



## **Cisco ASR 9000 シリーズ アグリゲーション サービス 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 リリース 4.2**

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



## 目次

### はじめに xv

マニュアルの変更履歴 xv

マニュアルの入手方法およびテクニカル サポート xv

### アクセス リスト コマンド 1

clear access-list ipv4	3
clear access-list ipv6	6
copy access-list ipv4	9
copy access-list ipv6	11
deny (IPv4)	13
deny (IPv6)	25
ipv4 access-group	31
ipv4 access-list	34
ipv4 access-list log-update rate	36
ipv4 access-list log-update threshold	38
ipv6 access-group	40
ipv6 access-list	43
ipv6 access-list log-update rate	47
ipv6 access-list log-update threshold	49
ipv6 access-list maximum ace threshold	51
ipv6 access-list maximum acl threshold	53
permit (IPv4)	55
permit (IPv6)	75
remark (IPv4)	81
remark (IPv6)	83
resequence access-list ipv4	85
resequence access-list ipv6	88
show access-lists afi-all	91

show access-lists ipv4	92
show access-lists ipv6	98
<b>ARP コマンド</b>	<b>103</b>
arp	104
arp dagr	107
arp purge-delay	109
arp timeout	111
clear arp-cache	113
peer (DAGR)	115
priority-timeout	117
proxy-arp	119
route distance	121
route metric	123
show arp	125
show arp dagr	130
show arp traffic	132
timers (DAGR)	135
<b>シスコ エクスプレス フォワーディング コマンド</b>	<b>137</b>
clear adjacency statistics	140
clear cef ipv4 drops	142
clear cef ipv4 exceptions	144
clear cef ipv4 interface bgp-policy-statistics	146
clear cef ipv4 interface rpf-statistics	148
clear cef ipv6 drops	150
clear cef ipv6 exceptions	152
clear cef ipv6 interface bgp-policy-statistics	154
ipv4 bgp policy accounting	156
ipv4 bgp policy propagation	159
ipv4 verify unicast source reachable-via	161
ipv6 verify unicast source reachable-via	164
rp mgmtethernet forwarding	166
show adjacency	168
show cef	171
show cef bgp-attribute	173
show cef external	175

show cef recursive-nextthop	178
show cef summary	180
show cef ipv4	183
show cef ipv4 adjacency	186
show cef ipv4 adjacency hardware	189
show cef ipv4 drops	192
show cef ipv4 exact-route	195
show cef ipv4 exceptions	198
show cef ipv4 hardware	201
show cef ipv4 interface	203
show cef ipv4 interface bgp-policy-statistics	206
show cef ipv4 non-recursive	209
show cef ipv4 resource	213
show cef ipv4 summary	215
show cef ipv4 unresolved	218
show cef ipv6	220
show cef ipv6 adjacency	224
show cef ipv6 adjacency hardware	226
show cef ipv6 drops	228
show cef ipv6 exact-route	232
show cef ipv6 exceptions	234
show cef ipv6 hardware	237
show cef ipv6 interface	239
show cef ipv6 non-recursive	241
show cef ipv6 resource	244
show cef ipv6 summary	246
show cef ipv6 unresolved	249
show cef mpls adjacency	251
show cef mpls adjacency hardware	254
show cef mpls interface	256
show cef mpls unresolved	258
show cef vrf	260
<b>DHCP コマンド</b>	<b>263</b>
clear dhcp ipv4 snoop binding	265
clear dhcp ipv6 proxy binding	267

destination (DHCP IPv6)	269
dhcp ipv4	272
dhcp ipv6	274
dhcp ipv4 none	276
giaddr policy	278
helper-address	280
helper-address (IPv6)	282
interface (DHCP)	285
profile (DHCP)	287
relay information check	291
relay information option	293
relay information option allow-untrusted	296
relay information policy	299
show dhcp ipv4 relay profile	302
show dhcp ipv4 relay profile name	304
show dhcp ipv4 relay statistics	306
show dhcp ipv4 snoop binding	308
show dhcp ipv6 interface	310
show dhcp ipv4 snoop statistics	313
show dhcp ipv6 proxy binding	315
trust relay-reply	317
trusted	319
vrf (relay profile)	321
ホスト サービスおよびアプリケーション コマンド	325
cinetd rate-limit	327
clear host	329
domain ipv4 host	331
domain ipv6 host	333
domain list	335
domain lookup disable	337
domain name (グローバル)	339
domain name-server	341
ftp client anonymous-password	343
ftp client passive	345
ftp client password	347

ftp client source-interface	349
ftp client username	351
ping (ネットワーク)	353
ping bulk (ネットワーク)	357
rcp client source-interface	360
rcp client username	362
show cinetd services	364
show hosts	366
telnet	369
telnet client source-interface	373
telnet dscp	375
telnet server	377
telnet transparent	379
tftp client source-interface	381
tftp server	383
traceroute	385
<b>HSRP コマンド</b>	<b>389</b>
address (hsrp)	391
address secondary (hsrp)	393
authentication (hsrp)	395
bfd fast-detect (hsrp)	397
clear hsrp statistics	399
hsrp authentication	401
hsrp bfd fast-detect	403
hsrp bfd minimum-interval	405
hsrp bfd multiplier	407
hsrp delay	409
hsrp ipv4	411
hsrp mac-address	413
hsrp preempt	416
hsrp priority	418
hsrp redirects	420
hsrp timers	422
hsrp track	425
hsrp use-bia	428

interface (HSRP)	430
mac-address (hsrp)	432
preempt (hsrp)	434
priority (hsrp)	436
router hsrp	438
session name	440
show hsrp	442
show hsrp bfd	447
show hsrp mgo	449
show hsrp statistics	451
show hsrp summary	453
slave follow	455
slave primary virtual IPv4 address	457
slave secondary virtual IPv4 address	459
slave virtual mac address	461
timers (hsrp)	463
track (hsrp)	466
<b>LPTS コマンド</b>	<b>469</b>
clear lpts ifib statistics	471
clear lpts pifib hardware statistics	473
clear lpts pifib statistics	476
flow (LPTS)	478
lpts pifib hardware police	485
show lpts bindings	487
show lpts clients	492
show lpts flows	495
show lpts ifib	499
show lpts ifib slices	503
show lpts ifib statistics	507
show lpts ifib times	509
show lpts mpa groups	511
show lpts pifib	513
show lpts pifib hardware context	519
show lpts pifib hardware entry	522
show lpts pifib hardware police	526



show lpts pifib hardware usage	530
show lpts pifib statistics	532
show lpts port-arbitrator statistics	534
show lpts vrf	536
ネットワーク スタック IPv4 および IPv6 コマンド	539
clear ipv6 neighbors	542
icmp ipv4 rate-limit unreachable	544
ipv4 address (ネットワーク)	546
ipv4 assembler max-packets	549
ipv4 assembler timeout	551
ipv4 conflict-policy	553
ipv4 directed-broadcast	555
ipv4 helper-address	557
ipv4 mask-reply	559
ipv4 mtu	561
ipv4 redirects	563
ipv4 source-route	565
ipv4 unnumbered (point-to-point)	567
ipv4 unreachable disable	570
ipv4 virtual address	572
ipv6 address	574
ipv6 address link-local	576
ipv6 assembler	578
ipv6 conflict-policy	580
ipv6 enable	582
ipv6 hop-limit	584
ipv6 icmp error-interval	586
ipv6 mtu	588
ipv6 nd dad attempts	590
ipv6 nd managed-config-flag	593
ipv6 nd ns-interval	595
ipv6 nd other-config-flag	597
ipv6 nd prefix	599
ipv6 nd ra-interval	602
ipv6 nd ra-lifetime	604

ipv6 nd reachable-time	606
ipv6 nd redirects	608
ipv6 nd scavenge-timeout	610
ipv6 nd suppress-ra	612
ipv6 neighbor	614
ipv6 source-route	617
ipv6 unreachable disable	619
local pool	621
show arm conflicts	625
show arm database	628
show arm router-ids	631
show arm registrations producers	633
show arm summary	635
show arm vrf-summary	637
show clns statistics	639
show ipv4 interface	641
show local pool	645
show ipv4 traffic	647
show ipv6 interface	650
show ipv6 neighbors	654
show ipv6 neighbors summary	660
show ipv6 traffic	662
show mpa client	665
show mpa groups	667
show mpa ipv4	669
show mpa ipv6	671
show vrf	673
vrf	676
vrf (address-family)	678
vrf (description)	680
vrf (mhost)	682
vrf mode	684
プレフィックス リスト コマンド	687
clear prefix-list ipv4	688
clear prefix-list ipv6	690

copy prefix-list ipv4	692
copy prefix-list ipv6	694
deny (プレフィックス リスト)	696
ipv4 prefix-list	699
ipv6 prefix-list	702
permit (プレフィックス リスト)	704
remark (プレフィックス リスト)	707
resequence prefix-list ipv4	709
resequence prefix-list ipv6	712
show prefix-list	714
show prefix-list afi-all	715
show prefix-list ipv4	716
show prefix-list ipv4 standby	718
show prefix-list ipv6	720
トランスポート スタック コマンド	723
clear nsr ncd client	725
clear nsr ncd queue	727
clear raw statistics pcb	730
clear tcp nsr client	732
clear tcp nsr pcb	734
clear tcp nsr session-set	737
clear tcp nsr statistics client	739
clear tcp nsr statistics pcb	741
clear tcp nsr statistics session-set	744
clear tcp nsr statistics summary	746
clear tcp pcb	748
clear tcp statistics	750
clear udp statistics	752
forward-protocol udp	754
nsr process-failures switchover	756
service tcp-small-servers	757
service udp-small-servers	759
show nsr ncd client	761
show nsr ncd queue	764
show raw brief	766

show raw detail pcb	768
show raw extended-filters	770
show raw statistics pcb	773
show tcp brief	776
show tcp detail	778
show tcp extended-filters	780
show tcp statistics	782
show tcp nsr brief	784
show tcp nsr client brief	787
show tcp nsr detail client	789
show tcp nsr detail pcb	791
show tcp nsr detail session-set	794
show tcp nsr session-set brief	796
show tcp nsr statistics client	799
show tcp nsr statistics pcb	801
show tcp nsr statistics session-set	804
show tcp nsr statistics summary	806
show udp brief	808
show udp detail pcb	810
show udp extended-filters	812
show udp statistics	814
tcp mss	816
tcp path-mtu-discovery	818
tcp selective-ack	820
tcp synwait-time	822
tcp timestamp	823
tcp window-size	825
<b>VRRP コマンド</b>	<b>827</b>
accept-mode	829
address-family	831
address (VRRP)	833
address global	835
address linklocal	837
address secondary	839
bfd minimum-interval (VRRP)	841

bfd multiplier (VRRP)	843
clear vrrp statistics	845
delay (VRRP)	850
interface (VRRP)	852
message state disable	854
router vrrp	856
show vrrp	858
snmp-server traps vrrp events	864
vrrp	866
vrrp assume-ownership disable	868
vrrp bfd fast-detect	870
vrrp bfd minimum-interval	872
vrrp bfd multiplier	874
vrrp delay	876
vrrp ipv4	878
vrrp preempt	880
vrrp priority	882
vrrp text-authentication	884
vrrp timer	886
vrrp track interface	888
<b>Cisco ASR 9000 シリーズ ルータでのビデオ モニタリング コマンド</b>	<b>891</b>
clear performance traffic clone profile	892
clear performance traffic statistics	893
show performance traffic alerts	895
show performance traffic clone profile	897
show policy-map type performance-traffic	899





## はじめに

『Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference』には、IP アドレスおよびサービスの機能に関するコマンドが記載されています。

では、次のトピックについて取り上げます。

- [マニュアルの変更履歴](#), xv 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](#), xv ページ

## マニュアルの変更履歴

次の表に、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

リビジョン	日付	変更点
OL-26072-01-J	2011 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

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は Really Simple Syndication (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がデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。







## アクセス リスト コマンド

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの IP Version 4 (IPv4) および IP Version 6 (IPv6) のアクセス リストを設定するために使用する Cisco IOS XR ソフトウェアコマンドについて説明します。

アクセス コントロール リスト (ACL) は、ネットワーク トラフィック プロファイルをまとめて定義する 1 つ以上の **Access Control Entry (ACE)** (アクセス コントロール エントリ) です。このプロファイルは、トラフィック フィルタリング、プライオリティ キューイングまたはカスタム キューイング、およびダイナミック アクセス コントロールなどの Cisco IOS XR ソフトウェア ソフトウェア機能によって参照されるようになります。各 ACL には、送信元アドレス、宛先アドレス、プロトコル、およびプロトコルに固有のパラメータなどの基準に基づく、アクション要素 (許可または拒否) やフィルタ要素が含まれています。

ACL の概念、設定タスク、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [clear access-list ipv4](#), 3 ページ
- [clear access-list ipv6](#), 6 ページ
- [copy access-list ipv4](#), 9 ページ
- [copy access-list ipv6](#), 11 ページ
- [deny \(IPv4\)](#), 13 ページ
- [deny \(IPv6\)](#), 25 ページ
- [ipv4 access-group](#), 31 ページ
- [ipv4 access-list](#), 34 ページ
- [ipv4 access-list log-update rate](#), 36 ページ
- [ipv4 access-list log-update threshold](#), 38 ページ
- [ipv6 access-group](#), 40 ページ
- [ipv6 access-list](#), 43 ページ
- [ipv6 access-list log-update rate](#), 47 ページ

- [ipv6 access-list log-update threshold](#) , 49 ページ
- [ipv6 access-list maximum ace threshold](#) , 51 ページ
- [ipv6 access-list maximum acl threshold](#) , 53 ページ
- [permit \(IPv4\)](#) , 55 ページ
- [permit \(IPv6\)](#) , 75 ページ
- [remark \(IPv4\)](#) , 81 ページ
- [remark \(IPv6\)](#) , 83 ページ
- [resequence access-list ipv4](#) , 85 ページ
- [resequence access-list ipv6](#) , 88 ページ
- [show access-lists afi-all](#) , 91 ページ
- [show access-lists ipv4](#) , 92 ページ
- [show access-lists ipv6](#) , 98 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、EXEC モードで **clear access-list ipv4** コマンドを使用します。

**clear access-list ipv4** *access-list name* [ *sequence-number* | hardware { *ingress* | *egress* } ] [ *interface type interface-path-id* ] [ *location node-id* | *sequence number* ]

### 構文の説明

<b>access-list-name</b>	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。
<b>sequence-number</b>	(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。
<b>hardware</b>	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。
<b>ingress</b>	着信方向を指定します。
<b>egress</b>	発信方向を指定します。
<b>interface</b>	(任意) インターフェイスの統計情報をクリアします。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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。
<b>location node-id</b>	(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。
<b>sequence number</b>	(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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**clear access-list ipv4** コマンドを使用すると、指定された設定済みのアクセス 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** コマンドを使用して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** 引数内にあるアスタリスク (\*) 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。

## タスク ID

タスク ID	操作
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/RSP0/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/RSP0/CPU0:router# clear access-list ipv4 marketing
RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing
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
次の例では、発信方向の acl_hw_1 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/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0
ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
 20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
 30 deny tcp any any (58 hw matches)
RP/0/RSP0/CPU0:router# clear access-list ipv4 acl_hw_1 hardware egress location 0/2/cp0
RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0
ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any
 20 permit ip 172.16.3.0 0.0.255.255 any
 30 deny tcp any any
```

関連コマンド

コマンド	説明
<a href="#">ipv4 access-group</a> , (31 ページ)	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセスリストを定義し、また、IPv4 アクセスリスト コンフィギュレーション モードを開始します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存のステートメントの番号を付け直して後続のステートメントの番号を増加して、新しい IPv4 アクセスリスト ステートメントを許可します。

## clear access-list ipv6

IPv6 アクセスリストのカウンタをクリアするには、EXEC モードで **clear access-list ipv6** コマンドを使用します。

**clear access-list ipv6** *access-list-name* [*sequence-number*] **hardware** {*ingress*|*egress*} [**interface** *type interface-path-id*] [**location** *node-id*] **sequence number**

### 構文の説明

<b>access-list-name</b>	特定の IPv6 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。
<b>sequence-number</b>	(任意) アクセスリストのカウンタをクリアする、特定のアクセスコントロールエントリ (ACE) の特定のシーケンス番号。範囲は 1 ~ 2147483644 です。
<b>hardware</b>	(任意) 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。
<b>ingress</b>	(任意) 着信方向を指定します。
<b>egress</b>	(任意) 発信方向を指定します。
<b>interface</b>	(任意) インターフェイスの統計情報をクリアします。
<b>type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>instance</b>	物理インターフェイスまたは仮想インターフェイス。
<b>interface-path-id</b>	(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、 <b>show interfaces</b> 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。
<b>location node-id</b>	(任意) カードインターフェイス上でイネーブルのアクセスリストの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。
<b>sequence number</b>	(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を指定します。範囲は 1 ~ 2147483644 です。

### コマンド モデル

EXEC モデルでは、指定された IPv6 アクセスリストがクリアされます。

コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**clear access-list ipv6** コマンドは、IPv6 に固有のものを除き、**clear access-list ipv4** コマンドと類似しています。

**clear access-list ipv6** コマンドを使用すると、指定された設定済みのアクセス 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、**ipv6 access-group** コマンドを使用して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** 引数内にあるアスタリスク (\*) 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。

タスク ID

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

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/RSP0/CPU0:router# show access-lists ipv6 marketing
ipv6 access-list marketing
 10 permit ipv6 3333:1:2:3::/64 any (51 matches)
 20 permit ipv6 4444:1:2:3::/64 any (26 matches)
```

## clear access-list ipv6

```

30 permit ipv6 5555:1:2:3::/64 any (5 matches)
RP/0/RSP0/CPU0:router# clear access-list ipv6 marketing
RP/0/RSP0/CPU0:router# show access-lists ipv6 marketing
ipv6 access-list marketing
10 permit ipv6 3333:1:2:3::/64 any
20 permit ipv6 4444:1:2:3::/64 any
30 permit ipv6 5555:1:2:3::/64 any

```

次の例では、発信方向の `acl_hw_1` 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/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0
ipv6 access-list acl_hw_1
10 permit ipv6 3333:1:2:3::/64 any (251 hw matches)
20 permit ipv6 4444:1:2:3::/64 any (29 hw matches)
30 deny tcp any any (58 hw matches)
RP/0/RSP0/CPU0:router# clear access-list ipv6 acl_hw_1 hardware egress location 0/2/cp0
RP/0/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0
ipv6 access-list acl_hw_1
10 permit ipv6 3333:1:2:3::/64 any
20 permit ipv6 4444:1:2:3::/64 any
30 deny tcp any any

```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。



## 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、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

source-acl	コピー元のアクセス リストの名前
destination-acl	<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

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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**copy access-list ipv4** コマンドを使用すると、設定済みのアクセス リストをコピーすることができます。 *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* 引数を使用すると、送信元アクセス リストの内容のコピー先を指定することができます。 *destination-acl* 引数は一意な名前である必要があり、アクセスリストまたはプレフィックスリストに *destination-acl* 引数名が存在する場合は、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していたら既存のリスト名を確認して、既存のアクセスリストまたは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	操作
acl	読み取り、書き込み

タスク ID	操作
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/RSP0/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/RSP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RSP0/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/RSP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list
RP/0/RSP0/CPU0:router# show access-lists ipv4 list-3

ipv4 access-list list-3
 10 permit ip any any
 20 deny tcp any any log
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセス リストすべての内容を表示します。

## copy access-list ipv6

既存の IPv6 アクセスリストのコピーを作成するには、EXEC モードで **copy access-list ipv6** コマンドを使用します。

**copy access-list ipv6** *source-acl destination-acl*

### 構文の説明

source-acl	コピー元のアクセス リストの名前
destination-acl	<i>source-acl</i> 引数の内容のコピー先のアクセス 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**copy access-list ipv6** コマンドを使用すると、設定済みのアクセス リストをコピーすることができます。 *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* 引数を使用すると、送信元アクセス リストの内容のコピー先を指定することができます。 *destination-acl* 引数は一意な名前である必要があり、アクセスリストまたはプレフィックスリストに *destination-acl* 引数名が存在する場合は、そのアクセス リストはコピーされません。 **copy access-list ipv6** コマンドは、送信元アクセスリストが存在していたら既存のリスト名を確認して、既存のアクセスリストまたはプレフィックス 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	操作
acl	読み取り、書き込み

タスク ID	操作
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/RSP0/CPU0:router# show access-lists ipv6 list-1

ipv6 access-list list-1
 10 permit tcp any any log
 20 permit ipv6 any any

RP/0/RSP0/CPU0:router# copy access-list ipv6 list-1 list-2

RP/0/RSP0/CPU0:router# show access-lists ipv6 list-2

ipv6 access-list list-2
 10 permit tcp any any log
 20 permit ipv6 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/RSP0/CPU0:router# copy access-list ipv6 list-1 list-3

list-3 exists in access-list

RP/0/RSP0/CPU0:router# show access-lists ipv6 list-3

ipv6 access-list list-3
 10 permit ipv6 any any
 20 deny tcp any any log
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">show access-lists ipv6</a> , (98 ページ)	現在のすべての IPv6 アクセス リストの内容を表示します。

## deny (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 **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 ] [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 ttl value [value1....value2]]
```

```
no sequence-number
```

### Internet Control Message Protocol (ICMP)

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

### Internet Group Management Protocol (IGMP)

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

### User Datagram Protocol (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]
```

### 構文の説明

sequence-number	(任意) アクセスリスト中の <b>deny</b> 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、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます)。 <b>resequence access-list</b> コマンドを使用すると、設定済みアクセスリスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
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。 <ul style="list-style-type: none"> <li>• 32 ビットの 4 分割ドット付き 10 進表記を使用する。</li> <li>• <b>any</b> キーワードを、0.0.0.0 255.255.255.255 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li> <li>• <b>host source</b> の組み合わせを、<i>source</i> 0.0.0.0 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li> </ul>

source-wildcard	<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"> <li>• 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。</li> <li>• <b>any</b> キーワードを、<b>0.0.0.0 255.255.255.255</b> の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li> <li>• <b>host source</b> の組み合わせを、<i>source 0.0.0.0</i> の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li> </ul>
protocol	<p>IP プロトコルの名前または番号。キーワード <b>ahp</b>、<b>esp</b>、<b>eigrp</b>、<b>gre</b>、<b>icmp</b>、<b>igmp</b>、<b>igrp</b>、<b>ip</b>、<b>ipinip</b>、<b>nos</b>、<b>ospf</b>、<b>pim</b>、<b>pcp</b>、<b>tcp</b>、または <b>udp</b> のいずれか1つ、あるいはIPプロトコル番号を表す0～255の整数にすることができます。任意のインターネットプロトコル (ICMP、TCP、およびUDPを含む) に一致させるには、<b>ip</b> 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>
destination	<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"> <li>• 32 ビットの4分割ドット付き10進表記を使用する。</li> <li>• <b>any</b> キーワードを、<b>0.0.0.0 255.255.255.255</b> の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li> <li>• <b>host destination</b> の組み合わせを、<i>destination 0.0.0.0</i> の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li> </ul>
destination-wildcard	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• <b>any</b> キーワードを、<b>0.0.0.0 255.255.255.255</b> の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li> <li>• <b>host destination</b> の組み合わせを、<i>destination 0.0.0.0</i> の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li> </ul>

**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** : パケットを routine precedence (0) と一致させます。
- **priority** : パケットを priority precedence (1) と一致させます。
- **immediate** : パケットを immediate precedence (2) と一致させます。
- **flash** : パケットを flash precedence (3) と一致させます。
- **flash-override** : パケットを flash override precedence (4) と一致させます。
- **critical** : パケットを critical precedence (5) と一致させます。
- **internet** : パケットを internetwork control precedence (6) と一致させます。
- **network** : パケットを network control precedence (7) と一致させます。

---

<b>dscp</b> <i>dscp</i>	<p>(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。 <i>dscp</i> の値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>0-63</b> : DiffServ コードポイント値</li> <li>• <b>af11</b> : パケットを AF11 dscp (001010) と一致させます。</li> <li>• <b>af12</b> : パケットを AF12 dscp (001100) と一致させます。</li> <li>• <b>af13</b> : パケットを AF13 dscp (001110) と一致させます。</li> <li>• <b>af21</b> : パケットを AF21 dscp (010010) と一致させます。</li> <li>• <b>af22</b> : パケットを AF22 dscp (010100) と一致させます。</li> <li>• <b>af23</b> : パケットを AF23 dscp (010110) と一致させます。</li> <li>• <b>af31</b> : パケットを AF31 dscp (011010) と一致させます。</li> <li>• <b>af32</b> : パケットを AF32 dscp (011100) と一致させます。</li> <li>• <b>af33</b> : パケットを AF33 dscp (011110) と一致させます。</li> <li>• <b>af41</b> : パケットを AF41 dscp (100010) と一致させます。</li> <li>• <b>af42</b> : パケットを AF42 dscp (100100) と一致させます。</li> <li>• <b>af43</b> : パケットを AF43 dscp (100110) と一致させます。</li> <li>• <b>cs1</b> : パケットを CS1 (precedence 1) dscp (001000) と一致させます。</li> <li>• <b>cs2</b> : パケットを CS2 (precedence 2) dscp (010000) と一致させます。</li> <li>• <b>cs3</b> : パケットを CS3 (precedence 3) dscp (011000) と一致させます。</li> <li>• <b>cs4</b> : パケットを CS4 (precedence 4) dscp (100000) と一致させます。</li> <li>• <b>cs5</b> : パケットを CS5 (precedence 5) dscp (101000) と一致させます。</li> <li>• <b>cs6</b> : パケットを CS6 (precedence 6) dscp (110000) と一致させます。</li> <li>• <b>cs7</b> : パケットを CS7 (precedence 7) dscp (111000) と一致させます。</li> <li>• <b>default</b> : デフォルト DSCP (000000)</li> <li>• <b>ef</b> : パケットを EF dscp (101110) と一致させます。</li> </ul>
-------------------------	---

---

<b>fragments</b>	<p>(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せん。</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。(コンソールに記憶されるメッセージのレベルは <b>logging console</b> 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	(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、 <b>log</b> キーワードと同じ機能を提供します。
ttl	(任意) Time-To-Life (TTL) 値との一致をオンにします。
ttl value [value1. value2]	<p>(任意) フィルタリングに使用される TTL 値 値の範囲は 1 ~ 255 です。 <i>value</i> が指定される場合にだけ、この値に対する一致になります。</p> <p><i>value1</i> および <i>value2</i> の両方が指定された場合、<i>value1</i> と <i>value2</i> の間の TTL の範囲に対してパケット TTL が一致されます。</p>
icmp-off	(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。
icmp-type	(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。
icmp-code	(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。
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"> <li>• dvmrp</li> <li>• host-query</li> <li>• host-report</li> <li>• mtrace</li> <li>• mtrace-response</li> <li>• pim</li> <li>• precedence</li> <li>• トレース</li> <li>• v2-leave</li> <li>• v2-report</li> <li>• v3-report</li> </ul>

operator	<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。オペランドとして使用可能なものには、<b>lt</b> (less than : より小さい)、<b>gt</b> (greater than : より大きい)、<b>eq</b> (equal : 等しい)、<b>neq</b> (not equal : 等しくない)、および <b>range</b> (inclusive range : 包含範囲) があります。</p> <p>演算子を <i>source</i> および <i>source-wildcard</i> の値の後に置く場合、送信元ポートと一致する必要があります。</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 <b>ttl</b> キーワードの後に置く場合、TTL 値と一致します。</p> <p><b>range</b> 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>
port	<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>
protocol-port	<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	<p>(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。</p>
match-any	<p>(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。</p>
match-all	<p>(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。</p>
+ -	<p>(必須) TCP プロトコル <b>match-any</b>、<b>match-all</b> の場合、プレフィックス <i>flag-name</i> の前に + または - を付けます。TCP フラグを設定したパケットを一致させるには、+<i>flag-name</i> 引数を使用します。TCP フラグを設定していないパケットを一致させるには、-<i>flag-name</i> 引数を使用します。</p>
flag-name	<p>(任意) TCP プロトコルが <b>match-any</b>、<b>match-all</b> の場合。フラグの名前は、<b>ack</b>、<b>fin</b>、<b>psh</b>、<b>rst</b>、<b>syn</b> になります。</p>

#### 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 リストの設定

## コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv4 access-list** コマンドに続いて **deny** コマンドを使用すると、パケットがアクセス リストを通過できない条件を指定することができます。

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。

**permit**、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。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。

2 つの連続した番号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、最初に **resequence access-list** コマンドを使用して、最初のステートメントに番号を付け直して、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
- ネットワーク
- 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。ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- ホスト名
- 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。ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- 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することができます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all + ack + syn** は TCP パケットを **ack** および **syn** フラグをセットして表示し、**match-any + ack - syn** は TCP パケットを **ack** をセットするか **syn** をセットしないで表示します。

タスク ID

タスク ID	操作
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 リストの拒否条件を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RSP0/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/RSP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

関連コマンド

コマンド	説明
<a href="#">ipv4 access-group</a> , (31 ページ)	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。

コマンド	説明
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセスリストを定義し、また、IPv4 アクセスリスト コンフィギュレーションモードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセスリストの許可条件を設定します。
<a href="#">remark (IPv4)</a> , (81 ページ)	IPv4 アクセスリスト エントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存の IPv4 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセスリストすべての内容を表示します。



## deny (IPv6)

IPv6 アクセスリストの拒否条件を設定するには、IPv6 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。拒否条件を削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] deny protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator {port | protocol-port}] [dscpvalue] [routing] [authen] [destopts] [ fragments] [packet-length operator packet-length value] [ log | log-input] [ttl operator ttl value ]
```

```
no sequence-number
```

### Internet Control Message Protocol (ICMP)

```
[ sequence-number] deny icmp {source-ipv6-prefix/ prefix-length | any | host source-ipv6-address} {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [icmp-type] [ icmp-code] [dscp value] [ routing] [authen] [destopts] [ fragments] [ log] [log-input] [icmp-off]
```

### Transmission Control Protocol (TCP)

```
[sequence-number] deny tcp {source-ipv6-prefix/ prefix-length | any | host source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator {port | protocol | port}] [dscpvalue] [routing] [authen] [destopts] [fragments] [established] {match-any | match-all | + | -} [flag-name] [log] [log-input]
```

### User Datagram Protocol (UDP)

```
[sequence-number] deny tcp {source-ipv6-prefix/ prefix-length | any | host source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator {port | protocol | port}] [dscpvalue] [routing] [authen] [destopts] [fragments] [established] [flag-name] [log] [log-input]
```

#### 構文の説明

sequence-number	(任意) アクセスリスト中の <b>deny</b> 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、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます)。 <b>resequence access-list</b> コマンドを使用すると、設定済みアクセスリスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
protocol	インターネットプロトコルの名前または番号。キーワード <b>ahp</b> 、 <b>eigrp</b> 、 <b>esp</b> 、 <b>gre</b> 、 <b>icmp</b> 、 <b>igmp</b> 、 <b>igrp</b> 、 <b>ipinip</b> 、 <b>ipv6</b> 、 <b>nos</b> 、 <b>ospf</b> 、 <b>pcp</b> 、 <b>tcp</b> 、または <b>udp</b> のいずれか 1 つ、あるいは IPv6 プロトコル番号を表す 0 ~ 255 の整数にすることができます。

<i>source-ipv6-prefix / prefix-length</i>	<p>拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。</p> <p>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。</p>
any	IPv6 プレフィックス ::0 の省略形。
<b>host</b> <i>source-ipv6-address</i>	<p>拒否条件の設定先に関する送信元の IPv6 ホスト アドレス。</p> <p><i>source-ipv6-address</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。</p>
<i>operator {port   protocol-port}</i>	<p>(任意) 指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。オペランドには、<b>lt</b> (less than : より小さい)、<b>gt</b> (greater than : より大きい)、<b>eq</b> (equal : 等しい)、<b>neq</b> (not equal : 等しくない)、および <b>range</b> (inclusive range : 包含範囲) があります。</p> <p><i>source-ipv6-prefix / prefix-length</i> 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。</p> <p><i>destination-ipv6-prefix / prefix-length</i> 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。</p> <p><b>range</b> 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> <p><i>port</i> 引数は、TCP または UDP ポートの 16 進数です。範囲は 0 ~ 65535 です。<i>protocol-port</i> 引数は、TCP または UDP ポートの名前です。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。</p>
<i>destination-ipv6-prefix / prefix-length</i>	<p>拒否条件の設定先に関する宛先の IPv6 ネットワークまたはネットワーククラス。</p> <p>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。</p>
<b>host</b> <i>destination-ipv6-address</i>	<p>拒否条件の設定先に関する宛先の IPv6 ホスト アドレス。</p> <p><i>destination-ipv6-address</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。</p>
<b>dscp value</b>	(任意) DiffServ コードポイント (DSCP) 値を、各 IPv6 パケットヘッダーのトラフィック クラス フィールド内のトラフィック クラス値に、一致させます。指定できる範囲は、0 ~ 63 です。
ルーティング	(任意) ソースルート パケットを、各 IPv6 パケットヘッダー内の拡張ヘッダーに一致させます。

authen	(任意) IPv6 認証ヘッダーが存在する場合に一致します。
destopts	(任意) IPv6 宛先オプションヘッダーが存在する場合に一致します。
fragments	(任意) フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれているフラグメント化された非初期パケットと一致させます。 <b>fragments</b> キーワードは、 <i>operator [port-number]</i> 引数が指定されていない場合に限り指定できるオプションです。
log	(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。(コンソールに記憶されるメッセージのレベルは <b>logging console</b> コマンドで制御します)  メッセージには、アクセスリスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル (TCP、UDP、ICMP または番号のいずれか)、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。
log-input	(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、 <b>log</b> キーワードと同じ機能を提供します。
ttl	(任意) Time-To-Life (TTL) 値との一致をオンにします。
operator	(任意) 指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。オペランドには、 <b>lt</b> (less than : より小さい)、 <b>gt</b> (greater than : より大きい)、 <b>eq</b> (equal : 等しい)、 <b>neq</b> (not equal : 等しくない)、および <b>range</b> (inclusive range : 包含範囲) があります。
<i>ttl value [value1 ... value2]</i>	(任意) フィルタリングに使用される TTL 値 値の範囲は 1 ~ 255 です。 <i>value</i> が指定される場合にだけ、この値に対する一致になります。  <i>value1</i> および <i>value2</i> の両方が指定された場合、 <i>value1</i> と <i>value2</i> の間の TTL の範囲に対してパケット TTL が一致されます。
icmp-off	(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。
icmp-type	(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。ICMP パケットは、ICMP メッセージタイプでフィルタリングできます。範囲は 0 ~ 255 です。
icmp-code	(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。ICMP メッセージタイプによってフィルタリングされる ICMP パケットは、ICMP メッセージコードによってもフィルタリングできます。範囲は 0 ~ 255 です。
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 <b>match-any</b> 、 <b>match-all</b> の場合、プレフィックス <i>flag-name</i> の前に + または - を付けます。TCP フラグを設定したパケットを一致させるには、+ <i>flag-name</i> 引数を使用します。TCP フラグを設定していないパケットを一致させるには、- <i>flag-name</i> 引数を使用します。
flag-name	(任意) TCP プロトコルが <b>match-any</b> 、 <b>match-all</b> の場合。フラグの名前は、 <b>ack</b> 、 <b>fin</b> 、 <b>psh</b> 、 <b>rst</b> 、 <b>syn</b> になります。

## コマンド デフォルト

IPv6 アクセス リストは定義されていません。  
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

IPv6 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 3.7.2	このコマンドが追加されました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**deny** (IPv6) コマンドは、IPv6 に固有のものを除き、**deny** (IPv4) コマンドと類似しています。

**ipv6 access-list** コマンドに続いて、**deny** (IPv6) コマンドを使用すると、パケットがアクセス リストを通過する条件を定義することができます。

*protocol* 引数に **ipv6** を指定すると、パケットの IPv6 ヘッダーを一致対象とします。

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の番号は 10 で、その次のステートメントからは 10 ずつ増加します。

**permit**、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。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。

*source-ipv6-prefix/prefix-length* および *destination-ipv6-prefix/prefix-length* の引数は両方とも、トラフィックフィルタリング（送信元プレフィックスがトラフィック送信元に基づいてトラフィックをフィルタリングし、宛先プレフィックスがトラフィック宛先に基づいてトラフィックをフィルタリングする）に使用されます。



(注) アクセスリストでなく、IPv6プレフィックスリストは、ルーティングプロトコルプレフィックスのフィルタリングに使用する必要があります。

**fragments** キーワードは、*operator [port | protocol-port]* 引数が指定されない場合だけのオプションです。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次に、toCISCO という名前の IPv6 アクセスリストを設定し、そのアクセスリストを GigabitEthernet インターフェイス 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。具体的には、リスト中の最初の拒否エントリにより、5000 を超える宛先 TCP ポート番号を持つすべてのパケットは GigabitEthernet インターフェイス 0/2/0/2 から出て行かないようになります。リスト中の 2 番目の拒否エントリにより、5000 より小さい送信元 UDP ポート番号を持つすべてのパケットは GigabitEthernet インターフェイス 0/2/0/2 から出て行かないようになります。2 番目の拒否エントリは、コンソールにもすべての一致を記録します。リスト中の最初の許可エントリは、すべての ICMP パケットが GigabitEthernet インターフェイス 0/2/0/2 から出て行くことを許可します。リスト中の 2 番目の許可エントリは、他のすべてのトラフィックが GigabitEthernet インターフェイス 0/2/0/2 から出て行くことを許可します。2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセスリストの最後にあるという理由で必要です。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group toCISCO out
```

関連コマンド

コマンド	説明
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーションモードを開始します。

コマンド	説明
<a href="#">permit (IPv6)</a> , (75 ページ)	IPv6 アクセスリストに許可条件を設定します。
<a href="#">remark (IPv6)</a> , (83 ページ)	IPv6 アクセスリスト エントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv6</a> , (88 ページ)	既存の IPv6 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

## 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**} [**hardware-count**] [**interface-statistics**]

**no ipv4 access-group** *access-list-name* {**ingress**| **egress**} [**hardware-count**] [**interface-statistics**]

### 構文の説明

access-list-name	<b>ipv4 access-list</b> コマンドで指定された IPv4 アクセスリストの名前。
ingress	着信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。
hardware-count	(任意) アクセスグループのハードウェアカウンタにアクセスするように指定します。
interface-statistics	(任意) ハードウェア内のインターフェイス単位の統計情報を指定します。

### 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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。*access-list-name* 引数を使用すると、特定の IPv4 アクセスリストを指定することができます。

**ingress** キーワードを使用すると着信パケットをフィルタリングでき、または **egress** キーワードを使用すると発信パケットをフィルタリングできます。 **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。

許可されたパケットは、**hardware-count** 引数を使用してハードウェアカウンタがイネーブルにされた場合にだけカウントされます。拒否されたパケットは、ハードウェアカウンタがイネーブルかどうかにかかわらずカウントされます。



(注) **ipv4 access-group** コマンドを使用したパケットフィルタリングアプリケーションの場合、パケットカウンタは各方向のハードウェア内に維持されます。同じ方向の複数のインターフェイス上で1つのアクセスグループを使用すると、イネーブルにされた **hardware-count** 引数を持つ各インターフェイスに対してパケットがカウントされます。

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続けます。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。

デフォルトでは、一意のまたはインターフェイス単位の ACL 統計情報はディセーブルになっています。

## タスク ID

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

## 例

次に、GigabitEthernet Packet-over-SONET (POS) インターフェイス 0/2/0/2 との間の着信または発信パケットへのフィルタリングの適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-egress-filter egress
```

