(注) 到達可能性検出は、IPv6 ネイバー探索キャッシュのスタティック エントリには適用されません。そのため、INCMP (incomplete) および reach (reachable) 状態の説明は、ダイナミックおよびスタティック キャッシュ エントリで異なります。</p>
Interface	アドレスに到達可能なインターフェイス。

show ipv6 neighbors summary

ネイバー エントリの要約情報を表示するには、`show ipv6 neighbors summary` コマンドを使用します。

show ipv6 neighbors summary

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルト値はディセーブルです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
ipv6	読み取り

例

次の `show ipv6 neighbors summary` コマンドの出力例は、ネイバー エントリのサマリー情報を示しています。

```
RP/0/# show ipv6 neighbors summary

Mcast nbr entries:
  Subtotal: 0
Static nbr entries:
  Subtotal: 0
Dynamic nbr entries:
  Subtotal: 0

Total nbr entries: 0
```

show ipv6 path-mtu

IPv6 パケットの最大伝送ユニット (MTU) の詳細を表示するには、XR コンフィギュレーション モードで **show ipv6 path-mtu** コマンドを使用します。

```
show ipv6 path-mtu [ vrf { vrf-name | all } ] [ locationnode-id ] [ locationnode-id ]
```

構文の説明

locationnode-id (任意) 指定されたノード。node-id 引数はラック/スロット/モジュールの形式で入力します。

コマンド デフォルト

なし。

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

location オプションを指定した場合は、**locationnode-id** キーワードと引数で指定したノードの詳細だけが表示されます。IPv6 パケットのパス MTU ディスカバリは、TCP と Ping プロトコルを使用しているアプリケーションでのみサポートされます。

タスク ID

タスク ID	動作
ipv6	読み取り、書き込み
network	読み取り、書き込み
config-services	読み取り、書き込み

例 次の例は、IPv6 パケットのパス MTU の詳細を表示する方法を示しています。

```
RP/0/RP0/CPU0:router(config)# show ipv6 pmtu
```

Destination	Ifhandle	Vrfid	Path Mtu	Time Left
bb::1	0x300	0x60000000	1300	00:01:27
cd::1	0x300	0x60000000	1300	00:01:42

show ipv6 traffic

IPv6 トラフィックの統計情報を表示するには、で **show traffic** コマンドを使用します。

show ipv6 traffic [brief]

構文の説明

brief (任意) IPv6 およびインターネット制御メッセージプロトコルバージョン 6 (ICMPv6) トラフィック統計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

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

showipv6traffic コマンドの出力は、IPv6 に固有である点を除き、**showipv4traffic** コマンドの出力と似ています。

タスク ID

タスク ID	動作
ipv6	読み取り
network	読み取り

例

次の例は、**show ipv6 traffic** コマンドの出力を示しています。

```
RP/0/# show ipv6 traffic

IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
```

```

    0 bad header, 0 unknown option, 0 bad source
    0 unknown protocol
    0 fragments, 0 total reassembled
    0 reassembly timeouts, 0 reassembly failures
    0 reassembly max drop
    0 sanity address check drops
Sent: 0 generated, 0 forwarded
      0 fragmented into 0 fragments, 0 failed
      0 no route, 0 too big
Mcast: 0 received, 0 sent

ICMP statistics:
Rcvd: 0 input, 0 checksum errors, 0 too short
      0 unknown error type
      unreachable: 0 routing, 0 admin, 0 neighbor,
                  0 address, 0 port, 0 unknown
      parameter: 0 error, 0 header, 0 option,
                 0 unknown
      0 hopcount expired, 0 reassembly timeout,
      0 unknown timeout, 0 too big,
      0 echo request, 0 echo reply
Sent: 0 output, 0 rate-limited
      unreachable: 0 routing, 0 admin, 0 neighbor,
                  0 address, 0 port, 0 unknown
      parameter: 0 error, 0 header, 0 option
                 0 unknown
      0 hopcount expired, 0 reassembly timeout,
      0 unknown timeout, 0 too big,
      0 echo request, 0 echo reply

Neighbor Discovery ICMP statistics:
Rcvd: 0 router solicit, 0 router advert, 0 redirect
      0 neighbor solicit, 0 neighbor advert
Sent: 0 router solicit, 0 router advert, 0 redirect
      0 neighbor solicit, 0 neighbor advert

UDP statistics:
    0 packets input, 0 checksum errors
    0 length errors, 0 no port, 0 dropped
    0 packets output

TCP statistics:s
    0 packets input, 0 checksum errors, 0 dropped
    0 packets output, 0 retransmitted

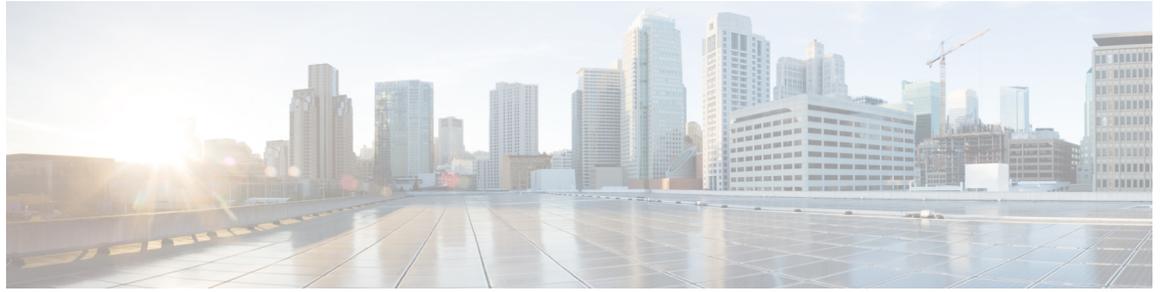
```

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 50 : show ipv6 traffic コマンドのフィールドの説明

フィールド	説明
Rcvd:	この項の統計情報は、ルータにより受信されたパケットについての情報です。
total	ソフトウェアにより受信されたパケットの合計数。
local destination	ローカルに送信され、ソフトウェアにより受信されたパケットの合計数。
source-routed	RHでソフトウェアにより参照されるパケット。

フィールド	説明
truncated	ソフトウェアにより参照される、切り捨てられたパケット。
bad header	通常の HBH、RH、DH または HA でエラーが検出されました。ソフトウェア限定。
unknown option	IPv6 ヘッダーの不明なオプションタイプ。
unknown protocol	受信されたパケットの IP ヘッダーで指定されているプロトコルが到達不能です。
Sent:	この項の統計情報は、ルータにより送信されたパケットについての情報です。
forwarded	ソフトウェアにより送信されたパケット。パケットが最初のルックアップで転送できない場合（たとえば、パケットでオプション処理が必要な場合）、ソフトウェアにより転送された場合でも、パケットはこのカウントに含まれません。
Mcast:	マルチキャストパケット。
ICMP statistics:	インターネット制御メッセージプロトコルの統計情報。



プレフィックス リスト コマンド

この章では、NCS 5000 で IP バージョン 4 (IPv4) や IP バージョン 6 (IPv6) のプレフィックス リストを設定する際に使用する Cisco IOS XR ソフトウェアのコマンドについて説明します。

プレフィックスリストの概念、設定作業、例に関する詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [clear prefix-list ipv4](#), 372 ページ
- [copy prefix-list ipv4](#), 374 ページ
- [deny \(プレフィックス リスト\)](#), 376 ページ
- [ipv4 prefix-list](#), 379 ページ
- [permit \(プレフィックス リスト\)](#), 381 ページ
- [remark \(プレフィックス リスト\)](#), 384 ページ
- [resequence prefix-list ipv4](#), 386 ページ
- [show prefix-list afi-all](#), 388 ページ
- [show prefix-list](#), 389 ページ
- [show prefix-list ipv4](#), 390 ページ
- [show prefix-list ipv4 standby](#), 392 ページ

clear prefix-list ipv4

IP Version 4 (IPv4) プレフィックスリストのヒットカウントをリセットするには、**clear prefix-list ipv4** コマンドを使用します。

clear prefix-list ipv4 *name* [*sequence-number*]

構文の説明

<i>name</i>	ヒットカウントをクリアするプレフィックスリストの名前。
<i>sequence-number</i>	(任意) プレフィックスリストのシーケンス番号。範囲は 1 ～ 2147483646 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ヒットカウントは、特定のプレフィックスリスト エントリに一致する数を示す値です。特定の設定済みプレフィックスリストのカウンタをクリアするには、**clear prefix-list ipv4** コマンドを使用します。