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/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
interface-statistics
```



## 関連コマンド

コマンド	説明
<a href="#">clear access-list ipv4</a> , (3 ページ)	IPv4 アクセス リスト一致カウンタをリセットします。
<a href="#">deny (IPv4)</a> , (13 ページ)	IPv4 アクセスリストの拒否条件を設定します。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセスリストの許可条件を設定します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセス リストすべての内容を表示します。
<a href="#">show ipv4 interface</a>	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します。

## ipv4 access-list

IPv4 アクセス リストを名前で定義するには、グローバル 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 リスト中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

name	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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.3.0	このコマンドは、BNG でサポートされていました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv4 access-list** コマンドを使用すると、IPv4 アクセス リストを設定することができます。このコマンドはルータをアクセス リスト コンフィギュレーション モードに設定します。このモードでは、拒否または許可されたアクセス条件は **deny** or **permit** コマンドを使用して定義される必要があります。

既存の IPv4 アクセス リスト中の連続したエントリ間に **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。最初のエントリ番号 (*base*) とステートメントのエントリ番号を分け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。

**ipv4 access-group** コマンドを使用すると、アクセスリストをインターフェイスに適用することができます。

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-if)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-if)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-if)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config-if)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RSP0/CPU0:router(config-if)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
range 1300 1400
```

関連コマンド

コマンド	説明
<a href="#">clear access-list ipv4</a> , (3 ページ)	IPv4 アクセスリスト一致カウンタをリセットします。
<a href="#">deny (IPv4)</a> , (13 ページ)	名前付き IPv4 アクセスリストの拒否条件を設定します。
<a href="#">ipv4 access-group</a> , (31 ページ)	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
<a href="#">permit (IPv4)</a> , (55 ページ)	名前付き IPv4 アクセスリストの許可条件を設定します。
<a href="#">remark (IPv4)</a> , (81 ページ)	IPv4 アクセスリストエントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存の IPv4 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセスリストすべての内容を表示します。

## 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、グローバル 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

rate-number	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

デフォルトは 1 です。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

*rate-number* 引数は、インターフェイスに設定されたすべての 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	操作
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 ログイング レートを設定する方法の例を示します。

```
RP/0/RSP0/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更新数を指定するには、グローバルコンフィギュレーションモードで **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

update-number	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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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	操作
basic-services	読み取り、書き込み
acl	読み取り、書き込み

## 例

次に、ルータに設定された IPv4 アクセス リストごとに 10 の更新のロギングしきい値を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv4)</a> , (13 ページ)	IPv4 アクセスリストの拒否条件を設定します。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセスリストの許可条件を設定します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセス リストすべての内容を表示します。

## ipv6 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 **ipv6 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。

**ipv6 access-group** *access-list-name* {**ingress**|**egress**} [**interface-statistics**]

**no ipv6 access-group** *access-list-name* {**ingress**|**egress**} [**interface-statistics**]

### 構文の説明

access-list-name	<b>ipv6 access-list</b> コマンドで指定されたとおりの IPv6 アクセスリストの名前。
ingress	着信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。
interface-statistics	(任意) ハードウェア内のインターフェイス単位の統計情報を指定します。

### コマンド デフォルト

インターフェイスには、適用される IPv6 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  
L2 トランスポート

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 access-group** コマンドは、IPv6 に固有のものを除き、**ipv4 access-group** コマンドと類似しています。



**ipv6 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。**access-list-name** を使用すると、特定の IPv6 アクセスリストを指定することができます。**ingress** キーワードを使用すると着信パケットをフィルタリングすることができ、また、**egress** キーワードを使用すると発信パケットをフィルタリングすることができます。

L2 インターフェイスの IPv6 ACL に L2 トランスポート モードで **ipv6 access-group** コマンドを使用します。



(注) **ipv6 access-group** コマンドを使用したパケットフィルタリングアプリケーションの場合、パケットカウンタは各方向のハードウェア内に維持されます。同じ方向の複数のインターフェイス上で1つのアクセスグループが使用される場合、各インターフェイスでパケットがカウントされます。

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続けます。アクセスリストがアドレスを拒否する場合は、ソフトウェアはパケットをドロップして、レートが制限された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戻します。

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。

デフォルトでは、一意のまたはインターフェイス単位の ACL 統計情報はディセーブルになっています。

## タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

## 例

次に、GigabitEthernet interface 0/2/0/2 との間の着信または発信パケットへのフィルタリングの適用方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-out-filter egress
```

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/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group p-in-filter ingress interface-statistics
```

次に、L2 インターフェイス用に設定された IPv6 ACL の例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/1/0/4
RP/0/RSP0/CPU0:router(config-if)# l2transport
```

```
RP/0/RSP0/CPU0:router(config-if-12)# ipv6 access-group access-grp1 ingress
RP/0/RSP0/CPU0:router(config-if-12)# ipv6 access-group access-grp2 ingress
```

## 関連コマンド

コマンド	説明
<a href="#">copy access-list ipv6</a> , (11 ページ)	既存の IPv6 アクセス リストをコピーします。
<a href="#">deny (IPv6)</a> , (25 ページ)	IPv6 アクセス リストの拒否条件を設定します。
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv6)</a> , (75 ページ)	パケットが名前付き IPv6 アクセス リストを渡す条件を設定します。
<a href="#">show ipv6 interface</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 access-list

IPv6 アクセスリストを定義してルータを IPv6 アクセスリスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセ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。

**ipv6 access-list name**

**no ipv6 access-list name**

### 構文の説明

name	IPv6 アクセスリスト名。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
------	--

### コマンド デフォルト

定義されている IPv6 アクセスリストはありません。

### コマンド モード

グローバル コンフィギュレーション

L2 トランスポート

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 access-list** コマンドは、IPv6 に固有のものを除き、**ipv4 access-list** コマンドと類似しています。

IPv6 アクセスリストは、送信元と宛先アドレス、IPv6 オプションヘッダー、およびより細かな精度の制御のための上位層プロトコルタイプの情報に基づくトラフィックフィルタリングに使用されます。IPv6 アクセスリストは **ipv6 access-list** コマンドをグローバル コンフィギュレーション モードで使用することにより定義され、その許可と拒否の条件は **deny** および **permit** コマンドを IPv6 アクセスリスト コンフィギュレーション モードで使用することにより設定されます。**ipv6 access-list** コマンドを設定すると、ルータを IPv6 アクセスリスト コンフィギュレーション モードに設定し、プロンプト `router` は `router (config-ipv6-acl)#` に変わります。IPv6 アクセスリストコン

フィギュレーションモードから、定義済みの IPv6 アクセスリストに許可および拒否の条件を設定できます。

L2 インターフェイスの IPv6 ACL に I2 トランスポートモードで **ipv6 access-list** コマンドを使用します。

IPv6 オプションヘッダーおよび省略可能な上位層プロトコルタイプ情報に基づく IPv6 トラフィックのフィルタリングの詳細については、[deny \(IPv6\)](#)、(25 ページ) および [permit \(IPv6\)](#)、(75 ページ) コマンドを参照してください。変換済み IPv6 アクセスコントロールリスト (ACL) コンフィギュレーションの例については、「例」を参照してください。



(注) 方向単位に 1 つのインターフェイスに適用できる IPv6 アクセスリストは 1 つだけです。



(注) どの IPv6 アクセスリストにも最後の一致条件として暗黙の **deny ipv6 any any** ステートメントがあります。1 つの IPv6 アクセスリストには、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。



(注) アクセスリストでなく、IPv6 プレフィックスリストは、ルーティングプロトコルプレフィックスのフィルタリングに使用する必要があります。

*access-list-name* 引数を持つ **ipv6 access-group** インターフェイス コンフィギュレーションコマンドを使用すると、IPv6 アクセスリストを IPv6 インターフェイスに適用することができます。



(注) **ipv6 access-group** コマンドを持つインターフェイスに適用される IPv6 アクセスリストは、ルータが発信でなく転送するトラフィックをフィルタリングします。



(注) すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および **deny ipv6 any any** ステートメントがあります (元の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります)。1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。 **permit icmp any any nd-na permit icmp any any nd-ns deny ipv6 any any deny ipv6 any any**

IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル (ARP) では、個別のデータリンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

## タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

## 例

次に、list2 という名前の IPv6 アクセス リストの設定してその ACL をインターフェイス GigabitEthernet 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。具体的には、1 番目の ACL エントリにより、ネットワーク fec0:0:0:2::/64 (発信元 IPv6 アドレスの 1 番目の 64 ビットのようなサイトローカルプレフィックス fec0:0:0:2) からのすべてのパケットがインターフェイス GigabitEthernet 0/2/0/2 から出て行くのが防止されます。ACL の 2 番目のエントリは、その他のすべてのトラフィックがインターフェイス GigabitEthernet 0/2/0/2 から出て行くことを許可します。2 番目のエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list list2
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit any any

RP/0/RSP0/CPU0:router# show ipv6 access-lists list2

ipv6 access-list list2
 10 deny ipv6 fec0:0:0:2::/64 any
 20 permit ipv6 any any

RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group list2 out
```



(注) IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。



(注) IPv6 ルータは、送信元または宛先アドレスのいずれかとしてリンクローカルアドレスを持つ別のネットワークの IPv6 パケットに転送されません (パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります)。

次に、L2 インターフェイス用に設定された IPv6 ACL の例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet 0/1/0/4
RP/0/RSP0/CPU0:router(config-if)# l2transport
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-list LIST1 ingress
RP/0/RSP0/CPU0:router(config-if-l2)# ipv6 access-list LIST2 ingress
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv6)</a> , ( <a href="#">25 ページ</a> )	IPv6 アクセスリストの拒否条件を設定します。
<a href="#">permit (IPv6)</a> , ( <a href="#">75 ページ</a> )	IPv6 アクセスリストの許可条件を設定します。
<a href="#">remark (IPv6)</a> , ( <a href="#">83 ページ</a> )	IPv6 アクセスリスト エントリに関する有益な設定を挿入します。

## ipv6 access-list log-update rate

IPv6 アクセスリストが記録されるレートを指定するには、グローバル コンフィギュレーション モードで **ipv6 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。

**ipv6 access-list log-update rate** *rate-number*

**no ipv6 access-list log-update rate** *rate-number*

### 構文の説明

rate-number	ルータ上で IPv6 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

デフォルトは 1 です。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

*rate-number* 引数は、インターフェイスに設定されたすべての IPv6 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	操作
ipv6	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 IPv6 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/RSP0/CPU0:router(config)# ipv6 access-list log-update rate 10
```



## ipv6 access-list log-update threshold

IPv6アクセスリスト（ACL）に記録される更新数を指定するには、グローバルコンフィギュレーションモードで **ipv6 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。

**ipv6 access-list log-update threshold** *update-number*

**no ipv6 access-list log-update threshold** *update-number*

### 構文の説明

update-number	ルータに設定された IPv6 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

IPv6 アクセス リストの場合、350000 の更新が記録されます。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 access-list log-update threshold** コマンドは、IPv6 固有のものを除き、**ipv4 access-list log-update threshold** コマンドと類似しています。

IPv6 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	操作
acl	読み取り、書き込み

タスク ID	操作
ipv6	読み取り、書き込み

**例**

次に、ルータに設定された IPv6 アクセス リストごとに 10 の更新のロギングしきい値を設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list log-update threshold 10
```

# ipv6 access-list maximum ace threshold

IPv6 アクセスリストのアクセスコントロールエントリ (ACE) の最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list maximum ace threshold** コマンドを使用します。IPv6 アクセスリストの ACE 制限をリセットするには、このコマンドの **no** 形式を使用します。

**ipv6 access-list maximum ace threshold** *ace-number*

**no ipv6 access-list maximum ace threshold** *ace-number*

構文の説明	<p><b>ace-number</b> ACE の設定可能最大数。範囲は 50000 ~ 350000 です。</p>
-------	--

**コマンド デフォルト** IPv6 アクセス リストでは、50,000 の ACE が設定可能です。

**コマンド モード** グローバル コンフィギュレーション

<b>コマンド履歴</b>	<table border="1"> <tr> <th style="width: 40%;">リリース</th> <th>変更箇所</th> </tr> <tr> <td>リリース 3.7.2</td> <td>このコマンドが導入されました。</td> </tr> </table>	リリース	変更箇所	リリース 3.7.2	このコマンドが導入されました。
リリース	変更箇所				
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 access-list maximum ace threshold** コマンドを使用すると、IPv6 アクセス リストの ACE の設定可能最大数を設定することができます。Out Of Resource (OOR) は、システムに設定可能な ACE 数を制限します。ACE の設定可能最大数に達した場合、新しい ACE の設定は拒否されます。

<b>タスク ID</b>	<table border="1"> <tr> <th style="width: 30%;">タスク ID</th> <th>操作</th> </tr> <tr> <td>acl</td> <td>読み取り、書き込み</td> </tr> <tr> <td>ipv6</td> <td>読み取り、書き込み</td> </tr> </table>	タスク ID	操作	acl	読み取り、書き込み	ipv6	読み取り、書き込み
タスク ID	操作						
acl	読み取り、書き込み						
ipv6	読み取り、書き込み						

## 例

次に、IPv6 アクセス リストの ACE の最大数を 75000 に設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list maximum ace threshold 75000
```

## 関連コマンド

コマンド	説明
<a href="#">show access-lists ipv6, (98 ページ)</a>	現在のすべての IPv6 アクセス リストの内容を表示します。

## ipv6 access-list maximum acl threshold

IPv6 アクセス コントロール リスト (ACL) の設定可能最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list maximum acl threshold** コマンドを使用します。IPv6 ACL 制限をリセットするには、このコマンドの **no** 形式を使用します。

**ipv6 access-list maximum acl threshold** *acl-number*

**no ipv6 access-list maximum ace threshold** *acl-number*

### 構文の説明

*acl-number* ACL の設定可能最大数。範囲は 1000 ~ 16000 です。

### コマンド デフォルト

1000 の IPv6 ACL を設定できます。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 access-list maximum acl threshold** コマンドを使用すると、IPv6 ACL の設定可能最大数を設定することができます。Out Of Resource (OOR) は、システムに設定可能な ACL 数を制限します。この制限に達すると、新しい ACL が拒否されます。

### タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

## 例

次に、IPv6 ACL の設定可能最大数を 1500 に設定する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list maximum acl threshold 1500
```

## 関連コマンド

コマンド	説明
<a href="#">show access-lists ipv6, (98 ページ)</a>	現在のすべての IPv6 アクセス リストの内容を表示します。

## 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 (source)**、および **permit (protocol)** 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 source source-wildcard destination destination-wildcard [capture]
[precedence precedence] [default nexthop [ ipv4-address1 ] [ ipv4-address2 ] [ ipv4-address3 ]] [dscp dscp]
[fragments] [log| log-input] [nexthop [track track-name] [ ipv4-address1 ] [ ipv4-address2 ] [ ipv4-address3 ]]
[ttl ttl value [value1 ... value2]]
```

```
no sequence-number
```

### Internet Control Message Protocol (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]
```

### Internet Group Management Protocol (IGMP)

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

### User Datagram Protocol (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]
```

#### 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、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます)。 **resequence access-list** コマンドを使用すると、設定済みアクセスリスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。

---

source	<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"><li>• 32 ビットの 4 分割ドット付き 10 進表記を使用する。</li><li>• <b>any</b> キーワードを、0.0.0.0 255.255.255.255 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li><li>• <b>host source</b> の組み合わせを、<i>source</i> 0.0.0.0 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li></ul>
source-wildcard	<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"><li>• 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。</li><li>• <b>any</b> キーワードを、0.0.0.0 255.255.255.255 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li><li>• <b>host source</b> の組み合わせを、<i>source</i> 0.0.0.0 の <i>source</i> および <i>source-wildcard</i> の短縮形として使用する。</li></ul>

---



protocol	<p>IP プロトコルの名前または番号。キーワード <b>ahp</b>、<b>esp</b>、<b>eigrp</b>、<b>gre</b>、<b>icmp</b>、<b>igmp</b>、<b>igrp</b>、<b>ip</b>、<b>ipinip</b>、<b>nos</b>、<b>ospf</b>、<b>pim</b>、<b>pcp</b>、<b>tcp</b>、または <b>udp</b> のいずれか1つ、あるいは IP プロトコル番号を表す 0 ~ 255 の整数にすることができます。任意のインターネットプロトコル (ICMP、TCP、および UDP を含む) に一致させるには、<b>ip</b> 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>
destination	<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"><li>• 32 ビットの 4 分割ドット付き 10 進表記を使用する。</li><li>• <b>any</b> キーワードを、0.0.0.0 255.255.255.255 の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li><li>• <b>host destination</b> の組み合わせを、<i>destination</i> 0.0.0.0 の <i>destination</i> および <i>destination-wildcard</i> の短縮形として使用する。</li></ul>

---

**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、0.0.0.0 255.255.255.255 の *destination* および *destination-wildcard* の短縮形として使用する。
  - **host destination** の組み合わせを、*destination* 0.0.0.0 の *destination* および *destination-wildcard* の短縮形として使用する。
-

---

**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** : パケットを routine precedence (0) と一致させます。
  - **priority** : パケットを priority precedence (1) と一致させます。
  - **immediate** : パケットを immediate precedence (2) と一致させます。
  - **flash** : パケットを flash precedence (3) と一致させます。
  - **flash-override** : パケットを flash override precedence (4) と一致させます。
  - **critical** : パケットを critical precedence (5) と一致させます。
  - **internet** : パケットを internetwork control precedence (6) と一致させます。
  - **network** : パケットを network control precedence (7) と一致させます。
-

---

**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り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を指定しない場合だけとなります。

---

**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で **acl** コマンドを設定するときに、ACL コンフィギュレーションコマンドが **capture** キーワードを使用しない場合、トラフィックはミラーリングされません。ACL 設定が **capture** キーワードを使用し、**acl** コマンドが送信元ポートで設定されていない場合、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。



fragments	(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。
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。(コンソールに記憶されるメッセージのレベルは <b>logging console</b> 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せん。</p>
log-input	(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、 <b>log</b> キーワードと同じ機能を提供します。
nexthop1、nexthop2、nexthop3	(任意) このエントリの指定されたネクストホップを転送します。
<b>track</b> <i>track-name</i>	このネクストホップの TRACK 名を指定します。
ttl	(任意) Time-To-Life (TTL) 値との一致をオンにします。

<code>ttl value [value1 ... value2]</code>	<p>(任意) フィルタリングに使用される TTL 値 値の範囲は 1 ～ 255 です。</p> <p><i>value</i> が指定される場合にだけ、この値に対する一致になります。</p> <p><i>value1</i> および <i>value2</i> の両方が指定された場合、<i>value1</i> と <i>value2</i> の間の TTL の範囲に対してパケット TTL が一致されます。</p>
<code>icmp-off</code>	<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>
<code>icmp-type</code>	<p>(任意) ICMP パケットのフィルタリングのための ICMP メッセージタイプ。範囲は 0 ～ 255 です。</p>
<code>icmp-code</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>
<code>igmp-type</code>	<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"><li>• dvmrp</li><li>• host-query</li><li>• host-report</li><li>• mtrace</li><li>• mtrace-response</li><li>• pim</li><li>• precedence</li><li>• トレース</li><li>• v2-leave</li><li>• v2-report</li><li>• v3-report</li></ul>

operator	<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。オペランドとして使用可能なものには、<b>lt</b> (less than : より小さい) 、 <b>gt</b> (greater than : より大きい) 、 <b>eq</b> (equal : 等しい) 、 <b>neq</b> (not equal : 等しくない) 、 および <b>range</b> (inclusive range : 包含範囲) があります。</p> <p>演算子を <i>source</i> および <i>source-wildcard</i> の値の後に置く場合、送信元ポートと一致する必要があります。</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 <b>ttl</b> キーワードの後に置く場合、TTL 値と一致します。</p> <p><b>range</b> 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>
port	<p>TCP または UDP ポートの 10 進数。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>
protocol-port	<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 <b>match-any</b> 、 <b>match-all</b> の場合、プレフィックス <i>flag-name</i> の前に + または - を付けます。TCP フラグを設定したパケットを一致させるには、 <i>+flag-name</i> 引数を使用します。TCP フラグを設定していないパケットを一致させるには、 <i>-flag-name</i> 引数を使用します。
flag-name	(任意) TCP プロトコルが <b>match-any</b> 、 <b>match-all</b> の場合。フラグの名前は、 <b>ack</b> 、 <b>fin</b> 、 <b>psh</b> 、 <b>rst</b> 、 <b>syn</b> になります。

## 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 リストの設定

## コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.0.1	<b>capture</b> キーワードが追加されました。

**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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv4 access-list** コマンドに続いて **permit** コマンドを使用すると、パケットがアクセス リストを通過できる条件を指定することができます。

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。

**permit**、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。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。

2 つの連続した番号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、最初に **resequence access-list** コマンドを使用して、最初のステートメントに番号を付け直して、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。

次に、**precedence** の名前のリストを示します。

- critical
- flash
- flash-override
- immediate
- internet
- ネットワーク
- 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。ポート番号の位置に ? を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- ホスト名
- 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。?を入力すると、これらのプロトコルに対応するポート番号を見つけることができます。

- 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することができます。

- ack
- fin
- psh
- rst
- syn

たとえば、**match-all + ack + syn** は TCP パケットを ack および syn フラグを設定して表示し、**match-any + ack - syn** は TCP パケットを ack を設定するか syn を設定しないで表示します。

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RSP0/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/RSP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

関連コマンド

コマンド	説明
<a href="#">deny (IPv4) , (13 ページ)</a>	IPv4 アクセスリストの条件を設定します。
<a href="#">ipv4 access-group, (31 ページ)</a>	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
<a href="#">ipv4 access-list , (34 ページ)</a>	IPv4 アクセスリストを定義し、また、IPv4 アクセスリスト コンフィギュレーション モードを開始します。
<a href="#">remark (IPv4) , (81 ページ)</a>	IPv4 アクセスリスト エントリに関する有益な設定を挿入します。

コマンド	説明
<a href="#">deny (IPv4)</a> , (13 ページ)	<b>IPv4</b> アクセス リストの条件を設定します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存の IPv4 アクセス リスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセス リストすべての内容を表示します。

## permit (IPv6)

IPv6 アクセスリストの許可条件を設定するには、IPv6 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。許可条件を削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] permit protocol {source-ipv6-prefix/ prefix-length | any | host
source-ipv6-address} [operator {port | protocol-port} capture ] [dscp value] [routing] [authen] [destopts]
[ fragments] [packet-length operator packet-length value ] [ log | log-input] [ttl operator ttl value ][default]
nexthop1 [vrf vrf-name-1] [ipv6 ipv6-address-1] [nexthop2 [vrf vrf-name-2] [ipv6 ipv6-address-2] [nexthop3
[vrf vrf-name-3] [ipv6 ipv6-address-3]]]
no sequence-number
```

### Internet Control Message Protocol (ICMP)

```
[ sequence-number] permit icmp {source-ipv6-prefix/ prefix-length | any | host
source-ipv6-address} {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [icmp-type]
[ icmp-code][dscp value] [ routing] [authen] [destopts] [ fragments] [ log] [log-input] [icmp-off]
```

### Transmission Control Protocol (TCP)

```
[sequence-number] permit tcp {source-ipv6-prefix/ prefix-length | any | host
source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/ prefix-length | any | host
destination-ipv6-address} [operator {port | protocol | port}] [dscp value] [routing] [authen] [destopts]
[fragments] [established] {match-any | match-all | + | -} [flag-name] [log] [log-input]
```

### User Datagram Protocol (UDP)

```
[sequence-number] permit tcp {source-ipv6-prefix/ prefix-length | any | host
source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/ prefix-length | any | host
destination-ipv6-address} [operator {port | protocol | port}] [dscp value] [routing] [authen] [destopts]
[fragments] [established] [flag-name] [log] [log-input]
```

#### 構文の説明

sequence-number	(任意) アクセスリスト中の <b>permit</b> 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、最初のステートメントの番号は 10 で、後続のステートメントは 10 ずつ増加していきます)。 <b>resequence access-list</b> コマンドを使用すると、設定済みアクセスリスト中の最初のステートメントの番号を変更し、後続のステートメントの番号を増加することができます。
protocol	インターネットプロトコルの名前または番号。次のキーワードのいずれかになります。 <b>ahp</b> 、 <b>eigrp</b> 、 <b>esp</b> 、 <b>gre</b> 、 <b>icmp</b> 、 <b>igmp</b> 、 <b>igrp</b> 、 <b>isnip</b> 、 <b>ipv6</b> 、 <b>nos</b> 、 <b>ospf</b> 、 <b>pep</b> 、 <b>sctp</b> 、 <b>tcp</b> 、 <b>or udp</b> 、または IPv6 プロトコル番号を表す 0 ~ 255 の範囲の整数。

<i>source-ipv6-prefix / prefix-length</i>	許可条件が設定される送信元の IPv6 ネットワークまたはネットワークのクラス。  この引数は、RFC 2373 に記載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。
any	IPv6 プレフィックス ::0 の省略形。
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で <b>acl</b> コマンドを設定するときに、ACL コンフィギュレーションコマンドが <b>capture</b> キーワードを使用しない場合、トラフィックはミラーリングされません。ACL 設定が <b>capture</b> キーワードを使用し、 <b>acl</b> コマンドが送信元ポートで設定されていない場合、ポートトラフィック全体がミラーリングされ、 <b>capture</b> アクションは影響を受けません。
<b>host</b> <i>source-ipv6-address</i>	許可条件の設定先に関する、送信元の IPv6 ホストアドレス。  <i>source-ipv6-address</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
<b>vrf vrf-name</b>	VPN ルーティング/転送 (VRF) インスタンスを指定します。
<b>nexthop1、 nexthop2、nexthop3</b>	(任意) このエントリのネクストホップを指定します。
<i>operator {port   protocol-port}</i>	(任意) 指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。オペランドには、 <b>lt</b> (less than : より小さい)、 <b>gt</b> (greater than : より大きい)、 <b>eq</b> (equal : 等しい)、 <b>neq</b> (not equal : 等しくない)、および <b>range</b> (inclusive range : 包含範囲) があります。  <i>source-ipv6-prefix / prefix-length</i> 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。  <i>destination-ipv6-prefix / prefix-length</i> 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。  <b>range</b> 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。  <i>port</i> 引数は、TCP または UDP ポートの 16 進数です。ポート番号の範囲は 0 ~ 65535 です。 <i>protocol-port</i> 引数は、TCP または UDP ポートの名前です。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せん。

<i>destination-ipv6-prefix / prefix-length</i>	許可条件が設定される宛先の IPv6 ネットワークまたはネットワークのクラス。  この引数は、RFC 2373 に記載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。
<b>host</b> <i>destination-ipv6-address</i>	許可条件が設定される宛先の IPv6 ホスト アドレスを指定します。 <i>destination-ipv6-address</i> 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
<b>dscp value</b>	(任意) DiffServ コードポイント (DSCP) 値を、各 IPv6 パケットヘッダーの Traffic Class フィールドのトラフィッククラス値に一致させます。範囲は 0 ~ 63 です。
ルーティング	(任意) ソースルートパケットを、各 IPv6 パケットヘッダー内の拡張ヘッダーに一致させます。
authen	(任意) IPv6 認証ヘッダーが存在する場合に一致します。
destopts	(任意) IPv6 宛先オプションヘッダーが存在する場合に一致します。
fragments	(任意) フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれているフラグメント化された非初期パケットと一致させます。 <b>fragments</b> キーワードは、 <i>operator [port-number]</i> 引数が指定されていない場合に限り指定できるオプションです。
log	(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。(コンソールに記憶されるメッセージのレベルは <b>logging console</b> コマンドで制御します)  このメッセージに含まれるものには、アクセスリスト名とシーケンス番号、パケットが許可されているか、プロトコルが TCP、UDP、ICMP、または番号であるか、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。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で、その 5 分間隔の前に許可されたパケット数を含めて生成されます。
log-input	(任意) <b>log</b> キーワードと同じ機能を提供しますが、ロギングメッセージに入力インターフェイスも含まれます。
ttl	(任意) 存続可能時間 (TTL) 値との一致をオンにします。
operator	(任意) 指定されたプロトコルの送信元ポートまたは宛先ポートを比較するオペランド。オペランドには、 <b>lt</b> (less than : より小さい) 、 <b>gt</b> (greater than : より大きい) 、 <b>eq</b> (equal : 等しい) 、 <b>neq</b> (not equal : 等しくない) 、および <b>range</b> (inclusive range : 包含範囲) があります。

<i>ttl value</i> [ <i>value1 value2</i> ]	(任意) フィルタリングに使用される TTL 値 範囲は 1 ~ 255 です。 <i>value</i> が指定される場合にだけ、この値に対する一致になります。 <i>value1</i> および <i>value2</i> の両方が指定された場合、 <i>value1</i> と <i>value2</i> の間の TTL の範囲に対してパケット TTL が一致されます。
<i>icmp-off</i>	(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。
<i>icmp-type</i>	(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。
<i>icmp-code</i>	(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。
<i>established</i>	(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。
<i>match-any</i>	(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。
<i>match-all</i>	(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 <b>match-any</b> 、 <b>match-all</b> の場合、プレフィックス <i>flag-name</i> の前に + または - を付けます。 TCP フラグを設定したパケットを一致させるには、+ <i>flag-name</i> 引数を使用します。 TCP フラグを設定していないパケットを一致させるには、- <i>flag-name</i> 引数を使用します。
<i>flag-name</i>	(必須) TCP プロトコルが <b>match-any</b> 、 <b>match-all</b> の場合。 フラグの名前は、 <b>ack</b> 、 <b>fin</b> 、 <b>psh</b> 、 <b>rst</b> 、 <b>syn</b> になります。

## コマンド デフォルト

IPv6 アクセス リストは定義されていません。  
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

IPv6 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 3.7.2	このコマンドが追加されました。
リリース 4.0.1	<b>capture</b> キーワードが追加されました。

リリース	変更内容
リリース 4.2.0	VRF-Aware ABF に対して IPv6 サポートがイネーブルにされています。

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**permit (IPv6)** コマンドは、IPv6 に固有のものを除き、**permit (IPv4)** コマンドと類似しています。

**ipv6 access-list** コマンドに続いて、**permit (IPv6)** コマンドを使用すると、パケットがアクセス リストを通過する条件を定義することができます。

*protocol* 引数に **ipv6** を指定すると、パケットの IPv6 ヘッダーを一致対象とします。

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の番号は 10 で、その次のステートメントからは 10 ずつ増加します。

**permit**、**deny**、または **remark** ステートメントを、リスト全体を再入力せずに既存のアクセス リストに追加できます。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。

*source-ipv6-prefix/prefix-length* および *destination-ipv6-prefix/prefix-length* の引数は両方とも、トラフィック フィルタリング（送信元プレフィックスがトラフィック送信元に基づいてトラフィックをフィルタリングし、送信先プレフィックスがトラフィック宛先に基づいてトラフィックをフィルタリングする）に使用されます。



(注) アクセスリストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

**fragments** キーワードは、*operator [port | protocol-port]* 引数が指定されない場合だけに使用可能なオプションです。

タスク ID

タスク ID	操作
acl	読み取り、書き込み

例

次に、toCISCO という名前の IPv6 アクセス リストを設定し、そのアクセス リストを GigabitEthernet interface 0/2/0/2 上の発信トラフィックに適用する方法の例を示します。具体的には、リスト中の

最初の拒否エントリにより、5000 を超える宛先 TCP ポート番号を持つすべてのパケットは GigabitEthernet interface 0/2/0/2 から出て行かないようになります。リスト中の 2 番目の拒否エントリによって、5000 より小さい、送信元 UDP ポート番号を持つすべてのパケットは GigabitEthernet interface 0/2/0/2 から出て行かないようになります。2 番目の拒否エントリは、コンソールにもすべての一致を記録します。リスト中の最初の許可エントリは、すべての ICMP パケットが GigabitEthernet interface 0/2/0/2 から出て行くことを許可します。リスト中の 2 番目の許可エントリは、他のすべてのトラフィックが GigabitEthernet interface 0/2/0/2 から出て行くことを許可します。2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセスリストの最後にあるという理由で必要です。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list toCISCO
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RSP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# permit any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group toCISCO out
```

次に、v6-abf-acl という名前の IPv6 アクセスリストを設定し、そのアクセスリストを GigabitEthernet interface 0/0/2/0 上の着信トラフィックに適用する方法の例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list v6-abf-acl
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 any any default nexthop1 vrf vrf_A
ipv6 11:::1 nexthop2 vrf vrf_B ipv6 22:::2 nexthop3 vrf vrf_C ipv6 33:::3
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit ipv4 any any
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/0/2/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 access-group v6-abf-acl ingress
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv6)</a> , (25 ページ)	IPv6 アクセスリストに拒否条件を設定します。
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。
<a href="#">remark (IPv6)</a> , (83 ページ)	IPv6 アクセスリスト エントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv6</a> , (88 ページ)	既存の IPv6 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。



## remark (IPv4)

IPv4 アクセス リスト中のエントリに有益なコメント（注釈）を書くには、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

sequence-number	(任意) アクセス リスト中の <b>remark</b> 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 リストの設定

### コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**remark** コマンドを使用すると、IPv4 アクセス リスト中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。

削除する注釈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せん。

既存のアクセスリストにステートメントを追加する場合に **resequence access-list ipv4** コマンドを使用すると、連続したエントリのシーケンス番号は追加ステートメントを許可しなくなります。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RSP0/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
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv4)</a> , (13 ページ)	IPv4 アクセスリストの拒否条件を設定します。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセスリストを定義し、また、IPv4 アクセスリスト コンフィギュレーションモードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセスリストの許可条件を設定します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存の IPv4 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセスリストすべての内容を表示します。

## remark (IPv6)

IPv6 アクセス リスト中のエントリに有益なコメント（注釈）を書くには、IPv6 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

sequence-number	(任意) アクセス リスト中の <b>remark</b> 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

IPv6 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

IPv6 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 3.7.2	このコマンドが追加されました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**remark (IPv6)** コマンドは、IPv6 に固有のものを除き、**remark (IPv4)** コマンドと類似しています。

**remark** コマンドを使用すると、IPv6 アクセス リスト中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。

削除する注釈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せん。

既存のアクセスリストにステートメントを追加する場合に `resequence access-list ipv6` コマンドを使用すると、連続したエントリのシーケンス番号は追加ステートメントを許可しなくなります。

## タスク ID

タスク ID	操作
acl	読み取り、書き込み

## 例

次の例では、1つの注釈が追加されています。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 3333:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 20 permit ipv6 4444:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 30 permit ipv6 5555:1:2:3::/64 any
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 39 remark Block BGP traffic from a given host
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 40 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RSP0/CPU0:router# show ipv6 access-list Internetfilter

ipv6 access-list Internetfilter
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
 39 remark Block BGP traffic from a given host
 40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range host 6666:1:2:3::10 eq
bgp host 7777:1:2:3::20 range 1300 1400
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv6)</a> , (25 ページ)	IPv6 アクセスリストの拒否条件を設定します。
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv6)</a> , (75 ページ)	IPv6 アクセスリストの許可条件を設定します。
<a href="#">resequence access-list ipv6</a> , (88 ページ)	既存の IPv6 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

## resequence access-list ipv4

既存のステートメントに番号を付け直し、後続のステートメントの番号を増加させて、新しいIPv4 アクセスリストステートメント (**permit**、**deny**、または **remark**) を追加できるようにするには、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

name	IPv4 アクセス リストの名前。
base	(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。デフォルトは 10 です。
increment	(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。デフォルトは 10 です。

### コマンド デフォルト

```
base: 10
increment: 10
```

### コマンド モード

```
EXEC
```

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**resequence access-list ipv4** コマンドを使用すると、**permit**、**deny**、または **remark** ステートメントを既存の IPv4 アクセス リスト中の連続したエントリ間に追加することができます。最初のエントリ番号 (*base*) とステートメントのエントリ番号を分け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	操作
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としています。

```
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
```

アクセスリスト中に追加エントリを追加する場合は次のようにします。最初に、エントリに順番を付け直して（ステートメントを番号 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 4 つの追加ステートメントを挿入できるスペースを取ります。

```
RP/0/RSP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RSP0/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/RSP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RSP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RSP0/CPU0:router# show access-lists ipv4 marketing
```

```
ipv4 access-list marketing
 3 remark Do not allow user1 to telnet out
 4 deny tcp host 171.69.2.88 255.255.0.0 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
```

## 関連コマンド

コマンド	説明
<a href="#">deny (IPv4)</a> , (13 ページ)	IPv4 アクセスリストの拒否条件を設定します。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセスリストを定義し、また、IPv4 アクセスリスト コンフィギュレーションモードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセスリストの許可条件を設定します。

コマンド	説明
<a href="#">remark (IPv4)</a> , (81 ページ)	IPv4 アクセス リストに関する有益な注釈を挿入します。
<a href="#">show access-lists ipv4</a> , (92 ページ)	現在の IPv4 アクセス リストすべての内容を表示します。

## resequence access-list ipv6

既存のステートメントに番号を付け直して後続のステートメントの番号を増加させて、新しいIPv6 アクセスリストステートメント (**permit**、**deny**、または **remark**) を追加できるようにするには、EXEC モードで **resequence access-list ipv6** コマンドを使用します。

**resequence access-list ipv6 name [base [ increment ]]**

### 構文の説明

name	IPv6 アクセス リストの名前。
base	(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 2147483646 です。デフォルトは 10 です。
increment	(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。デフォルトは 10 です。

### コマンド デフォルト

base: 10  
increment: 10

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**resequence access-list ipv6** コマンドは、IPv6 に固有のものを除き、**resequence access-list ipv4** コマンドと類似しています。

**resequence access-list ipv6** コマンドを使用すると、**permit**、**deny**、または **remark** ステートメントを既存の IPv6 アクセス リスト中の連続したエントリ間に追加することができます。最初のエントリ番号 (*base*) とステートメントのエントリ番号を分けるための増分を指定します。既存のス



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	操作
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しています。

```
ipv6 access-list Internetfilter
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

アクセスリスト中に追加エントリを追加する場合は次のようにします。最初に、エントリに番号を付け直して（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 4 つの追加ステートメントを挿入できるスペースを取ります。

```
RP/0/RSP0/CPU0:router# resequence access-list ipv6 Internetfilter 20 5
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter
```

```
ipv6 access-list Internetfilter
 20 permit ipv6 3333:1:2:3::/64 any
 25 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

これで、新しいエントリを追加できます。

```
RP/0/RSP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 3 remark Block BGP traffic from a given host
RP/0/RSP0/CPU0:router(config-ipv6-acl)# 4 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter
```

```
ipv6 access-list Internetfilter
 3 remark Block BGP traffic from a given host
 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
 20 permit ipv6 3333:1:2:3::/64 any
 25 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

関連コマンド

コマンド	説明
<a href="#">deny (IPv6)</a> , <a href="#">(25 ページ)</a>	IPv6 アクセスリストの拒否条件を設定します。
<a href="#">ipv6 access-list</a> , <a href="#">(43 ページ)</a>	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーションモードを開始します。
<a href="#">permit (IPv6)</a> , <a href="#">(75 ページ)</a>	IPv6 アクセスリストの許可条件を設定します。

コマンド	説明
remark (IPv6) , (83 ページ)	IPv6 アクセスリスト エントリに関する有益な設定を挿入します。

## 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、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、キーワードと引数はありません。

#### コマンドモード

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
acl	読み取り

#### 例

次に、**show access-lists afi-all** コマンドからの出力例を示します。