特定のシーケンス番号を持つプレフィックスリストのカウンタをクリアするには、*sequence-number* 引数を使用します。

タスク ID

タスク ID	動作
acl	読み取り、書き込み

例

次に、IPv4 プレフィックスリストを表示し、list3 のカウンタをクリアする例を示します。その後、IPv4 プレフィックスリストを再度表示して、list3 のカウンタがクリアされていることを確認します。

```
RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
ipv4 prefix-list list3
 30 permit 172.19.31.154/16 (32 matches)

RP/0/# clear prefix-list ipv4 list3

RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.18.30.154/16 (8 matches)
ipv4 prefix-list list2
 20 deny 172.24.30.164/16 (12 matches)
ipv4 prefix-list list3
 30 permit 172.19.31.154/16
```

copy prefix-list ipv4

既存の IP バージョン 4 (IPv4) プレフィックスリストのコピーを作成するには、で **copy prefix-list ipv4** コマンドを使用します。

copy prefix-list ipv4 *source-name destination-name*

構文の説明

<i>source-name</i>	コピー対象のプレフィックス リストの名前。
<i>destination-name</i>	<i>source-name</i> の内容のコピー先のプレフィックス リスト。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

設定済みプレフィックス リストをコピーするには、**copy prefix-list ipv4** コマンドを使用します。*source-name* 引数を使用してコピー元のプレフィックス リストを指定し、*destination-name* 引数を使用して、ソースプレフィックス リストの内容のコピー先を指定できます。*destination-name* 引数は一意の名前でなければなりません。プレフィックス リストまたはアクセス リストを示す *destination-name* 引数名が存在する場合、そのプレフィックス リストはコピーされません。**copy prefix-list ipv4** コマンドは、送信元プレフィックス リストが存在することをチェックしてから既存のリスト名をチェックし、既存のプレフィックス リストが上書きされないようにします。

タスク ID

タスク ID	動作
acl	読み取り、書き込み
filesystem	実行

例

次に、IPv4プレフィックスリストを表示し、プレフィックスリスト list1 を list4 にコピーし、IPv4プレフィックスリストを再表示して list4 を表示する例を示します。

```
RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16

RP/0/# copy prefix-list ipv4 list1 list4

RP/0/# show prefix-list ipv4
ipv4 prefix-list list1
 10 permit 172.24.20.164/16
ipv4 prefix-list list2
 20 deny 172.18.30.154/16
ipv4 prefix-list list3
 30 permit 172.29.30.154/16
ipv4 prefix-list list4
 10 permit 172.24.20.164/16
```

deny (プレフィックスリスト)

IP バージョン 4 (IPv4) プレフィックスリストの拒否条件を設定するには、IPv4 プレフィックスリスト コンフィギュレーションモードで **deny** コマンドを使用します。プレフィックスリストから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。

```
[sequence-number] deny network/length [ge value] [le value] [eq value]
```

```
no sequence-number deny
```

構文の説明

<i>sequence-number</i>	(任意) 特定のシーケンス番号を持つプレフィックスリストに対し拒否条件を設定します。シーケンス番号を使用しない場合、デフォルトではプレフィックスリスト中の次に空いているシーケンス番号で条件が設定されます。範囲は 1 ~ 2147483646 です。デフォルトでは、最初のステートメントが番号 10 で、以降のステートメントは 10 ずつ増分されます。 sequence-number 引数は、コマンドの no 形式で使用する必要があります。
<i>network/length</i>	ネットワーク マスクのネットワーク番号と長さ (ビット単位)。
<i>gevalue</i>	(任意) 値に等しいかそれよりも長いプレフィックス長を指定します。これは <i>length</i> の範囲の最小値です (長さ範囲の「下限」に該当する値)。
<i>levalue</i>	(任意) 値に等しいかそれよりも短いプレフィックス長を指定します。これは <i>length</i> の範囲の最大値です (長さ範囲の「上限」に該当する値)。
<i>eqvalue</i>	(任意) <i>length</i> の正確な値。

コマンド デフォルト

IPv4 プレフィックスリストでパケットが拒否される特定の条件はありません。

コマンド モード

IPv4 プレフィックスリスト 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン プレフィックスリストでパケットを拒否する条件を指定するには、**deny** コマンドを使用します。

ge、**le**、**eq** の各キーワードを使用すると、*network/length* 引数よりも詳細にプレフィックス長の照合範囲を指定できます。**ge** も **le** も指定しない場合は、完全一致と見なされます。**ge** キーワードのみを指定した場合、範囲は **gevalue** から 32 までと仮定されます。**le** 属性のみを指定した場合、範囲は *length* から **le value** 引数までと見なされます。

指定する **gevalue** または **levalue** は、次の条件を満たしている必要があります。

length < **gevalue** < **levalue** <= 32 (IPv4 の場合)

length < **gevalue** < **le value** <= 128 (IPv6 の場合)

タスク ID

タスク ID	動作
acl	読み取り、書き込み

例

次に、ルート 10.0.0.0/0 を拒否する例を示します。

```
RP/0/(config)# ipv4 prefix-list list1
RP/0/(config-ipv4_pfx)# 50 deny 10.0.0.0/0
```

次に、プレフィックスが 10.3.32.154 のすべてのルートを拒否する例を示します。

```
RP/0/(config)# ipv4 prefix-list list1
RP/0/(config-ipv4_pfx)#80 deny 10.3.32.154 le 32
```

次に、プレフィックスが 172.18.30.154/16 の、25 ビットよりも長いルートのすべてのマスクを拒否する例を示します。

```
RP/0/(config)# ipv4 prefix-list list1
RP/0/(config-ipv4_pfx)#100 deny 172.18.30.154/16 ge 25
```

次に、すべてのアドレス空間で 25 ビットよりも大きいマスク長を拒否する例を示します。

```
RP/0/(config)# ipv6 prefix-list list2
RP/0/(config-ipv6_pfx)# 70 deny 2000:1::/64 ge 25
```

次の例は、list3 に拒否条件を追加し、コマンドの **no** 形式を使用してシーケンス番号が 30 の条件を削除する方法を示しています。

```
RP/0/(config)# ipv6 prefix-list list3

RP/0/(config-ipv6_pfx)# deny 2000:1::/64 ge 25
RP/0/(config-ipv6_pfx)# deny 3000:1::/64 le 32
RP/0/(config-ipv6_pfx)# deny 4000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y

RP/0/# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25
```

deny (プレフィックスリスト)

```
RP/0/# configure
RP/0/(config)# ipv6 prefix-list list3
RP/0/(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
```

ipv4 prefix-list

IP バージョン 4 (IPv4) プレフィックス リストを名前で定義するには、で **ipv4 prefix-list** コマンドを使用します。プレフィックス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。

ipv4 prefix-list name

no ipv4 prefix-list name

構文の説明

<i>name</i>	プレフィックス リストの名前。名前にはスペースや疑問符を使用できません。
-------------	--------------------------------------

コマンド デフォルト

IPv4 プレフィックス リストは定義されていません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ipv4 prefix-list コマンドは、IPv4 プレフィックス リストを設定するために使用します。このコマンドを指定すると、ルータはプレフィックスリストコンフィギュレーションモードになります。このモードでは、アクセスを拒否または許可する条件を **deny** または **permit** コマンドを使用して定義する必要があります。プレフィックス リストを作成するには条件を追加する必要があります。

新しい IPv4 プレフィックス リスト ステートメント (**permit**、**deny**、**remark**) を追加するには、**resequence prefix-list ipv4** コマンドを使用して、既存のステートメントの番号を再設定し、以降のステートメントを増分します。先頭のエン트리番号 (*base*) を指定し、ステートメントのエン트리番号を隔てるための増分を指定します。既存のステートメントの番号が再設定され、未使用のエン트리番号で新しいステートメントが追加できるようになります。