```
RP/0/RSP0/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、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 interface-path-id]
{sequence number|location node-id}| summary [ access-list-name ]| access-list-name [ sequence-number ]|
maximum [detail] [usage pfilter {location node-id|all}]]
```

### 構文の説明

<b>access-list-name</b>	(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。
<b>hardware</b>	(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。
<b>ingress</b>	(任意) 着信インターフェイスを指定します。
<b>egress</b>	(任意) 発信インターフェイスを指定します。
<b>interface</b>	(任意) インターフェイス統計情報を表示します。
<b>type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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。
<b>sequence number</b>	(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。
<b>location node-id</b>	(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。
<b>summary</b>	(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。
<b>sequence-number</b>	(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。
<b>maximum</b>	(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** EXEC

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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することができます。

**hardware**、**ingress** または **egress**、および **location** キーワードを使用すると、ハードウェア内容、および指定された方向 (入力または出力) の指定されたアクセス リストを使用するすべてのインターフェイスのアクセス リストを表示することができます。特定のアクセス リストエントリの内容を表示するには、**sequence number** キーワードおよび引数を使用します。インターフェイスのアクセス グループは、イネーブルにするアクセス リスト ハードウェア カウンタ用の **ipv4 access-group** コマンドを使用して設定する必要があります。

**show access-lists ipv4 summary** コマンドを使用すると、現在のすべての IPv4 アクセス リストのサマリーを表示することができます。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 の詳細を表示することができます。 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、指定されたラインカードにプログラミングされたすべてのインターフェイスおよびアクセ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	操作
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/RSP0/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
```

次の例では、**acl\_hw\_1** という名前のアクセスリストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv4 acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
 20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
 30 deny tcp any any (58 hw matches)
```

次の表に、この出力で表示される重要なフィールドについて説明します。

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
next-hop	ネクストホップがプログラミングされ、FIB から到達可能。
ACL name	ハードウェアにプログラミングされた ACL の名前。

フィールド	説明
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。
Statistics pointer	Statistics pointer は、ハードウェア カウンタに割り当てられたポインタです。
Number of TCAM entries	ACE をハードウェアにプログラミングするために使用される TCAM エントリの数。

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/RSP0/CPU0:router# show access-lists ipv4 summary
```

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

次の表に、この出力で表示される重要なフィールドについて説明します。

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/RSP0/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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

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

#### 関連コマンド

コマンド	説明
<a href="#">clear access-list ipv4</a> , (3 ページ)	IPv4 アクセス リスト一致カウンタをリセットします。
<a href="#">copy access-list ipv4</a> , (9 ページ)	既存の IPv4 アクセス リストをコピーします。
<a href="#">deny (IPv4)</a> , (13 ページ)	IPv4 アクセス リストの拒否条件を設定します。
<a href="#">ipv4 access-group</a> , (31 ページ)	インターフェイス上の着信または発信の IPv4 トラフィックをフィルタリングします。
<a href="#">ipv4 access-list</a> , (34 ページ)	IPv4 アクセス リストを定義し、また、IPv4 アクセス リスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv4)</a> , (55 ページ)	IPv4 アクセス リストの許可条件を設定します。



コマンド	説明
<a href="#">remark (IPv4)</a> , (81 ページ)	IPv4 アクセスリスト エントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv4</a> , (85 ページ)	既存の IPv4 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。

## show access-lists ipv6

現在の IPv6 アクセス リストの内容を表示するには、EXEC モードで **show access-lists ipv6** コマンドを使用します。

```
show access-lists ipv6 [access-list-name hardware {ingress|egress} [interface type interface-path-id]
{sequence number|location node-id}| summary [ access-list-name ]| access-list-name [ sequence-number ]|
maximum [detail] [usage pfilter {location node-id|all}]]
```

### 構文の説明

access-list-name	(任意) 特定の IPv6 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	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。
type	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

<b>interface-path-id</b>	<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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> </ul> <p>(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に関しては、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</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul> <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>
<b>sequence number</b>	(任意) 特定の IPv6 アクセス リストのシーケンス番号。範囲は 1 ~ 2147483644 です。
<b>location node-id</b>	(任意) 特定の IPv6 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。
<b>summary</b>	(任意) 現在のすべての IPv6 アクセス リストのサマリーを表示します。
<b>sequence-number</b>	(任意) 特定の IPv6 アクセス リストのシーケンス番号。範囲は 1 ~ 2147483644 です。
<b>maximum</b>	(任意) IPv6 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。
<b>detail</b>	(任意) 完全な <i>out-of-resource</i> (OOR) の詳細を表示します。
<b>usage</b>	(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。
<b>pfilter</b>	(任意) 指定されたラインカードの packets フィルタリングの使用方法を表示します。
<b>all</b>	(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** すべての IPv6 アクセス リストを表示します。

**コマンド モード** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show access-list ipv6** コマンドは、IPv6 に固有のものを除き、**show access-list ipv4** コマンドと類似しています。

**show access-lists ipv6** コマンドを使用すると、すべての IPv6 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 IPv6 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することができます。

**hardware**、**ingress** または **egress**、および **location** キーワードを使用すると、ハードウェア内容、および指定された方向（入力または出力）の指定されたアクセス リストを使用するすべてのインターフェイスのアクセス リストを表示することができます。特定のアクセス リスト エントリの内容を表示するには、**sequence number** キーワードおよび引数を使用します。インターフェイスのアクセス グループは、イネーブルにするアクセス リストハードウェア カウンタ用の **ipv6 access-group** コマンドを使用して設定する必要があります。

**show access-lists ipv6 summary** コマンドを使用すると、現在のすべての IPv6 アクセス リストのサマリーを表示することができます。特定の IPv6 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 ipv6 maximum detail** コマンドを使用すると、IPv6 アクセス リストの OOR の詳細を表示することができます。OOD 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 ipv6 ipv4 usage** コマンドを使用すると、指定されたラインカードにプログラミングされたすべてのインターフェイスおよびアクセス 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	操作
acl	読み取り

例

次の例では、すべての IPv6 アクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6

ipv6 access-list Internetfilter
 3 remark Block BGP traffic from a given host
 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
 20 permit ipv6 3333:1:2:3::/64 any
 25 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
ipv6 access-list marketing
 10 permit ipv6 7777:1:2:3::/64 any (51 matches)
 20 permit ipv6 8888:1:2:3::/64 any (26 matches)
 30 permit ipv6 9999:1:2:3::/64 any (5 matches)
```

次の例では、Internetfilter という名前のアクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 Internetfilter

ipv6 access-list Internetfilter
 3 remark Block BGP traffic from a given host
 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
 20 permit ipv6 3333:1:2:3::/64 any
 25 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

次の例では、acl\_hw\_1 という名前のアクセス リストの内容が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
 10 permit icmp any any (251 hw matches)
 20 permit ipv6 3333:1:2:3::/64 any (29 hw matches)
 30 deny tcp any any (58 hw matches)
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 5: show access-lists ipv6 hardware コマンドのフィールドの説明

フィールド	説明
hw matches	ハードウェア一致の数

次の例では、すべての IPv6 アクセス リストのサマリーが表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 summary

ACL Summary:
```

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

次の表に、この出力で表示される重要なフィールドについて説明します。

表 6 : `show access-lists ipv6 summary` コマンドのフィールドの説明

フィールド	説明
Total ACLs configured	設定された IPv6 ACL の数
Total ACEs configured	設定された IPV6 ACE の数

次の例では、すべての IPv6 アクセスリストの OOR の詳細が表示されています。

```
RP/0/RSP0/CPU0:router# show access-lists ipv6 maximum detail
```

```
Default max configurable acls :1000
Default max configurable aces :50000
Current configured acls      :1
Current configured aces     :2
Current max configurable acls :1000
Current max configurable aces :50000
Max configurable acls       :2000
Max configurable aces       :100000
```

## 関連コマンド

コマンド	説明
<a href="#">copy access-list ipv6</a> , (11 ページ)	既存の IPv6 アクセスリストをコピーします。
<a href="#">deny (IPv6)</a> , (25 ページ)	IPv6 アクセスリストの拒否条件を設定します。
<a href="#">ipv6 access-list</a> , (43 ページ)	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。
<a href="#">permit (IPv6)</a> , (75 ページ)	IPv6 アクセスリストの許可条件を設定します。
<a href="#">remark (IPv6)</a> , (83 ページ)	IPv6 アクセスリスト エントリに関する有益な設定を挿入します。
<a href="#">resequence access-list ipv6</a> , (88 ページ)	既存の IPv4 アクセスリスト中の最初のステートメントの開始エントリ番号、および後続のステートメントの番号の増分を変更します。



## ARP コマンド

---

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータのアドレス解決プロトコル (ARP) の設定およびモニタをする場合に使用するコマンドについて説明します。

ARP の概念、設定、タスク、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [arp, 104 ページ](#)
- [arp dagr, 107 ページ](#)
- [arp purge-delay, 109 ページ](#)
- [arp timeout, 111 ページ](#)
- [clear arp-cache, 113 ページ](#)
- [peer \(DAGR\) , 115 ページ](#)
- [priority-timeout, 117 ページ](#)
- [proxy-arp, 119 ページ](#)
- [route distance, 121 ページ](#)
- [route metric, 123 ページ](#)
- [show arp, 125 ページ](#)
- [show arp dagr, 130 ページ](#)
- [show arp traffic, 132 ページ](#)
- [timers \(DAGR\) , 135 ページ](#)

## arp

パーマネント エントリをアドレス解決プロトコル (ARP) キャッシュに追加するには、グローバル 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"> <li>• arpa</li> <li>• srp</li> <li>• srpa</li> <li>• srpb</li> </ul> <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

グローバル コンフィギュレーション



## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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、エントリが対応付けられた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、その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持つネットワーク層アドレスのための 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にかぎり、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。

すべての非スタティック エントリを ARP キャッシュ から削除するには、EXEC モードで **clear arp-cache**、(113 ページ) を入力します。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# arp 192.168.7.19 0800.0900.1834 arpa
```

## 関連コマンド

コマンド	説明
<a href="#">clear arp-cache</a> , (113 ページ)	ARP キャッシュからすべてのダイナミック エントリを削除します。
<a href="#">show arp</a> , (125 ページ)	ARP キャッシュを表示します。

# 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、キーワードと引数はありません。

### 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	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0.1
RP/0/RSP0/CPU0:router(config-if)# arp dagr
RP/0/RSP0/CPU0:router(config-if-dagr)#
```

## 関連コマンド

コマンド	説明
<a href="#">peer (DAGR)</a> , (115 ページ)	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">priority-timeout</a> , (117 ページ)	ハイ プライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route distance</a> , (121 ページ)	指定された DAGR グループのルート ディスタンスを設定します。
<a href="#">route metric</a> , (123 ページ)	指定された DAGR グループのルート メトリックを設定します。
<a href="#">show arp dagr</a> , (130 ページ)	すべての DAGR グループの動作状態を表示します。
<a href="#">timers (DAGR)</a> , (135 ページ)	ARP 要求の送信のための DAGR タイマーを設定します。

## 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。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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
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/RSP0/CPU0:router# configure  
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RP1/CPU0/0  
RP/0/RSP0/CPU0:router(config-if)# arp purge-delay 50
```

## arp timeout

インターフェイス上で学習されるダイナミックエントリがアドレス解決プロトコル (ARP) キャッシュ内に残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。 **arp timeout** 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、このコマンドに関してシステムをデフォルト状態に復元するには、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。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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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だけに対して適用されます。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	操作
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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RP1/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# arp timeout 3600
```

## 関連コマンド

コマンド	説明
<a href="#">clear arp-cache</a> , (113 ページ)	ARP キャッシュからすべてのダイナミック エントリを削除します。
<a href="#">show arp</a> , (125 ページ)	ARP キャッシュを表示します。
show interfaces	ネットワークデバイスで設定されたすべてのインターフェイスの統計情報を表示します。  <b>show interfaces</b> コマンドの使用方法の詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services RouterCisco IOS XR ソフトウェア Interface and Hardware Component Command Reference</i> 』を参照してください。



## clear arp-cache

すべてのダイナミックエントリをアドレス解決プロトコル (ARP) キャッシュから削除するには、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し、EXEC モードで **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

<b>traffic</b>	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。
<b>t type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサ カード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0。</li> <li>• 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。</li> </ul> <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>
<b>location node-id</b>	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 モード

EXEC モードの動作または値はありません。

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**clear arp-cache** コマンドは、キーワードまたは引数なしで発行されると、ARP キャッシュ内のすべてのエントリをクリアします。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear arp-cache traffic gigabitEthernet 0/1/5/1 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/RSP0/CPU0:router# clear arp-cache location 0/1/CPU0
```

## 関連コマンド

コマンド	説明
<a href="#">arp</a> , (104 ページ)	パーマネント エントリを ARP キャッシュに追加します。
<a href="#">show arp</a> , (125 ページ)	ARP キャッシュを表示します。

## peer (DAGR)

仮想 IP アドレスの Direct Attached Gateway Redundancy (DAGR) グループを作成するには、DAGR インターフェイス コンフィギュレーション モードで **peer** コマンドを使用します。

**peer ipv4** *IP-address*

### 構文の説明

IP-address	DAGR グループの仮想 IPv4 アドレス
------------	------------------------

### コマンド デフォルト

なし

### コマンド モード

DAGR 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	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
cef	書き込み

### 例

次の例では、DAGR グループ ピアを設定しています。

```
RP/0/RSP0/CPU0:router(config-if-dagr)# peer ipv4 192.168.7.19
RP/0/RSP0/CPU0:router(config-if-dagr-peer)#
```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr, (107 ページ)</a>	DAGR を設定します。
<a href="#">priority-timeout, (117 ページ)</a>	ハイ プライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route distance, (121 ページ)</a>	指定された DAGR グループのルート ディスタンスを設定します。
<a href="#">route metric, (123 ページ)</a>	指定された DAGR グループのルート メトリックを設定します。
<a href="#">show arp dagr, (130 ページ)</a>	すべての DAGR グループの動作状態を表示します。

# priority-timeout

タイマーがハイ プライオリティ Direct Attached Gateway Redundancy (DAGR) ルートをタイムアウトして通常のプライオリティに戻るようには、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	変更箇所
リリース 3.7.2	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	操作
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/RSP0/CPU0:router(config-if-dagr-peer)# priority-timeout 25
RP/0/RSP0/CPU0:router(config-if-dagr-peer)#
```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr</a> , (107 ページ)	DAGR を設定します。
<a href="#">peer (DAGR)</a> , (115 ページ)	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">route distance</a> , (121 ページ)	指定された DAGR グループのルート ディスタンスを設定します。
<a href="#">route metric</a> , (123 ページ)	指定された DAGR グループのルート メトリックを設定します。
<a href="#">show arp dagr</a> , (130 ページ)	すべての DAGR グループの動作状態を表示します。
	ARP 要求の送信のための DAGR タイマーを設定します。

## proxy-arp

インターフェイス上の代理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、キーワードと引数はありません。

### 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

プロキシ ARP がディセーブルされると、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	操作
cef	読み取り、書き込み

---

**例**

次に、MgmtEth インターフェイス 0/RP1/CPU0/0 上のプロキシ ARP をイネーブルにする方法の例を示します。

```
RP/0/RSP0/CPU0:router#(config)# interface MgmtEth 0/RP1/CPU0/0
RP/0/RSP0/CPU0:router#(config-if)# proxy-arp
```



## route distance

指定された 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

<b>normal normal-distance</b>	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。
<b>priority priority-distance</b>	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 で、*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	変更箇所
リリース 3.7.2	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。

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	操作
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/RSP0/CPU0:router(config-if-dagr-peer)# route distance normal 48 priority 5
RP/0/RSP0/CPU0:router(config-if-dagr-peer)#
```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr</a> , (107 ページ)	DAGR を設定します。
<a href="#">peer (DAGR)</a> , (115 ページ)	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">priority-timeout</a> , (117 ページ)	ハイプライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route metric</a> , (123 ページ)	指定された DAGR グループのルートメトリックを設定します。
<a href="#">show arp dagr</a> , (130 ページ)	すべての DAGR グループの動作状態を表示します。
<a href="#">timers (DAGR)</a> , (135 ページ)	ARP 要求の送信のための DAGR タイマーを設定します。

## route metric

指定された Direct Attached Gateway Redundancy (DAGR) グループの通常のルートメトリックおよび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

<b>normal normal-metric</b>	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。
<b>priority priority-metric</b>	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 で、*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	変更箇所
リリース 3.7.2	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。

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	操作
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/RSP0/CPU0:router(config-if-dagr-peer)# route metric normal 48 priority 5
RP/0/RSP0/CPU0:router(config-if-dagr-peer)#
```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr</a> , (107 ページ)	DAGR を設定します。
<a href="#">peer (DAGR)</a> , (115 ページ)	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">priority-timeout</a> , (117 ページ)	ハイプライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route distance</a> , (121 ページ)	指定された DAGR グループのルートディスタンスを設定します。
<a href="#">show arp dagr</a> , (130 ページ)	すべての DAGR グループの動作状態を表示します。
<a href="#">timers (DAGR)</a> , (135 ページ)	ARP 要求の送信のための DAGR タイマーを設定します。

# show arp

アドレス解決プロトコル (ARP) を表示するには、EXECモードで **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。
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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(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に関しては、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</li> <li>• 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。</li> </ul> <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	(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 モデル

EXECタイプ RSP はデフォルトの場所です。

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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** 形式については、バンドルのキャッシュ エントリがどの場所を表示する必要があるかを **Bundle and VLAN-on-Bundle** インターフェイスが示すために **location node-id** キーワードおよび引数が必須になります。物理インターフェイスについては、インターフェイスが 1 つのノード上にしか存在できないため、**location node-id** キーワードおよび引数の指定は任意になります。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、場所を指定しない **show arp** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arp
-----
0/3/CPU0
-----
Address      Age          Hardware Addr  State   Type   Interface
10
.4.1.1      -           000c.cfe6.3336  Interface  ARPA  GigabitEthernet0/3/1/3
10
.4.1.2      01:37:50    0000.c004.0102  Dynamic   ARPA  GigabitEthernet0/3/1/3
10
.1.4.2      -           000c.cfe6.33b5  Interface  ARPA  FastEthernet0/3/3/4
10
.1.0.2      -           000c.cfe6.33b1  Interface  ARPA  FastEthernet0/3/3/0
10
.1.0.1      00:37:56    000a.8b08.857a  Dynamic   ARPA  FastEthernet0/3/3/0
10
.1.4.1      01:37:51    000a.8b08.857e  Dynamic   ARPA  FastEthernet0/3/3/4
10
.11.1.1     -           000c.cfe6.32fa  Interface  ARPA  FastEthernet0/3/0/6
10
.1.5.2      -           000c.cfe6.33b6  Interface  ARPA  FastEthernet0/3/3/5
```

```

10
.1.1.2      -          000c.cfe6.33b2  Interface  ARPA FastEthernet0/3/3/1
10
.1.1.1      01:37:51 000a.8b08.857b  Dynamic    ARPA FastEthernet0/3/3/1
10
.1.5.1      01:37:50 000a.8b08.857f  Dynamic    ARPA FastEthernet0/3/3/5

```

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

```

Address      Age      Hardware Addr  State      Type      Interface
10
.6.9.1       01:11:55 0003.fe4c.0bff  Dynamic    ARPA MgmtEth0/2/CPU0/0
10
.6.25.6      01:09:29 000c.cfe6.2000  Dynamic    ARPA MgmtEth0/2/CPU0/0
10
.6.5.10      00:39:58 0009.7b49.0bff  Dynamic    ARPA MgmtEth0/2/CPU0/0

```

次に、*interface-type interface-instance* 引数を持つ **show arp** コマンドからの出力例を示します。

```
RRP/0/RSP0/CPU0:router# show arp MgmtEth 0/RP1/CPU0/0
```

```

Address      Age      Hardware Addr  State      Type      Interface
10.4.9.2      00:35:55 0030.7131.abfc  Dynamic    ARPA MgmtEth0/RP1/CPU0/0
10.4.9.1      00:35:55 0000.0c07.ac24  Dynamic    ARPA MgmtEth0/RP1/CPU0/0
10.4.9.99     00:49:12 0007.ebea.44d0  Dynamic    ARPA MgmtEth0/RP1/CPU0/0
10.4.9.199    -          0001.c9eb.dffe  Interface  ARPA MgmtEth0/RP1/CPU0/0

```

次に、*hardware-address* を指定した **show arp** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arp 0005.5f1d.8100
```

```

Address Age Hardware Addr State Type Interface
172.16.7.2 - 0005.5f1d.8100 Interface ARPA GigabitEthernet2/0/1/2

```

次に、**location** キーワードおよび *node-id* 引数を持つ **show arp** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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 GigabitEthernet2/0/1/2
172.16.7.2 - 0005.5f1d.8100 Interface ARPA GigabitEthernet2/0/1/2

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 7: **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。
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。

フィールド	説明
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"> <li>• Dynamic</li> <li>• Interface</li> <li>• Alias</li> <li>• Static</li> <li>• "-" (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)</li> </ul>
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。  (注) */*/* は、ノード ID を <i>rack/slot/module</i> のフォーマットで表します。

## 関連コマンド

コマンド	説明
<a href="#">arp</a> , (104 ページ)	パーマネント エントリを ARP キャッシュに追加します。
<a href="#">clear arp-cache</a> , (113 ページ)	ARP キャッシュからすべてのダイナミック エントリを削除します。
<a href="#">show arp traffic</a> , (132 ページ)	ARP トラフィック統計情報を表示します。





## show arp dagr

すべての Direct Attached Gateway Redundancy (DAGR) グループの状態を表示するには、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# 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

```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr</a> , (107 ページ)	DAGR を設定します。
<a href="#">peer (DAGR)</a> , (115 ページ)	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">priority-timeout</a> , (117 ページ)	ハイ プライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route distance</a> , (121 ページ)	指定された DAGR グループのルート ディスタンスを設定します。
<a href="#">route metric</a> , (123 ページ)	指定された DAGR グループのルート メトリックを設定します。
<a href="#">timers (DAGR)</a> , (135 ページ)	ARP 要求の送信のための DAGR タイマーを設定します。

## 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、EXEC モードで **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

<i>vrf</i>	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
<i>vrf-name</i>	(任意) VPN を識別する VRF インスタンス。
<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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> </ul> <p>(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に関しては、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 <b>MgmtEth0/RSP0/CPU0/0</b></p> <ul style="list-style-type: none"> <li>• 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。</li> </ul> <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>
<b>location</b> <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。



(注)

The active RSP is the default location.

コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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* については、バンドルのキャッシュ エントリがどの場所を表示する必要があるかを **Bundle and VLAN-on-Bundle** インターフェイスが示すために **location node-id** キーワードおよび引数が必須になります。物理インターフェイスについては、インターフェイスが 1 つのノード上にしか存在できないため、**location node-id** キーワードおよび引数の指定は任意になります。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、コマンドを持つ **show arp** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arp traffic

ARP statistics:
  Recv: 2691 requests, 91 replies
  Sent: 67 requests, 2 replies (0 proxy, 1 gratuitous)
  Resolve requests rcvd: 1
  Resolve requests dropped: 0
  Errors: 0 out of memory, 0 no buffers

ARP cache:
  Total ARP entries in cache: 4
  Dynamic: 3, Interface: 1, Standby: 0
  Alias: 0,   Static: 0
```

IP Packet drop count for node 0/0/CPU0: 1

次に **location** キーワードと *node-id* 引数を持つ **show arp traffic** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arp traffic location 0/2/CPU0

ARP statistics:
  Recv: 0 requests, 1 replies
  Sent: 0 requests, 2 replies (0 proxy, 2 gratuitous)
```

## show arp traffic

```
Resolve requests rcvd: 0
Resolve requests dropped: 0
Errors: 0 out of memory, 0 no buffers
```

```
ARP cache:
Total ARP entries in cache: 4
Dynamic: 1, Interface: 1, Static: 1
```

```
Alias: 1, Standby: 0
```

```
IP Packet drop count for node 0/2/CPU0: 1
```

## 関連コマンド

コマンド	説明
<a href="#">arp, (104 ページ)</a>	パーマネント エントリを ARP キャッシュに追加します。
<a href="#">clear arp-cache, (113 ページ)</a>	ARP キャッシュからすべてのダイナミック エントリを削除します。
<a href="#">show arp, (125 ページ)</a>	ARP 統計情報を表示します。

## 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

<b>query query-time</b>	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。
<b>standby standby-time</b>	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 秒で、*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	変更箇所
リリース 3.7.2	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	操作
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。

```
RP/0/RSP0/CPU0:router(config-if-dagr-peer)# timers query 2 standby 40
RP/0/RSP0/CPU0:router(config-if-dagr-peer)#
```

## 関連コマンド

コマンド	説明
<a href="#">arp dagr, (107 ページ)</a>	DAGR を設定します。
<a href="#">peer (DAGR) , (115 ページ)</a>	バーチャル IP アドレスの DAGR グループを作成します。
<a href="#">priority-timeout, (117 ページ)</a>	ハイ プライオリティ DAGR ルートのタイムアウトを設定します。
<a href="#">route distance, (121 ページ)</a>	指定された DAGR グループのルート ディスタンスを設定します。
<a href="#">route metric, (123 ページ)</a>	指定された DAGR グループのルート メトリックを設定します。
<a href="#">show arp dagr, (130 ページ)</a>	すべての DAGR グループの動作状態を表示します。





# 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、シスコエクスプレスフォワーディング（CEF）を Cisco ASR 9000 シリーズ アグリゲーションサービス ルータで設定および監視するために使用されるコマンドについて説明します。

CEF の概念、設定タスク、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [clear adjacency statistics, 140 ページ](#)
- [clear cef ipv4 drops, 142 ページ](#)
- [clear cef ipv4 exceptions, 144 ページ](#)
- [clear cef ipv4 interface bgp-policy-statistics, 146 ページ](#)
- [clear cef ipv4 interface rpf-statistics, 148 ページ](#)
- [clear cef ipv6 drops, 150 ページ](#)
- [clear cef ipv6 exceptions, 152 ページ](#)
- [clear cef ipv6 interface bgp-policy-statistics, 154 ページ](#)
- [ipv4 bgp policy accounting, 156 ページ](#)
- [ipv4 bgp policy propagation, 159 ページ](#)
- [ipv4 verify unicast source reachable-via, 161 ページ](#)
- [ipv6 verify unicast source reachable-via, 164 ページ](#)
- [rp mgmtethernet forwarding, 166 ページ](#)
- [show adjacency, 168 ページ](#)
- [show cef, 171 ページ](#)
- [show cef bgp-attribute, 173 ページ](#)

- [show cef external, 175 ページ](#)
- [show cef recursive-nextthop, 178 ページ](#)
- [show cef summary, 180 ページ](#)
- [show cef ipv4, 183 ページ](#)
- [show cef ipv4 adjacency, 186 ページ](#)
- [show cef ipv4 adjacency hardware, 189 ページ](#)
- [show cef ipv4 drops, 192 ページ](#)
- [show cef ipv4 exact-route, 195 ページ](#)
- [show cef ipv4 exceptions, 198 ページ](#)
- [show cef ipv4 hardware, 201 ページ](#)
- [show cef ipv4 interface, 203 ページ](#)
- [show cef ipv4 interface bgp-policy-statistics, 206 ページ](#)
- [show cef ipv4 non-recursive, 209 ページ](#)
- [show cef ipv4 resource, 213 ページ](#)
- [show cef ipv4 summary, 215 ページ](#)
- [show cef ipv4 unresolved, 218 ページ](#)
- [show cef ipv6, 220 ページ](#)
- [show cef ipv6 adjacency, 224 ページ](#)
- [show cef ipv6 adjacency hardware, 226 ページ](#)
- [show cef ipv6 drops, 228 ページ](#)
- [show cef ipv6 exact-route, 232 ページ](#)
- [show cef ipv6 exceptions, 234 ページ](#)
- [show cef ipv6 hardware, 237 ページ](#)
- [show cef ipv6 interface, 239 ページ](#)
- [show cef ipv6 non-recursive, 241 ページ](#)
- [show cef ipv6 resource, 244 ページ](#)
- [show cef ipv6 summary, 246 ページ](#)
- [show cef ipv6 unresolved, 249 ページ](#)
- [show cef mpls adjacency, 251 ページ](#)
- [show cef mpls adjacency hardware, 254 ページ](#)
- [show cef mpls interface, 256 ページ](#)

- [show cef mpls unresolved, 258 ページ](#)
- [show cef vrf, 260 ページ](#)

## clear adjacency statistics

隣接パケットおよびバイトカウンタ統計情報をクリアするには、EXEC モードで **clear adjacency statistics** コマンドを使用します。

**clear adjacency statistics** [**ipv4** [**nexthop** *ipv4-address*]] **mpls**| **ipv6**] [*interface-type interface-instance* | *location node-id*]

### 構文の説明

<b>ipv4</b>	(任意) IPv4 隣接パケットおよびバイトカウンタ統計情報だけをクリアします。
<b>nexthop</b> <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統計情報をクリアします。
<b>mpls</b>	(任意) MPLS 隣接統計情報だけをクリアします。
<b>ipv6</b>	(任意) IPv6 隣接統計情報だけをクリアします。
<b>interface-type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-instance</b>	(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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <i>slot</i> : ラインカードの物理スロット番号。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (<i>RSP0 RP0</i> または <i>RP1</i>) で、モジュールは CPU0 です。例: インターフェイス <i>MgmtEth0/RSP0 RP1/CPU0/0</i>。</li> <li>• 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。</li> </ul>

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** *node-id* (任意) 指定されたノードの詳しい隣接統計情報をクリアします。 *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** EXEC

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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。

**clear adjacency statistics** コマンドは、ネットワーク接続の問題を解決し、問題を転送する場合に役立ちます。

いずれのオプションキーワードも指定しない場合、コマンドが発行されるノードのすべての隣接統計情報がクリアされます。

**タスク ID**

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

**関連コマンド**

コマンド	説明
<a href="#">show adjacency</a> , (168 ページ)	IPv4 CEF 隣接関係テーブルを表示します。

## 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、EXEC モードで **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

<b>location <i>node-id</i></b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、コマンドが発行されるノードだけで 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	操作
basic-services	読み取り、書き込み
cef	読み取り、書き込み

## 例

次に、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 の出力例、およびロケーション 0/1/CPU0 で IPv4 CEF ドロップ カウンタをクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/1/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
Node: 0/6/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
Node: 0/RSP0RP00/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
Node: 0/RSP0RP00/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

RP/0/RSP0/CPU0:router# clear cef ipv4 drops location 0/1/CPU0

Node: 0/1/CPU0
Clearing CEF Drop Statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show cef ipv4 drops</a> , (192 ページ)	IPv4 パケット ドロップ カウンタを表示します。

## 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、EXEC 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

<b>location node-id</b>	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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
basic-services	読み取り、書き込み
cef	読み取り、書き込み



## 例

次に、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例、およびノード 0/1/CPU0 の IPv4 CEF 例外パケットカウンタをクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/1/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
Node: 0/6/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
Node: 0/RSP0RP00/CPU0
  Slow encap packets :          1
  Unsupported packets :          0
  Redirect packets :            0
  Receive packets :             71177
  Broadcast packets :          23648
  IP options packets :          0
  TTL expired packets :         0
  Fragmented packets :         0
Node: 0/RSP0RP00/CPU0
  Slow encap packets :          0
  Unsupported packets :          0
  Redirect packets :            0
  Receive packets :            167314
  Broadcast packets :          22656
  IP options packets :          0
  TTL expired packets :         0
  Fragmented packets :         0

RP/0/RSP0/CPU0:router# clear cef ipv4 exceptions location 0/1/CPU0

Node: 0/1/CPU0
Clearing CEF Exception Statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show cef ipv4 exceptions</a> , (198 ページ)	IPv4 CEF 例外パケットカウンタを表示します。

## clear cef ipv4 interface bgp-policy-statistics

シスコ エクスプレス フォワーディング (CEF) IPv4 インターフェイス ボーダー ゲートウェイ プロトコル (BGP) ポリシー統計情報をクリアするには、EXEC モードで **clear cef ipv4 interface bgp-policy-statistics** コマンドを使用します。

**clear cef ipv4 interface** *type interface-path-id* **bgp-policy-statistics**

### 構文の説明

<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
<b>interface-path-id</b>	物理インターフェイスまたは仮想インターフェイス。 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、 <b>show interfaces</b> 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

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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

このコマンドは ASR 9000 イーサネットラインカードではサポートされていません。このコマンドは、指定されたインターフェイスのボーダーゲートウェイプロトコル (BGP) ポリシーアカウンティングカウンタをクリアします。

## タスク ID

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

## 例

次に、tenGigE インターフェイスで IPv4 CEF BGP ポリシー統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear cef ipv4 interface tenGigE 0/4/0/0 bgp-policy-statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show cef ipv4 interface bgp-policy-statistics</a> , (206 ページ)	IPv4 CEF BGP ポリシー統計情報を表示します。

## clear cef ipv4 interface rpf-statistics

シスコ エクスプレス フォワーディング (CEF) IPv4 インターフェイス ユニキャスト リバース パス 転送 (RPF) 統計情報をクリアするには、EXEC モードで **clear cef ipv4 interface rpf-statistics** コマンドを使用します。

**clear cef ipv4 interface** *type interface-path-id* **rpf-statistics** [*location node-id*]

### 構文の説明

**type** インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

**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 カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/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。

**location node-id** (任意) 指定されたノードの IPv4 ユニキャスト Reverse Path Forwarding (RPF) 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**clear cef ipv4 interface rpf-statistics** コマンドは、指定されたインターフェイスのユニキャスト Reverse Path Forwarding (RPF) カウンタをクリアします。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、IPv4 CEF RPF 統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear cef ipv4 interface tenGigE 0/4/0/0 rpf-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、EXEC モードで **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

<b>location <i>node-id</i></b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
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) テーブル パケット ドロップ カウンタ の出力例、およびロケーション 0/1/CPU0 で IPv6 CEF ドロップ カウンタをクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear cef ipv6 drops

CEF Drop Statistics
Node: 0/1/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
Node: 0/6/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
Node: 0/RSP0/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
Node: 0/RSP0/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

RP/0/RSP0/CPU0:router# clear cef ipv6 drop

Node: 0/1/CPU0
Clearing CEF Drop Statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show cef ipv6 drops</a> , ( <a href="#">228 ページ</a> )	IPv6 パケット ドロップ カウンタを表示します。

## 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、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
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/RSP0/CPU0:router# show cef ipv6 exceptions

CEF Exception Statistics
Node: 0/1/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
Node: 0/6/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
Node: 0/RSP0/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
Node: 0/RSP0/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/RSP0/CPU0:router# clear cef ipv6 exceptions location 0/1/CPU0

Node: 0/1/CPU0
Clearing CEF Exception Statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show cef ipv6 exceptions</a> , <a href="#">(234 ページ)</a>	IPv6 CEF 例外パケットカウンタを表示します。

## clear cef ipv6 interface bgp-policy-statistics

シスコ エクスプレス フォワーディング (CEF) IPv6 インターフェイス ボーダー ゲートウェイ プロトコル (BGP) ポリシー統計情報をクリアするには、EXEC モードで **clear cef ipv6 interface bgp-policy-statistics** コマンドを使用します。

**clear cef ipv6 interface** *type interface-path-id* **bgp-policy-statistics**

### 構文の説明

<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
<b>interface-path-id</b>	物理インターフェイスまたは仮想インターフェイス。 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、 <b>show interfaces</b> 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

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

EXEC

### 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。

**clear cef ipv6 interface bgp-policy-statistics** コマンドは、指定されたインターフェイスのボーダー ゲートウェイ プロトコル (BGP) ポリシー アカウンティング カウンタをクリアします。

### タスク ID

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

例 次に、IPv6 CEF BGP ポリシー統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear cef ipv6 interface MgmtEth 0/CPU0/0 bgp-policy-statistics
```

## ipv4 bgp policy accounting

ボーダーゲートウェイプロトコル (BGP) ポリシーアカウンティングをイネーブルにするには、インターフェイス コンフィギュレーションモードで **ipv4 bgp policy accounting** コマンドを使用します。BGP ポリシーアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ipv4 bgp policy accounting {input|output} {destination-accounting [source-accounting]| source-accounting [destination-accounting]}
```

```
no ipv4 bgp policy accounting {input|output} {destination-accounting [source-accounting]| source-accounting [destination-accounting]}
```

### 構文の説明

input	BGP ポリシーアカウンティングポリシーを入力 IPv4 ユニキャストインターフェイスでイネーブルにします。
output	BGP ポリシーアカウンティングポリシーを出力 IPv4 ユニキャストインターフェイスでイネーブルにします。
{ <b>destination-accounting</b> [ <b>source-accounting</b> ]   <b>source-accounting</b> [ <b>destination-accounting</b> ]}	<p>入力または出力インターフェイスを指定する場合、次のいずれかのキーワードを指定する必要があります。</p> <ul style="list-style-type: none"> <li>• <b>destination-accounting</b> : 宛先アドレスに基づいてアカウンティングポリシーをイネーブルにします。</li> <li>• <b>source-accounting</b> : 送信元アドレスに基づいてアカウンティングポリシーをイネーブルにします。</li> </ul> <p><b>destination-accounting</b> を指定すると、オプションで <b>source-accounting</b> を指定できます。または、<b>source-accounting</b> を指定すると、オプションで <b>destination-accounting</b> を指定できます。</p>

### コマンド デフォルト

BGP ポリシーアカウンティングはありません。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

このコマンドの **no** 形式を使用すると、アカウントリングは、送信元および宛先の両方でディセーブルになります。宛先または送信元アドレスのいずれかでアカウントリングを変更するには、**destination-accounting** または **source-accounting** キーワードを指定して、**ipv4 bgp policy accounting** コマンドを再設定します。次の例では、送信元および宛先アドレスアカウントリングを事前にイネーブルにした後で、送信元アドレスの BGP ポリシー アカウントリングをディセーブルにします。

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 bgp policy accounting output destination-accounting
```

BGP ポリシーの設定については、『Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide』を参照してください。BGP アカウントリング ポリシーは、コミュニティ リスト、自律システム番号または自律システム パスに基づきます。

BGP ポリシー伝達機能を使用するには、BGP をイネーブルにする必要があります。

アカウントリングポリシーを指定するには、**set traffic-index** コマンドを使用して、特定の BGP 属性と一致するように、ルートポリシーを正しく設定しなければなりません。BGP ルータ コンフィギュレーション モードで、**table-policy** コマンドを使用して、IP ルーティング テーブルが BGP から学習されたルートで更新されるときにアカウントリング バケットを修正します。アカウントリング ポリシー情報を表示するには、**show cef ipv4 interface bgp-policy-statistics**、**show bgp policy** および **show route bgp** コマンドを使用します。

このコマンドは ASR 9000 イーサネット ラインカードではサポートされていません。

**タスク ID**

タスク ID	操作
network	読み取り、書き込み

**例**

次に、BGP ポリシー アカウントリングを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet pos 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 bgp policy accounting output source-accounting
```

## 関連コマンド

コマンド	説明
route-policy (BGP)	ルート ポリシーを定義します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</i> 』を参照してください。
show bgp policy	提示されたポリシーの元での BGP アドバタイズメントに関する情報を表示します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</i> 』を参照してください。
<a href="#">show cef ipv4 interface bgp-policy-statistics, (206 ページ)</a>	IPv4 CEF BGP ポリシー統計情報を表示します。
show route	RIB で BGP の現在ルートを表示します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</i> 』を参照してください。
table-policy	ルーティング テーブルにインストールされるルートにルーティングポリシーを適用します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</i> 』を参照してください。

## ipv4 bgp policy propagation

QoS Policy Propagation on BGP (QPPB; BGP による QoS ポリシー伝達) をインターフェイスで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、**ipv4 bgp policy propagation** コマンドを使用します。BGP による QoS ポリシー伝達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 bgp policy propagation** {input} {ip-precedence | qos-group} {destination | source}

**no ipv4 bgp policy propagation** {input} {ip-precedence | qos-group} {destination | source}

### 構文の説明

input	QPPB を入力 IPv4 ユニキャスト インターフェイスでイネーブルにします。
ip-precedence	QoS ポリシーが IP precedence に基づいていることを指定します。
qos-group	QoS ポリシーが QoS グループ ID に基づいていることを指定します。
destination	宛先アドレス エントリの IP precedence bit または QoS グループ ID がルート テーブルで使用されることを指定します。
source	送信元アドレス エントリの IP precedence bit または QoS グループ ID がルート テーブルで使用されることを指定します。

### コマンド デフォルト

デフォルトではディセーブルになっています。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

QPPB 機能を使用するには、BGP および CEF をイネーブルにする必要があります。また、ルートマップを正しく設定して、IP precedence または QoS グループ ID（たとえば、**set precedence** コマンド）を指定しなければなりません。

送信元と宛先の両方をインターフェイスで指定した場合、最初に、ルーティングテーブルの送信元アドレスが参照され、送信元アドレスに基づいてパケットが分類されます。その後、ルーティングテーブルの宛先アドレスが参照され、宛先アドレスに基づいてパケットが再分類されます。

## タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス上で QPPB をイネーブルにする例を示します。

次に、Packet-over-SONET/SDH (POS) インターフェイス上で QPPB をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet pos 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.3.1.1 255.255.255.252
RP/0/RSP0/CPU0:router(config-if)# ipv4 bgp policy propagation input ip-precedence destination
```

## 関連コマンド

コマンド	説明
route-policy (BGP)	ルート ポリシーを定義します。
show bgp policy	提示されたポリシーの元での BGP アドバタイズメントに関する情報を表示します。
<a href="#">show cef ipv4 interface bgp-policy-statistics, (206 ページ)</a>	IPv4 CEF BGP ポリシー統計情報を表示します。
show route	RIB で BGP の現在ルートを表示します。
table-policy	ルーティングテーブルにインストールされるルートにルーティングポリシーを適用します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</i> 』を参照してください。



## ipv4 verify unicast source reachable-via

IPv4 ユニキャスト リバースパス転送 (RPF) チェック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 **ipv4 verify unicast source reachable-via** コマンドを使用します。ユニキャスト RPF 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 verify unicast source reachable-via {any| rx} [allow-default] [allow-self-ping]**

**no ipv4 verify unicast source reachable-via {any| rx} [allow-default] [allow-self-ping]**

### 構文の説明

any	ルーズユニキャスト RPF チェックをイネーブルにします。ルーズユニキャスト RPF がイネーブルの場合、パケットは、その送信元プレフィックスがルーティングテーブルに存在しない限り転送されません。
rx	ストリクトユニキャスト RPF チェックをイネーブルにします。ストリクトユニキャスト RPF がイネーブルの場合、パケットは、その送信元プレフィックスがルーティングテーブルに存在し、出力インターフェイスがパケットの受信インターフェイスと一致しない限り転送されません。
allow-default	(任意) デフォルトルートとのマッチングをイネーブルにします。このオプションは、ルーズおよびストリクトの両方の RPF に適用されます。
allow-self-ping	(任意) ルータによるインターフェイスの PING をイネーブルにします。このオプションは、ルーズおよびストリクトの両方の RPF に適用されます。

### コマンド デフォルト

IPv4 ユニキャスト RPF 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  
動的なテンプレート コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドは、BNG の動的なテンプレートコンフィギュレーション モードでサポートされていました。

## 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。

動的なテンプレート コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dynamic-template** コマンドを実行します。

ルータを通過する変形または偽造（スプーフィング）された IP 送信元アドレスによって発生する問題を減少させるには、**ipv4 verify unicast source reachable-via** インターフェイス コマンドを使用します。変形または偽造（スプーフィング）されたソース アドレスは、ソース IP アドレスのスプーフィングに基づいたサービス拒絶（DoS）攻撃を示すことができます。

ストリクトユニキャスト RPF がインターフェイスでイネーブルの場合、ルータは、そのインターフェイスで受信されるすべてのパケットを検証します。ルータは、送信元アドレスがルーティング テーブルにあり、パケットが受信されるインターフェイスと一致するか確認します。

ルーズユニキャスト RPF がインターフェイスでイネーブルの場合、ルータは、そのインターフェイスで受信されるすべてのパケットを検証します。ルータは、送信元アドレスが任意のルータ インターフェイスを介して送信できるか確認します。

## タスク ID

タスク ID	操作
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

次に、gigabitethernet インターフェイス 0/1/0/0 でストリクト RPF を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 verify unicast source reachable-via rx
```

次に、gigabitethernet インターフェイス 0/0/0/1 でルーズ RPF を設定する例を示します。

```
RP/0/RSP0/CPU0:routeros(config)# interface gigabitethernet 0/0/0/1
RP/0/RSP0/CPU0:routeros(config-if)# ipv4 verify unicast source reachable-via any
```

次に、動的なテンプレート コンフィギュレーション モードでストリクト RPF を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 verify unicast source reachable-via
rx
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 verify unicast source reachable-via</a> , (164 ページ)	ルーズ IPv6 ユニキャスト RPF チェックをイネーブルにします。

## ipv6 verify unicast source reachable-via

IPv6 ユニキャスト Reverse Path Forwarding (RPF) チェック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 verify unicast source reachable-via** コマンドを使用します。IPv6 ユニキャスト RPF 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 verify unicast source reachable-via {any| rx} [allow-default] [allow-self-ping]**

**no ipv6 verify unicast source reachable-via {any| rx} [allow-default] [allow-self-ping]**

### 構文の説明

any	ルーズユニキャスト RPF チェックをイネーブルにします。ルーズユニキャスト RPF がイネーブルの場合、パケットは、その送信元プレフィックスがルーティング テーブルに存在しない限り転送されません。
rx	ストリクトユニキャスト RPF チェックをイネーブルにします。ストリクトユニキャスト RPF がイネーブルの場合、パケットは、その送信元プレフィックスがルーティング テーブルに存在し、出力インターフェイスがパケットの受信インターフェイスと一致しない限り転送されません。
allow-default	(任意) デフォルトルートのマッチングをイネーブルにします。このオプションは、ルーズおよびストリクトの両方の RPF に適用されます。
allow-self-ping	(任意) ルータによるインターフェイスの PING をイネーブルにします。このオプションは、ルーズおよびストリクトの両方の RPF に適用されます。

**コマンド デフォルト** ルーズ IPv6 ユニキャスト RPF 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	変更箇所
リリース 4.1.1	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。

## タスク ID

タスク ID	操作
network	読み取り、書き込み
ipv6	読み取り、書き込み

## 例

次に、POS インターフェイス 0/1/0/0 でルーズ RPF チェックをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface pos 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 verify unicast source reachable-via any
```

次に、gigabitethernet インターフェイス 0/1/0/0 でストリクト RPF を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 verify unicast source reachable-via rx
```

次に、gigabitethernet インターフェイス 0/0/0/1 でルーズ RPF を設定する例を示します。

```
RP/0/RSP0/CPU0:routeros(config)# interface gigabitethernet 0/0/0/1
RP/0/RSP0/CPU0:routeros(config-if)# ipv6 verify unicast source reachable-via any
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 verify unicast source reachable-via</a> , (161 ページ)	IPv4 ユニキャスト RPF チェックをイネーブルにします。

## rp mgmtethernet forwarding

ラインカードからルートプロセッサ管理イーサネットインターフェイスへのスイッチングをイネーブルにするには、グローバル コンフィギュレーション モードで **rp mgmtethernet forwarding** コマンドを使用します。 モジュラ サービス カードからルートプロセッサ管理イーサネットインターフェイスへのスイッチングをディセーブルにするには、このコマンドの **no** 形式を使用します。

**rp mgmtethernet forwarding**

**no rp mgmtethernet forwarding**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

スイッチングはディセーブルです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース

変更箇所

リリース 3.7.2

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。

rp mgmtethernet forwarding コマンドは LC のリロードを有効にする必要があります。



(注)

イネーブルの場合、RPCPU がパケット転送に使用されます。これは、RP には、ラインカードのような、パケット処理エンジンがないからです。

### タスク ID

タスク ID

操作

cef

読み取り、書き込み

## 例

次に、モジュラ サービス カードから RP 管理イーサネット インターフェイスへのスイッチングをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# rp mgmtethernet forwarding
```

# 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、EXEC モードで **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

<b>ipv4</b>	(任意) IPv4 隣接だけを表示します。
<b>nexthop</b> <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。
<b>mpls</b>	(任意) MPLS 隣接だけを表示します。
<b>ipv6</b>	(任意) IPv6 隣接だけを表示します。
<b>interface-type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-instance</b>	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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <i>slot</i> : ラインカードの物理スロット番号。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>• 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。</li> </ul>

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。



<b>remote</b>	(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。
<b>detail</b>	(任意) レイヤ 2 情報など、隣接の詳細情報を表示します。
<b>location node-id</b>	(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** EXEC

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

**例**

次に、**location** キーワードを指定した **show adjacency** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show adjacency location 0/0/CPU0

Interface Address Version Refcount Protocol
gigabitethernet0
/0/1/2(src mac only) 6 1 ipv4
gigabitethernet0
```

## show adjacency

```

/0/1/2 point to point 7 100004
gigabitethernet0
/0/1/2                (interface)                3 1

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 8: *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。
Address	Address は、次のいずれかのアドレスです。 <ul style="list-style-type: none"> <li>• ネクストホップ IPv4 または IPv6 アドレス</li> <li>• Point-to-Point アドレス</li> </ul> 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	隣接に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。

## 関連コマンド

コマンド	説明
<a href="#">clear adjacency statistics</a> , (140 ページ)	IPv4 CEF 隣接関係テーブルをクリアします。

## 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、EXEC モードで **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

<b>prefix</b>	(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。
<b>mask</b>	(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。
<b>hardware</b>	(任意) ハードウェアの詳細情報を表示します。
<b>egress</b>	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。
<b>ingress</b>	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。
<b>detail</b>	(任意) 詳細情報を表示します。
<b>location</b> <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。
<b>all</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

タスク ID	タスク ID	操作
	cef	読み取り

**例** 次に、**hardware** および **ingress** キーワードの両方を指定した **show cef** コマンドの load information フラグの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef 101.1.3.0/24 hardware ingress location 0/3/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
[ 0x0081a600 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 bgp-attribute

シスコ エクスプレス フォワーディング (CEF) のボーダー ゲートウェイ プロトコル (BGP) 属性を表示するには、EXEC モードで **show cef bgp-attribute** コマンドを使用します。

**show cef bgp-attribute** [**attribute-id index-id**] [**local-attribute-id index-id**] [**location node-id**]

### 構文の説明

<b>attribute-id index-id</b>	(任意) FIB 属性インデックスを表示します。
<b>local-attribute-id index-id</b>	(任意) FIB ローカル属性インデックスを表示します。
<b>location node-id</b>	(任意) 指定されたノードの BGP 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 location はアクティブ RP です。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef bgp-attribute** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router# show cef bgp-attribute

Total number of entries: 75742
BGP Attribute ID: 0x2058a, Local Attribute ID: 0x1
  Origin AS: 195, Next Hop AS: 195
BGP Attribute ID: 0x20583, Local Attribute ID: 0x2
  Origin AS: 22, Next Hop AS: 22
BGP Attribute ID: 0x20582, Local Attribute ID: 0x3
  Origin AS: 21, Next Hop AS: 21
BGP Attribute ID: 0x20585, Local Attribute ID: 0x4
  Origin AS: 28, Next Hop AS: 28
BGP Attribute ID: 0x20584, Local Attribute ID: 0x5
  Origin AS: 27, Next Hop AS: 27
BGP Attribute ID: 0x2057f, Local Attribute ID: 0x6
  Origin AS: 86, Next Hop AS: 86
BGP Attribute ID: 0x2058b, Local Attribute ID: 0x7
  Origin AS: 196, Next Hop AS: 196
BGP Attribute ID: 0x20589, Local Attribute ID: 0x8
  Origin AS: 194, Next Hop AS: 194
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 9 : *show cef bgp-attribute* コマンドのフィールドの説明

フィールド	説明
BGP Attribute ID	BGP により割り当てられた ID を表示します。
Local Attribute ID	FIB により割り当てられた ID を表示します。
Origin AS	この属性 ID を伝送するプレフィックスの元の AS を表示します。
Next Hop AS	このプレフィックスの BGP ネクストホップを含む AS を表示します。

## 関連コマンド

コマンド	説明
<a href="#">show cef</a> , (171 ページ)	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します。

## show cef external

シスコ エクスプレス フォワーディング (CEF) 外部クライアント依存関係情報を表示するには、EXEC モードで **show cef external** コマンドを使用します。

```
show cef external [hardware {ingress| egress}] [prefix] {ifhandle| tunnel-id| client-name} {6vpe|
6vpe-ipvpn| eos0-ldi| ip-reachability} [detail] [location node-id]
```

### 構文の説明

hardware	(任意) ハードウェアの情報を表示します。
ingress	(任意) 入力パケット フォワーディング ハードウェアでプログラミングされたハードウェア情報を表示します。
egress	(任意) 出力パケット フォワーディング ハードウェアでプログラミングされたハードウェア情報を表示します。
prefix	(任意) 特定のプレフィックスの外部クライアント情報を表示します。
ifhandle	インターフェイス ハンドルを指定します。
tunnel-id	トンネル識別子を指定します。
client-name	特定のクライアントの名前。特定のクライアント名の依存関係情報が表示されます。
6vpe	6VPE (IPv6 VPN Provide Edge) 依存関係情報を表示します。
6vpe-ipvpn	6VPE over IP-VPN 依存関係情報を表示します。
eos0-ldi	スタック 0 (EOS0) ロード バランシング依存関係のマルチプロトコル ラベル スイッチング (MPLS) 側の情報を表示します。
ip-reachability	インターネット プロトコル (IP) 到達可能性情報を表示します。
detail	(任意) 依存関係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外部クライアント依存関係情報を表示します。 <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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、show cef external コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router#show cef external hardware egress location 0/0/CPU0
Mon Dec 13 11:09:21.041 UTC
```

```
IPV4:
-----
Client Name       : l2fib_mgr (comp-id: 0x7e6d) (0x9f6f70fc)
Protocol          : ipv4
Prefix            : 3.3.3.3 (0x9f13d22c)
Gateway array     : 9e8fb058 (0x201500/1)
Loadinfo          : 9fbd41a8 (0x10181101/1)
Number of notif  : 1
Interest type     : EOS0 LDI updates
Table Id          : 0xe0000000
Cookie Value      : 6c326669625f6d67720000000
State             : resolved, cached plat context
Via               : 16000/0
Added to pend list: Dec 13 11:08:37.920
  Load distribution: 0 (refcount 1)
```

```
Hash OK Interface Address
0 Y GigabitEthernet0/0/0/9 10.0.9.2
```

Data identical on all NPs:

```
---- ECD LDI platform context data ----
Flags: 0x21
L2VPN LDI index: 0x1 (Search Key:0x100)
Preferred path index: 0x5002dea0
Cached L2FIB notification data:
  l2vpn_ldi_index: 0x1 (Search Key:0x100)
  recursion_level: 1 (RECURSION_NONE), num_paths: 1

  IGP Path info #0
  is unresolved: 0
  Primary path: is_lag: 0, sfp_or_lagid: 1, ifhandle: 0x4000440
```



```

      Bkup path: is not valid
---- End of platform context data ----

RP/0/RSP0/CPU0:router#show cef external hardware egress location 0/0/CPU0
Mon Dec 13 11:22:47.605 UTC

IPV4:
-----
Client Name      : l2fib_mgr (comp-id: 0x7e6d) (0x9f6f70fc)
Protocol         : ipv4
Prefix          : 100.100.100.2 (0x9f13d22c)
Gateway array   : 9e8fb058 (0x201500/1)
Loadinfo        : 9fbd41a8 (0x10181101/1)
Number of notif : 2
Interest type   : EOS0 LDI updates
Table Id        : 0xe0000000
Cookie Value    : 6c326669625f6d677200000000
State           : resolved, cached plat context
Via             : 16006/0
Added to pend list: Dec 13 11:21:23.037

      Load distribution: 0 (refcount 1)

      Hash OK Interface Address
      0 Y recursive 16006/0

Data identical on all NPs:
---- ECD LDI platform context data ----
Flags: 0x21
L2VPN LDI index: 0x2 (Search Key:0x200)
Preferred path index: 0x5002dea8
Cached L2FIB notification data:
  l2vpn_ldi_index: 0x2 (Search Key:0x200)
  recursion_level: 2 (RECURSION_ONE), num_paths: 1

      BGP Path info #0

      IGP Path info #0
      is unresolved: 0
      Primary path: is_lag: 0, sfp_or_lagid: 1, ifhandle: 0x4000440
      Bkup path: is not valid
---- End of platform context data ----

```

## 関連コマンド

コマンド	説明
<a href="#">show cef</a> , ( <a href="#">171 ページ</a> )	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します。

# show cef recursive-nexthop

シスコ エクスプレス フォワーディング (CEF) 再帰的ネクストホップ情報を表示するには、EXEC モードで **show cef recursive-nexthop** コマンドを使用します。

**show cef recursive-nexthop [hardware] [location node-id]**

## 構文の説明

<b>hardware</b>	(任意) 再帰的ネクストホップに関するハードウェア情報を表示します。
<b>location node-id</b>	(任意) 指定されたノードの再帰的ネクストホップ情報を表示します。 <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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 関連コマンド

コマンド	説明
<a href="#">show cef</a> , (171 ページ)	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 します。

# 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、EXEC モードで **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

<b>location</b> <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。
<b>all</b>	(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 テーブルおよびアクティブ 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

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

```
RP/0/RSP0/CPU0:router# show cef summary location 0/1/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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 10: `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。
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。
revisions of existing leaves	既存のプレフィックスへの更新数。

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

## 関連コマンド

コマンド	説明
<a href="#">show cef</a> , (171 ページ)	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します。

## 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、EXEC モードで **show cef ipv4** コマンドを使用します。

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

### 構文の説明

vrf	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
vrf-name	(任意) VRF の名前。
prefix	(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。
mask	(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。
interface-type	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
interface-instance	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"> <li>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"> <li>° <i>rack</i> : ラックのシャーシ番号。</li> <li>° <i>slot</i> : ラインカードの物理スロット番号。</li> <li>° <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。</li> <li>° <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>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。</li> </ul> <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。 *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 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 EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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、**location** *node-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	操作
cef	読み取り

例 次に、**show cef ipv4** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4
Prefix          Next Hop          Interface
10.0.0.0/0      10.25.0.1         MgmtEth0/RSP0/CPU0/0
10.0.0.0/32     broadcast
10.25.0.0/16    attached          MgmtEth0/RSP0/CPU0/0
10.25.12.10/32  receive           MgmtEth0/RSP0/CPU0/0
10.25.13.12/32  10.25.13.12      MgmtEth0/RSP0/CPU0/0
10.25.16.11/32  10.25.16.11      MgmtEth0/RSP0/CPU0/0
10.25.22.10/32  10.25.22.10      MgmtEth0/RSP0/CPU0/0
10.25.26.10/32  10.25.26.10      MgmtEth0/RSP0/CPU0/0
10.25.41.2/32   10.25.41.2       MgmtEth0/RSP0/CPU0/0
10.25.41.5/32   10.25.41.5       MgmtEth0/RSP0/CPU0/0
10.25.42.5/32   10.25.42.5       MgmtEth0/RSP0/CPU0/0
10.25.44.15/32  10.25.44.15      MgmtEth0/RSP0/CPU0/0
10.25.55.2/32   10.25.55.2       MgmtEth0/RSP0/CPU0/0
10.25.255.255/32 10.25.255.255    MgmtEth0/RSP0/CPU0/0
```



```
10.0.0.0/4          0.0.0.0
10.0.0.1/32        0.0.0.0
10.255.255.255/32 broadcast
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 11: *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 隣接ステータスおよび設定情報を表示するには、EXEC モードで **show cef ipv4 adjacency** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>interface-type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface- path-id</b>	(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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <i>slot</i> : ラインカードの物理スロット番号。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>• 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。</li> </ul> <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>
<b>location node-id</b>	(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。
<b>detail</b>	(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-FastReroute (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 EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、**show cef ipv4 adjacency** コマンドは、コマンドが発行されるノードの CEF 隣接関係テーブルを表示します。

タスク ID

タスク ID	操作
cef	読み取り

例 次に、**show cef ipv4 adjacency** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router:# show cef ipv4 adjacency MgmtEth 0/RSP0/CPU0/0
Display protocol is ipv4
```

## show cef ipv4 adjacency

```

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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 12: 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 adjacency hardware

シスコ エクスプレス フォワーディング (CEF) IPv4 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、EXEC モードで **show cef ipv4 adjacency hardware** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv4 adjacency hardware** {*egress*|*ingress*} [*detail*|*discard*|*drop*|*glean*|*location node-id*] *null*|*punt*|*protected*|*remote*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>egress</b>	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。
<b>ingress</b>	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。
<b>detail</b>	(任意) 詳細情報を表示します。
<b>discard</b>	(任意) 廃棄隣接情報を表示します。
<b>drop</b>	(任意) ドロップ隣接情報を表示します。
<b>glean</b>	(任意) glean 隣接情報を表示します。
<b>location node-id</b>	(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。
<b>null</b>	(任意) ヌル隣接情報を表示します。
<b>punt</b>	(任意) パント隣接情報を表示します。
<b>protected</b>	(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。
<b>remote</b>	(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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**egress** キーワードを指定した **show cef ipv4 adjacency hardware** コマンドの load information フラグの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 adjacency hardware egress detail location 0/2/CPU0
```

```
Display protocol is ipv4
Interface      Address                                     Type      Refcount
-----
tt0            Prefix: 0.0.0.0/32                          local     5
               no next-hop adj
               Interface: NULLIFHNDL
               Mac-length is 0
               tunnel interface
               Interface Type: 0x24, Base Flags: 0x2001
               Dependent adj type: remote
               Dependent adj intf: tt0

TE Flags      : 0x41
TLU3(temp)   : 0x200b801
[HW: 0x00000001 0x20020000 0x08000000 0x00080000]
  type       : FWD
  num. entries : 1
  uidb index : 2
  num. labels : 0
  label      : 0
  encapsulation : unknown (0x8000000)
  next ptr   : 0x800
TLU4        : 0x3000800
Entry[0]
[HW: 0x00000080 0x0013c48f 0x880b05ea 0x00580000]
  label      : 0
  num. labels : 0
  local     : 1
  mtu       : 1514
  default sharq : 11
  member link : 0

Te0/2/0/1                                     special 2
```

```
Interface: Te0/2/0/1 Type: glean
Interface Type: 0x1e, Base Flags: 0x4400
Dependent adj type: remote
Dependent adj intf: Te0/2/0/1
```

TLU 3 Unavailable

次の表に、この出力で表示される重要なフィールドについて説明します。

表 13: *show cef ipv4 adjacency hardware* 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、EXEC モードで **show cef ipv4 drops** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

例 次に、ロケーション コマンドの **show cef ipv4 drops** の出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 drops

CEF Drop Statistics
Node: 0/0/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
```

表 14 : **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 によるドロップ <sup>1</sup>
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

<sup>1</sup> RPF = Reverse Path Forwarding

## 関連コマンド

コマンド	説明
<a href="#">clear cef ipv4 drops</a> , ( <a href="#">142 ページ</a> )	IPv4 CEF パケット ドロップ カウンタをクリアします。

## 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、EXEC モードで **show cef ipv4 exact-route** コマンドを使用します。

```
show cef [vrf vrf-name]ipv4 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

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>source-address</b>	x.x.x.x フォーマットの IPv4 送信元アドレス。
<b>destination-address</b>	x.x.x.x フォーマットの IPv4 宛先アドレス。
<b>protocol protocol name</b>	(任意) 指定したルートのプロトコルを表示します。
<b>source-port source-port</b>	(任意) UDP 送信元ポートを設定します。範囲は 0 ~ 65535 です。
<b>destination-port destination-port</b>	(任意) UDP 宛先ポートを設定します。範囲は 0 ~ 65535 です。
<b>ingress-interface</b>	(任意) 入力インターフェイスを設定します。
<b>type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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。
<b>policy-class value</b>	(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。
<b>detail</b>	(任意) CEF エントリの詳細情報を表示します。
<b>location node-id</b>	(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** EXEC

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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。

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 ipv4 exact-route** コマンドは、正しい結果を出力しません。

**タスク ID**

タスク ID	操作
cef	読み取り

**例**

次に、**show cef ipv4 exact-route** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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 MgmtEth0/RSP0RP1/CPU0/0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

**表 15: 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

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

## 関連コマンド

コマンド	説明
show mpls forwarding exact-route	送信元および宛先アドレスで構成される MPLS フローが通過するパスを表示します。

## 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、EXEC モードで **show cef ipv4 exceptions** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv4 exceptions** [*location node-id*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

## 例

次に、**show cef ipv4 exceptions** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 exceptions

CEF Exception Statistics
Node: 0/0/CPU0
  Slow encap packets :           0
  Redirect packets :           0
  Receive packets :          306404
  Broadcast packets :           0
  IP options packets :          0
  TTL expired packets :         0
  Fragmented packets :         0
Node: 0/1/CPU0
  Slow encap packets :           0
  Redirect packets :           0
  Receive packets :           0
  Broadcast packets :           0
  IP options packets :          0
  TTL expired packets :         0
  Fragmented packets :         0
Node: 0/2/CPU0
  Slow encap packets :           0
  Redirect packets :           0
  Broadcast packets :           0
  IP options packets :          0
  TTL expired packets :         314
  Fragmented packets :           0
Node: 0/3/CPU0
  Slow encap packets :           0
  Redirect packets :           0
  Receive packets :           0
  Broadcast packets :           0
  IP options packets :          0
  TTL expired packets :         0
  Fragmented packets :           0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 16: **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	ICMP の数 <sup>2</sup> 送信されるリダイレクトメッセージ
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 が期限切れとなったパケット数 <sup>3</sup>

## show cef ipv4 exceptions

フィールド	説明
Fragmented	フラグメントされたパケット数

<sup>2</sup> ICMP = インターネット制御メッセージプロトコル

<sup>3</sup> TTL = 存続可能時間

## 関連コマンド

コマンド	説明
<a href="#">clear cef ipv4 exceptions, (144 ページ)</a>	IPv4 CEF 例外パケット カウンタをクリアします。



## 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、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 ルーティングおよび転送 (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 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


EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

 show cef ipv4 hardware

タスク ID

タスク ID

操作

cef

読み取り

## show cef ipv4 interface

インターフェイスの IPv4 シスコ エクスプレス フォワーディング (CEF) に関連する情報を表示するには、EXEC モードで **show cef ipv4 interface** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv4 interface** *type interface-path-id* [**detail**] [**location node-id**]

### 構文の説明

<b>vrf</b>	(任意) VPNルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用してください。
<b>in interface-path-id</b>	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"> <li>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"> <li><i>rack</i> : ラックのシャーシ番号。</li> <li><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。</li> <li><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。</li> <li><i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>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。</li> </ul> <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>
<b>detail</b>	(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。
<b>location node-id</b>	(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。

**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** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、**show cef ipv4 interface rpf-statistics** 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	操作
	cef	読み取り

**例** 次に、**show cef ipv4 interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 interface MgmtEth 0/RSP0RP0/CPU0/0

MgmtEth0/0/CPU0/0 is up (if_handle 0x01000100)
  Forwarding is enabled
  ICMP redirects are never sent
  IP MTU 1500, TableId 0xe0000000
  Reference count 2
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 17: **show cef ipv4 interface** コマンドのフィールドの説明

フィールド	説明
MgmtEth 0/ RSP0 RP0 /CPU0/0 is up	インターフェイスのステータス
if_handle	内部インターフェイス ハンドル

フィールド	説明
Forwarding is enabled	シスコエクスプレスフォワーディング (CEF) がイネーブルであることを示します。
ICMP redirects are always sent or never sent	ICMPかどうかを示します。 <sup>4</sup> リダイレクトメッセージが送信されます。デフォルトでは、ICMPリダイレクトメッセージは必ず送信されます。
IP MTU	IPv4 MTUの値 <sup>5</sup> インターフェイスで設定されているサイズ
Reference count	内部リファレンス カウンタ

<sup>4</sup> ICMP = インターネット制御メッセージプロトコル

<sup>5</sup> MTU = 最大伝送ユニット

## show cef ipv4 interface bgp-policy-statistics

インターフェイスの IPv4 シスコ エクスプレス フォワーディング (CEF) に関連する ボーダー ゲートウェイ プロトコル (BGP) ポリシー 統計情報を表示するには、EXEC モードで **show cef ipv4 interface bgp-policy-statistics** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv4 interface** *type interface-path-id* **bgp-policy-statistics** [*location node-id*]

### 構文の説明

vrf	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
vrf-name	(任意) VRF の名前。
type	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
interface-path-id	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、 <b>show interfaces</b> 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) 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。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

このコマンドは ASR 9000 イーサネット ラインカードではサポートされていません。このコマンドは、指定されたインターフェイスに設定されているすべての BGP ポリシーカウンタを表示しません。

**タスク ID**

タスク ID	操作
cef	読み取り

**例**

次に、**show cef ipv4 interface bgp-policy-statistics** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 interface TenGigE 0/2/0/4 bgp-policy-statistics
```

```
TenGigE0/2/0/4 is up
Input BGP policy accounting on src IP address enabled
buckets packets bytes
0 184054 10157753
6 65688590 4204069760
7 65688590 4204069760
8 65688654 4204073856
9 65688656 4204073984
10 65688655 4204073920
30 32844290 1510837340
31 32844291 1510837386
32 32844294 1510837524
33 32844296 1510837616
34 32844298 1510837708
35 32844302 1510837892
36 32844302 1510837892
37 32844303 1510837938
38 32844305 1510838030
39 32844307 1510838122
Output BGP policy accounting on dst IP address enabled
buckets packets bytes
0 754 43878
Output BGP policy accounting on src IP address enabled
buckets packets bytes
0 857 51706
```

次の表に、この出力で表示される重要なフィールドについて説明します。

**表 18: show cef ipv4 interface bgp-policy-statistics コマンドのフィールドの説明**

フィールド	説明
TenGigE 0/2/0/4 is up	インターフェイスのステータス
Input BGP policy accounting on src IP address enabled	イネーブルにされている BGP ポリシー アカウンティング機能

## show cef ipv4 interface bgp-policy-statistics

フィールド	説明
buckets	トラフィック インデックス
packets	バケットでカウントされたパケット数
bytes	バケットでカウントされたバイト数



## show cef ipv4 non-recursive

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、EXEC モードで **show cef ipv4 non-recursive** コマンドを使用します。

```
show cef [vrf vrf-name] ipv4 non-recursive [detail] [hardware {egress|ingress}] [interface-type interface-instance] [location node-id]
```

### 構文の説明

vrf	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
vrf-name	(任意) VRF の名前。
detail	(任意) IPv4 CEF テーブルの非再帰的プレフィックス エントリの詳細を表示します。
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。
interface-type	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。

**interface-instance** (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に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/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。

**location node-id** (任意) 指定されたノードの IPv4 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      EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

## 例

次に、**show cef ipv4 non-recursive** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:routerrouter# show cef ipv4 non-recursive

Prefix          Next Hop          Interface
0.0.0.0/0       1012.8.0.1
0.0.0.0/32      broadcast
10.8.0.0/16     attached         MgmtEth0/0/CPU0/0
10.8.0.0/32     broadcast        MgmtEth0/0/CPU0/0
10.8.0.1/32     12.8.0.1        MgmtEth0/0/CPU0/0
10.8.0.2/32     12.8.0.2        MgmtEth0/0/CPU0/0
10.8.0.3/32     12.8.0.3        MgmtEth0/0/CPU0/0
10.8.16.10/32   12.8.16.10     MgmtEth0/0/CPU0/0
10.8.16.30/32   12.8.16.30     MgmtEth0/0/CPU0/0
10.8.16.40/32   12.8.16.40     MgmtEth0/0/CPU0/0
10.8.28.8/32    12.8.28.8      MgmtEth0/0/CPU0/0
10.8.28.101/32  12.8.28.101    MgmtEth0/0/CPU0/0
10.8.28.103/32  12.8.28.103    MgmtEth0/0/CPU0/0
10.8.28.104/32  12.8.28.104    MgmtEth0/0/CPU0/0
10.8.28.106/32  receive         MgmtEth0/0/CPU0/0
10.8.29.113/32  12.8.29.113    MgmtEth0/0/CPU0/0
10.8.29.118/32  12.8.29.118    MgmtEth0/0/CPU0/0
10.8.29.140/32  12.8.29.140    MgmtEth0/0/CPU0/0
10.8.33.101/32  12.8.33.101    MgmtEth0/0/CPU0/0
10.8.33.103/32  12.8.33.103    MgmtEth0/0/CPU0/0
10.8.33.105/32  12.8.33.105    MgmtEth0/0/CPU0/0
10.8.33.110/32  12.8.33.110    MgmtEth0/0/CPU0/0
10.8.57.1/32    12.8.57.1      MgmtEth0/0/CPU0/0
10.8.255.255/32 broadcast        MgmtEth0/0/CPU0/0
10.29.31.2/32   12.29.31.2     MgmtEth0/0/CPU0/0
10.255.0.0/16   attached        MgmtEth0/0/CPU0/0
10.255.254.254/32 10223.255.254.254 MgmtEth0/0/CPU0/0
10.0.0.0/4      0.0.0.0
10.0.0.0/24     receive
255.255.255.255/32 broadcast
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 19: **show cef ipv4 non-recursive** コマンドのフィールドの説明

フィールド	説明
Prefix	ノードで検出された非再帰的プレフィックス

## show cef ipv4 non-recursive

フィールド	説明
Next Hop	ルーティング ネクスト ホップ
Interface	非再帰的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 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、EXEC モードで **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

<b>detail</b>	(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。
<b>hardware</b>	(任意) ハードウェアの詳細情報を表示します。
<b>egress</b>	(任意) 出力パケット スイッチ交換 (PSE) を表示します。
<b>ingress</b>	(任意) 入力パケット スイッチ交換 (PSE) を表示します。
<b>location</b> <i>node-id</i>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
	cef	読み取り

## 例

次に、**show cef ipv4 resource** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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情報を表示するには、EXEC モードで **show cef ipv4 summary** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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情報が表示されます。

### タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef ipv4 summary** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 summary
Router ID is
10
0
.0.0.0

IP CEF with switching (Table Version 0)

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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 20: **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	Virtual router identification (vrid; 仮想ルータ ID) 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。



フィールド	説明
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。
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。

## 関連コマンド

コマンド	説明
bundle-hash	送信元および宛先アドレスで構成されるバンドルフローが通過するパスを表示します。

## 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、EXEC モードで **show cef ipv4 unresolved** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>detail</b>	(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。
<b>hardware</b>	(任意) ハードウェアの詳細情報を表示します。
<b>egress</b>	(任意) 出力パケット スイッチ交換 (PSE) を表示します。
<b>ingress</b>	(任意) 入力パケット スイッチ交換 (PSE) を表示します。
<b>location</b> <i>node-id</i>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

---



---

**例**

次に、未解決ルートが検出されるとき **show cef ipv4 unresolved** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv4 unresolved
```

```
Prefix           Next Hop           Interface
10.3.3.3         102.2.2.2         ?
```

次の表に、この出力で表示される重要なフィールドについて説明します。

**表 21: 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、EXEC モードで **show cef ipv6** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>interface-type</b> <b>interface-number</b>	(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。
<b>ipv6-prefix/prefix-length</b>	(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。
<b>detail</b>	(任意) IPv6 CEF テーブルの詳細情報を表示します。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

## 例

次に、**show cef ipv6** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6

::/0

::/128
  drop
::1/128
  loopback
66::4/128
  receive      Loopback0
2222::/64
  connected    gigabitethernet0/4/0/0
2222::1/128
  receive      gigabitethernet0/4/0/0
3333::/64
  connected    gigabitethernet0/3/0/0
3333::2/128
  receive      gigabitethernet0/3/0/0
5656::2/128
  recursive    fe80::3031:48ff:fe53:5533, gigabitethernet0/3/0/0
7777::/64
  connected    gigabitethernet0/0/0/0
7777::2/128
  receive      gigabitethernet0/0/0/0
9999::1/128
  recursive    fe80::205:5fff:fe1d:7600, gigabitethernet0/4/0/0
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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 22: **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。

フィールド	説明
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。
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。

次に、**detail** キーワードを持つ **show cef ipv6** の出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 detail
```

```
::/0
  flags: source_rib
  Loadinfo owner: <this route>
  fast adj: glean
  path 1:
    flags      :
    next hop   : ::
    interface  :
gigabitethernet0

/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
```

次の表に、この出力で表示される重要な出力フィールドについて説明します。

表 23: `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。
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"> <li>• flags : パスのプロパティ。</li> <li>• 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)。</li> <li>• 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)。</li> </ul>

## show cef ipv6 adjacency

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

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>interface-type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface- path-id</b>	(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"> <li>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"> <li>° <i>rack</i> : ラックのシャーシ番号。</li> <li>° <i>slot</i> : ラインカードの物理スロット番号。</li> <li>° <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。</li> <li>° <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>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。</li> </ul> <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>
<b>location node-id</b>	(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。
<b>detail</b>	(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) ノ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** EXEC

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

**例**

次に、**show cef ipv6 adjacency** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 adjacency
```

## 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、EXEC モードで **show cef ipv6 adjacency hardware** コマンドを使用します。

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

### 構文の説明

<i>vrf</i>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<i>vrf-name</i>	(任意) VRF の名前。
<i>egress</i>	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。
<i>ingress</i>	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。
<i>detail</i>	(任意) 詳細情報を表示します。
<i>discard</i>	(任意) 廃棄隣接情報を表示します。
<i>drop</i>	(任意) ドロップ隣接情報を表示します。
<i>glean</i>	(任意) <i>glean</i> 隣接情報を表示します。
<b>location</b> <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。
<i>null</i>	(任意) ヌル隣接情報を表示します。
<i>punt</i>	(任意) パント隣接情報を表示します。
<i>remote</i>	(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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef ipv6 adjacency hardware** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 adjacency hardware
```

## 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、EXEC モードで **show cef ipv6 drops** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv6 drops** [*location node-id*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

## 例

次に、**show cef ipv6 drops** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 drops location 0/2/CPU0
```

```
IPv6 CEF Drop Statistics
Line status down      ingress :          0 egress : Not Applicable
Packet sanity fail    ingress :          0 egress :          0
PLU set to drop       ingress :          0 egress :          0
Unknown type,plu drop ingress :          0 egress :          0
Packet length err     ingress :          0 egress :          0
TCAM src-comp err    ingress :          0 egress :          0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 24: **show cef ipv6 drop** コマンドのフィールドの説明

フィールド	説明
Line status down	着信インターフェイスの回線プロトコルがダウンしているため、パケットはドロップされます。
Packet sanity fail	プレフィックスが IPv6 健全性テストに失敗したため、パケットはドロップされます。健全性テストは、IPv6 パケットが有効かどうか検証されます。
PLU set to drop	IPv6 送信先プレフィックスがドロップするように設定されているため、パケットはドロップされます。
Unknown type, plu drop	プレフィックスのタイプが不明なため、パケットはドロップされます。
Packet length errs	ヘッダーに指定されている長さが、受信されたパケットの実際の長さとは一致しません。

フィールド	説明
TCAM src-comp err	ハードウェアで発生した送信元圧縮エラーのため、パケットはドロップされます。