タスク ID

タスク ID	動作
acl	読み取り、書き込み

タスク ID	動作
ipv4	読み取り、書き込み

例

次に、プレフィックスリストを表示し、list2を設定し、両方のプレフィックスリストの条件を表示する例を示します。

```
RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25

RP/0/# configure
RP/0/(config)# ipv4 prefix-list list2

RP/0/(config-ipv4_pfx)#deny 172.18.30.154/16 ge 25
RP/0/(config-ipv4_pfx)#
Uncommitted changes found, commit them? [yes]: Y

RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

permit (プレフィックス リスト)

IP バージョン 4 (IPv4) プレフィックス リストの許可条件を設定するには、IPv4 プレフィックス リスト コンフィギュレーション モードで **permit** コマンドを使用します。プレフィックス リスト から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。

[*sequence-number*] **permit** *network/length* [**ge** *value*] [**le** *value*] [**eq** *value*]
no *sequence-number* **permit**

構文の説明

<i>sequence-number</i>	(任意) プレフィックス リスト中の permit ステートメントの番号。この番号により、プレフィックス リスト中のステートメントの順番が決まります。範囲は 1 ~ 2147483646 です。デフォルトでは、最初のステートメントが番号 10 で、以降のステートメントは 10 ずつ増分されます。
<i>network/length</i>	ネットワーク マスクのネットワーク番号と長さ (ビット単位)。
gevalue	(任意) 値に等しいかそれよりも長いプレフィックス長を指定します。これは <i>length</i> の範囲の最小値です (長さ範囲の「下限」に該当する値)。範囲は 1 ~ 128 です。
levalue	(任意) 値に等しいかそれよりも短いプレフィックス長を指定します。これは <i>length</i> の範囲の最大値です (長さ範囲の「上限」に該当する値)。範囲は 1 ~ 128 です。
eqvalue	(任意) <i>length</i> の正確な値。範囲は 1 ~ 128 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

IPv4 プレフィックス 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン プレフィックスリストでパケットを許可する条件を指定するには、**permit** コマンドを使用します。

ge、**le**、**eq** の各キーワードを使用すると、*network/length* 引数よりも詳細にプレフィックス長の照合範囲を指定できます。**ge** も **le** も指定しない場合は、完全一致と見なされます。**ge** キーワードのみを指定した場合、範囲は **gevalue** から 32 までと仮定されます。**le** 属性のみを指定した場合、範囲は *length* から **le value** 引数までと見なされます。

指定する **gevalue** または **levalue** は、次の条件を満たしている必要があります。

length < **gevalue** < **levalue** <= 32 (IPv4 の場合)

length < **gevalue** < **levalue** <= 128 (IPv6 の場合)

タスク ID

タスク ID	動作
acl	読み取り、書き込み

例

次に、プレフィックス 172.18.0.0/16 を許可する例を示します。

```
RP/0/(config)# ipv4 prefix-list list1
RP/0/(config-ipv4_pfx)# permit 172.18.0.0/16
```

次に、プレフィックスが 172.20.10.171/16 のルートで、24 ビットまでのマスク長を許可する例を示します。

```
RP/0/(config)# ipv4 prefix-list list1
RP/0/(config-ipv4_pfx)# permit 172.20.10.171/16 le 24
```

次に、すべてのアドレス空間で 8 ~ 24 ビットのマスク長を許可する例を示します。

```
RP/0/(config)# ipv6 prefix-list list1
RP/0/(config-ipv6_pfx)# permit 2000:1::/64 ge 8 le 24
```

次に、list3 に許可条件を追加し、シーケンス番号 30 の条件を削除する例を示します。

```
RP/0/(config)# ipv6 prefix-list list3
RP/0/(config-ipv6_pfx)# permit 2000:1::/64 ge 25
RP/0/(config-ipv6_pfx)# permit 3000:1::/64 le 32
RP/0/(config-ipv6_pfx)# permit 3000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y
RP/0/#show ipv6 prefix-list

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32
 30 permit 4000:1::/64 ge 25

RP/0/# configure
RP/0/(config)# ipv6 prefix-list list3
RP/0/(config-ipv6_pfx)# no 30
```

```
Uncommitted changes found, commit them? [yes]: y
RP/0/# show prefix-list ipv6

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
 20 permit 3000:1::/64 le 32

10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
 30 deny 4000:1::/64 ge 25
```

remark (プレフィックスリスト)

IPバージョン4 (IPv4) プレフィックスリストのエントリに有益なコメント (注釈) を記入するには、IPv4 プレフィックスリスト コンフィギュレーションモードで **remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no *sequence-number*

構文の説明

<i>sequence-number</i>	(任意) プレフィックスリスト内の remark ステートメントの番号。この番号により、プレフィックスリスト中のステートメントの順番が決まります。番号の範囲は1～2147483646です (デフォルトでは、最初のステートメントの番号が10で、以降のステートメントは10ずつ増分されます)。
<i>remark</i>	プレフィックスリストのエントリを説明する、最大255文字のコメント。

コマンド デフォルト

プレフィックスリスト エントリに注釈はありません。

コマンド モード

IPv4 プレフィックスリスト 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

remark コマンドを使用すると、プレフィックスリストのエントリに有益なコメントを書き込むことができます。注釈の長さは最大255文字で、これより長い注釈は切り捨てられます。

削除するコメントのシーケンス番号がわかっている場合は、**no sequence-number** コマンドで削除できます。

既存の IPv4 プレフィックスリストにステートメントを追加するには、**resequence prefix-list ipv4** コマンドを使用します。

タスク ID

タスク ID

動作

acl

読み取り、書き込み

例

次に、プレフィックスリスト エントリを説明する注釈を設定する例を示します。

```
RP/0/(config)# ipv4 prefix-list deny-ten
RP/0/(config-ipv4_pfx)# 10 remark Deny all routes with a prefix of 10/8
RP/0/(config-ipv4_pfx)# 20 deny 10.0.0.0/8 le 32
RP/0/(config-ipv4_pfx)# end
```

次に、使用方法を説明する注釈を設定する例を示します。

```
RP/0/# show prefix-list ipv6
```

```
ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

```
RP/0/# configure
```

```
RP/0/(config)# ipv6 prefix-list list1
RP/0/(config-ipv6-pfx)# 10 remark use from july23 forward
RP/0/(config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y
```

```
RP/0/0/CPU0:Apr  4 02:20:34.851 : config[65700]: %LIBTARCFG-6-COMMIT : Configura
tion committed by user 'UNKNOWN'. Use 'show commit changes 1000000023' to view
the changes.
```

```
RP/0/0/CPU0:Apr  4 02:20:34.984 : config[65700]: %SYS-5-CONFIG_I : Configured fr
om console by console
```

```
RP/0/# show prefix-list ipv6
```

```
ipv6 prefix-list list1
 10 remark use from july23 forward
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

resequence prefix-list ipv4

既存のステートメントの番号を再設定して以降のステートメントを増分し、新しいプレフィックスリストステートメント（**permit**、**deny**、**remark**）を追加できるようにするには、で **resequence prefix-list ipv4** コマンドを使用しま

```
resequence prefix-list ipv4 name [base [ increment ]]
```

構文の説明

<i>name</i>	プレフィックスリストの名前。
<i>base</i>	(任意) プレフィックスリスト中の順序を決定する、指定したプレフィックスリスト中の最初のステートメントの番号。最大値は 2147483646 です。
<i>increment</i>	(任意) 以降のステートメントでの、ベースシーケンス番号に対する増分。最大値は 2147483646 です。

コマンド デフォルト

base: 10
increment: 10

コマンド モード

XR 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
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

プレフィックスリストエントリのシーケンス番号によって、リスト中のエントリの順番が決まります。ルータは、ネットワーク アドレスとプレフィックスリスト エントリを比較します。ルータは、プレフィックスリストの先頭（最も小さいシーケンス番号）から比較を開始します。

プレフィックスリストの複数のエントリがプレフィックスに一致する場合、シーケンス番号が最も小さいエントリが実際の一致と見なされます。一致または拒否が発生すると、プレフィックスリストの残りのエントリは処理されません。

デフォルトでは、プレフィックスリストの最初のステートメントのシーケンス番号が 10 で、以降のステートメントは 10 ずつ増分されます。

既存の IPv4 プレフィックスリストの連続しているエントリの間には **permit**、**deny**、または **remark** ステートメントを追加するには、**resequence prefix-list ipv4** コマンドを使用します。先頭のエントリ番号 (*base*) を指定し、ステートメントのエントリ番号を隔てるための増分を指定します。既存のステートメントの番号が再設定され、未使用のエントリ番号で新しいステートメントが追加できるようになります。

タスク ID

タスク ID

動作

acl

読み取り、書き込み

例

次に、プレフィックスリスト list1 のシーケンス番号の間隔を表示し、list1 のシーケンス番号を 10 から 30 間隔に再設定し、変更後のシーケンス番号を表示する例を示します。