```
RP/0/RSP0/CPU0:router# show cef ipv6 drops location 0/RSP0/CPU0
```

```
CEF Drop Statistics
Node: 0/RSP0/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 :
```

表 25 : `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 によるドロップ <sup>6</sup>
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	廃棄されたドロップ
GRE lookup drops	

フィールド	説明
GRE processing drops	

<sup>6</sup> RPF = Reverse Path Forwarding

## 関連コマンド

コマンド	説明
<a href="#">clear cef ipv6 drops</a> , ( <a href="#">150 ページ</a> )	IPv6 CEF パケット ドロップ カウンタをクリアします。

## show cef ipv6 exact-route

送信元および宛先アドレスで構成される IPv6 フローが通過するパスを表示するには、EXEC モードで **show cef ipv6 exact-route** コマンドを使用します。

```
show cef [ vrf vrf-name ] ipv6 exact-route { source-address destination-address } [ protocol name ] [ source-port ] [ destination-port ] [ ingress-interface type interface-path-id ] [ policy-class value ] [ detail ] [ location node-id ]
```

### 構文の説明

<b>vrf</b>	(任意) VPNルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>source-address</b>	x:x::x フォーマットの IPv6 送信元アドレス。
<b>destination-address</b>	x:x::x フォーマットの IPv6 宛先アドレス。
<b>protocol <i>protocol name</i></b>	(任意) 指定したルートのプロトコルを表示します。
<b>source-port <i>source-port</i></b>	(任意) UDP 送信元ポートを設定します。範囲は 0 ~ 65535 です。
<b>destination-port <i>destination-port</i></b>	(任意) UDP 宛先ポートを設定します。範囲は 0 ~ 65535 です。
<b>ingress-interface</b>	(任意) 入力インターフェイスを設定します。
<b>type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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。
<b>policy-class <i>value</i></b>	(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。
<b>detail</b>	(任意) CEF エントリの詳細情報を表示します。
<b>location <i>node-id</i></b>	(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** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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。

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、正しい結果を出力しません。

タスク ID	タスク ID	操作
	cef	読み取り

**例** 次に、**show cef ipv6 exact-route** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 exact-route 222::2 9999::6751 location
0/3/CPU0 source address: 222::2 destination address: 9999::6751
interface : TenGigE0/3/0/3 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、EXEC モードで **show cef ipv6 exceptions** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv6 exceptions** [*location node-id*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

例

次に、**show cef ipv6 exceptions** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 exceptions location 0/3/CPU0

IPv6 CEF Exception Statistics
Node: 0/3/CPU0
  TTL err          ingress :          0 egress : Not Applicable
  Link-local dst addr ingress :          0 egress :          0
  Hop-by-Hop header ingress :          0 egress :          0
  PLU entry set to punt ingress :          0 egress :          0
  Packet too big   ingress : Not Applicable egress :          0
  Med priority punt ingress :          0 egress : Not Applicable
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 26: **show cef ipv6 exceptions** コマンドのフィールドの説明

フィールド	説明
TTL err	IPv6 プレフィックスのパケットヘッダーで TTL エラーが発生したため、ソフトウェアに送信され処理されるパケット。★セグメント分割 <sup>7</sup> ★セグメント分割★
Link-local dst addr	IPv6 プレフィックスの宛先アドレスがリンクローカルのため、ソフトウェアに送信され処理されるパケット。
Hop-by-Hop header	IPv6 パケットにホップバイホップヘッダーがあるため、ソフトウェアに送信され処理されるパケット。
PLU entry set to punt	IPv6 プレフィックスがパントに設定されているため、ソフトウェアに送信され処理されるパケット。
Packet too big	パケットサイズが MTU を超えていたため、ソフトウェアに送信され処理されるパケット。 <sup>8</sup>
Med priority punt	トラブルシューティングのために内部的に使用されるフィールド。

<sup>7</sup> TTL = 存続可能時間<sup>8</sup> MTU = 最大伝送ユニット

## 関連コマンド

コマンド	説明
<a href="#">clear cef ipv6 exceptions, (152 ページ)</a>	IPv6 CEF 例外パケット カウンタをクリアします。

## 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、EXEC モードで **show cef ipv6 hardware** コマンドを使用します。

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

### 構文の説明

vrf	(任意) VPN ルーティングおよび転送 (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 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef ipv6 hardware** コマンドから詳細情報を表示した出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 hardware egress detail

::/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、EXEC モードで **show cef ipv6 interface** コマンドを使用します。

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

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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。
<b>detail</b>	(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。
<b>location node-id</b>	(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。
<b>rpf-drop</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

リリース	変更箇所
リリース 4.1.1	<b>rpf-drop</b> キーワードが追加されました。

**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。

**location** キーワードおよび *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	操作
	cef	読み取り

**例** 次に、**show cef ipv6 interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 interface
```



## show cef ipv6 non-recursive

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、EXEC モードで **show cef ipv6 non-recursive** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv6 non-recursive** [**hardware** {*egress*|*ingress*}] [**detail**] [**location** *node-id*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>hardware</b>	(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。
<b>egress</b>	(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。
<b>ingress</b>	(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。
<b>detail</b>	(任意) 詳細情報を表示します。
<b>location</b> <i>node-id</i>	(任意) 指定されたノードの IPv6 CEF テーブルの非再帰的プレフィックス 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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

タスク ID	タスク ID	操作
	cef	読み取り

**例** 次に、**show cef ipv6 non-recursive** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 non-recursive
::/0
::/128
  drop
::1/128
  loopback
66::4/128
  receive    Loopback0
2222::/64
  connected  gigabitethernet0/4/0/0
2222::1/128
  receive    gigabitethernet0/4/0/0
3333::/64
  connected  gigabitethernet0/3/0/0
3333::2/128
  receive    gigabitethernet0/3/0/0
7777::/64
  connected  gigabitethernet0/0/0/0
7777::2/128
  receive    gigabitethernet0/0/0/0
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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 27: *show cef ipv6 non-recursive* 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。
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。

## 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、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
	cef	読み取り

## 例

次に、**show cef ipv6 resource** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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情報を表示するには、EXEC モードで **show cef ipv6 summary** コマンドを使用します。

**show cef** [*vrf vrf-name*] **ipv6 summary** [*location node-id*]

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>location node-id</b>	(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。 <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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情報が表示されます。

### タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef ipv6 summary** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 28 : **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。

## show cef ipv6 summary

フィールド	説明
Router ID	ルータ ID。
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。

## 関連コマンド

コマンド	説明
bundle-hash	送信元および宛先アドレスで構成されるバンドルフローが通過するパスを表示します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference</i> 』を参照してください。



# 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、EXEC モードで **show cef ipv6 unresolved** コマンドを使用します。

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

## 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>detail hardware</b>	(任意) 詳細情報を表示します。 (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。
<b>hardware egress</b>	(任意) 出力パケット スイッチ交換 (CEF PSE) IPv6 ハードウェア ステータスおよび設定ファイルからシスコ エクスプレス フォワーディング情報を表示します。
<b>egress ingress</b>	(任意) 出力入力パケット スイッチ交換 (PSE) ファイルから情報を表示します。
<b>ingress detail</b>	(任意) 入力パケット スイッチ交換 (PSE) ファイル詳細情報から情報を表示します。
<b>location node-id</b>	(任意) 指定されたノードの IPv6 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、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	操作
cef	読み取り

#### 例

次に、未解決ルートが検出されるときの **show cef ipv6 unresolved** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef ipv6 unresolved
9999::/64
  unresolved
```

次の表に、この出力で表示される重要なフィールドについて説明します。

**表 29: 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、EXEC モードで **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) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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"> <li>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"> <li>° <i>rack</i> : ラックのシャーシ番号。</li> <li>° <i>slot</i> : ラインカードの物理スロット番号。</li> <li>° <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。</li> <li>° <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>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。</li> </ul> <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>
<b>detail</b>	(任意) 詳細情報を表示します。
<b>discard</b>	(任意) 廃棄隣接情報を表示します。
<b>drop</b>	(任意) ドロップ隣接情報を表示します。
<b>glean</b>	(任意) glean 隣接情報を表示します。
<b>null</b>	(任意) nul隣接情報を表示します。

## show cef mpls adjacency

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。
<b>location</b> <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 EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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。

**location** キーワードおよび *node-id* 引数でノードを指定しない場合、**show cef mpls adjacency** コマンドは、コマンドが発行されるノードの MPLS 隣接関係テーブルを表示します。

タスク ID	タスク ID	操作
	cef	読み取り

例 次に、**show cef mpls adjacency** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef mpls adjacency
```

## 関連コマンド

コマンド	説明
<a href="#">show cef mpls adjacency hardware, (254 ページ)</a>	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 ステータスおよび設定情報を表示します。
<a href="#">show cef mpls interface, (256 ページ)</a>	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) の関連情報を表示します。
<a href="#">show cef mpls unresolved, (258 ページ)</a>	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します。

## 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 ステータスおよび設定情報を表示するには、EXEC モードで **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) ヌ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 EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**タスク ID**

タスク ID	操作
cef	読み取り

**例**

次に、**show cef mpls adjacency hardware** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef mpls adjacency hardware
```

**関連コマンド**

コマンド	説明
<a href="#">show cef mpls adjacency, (251 ページ)</a>	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します。
<a href="#">show cef mpls interface, (256 ページ)</a>	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) の関連情報を表示します。
<a href="#">show cef mpls unresolved, (258 ページ)</a>	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します。

## 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、EXEC モードで **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

<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>in</b> <i>interface-path-id</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"> <li>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"> <li><i>rack</i> : ラックのシャーシ番号。</li> <li><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。</li> <li><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。</li> <li><i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルート プロセッサ カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0 RP0 または RP1) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 RP1/CPU0/0。</li> <li>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。</li> </ul> <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>
<b>detail</b>	(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。
<b>location</b> <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。

**コマンド モデル** EXEC ルートの動作または値はありません。



## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードおよび *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	操作
cef	読み取り

## 例

次に、**show cef mpls interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef mpls interface
```

## 関連コマンド

コマンド	説明
<a href="#">show cef mpls adjacency, (251 ページ)</a>	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します。
<a href="#">show cef mpls adjacency hardware, (254 ページ)</a>	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 ステータスおよび設定情報を表示します。
<a href="#">show cef mpls unresolved, (258 ページ)</a>	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します。

# 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、EXEC モードで **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

<b>detail</b>	(任意) レイヤ 2 情報など、隣接の詳細情報を表示します。
<b>location node-id</b>	(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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
cef	読み取り

## 例

次に、**show cef mpls unresolved** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef mpls unresolved
Label/EOS           Next Hop           Interface
```

20001/0  
20001/1

次の表に、この出力で表示される重要なフィールドについて説明します。

表 30 : *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

#### 関連コマンド

コマンド	説明
<a href="#">show cef mpls adjacency, (251 ページ)</a>	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します。
<a href="#">show cef mpls adjacency hardware, (254 ページ)</a>	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 ステータスおよび設定情報を表示します。
<a href="#">show cef mpls interface, (256 ページ)</a>	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) の関連情報を表示します。

## show cef vrf

VPNルーティング/転送（VRF）インスタンスのコンテンツを表示するには、EXECモードで **show cef vrf** コマンドを使用します。

**show cef vrf** [ *vrf-name* ]

構文の説明	vrf-name	VRF インスタンスの名前。
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	EXEC	
コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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。

未解決ルートを表示するには、**unresolved** キーワードを明示的に使用する必要があります。

タスク ID	タスク ID	操作
	cef	読み取り

**例** 次に、未解決ルートが検出されるとき **show cef vrf** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show cef vrf 0
Prefix          Next Hop      Interface
0.0.0.0/0      drop         default handler
0.0.0.0/32     broadcast
```

```
224.0.0.0/4          0.0.0.0
224.0.0.0/24        receive
255.255.255.255/32 broadcast
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 31: `show cef vrf` 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 vrf**



## DHCP コマンド

---

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータのダイナミック ホスト コンフィギュレーション プロトコル (DHCP) 機能の設定およびモニタに使用する Cisco IOS XR ソフトウェア コマンドについて説明します。

DHCP の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Addresses and Services Configuration Guide*』を参照してください。

- [clear dhcp ipv4 snoop binding, 265 ページ](#)
- [clear dhcp ipv6 proxy binding, 267 ページ](#)
- [destination \(DHCP IPv6\) , 269 ページ](#)
- [dhcp ipv4, 272 ページ](#)
- [dhcp ipv6, 274 ページ](#)
- [dhcp ipv4 none, 276 ページ](#)
- [giaddr policy, 278 ページ](#)
- [helper-address, 280 ページ](#)
- [helper-address \(IPv6\) , 282 ページ](#)
- [interface \(DHCP\) , 285 ページ](#)
- [profile \(DHCP\) , 287 ページ](#)
- [relay information check, 291 ページ](#)
- [relay information option, 293 ページ](#)
- [relay information option allow-untrusted, 296 ページ](#)
- [relay information policy, 299 ページ](#)
- [show dhcp ipv4 relay profile, 302 ページ](#)
- [show dhcp ipv4 relay profile name, 304 ページ](#)
- [show dhcp ipv4 relay statistics, 306 ページ](#)

- [show dhcp ipv4 snoop binding, 308 ページ](#)
- [show dhcp ipv6 interface, 310 ページ](#)
- [show dhcp ipv4 snoop statistics, 313 ページ](#)
- [show dhcp ipv6 proxy binding, 315 ページ](#)
- [trust relay-reply, 317 ページ](#)
- [trusted, 319 ページ](#)
- [vrf \(relay profile\) , 321 ページ](#)



# clear dhcp ipv4 snoop binding

スヌープ バインディングをクリアするには、EXEC モードで **clear dhcp ipv4 snoop binding** コマンドを使用します。

**clear dhcp ipv4 snoop binding** [*bridge-domain name*] [*mac-address mac-address*]

## 構文の説明

bridge-domain	(任意) 特定のブリッジドメインの DHCP スヌーピング バインディングをクリアします。
name	(任意) ブリッジドメイン名
mac-address	(任意) 指定された MAC アドレスの DHCP スヌーピング バインディングをクリアします。
mac-address	(任意) MAC アドレス

## コマンド デフォルト

すべてのスヌーピング バインディングをクリアします。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、**clear dhcp snoop binding** コマンドによりブリッジ ドメイン ISP1 を削除する例を示します

```
RP/0/RSP0/CPU0:router# clear dhcp ipv4 snoop binding bridge-domain ISP1
```

## clear dhcp ipv6 proxy binding

プレフィックス委任のダイナミック ホスト コンフィギュレーション プロトコル (DHCP) リレー バインディングをクリアするには、EXEC モードで **clear dhcp ipv6 proxy binding** コマンドを使用します。

**clear dhcp ipv6 proxy binding** [ *ipv6-prefix* ]

### 構文の説明

*ipv6-prefix* 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 に記載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 進数形式で指定します。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.1.1	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ip-services	実行

### 例

次に、**clear dhcp ipv6 proxy binding** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# clear dhcp ipv6 proxy binding
```

## 関連コマンド

コマンド	説明
<a href="#">show dhcp ipv6 proxy binding</a> , (315 ページ)	プレフィックス委任のダイナミック ホスト コンフィギュレーションプロトコル (DHCP) リレー バインディングを表示します。

## destination (DHCP IPv6)

クライアントメッセージの転送先宛先アドレスを指定し、インターフェイスでIPv6用ダイナミックホストコンフィギュレーションプロトコル (DHCP) リレーサービスをイネーブルにするには、DHCP IPv6 インターフェイスリレーコンフィギュレーションモードで **destination** コマンドを使用します。インターフェイス上のリレー宛先を削除するか、または宛先の出カインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**destination** *ipv6 address interface-path-id*

**no destination** *ipv6 address interface-path-id*

### 構文の説明

**ipv6 address address** IPv6 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。

**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にある管理イーサネットインターフェイスについては、物理スロット番号は英数字 (RP0 または RP1)、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RP1/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 モード

リレー機能はディセーブルになっており、インターフェイスにリレー宛先はありません。DHCP IPv6 インターフェイスリレーコンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**destination** コマンドは、クライアント メッセージを転送する宛先アドレスを指定し、インターフェイスで IPv6 用 DHCP リレー サービスをイネーブルにします。リレー サービスが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受信した IPv6 用 DHCP メッセージは、設定されたすべてのリレー宛先に転送されます。IPv6 用 DHCP 着信メッセージは、そのインターフェイスのクライアントから届いたか、または別のリレー エージェントによってリレーされた可能性があります。

リレー宛先は、サーバまたは別のリレー エージェントのユニキャストアドレス、またはマルチキャストアドレスにすることができます。次の 2 種類のリレーの宛先アドレスがあります。

- リンクスコープのユニキャストまたはマルチキャスト IPv6 アドレス。ユーザが出力インターフェイスを指定する必要があります。
- グローバルユニキャスト IPv6 アドレス。ユーザはこの種のアドレスに対する出力インターフェイスを指定できます。
- グローバルまたはサイトスコープのマルチキャスト IPv6 アドレス。ユーザは、'mhost ipv6 default-interface' が指定されている場合、この種のアドレスに対する出力インターフェイスを指定できます。

出力インターフェイスが宛先に設定されていない場合、出力インターフェイスはルーティング テーブルによって決まります。この場合、ユニキャストまたはマルチキャストルーティング プロトコルがルータで実行されていることを推奨します。

複数の宛先を 1 つのインターフェイスに設定でき、複数の出力インターフェイスを 1 つの宛先に設定することができます。リレー エージェントは、マルチキャストアドレスにメッセージをリレーする場合、IPv6 パケット ヘッダーのホップ制限フィールドを 32 に設定します。

指定されていない場合、ループバックおよびノードローカルマルチキャストアドレスは、リレー宛先として受け入れられません。いずれか 1 つが設定されている場合は、メッセージ「Invalid destination address」が表示されます。

サーバからの着信リレー応答メッセージを受信して転送するために、インターフェイスのリレー機能をイネーブルにする必要はないことに注意してください。デフォルトでは、リレー機能はディセーブルになっており、インターフェイスにリレー宛先はありません。このコマンドの **no** 形式は、インターフェイスのリレー宛先を削除するか、または宛先の出力インターフェイスを削

除します。すべてのリレー宛先が削除された場合、リレー サービスはインターフェイスでディセーブルになります。

IPv6 用 DHCP クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。これらの機能の1つがすでにイネーブルになっている場合、ユーザが同じインターフェイスに別の機能を設定しようとすると、「Interface is in DHCP client mode」、「Interface is in DHCP server mode」、または「Interface is in DHCP relay mode」のいずれかのメッセージが表示されます。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、Packet over Sonet/SDH (POS) インターフェイスでの **destination** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface pos 0/5/0/0 relay
RP/0/RSP0/CPU0:router(config-dhcpv6-if)# destination 10:10::10
```

## 関連コマンド

コマンド	説明
<a href="#">interface (DHCP)</a> , (285 ページ)	インターフェイスで IPv6 用 DHCP をイネーブルにします。

# dhcp ipv4

IPv4 用ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dhcp ipv4** コマンドを使用します。IPv4 の DHCP をディセーブルにして DHCP IPv4 コンフィギュレーション モードを終了するには、このコマンドの **no** 形式を使用します。

**dhcp ipv4**

**no dhcp ipv4**

## 構文の説明

このコマンドには、キーワードと引数はありません。

## コマンド モード

デフォルトの動作や値はありません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

リリース

変更箇所

リリース 3.7.2

このコマンドが導入されました。

リリース 4.2.0

このコマンドは、BNG でサポートされていました。

## 使用上のガイドライン

DHCP IPv4 コンフィギュレーション モードを開始するには、**dhcp ipv4** コマンドを使用します。

## タスク ID

タスク ID

操作

ip-services

読み取り、書き込み

## 例

次に、IPv4 の DHCP をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# dhcp ipv4
RP/0/RSP0/CPU0:router (config-dhcpv4) #
```



## 関連コマンド

コマンド	説明
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">vrf (relay profile)</a> , (321 ページ)	VRF 上のリレープロファイルを指定します。

## dhcp ipv6

IPv6 用ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) をイネーブルにし、DHCP IPv6 コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dhcp ipv6** コマンドを使用します。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。

**dhcp ipv6**

**no dhcp ipv6**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンドモード

グローバル コンフィギュレーション

### コマンド履歴

リリース

変更箇所

リリース 4.1.0

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID

操作

ip-services

読み取り、書き込み

### 例

次に、IPv6 の DHCP をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)#
```

## 関連コマンド

コマンド	説明
<a href="#">interface (DHCP)</a> , (285 ページ)	インターフェイスで IPv6 用ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) をイネーブルにします。

## dhcp ipv4 none

特定のポート上のDHCPスヌーピングをディセーブルにするには、l2vpnブリッジグループブリッジドメインインターフェイス コンフィギュレーション モードで **dhcp ipv4 none** コマンドを使用します。

### dhcp ipv4 none

#### 構文の説明

このコマンドには、キーワードと引数はありません。

#### 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

l2vpn ブリッジ グループ ブリッジ ドメイン インターフェイス コンフィギュレーション

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

#### タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

#### 例

次に、GigabitEthernet インターフェイス 0/0/0/0 上の DHCP スヌーピングをディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd) # interface gigabitethernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if) # dhcp ipv4 none
```

## 関連コマンド

コマンド	説明
<a href="#">show dhcp ipv4 snoop binding</a> , (308 ページ)	リレープロファイルに固有の DHCP リレーエージェント ステータスを表示します。

# giaddr policy

ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST パケットを Dynamic Host Configuration Protocol (DHCP) IPv4 Relay が処理する方法を設定するには、DHCP IPv4 プロファイルリレー コンフィギュレーションサブモードで **giaddr policy** コマンドを使用します。デフォルトの giaddr ポリシーに戻すには、このコマンドの **no** 形式を使用します。

**giaddr policy {replace| drop}**

**no giaddr policy {replace| drop}**

## 構文の説明

replace	既存の giaddr 値を、生成された値に置き換えます。
drop	既存のゼロ以外の giaddr 値を持つパケットをドロップします。

## コマンド デフォルト

DHCP IPv4 リレーは、クライアントの値から受信した DHCP IPv4 パケット内の既存のゼロ以外の giaddr 値を保持します。

## コマンド モード

DHCP IPv4 プロファイル リレー コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

## 使用上のガイドライン

**giaddr policy** コマンドは、ゼロ以外の giaddr 属性を持つ DHCP IPv4 クライアントから受信したパケットに対してだけ作用します。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、**giaddr policy** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# giaddr policy drop
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4</a> , (272 ページ)	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">helper-address</a> , (280 ページ)	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information check</a> , (291 ページ)	転送された BOOTREPLY メッセージ内のリレーエージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option</a> , (293 ページ)	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted</a> , (296 ページ)	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された <b>giaddr</b> を持つ BOOTREQUEST メッセージをドロップしないように設定します。
<a href="#">relay information policy</a> , (299 ページ)	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。

# helper-address

ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv4 および IPv6 リレー エージェントが BOOTREQUEST パケットを特定の DHCP サーバに中継するように設定するには、適切なコンフィギュレーションモードで **helper-address** コマンドを使用します。アドレスを消去するには、このコマンドの **no** 形式を使用します。

**helper-address** [*vrf vrf-name*] [*address*]

**no helper-address** [*vrf vrf-name*] [*address*]

## 構文の説明

<i>vrf-name</i>	(任意) 特定の VRF の名前を指定します。
<i>address</i>	4 分割ドット付き 10 進表記の IPv4 および IPv6 アドレス。

## コマンド デフォルト

ヘルパー アドレスは設定されていません。

## コマンド モード

DHCP IPv4 プロファイル リレー コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

8 つまでのヘルパー アドレスを設定できます。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み



## 例

次に、DHCP IPv4 プロファイルリレー コンフィギュレーションモードで **helper-address** コマンドを使用して VRF 用のヘルパー アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf v1 10.10.10.1
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4</a> , (272 ページ)	IPv4 の Dynamic Host Configuration Protocol (DHCP) をイネーブルにし、DHCP IPv4 コンフィギュレーションモードを開始します。
<a href="#">giaddr policy</a> , (278 ページ)	ゼロ以外の <b>giaddr</b> 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレー プロファイルを設定します。
<a href="#">relay information check</a> , (291 ページ)	転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option</a> , (293 ページ)	転送された BOOTREQUEST メッセージ内の DHCP リレー エージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted</a> , (296 ページ)	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された <b>giaddr</b> を持つ BOOTREQUEST メッセージをドロップしないように設定します。
<a href="#">relay information policy</a> , (299 ページ)	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">vrf (relay profile)</a> , (321 ページ)	VRF 上のリレー プロファイルを指定します。

## helper-address (IPv6)

プレフィックス委任のダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv6 リレーエージェントが DHCP パケットを特定の DHCP サーバに中継するように設定するには、DHCP IPv6 プロファイル コンフィギュレーション サブモードで **helper-address** コマンドを使用します。アドレスを消去するには、このコマンドの **no** 形式を使用します。

**helper-address** *ipv6-address* [ **interface** *type interface-path-id* ]

**no helper-address** *ipv6-address* [ **interface** *type interface-path-id* ]

### 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 に記載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 進数形式で指定します。
<b>interface</b> <i>type</i>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

*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。

- 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* : ラックのシャーン番号。

◦ *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に関しては、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

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

DHCP IPv6 プロファイル コンフィギュレーション

## コマンド履歴

リリース

変更箇所

リリース 4.1.1

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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

**例** 次に、**helper-address** コマンドを使用してヘルパーアドレスを設定する方法を示す出力例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config) # dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6) # profile p1 proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-profile) # helper-address 2001:db8::3 GigabitEthernet
0/2/0/0
```

#### 関連コマンド

コマンド	説明
<a href="#">dhcp ipv6</a> , <a href="#">(274 ページ)</a>	IPv6 用ダイナミック ホスト コンフィギュレーションプロトコル (DHCP) をイネーブルにします。

## interface (DHCP)

インターフェイスでIPv4/IPv6用ダイナミックホストコンフィギュレーションプロトコル (DHCP) 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 **interface** コマンドを使用します。インターフェイスの DHCPv4/DHCPv6 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。

**interface** *interface-type* *interface-instance* {**relay**}

### 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 カードにある管理イーサネット インターフェイスについては、物理スロット番号は英数字 (RP0 または RP1)、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RP1/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。

ルータ構文の詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。

**relay** 宛先アドレスを指定します。

### コマンド デフォルト コマンド モード

デフォルトの動作または値はありません。  
DHCP IPv4 configuration

## コマンド履歴

リリース	変更内容
リリース 4.1.0	このコマンドが追加されました。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、**interface** コマンドを使用して、Packet over Sonet/SDH (POS) インターフェイスで DHCP インターフェイス モードをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# interface POS 0/5/0/0 relay
```

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# interface POS 0/5/0/0 relay
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv6, (274 ページ)</a>	IPv6 用ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) をイネーブルにし、DHCP IPv6 コンフィギュレーション モードを開始します。
<a href="#">dhcp ipv4, (272 ページ)</a>	IPv4 の Dynamic Host Configuration Protocol (DHCP) をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">show dhcp ipv6 interface, (310 ページ)</a>	IPv6 用 DHCP のインターフェイス情報を表示します。

## profile (DHCP)

Dynamic Host Configuration Protocol (DHCP) IPv4 コンポーネントの DHCP リレー プロファイルまたは DHCP スヌーピング プロファイルを設定し、プロファイル モードを開始するには、DHCP IPv4 コンフィギュレーション モードで **profile** コマンドを使用します。この機能をディセーブルにしてプロファイル モードを終了するには、このコマンドの **no** 形式を使用します。

**profile name** {relay | snoop}

**noprofile name** {relay | snoop}

### 構文の説明

**profile-name** リレーまたはスヌーピング プロファイルを一意に識別する名前。

**relay** DHCP リレー プロファイルを設定します。DHCP リレー エージェントとは、クライアントとサーバ間で DHCP パケットを転送するホストです。クライアントとサーバが同じ物理サブネット上にない場合、リレー エージェントがクライアントとサーバ間で要求および応答を転送するために使用されます。

DHCP リレー エージェントとは、クライアントとサーバ間で DHCP パケットを転送するホストです。リレー エージェントは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送するために使用されます。リレー エージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間である程度透過的にスイッチングされます。対照的に、リレー エージェントは DHCP メッセージを受信すると、新たに DHCP メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ IP アドレスを設定し (DHCP パケットの **giaddr** フィールド)、設定されている場合にはパケットにリレー エージェント情報オプション (Option 82) を追加して、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Cisco IOS DHCP リレー エージェントは、スマート リレー エージェント転送の使用を含め、アンナンバードインターフェイスの使用をサポートしています。アンナンバードインターフェイスを介して DHCP クライアントが接続される場合、DHCP リレー エージェントでは、その DHCP クライアントがアドレスを取得してからスタティック ホスト ルートを自動で追加します。このとき、アンナンバードインターフェイスは、発信インターフェイスに指定されます。リース時間経過後、またはクライアントがアドレスをリリースした場合、ルートは自動的に削除されます。

**snoop** DHCP スヌーピング プロファイルを設定します。DHCP スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング テーブルを構築およびメンテナンスすることで安全性を持たせる DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できない DHCP メッセージをフィルタリングし、DHCP スヌーピング バインディング テーブルを構築およびメンテナンスすることで安全性を持たせる DHCP セキュリティ機能です。信頼できないメッセージとは、ネットワークまたはファイアウォール外部からの受信メッセージのうち、ネットワーク内でトラフィック攻撃を引き起こす可能性のあるメッセージです。

DHCP スヌーピング バインディング テーブルには、MAC アドレス、IP アドレス、リース時間、バインディング タイプ、VLAN 番号、およびスイッチの信頼できない ローカル インターフェイスに対応する インターフェイス情報が含まれています。このデータベースには、信頼できる インターフェイスに相互接続されたホストの情報はありません。信頼できない インターフェイスとは、ネットワークまたはファイアウォール外部からのメッセージを受信するように設定された インターフェイスです。信頼できる インターフェイスとは、ネットワーク内からのメッセージのみを受信するように設定された インターフェイスです。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。また、DHCP スヌーピングはエンドユーザに接続する信頼できない インターフェイスと、DHCP サーバまたは別のスイッチに接続する信頼できる インターフェイスとを差異化する方法を提供します。

**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** DHCP IPv4 configuration

**コマンド履歴**

リリース	変更箇所
リリース 3.7.2	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。



## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、**relay** プロファイルのために **profile** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4, (272 ページ)</a>	DHCP IPv4 コンフィギュレーションモードを開始します。
<a href="#">giaddr policy, (278 ページ)</a>	ゼロ以外の <b>giaddr</b> 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address, (280 ページ)</a>	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">relay information check, (291 ページ)</a>	転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option, (293 ページ)</a>	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted, (296 ページ)</a>	DHCP コンポーネントが、設定されたりレー情報オプションおよびゼロに設定された <b>giaddr</b> を持つ BOOTREQUEST メッセージをドロップしないように設定します。
<a href="#">relay information policy, (299 ページ)</a>	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">vrf (relay profile) , (321 ページ)</a>	VRF 上のリレー プロファイルを指定します。



# relay information check

転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを Dynamic Host Configuration Protocol (DHCP) IPv4 Relay が検証するように設定するには、DHCP IPv4 リレー プロファイル コンフィギュレーション サブモードで **relay information check** 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。

**relay information check**

**no relay information check**

## 構文の説明

このコマンドには、キーワードと引数はありません。

## コマンド デフォルト

DHCP は、リレー エージェント情報オプションを検証します。

## コマンド モード

DHCP IPv4 リレー プロファイル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

## 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。

## タスク ID

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

## 例

次に、**relay information check** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information check
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4</a> , (272 ページ)	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">giaddr policy</a> , (278 ページ)	ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address</a> , (280 ページ)	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information option</a> , (293 ページ)	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted</a> , (296 ページ)	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された giaddr を持つ BOOTREQUEST メッセージをドロップしないように設定します。
<a href="#">relay information policy</a> , (299 ページ)	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">vrf (relay profile)</a> , (321 ページ)	VRF 上のリレー プロファイルを指定します。

## relay information option

転送された BOOTREQUEST メッセージ内のリレー エージェント 情報オプションを DHCP サーバに挿入するように、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv4 リレーまたは DHCP スヌーピング Relay を設定するには、DHCP IPv4 リレー プロファイル リレー コンフィギュレーションまたは DHCP IPv4 プロファイル スヌーピング サブモードで **relay information option** コマンドを使用します。転送された BOOTREQUEST メッセージにリレー情報を挿入すること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。

**relay information option**

**no relay information option**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### 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

DHCP IPv4 リレー プロファイル リレー コンフィギュレーション

DHCP IPv4 プロファイル スヌーピング コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

### 使用上のガイドライン

**relay information option** コマンドは、回線 ID 情報サブオプションおよびリモート ID サブオプションを DHCP リレー エージェント情報オプションに自動的に追加します。

**relay information option** コマンドは、DHCP サーバが、要求を送信するユーザ（ケーブル アクセスマルータなど）を識別してこの情報に基づく適切なアクションを開始することをイネーブルにします。デフォルトでは、DHCP はリレー情報を挿入しません。

**information option** コマンドがイネーブルにされると、DHCP スヌーピング モードは DHCP パケット内の giaddr フィールドを設定しません。

アップストリーム DHCP サーバまたは DHCP リレー インターフェイスは、このタイプのパケットを受け入れるように、**relay information option allow-untrusted** コンフィギュレーションを使用し

て設定する必要があります。この設定により、サーバまたはリレーが DHCP メッセージをドロップしないようになります。

## タスク ID

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

## 例

次に、**relay information option** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4</a> , (272 ページ)	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">giaddr policy</a> , (278 ページ)	ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address</a> , (280 ページ)	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information check</a> , (291 ページ)	転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option allow-untrusted</a> , (296 ページ)	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された giaddr を持つ BOOTREQUEST メッセージをドロップしないように設定します。

コマンド	説明
<a href="#">relay information policy</a> , (299 ページ)	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">vrf (relay profile)</a> , (321 ページ)	VRF 上のリレー プロファイルを指定します。

# relay information option allow-untrusted

ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv4 リレー または DHCP スヌーピング リレーが、設定されたリレー情報オプションおよびゼロに設定した `giaddr` を持つパケットをドロップ BOOTREQUEST を廃棄しないように設定するには、DHCP IPv4 リレー プロファイル コンフィギュレーション サブモード または DHCP IPv4 プロファイル スヌーピング コンフィギュレーション サブモード で **relay information option allow-untrusted** コマンドを使用します。デフォルト動作、つまり、リレー情報オプションを持ち、`giaddr` をゼロに設定する BOOTREQUEST パケットを廃棄する動作に戻すには、このコマンドの **no** 形式を使用します。

**relay information option allow-untrusted**

**no relay information option allow-untrusted**

## 構文の説明

このコマンドには、キーワードと引数はありません。

## コマンド デフォルト

リレー情報が設定されて `giaddr` がゼロに設定されている場合、パケットはドロップされます。

## コマンド モード

DHCP IPv4 リレー プロファイル リレー コンフィギュレーション  
DHCP IPv4 プロファイル スヌーピング コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

RFC 3046 に従い、`giaddr` がゼロに設定されていてもリレー エージェント オプションがすでにパケット内に存在する信頼できない回線から DHCP パケットを受信するリレー エージェント (およびサーバ) は、パケットを廃棄して、エラー数を増加させるものとします。この設定により、サーバまたはリレーが DHCP メッセージをドロップしないようになります。



## タスク ID

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

## 例

次に、**relay information option allow-untrusted** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4, (272 ページ)</a>	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーションモードを開始します。
<a href="#">giaddr policy, (278 ページ)</a>	ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address, (280 ページ)</a>	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP) , (287 ページ)</a>	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information check, (291 ページ)</a>	転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option, (293 ページ)</a>	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information policy, (299 ページ)</a>	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。

コマンド	説明
vrf (relay profile) , (321 ページ)	VRF 上のリレー プロファイルを指定します。

## relay information policy

リレー情報オプションがすでに含まれている BOOTREQUEST パケットをダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv4 リレー Relay が処理する方法を設定するには、DHCP IPv4 プロファイル リレー プロファイル コンフィギュレーション モードで **relay information policy** コマンドを使用します。デフォルトのリレー情報ポリシーに戻すには、このコマンドの **no** 形式を使用します。

**relay information policy {drop| keep}**

**no relay information policy {drop| keep}**

### 構文の説明

drop	既存のリレー情報オプションを持つ BOOTREQUEST パケットを廃棄するように、DHCP IPv4 リレーに指示します。
keep	既存のリレー情報オプションとともに受信された BOOTREQUEST パケットを廃棄しないで、既存のリレー情報オプション値を保持するように、DHCP IPv4 Relay に指示します。

### コマンド デフォルト

DHCP IPv4 Relay は、既存のリレー情報オプションを持つ BOOTREQUEST パケットを廃棄しません。オプションと既存のリレー情報オプション値は置き換えられます。

### コマンド モード

DHCP IPv4 リレー プロファイル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

### 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。

## タスク ID

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

## 例

次に、**relay information policy** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay
RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information policy keep
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4, (272 ページ)</a>	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">giaddr policy, (278 ページ)</a>	ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address, (280 ページ)</a>	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP) , (287 ページ)</a>	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information check, (291 ページ)</a>	転送された BOOTREPLY メッセージ内のリレーエージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option, (293 ページ)</a>	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted, (296 ページ)</a>	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された giaddr を持つ BOOTREQUEST メッセージをドロップしないように設定します。

コマンド	説明
vrf (relay profile) , (321 ページ)	VRF 上のリレー プロファイルを指定します。

# show dhcp ipv4 relay profile

Dynamic Host Configuration Protocol (DHCP) リレー エージェント ステータスを表示するには、EXEC モードで **show dhcp ipv4 relay profile** コマンドを使用します。

## show dhcp ipv4 relay profile

### 構文の説明

このコマンドには、キーワードと引数はありません。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドは、DHCP IPv4 に作成されたリレー プロファイルを表示します。

### タスク ID

タスク ID	操作
ip-services	読み取り

### 例

次に、**show dhcp ipv4 relay profile** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 relay profile
DHCP IPv4 Relay Profiles
-----
r1
r2
```

## 関連コマンド

コマンド	説明
<a href="#">show dhcp ipv4 relay profile name, (304 ページ)</a>	リレープロファイルに固有の Dynamic Host Configuration Protocol (DHCP) リレーエージェントステータスを表示します。

## show dhcp ipv4 relay profile name

リレー プロファイルに固有の Dynamic Host Configuration Protocol (DHCP) リレー エージェント ステータスを表示するには、EXEC モードで **show dhcp ipv4 relay profile name** コマンドを使用します。

**show dhcp ipv4 relay profile [name]**

### 構文の説明

name	(任意) リレー プロファイルを一意に識別する名前。
------	----------------------------

### コマンド デフォルト

*name* が指定されない場合、設定済みの DHCP プロファイル名のリストを表示します。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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ip-services	読み取り

### 例

次に、**show dhcp ipv4 relay profile name** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 relay profile name r1
DHCP IPv4 Relay Profile r1:
```



```
Helper Addresses:  
10.10.10.1, vrf default  
Information Option: Disabled  
Information Option Allow Untrusted: Disabled  
Information Option Policy: Replace  
Information Option Check: Disabled  
Giaddr Policy: Keep  
Broadcast-flag Policy: Ignore  
  
VRF References:  
default  
Interface References:  
FINT0_RSP1_CPU0  
MgmtEth0_RSP1_CPU0_0
```