```
RP/0/# show prefix-list ipv4
```

```
ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

```
RP/0/# resequence prefix-list ipv4 list1 10 30
```

```
RP/0/0/CPU0:Apr  4 02:29:39.513 : ipv4_acl_action_edm[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.  Use 'show commit changes 10000000
24' to view the changes.
```

```
RP/0/# resequence prefix-list ipv4 ldp_filter 30 10
```

```
RP/0/# show prefix-list ipv4
```

```
ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 40 permit 172.18.0.0/16
 70 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

show prefix-list afi-all

すべてのアドレスファミリのプレフィックスリストの内容を表示するには、で **show prefix-list afi-all** コマンドを使用します。

show prefix-list afi-all

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
acl	読み取り

例

次の例は、**show prefix-list afi-all** コマンドの出力を示しています。

```
RP/0/# show prefix-list afi-all
ipv4 prefix-list ldp_filter
 10 permit 120.0.0.0/8 ge 8 le 32 (2000 matches)
 30 permit 130.3.0.0/24 ge 8 le 32
```

show prefix-list

プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示するには、**show prefix-list** コマンドを使用します。

show prefix-list [*list-name*] [*sequence-number*]

構文の説明

<i>list-name</i>	(任意) プレフィックス リストの名前。
<i>sequence-number</i>	(任意) プレフィックス リスト エントリのシーケンス番号。範囲は 1 ~ 2147483646 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
acl	読み取り

例

次の例は、**show prefix-list** コマンドの出力を示しています。

```
RP/0/# show prefix-list ipv4 summary
Prefix List Summary:
  Total Prefix Lists configured:          0
  Total Prefix List entries configured : 0
```

show prefix-list ipv4

現在の IP バージョン 4 (IPv4) プレフィックス リストの内容を表示するには、で **show prefix-list ipv4** コマンドを使用します。

show prefix-list ipv4 [*list-name*] [*sequence-number*] [**summary**]

構文の説明

<i>list-name</i>	(任意) プレフィックス リストの名前。
<i>sequence-number</i>	(任意) プレフィックス リスト エントリのシーケンス番号。範囲は 1 ~ 2147483646 です。
summary	(任意) プレフィックス リストの内容の要約を出力します。

コマンド デフォルト

すべての IPv4 プレフィックス リストが表示されます。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 prefix-list ipv4 コマンドは、すべての IPv4 プレフィックス リストの内容を表示するために使用します。特定の IPv4 プレフィックス リストの内容を表示するには、*name* 引数を使用します。特定のプレフィックス リスト エントリを指定するには、*sequence-number* 引数を使用します。プレフィックス リストの内容のサマリーを表示するには、**summary** キーワードを使用します。

タスク ID

タスク ID	動作
acl	読み取り

例

次に、設定されているすべてのプレフィックスリストを表示する例を示します。

```
RP/0/# show prefix-list ipv4

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
ipv4 prefix-list list2
 10 deny 172.18.30.154/16 ge 25
```

次の例では、*list-name* 引数を使用して、list1 というプレフィックスリストを表示しています。

```
RP/0/# show prefix-list ipv4 list1

ipv4 prefix-list list1
 10 permit 172.20.10.171/16 le 24
 20 permit 172.18.0.0/16
 30 deny 172.24.20.164/16 ge 25
```

次の例では、*list-name* 引数と *sequence-number* 引数を使用して、シーケンス番号 10 の list1 というプレフィックスリストを表示しています。

```
RP/0/# show prefix-list ipv4 list1 30

ipv4 prefix-list list1
 30 deny 172.24.20.164/16 ge 25
```

show prefix-list ipv4 standby

現在の IPv4 スタンバイ アクセス リストの内容を表示するには、で **show access-listsipv4 standby** コマンドを使用します。

show prefix-list ipv4 standby [*prefix-list name*] [**summary**]

構文の説明

prefix-list name (任意) 特定の IPv4 プレフィックス リストの名前。prefix-list-name 引数の値は英数字の文字列で、スペースまたは引用符を含めることはできません。

summary (任意) 現在のすべての IPv4 スタンバイ プレフィックス リストのサマリーを表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 prefix-listipv4 standby コマンドを使用すると、現在の IPv4 スタンバイ プレフィックス リストの内容を表示することができます。特定の IPv4プレフィックスリストの内容を表示するには、*name* 引数を使用します。

show prefix-list ipv4 standby summary コマンドを使用すると、すべての IPv4 スタンバイプレフィックス リストのサマリーを表示することができます。

タスク ID

タスク ID	動作
acl	読み取り

例 次の例では、すべての IPv4 アクセス リストの内容が表示されています。

```
RP/0/# show prefix-list ipv4 standby summary
Prefix List Summary:
  Total Prefix Lists configured:      2
  Total Prefix List entries configured : 6
```

```
show prefix-list ipv4 standby
```



トランスポート スタック コマンド

この章では、トランスポート スタック（ノンストップルーティング、ストリーム制御転送プロトコル（SCTP）、NSR、TCP、ユーザデータグラムプロトコル（UDP）、RAW）に関連する機能を設定したりモニタする際に使用する Cisco IOS XR ソフトウェアのコマンドについて説明します。TCP あるいは UDP 以外のすべての IP プロトコルは、*RAW* プロトコルと考えられています。

トランスポート スタックの概念、設定作業、および例の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*』を参照してください。

- [clear raw statistics pcb, 397 ページ](#)
- [clear tcp pcb, 399 ページ](#)
- [clear tcp statistics, 401 ページ](#)
- [clear udp statistics, 403 ページ](#)
- [forward-protocol udp, 405 ページ](#)
- [service tcp-small-servers, 407 ページ](#)
- [service udp-small-servers, 409 ページ](#)
- [show raw brief, 411 ページ](#)
- [show raw detail pcb, 413 ページ](#)
- [show raw extended-filters, 415 ページ](#)
- [show raw statistics pcb, 417 ページ](#)
- [show tcp brief, 420 ページ](#)
- [show tcp detail, 422 ページ](#)
- [show tcp extended-filters, 424 ページ](#)
- [show tcp statistics, 426 ページ](#)
- [show udp brief, 428 ページ](#)

- [show udp detail pcb, 430 ページ](#)
- [show udp extended-filters, 432 ページ](#)
- [show udp statistics, 434 ページ](#)
- [tcp mss, 436 ページ](#)
- [tcp path-mtu-discovery, 438 ページ](#)
- [tcp selective-ack, 440 ページ](#)
- [tcp synwait-time, 442 ページ](#)
- [tcp timestamp, 443 ページ](#)
- [tcp window-size, 444 ページ](#)

clear raw statistics pcb

1 つの RAW 接続またはすべての RAW 接続の統計をクリアするには、XR EXEC モードで **clear raw statistics pcb** コマンドを使用します。

```
clear raw statistics pcb {all|pcb-address} [locationnode-id]
```

構文の説明

all	すべての RAW 接続の統計をクリアします。
<i>pcb-address</i>	特定の RAW 接続の統計をクリアします。
locationnode-id	(任意) 指定されたノードの統計をクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

all キーワードを使用すると、すべての RAW 接続をクリアします。特定の RAW 接続をクリアするには、RAW 接続のプロトコルコントロールブロック (PCB) アドレスを入力します。PCB アドレスを取得するには、**show raw brief** コマンドを使用します。

location キーワードと *node-id* 引数を使用すると、指定したノードの RAW 統計をクリアできます。

タスク ID

タスク ID	動作
transport	実行

例

次の例では、PCB アドレス 0x80553b0 を使用して、RAW 接続の統計をクリアする方法を示しています。

```
RP/0/RP0/CPU0:router# clear raw statistics pcb 0x80553b0
RP/0/RP0/CPU0:router# show raw statistics pcb 0x80553b0
```

```
Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

次の例では、すべての RAW 接続の統計をクリアする方法を示しています。

```
RP/0/RP0/CPU0:router# clear raw statistics pcb all
RP/0/RP0/CPU0:router# show raw statistics pcb all
```

```
Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

```
Statistics for PCB 0x8054f80
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

```
Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

clear tcp pcb

TCP プロトコル コントロール ブロック (PCB) 接続をクリアするには、で **clear tcp pcb** コマンドを使用します。