## show dhcp ipv4 relay statistics

VPNルーティングおよび転送（VRF）インスタンスのダイナミック ホスト コンフィギュレーション プロトコル（DHCP）IPv4 リレー エージェント パケット 統計 情報を表示するには、EXEC モードで **show dhcp ipv4 relay statistics** コマンドを使用します。

**show dhcp [vrf {vrf-name| default}] ipv4 relay statistics**

### 構文の説明

<b>vrf</b> <i>vrf-name</i>	(任意) VRF を一意に識別する名前。
<b>default</b>	(任意) デフォルト VRF のリレー統計情報を表示します。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ip-services	読み取り

### 例

次に、省略可能なキーワードや引数を使用されない場合の **show dhcp ipv4 relay statistics** コマンド コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 relay statistics
```

```

----- Bridge | RX | TX | DR |
default | 0 | 0 | 0 |

```

次に、**vrf** および **default** キーワードを使用した **show dhcp ipv4 relay statistics** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp vrf default ipv4 relay statistics
Sun Apr 6 07:10:35.873 UTC
```

DHCP IPv4 Relay Statistics for VRF default:

```

----- TYPE | RECEIVE | TRANSMIT | DROP |
DISCOVER | 0 | 0 | 0 |
OFFER | 0 | 0 | 0 |
REQUEST | 0 | 0 | 0 |
DECLINE | 0 | 0 | 0 |
ACK | 0 | 0 | 0 |
NAK | 0 | 0 | 0 |
RELEASE | 0 | 0 | 0 |
INFORM | 0 | 0 | 0 |
LEASEQUERY | 0 | 0 | 0 |
LEASEUNASSIGNED | 0 | 0 | 0 |
LEASEUNKNOWN | 0 | 0 | 0 |
LEASEACTIVE | 0 | 0 | 0 |
BOOTP-REQUEST | 0 | 0 | 0 |
BOOTP-REPLY | 0 | 0 | 0 |
BOOTP-INVALID | 0 | 0 | 0 |

```

# show dhcp ipv4 snoop binding

DHCP スヌーピング バインディングに関する情報を表示するには、EXEC モードで **show dhcp ipv4 snoop binding** コマンドを使用します。

**show dhcp ipv4 snoop binding** [**mac-address** *mac-address*] **summary**]

## 構文の説明

<b>mac-address</b> <i>mac-address</i>	(任意) 指定された MAC アドレスに関連付けられた DHCP スヌーピング クライアント バインディングの詳細を表示します。
<b>summary</b>	(任意) DHCP スヌーピング クライアント バインディングの総数を表示します。

## コマンド デフォルト

すべての DHCP スヌーピング クライアント バインディングに関する情報の要約を表示します。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
ip-services	読み取り

## 例

次に、すべての MAC アドレスの **dhcp ipv4 snoop binding** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 snoop binding
```

Sun Apr 6 05:58:07.741 UTC

MAC Address	IP Address	State	Lease Remaining	Interface	Bridge Domain
0000.6402.0102	192.128.0.1	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0103	192.128.0.2	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0104	192.128.0.3	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0105	192.128.0.4	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0106	192.128.0.5	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0107	192.128.0.6	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0108	192.128.0.7	BOUND	2499	Gi0/2/0/20.111	mgmtEth
0000.6402.0109	192.128.0.8	BOUND	2499	Gi0/2/0/20.111	mgm:mhd
0000.6402.010a	192.128.0.9	BOUND	2499	Gi0/2/0/20.111	mgm:mhd
0000.6402.010b	192.128.0.10	BOUND	2499	Gi0/2/0/20.111	mgm:mhd

次に、省略可能な **summary** キーワードを使用した **show dhcp ipv4 snoop binding** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 snoop binding summary
Sun Apr 6 06:45:03.878 UTC
```

Number of IPv4 DHCP Snoop bindings: 10

次に、特定の MAC アドレスを使用した **show dhcp ipv4 snoop binding** コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 snoop binding mac-address 0000.6402.0102
Sun Apr 6 06:45:03.878 UTC
```

```
MAC Address:      0000.6402.0102
IP Address:       192.128.0.1
Client ID:        0064
Profile:          s1
State:            BOUND
Lease (sec):      3600
Remaining (sec):  2833
Bridge Domain:    mgm:mhd
Interface:        GigabitEthernet0/2/0/10.111
```

## 関連コマンド

コマンド	説明
<a href="#">clear dhcp ipv4 snoop binding</a> , (265 ページ)	DHCP スヌーピングバインディングをクリアします。
<a href="#">show dhcp ipv4 snoop statistics</a> , (313 ページ)	特定のブリッジドメインの統計情報を表示します。

## show dhcp ipv6 interface

IPv6用ダイナミックホストコンフィギュレーションプロトコル (DHCP) インターフェイス情報を表示するには、EXEC モードで、**show dhcp ipv6 interface** コマンドを使用します。

**show dhcp ipv6 interface** *interface-type interface-instance*

### 構文の説明

*interface-type* インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

*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にある管理イーサネットインターフェイスについては、物理スロット番号は英数字 (RP0 または RP1)、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RP1/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      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          EXEC

## コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

インターフェイスが指定されていない場合は、IPv6 用 DHCP (クライアントまたはサーバ) がイネーブルになっているすべてのインターフェイスが表示されます。インターフェイスが指定される場合、指定されているインターフェイスに関する情報だけが表示されます。

## タスク ID

タスク ID	操作
ip-services	読み取り

## 例

次に、インターフェイスが指定されていない場合の **show dhcp ipv6 interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 interface
GigabitEthernet 0/0/0/1 is in relay mode
Relay destinations:
  2001:eb8:1::1
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 32: **show dhcp ipv6 interface** コマンドのフィールドの説明

フィールド	説明
GigabitEthernet 0/0/0/1 is in relay mode	指定されたインターフェイスがリレーモードであるかどうかを表示します。

## 関連コマンド

コマンド	説明
<a href="#">interface (DHCP)</a> , (285 ページ)	インターフェイスで IPv6 用 DHCP をイネーブルにします。

```
show dhcp ipv6 interface
```



# show dhcp ipv4 snoop statistics

特定のブリッジドメインの統計情報を表示するには、EXEC モードで **show dhcp ipv4 snoop statistics** コマンドを使用します。

**show dhcp ipv4 snoop statistics** [**bridge-domain** *bridge-domain-name*]

## 構文の説明

**bridge-domain** *bridge-domain-name* (任意) 特定のブリッジドメインを指定します。

## コマンド デフォルト

各ブリッジドメインのDHCPスヌーピングの受信 (RX)、送信 (TX)、およびドロップ (DR) のパケット統計情報を表示します。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
ip-services	読み取り

## 例

次に、**show dhcp ipv4 snoop statistics** コマンドからの出力例、および各ブリッジドメインのDHCPスヌーピング RX、TX、および DR のパケット統計情報のテーブルを示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 snoop statistics
Sun Apr 6 05:55:57.524 UTC
```

Bridge	RX	TX	DR
--------	----	----	----

## show dhcp ipv4 snoop statistics

```
-----
mgm:mhd | 964 | 964 | 0 |
```

次に、**show dhcp ipv4 snoop statistics** コマンドからの出力例、および特定のブリッジドメインの DHCP スヌーピング RX、Tx、およびドロップのパケット統計情報のテーブルを示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv4 snoop statistics bridge-domain mgm:mhd
Sun Apr 6 05:57:03.600 UTC
```

DNCP IPv4 Snoop Statistics for Bridge mgm:mhd:

TYPE	RECEIVE	TRANSMIT	DROP
DISCOVER	111	111	0
OFFER	111	111	0
REQUEST	371	371	0
DECLINE	0	0	0
ACK	371	371	0
NAK	0	0	0
RELEASE	0	0	0
INFORM	0	0	0
LEASEQUERY	0	0	0
LEASEUNASSIGNED	0	0	0
LEASEUNKNOWN	0	0	0
LEASACTIVE	0	0	0
BOOTP-REQUEST	0	0	0
BOOTP-REPLY	0	0	0
BOOTP-INVALID	0	0	0

## 関連コマンド

コマンド	説明
<a href="#">show dhcp ipv6 binding</a>	DHCP スヌーピング クライアント バインディングを表示します。
<a href="#">show dhcp ipv4 snoop binding</a> , (308 ページ)	特定の DHCP スヌーピング プロファイルの詳細を表示します。

## show dhcp ipv6 proxy binding

ダイナミックホストコンフィギュレーションプロトコル (DHCP) プロキシのクライアントバインディングを表示するには、EXEC モードで **show dhcp ipv6 proxy binding** コマンドを使用します。

**show dhcp ipv6 proxy binding** {detail| duid| interface| interface-id| location| mac-address| remote-id| summary| vrf}

### 構文の説明

<b>detail</b>	プロキシの詳細なバインディングを表示します。
<b>duid</b>	DUID のクライアントバインディングを表示します。
<b>interface</b>	インターフェイス別のクライアントバインディングを表示します。
<b>interface-id</b>	インターフェイス ID 別のクライアントバインディングを表示します。
<b>location</b>	ノードの場所を指定します。
<b>mac-address</b>	詳細なクライアントバインディング情報を表示します。
<b>remote-id</b>	リモート ID 別のクライアントバインディングを表示します。
<b>summary</b>	プロキシのサマリーバインディングを表示します。
<b>vrf</b>	VRF 名別のクライアントバインディングを表示します。

**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** EXEC

### コマンド履歴

リリース	変更内容
リリース 4.1.1	このコマンドが追加されました。

**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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID	タスク ID	操作
	ip-services	読み取り

**例** 次に、**show dhcp ipv6 proxy binding** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy binding
Summary:
  Total number of Proxy bindings = 1
Prefix: 2001::/60 (Gi0/0/0/1)
DUID: 00030001ca004a2d0000
IAID: 00020001
lifetime: 2592000
expiration: Nov 25 2010 16:47

RP/0/RSP0/CPU0:router# show dhcp ipv6 proxy binding summary
Total number of clients: 2

      STATE                |          COUNT          |
      |                   | IA-NA | IA-PD |
-----|-----|-----|-----|
INIT                |          0          | 0 |
SUB VALIDATING      |          0          | 0 |
ADDR/PREFIX ALLOCATING |          0          | 0 |
REQUESTING          |          0          | 0 |
SESSION RESP PENDING |          2          | 0 |
ROUTE UPDATING      |          0          | 0 |
BOUND               |          0          | 0 |
```

#### 関連コマンド

コマンド	説明
<a href="#">clear dhcp ipv6 proxy binding</a> , (267 ページ)	プレフィックス委任のダイナミック ホスト コンフィギュレーションプロトコル (DHCP) リレー バインディングをクリアします。

## trust relay-reply

relay-reply の処理をイネーブルにするように DHCP IPv6 プロファイルを設定するには、DHCP IPv6 プロファイル コンフィギュレーション モードで **trust relay-reply** コマンドを使用します。インターフェイスをデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

**trust relay-reply**

**no trust relay-reply**

このコマンドには、キーワードと引数はありません。

**コマンド デフォルト** デフォルトでは、すべてのインターフェイスは信頼できます。

**コマンド モード** DHCP IPv6 プロファイル コンフィギュレーション

**コマンド履歴**

リリース	変更箇所
リリース 4.1.1	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**タスク ID**

タスク ID	操作
ip-services	読み取り、書き込み

**例**

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dhcp ipv6
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile downstream proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# helper-address ff05::1:3
RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# exit
RP/0/RSP0/CPU0:router(config-dhcpv6)# profile upstream proxy
RP/0/RSP0/CPU0:router(config-dhcpv6-profile)# trust relay-reply
```

## 関連コマンド

コマンド	説明
<a href="#">helper-address (IPv6)</a> , (282 ページ)	プレフィックス委任のダイナミック ホスト コンフィギュレーションプロトコル (DHCP) IPv6 リレー エージェントを設定します。

# trusted

サポートおよび信頼されている発信元に対して DHCP スヌーピング プロファイルを設定するには、DHCP IPv4 Profile Snoop コンフィギュレーション モードで **trusted** コマンドを使用します。インターフェイスをデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

**trusted**

**no trusted**

## コマンド デフォルト

デフォルトでは、DHCP スヌーピング プロファイルは、信頼できない発信元です。

## コマンド モード

DHCP IPv4 Snoop Profile コンフィギュレーション モード

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

ブリッジ ポートは、この DHCP スヌーピング プロファイルをブリッジ ポートまたはブリッジ ドメインに割り当てることによって、信頼できる設定にできます。

DHCP スヌーピングは、DHCP DISCOVER および DHCP REQUEST メッセージを、信頼できるインターフェイスだけに選択的に転送することにより、異常なホストで DHCP 交換が行われなくなります。

## タスク ID

タスク ID	操作
ip-services	読み取り

## 例

次に、trustedServerProfile という名前のスヌープ プロファイルを信頼できる設定にする例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# profile trestedServerProfile snoop
RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# trusted
```

## 関連コマンド

コマンド	説明
<a href="#">pool (DHCP IPv6)</a>	DHCP Relay または DHCP Snooping プロファイルを設定します。
<a href="#">relay information option, (293 ページ)</a>	DHCP サーバ上の転送された BOOTREQUEST メッセージ内に DHCP リレー エージェント情報オプションを挿入できます。
<a href="#">relay information option allow-untrusted, (296 ページ)</a>	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された giaddr を持つ BOOTREQUEST メッセージをドロップしないように設定します。



## vrf (relay profile)

VPNルーティングおよび転送 (VRF) インスタンス上のリレープロファイルを設定するには、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) IPv4 コンフィギュレーション モードで **vrf (relay profile)** 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。

**vrf** {vrf-name relay profile-name| default| all}

**novrf** {vrf-name relay profile-name| default| all}

### 構文の説明

vrf-name	VRF のユーザ定義名。
relay	リレー プロファイルを指定します。
profile-name	リレー プロファイルの名前を指定します。
default	デフォルト VRF のプロファイルを指定します。
all	すべての VRF のプロファイルを指定します。

### コマンド デフォルト

**default** が選択された場合、設定はデフォルトの VRF になります。

### コマンド モード

DHCP IPv4 configuration

### コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

### 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。

## タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、すべての VRF のリレー プロファイルを設定する例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# dhcp ipv4
RP/0/RSP0/CPU0:router(config-dhcpv4)# vrf all
```

## 関連コマンド

コマンド	説明
<a href="#">dhcp ipv4</a> , (272 ページ)	IPv4 の DHCP をイネーブルにし、DHCP IPv4 コンフィギュレーション モードを開始します。
<a href="#">giaddr policy</a> , (278 ページ)	ゼロ以外の giaddr 属性がすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。
<a href="#">helper-address</a> , (280 ページ)	DHCP リレーエージェントがパケットを特定の DHCP サーバに中継するように設定します。
<a href="#">profile (DHCP)</a> , (287 ページ)	DHCP IPv4 コンポーネントのリレープロファイルを設定します。
<a href="#">relay information check</a> , (291 ページ)	転送された BOOTREPLY メッセージ内のリレー エージェント情報オプションを DHCP サーバが検証するように設定します。
<a href="#">relay information option</a> , (293 ページ)	転送された BOOTREQUEST メッセージ内の DHCP リレーエージェント情報オプションをシステムが DHCP サーバに挿入することをイネーブルにします。
<a href="#">relay information option allow-untrusted</a> , (296 ページ)	DHCP コンポーネントが、設定されたリレー情報オプションおよびゼロに設定された giaddr を持つ BOOTREQUEST メッセージをドロップしないように設定します。

コマンド	説明
<a href="#">relay information policy</a> , (299 ページ)	リレー情報オプションがすでに含まれている BOOTREQUEST メッセージをリレー エージェントが処理する方法を設定します。

vrf (relay profile)



# 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)、Trivial File Transfer Protocol (TFTP)、およびリモートコピープロトコル (RCP) などのホストサービスやアプリケーションの設定や監視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、例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [cinetd rate-limit](#), 327 ページ
- [clear host](#), 329 ページ
- [domain ipv4 host](#), 331 ページ
- [domain ipv6 host](#), 333 ページ
- [domain list](#), 335 ページ
- [domain lookup disable](#), 337 ページ
- [domain name \(グローバル\)](#), 339 ページ
- [domain name-server](#), 341 ページ
- [ftp client anonymous-password](#), 343 ページ
- [ftp client passive](#), 345 ページ
- [ftp client password](#), 347 ページ
- [ftp client source-interface](#), 349 ページ
- [ftp client username](#), 351 ページ
- [ping \(ネットワーク\)](#), 353 ページ
- [ping bulk \(ネットワーク\)](#), 357 ページ
- [rcp client source-interface](#), 360 ページ

- [rcp client username, 362 ページ](#)
- [show cinetd services, 364 ページ](#)
- [show hosts, 366 ページ](#)
- [telnet, 369 ページ](#)
- [telnet client source-interface, 373 ページ](#)
- [telnet dscp, 375 ページ](#)
- [telnet server, 377 ページ](#)
- [telnet transparent, 379 ページ](#)
- [tftp client source-interface, 381 ページ](#)
- [tftp server, 383 ページ](#)
- [traceroute, 385 ページ](#)

## cinetd rate-limit

Ciscoinetd (Cinetd) で許容されるサービスリクエストにレート制限を設定するには、グローバルコンフィギュレーションモードで **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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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	操作
ip-services	読み取り、書き込み

---

**例**

次に、**cinetd rate-limit** を 10 に設定する例を示します。

```
RP/0/RSP0/CPU0:router# config  
RP/0/RSP0/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、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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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, \(331 ページ\)](#) コマンドまたは [domain ipv6 host, \(333 ページ\)](#) 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	操作
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/RSP0/CPU0:router# clear host *
```

関連コマンド

コマンド	説明
<a href="#">domain ipv4 host, (331 ページ)</a>	ホスト キャッシュにスタティック IPv4 hostname-to-address マッピングを定義します。
<a href="#">domain ipv6 host, (333 ページ)</a>	ホスト キャッシュにスタティック IPv6 hostname-to-address マッピングを定義します。
<a href="#">show hosts, (366 ページ)</a>	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

## domain ipv4 host

IPv4 を使用するホストにスタティックな `hostname-to-address` マッピングを定義するには、グローバル 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復元するには、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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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、実行できる操作 (**ping** など) が制限されます。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# domain ipv4 host host1 192.168.7.18  
RP/0/RSP0/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、グローバル 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復元するには、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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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、実行できる操作 (**ping** など) が制限されます。

タスク ID	タスク ID	操作
	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/RSP0/CPU0:router(config)# domain ipv6 host host1 ff02::2  
RP/0/RSP0/CPU0:router(config)# domain ipv6 host host2 ff02::1
```

# domain list

未修飾のホスト名を完成するデフォルトのドメイン名のリストを定義するには、グローバル 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

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ドメインリストがない場合、**domain name (グローバル)**、[\(339 ページ\)](#) 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。ドメインリストが存在する場合、この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 (グローバル)**、[\(339 ページ\)](#) コマンドとほぼ同じですが、**domain list** コマンドを使用する場合は、交互に実行されるドメインのリストが定義できる点が異なります。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# domain list domain1.com
RP/0/RSP0/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/RSP0/CPU0:router(config)# domain list domain3.edu
RP/0/RSP0/CPU0:router(config)# no domain list domain2.edu
```

## 関連コマンド

コマンド	説明
<a href="#">domain name (グローバル)</a> , <a href="#">(339 ページ)</a>	デフォルトのドメイン名を定義して、未修飾のホスト名（ドット付き 10 進表記で記載されていない名前）を完成します。
<a href="#">show hosts</a> , <a href="#">(366 ページ)</a>	デフォルトのドメイン名、名前ルックアップサービス、ネームサーバホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。



# domain lookup disable

IP ドメイン ネーム システム (DNS) に基づいた `hostname-to-address` 変換をディセーブルにするには、グローバル コンフィギュレーション モードで **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、キーワードと引数はありません。

## 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

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
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/RSP0/CPU0:router(config)# domain lookup disable
```

## 関連コマンド

コマンド	説明
<a href="#">domain name</a> (グローバル) , (339 ページ)	デフォルトのドメイン名を定義して、未修飾のホスト名 (ドット付き 10 進表記で記載されていない名前) を完成します。
<a href="#">domain name-server</a> , (341 ページ)	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。
<a href="#">show hosts</a> , (366 ページ)	デフォルトのドメイン名、名前ルックアップサービス、ネーム サーバホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

## domain name (グローバル)

未修飾のホスト名の完成にソフトウェアが使用するデフォルトのドメイン名を定義するには、グローバル コンフィギュレーション 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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

**domain name** コマンドで設定されているドメイン名がなく、ユーザによる指定がホスト名だけの場合、要求は検索されません。

### タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、デフォルトのドメイン名として `cisco.com` を定義する例を示します。

```
RP/0/RSP0/CPU0:router(config)# domain name cisco.com
```

## 関連コマンド

コマンド	説明
<a href="#">domain list</a> , (335 ページ)	修飾されていないホスト名を完全なものにするためにデフォルトドメイン名のリストを定義します。
<a href="#">domain name-server</a> , (341 ページ)	名前とアドレスの解決に使用する1つまたは複数のネームサーバのアドレスを指定します。
<a href="#">show hosts</a> , (366 ページ)	デフォルトのドメイン名、名前ルックアップサービス、ネームサーバホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

## domain name-server

名前とアドレスの解決に使用するための1つ以上のネームサーバアドレスを指定するには、グローバルコンフィギュレーションモードで **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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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の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	操作
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/RSP0/CPU0:router(config)# domain name-server 192.168.1.111
RP/0/RSP0/CPU0:router(config)# domain name-server 192.168.1.2
```

関連コマンド

コマンド	説明
<a href="#">domain lookup disable</a> , (337 ページ)	ドメインのルックアップをディセーブルにします。
<a href="#">domain name</a> (グローバル) , (339 ページ)	デフォルトのドメイン名を定義して、未修飾のホスト名 (ドット付き 10 進表記で記載されていない名前) を完成します。

## ftp client anonymous-password

匿名のユーザにパスワードを割り当てるには、グローバル 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復元するには、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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router (config)# ftp client anonymous-password xxxx
```

## 関連コマンド

コマンド	説明
<a href="#">ftp client passive</a> , (345 ページ)	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します。
<a href="#">ftp client password</a> , (347 ページ)	ファイル転送プロトコル (FTP) 接続で使用するパスワードを指定します。
<a href="#">ftp client source-interface</a> , (349 ページ)	ファイル転送プロトコル (FTP) 接続の送信元 IP アドレスを指定します。
<a href="#">ftp client username</a> , (351 ページ)	ファイル転送プロトコル (FTP) 接続で使用するユーザ名を指定します。



## 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、グローバル 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復元するには、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、キーワードと引数はありません。

### 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**ftp client passive** コマンドを使用すると、パッシブ モードの FTP 接続だけが確立できます。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	操作
ip-services	読み取り、書き込み

## 例

次に、ネットワーク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/RSP0/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.
```

## 関連コマンド

コマンド	説明
<a href="#">ftp client anonymous-password, (343 ページ)</a>	匿名ユーザ用のパスワードを割り当てます。
<a href="#">ftp client password, (347 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するパスワードを指定します。
<a href="#">ftp client source-interface, (349 ページ)</a>	ファイル転送プロトコル (FTP) 接続の送信元 IP アドレスを指定します。
<a href="#">ftp client username, (351 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するユーザ名を指定します。

## 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、グローバル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

<b>clear-text-password</b>	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。
<b>clear</b> <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。
<b>encrypted</b> <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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router (config)# ftp client password lab
```

## 関連コマンド

コマンド	説明
<a href="#">ftp client anonymous-password, (343 ページ)</a>	匿名ユーザ用のパスワードを割り当てます。
<a href="#">ftp client passive, (345 ページ)</a>	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します。
<a href="#">ftp client source-interface, (349 ページ)</a>	ファイル転送プロトコル (FTP) 接続の送信元 IP アドレスを指定します。
<a href="#">ftp client username, (351 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するユーザ名を指定します。

## 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、グローバル 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復元するには、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

<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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	操作
ip-services	読み取り、書き込み

例

次に、GigabitEthernet インターフェイス 0/1/2/1 に対応付けられている IP アドレスを、実際にパケット送信に使用されるインターフェイスが何かにはかかわらず、すべての FTP パケットの送信元アドレスとして設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# ftp client source-interface gigabitethernet 0/1/2/1
```

関連コマンド

コマンド	説明
<a href="#">ftp client anonymous-password, (343 ページ)</a>	匿名ユーザ用のパスワードを割り当てます。
<a href="#">ftp client passive, (345 ページ)</a>	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します。
<a href="#">ftp client password, (347 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するパスワードを指定します。
<a href="#">ftp client username, (351 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するユーザ名を指定します。

## 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、グローバル 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、このコマンドの **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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ftp client username brownfox
```

## 関連コマンド

コマンド	説明
<a href="#">ftp client anonymous-password, (343 ページ)</a>	匿名ユーザ用のパスワードを割り当てます。
<a href="#">ftp client passive, (345 ページ)</a>	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します。
<a href="#">ftp client password, (347 ページ)</a>	ファイル転送プロトコル (FTP) 接続で使用するパスワードを指定します。
<a href="#">ftp client source-interface, (349 ページ)</a>	ファイル転送プロトコル (FTP) 接続の送信元 IP アドレスを指定します。



## ping (ネットワーク)

IP ネットワークでのホストの到達可能性と接続性をチェックするには、EXEC モードで **ping** コマンドを使用します。

```
ping [ipv4|ipv6] vrf vrf-name [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

<b>ipv4</b>	(任意) IPv4 アドレス プレフィックスを指定します。
<b>ipv6</b>	(任意) IPv6 アドレス プレフィックスを指定します。
<b>vrf</b>	(任意) VPN ルーティング/転送 (VRF) インスタンスを指定します。
<b>vrf-name</b>	(任意) ping を実行するためのシステムの VRF 名。
<b>host-name</b>	(任意) ping を実行するためのシステムのホスト名。
<b>ip-address</b>	(任意) ping を実行するためのシステムの IP アドレス。
<b>count number</b>	(任意) 繰り返しのカウントを設定します。範囲は 0 ~ 2147483647 です。
<b>size number</b>	(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。
<b>source</b>	(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。
<b>type number</b>	(任意) サービス タイプを設定します。範囲は 0 ~ 255 です。 <b>ipv4</b> キーワードが指定されている場合に有効です。
<b>timeout seconds</b>	(任意) タイムアウトを設定します (秒数)。範囲は 0 ~ 3600 です。
<b>priority number</b>	(任意) パケットの優先順位を設定します。範囲は 0 ~ 15 です。 <b>ipv6</b> キーワードが指定されている場合に有効です。
<b>pattern number</b>	(任意) データ パターンを設定します。範囲は 0 ~ 65535 です。
<b>verbose</b>	(任意) 詳細な出力を設定します。
<b>donnotfrag</b>	(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weepを設定します。

**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**            EXEC

<b>コマンド履歴</b>	リリース	変更箇所
	リリース 3.7.2	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。

**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 ネットワークでだけサポートされます。

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するには、デフォルトで Ctrl-C のエスケープ シーケンスを入力します。Ctrl キーと C キーを同時に押してから離すと入力されます。

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 33 : 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。
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	操作
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/RSP0/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** コマンドと同一行にホスト名またはアドレスを入力すると、次の出力例に示すように、このコマンドはそのホスト名またはアドレスのプロトコルタイプに該当するデフォルトの動作を実行します。

```
RP/0/RSP0/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 ネットワークでの複数のホストへの到達可能性と接続性をチェックするには、EXEC モードで **ping bulk** コマンドを使用します。

```
ping bulk ipv4 [input cli [batch| inline]]
[vrf vrf-name] [ip-address| domain-name]
```

### 構文の説明

<b>ipv4</b>	IPv4 アドレス プレフィックスを指定します。
<b>input</b>	入力モードを指定します。
<b>cli</b>	CLI によって入力を指定します。
<b>batch</b>	すべての宛先の後の ping は入力です。
<b>inline</b>	各宛先の後の ping は入力です。
<b>vrf vrf-name ip-address domain-name</b>	(任意) 特定の VPN Routing and Forwarding (VRF; VPN ルーティング/ 転送) を指定します。  ping を実行するシステムの IP アドレス。  (任意) ping を実行するためのシステムのドメイン名。  (注) Enter ボタンを押して、回線あたり 1 つの宛先アドレスを指 定する必要があります。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.1.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

Enter ボタンを押して、回線あたり 1 つの宛先アドレスを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	操作
	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/RSP0/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/RSP0/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
```

## 関連コマンド

コマンド	説明
<a href="#">ping (ネットワーク)</a> , <a href="#">(353 ページ)</a>	IP ネットワークでのホストの到達可能性とネットワーク接続を確認します。

# rcp client source-interface

Remote Copy Protocol (rcp) の送信元 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **rcp 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 **rcp 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復元するには、このコマンドの **no** 形式を使用します。

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

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

## 構文の説明

type	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
interface-path-id	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、 <b>show interfaces</b> 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

rcp 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 rcp 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

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

すべての rcp 接続の送信元としてのインターフェイスの IP アドレスを設定するために **rcp client source-interface** コマンドを使用します。rcp を使用してリモート コピーが要求された場合に使用するリモート ユーザ名を設定するには、**rcp client username** コマンドを使用します。



タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

例

次に、rcp 接続の送信元アドレスとして GigabitEthernet インターフェイス 1/0/2/1 の IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# rcp client source-interface gigabitethernet 1/0/2/1
```

関連コマンド

コマンド	説明
<a href="#">rcp client username</a> , (362 ページ)	rcp を使用してリモート コピーが要求された場合に使用するリモートユーザ名を設定します。

# rcp client username

リモート コピー プロトコル (rcp) を使用してリモート コピーを要求する場合にクライアント側のローカル ユーザを使用するように設定するには、グローバル コンフィギュレーション モードで **rcp client username** 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。

**rcp client username** *username*

**no rcp client username** *username*

## 構文の説明

**username**      rcp サーバのリモート ユーザの名前。rcp コピー要求を実行するのにこの名前を使用します。rcp サーバにディレクトリ構造が存在する場合、コピー対象のすべてのファイルおよびイメージは、リモート ユーザのアカウント内のサーバディレクトリに該当する場所で検索されるか書き込まれます。

## コマンド デフォルト

ユーザがこのコマンドを発行しないと、現在の tty プロセスに対応付けられているリモート ユーザ名が rcp のコピー コマンドで有効な場合に、ソフトウェアからこのユーザ名が送信されます。たとえば、ユーザがネットワーク デバイスに Telnet 経由で接続し、**username** コマンドを通じて認証された場合、ソフトウェアからこのユーザ名がリモートのユーザ名として送信されます。

現在の tty プロセスでこのユーザ名が有効でない場合は、リモート ユーザ名としてホスト名が送信されます。rcp のブート コマンドの場合、ソフトウェアからネットワーク サーバがデフォルトで送信されます。



(注)

シスコでは、tty 行は主にサービスのアクセスに使用されます。TTY の概念は、UNIX に由来します。UNIX システムでは、各物理デバイスがファイル システムで表現されます。端末は tty デバイスと呼ばれます (tty は、UNIX 端末の teletype が元になった省略形です)。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

リリース

変更箇所

リリース 3.7.2

このコマンドが導入されました。

コマンド履歴

リリース	変更箇所
リリース 3.2	このコマンドがサポート対象になりました。

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。

rcp プロトコルでは、クライアントは rcp 要求でリモート ユーザ名をネットワーク サーバに送信する必要があります。rcp のコピー要求でネットワーク サーバに送信する必要があるリモート ユーザ名を指定するには、**rcp client username** コマンドを使用します。ネットワーク サーバにディレクトリ構造が存在する場合、コピー対象のすべてのファイルおよびイメージは、UNIX システムと同様に、リモートユーザのアカウント内のサーバディレクトリに該当する場所で検索されるか書き込まれます。rcp 接続の送信元アドレスを指定するには、**rcp client source-interface** コマンドを使用します。



(注) リモートのユーザ名は、宛先サーバのアカウントに対応付けられている必要があります。

タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

例

次の例は、リモートのユーザ名を netadmin1 に設定する方法を示します。

```
RP/0/RSP0/CPU0:router(config)# rcp client username netadmin1
```

関連コマンド

コマンド	説明
<a href="#">rcp client source-interface</a> , (360 ページ)	rcp 接続の送信元 IP アドレスを指定します。

# show cinetd services

要求の受信時に Cinetd によってプロセスが発生したサービスを表示するには、EXEC 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、キーワードと引数はありません。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
ip-services	読み取り

### 例

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

```
RP/0/RSP0/CPU0:router# show cinetd services
Family Service  Proto  Port  ACL  max_cnt  curr_cnt  wait  Program Option
-----
v4      telnet   tcp    23   unlimited  0        nowait   telnet
v4      tftp    udp    69   unlimited  0        wait     tftpd  disk0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 34 : 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。

関連コマンド

コマンド	説明
<a href="#">telnet server, (377 ページ)</a>	Telnet サービスをネットワークング デバイスでイネーブルにします。
<a href="#">tftp server, (383 ページ)</a>	TFTP サーバで実行中の TFTP サーバまたは機能をイネーブルまたはディセーブルにします。

# 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、および、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、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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
ip-services	読み取り

## 例

次に、**show hosts** コマンドの出力例を示します。

```
RP/0/RSP0/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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 35 : 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"> <li>• 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。</li> <li>• 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。</li> <li>• OK : エントリは有効と見なされます。</li> <li>• ?? : 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。</li> <li>• EX : エントリは期限切れです。</li> </ul>
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。

## 関連コマンド

コマンド	説明
<a href="#">clear host</a> , (329 ページ)	ホスト名とアドレスのキャッシュからエントリを削除します。
<a href="#">domain list</a> , (335 ページ)	修飾されていないホスト名を完全なものにするためにデフォルトドメイン名のリストを定義します。
<a href="#">domain lookup disable</a> , (337 ページ)	IP DNS に基づいたホスト名からのアドレス変換をディセーブルにします。
<a href="#">domain name</a> (グローバル), (339 ページ)	デフォルトのドメイン名を定義して、未修飾のホスト名 (ドット付き 10 進表記で記載されていない名前) を完成します。
<a href="#">domain name-server</a> , (341 ページ)	名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。



# telnet

Telnetをサポートするホストにログインするには、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"> <li>• IPv4 アドレス形式：(x.x.x.x) 形式で入力する必要があります。</li> <li>• IPv6 アドレス形式：アドレスは、RFC2373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。</li> </ul>
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、 <a href="#">表 36 : Telnet 接続オプション</a> 、(369 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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 36: 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-to-UNIX Copy Program (UUCP; UNIX 間コピープログラム) 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。

利用可能なホストを一覧表示するには、**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。論理名は、その名前が使用中の場合と、**name-connection EXEC** コマンドで接続名が変更された場合を除き、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 37: 特殊な Telnet のエスケープ シーケンス、(370 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 37: 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 <sup>9</sup>	目的
Ctrl-^ c	プロセスの割り込み (IP)
Ctrl-^ o	出力の中断 (AO)
Ctrl-^ u	行の消去 (EL)

<sup>9</sup> 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/RSP0/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	操作
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/RSP0/CPU0:router# telnet host1
```

## 関連コマンド

コマンド	説明
aaa authentication login default local	ログイン時の AAA 認証を設定します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』を参照してください。
<a href="#">telnet server</a> , (377 ページ)	Telnet サービスをネットワークングデバイスでイネーブルにします。
terminal length	現在の端末画面に表示する、現在のセッションの行数を指定します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』を参照してください。
terminal width	現在の端末画面に表示する、現在のセッションの文字列の数を指定します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』を参照してください。

## telnet client source-interface

Telnet 接続の送信元の IP アドレスを指定するには、グローバル コンフィギュレーション モードで **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復元するには、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。
type	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
interface-path-id	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、 <b>show interfaces</b> 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

すべての telnet 接続の送信元としてのインターフェイスの IP アドレスを設定するために **telnet client source-interface** コマンドを使用します。

#### タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
ip-services	読み取り、書き込み

#### 例

次に、Telnet 接続の送信元アドレスとして GigabitEthernet インターフェイス 1/0/2/1 の IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# telnet ipv4 client source-interface gigabitethernet 1/0/2/1
```

#### 関連コマンド

コマンド	説明
<a href="#">telnet server</a> , (377 ページ)	Telnet サービスをネットワークングデバイスでイネーブルにします。

## telnet dscp

ネットワークデバイスの Telnet トラフィックをマーキングする QoS (Quality of Service) を設定するための DiffServ コードポイント (DSCP) の値および IPv4 の優先度を定義するには、グローバル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 [vrf {vrf-name| default}] ipv4 dscp dscp-value
```

```
no telnet [vrf {vrf-name| default}] ipv4 dscp dscp-value
```

### 構文の説明

vrf	(任意) 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。
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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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。

DSCP は、特定の VRF を実行するサーバとクライアントの両者の動作に影響を与える場合があります。

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# telnet vrf default ipv4 dscp 40
RP/0/RSP0/CPU0:router(config)# telnet vrf default ipv4 dscp 10
```

関連コマンド

コマンド	説明
<a href="#">telnet</a> , <a href="#">(369 ページ)</a>	Telnet をサポートするホストにログインします。



## 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ために、グローバル 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

ネットワークング デバイスから **telnet** コマンドで着信 Telnet 接続が受け入れられるのを防ぐために 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 サービスがイネーブルにする場合は、**max-servers** キーワードを 1 以上の値に設定します。このように設定すると、着信 Telnet 接続がネットワークング デバイスで許可されます。

このコマンドは、ネットワークング 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復元されます。



(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 Router System Management Command Reference』、『Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide』、および『Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide』を参照してください)。

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 1
```

関連コマンド

コマンド	説明
telnet, (369 ページ)	Telnet をサポートするホストにログインします。

# 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復元するには、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、キーワードと引数はありません。

## 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

変更箇所

リリース 3.7.2

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。

**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分かれる場合の対処に役立ちます。

## タスク ID

タスク ID

操作

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-NULキーの組み合わせで送信されます。

```
RP/0/RSP0/CPU0:router(config)# line console
RP/0/RSP0/CPU0:router(config-line)# telnet transparent
```

## 関連コマンド

コマンド	説明
<a href="#">telnet</a> , <a href="#">(369 ページ)</a>	Telnetをサポートするホストにログインします。

# tftp client source-interface

TFTP 接続の送信元の IP アドレスを指定するには、グローバル コンフィギュレーション モードで **tftp 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 **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復元するには、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

<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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、 <b>show interfaces</b> 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

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

すべての TFTP 接続の送信元としてのインターフェイスの IP アドレスを設定するために **tftp client source-interface** コマンドを使用します。

タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

例

次に、TFTP 接続の送信元アドレスとして GigabitEthernet インターフェイス 1/0/2/1 の IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tftp client source-interface gigabitethernet 1/0/2/1
```

関連コマンド

コマンド	説明
<a href="#">tftp server</a> , (383 ページ)	TFTP サーバで実行中の TFTP サーバまたは機能をイネーブルまたはディセーブルにします。

## 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、グローバル 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。
<b>homedir</b> <i>tftp-home-directory</i>	ホーム ディレクトリを指定します。
<b>max-servers</b> <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。
<b>max-servers</b> <b>no-limit</b>	(任意) 許容可能な TFTP サーバを処理する最大数に上限がないことを設定します。
<b>access-list</b> <i>name</i>	(任意) TFTP サーバに対応付けられるアクセス 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。指定しないと、デフォルト値の **max-servers** キーワードは無制限になります。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**tftp server** コマンドの **no** 形式を使用すると、指定の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復元されます。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	操作
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/RSP0/CPU0:router(config)# tftp ipv4 server homedir disk0 access-list test
```

**関連コマンド**

コマンド	説明
<a href="#">show cinetd services</a> , (364 ページ)	cinetd でプロセスが生成されるサービスを表示します。



## traceroute

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とるルートを検出するには、EXEC モードで **traceroute** コマンドを使用します。

**traceroute** [**ipv4**|**ipv6**]**vrf** *vrf-name*] [*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

<b>ipv4</b>	(任意) IPv4 アドレス プレフィックスを指定します。
<b>ipv6</b>	(任意) IPv6 アドレス プレフィックスを指定します。
<b>vrf</b>	(任意) VPNルーティング/転送 (VRF) インスタンスを指定します。
<b>vrf-name</b>	(任意) ping を実行するためのシステムの VRF 名。
<b>host-name</b>	(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。
<b>ip-address</b>	(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。
<b>source</b>	(任意) 送信元アドレス。
<b>ip-address-name</b>	(任意) IP アドレス A.B.C.D またはホスト名。
<b>numeric</b>	(任意) 数字だけを表示。
<b>timeout seconds</b>	(任意) タイムアウト値。範囲は 0 ~ 3600 です。
<b>probe count</b>	(任意) プローブ カウント。範囲は 0 ~ 65535 です。
<b>minttl seconds</b>	(任意) 最小存続可能時間。範囲は 0 ~ 255 です。
<b>maxttl seconds</b>	(任意) 最大存続可能時間。範囲は 0 ~ 255 です。
<b>port number</b>	(任意) ポート番号。範囲は 0 ~ 65535 です。
<b>priority number</b>	(任意) パケットのプライオリティ。範囲は 0 ~ 15 です。 <b>ipv6</b> キーワードが指定されている場合に有効です。
<b>verbose</b>	(任意) 詳細な出力。

### コマンド モラボルト

EXEC ルートの動作または値はありません。

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**tracert** 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。

**tracert** コマンドは、データグラムが存続可能時間 (TTL) の値を超過するとネットワークング デバイスで生成されるエラー メッセージを活用して動作します。

**tracert** コマンドは、最初に、TTL 値 1 のプローブ データグラムを送信します。これにより、先のネットワークング デバイスはこのプローブ データグラムを破棄してエラー メッセージを送り返します。**tracert** 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。

**tracert** コマンドでは 1 回に送信されるプローブは 1 つです。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ると、**tracert** コマンドはアスタリスク (\*) を出力します。

**tracert** コマンドは、宛先の応答時、最大 TTL の超過時、あるいは、ユーザがエスケープ シーケンス (デフォルトでは Ctrl-C) を使用してトレースに割り込んだ場合にそれぞれ終了します。Ctrl キーと C キーを同時に押してから離すと入力されます。

デフォルト以外のパラメータを使用して拡張 **tracert** テストを呼び出すには、引数の *host-name* または *ip-address* を指定せずにコマンドを入力します。**tracert** テストで希望するパラメータ値を選択するためのダイアログが表示され、選択を行います。

多様なネットワークング デバイスに応じて IP の実装方法もさまざまであることから、IP **tracert** コマンドは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 ホップ分離れて位置する場合、**traceroute** コマンドは、6 から 11 回の応答の間にタイムアウトします。

タスク ID

タスク ID	操作
basic-services	読み取り、書き込み、実行

例

次に、宛先のホスト名が指定されている **traceroute** セッションの出力例を示します。

```
RP/0/RSP0/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
```

次の表示は、宛先が指定されていない場合の拡張 **traceroute** セッションの例です。

```
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 38: **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。



## HSRP コマンド

---

この章では、ホットスタンバイルータプロトコル（HSRP）の設定およびモニタをする場合に使用する Cisco IOS XR ソフトウェアコマンドについて説明します。

HSRP の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [address \(hsrp\)](#) , 391 ページ
- [address secondary \(hsrp\)](#) , 393 ページ
- [authentication \(hsrp\)](#) , 395 ページ
- [bfd fast-detect \(hsrp\)](#) , 397 ページ
- [clear hsrp statistics](#), 399 ページ
- [hsrp authentication](#), 401 ページ
- [hsrp bfd fast-detect](#), 403 ページ
- [hsrp bfd minimum-interval](#), 405 ページ
- [hsrp bfd multiplier](#), 407 ページ
- [hsrp delay](#), 409 ページ
- [hsrp ipv4](#), 411 ページ
- [hsrp mac-address](#), 413 ページ
- [hsrp preempt](#), 416 ページ
- [hsrp priority](#), 418 ページ
- [hsrp redirects](#), 420 ページ
- [hsrp timers](#), 422 ページ
- [hsrp track](#), 425 ページ
- [hsrp use-bia](#), 428 ページ

- interface (HSRP) , 430 ページ
- mac-address (hsrp) , 432 ページ
- preempt (hsrp) , 434 ページ
- priority (hsrp) , 436 ページ
- router hsrp, 438 ページ
- session name, 440 ページ
- show hsrp, 442 ページ
- show hsrp bfd, 447 ページ
- show hsrp mgo, 449 ページ
- show hsrp statistics, 451 ページ
- show hsrp summary, 453 ページ
- slave follow, 455 ページ
- slave primary virtual IPv4 address, 457 ページ
- slave secondary virtual IPv4 address, 459 ページ
- slave virtual mac address, 461 ページ
- timers (hsrp) , 463 ページ
- track (hsrp) , 466 ページ

## address (hsrp)

IP のホットスタンバイプロトコルをイネーブルにするには、HSRP グループサブモードで **address (hsrp)** コマンドを使用します。IP のホットスタンバイプロトコル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。

**address** {**learn**| *address*}

**no address** {**learn**| *address*}

### 構文の説明

<b>learn</b>	ピアから仮想 IP アドレスを学習します。
<i>address</i>	ホットスタンバイ IP アドレス。

### コマンド デフォルト

なし

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、グループをイネーブルにして、受信された HSRP 制御パケットからプライマリ仮想 IPv4 アドレスを学習する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# address learn
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">address secondary (hsrp)</a> , <a href="#">(393 ページ)</a>	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。



## address secondary (hsrp)

仮想ルータのセカンダリ仮想 IPv4 アドレスを設定するには、ホットスタンバイ ルータ プロトコル (HSRP) 仮想ルータ サブモードで **address secondary** コマンドを使用します。仮想ルータのセカンダリ仮想 IPv4 アドレスの設定を解除するには、このコマンドの **no** 形式を使用します。

**address address secondary**

**no address address secondary**

### 構文の説明

<b>secondary</b>	セカンダリ HSRP IP アドレスを設定します。
<i>address</i>	HSRP IPv4 アドレス。

### コマンド デフォルト

なし

### コマンド モード

HSRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、仮想ルータのセカンダリ仮想 IPv4 アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 3
RP/0/RSP0/CPU0:router(config-hsrp-gp)# address 10.20.30.1 secondary
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">address (hsrp)</a> , (391 ページ)	IP のホットスタンバイ プロトコルをイネーブルにします。

## authentication (hsrp)

ホットスタンバイ ルータ プロトコル (HSRP) の認証文字列を設定するには、HSRP グループ サブモードで **hsrp authentication** コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

**authentication** *string*

**no authentication** [*string*]

### 構文の説明

string	認証文字列。文字列は最大 8 文字の長さにすることができます。デフォルトは「cisco」です。
--------	---

### コマンド デフォルト

デフォルトの認証文字列は「cisco」です。

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	このコマンドが導入されました。このコマンドは、 <b>hsrp authentication</b> コマンドを置き換えます。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。同じ認証文字列は、LAN 上のすべてのルータおよびアクセスサーバで相互運用できるように設定する必要があります。認証の不一致が発生すると、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびホットスタンバイ タイマー値を学習できません。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、tenGigE インターフェイス 0/4/0/4 のグループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証文字列として「company1」を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# authentication company1
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## bfd fast-detect (hsrp)

HSRP インターフェイスで双方向フォワーディング (BFD) 高速検出をイネーブルにするには、HSRP グループサブモードで **hsrp bfd fast-detect** コマンドを使用します。これにより、HSRP ルータとそのピアの間に BFD セッションが作成されます。HSRP がバックアップ状態のときにセッションがダウンすると、HSRP フェールオーバーが開始されます。BFD 高速検出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。

**bfd fast detect** [*peer ipv4 ipv4-address interface-type interface-path-id*]

**no bfd fast-detect**

### 構文の説明

<b>peer ipv4</b> <i>ipv4-address</i>	BFD ピア インターフェイスの IPv4 アドレス。
<i>interface-type</i> <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、 <b>show interfaces</b> 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

BFD はディセーブルです。

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	このコマンドが導入されました。このコマンドは、 <b>hsrp bfd-fast detect</b> コマンドを置き換えます。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、bfd fast-detect をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# bfd fast-detect
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp bfd multiplier, (407 ページ)</a>	BFD の乗数値を設定します。
<a href="#">hsrp bfd minimum-interval, (405 ページ)</a>	BFD の最小間隔を特定のインターフェイス上のすべての HSRP BFD セッションで使用するよう設定します。

## clear hsrp statistics

ホットスタンバイ ルーティング プロトコル (HSRP) の統計情報をゼロにリセットするには、EXEC モードで **clear hsrp statistics** コマンドを使用します。

**clear hsrp statistics** [*interface interface-path-id group*]

### 構文の説明

<b>interface</b> <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、 <b>show interfaces</b> 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>group</i>	グループ番号。

### コマンド デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、**clear hsrp statistics** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# clear hsrp statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。



## hsrp authentication

ホットスタンバイルータプロトコル (HSRP) の認証文字列を設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp authentication** コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

**hsrp** [ *group-number* ] **authentication** *string*

**no hsrp** [ *group-number* ] **authentication** [ *string* ]

### 構文の説明

group-number	(任意) この認証ストリングを適用するインターフェイス上のグループ番号。デフォルトは 0 です。
string	認証文字列。文字列は最大 8 文字の長さにすることができます。デフォルトは「cisco」です。

### コマンド デフォルト

デフォルトのグループ番号は 0 です。

デフォルトの認証文字列は「cisco」です。

### コマンド モード

HSRP 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	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>authentication hsrp</b> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

認証ストリングはすべての HSRP メッセージで暗号化されずに送信されます。同じ認証文字列は、LAN 上のすべてのルータおよびアクセスサーバで相互運用できるように設定する必要があります。認証の不一致が発生すると、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびホットスタンバイ タイマー値を学習できません。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 のグループ 1 のホット スタンバイ ルータを相互運用させるために必要な認証文字列として「company1」を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 authentication company1
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## hsrp bfd fast-detect

HSRP インターフェイスで双方向フォワーディング (BFD) 高速検出をイネーブルにするには、HSRP インターフェイス コンフィギュレーション モードで **hsrp bfd fast-detect** コマンドを使用します。これにより、HSRP ルータとそのピアの間に BFD セッションが作成されます。HSRP がバックアップ状態のときにセッションがダウンすると、HSRP フェールオーバーが開始されます。BFD 高速検出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。

**hsrp [group number] bfd fast-detect**

**no hsrp [group number] bfd fast-detect**

### 構文の説明

group number (任意) HSRP グループ番号。範囲は 0 ~ 255 です。

### コマンド デフォルト

BFD はディセーブルです。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9.0	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>bfd fast-detect (hsrp)</b> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、bfd fast-detect をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 bfd fast-detect
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp bfd multiplier</a> , (407 ページ)	BFD の乗数値を設定します。



## 例

次に、100 ミリ秒の最小間隔を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd minimum-interval 100
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp bfd fast-detect, (403 ページ)</a>	HSRP インターフェイスで BFD fast-detection をイネーブルにします。
<a href="#">hsrp bfd multiplier, (407 ページ)</a>	BFD の乗数値を設定します。

## hsrp bfd multiplier

BFD 乗数値を設定するには、インターフェイス コンフィギュレーション モードで **hsrp bfd multiplier** コマンドを使用します。設定した乗数値を削除し、乗数値をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**hsrp bfd multiplier multiplier**

**no hsrp bfd multiplier multiplier**

### 構文の説明

**multiplier** BFD 乗数値を指定します。範囲は 2 ~ 50 です。

### コマンド デフォルト

デフォルト値は 3 です。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

乗数値によって、期待どおりに受信していない場合に BFD セッションがダウンする連続 BFD パケットの数が指定されます。BFD 乗数値は、インターフェイス上に設定されたすべての BFD セッションに適用されます。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、乗数値 10 を使用して BFD 乗数値を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp bfd multiplier 10
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp bfd fast-detect</a> , (403 ページ)	HSRP インターフェイスで BFD fast-detection をイネーブルにします。



## hsrp delay

ホットスタンバイルータプロトコル (HSRP) のアクティベーション遅延を設定するには、HSRP インターフェイス コンフィギュレーションモードで **hsrp delay** コマンドを使用します。アクティベーション遅延を削除するには、このコマンドの **no** 形式を使用します。

**hsrp delay minimum value reload value**

**no hsrp delay**

### 構文の説明

<b>minimum value</b>	すべてのインターフェイス起動イベントの最小遅延 (秒単位) を設定します。範囲は 0 ~ 10000 です。
<b>reload value</b>	最初のインターフェイス起動イベントのリロード遅延 (秒単位) を設定します。範囲は 0 ~ 10000 です。

### コマンド デフォルト

**minimum value** : 1  
**reload value** : 5

### コマンド モード

HSRP 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp delay** コマンドは、インターフェイス起動イベントで HSRP 有限状態マシン (FSM) の開始を遅らせて、インターフェイスがトラフィックを通過する準備を整えます。これにより、hello パケットの損失によるエラー状態にならないようにします。最小遅延はすべてのインターフェイス起動イベントに適用され、リロード遅延は最初のインターフェイス イベントに適用されます。

この機能をオフにするには、ゼロの値を明示的に設定する必要があります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、最小遅延を 10 秒にしてリロード遅延を 100 秒にする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface mgmtEth 0/RP0/CPU0/0
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp delay minimum 10 reload 100
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## hsrp ipv4

ホットスタンバイ ルータ プロトコル (HSRP) をアクティブにするには、HSRP インターフェイス コンフィギュレーション モードで **hsrp ipv4** コマンドを使用します。HSRP をディセーブルに設定するには、このコマンドの **no** 形式を使用します。

**hsrp** [ *group-number* ] **ipv4** [*ip-address* [*secondary*]]

**no hsrp** [ *group-number* ] **ipv4** [*ip-address* [*secondary*]]

### 構文の説明

group-number	(任意) HSRP をアクティブ化するインターフェイスのグループ番号。範囲は 0 ~ 255 です。デフォルトは 0 です。
ip-address	(任意) ホットスタンバイ ルータ インターフェイスの IP アドレス。
secondary	(任意) IP アドレスがセカンダリ ホットスタンバイ ルータ インターフェイスであることを指定します。プライマリおよびセカンダリ アドレスを持つインターフェイスで有効であり、プライマリおよびセカンダリ HSRP アドレスを設定できます。

### コマンド デフォルト

*group-number* : 0

HSRP はデフォルトでディセーブルになっています。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp ipv4** コマンドは、設定されているインターフェイスで HSRP をアクティブ化します。IP アドレスを指定した場合は、IP アドレスがホットスタンバイグループの指定アドレスとして使用されます。IP アドレスが指定されていない場合、仮想アドレスはアクティブ ルータから学習されま

す。HSRP が指定ルータを選択するには、ホットスタンバイグループで少なくとも1つのルートに代表アドレスを設定、または取得する必要があります。アクティブルータ上の指定アドレスを設定すると、常に現在使用されている指定アドレスが上書きされます。

**hsrp ipv4** コマンドがインターフェイスでイネーブルに設定されている場合、プロキシアドレス解決プロトコル (ARP) 要求の処理方法が変更されます (プロキシ ARP がディセーブルに設定されていない場合)。ホットスタンバイステートグループが設定されているか、または指定アドレスを学習した場合、プロキシ ARP 要求は、ホットスタンバイグループの MAC アドレスを使用して応答されます。その他の場合、プロキシ ARP 要求は停止されます。

インターフェイスにセカンダリ IP アドレスが設定され、これらのアドレスのネットワークに冗長性が提供される必要がある場合、セカンダリホットスタンバイルータの IP アドレスを設定する必要があります。

プライマリアドレスはセカンダリアドレスの前に設定する必要があります。同様に、セカンダリアドレスはプライマリアドレスを設定解除する前に設定解除する必要があります。 **no hsrp ipv4** コマンドを使用して、すべての IP アドレスの設定を解除できます。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10ギガビットイーサネットインターフェイス 0/2/0/1 上でグループ 1 用の HSRP をアクティブにする例を示します。ホットスタンバイグループで使用される IP アドレスは、HSRP を使用して学習されます。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:routerrouter(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp redirects</a> , (420 ページ)	HSRP がインターフェイスで設定されるときに送信される ICMP リダイレクトメッセージを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## hsrp mac-address

ホットスタンバイルータプロトコル (HSRP) の MAC アドレスを指定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp mac-address** コマンドを使用します。標準の仮想 MAC アドレス (0000.0C07.ACn) に戻すには、このコマンドの **no** 形式を使用します。

**hsrp** [ *group-number* ] **mac-address** *address*

**no hsrp** [ *group-number* ] **mac-address**

### 構文の説明

group-number	(任意) HSRP をアクティブ化するインターフェイスのグループ番号。デフォルトは 0 です。
address	MAC アドレス。

### コマンド デフォルト

*group-number* : 0

このコマンドが設定されておらず、**hsrp use-bia** コマンドが設定されていない場合、標準の仮想 MAC アドレスの 0000.0C07.ACn が使用されます。n は 16 進数のグループ番号です。このアドレスは RFC 2281 『Cisco Hot Standby Router Protocol (HSRP)』で指定されています。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>mac-address hsrp</b> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp mac-address** コマンドは、ファーストホップの冗長性が仮想 MAC アドレスを使用できることに基づいており、イーサネット スイッチに接続されている PC のファーストホップ アドレスを変更できない IBM ネットワーキング環境を除き、推奨されません。

HSRPを使用すると、エンドステーションでIPルーティングのファーストホップゲートウェイを見つけるのに役立ちます。エンドステーションは、デフォルトゲートウェイで設定されます。ただし、HSRPはその他のプロトコルにファーストホップの冗長性を提供できます。拡張分散ネットワーク機能（APPN）などの一部のプロトコルでは、MACアドレスを使用して、ルーティングのためのファーストホップを特定します。この際、多くの場合で仮想MACアドレスを指定する必要があります。仮想IPアドレスは、これらのプロトコルには重要ではありません。

仮想MACアドレスを指定するには、**hsrp mac-address** コマンドを使用します。ルータがアクティブな場合、指定されたMACアドレスが仮想MACアドレスとして使用されます。このコマンドは、特定のAPPN設定を対象としています。

次の表に、APPNとIPの平行な用語を示します。

表 39: APPNとIPの平行な用語

APPN	IP
エンド ノード	ホスト
ネットワーク ノード	ルータまたはゲートウェイ



(注) APPNネットワークでは、エンドノードは隣接するネットワークノードのMACアドレスを使用して設定されていることがほとんどです。仮想MACアドレスをエンドノードで使用される値に設定するには、ルータで**hsrp mac-address** コマンドを使用します。

#### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

#### 例

ネットワークノードのMACアドレスとして4000.1000.1060を使用するようにエンドノードが設定されている場合、仮想MACアドレスを設定するコマンドは次のとおりです。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 5 mac-address 4000.1000.1060
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp use-bia, (428 ページ)</a>	HSRP を、割り当て済みの MAC アドレスの代わりに仮想 MAC アドレスとしてインターフェイスのバーndインアドレスを使用するよう設定します。
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## hsrp preempt

ホットスタンバイ ルータ プロトコル (HSRP) プリエンプションおよびプリエンプレションの遅延を設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp preempt** 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。

**hsrp** [ *group-number* ] **preempt** [ *delay seconds* ]

**no hsrp** [ *group-number* ] **preempt** [ *delay seconds* ]

### 構文の説明

<b>group-number</b>	(任意) このコマンドの他の引数を適用するインターフェイス上のグループ番号。デフォルトは 0 です。
<b>delay seconds</b>	(任意) 時間 (秒単位)。 <i>seconds</i> 引数によって、指定されたプリエンプレションの遅延の <i>seconds</i> 値の間、ローカル ルータによるアクティブな役割の引き継ぎが延期されます。範囲は 0 ~ 3600 秒 (1 時間) です。デフォルトは 0 秒 (遅延なし) です。

### コマンド デフォルト

*group-number* : 0

*seconds* : 0 秒 (ルータがプリエンプレション処理する場合、ただちに実行されます)

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>preempt hsrp</b> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp preempt** コマンドが設定されると、ホットスタンバイ プライオリティが現在のアクティブ ルータよりも高い場合、ローカルルータはアクティブルータとして制御を行います。 **hsrp preempt**



コマンドが設定されていない場合、ローカルルータは、他にアクティブ状態のルータがない場合にのみ、アクティブルータとして制御を行います。

ルータが最初に起動したとき、ルータのルーティングテーブルは完全ではありません。HSRP がプリエンプション処理するように設定されている場合、ローカル HSRP グループがアクティブルータになりますが、適切なルーティングサービスを提供できません。この問題は、プリエンプション処理を行うルータが実際に現在のアクティブルータをプリエンプション処理する前に、遅延の設定によって解決できます。

`preempt delay seconds` 値は、現在、アクティブ状態のルータがない場合は適用されません。この場合、ローカルルータは、`preempt delay seconds` の値に関係なく適切なタイムアウト (`hsrp timers` コマンドを参照) 後にアクティブになります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、アクティブルータをプリエンプション処理する前に、プリエンプション処理する必要があることを決定してからルータが 300 秒 (5 分) 待機します。アクティブルータがない場合は、遅延が設定されている場合でも、ルータがより短い期間でアクティブルータになる可能性があります。アクティブルータのプリエンプション処理だけが延期されます。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp ipv4 172.19.108.254
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp preempt delay 300
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp priority</a> , (418 ページ)	HSRP プライオリティを設定します。
<a href="#">hsrp track</a> , (425 ページ)	ホットスタンバイプライオリティが他のインターフェイスの可用性に基づいて変化するように、インターフェイスを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## hsrp priority

ホットスタンバイルータプロトコル (HSRP) のプライオリティを設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**hsrp** [ *group-number* ] **priority** *priority*

**no hsrp** [ *group-number* ] **priority** *priority*

### 構文の説明

<i>group-number</i>	(任意) プライオリティが適用されるインターフェイス上のグループ番号。デフォルトは 0 です。
<i>priority</i>	使用可能なホットスタンバイルータにプライオリティを設定するプライオリティ値。範囲は 1 ~ 255 です。デフォルトは 100 です。

### コマンド デフォルト

*group-number* : 0

*priority* : 100

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	このコマンドがサポート対象になりました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>preempt hsrp</b> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

割り当てられたプライオリティは、アクティブルータとスタンバイルータを選択するために使用されます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータが指定されたアクティブルータになります。プライオリティが等しい場合、インターフェイスの IP アドレスが比較され、大きい IP アドレスを持つインターフェイスが優先されます。

インターフェイスが **hsrp track** コマンドによって設定されている場合、デバイス上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。

プリエンプションがイネーブルでない場合、ルータは、他の HSRP ルータよりもプライオリティが高い場合でもアクティブになっていない可能性があります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、ルータのプライオリティが 120 です。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp ipv4 172.19.108.254
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp priority 120
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp preempt</a> , (416 ページ)	HSRP プリエンプションとプリエンプション遅延を設定します。
<a href="#">hsrp track</a> , (425 ページ)	ホットスタンバイプライオリティが他のインターフェイスの可用性に基づいて変化するように、インターフェイスを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## hsrp redirects

ホットスタンバイ ルータ プロトコル (HSRP) がインターフェイスで設定されているときに送信される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設定するには、HSRP インターフェイス コンフィギュレーションモードで **hsrp redirects** コマンドを使用します。ICMP メッセージがイネーブルになっている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。

**hsrp redirects disable**

**no hsrp redirects disable**

### 構文の説明

disable	HSRP で設定されるインターフェイス上の ICMP リダイレクトメッセージのフィルタリングをディセーブルにします。
---------	--

### コマンド デフォルト

HSRP ICMP リダイレクトはデフォルトでイネーブルです。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp redirects** コマンドはインターフェイス単位で設定できます。インターフェイス上で最初に HSRP を設定する場合、このインターフェイスの設定ではグローバル値を継承します。**hsrp redirects** コマンドがイネーブルになっている場合、リダイレクトパケットのネクストホップアドレスの実際の IP アドレスを仮想 IP アドレス（このアドレスが HSRP に認識されている場合）に置き換えることによって、ICMP リダイレクトメッセージがフィルタリングされます。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 上で HSRP がリダイレクトメッセージをフィルタリングできるようにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4 172.16.0.1  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp redirects disable
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , ( <a href="#">442 ページ</a> )	HSRP 情報を表示します。

## hsrp timers

hello パケット間の時間と他のルータがアクティブ ホットスタンバイまたはスタンバイ ルータのダウンを宣言するまでの時間を設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp timers** コマンドを使用します。タイマー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。

```
hsrp [ group-number ] timers {hello-seconds| msec hello-milliseconds} {hold-seconds| msec hold-milliseconds}
no hsrp [ group-number ] timers
```

### 構文の説明

group-number	(任意) タイマーが適用されるインターフェイス上のグループ番号。デフォルトは 0 です。
hello-seconds	秒単位の hello 間隔。範囲は 1 ~ 255 です。デフォルト値は 3 秒です。
msec hello-milliseconds	ミリ秒単位の hello 間隔。範囲は 100 ~ 3000 ミリ秒です。
hold-seconds	アクティブまたはスタンバイルータがダウンを宣言されるまでの時間 (秒)。範囲は 1 ~ 255 です。デフォルト値は 10 秒です。
msec hold-milliseconds	アクティブまたはスタンバイルータがダウンを宣言されるまでの時間 (ミリ秒)。範囲は 100 ~ 3000 ミリ秒です。

### コマンド デフォルト

group-number : 0  
 hello seconds : 3 秒 (msec キーワードが指定されている場合、デフォルト値はありません)  
 hold-seconds : 10 秒 (msec キーワードが指定されている場合、デフォルト値はありません)

### コマンド モード

HSRP 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	変更箇所
リリース 3.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>preempt hsrp</b> コマンドに置き換えられました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

非アクティブルータは、ミリ秒のタイマー値が使用されていない場合、アクティブルータのタイマー値を学習します。ミリ秒のタイマー値が使用されている場合は、すべてのルータはミリ秒のタイマー値を使用して設定されていなければなりません。このルールは、hello 時間とホールド時間のどちらかがミリ秒単位で指定されている場合に当てはまります。

アクティブルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常、ホールドタイムは hello タイムの 3 倍以上となります ( $\text{holdtime} > 3 * \text{hellotime}$ )。

hello タイムを秒単位またはミリ秒単位のいずれにするかに応じて、*hello-seconds* 引数または **msec** キーワードおよび *hello-milliseconds* 引数を指定する必要があります。また、ホールドタイムを秒単位またはミリ秒単位のいずれにするかに応じて、*hold-seconds* 引数または **msec** キーワードおよび *hold-milliseconds* 引数を指定する必要があります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 上のグループ番号 1 に対して、hello パケットの間隔を 5 秒に設定し、ルータがダウンしたと見なされるまでに時間を 15 秒に設定する例を示します。設定されたタイマー値は、ルータがアクティブである場合にのみ使用されます（または、タイマー値が学習される前）。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 timers 5 15
```

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 上のグループ番号 1 に対して、hello パケットの間隔を 200 ミリ秒に設定し、ルータがダウンしたと見なされるまでに時間を 1000 ミリ秒に設定する例を示します。ミリ秒が指定されているため、設定されたタイマー値は常に使用されます。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 ipv4
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 timers msec 200 msec 1000
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , <a href="#">(442 ページ)</a>	HSRP 情報を表示します。



## hsrp track

ホットスタンバイプライオリティが他のインターフェイスのアベイラビリティに基づいて変更されるようにインターフェイスを設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

**hsrp** [ *group-number* ] **track** *type interface-path-id* [ *priority-decrement* ]

**no hsrp** [ *group-number* ] **track** *type interface-path-id* [ *priority-decrement* ]

### 構文の説明

<i>group-number</i>	(任意) トラッキングが適用されるインターフェイス上のグループ番号。デフォルトは 0 です。
<i>type</i>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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、 <b>show interfaces</b> 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>priority-decrement</i>	(任意) インターフェイスがダウンした (または復旧した) ときに、ルータのホットスタンバイプライオリティを減少 (または増加) させる分量。範囲は 1 ~ 255 です。

### コマンド デフォルト

*group-number* : 0

*priority-decrement* : 10

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	このコマンドが導入されました。
リリース 4.2.0	このコマンドはすでに廃止されています。このコマンドは、 <b>preempt hsrp</b> コマンドに置き換えられました。

**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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp track** コマンドは、ホットスタンバイプライオリティを、そのインターフェイスのアベイラビリティに結合します。これは、ホットスタンバイ ルータ プロトコル (HSRP) 用に設定されていないインターフェイスのトラッキングに役立ちます。IP インターフェイスだけがトラッキングされます。トラッキングされるインターフェイスは、そのインターフェイス上の IP が立ち上がると起動します。IP が立ち上がらないと、トラッキングされるインターフェイスはダウンします。

トラッキングされるインターフェイスがダウンすると、ホットスタンバイプライオリティは 10 減少します。インターフェイスがトラッキングされていない場合は、ステートが変化した場合でもホットスタンバイプライオリティに影響することはありません。ホットスタンバイ用に設定されたグループごとに、トラッキングするインターフェイスのリストを個別に設定できます。

オプションの *priority-decrement* 引数は、トラッキングされるインターフェイスがダウンした場合にホットスタンバイプライオリティがどれだけ下がるかを指定します。トラッキングされるインターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。

トラッキング対象の複数のインターフェイスがダウンした場合、*priority-decrement* の値が設定されていれば、設定されているプライオリティの減分值が累積されます。トラッキング対象のインターフェイスがダウンした場合、どのオブジェクトにもプライオリティの減分值が設定されていない場合は、デフォルトの減分值は 10 で、累積されます。

**hsrp preempt** コマンドは、使用可能な最善のルータを使用してパケットを転送する場合に、グループ内のすべてのルータでこのコマンドと組み合わせる必要があります。**hsrp preempt** コマンドが使用されていない場合、アクティブルータは他の HSRP ルータの現在のプライオリティに関係なくアクティブになります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、10 ギガビットイーサネット インターフェイス 0/2/0/1 がインターフェイス 0/1/0/1 および 0/3/0/1 をトラッキングしています。これらの 2 つのインターフェイスのいずれか、または両方がダウンすると、ルータのホットスタンバイプライオリティが 10 だけ減少します。デフォルトのホットスタンバイプライオリティが 100 であるため、トラッキングされるインターフェイスのうちの 1 つがダウンするとプライオリティが 90 になり、両方のインターフェイスがダウンするとプライオリティが 80 になります。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1
```

```
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp track TenGigE 0/1/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp track TenGigE 0/3/0/1
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp preempt
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp ipv4 192.92.72.46
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp preempt</a> , (416 ページ)	HSRP プリエンプションとプリエンブション遅延を設定します。
<a href="#">hsrp priority</a> , (418 ページ)	HSRP プライオリティを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## hsrp use-bia

割り当て済みの MAC アドレスまたは機能アドレスの代わりに、インターフェイスの Burned-In Address を仮想 MAC アドレスとして使用するようホットスタンバイルータプロトコル (HSRP) を設定するには、HSRP インターフェイス コンフィギュレーション モードで **hsrp use-bia** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

**hsrp use-bia**

**no hsrp use-bia**

### コマンド デフォルト

HSRP は、イーサネット で事前に割り当てられた MAC アドレスを使用します。

### コマンド モード

HSRP 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	変更箇所
リリース 3.9	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

機能アドレスに設定された送信元ハードウェア アドレスでのアドレス解決プロトコル (ARP) 応答を拒否するデバイスがある場合、インターフェイスで **hsrp use-bia** コマンドを設定することをお勧めします。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、10 ギガビットイーサネットインターフェイス 0/2/0/1 の Burned-In Address が、10 ギガビットイーサネットインターフェイス 0/1/0/1 で設定されたすべてのホットスタンバイグループの仮想 IP アドレスにマッピングされる仮想 MAC アドレスとなります。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp use-bia
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp mac-address</a> , (413 ページ)	HSRP の仮想 MAC アドレスを指定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## interface (HSRP)

ホットスタンバイルータプロトコル (HSRP) インターフェイス コンフィギュレーション コマンド モードをイネーブルにするには、ルータ コンフィギュレーション モードで **interface** コマンドを使用します。インターフェイス モードを終了するには、このコマンドの **no** 形式を使用します。

**interface** *type interface-path-id*

**no interface** *type interface-path-id*

### 構文の説明

type	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
interface-path-id	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、 <b>show interfaces</b> 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

HSRP はディセーブルです。

### コマンド モード

ルータ HSRP コンフィギュレーション

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

HSRP の設定に使用するすべてのコマンドは、HSRP インターフェイス コンフィギュレーション モードで使用します。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 で HSRP インターフェイス コンフィギュレーション モードをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp  
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1  
RP/0/RSP0/CPU0:router(config-hsrp-if)#
```

## 関連コマンド

コマンド	説明
<a href="#">router hsrp</a> , (438 ページ)	HSRP をイネーブルにします。

## mac-address (hsrp)

ホットスタンバイルータプロトコル (HSRP) の MAC アドレスを指定するには、HSRP グループサブモードで **hsrp mac-address** コマンドを使用します。標準の仮想 MAC アドレス (0000.0C07.ACn) に戻すには、このコマンドの **no** 形式を使用します。

**mac-address** *address*

**nomac-address**

### 構文の説明

address	MAC アドレス。
---------	-----------

### コマンド デフォルト

このコマンドが設定されておらず、**hsrp use-bia** コマンドが設定されていない場合、標準の仮想 MAC アドレスの 0000.0C07.ACn が使用されます。n は 16 進数のグループ番号です。このアドレスは RFC 2281 『Cisco Hot Standby Router Protocol (HSRP)』で指定されています。

### コマンド モード

HSRP インターフェイス コンフィギュレーション

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp mac-address** コマンドは、ファーストホップの冗長性が仮想 MAC アドレスを使用できることに基いており、イーサネットスイッチに接続されている PC のファーストホップアドレスを変更できない IBM ネットワーキング環境を除き、推奨されません。

HSRP を使用すると、エンドステーションで IP ルーティングのファーストホップゲートウェイを見つけるのに役立ちます。エンドステーションは、デフォルトゲートウェイで設定されます。ただし、HSRP はその他のプロトコルにファーストホップの冗長性を提供できます。拡張分散ネットワーク機能 (APPN) などの一部のプロトコルでは、MAC アドレスを使用して、ルーティングのためのファーストホップを特定します。この際、多くの場合で仮想 MAC アドレスを指定する必要があります。仮想 IP アドレスは、これらのプロトコルには重要ではありません。

仮想 MAC アドレスを指定するには、**hsrp mac-address** コマンドを使用します。ルータがアクティブな場合、指定された MAC アドレスが仮想 MAC アドレスとして使用されます。このコマンドは、特定の APPN 設定を対象としています。

次の表に、APPN と IP のパラレルな用語を示します。



表 40: APPN と IP の平行な用語

APPN	IP
エンド ノード	ホスト
ネットワーク ノード	ルータまたはゲートウェイ



(注) APPN ネットワークでは、エンド ノードは隣接するネットワーク ノードの MAC アドレスを使用して設定されていることがほとんどです。仮想 MAC アドレスをエンド ノードで使用される値に設定するには、ルータで **hsrp mac-address** コマンドを使用します。

#### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

#### 例

ネットワーク ノードの MAC アドレスとして 4000.1000.1060 を使用するようにエンド ノードが設定されている場合、仮想 MAC アドレスを設定するコマンドは次のとおりです。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# mac-address 4000.1000.1060
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

#### 関連コマンド

コマンド	説明
<a href="#">hsrp use-bia, (428 ページ)</a>	HSRP を、割り当て済みの MAC アドレスの代わりに仮想 MAC アドレスとしてインターフェイスのバーンドインアドレスを使用するように設定します。
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## preempt (hsrp)

ホットスタンバイ ルータ プロトコル (HSRP) プリエンプションおよびプリエンプレションの遅延を設定するには、HSRP グループ サブモードで **hsrp preempt** 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。

**preempt** [*delay seconds*]

**no preempt** [*delay seconds*]

### 構文の説明

**delay seconds** (任意) 時間 (秒単位)。seconds 引数によって、指定されたプリエンプレションの遅延の seconds 値の間、ローカル ルータによるアクティブな役割の引き継ぎが延期されます。値の範囲は 0 ~ 3600 (1 時間) です。デフォルトは 0 (遅延なし) です。

### コマンド デフォルト

デフォルトの遅延は 0 です。

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	このコマンドが導入されました。このコマンドは、 <b>hsrp preempt</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp preempt** コマンドが設定されると、ホットスタンバイ プライオリティが現在のアクティブ ルータよりも高い場合、ローカルルータはアクティブルータとして制御を行います。**hsrp preempt** コマンドが設定されていない場合、ローカルルータは、他にアクティブ状態のルータがない場合にのみ、アクティブルータとして制御を行います。

ルータが最初に起動したとき、ルータのルーティング テーブルは完全ではありません。HSRP がプリエンプレション処理するように設定されている場合、ローカル HSRP グループがアクティブルータになりますが、適切なルーティング サービスを提供できません。この問題は、プリエンプレ

ション処理を行うルータが実際に現在のアクティブルータをプリエンプション処理する前に、遅延の設定によって解決できます。

`preempt delay seconds` 値は、現在、アクティブ状態のルータがない場合は適用されません。この場合、ローカルルータは、`preempt delay seconds` の値に関係なく適切なタイムアウト (`hsrp timers` コマンドを参照) 後にアクティブになります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、アクティブルータをプリエンプション処理する前に、プリエンプション処理する必要があることを決定してからルータが 300 秒 (5 分) 待機します。アクティブルータがない場合は、遅延が設定されている場合でも、ルータがより短い期間でアクティブルータになる可能性があります。アクティブルータのプリエンプション処理だけが延期されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-if)# preempt delay 300
RP/0/RSP0/CPU0:router(config-hsrp-if)#
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp priority</a> , (418 ページ)	HSRP プライオリティを設定します。
<a href="#">hsrp track</a> , (425 ページ)	ホットスタンバイ プライオリティが他のインターフェイスの可用性に基づいて変化するように、インターフェイスを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## priority (hsrp)

ホットスタンバイ ルータ プロトコル (HSRP) のプライオリティを設定するには、HSRP グループ サブモードで **priority** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**priority** *priority*