```
clear tcp pcb {pcb-address| all} [location node-id]
```

構文の説明

<i>pcb-address</i>	指定された PCB アドレスの TCP 接続をクリアします。
all	開いている TCP 接続をすべてクリアします。
location <i>node-id</i>	(任意) 指定されたノードの TCP 接続をクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ハングアップした TCP 接続をクリアする場合は、**clear tcp pcb** コマンドを使用すると便利です。[show tcp brief](#), (420 ページ) コマンドを使用すると、クリアする接続の PCB アドレスを検索します。

clear tcp pcb all コマンドを使用した場合、リスニング状態の TCP 接続はクリアされません。特定の PCB アドレスを指定する場合は、リスニング状態の接続もクリアされます。

タスク ID

タスク ID	動作
transport	実行

例

次の例では、PCB アドレス 60B75E48 で TCP 接続をクリアする例を示しています。

```
RP/0/# clear tcp pcb 60B75E48
```

clear tcp statistics

TCP 統計をクリアするには、で **clear tcp statistics** コマンドを使用します。

```
clear tcp statistics {pcb {all|pcb-address}| summary} [location node-id]
```

構文の説明

pcb all	(任意) すべての TCP 接続の統計をクリアします。
pcbpcb-address	(任意) 特定の TCP 接続の統計をクリアします。
summary	(任意) 特定のノードあるいは接続のサマリー統計をクリアします。
locationnode-id	(任意) 指定されたノードの TCP 統計をクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

TCP 統計をクリアするには、**clear tcp statistics** コマンドを使用します。 [show tcp statistics](#), (426 ページ) コマンドを使用すると、TCP 統計を表示します。TCP 統計を表示し、TCP のデバッグを開始する前に TCP 統計をクリアできます。

オプションの **location** キーワードと *node-id* 引数を使用すると、指定したノードの TCP 統計をクリアできます。

タスク ID

タスク ID	動作
transport	実行

例

次の例では、TCP 統計をクリアする方法を示しています。

```
RP/0/# clear tcp statistics
```

clear udp statistics

ユーザ データグラム プロトコル (UDP) 統計をクリアするには、で **clear udp statistics** コマンドを使用します。

clear udp statistics {*pcb* {**all**|*pcb-address*}| **summary**} [**location** *node-id*]

構文の説明

pcb <i>all</i>	すべての UDP 接続の統計をクリアします。
pcb <i>pcb-address</i>	特定の UDP 接続の統計をクリアします。
summary	UDP サマリー統計をクリアします。
location <i>node-id</i>	(任意) 指定されたノードの UDP 統計をクリアします。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

UDP 統計をクリアするには、**clear udp statistics** コマンドを使用します。 [show udp statistics](#), (434 ページ) コマンドを使用すると、UDP 統計を表示します。UDP 統計を表示し、UDP のデバッグを開始する前に、UDP 統計をクリアできます。

オプションの **location** キーワードと *node-id* 引数を使用すると、指定したノードの UDP 統計をクリアできます。

タスク ID

タスク ID	動作
transport	実行

例

次の例では、UDP サマリー統計をクリアする方法を示しています。

```
RP/0/# clear udp statistics summary
```

forward-protocol udp

ブロードキャスト パケットとして受信した任意のユーザ データグラム プロトコル (UDP) データグラムを特定のヘルパーアドレスに転送するようにシステムを設定するには、**forward-protocol udp** コマンドを使用します。このコマンドで設定したシステムの状態をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

```
forward-protocol udp {port-number| disable| domain| nameserver| netbios-dgm| netbios-ns| tacacs| tftp}
no forward-protocol udp {port-number| disable| domain| nameserver| netbios-dgm| netbios-ns| tacacs| tftp}
```

構文の説明

<i>port-number</i>	UDPブロードキャストパケットを指定されたポート番号に転送します。有効値の範囲は 1 ~ 65535 です。
disable	IP 転送プロトコル UDP をディセーブルにします。
domain	UDPブロードキャストパケットをドメインネームサービス (DNS、53) に転送します。
nameserver	UDPブロードキャストパケットを IEN116 ネームサービス (obsolete、42) に転送します。
netbios-dgm	UDPブロードキャストパケットをNetBIOSデータグラムサービス (138) に転送します。
netbios-ns	UDPブロードキャストパケットをNetBIOSネームサービス (137) に転送します。
tacacs	UDPブロードキャストパケットをTACACS (49) に転送します。
tftp	UDPブロードキャストパケットをTFTP (69) に転送します。

コマンド デフォルト

forward-protocol udp はディセーブルになります。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン **forward-protocol udp** コマンドを使用すると、着信インターフェイスで受信したUDPブロードキャストパケットを特定のヘルパーアドレスに転送するように指定できます。

forward-protocol udp コマンドを設定する場合は、**helper-address** コマンドも設定して、インターフェイスのヘルパーアドレスを指定する必要があります。ヘルパーアドレスはUDPデータグラムの転送先IPアドレスです。サービスを処理できるホストまたはネットワークデバイスのIPアドレスを、**helper-address** コマンドに設定します。ヘルパーアドレスはインターフェイスごとに設定されているため、転送するブロードキャストを受信する各受信インターフェイスで、ヘルパーアドレスを指定する必要があります。

転送するUDPポートごとに1つの**forward-protocol udp** コマンドを設定する必要があります。パケットのポートはポート53 (**domain**)、ポート69 (**tftp**)、または指定されたポート番号のいずれかです。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

次の例は、着信 tenGigE インターフェイス 0/RP0/CPU0 で受信した、ポート 53 またはポート 69 を持つすべてのUDPブロードキャストパケットを、172.16.0.1 に転送するための指定方法を示しています。UDPブロードキャストを受信する tenGigE インターフェイス 0/RP0/CPU0 にはヘルパーアドレス 172.16.0.1 が設定されています。これは、UDPデータグラムの転送先アドレスです。

```
RP/0/(config)# forward-protocol udp domain disable
RP/0/(config)# forward-protocol udp tftp disable
RP/0/(config)# interface tenGigE 0/RP0/CPU0
RP/0/(config-if)# ipv4 helper-address 172.16.0.1
```

service tcp-small-servers

ECHO などの小規模 TCP サーバをイネーブルにするには、で **service tcp-small-servers** コマンドを使用します。TCP 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。

```
service {ipv4| ipv6} tcp-small-servers [max-servers number| no-limit] [ access-list-name ]
```

```
no service {ipv4| ipv6} tcp-small-servers [max-servers number| no-limit] [ access-list-name ]
```

構文の説明

ip4	IPv4 小規模サーバを指定します。
ipv6	IPv6 小規模サーバを指定します。
max-servers	(任意) 許容 TCP 小規模サーバ数を設定します。
<i>number</i>	(任意) 数値です。範囲は 1 ~ 2147483647 です。
no-limit	(任意) 許容 TCP サーバ数を無制限に設定します。
<i>access-list-name</i>	(任意) アクセス リスト名です。

コマンド デフォルト

TCP 小規模サーバはディセーブルです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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、TCP 小規模サーバは、Discard (ポート 9)、Echo (ポート 7)、Chargen (ポート 19) の 3 つのサービスから構成されています。これらのサービスを使用して、TCP トランスポート機能をテストします。Discard サーバはデータを受信し、廃棄します。Echo サーバはデータを受信し、同じデータを送信ホストに返します。Chargen サーバは一連のデータを生成し、リモートホストに送信します。

タスク ID

タスク ID	動作
ipv4	読み取り、書き込み
ip-services	読み取り、書き込み

例

次の例では、小規模 IPv4 TCP サーバをイネーブルにします。

```
RP/0/(config)# service ipv4 tcp-small-servers max-servers 5 acl100
```

service udp-small-servers

ECHO などの小規模ユーザデータグラムプロトコル (UDP) サーバをイネーブルにするには、で **service udp-small-servers** コマンドを使用します。UDP 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。

```
service {ipv4| ipv6} udp-small-servers [max-servers number| no-limit] [ access-list-name ]
```

```
no service {ipv4| ipv6} udp-small-servers [max-servers number| no-limit] [ access-list-name ]
```

構文の説明

ip4	IPv4 小規模サーバを指定します。
ip6	IPv6 小規模サーバを指定します。
max-servers	(任意) 許容 UDP 小規模サーバ数を設定します。
number	(任意) 数値です。範囲は 1 ~ 2147483647 です。
no-limit	(任意) 許容 UDP 小規模サーバ数を無制限に設定します。
access-list-name	(任意) アクセス リストの名前。

コマンド デフォルト

UDP 小規模サーバはディセーブルです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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、UDP 小規模サーバは、Discard (ポート 9)、Echo (ポート 7)、Chargen (ポート 19) の 3 つのサービスから構成されています。これらのサービスを使用して、UDP トランスポート機能をテストします。Discard サーバはデータを受信し、廃棄します。Echo サーバはデータを受信し、同じデータを送信ホストに返します。Chargen サーバは一連のデータを生成し、リモートホストに送信します。

タスク ID	タスク ID	動作
	ipv6	読み取り、書き込み
	ip-services	読み取り、書き込み

例

次の例では、小規模 IPv6 UDP サーバをイネーブルにし、許容小規模サーバの最大数を 10 に設定する方法を示しています。

```
RP/0/ (config)# service ipv6 udp-small-servers max-servers 10
```

show raw brief

アクティブ RAW IP ソケットに関する情報を表示するには、で **show raw brief** コマンドを使用します。

show raw brief [*location node-id*]

構文の説明

location*node-id* (任意) 指定したノードの情報を表示します。*node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

オープン ショーテストパス ファースト (OSPF) やプロトコル独立マルチキャスト (PIM) などのプロトコルは、長寿命 RAW IP ソケットを使用します。**ping** および **traceroute** コマンドでは、存続期間が短い RAW IP ソケットが使用されます。これらのプロトコルのいずれかに関する問題があると思われる場合は、**show raw brief** コマンドを使用します。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show rawbrief** コマンドの出力を示しています。

```
RP/0/# show raw brief
PCB          Recv-Q  Send-Q  Local Address          Foreign Address Protocol
0x805188c    0        0  0 0.0.0.0              0.0.0.0              2
0x8051dc8    0        0  0 0.0.0.0              0.0.0.0              103
```

```
0x8052250      0      0 0.0.0.0      0.0.0.0      255
```

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 51 : *show raw brief* コマンドのフィールドの説明

フィールド	説明
PCB	プロトコル コントロールブロック アドレス。ローカル アドレス、外部アドレス、ローカルポート、外部ポートなどの接続情報を含む構造に対するアドレスです。
Recv-Q	受信キューのバイト数。
Send-Q	送信キューのバイト数。
Local Address	ローカル アドレスおよびローカル ポート。
Foreign Address	外部アドレスおよび外部ポート。
Protocol	RAW IP ソケットを使用するプロトコル。たとえば、番号 2 は IGMP、番号 103 は PIM、番号 89 は OSPF です。

show raw detail pcb

アクティブ RAW IP ソケットの詳細情報を表示するには、で **show raw detail pcb** コマンドを使用します。

```
show raw detail pcb {pcb-address| all} location node-id
```

構文の説明

<i>pcb-address</i>	指定された RAW 接続の統計を表示します。
all	すべての RAW 接続の統計を表示します。
location <i>node-id</i>	指定されたノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 raw detail pcb コマンドを使用すると、RAW トランスポートを使用するすべての接続に関する詳細情報が表示されます。表示される情報には、ファミリータイプ（たとえば、2 は IPv4 としても知られている AF_INET）、PCB アドレス、レイヤ 4（または、トランスポート）プロトコル、ローカルアドレス、外部アドレス、使用中のすべてのフィルタが含まれます。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show raw detail pcb** コマンドの出力を示しています。

```
RP/0/# show raw detail pcb 0x807e89c
=====
PCB is 0x807e89c, Family: 2, PROTO: 89
  Local host: 0.0.0.0
  Foreign host: 0.0.0.0

Current send queue size: 0
Current receive queue size: 0
Paw socket: Yes
```

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 52 : **show raw detail pcb** コマンドのフィールドの説明

フィールド	説明
JID	ソケットを作成したプロセスのジョブ ID。
Family	ネットワーク プロトコル。IPv4 は 2、IPv6 は 26 です。
PCB	プロトコル コントロール ブロック アドレス。
L4-proto	レイヤ 4 (または、トランスポート) プロトコル。
Laddr	ローカル アドレス。
Faddr	外部アドレス。
ICMP error filter mask	ICMP フィルタが設定されている場合、このフィールドにはゼロ以外の値が出力されます。
LPTS socket options	LPTS オプションが設定されている場合、このフィールドにはゼロ以外の値が出力されます。
Packet Type Filters	フィルタタイプのパケット数をはじめとする特定の RAW ソケットに設定されているパケットフィルタ。複数のフィルタを設定できます。

show raw extended-filters

アクティブ RAW IP ソケットに関する情報を表示するには、で **show raw extended-filters** コマンドを使用します。

```
show raw extended-filters {interface-filter location node-id| location node-id| paktype-filter location node-id}
```

構文の説明

interface-filter	設定されたインターフェイス フィルタを使用して、プロトコル コントロール ブロック (PCB) を表示します。
location <i>node-id</i>	指定されたノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
paktype-filter	設定されたパケットタイプフィルタを使用して、PCBを表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	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 raw extended-filters コマンドを使用すると、RAW トランスポートを使用するすべての接続に関する詳細情報が表示されます。表示される情報には、ファミリタイプ (たとえば、2 は IPv4 としても知られている AF_INET)、PCB アドレス、レイヤ 4 (または、トランスポート) プロトコル、ローカルアドレス、外部アドレス、使用中のすべてのフィルタが含まれます。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show raw extended-filters** コマンドの出力を示しています。

```
RP/0/# show raw extended-filters 0/RP0/CPU0

Total Number of matching PCB's in database: 1
JID: 0/0
Family: 2
PCB: 0x0803dd38
L4-proto: 1
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x3ff
LPTS socket options: 0x0020
Packet Type Filters:
0
[220 pkts in]
3
[0 pkts in]
4
[0 pkts in]
```

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 53 : **show raw extended-filters** コマンドの出力フィールドの説明

フィールド	説明
JID	ソケットを作成したプロセスのジョブ ID。
Family	ネットワーク プロトコル。IPv4 は 2、IPv6 は 26 です。
PCB	プロトコル コントロール ブロック アドレス。
L4-proto	レイヤ 4 (または、トランスポート) プロトコル。
Laddr	ローカル アドレス。
Faddr	外部アドレス。
ICMP error filter mask	ICMP フィルタが設定されている場合、このフィールドにはゼロ以外の値が出力されます。
LPTS socket options	LPTS オプションが設定されている場合、このフィールドにはゼロ以外の値が出力されます。
Packet Type Filters	フィルタタイプのパケット数をはじめとする特定の RAW ソケットに設定されているパケットフィルタ。複数のフィルタを設定できます。

show raw statistics pcb

1 つの RAW 接続またはすべての RAW 接続の統計を表示するには、で **show raw statistics pcb** コマンドを使用します。

show raw statistics pcb {**all**| **pcb-address**} **location** *node-id*

構文の説明

all	すべての RAW 接続の統計を表示します。
pcb-address	指定された RAW 接続の統計を表示します。
location <i>node-id</i>	(任意) 指定したノードの RAW 統計情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

all キーワードを使用すると、すべての RAW 接続を表示します。特定の RAW 接続が必要な場合は、該当する RAW 接続のプロトコルコントロールブロック (PCB) アドレスを入力します。PCB アドレスを取得するには、**show raw brief** コマンドを使用します。

location キーワードと *node-id* 引数を使用すると、特定のノードの RAW 統計を表示できます。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例では、PCB アドレス 0x80553b0 の RAW 接続統計が表示されます。

```
RP/0/# show raw statistics pcb 0x80553b0

Statistics for PCB 0x80553b0
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

この例では、すべての RAW 接続の統計が表示されます。

```
RP/0/# show raw statistics pcb all

Statistics for PCB 0x805484c
Send: 0 packets received from application
0 xipc pulse received from application
0 packets sent to network
0 packets failed getting queued to network
Rcvd: 0 packets received from network
0 packets queued to application
0 packets failed queued to application
```

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 54 : *show raw statistics pcb* コマンドのフィールドの説明

フィールド	説明
Send:	このセクションの統計は、アプリケーションから RAW に送信されるパケットを示しています。
Vrfid	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
xipc pulse received from application	アプリケーションから RAW に送信される通知数。
packets sent to network	ネットワークに送信されるパケット数。
packets failed getting queued to network	ネットワークキューイングに失敗したパケット数。
Rcvd:	このセクションの統計は、ネットワークから受信したパケットを示しています。
packets queued to application	アプリケーションキューイングされたパケット数。

フィールド	説明
packets failed queued to application	アプリケーション キューイングに失敗したパケット数。

show tcp brief

TCP 接続テーブルのサマリーを表示するには、で **show tcp brief** コマンドを使用します。

show tcp brief [*location node-id*]

構文の説明

location*node-id* (任意) 指定したノードの情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show tcp brief** コマンドの出力を示しています。

```
RP/0/# show tcp brief
```

TCPCB	Recv-Q	Send-Q	Local Address	Foreign Address	State
0x80572a8	0	0	0.0.0.0:513	0.0.0.0:0	LISTEN
0x8056948	0	0	0.0.0.0:23	0.0.0.0:0	LISTEN
0x8057b60	0	3	10.8.8.2:23	10.8.8.1:1025	ESTAB

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 55 : *show tcp brief* コマンドのフィールドの説明

フィールド	説明
TCPCB	TCP コントロール ブロックのメモリ アドレス
Recv-Q	読み取り待機中のバイト数
Send-Q	送信待機中のバイト数
Local Address	パケットのソース アドレスとポート番号
Foreign Address	パケットの送信先アドレスとポート番号
State	TCP 接続の状態

show tcp detail

TCP 接続テーブルの詳細を表示するには、で **show tcp detail** コマンドを使用します。

show tcp detail pcb [*value*| **all**]

構文の説明

pcb	TCP 接続情報を表示します。
<i>value</i>	特定の接続情報を表示します。範囲は 0 ~ ffffffff です。
all	すべての接続情報を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show tcp detail pcb all** コマンドの出力を示しています。

```
RP/0/# show tcp detail pcb all
Connection state is LISTEN, I/O status: 0, socket status: 0
PCB 0x8092774, vrfid 0x0
Local host: 0.0.0.0, Local port: 23
Foreign host: 0.0.0.0, Foreign port: 0
```

```
Current send queue size: 0 (max 16384)
Current receive queue size: 0 (max 16384)  mis-ordered: 0 bytes

Timer           Starts      Wakeups      Next (msec)
Retrans         0           0            0
SendWnd         0           0            0
TimeWait       0           0            0
AckHold        0           0            0
KeepAlive      0           0            0
PmtuAger       0           0            0
GiveUp         0           0            0
Throttle       0           0            0
iss: 0         snduna: 0    sndnxt: 0
sndmax: 0      sndwnd: 0    sndcwnd: 1073725440
irs: 0         rcvnxt: 0    rcvwnd: 16384  rcvadv: 0
```

show tcp extended-filters

TCP 拡張フィルタの詳細を表示するには、で **show tcp extended-filters** コマンドを使用します。

show tcp extended-filters [*location node-id*]**peer-filter** [*location node-id*]

構文の説明

location <i>node-id</i>	(任意) 指定したノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
peer-filter	(任意) ピア フィルタが設定されている接続を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、特定のロケーション (0/RP0/CPU0) に対する **show tcp extended-filters** コマンドの出力を示しています。

```
RP/0/# show tcp extended-filters location 0/RP0/CPU0
Total Number of matching PCB's in database: 3
-----
JID: 135
Family: 2
```

```
PCB: 0x4826c5dc
L4-proto: 6
Lport: 23
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x12
LPTS options: 0x00000000
```

```
-----
JID: 135
Family: 2
```

```
PCB: 0x4826dd8c
L4-proto: 6
Lport: 23
Fport: 59162
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12
LPTS options: 0x00000000
```

```
-----
JID: 135
Family: 2
PCB: 0x4826cac0
L4-proto: 6
Lport: 23
Fport: 59307
Laddr: 12.31.22.10
Faddr: 223.255.254.254
ICMP error filter mask: 0x12
LPTS options: 0x00000000
-----
```

show tcp statistics

TCP 統計を表示するには、で **show tcp statistics** コマンドを使用します。

show tcp statistics {**pcb** {**all**|*pcb-address*}| **summary**} [**location** *node-id*]

構文の説明

pcb <i>pcb-address</i>	(任意) 指定された接続の詳細統計を表示します。
pcb all	(任意) すべての接続の詳細統計を表示します。
summary	(任意) 特定のノードあるいは接続のサマリー統計をクリアします。
location <i>node-id</i>	(任意) 指定されたノードの統計を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show tcp statistics** コマンドの出力を示しています。

```
RP/0/# show tcp statistics pcb 0x08091bc8

Statistics for PCB 0x8091bc8 VRF Id 0x60000000
Send:  0 bytes received from application
        0 xipc pulse received from application
        0 bytes sent to network
        0 packets failed getting queued to network
Rcvd:  0 packets received from network
        0 packets queued to application
        0 packets failed queued to application
```

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 56 : **show tcp statistics** コマンドのフィールドの説明

フィールド	説明
vrfid	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Send	この項の統計情報は、ルータにより送信されたパケットについての情報です。
Rcvd:	この項の統計情報は、ルータにより受信されたパケットについての情報です。

show udp brief

ユーザ データグラム プロトコル (UDP) 接続テーブルのサマリーを表示するには、で **show udp brief** コマンドを使用します。

show udp brief [*location node-id*]

構文の説明

location*node-id* (任意) 指定したノードの情報を表示します。 *node-id* 引数は、*rack/slot/module* の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show udp brief** コマンドの出力を示しています。

```
RP/0/# show udp brief

PCB          Recv-Q  Send-Q  Local Address          Foreign Address
0x8040c4c    0        0       0.0.0.0:7             0.0.0.0:0
0x805a120    0        0       0.0.0.0:9             0.0.0.0:0
0x805a430    0        0       0.0.0.0:19            0.0.0.0:0
0x805a740    0        0       0.0.0.0:67            0.0.0.0:0
0x804ecb0    0        0       0.0.0.0:123           0.0.0.0:0
```

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 57 : *show udp brief* コマンドのフィールドの説明

フィールド	説明
PCB	プロトコルコントロールブロック アドレス。ローカルアドレス、外部アドレス、ローカルポート、外部ポートなどの接続情報を含む構造に対するアドレスです。
Recv-Q	受信キューのバイト数。
Send-Q	送信キューのバイト数。
Local Address	ローカルアドレスおよびローカルポート。
Foreign Address	外部アドレスおよび外部ポート。

show udp detail pcb

ユーザ データグラム プロトコル (UDP) 接続テーブルの詳細情報を表示するには、で **show udp detail pcb** コマンドを使用します。

show udp detail pcb {*pcb-address*| **all**} [**location** *node-id*]

構文の説明

<i>pcb-address</i>	指定された UDP 接続のアドレス。
all	すべての UDP 接続の統計を提供します。
location <i>node-id</i>	(任意) 指定したノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、**show udp detail pcb all** コマンドの出力を示しています。

```
RP/0/# show udp detail pcb all location 0/RP0/CPU0
=====
PCB is 0x4822fea0, Family: 2, VRF: 0x60000000
```

```

Local host: 0.0.0.0:3784
Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0
=====
PCB is 0x4822d0e0, Family: 2, VRF: 0x60000000
Local host: 0.0.0.0:3785
Foreign host: 0.0.0.0:0

Current send queue size: 0
Current receive queue size: 0

```

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 58 : *show raw pcb* コマンドのフィールドの説明

フィールド	説明
PCB	プロトコルコントロールブロック アドレス。
Family	ネットワーク プロトコル。IPv4 は 2、IPv6 は 26 です。
VRF	VPN ルーティング/転送 (VRF) インスタンス名。
Local host	ローカル ホスト アドレス。
Foreign host	外部ホスト アドレス。
Current send queue size	送信キューのサイズ (バイト単位)。
Current receive queue size	受信キューのサイズ (バイト単位)。

show udp extended-filters

UDP 拡張フィルタの詳細を表示するには、で **show udp extended-filters** コマンドを使用します。

show udp extended-filters {*location node-id*} **peer-filter** {*location node-id*}

構文の説明

location <i>node-id</i>	指定されたノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。
peer-filter	ピア フィルタが設定されている接続を表示します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り

例

次の例は、特定のロケーション（0/RP0/CPU0）に対する **show udp extended-filters** コマンドの出力を示しています。

```
RP/0/# show udp extended-filters location 0/RP0/CPU0
Total Number of matching PCB's in database: 1
-----
JID: 248
Family: 2
```

```
PCB: 0x48247e94
L4-proto: 17
Lport: 646
Fport: 0
Laddr: 0.0.0.0
Faddr: 0.0.0.0
ICMP error filter mask: 0x0
LPTS options: 0x00000000
-----
```

show udp statistics

ユーザ データグラム プロトコル (UDP) 統計を表示するには、で **show udp statistics** コマンドを使用します。

show udp statistics {**summary**|**pcb** {*pcb-address*|*all*}} [**location** *node-id*]

構文の説明

summary	サマリー統計を表示します。
pcb <i>pcb-address</i>	各接続の詳細統計を表示します。
pcb <i>all</i>	すべての接続の詳細統計を表示します。
location <i>node-id</i>	(任意) 指定したノードの情報を表示します。 <i>node-id</i> 引数は、 <i>rack/slot/module</i> の形式で入力します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

パケット受信に関する複数のマルチキャスト アプリケーションがある場合は、UDP は受信パケットをクローンします。

タスク ID

タスク ID	動作
transport	読み取り

例 次の例は、**show udp statistics summary** コマンドの出力を示しています。

```
RP/0/# show udp statistics summary

UDP statistics:
Rcvd: 0 Total, 0 drop, 0 no port
      0 checksum error, 0 too short
Sent: 0 Total, 0 error
0 Total forwarding broadcast packets
0 Cloned packets, 0 failed cloning
```

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 59: **show udp** コマンドのフィールドの説明

フィールド	説明
Rcvd: Total	受信されたパケットの合計数。
Rcvd: drop	削除された受信パケットの合計数
Rcvd: no port	ポートのない受信パケットの合計数
Rcvd: checksum error	チェックサムエラーを含む受信パケットの合計数
Rcvd: too short	短すぎる UDP パケットの受信パケットの合計数
Sent: Total	正常送信されたパケットの合計数
Sent: error	エラーにより送信できないパケットの合計数
Total forwarding broadcast packets	ヘルパーアドレスに転送されるパケットの合計数
Cloned packets	正常クローンされたパケットの合計数
failed cloning	クローンに失敗したパケットの合計数

tcp mss

TCPがデータ送信で使用するパケットのサイズを決定するTCP最大セグメントサイズを設定するには、で **tcp mss** コマンドを使用します。

tcp mss segment-size

構文の説明

segment-size	データ送信で TCP が使用するパケットのサイズ (バイト単位)。範囲は 68 ~ 10000 バイトです。
--------------	--

コマンド デフォルト

このコンフィギュレーションが存在しない場合、TCP はアプリケーションプロセス、インターフェイス最大転送ユニット (MTU)、パス MTU ディスカバリから受信した MTU のいずれかによって指定された設定に基づいて最大セグメントサイズを決定します。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

この例では、TCP 最大セグメントサイズを設定する方法を示しています。

```
RP/0/RSP0/CPU0:router(config)# tcp mss 1460
RP/0/RSP0/CPU0:router(config)# exit

Uncommitted changes found, commit them? [yes]:
RP/0/RSP0/CPU0:router:Sep  8 18:29:51.084 : config[65700]: %LIBTARCFG-6-COMMIT :
```

```
Configuration committed by user 'lab'. Use 'show commit changes 1000000596' to view the
changes.
Sep  8 18:29:51.209 : config[65700]: %SYS-5-CONFIG_I : Configured from console by lab
```

tcp path-mtu-discovery

接続の最大共通最大転送ユニット (MTU) を TCP で自動検出できるようにするには、で **tcp path-mtu-discovery** を使用します。デフォルトにリセットするには、このコマンドの **no** 形式を入力します。

tcp path-mtu-discovery [*age-timer minutes*| **infinite**]

no tcp path-mtu-discovery

構文の説明

age-timer*minutes* (任意) 値を指定します (分単位)。範囲は 10 ~ 30 です。

infinite (任意) エージング タイマーをオフにします。

コマンド デフォルト

tcp path-mtu-discovery はディセーブルになります。

age-timer のデフォルト値は 10 分です。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

tcp path-mtu-discovery コマンドを使用すると、TCP によって接続の最大共通 MTU を検出できるようになるので、パケットが送信ホストと受信ホストの間を移動するときに、パケットをフラグメント化して再構成する必要がなくなります。

時間タイマー値は分単位で設定します。デフォルト値は 10 分です。TCP は時間タイマーを使用して、自動的に特定の接続の MTU が増加したかどうかを検出します。**infinite** キーワードが指定されている場合、時間タイマーはオフになります。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例 次の例では、時間タイマーを 20 分に設定する方法を示しています。

```
RP/0/(config)# tcp path-mtu-discovery age-timer 20
```

tcp selective-ack

TCP 選択応答 (ACK) をイネーブルにして、リモート TCP が受信した TCP パケット内のセグメントを識別するには、で **tcp selective-ack** コマンドを使用します。デフォルトにリセットするには、このコマンドの **no** 形式を入力します。

tcp selective-ack

no tcp selective-ack

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

TCP 選択 ACK エクスポートはディセーブルです。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドがサポートされました。

使用上のガイドライン

TCP 選択 ACK がイネーブルになっている場合、各パケットにはリモート TCP が受信したセグメントを特定する情報が含まれています。これによって、送信側は失われたセグメントだけを再送信できます。選択 ACK がディセーブルになっている場合、送信側は失われたセグメントに関する情報は受信せず、応答が返されていない最初のパケットを自動的に送信して、他の TCP がデータストリームから失われた内容に応答するまで待機します。大規模な帯域 * 遅延製品で、価値のある帯域が再送信の待機で浪費されるような高速衛星リンクなどの高帯域遅延ネットワーク (LFN) の場合は、この方法は不十分です。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

次の例では、選択 ACK がイネーブルです。

```
RP/0/(config) # tcp selective-ack
```

tcp synwait-time

ソフトウェアがTCP接続の確立を試みながら、タイムアウトになるまで待機する時間を設定するには、で **tcp synwait-time** コマンドを使用します。デフォルト値に戻す場合は、このコマンドの **no** 形式を入力します。

tcp synwait-time *seconds*

no tcp synwait-time *seconds*

構文の説明

<i>seconds</i>	TCP 接続の確立を試みながら待機する時間（秒数）。範囲は5～30秒です。
----------------	---------------------------------------

コマンド デフォルト

synwait-time のデフォルト値は30秒です。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドがサポートされました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

次の例では、18秒間TCP接続の確立を試み続けるようにソフトウェアを設定する方法を示しています。

```
RP/0/(config)# tcp synwait-time 18
```

tcp timestamp

より正確にパケットの往復時間を測定するには、で **tcp timestamp** コマンドを使用します。デフォルトにリセットするには、このコマンドの **no** 形式を入力します。

tcp timestamp

no tcp timestamp

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

TCP タイムスタンプは使用しません。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドがサポートされました。

使用上のガイドライン

より正確にパケットの往復時間を測定するには、**tcp timestamp** コマンドを使用します。タイムスタンプを使用しない場合、TCP 送信側はパケットの応答が受信されるときに、往復時間を減少させます。応答の遅延、重複、消滅などの発生が考えられるため、これは非常に正確な方法です。タイムスタンプを使用する場合、各パケットには、応答が受信されるときに、パケットを特定するタイムスタンプと、該当パケットの往復時間が含まれます。

この機能は、大規模な帯域 * 遅延製品である高帯域遅延ネットワーク (LFN) で最も有効です。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

次の例では、タイムスタンプ オプションをイネーブルにする方法を示しています。

```
RP/0/(config)# tcp timestamp
```

tcp window-size

TCP ウィンドウサイズを変更するには、で **tcp window-size** 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。

tcp window-size *bytes*

no tcp window-size

構文の説明

bytes ウィンドウズ サイズ (バイト数)。範囲は 2048 ~ 65535 バイトです。

コマンド デフォルト

ウィンドウズ サイズのデフォルト値は 16k です。

コマンド モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドがサポートされました。

使用上のガイドライン

デフォルト値を変更する明らかな理由がない場合は、このコマンドを使用しないでください。

タスク ID

タスク ID	動作
transport	読み取り、書き込み

例

次の例では、TCP ウィンドウズ サイズを 3000 バイトに設定する方法を示しています。

```
RP/0/(config)# tcp window-size 3000
```