**no priority** *priority*

### 構文の説明

<i>priority</i>	使用可能なホットスタンバイ ルータにプライオリティを設定するプライオリティ値。範囲は 1 ~ 255 です。デフォルトは 100 です。
-----------------	--

### コマンド デフォルト

デフォルトのプライオリティは 100 です。

### コマンド モード

HSRP 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	変更箇所
リリース 4.2.0	このコマンドが導入されました。このコマンドは、 <b>hsrp priority</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

割り当てられたプライオリティは、アクティブルータとスタンバイルータを選択するために使用されます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータが指定されたアクティブルータになります。プライオリティが等しい場合、インターフェイスの IP アドレスが比較され、大きい IP アドレスを持つインターフェイスが優先されます。

インターフェイスが **hsrp track** コマンドによって設定されている場合、デバイス上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。

プリエンプションがイネーブルでない場合、ルータは、他の HSRP ルータよりもプライオリティが高い場合でもアクティブになっていない可能性があります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次の例では、ルータのプライオリティが 120 です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# priority 120
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp preempt, (416 ページ)</a>	HSRP プリエンプションとプリエンブション遅延を設定します。
<a href="#">hsrp track, (425 ページ)</a>	ホットスタンバイプライオリティが他のインターフェイスの可用性に基づいて変化するように、インターフェイスを設定します。
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## router hsrp

ホットスタンバイ ルータ プロトコル (HSRP) をイネーブルにするには、グローバル コンフィギュレーション モードで **router hsrp** コマンドを使用します。HSRP をディセーブルに設定するには、このコマンドの **no** 形式を使用します。

**router hsrp**

**no router hsrp**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

HSRP はディセーブルです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース

変更箇所

リリース 3.9

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

HSRP コンフィギュレーション コマンドは、HSRP インターフェイス コンフィギュレーション モードで設定する必要があります。

### タスク ID

タスク ID

操作

hsrp

読み取り、書き込み

### 例

次に、10 ギガビット イーサネット インターフェイス 0/2/0/1 の仮想ルータ グループ 1 が含まれている HSRP 冗長性プロセスを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router hsrp
```

```
RP/0/RSP0/CPU0:router(config-hsrp)# interface TenGigE 0/2/0/1  
RP/0/RSP0/CPU0:router(config-hsrp-if)# hsrp 1 priority 254
```

## session name

HSRP セッション名を設定するには、HSRP グループ サブモードで **session name** コマンドを使用します。HSRP セッション名の設定を解除するには、このコマンドの **no** 形式を使用します。

**name name**

### 構文の説明

<i>name</i>	MGO セッション名
-------------	------------

### コマンド デフォルト

なし

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り

### 例

次に、HSRP セッション名を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# name s1
```



```
RP/0/RSP0/CPU0:router(config-hsrp-gp) #
```

## 関連コマンド

コマンド	説明
<a href="#">mac-address (hsrp)</a> , (432 ページ)	ホットスタンバイルータプロトコル (HSRP) の仮想 MAC アドレスを設定します。

# show hsrp

ホットスタンバイ ルータ プロトコル (HSRP) 情報を表示するには、EXEC モードで **show hsrp** コマンドを使用します。

**show hsrp** [interface *type interface-path-id*] [*group-number*][*brief* | *detail*]

## 構文の説明

type	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用してください。
interface-path-id	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、 <b>show interfaces</b> 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。
group-number	(任意) 出力が表示されるインターフェイスのグループ番号。
brief	(任意) 出力の1つの行に、各スタンバイグループが要約されます。 <b>brief</b> キーワードは、 <b>detail</b> が指定されていない場合のデフォルトです。
detail	(任意) このキーワードには、 <b>brief</b> を指定しない場合と同じ効果があります。より多くの出力が提供されます。
	(任意) この縦棒 ( ) の後に、出力から出力修飾子のいずれか1つとキーワードを指定します。 <ul style="list-style-type: none"> <li>• <b>begin</b> : 指定した単語の出力を開始します。</li> <li>• <b>exclude</b> : 指定した単語と一致する行を除外します。</li> <li>• <b>include</b> : 指定した単語と一致する行を含めます。</li> </ul>

## コマンド デフォルト

デフォルトでは、各スタンバイグループを要約する出力の行が表示されます。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.9	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

HSRP 情報を表示するには、**show hsrp** コマンドを使用します。

*group-number* 引数の値を指定する場合は、インターフェイスの *type* および *number* を指定する必要があります。

## タスク ID

タスク ID	操作
hsrp	読み取り

## 例

次の例では、**show hsrp detail** コマンドの出力を示します。

```
RP/0/RSP0/CPU0:router# show hsrp detail
GigabitEthernet0/4/0/0 - Group 1
  Local state is Active, priority 100
  Hello time 3 sec holdtime 10 sec
  Next hello sent in 0.539
  Minimum delay 1 sec, reload delay 5 sec
  BFD enabled: state none, interval 15 ms multiplier 3
  Hot standby IP address is 4.0.0.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac01
  2 state changes, last state change 00:05:20
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 41 : **show hsrp** コマンドのフィールドの説明

フィールド	説明
TenGigE0/2/0/4	インターフェイスタイプおよびインターフェイスのホットスタンバイグループ番号。

フィールド	説明
Local state is	<p>ローカル ネットワーキング デバイスの状態。次のいずれになります。</p> <ul style="list-style-type: none"> <li>• <b>Active</b> : 現在のホットスタンバイルータ。</li> <li>• <b>Standby</b> : 次にホットスタンバイルータになるルータ。</li> <li>• <b>Speak</b> : ルータがアクティブまたはスタンバイ ロールを要求するパケットを送信中です。</li> <li>• <b>Listen</b> : ルータは、アクティブまたはスタンバイではありませんが、アクティブルータまたはスタンバイルータからメッセージが受信されない場合、「通話」を開始します。</li> <li>• <b>Learn</b> : ルータはアクティブまたはスタンバイではなく、アクティブ ロールまたはスタンバイ ロールを要求するのに十分な情報がありません。</li> <li>• <b>Init</b> : ルータは、関連インターフェイスが稼動していないため、HSRP に参加する準備ができていません。</li> </ul>
Hello time	アクティブ ホットスタンバイルータから受信した <b>hello</b> パケットから動的に学習した <b>hello</b> パケットの送信間の現在の時間 (秒単位)。
holdtime	アクティブ ホットスタンバイルータから受信した <b>hello</b> パケットから動的に学習した、他のルータがアクティブルータまたはスタンバイルータのダウンを宣言する前の現在の時間 (秒単位)。
Next hello sent in	ソフトウェアが次の <b>hello</b> パケットを送信する時間 (時間 : 分 : 秒)。
BFD enabled	BFD の関連情報が表示されます (乗数および最小間隔の細部)

フィールド	説明
Hot standby IP address is configured	現在のホットスタンバイ ルータの IP アドレス。単語「configured」は、このアドレスが <b>hsrp ip</b> コマンドを介して認識されていることを示しています。その他の場合、このアドレスは HSRP IP アドレスが設定されている他のルータからの HSRP hello パケットによって動的に学習されます。
Active router is	値は、「local」または IP アドレスです。現在のアクティブなホットスタンバイ ルータのアドレス。
Standby router is	値は、「local」またはスタンバイルータ（次にホットスタンバイ ルータになるルータ）の IP アドレスです。
Standby virtual mac address is	スタンバイ グループ アドレスに関連付けられている MAC アドレス。
state changes	ルータがスタンバイ状態を変更した回数。
last state change	最後に状態が変更されてからの経過時間（時間：分：秒）。
Tracking interface states for	トラッキング対象オブジェクトのリストと対応する状態。 <b>hsrp track</b> コマンドに基づきます。
Priority decrement	トラッキング対象のインターフェイスがダウンするか、または稼動する場合にそれぞれスタンバイ プライオリティを減少または増加させる値。デフォルトは 10 です。

## 関連コマンド

コマンド	説明
<a href="#">hsrp authentication, (401 ページ)</a>	HSRP の認証文字列を設定します。
<a href="#">hsrp ipv4, (411 ページ)</a>	HSRP をアクティブ化します。
<a href="#">hsrp mac-address, (413 ページ)</a>	HSRP の仮想 MAC アドレスを指定します。

コマンド	説明
<a href="#">hsrp preempt</a> , (416 ページ)	HSRP プリエンプションとプリエンプレション遅延を設定します。
<a href="#">hsrp priority</a> , (418 ページ)	HSRP プライオリティを設定します。
<a href="#">hsrp timers</a> , (422 ページ)	hello パケットの間隔と、他のルータがアクティブ ホット スタンバイまたはスタンバイ ルータの終了を宣言するまでの時間を設定します。
<a href="#">hsrp track</a> , (425 ページ)	ホット スタンバイ プライオリティが他のインターフェイスの可用性に基づいて変化するよう に、インターフェイスを設定します。
<a href="#">hsrp use-bia</a> , (428 ページ)	HSRP を、割り当て済みの MAC アドレスの代わりに仮想 MAC アドレスとしてインターフェイスのバインドインアドレスを使用するよう設定します。

## show hsrp bfd

すべてのインターフェイスにわたるホットスタンバイ ルータ プロトコル (HSRP) BFD 情報を表示するには、EXEC モードで **show hsrp bfd** コマンドを使用します。

**show hsrp bfd** [*interface-type interface-path-id ip-address*]

### 構文の説明

<i>interface-type</i>	物理インターフェイスまたは仮想インターフェイス。
<i>interface-path-id</i>	(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、 <b>show interfaces</b> 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>ip-address</i>	(任意) BFD セッションの宛先 IP アドレス。

### コマンド デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り

## 例

次に、すべてのインターフェイスにわたるホットスタンバイ ルータ プロトコル (HSRP) BFD 情報を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show hsrp bfd
```

BFD Interface	Destination IP	State	Intv	Mult	HSRP Interface	Grp
Gi0/3/0/2	10.0.0.2	up	100	3	Gi0/3/0/2	1
					Gi0/3/0/2	2
Gi0/3/0/2	10.0.0.3	inactive	100	3	Gi0/3/0/2	3
					Gi0/3/0/2	6
Gi0/3/0/3.1	10.0.1.2	down	15	3	Gi0/3/0/2	4

次に、GigabitEthernet 0/3/0/2 インターフェイスのホットスタンバイ ルータ プロトコル (HSRP) BFD 情報を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show hsrp bfd GigabitEthernet 0/3/0/2 10.0.0.2
```

BFD Interface	Destination IP	State	Intv	Mult	HSRP Interface	Grp
Gi0/3/0/2	10.0.0.2	up	100	3	Gi0/3/0/2	1
					Gi0/3/0/2	2

## 関連コマンド

コマンド	説明
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。



## show hsrp mgo

すべてのインターフェイスにわたるホットスタンバイルータプロトコル (HSRP) MGO 情報を表示するには、EXEC モードで **show hsrp mgo** コマンドを使用します。

**show hsrp mgo** [**brief**] *session-name*

### 構文の説明

<b>brief</b>	(任意) 簡単な形式で情報を表示します。
<i>session-name</i>	(任意) 単一 MGO セッションの情報を表示します。

### コマンド デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り

### 例

次に、インターフェイス HSRP3 のホットスタンバイルータプロトコル (HSRP) MGO 情報を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show hsrp mgo HSRP3
```

## show hsrp mgo

```

HSRP3
Primary group Bundle-Ether1.1 IPv4 group 1
State is Active
Slave groups:
Interface          Grp
Bundle-Ether1.2    2
Bundle-Ether1.3    3
Bundle-Ether1.4    4
Bundle-Ether1.5    5

```

次に、すべてのインターフェイスにわたるホットスタンバイルータプロトコル (HSRP) MGO情報を簡単な形式で表示する例を示します。

```
RP/0/RSP0/CPU0:router# show hsrp mgo brief
```

```

Name          Interface      AF  Grp  State Slaves
HSRP1         Gi0/0/0/1      IPv4  1    Active  100
HSRP2         Te0/1/0/0.1   IPv4  2    Standby  50
HSRP3         BE1            IPv4  1    Active   4
HSRP4         BE1            IPv6  10   Active  11

```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## show hsrp statistics

すべてのインターフェイスにわたるホットスタンバイ ルータ プロトコル (HSRP) 統計情報を表示するには、EXEC モードで **show hsrp statistics** コマンドを使用します。

**show hsrp** [*interface-type interface-path-id*] *group-number* **statistics**

### 構文の説明

<i>interface-type</i>	物理インターフェイスまたは仮想インターフェイス。
<i>interface-path-id</i>	(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、 <b>show interfaces</b> 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>group-number</i>	(任意) インターフェイスのグループ番号。

### コマンド デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り

## 例

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

```
RP/0/RSP0/CPU0:router# show hsrp statistics
Protocol:
  Transitions to Active          2
  Transitions to Standby        2
  Transitions to Speak          0
  Transitions to Listen         2
  Transitions to Learn          0
  Transitions to Init           0

Packets Sent:
  Hello:                         7
  Resign:                        0
  Coup:                          2
  Adver:                         3

Valid Packets Received:
  Hello:                         8
  Resign:                        2
  Coup:                          0
  Adver:                         3

Invalid packets received:
  Too long:                      0
  Too short:                     0
  Mismatching/unsupported versions: 0
  Invalid opcode:                0
  Unknown group:                 0
  Inoperational group:          0
  Conflicting Source IP:         0
  Failed Authentication:         2
  Invalid Hello Time:           0
  Mismatching Virtual IP:       0
```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## show hsrp summary

すべてのインターフェイスにわたるホットスタンバイ ルータ プロトコル (HSRP) サマリー情報を表示するには、EXEC モードで **show hsrp summary** コマンドを使用します。

### show hsrp summary

#### 構文の説明

このコマンドには、キーワードと引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
hsrp	読み取り

#### 例

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

```
RP/0/RSP0/CPU0:router# show hsrp summary
          Groups
State  Sessions  Slaves  Total    Up    Down  Total
-----
ALL           60     900    960     860  2020  2880

ACTIVE       10     190    200     200   300    500
STANDBY      15     235    250     250   600    850
SPEAK        10     190    200     200   400    600
```

## show hsrp summary

```

LISTEN      10    190   200   200   400   600
LEARN       5     5     10    10    20    30
INIT        10    90    100   0     300   300

48 HSRP IPv4 interfaces (43 up, 5 down)
5  Tracked IPv4 interfaces (4 up, 1 down)
5  BFD sessions (3 up, 2 down)

```

## 関連コマンド

コマンド	説明
<a href="#">show hsrp, (442 ページ)</a>	HSRP 情報を表示します。

## slave follow

指定したグループからステートを継承するようにスレーブグループに指示するには、HSRP スレーブサブモードモードで **slave follow** コマンドを使用します。

**follow** *mgo-session-name*

### 構文の説明

<i>mgo-session-name</i>	スレーブグループがステートを継承する MGO セッションの名前。
-------------------------	----------------------------------

### コマンドデフォルト

なし

### コマンドモード

HSRP スレーブサブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

### 例

次に、指定したグループからステートを継承するようにスレーブグループに指示する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
```

```
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp slave
RP/0/RSP0/CPU0:router(config-hsrp-slave)# follow m1
```

## 関連コマンド

コマンド	説明
<a href="#">slave virtual mac address, (461 ページ)</a>	スレーブ グループに仮想 MAC アドレスを設定します。



## slave primary virtual IPv4 address

スレーブグループのプライマリ仮想IPv4アドレスを設定するには、HSRP スレーブサブモードで **slave primary virtual IPv4 address** コマンドを使用します。

**address** *ip-address*

### 構文の説明

*ip-address* ホットスタンバイ ルータ インターフェイスの IP アドレス。

### コマンド デフォルト

なし

### コマンド モード

HSRP スレーブサブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

### 例

次に、スレーブグループのプライマリ仮想 IPv4 アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp slave
```

## ■ slave primary virtual IPv4 address

```
RP/0/RSP0/CPU0:router(config-hsrp-slave)# address 10.2.1.4
```

## 関連コマンド

コマンド	説明
<a href="#">slave follow, (455 ページ)</a>	指定したグループからステートを継承するようにスレーブ グループに指示します。
<a href="#">slave virtual mac address, (461 ページ)</a>	スレーブ グループに仮想 MAC アドレスを設定します。

## slave secondary virtual IPv4 address

スレーブグループのセカンダリ仮想IPv4アドレスを設定するには、HSRP スレーブサブモードで **slave secondary virtual IPv4 address** コマンドを使用します。

**address ip-address secondary**

### 構文の説明

<i>ip-address</i>	ホットスタンバイ ルータ インターフェイスの IP アドレス。
<b>secondary</b>	セカンダリ ホットスタンバイ IP アドレスを設定します。

### コマンド デフォルト

なし

### コマンド モード

HSRP スレーブサブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

### 例

次に、スレーブグループのセカンダリ仮想 IPv4 アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
```

## ■ slave secondary virtual IPv4 address

```
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp slave
RP/0/RSP0/CPU0:router(config-hsrp-slave)# address 10.2.1.4 secondary
```

## 関連コマンド

コマンド	説明
<a href="#">slave follow, (455 ページ)</a>	指定したグループからステートを継承するようにスレーブグループに指示します。
<a href="#">slave virtual mac address, (461 ページ)</a>	スレーブグループに仮想 MAC アドレスを設定します。

## slave virtual mac address

スレーブグループの仮想MACアドレスを設定するには、HSRP スレーブサブモードで **slave virtual mac address** コマンドを使用します。

**mac-address** *address*

### 構文の説明

*address* ARP エントリの 48 ビット ハードウェア アドレス。

### コマンド デフォルト

なし

### コマンド モード

HSRP スレーブ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

例 次に、スレーブグループの仮想MACアドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp slave
```

## ■ slave virtual mac address

```
RP/0/RSP0/CPU0:router(config-hsrp-slave)# mac-address 10.2.4
```

## 関連コマンド

コマンド	説明
<a href="#">slave follow</a> , (455 ページ)	指定したグループからステートを継承するようにスレーブ グループに指示します。

## timers (hsrp)

hello パケット間の時間と他のルータがアクティブ ホットスタンバイまたはスタンバイ ルータのダウンを宣言するまでの時間を設定するには、HSRP グループサブモードで **hsrp timers** コマンドを使用します。タイマー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。

**timers** {*hello-seconds*| **msec** *hello-milliseconds*} {*hold-seconds*| **msec** *hold-milliseconds*}

**no timers**

### 構文の説明

<b>hello-seconds</b>	秒単位の <b>hello</b> 間隔。範囲は 1 ~ 255 です。デフォルトは 3 です。
<b>msec</b> <i>hello-milliseconds</i>	ミリ秒単位の <b>hello</b> 間隔。範囲は 100 ~ 3000 です。
<b>hold-seconds</b>	アクティブまたはスタンバイ ルータがダウンを宣言されるまでの時間 (秒)。範囲は 1 ~ 255 です。デフォルトは 10 です。
<b>msec</b> <i>hold-milliseconds</i>	アクティブまたはスタンバイ ルータがダウンを宣言されるまでの時間 (ミリ秒)。範囲は 100 ~ 3000 です。

### コマンド デフォルト

デフォルトの **hello-seconds** は 3 です (**msec** キーワードが指定されている場合、デフォルト値はありません)。

デフォルトの **hold-seconds** は 10 です (**msec** キーワードが指定されている場合、デフォルト値はありません)。

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

非アクティブルータは、ミリ秒のタイマー値が使用されていない場合、アクティブルータのタイマー値を学習します。ミリ秒のタイマー値が使用されている場合は、すべてのルータはミリ秒のタイマー値を使用して設定されていなければなりません。このルールは、hello時間とホールド時間のどちらかがミリ秒単位で指定されている場合に当てはまります。

アクティブルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。ホットスタンバイグループのすべてのルータで、同じタイマー値を使用する必要があります。通常、ホールドタイムはhelloタイムの3倍以上となります ( $\text{holdtime} > 3 * \text{hellotime}$ )。

helloタイムを秒単位またはミリ秒単位のいずれにするかに応じて、*hello-seconds* 引数または **msec** キーワードおよび *hello-milliseconds* 引数を指定する必要があります。また、ホールドタイムを秒単位またはミリ秒単位のいずれにするかに応じて、*hold-seconds* 引数または **msec** キーワードおよび *hold-milliseconds* 引数を指定する必要があります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、10 ギガビットイーサネットインターフェイス 0/2/0/1 上のグループ番号 1 に対して、hello パケットの間隔を 5 秒に設定し、ルータがダウンしたと見なされるまでに時間を 15 秒に設定する例を示します。設定されたタイマー値は、ルータがアクティブである場合にのみ使用されます（または、タイマー値が学習される前）。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router (config)# router hsrp
RP/0/RSP0/CPU0:router (config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router (config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router (config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router (config-hsrp-gp)# timers 5 15
RP/0/RSP0/CPU0:router (config-hsrp-gp)#
```

次に、10 ギガビットイーサネットインターフェイス 0/2/0/1 上のグループ番号 1 に対して、hello パケットの間隔を 200 ミリ秒に設定し、ルータがダウンしたと見なされるまでに時間を 1000 ミリ秒に設定する例を示します。ミリ秒が指定されているため、設定されたタイマー値は常に使用されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router (config)# router hsrp
RP/0/RSP0/CPU0:router (config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router (config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router (config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router (config-hsrp-gp)# timers msec 200 msec 1000
RP/0/RSP0/CPU0:router (config-hsrp-gp)#
```



## 関連コマンド

コマンド	説明
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。

## track (hsrp)

ホットスタンバイプライオリティが他のインターフェイスのアベイラビリティに基づいて変更されるようにインターフェイスを設定するには、HSRP グループ サブモードで **hsrp track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

**track type interface-path-id** [ *priority-decrement* ]

**no track type interface-path-id** [ *priority-decrement* ]

### 構文の説明

<i>type</i>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<i>interface-path-id</i> <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、 <b>show interfaces</b> 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>priority-decrement</i>	(任意) インターフェイスがダウンした (または復旧した) ときに、ルータのホットスタンバイプライオリティを減少 (または増加) させる分量。範囲は 1 ~ 255 です。

### コマンド デフォルト

デフォルトの *priority-decrement* は 10 です。

### コマンド モード

HSRP グループ サブモード

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	このコマンドが導入されました。このコマンドは、 <b>hsrp track</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**hsrp track** コマンドは、ホットスタンバイプライオリティを、そのインターフェイスのアベイラビリティに結合します。これは、ホットスタンバイルータプロトコル (HSRP) 用に設定されていないインターフェイスのトラッキングに役立ちます。IP インターフェイスだけがトラッキングされます。トラッキングされるインターフェイスは、そのインターフェイス上の IP が立ち上がると起動します。IP が立ち上がらなると、トラッキングされるインターフェイスはダウンします。

トラッキングされるインターフェイスがダウンすると、ホットスタンバイプライオリティは 10 減少します。インターフェイスがトラッキングされていなければ、ステートが変化した場合でもホットスタンバイプライオリティに影響することはありません。ホットスタンバイ用に設定されたグループごとに、トラッキングするインターフェイスのリストを個別に設定できます。

オプションの *priority-decrement* 引数は、トラッキングされるインターフェイスがダウンした場合にホットスタンバイプライオリティがどれだけ下がるかを指定します。トラッキングされるインターフェイスが稼動状態に戻ると、プライオリティは同じ分だけ増加します。

トラッキング対象の複数のインターフェイスがダウンした場合、*priority-decrement* の値が設定されていれば、設定されているプライオリティの減分値が累積されます。トラッキング対象のインターフェイスがダウンした場合、どのオブジェクトにもプライオリティの減分値が設定されていなければ、デフォルトの減分値は 10 で、累積されます。

**hsrp preempt** コマンドは、使用可能な最善のルータを使用してパケットを転送する場合に、グループ内のすべてのルータでこのコマンドと組み合わせて使用する必要があります。**hsrp preempt** コマンドが使用されていない場合、アクティブルータは他の HSRP ルータの現在のプライオリティに関係なくアクティブになります。

## タスク ID

タスク ID	操作
hsrp	読み取り、書き込み

## 例

次に、ホットスタンバイプライオリティが他のインターフェイスのアベイラビリティに基づいて変更されるようにインターフェイスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router hsrp
RP/0/RSP0/CPU0:router(config-hsrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-hsrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-hsrp-ipv4)# hsrp 1
RP/0/RSP0/CPU0:router(config-hsrp-gp)# track tenGigE 0/4/0/4 2
RP/0/RSP0/CPU0:router(config-hsrp-gp)#
```

## 関連コマンド

コマンド	説明
<a href="#">hsrp preempt</a> , (416 ページ)	HSRP プリエンプションとプリエンブション遅延を設定します。

コマンド	説明
<a href="#">hsrp priority</a> , (418 ページ)	HSRP プライオリティを設定します。
<a href="#">show hsrp</a> , (442 ページ)	HSRP 情報を表示します。



## LPTS コマンド

---

この章では、Cisco ASR 9000 シリーズアグリゲーションサービスルータ上で Local Packet Transport Services (LPTS) を監視するために使用する Cisco IOS XR ソフトウェア コマンドについて説明します。

LPTS の概念、設定作業、例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [clear lpts ifib statistics, 471 ページ](#)
- [clear lpts pifib hardware statistics, 473 ページ](#)
- [clear lpts pifib statistics, 476 ページ](#)
- [flow \(LPTS\), 478 ページ](#)
- [lpts pifib hardware police, 485 ページ](#)
- [show lpts bindings, 487 ページ](#)
- [show lpts clients, 492 ページ](#)
- [show lpts flows, 495 ページ](#)
- [show lpts ifib, 499 ページ](#)
- [show lpts ifib slices, 503 ページ](#)
- [show lpts ifib statistics, 507 ページ](#)
- [show lpts ifib times, 509 ページ](#)
- [show lpts mpa groups, 511 ページ](#)
- [show lpts pifib, 513 ページ](#)
- [show lpts pifib hardware context, 519 ページ](#)
- [show lpts pifib hardware entry, 522 ページ](#)
- [show lpts pifib hardware police, 526 ページ](#)
- [show lpts pifib hardware usage, 530 ページ](#)

- [show lpts pifib statistics, 532 ページ](#)
- [show lpts port-arbitrator statistics, 534 ページ](#)
- [show lpts vrf, 536 ページ](#)

## clear lpts ifib statistics

Internal Forwarding Information Base (IFIB) 統計情報をクリアするには、EXEC モードで **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** (任意) 指定したノードの IFIB 統計情報をクリアします。 *node-id* 引数は、標準的な *rack/slot/module* 表記で入力します。

### 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**location** キーワードと *node-id* 引数でノードを指定しない場合、**clear lpts ifib statistics** コマンドは、コマンドを実行したノード上の IFIB 統計情報をクリアします。

### タスク ID

タスク ID	操作
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。

## clear lpts ifib statistics

```
RP/0/RSP0/CPU0:router# clear lpts ifib statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show lpts ifib statistics</a> , ( <a href="#">507 ページ</a> )	LPTS IFIB 統計情報を表示します。



## clear lpts pifib hardware statistics

Pre-Internal Forwarding Information Base (Pre-IFIB) ハードウェア統計情報をクリアするには、EXEC モードで **clear lpts pifib hardware statistics** コマンドを使用します。

**clear lpts pifib hardware statistics location node-id**

### 構文の説明

**location node-id** 指定したノードの Pre-IFIB ハードウェア統計情報をクリアします。  
*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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**location** キーワードと *node-id* 引数でノードを指定しない場合、コマンドを実行したノードの Pre-IFIB ハードウェア統計情報がクリアされます。

### タスク ID

タスク ID	操作
lpts	実行

### 例

次に、show lpts hardware police コマンドを実行し、RP の Pre-IFIB ハードウェア統計情報クリアする例を示します。

## clear lpts pifib hardware statistics

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/1/CPU0
```

```
-----
Node 0/1/CPU0:
-----
Burst = 100ms for all flow types
-----
```

FlowType	Policer	Type	Cur. Rate	Def. Rate	Accepted	Dropped
unconfigured-default	100	Static	2500	2500	0	0
Fragment	101	Static	2500	2500	0	0
OSPF-mc-known	102	Static	1500	1500	0	0
OSPF-mc-default	103	Static	2000	2000	0	0
OSPF-uc-known	104	Static	1000	1000	0	0
OSPF-uc-default	105	Static	2000	2000	0	0
ISIS-known	143	Static	1500	1500	0	0
ISIS-default	144	Static	2000	2000	0	0
BGP-known	106	Static	1500	1500	0	0
BGP-cfg-peer	107	Static	2000	2000	0	0
BGP-default	108	Static	2500	2500	0	0
PIM-mcast	109	Static	2000	2000	0	0
PIM-ucast	110	Static	1500	1500	0	0
IGMP	111	Static	500	500	0	0
ICMP-local	112	Static	1500	1500	0	0
ICMP-app	112	Static	1500	1500	0	0
na	140	Static	1000	1000	0	0
ICMP-default	112	Static	1500	1500	0	0
LDP-TCP-known	113	Static	1500	1500	0	0

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/2/CPU0
```

```
-----
Node 0/2/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	4285	0
OSPF-mc-default	111	Static	5000	5000	1	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
BGP-known	113	Static	25000	25000	891	0
BGP-cfg-peer	114	Static	10000	10000	6	0
BGP-default	115	Static	10000	10000	2	0
PIM-mcast	116	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

```

```
RP/0/RSP0/CPU0:router# clear lpts pifib hardware statistics location 0/2/CPU0
```

```
Clear "show controllers statistics" counters on this location [confirm]
```

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware police location 0/2/CPU0
```

```

-----
Node 0/2/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       14        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
BGP-known             113      Static  25000     25000        1         0
BGP-cfg-peer         114      Static  10000     10000        0         0
BGP-default           115      Static  10000     10000        0         0
PIM-mcast             116      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

```

## 関連コマンド

コマンド	説明
<a href="#">show lpts pifib hardware police, (526 ページ)</a>	ポリサー設定値セットを表示します。

## clear lpts pifib statistics

Pre-Internal Forwarding Information Base (Pre-IFIB) 統計情報をクリアするには、EXEC モードで **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

<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**location** キーワードと *node-id* 引数でノードを指定しない場合、コマンドを実行したノードの Pre-IFIB 統計情報がクリアされます。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear lpts pifib statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show lpts pifib statistics</a> , (532 ページ)	LPTS PIFIB 統計情報を表示します。

## flow (LPTS)

Local Packet Transport Services (LPTS) フロータイプのポリサーを設定するには、**pifib** ポリサーグローバルコンフィギュレーションモードまたは**pifib** ポリサーノードごとコンフィギュレーションモードで **flow** 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。

**flow** *flow-type rate rate*

**no flow** *flow-type rate rate*

### 構文の説明

<b>flow-type</b>	サポートされているフロータイプの一覧。
<b>rate rate</b>	レートをパケット/秒 (PPS) 単位で指定します。範囲は 0 ~ 4294967295 です。

### コマンド デフォルト

デフォルトでは、プラットフォーム依存の静的なコンフィギュレーションファイルからポリサー値がロードされます。

### コマンド モード

**pifib policer** グローバル コンフィギュレーション  
**pifib policer** ノードごとコンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

次の表に、サポートされているフロータイプと、ポリサーを定義するために使用されるパラメータの一覧を示します。

次の表に、サポートされているフロータイプと、ポリサーを定義するために使用されるパラメータの一覧を示します。

表 42: サポートされているフロータイプの一覧

フロータイプ	説明	デフォルトのパケットレート (推奨)
all-routers	all-routers マルチキャストアドレスに送信されたパケット (マルチキャスト LDP UDP パケットを含む)	1000
bgp-cfg-peer	設定されている BGP ピアからのパケット	2000
bgp-default	未設定、新規設定、ワイルドカード BGP ピアからのパケット	2500
bgp-known	確立済みの BGP ピアリングセッションからのパケット	1500
css-default	新規 CSS セッションまたは新たに確立された CSS セッションからのパケット	200
css-known	確立済み CSS セッションからのパケット	200
default-flow	デフォルトフロータイプ	2500
eigrp	設定済みインターフェイスの EIGRP パケット	1500
gre	総称ルーティング カプセル化パケット	1000
fragment	フラグメント化されたパケット。	2500
http-default	新規 HTTP セッションまたは新たに確立された HTTP セッションからのパケット	400
http-known	確立済み HTTP セッションからのパケット	200

フロー タイプ	説明	デフォルトのパケットレート (推奨)
icmp-app	アプリケーションに関する ICMP または ICMPv6 パケット	1500
icmp-default	その他の ICMP または ICMPv6 パケット	1500
icmp-local	ローカル関係の ICMP または ICMPv6 パケット	1500
igmp	IGMP パケット	500
ike	IKE パケット	100
ipsec-default	不明な SPI または新たに設定さ れた SPI を使用した AH または ESP パケット	100
ipsec-known	既知の SPI を使用した AH また は ESP パケット	400
ip-sla	IP SLA パケット (これは非表 示のフロー タイプです)	1000
isis-default	未設定の (または新規に設定さ れた) インターフェイスの IS-IS パケット	2000
isis-known	設定済みインターフェイスの IS-IS パケット	1500
ldp-tcp-cfg-peer	設定済み LDP TCP ピアからの パケット (SYN または新たに 確立されたセッション)	2000
ldp-tcp-default	未設定、新規設定、ワイルド カード LDP TCP ピアからのパ ケット	2500
ldp-tcp-known	確立済み LDP ピアリングセッ ションからのパケット	1500
ldp-udp	ユニキャスト LDP UDP パケッ ト	2000



フロータイプ	説明	デフォルトのパケットレート (推奨)
lmp-tcp-cfg-peer	設定済み LMP TCP ピアからの パケット (SYN または新たに 確立されたセッション)	2000
lmp-tcp-default	未設定、新規設定、ワイルド カード LMP TCP ピアからのパ ケット	2500
lmp-tcp-known	確立済み LMP ピアリングセッ ションからのパケット	1500
lmp-udp	ユニキャスト LMP UDP パケッ ト	2000
msdp-cfg-peer	設定済み MSDP ピアからのパ ケット	200
msdp-default	未設定、新規設定、ワイルド カード MSDP ピアからのパケッ ト	300
msdp-known	確立済み MSDP セッションか らのパケット	100
multicast-default	未設定または新規設定マルチ キャスト グループのパケット	2500
multicast-known	設定済みマルチキャストグルー プのパケット	2000
ntp	NTP パケット	200
ospf-mc_default	未設定の (または新たに設定さ れた) インターフェイスの OSPF マルチキャストパケット	2000
ospf-mc-known	設定済みインターフェイスの OSPF マルチキャストパケット	1500
ospf-uc-default	未設定の (または新たに設定さ れた) インターフェイスの OSPF ユニキャストパケット	2000

フロー タイプ	説明	デフォルトのパケットレート (推奨)
ospf-uc-known	設定済みインターフェイスの OSPF ユニキャスト パケット	1000
pim-multicast	PIM マルチキャスト パケット	2000
pim-unicast	PIM ユニキャスト パケット	1500
rip	RIP パケット	1500
rsh-default	新規 RSH セッションまたは新 たに確立された RSH セッシ ョンからのパケット	200
rsh-known	確立済み RSH セッションから のパケット	200
rsvp	RSVP パケット	2000
rsvp-udp	RSVP UDP パケット	2000
raw-default	未設定または新たに設定され た IPv4 または IPv6 プロトコ ルのパケット	2500
raw-listen	設定済み IP プロトコルのパ ケット	2500
shttp-default	新規 SHTTP セッションまたは 新たに確立された SHTTP セ ッションからのパケット	400
shttp-known	確立済み SHTTP セッションか らのパケット	200
snmp	SNMP パケット	300
ssh-default	新規 SSH セッションまたは新 たに確立された SSH セッシ ョンからのパケット	300
ssh-known	確立済み SSH セッションから のパケット	200

フロータイプ	説明	デフォルトのパケットレート (推奨)
tcp-cfg-peer	設定済み TCP ピアの packets	2000
tcp-default	未設定または新たに設定された TCP サービスの packets	2500
tcp-known	確立済み TCP セッションの packets	2000
tcp-listen	設定済み TCP サービスの packets	2500
telnet-default	新規 Telnet セッションまたは新たに確立された Telnet セッションからの packets	200
telnet-known	確立済み Telnet セッションからの packets	200
udp-cfg-peer	設定済み UDP ベース プロトコル セッションの packets	2500
udp-default	未設定または新たに設定された UDP サービスの packets	2500
udp-known	確立済み UDP セッションの packets	2000
udp-listen	設定済み UDP サービスの packets	2500

---

**タスク ID**


---

**タスク ID**


---

**操作**


---

config-services

---

読み取り、書き込み

---

**例**

次に、すべてのラインカードに対して bgp-known フロータイプの LPTS ポリサーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police  
RP/0/RSP0/CPU0:router(config-pifib-policer-global)# flow bgp-known rate 20000
```

次に、特定のラインカードに対して Intermediate System-to-Intermediate System (IS-IS)-known フロータイプの LPTS ポリサーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure  
RP/0/RSP0/CPU0:routerconfig)# lpts pifib hardware police location 0/2/CPU0  
RP/0/RSP0/CPU0:router(config-pifib-policer-per-node)# flow ISIS-known rate 22222
```

# lpts pifib hardware police

入力ポリサーを設定し、pifib policer グローバル コンフィギュレーションモードまたは pifib policer ノードごとコンフィギュレーションモードに移行するには、グローバルコンフィギュレーションモードで **lpts pifib hardware police** コマンドを使用します。ポリサーをデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**lpts pifib hardware police location node-id [flow flow-type rate rate]**

**no lpts pifib hardware police location node-id [flow flow-type rate rate]**

## 構文の説明

<b>location node-id</b>	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。
<b>flow flow-type rate rate</b>	Lpts のフロータイプおよびポリサーレート（パケット/秒（PPS）単位）。

## コマンドモード

グローバル コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2	dns、radius、tacacs、ntp known、rsvp known、pim multicast known などの新しいフロータイプが追加されました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
lpts	読み取り、書き込み
config-services	読み取り、書き込み

## 例

次の例は、すべてのラインカードに対して **lpts pifib hardware police** コマンドを設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police
RP/0/RSP0/CPU0:router(config-pifib-policer-global)#
```

次の例は、特定のラインカードに対して **lpts pifib hardware police** コマンドを設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0 flow dns rate
10
```

## 関連コマンド

コマンド	説明
<a href="#">flow (LPTS)</a> , (478 ページ)	LPTS フロー タイプのポリサーを設定します。
<a href="#">show lpts pifib hardware police</a> , (526 ページ)	ポリサー設定値セットを表示します。

## show lpts bindings

Port Arbitrator でのバインディング情報を表示するには、EXEC モードで **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

<b>location</b> <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。
<b>client-id</b>	(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"> <li>• <b>clnl</b> : ISO コネクションレス プロトコル (IS-IS で使用)</li> <li>• <b>ipsec</b> : セキュア IP</li> <li>• <b>ipv4-io</b> : IPv4 スタックによって処理されるトラフィック</li> <li>• <b>ipv6-io</b> : IPv6 スタックによって処理されるトラフィック</li> <li>• <b>mpa</b> : Multicast Port Arbitrator (マルチキャストグループ加入)</li> <li>• <b>tcp</b> : 伝送制御プロトコル</li> <li>• <b>test</b> : テスト アプリケーション</li> <li>• <b>udp</b> : ユーザ データグラム プロトコル</li> <li>• <b>raw</b> : ロー IP</li> </ul>
<b>brief</b>	(任意) 要約出力を表示します。
<b>vrf</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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リクエスト) 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。

任意の **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、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。任意の **location** キーワードと **node-id** 引数を指定した場合、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	操作
lpts	読み取り

## 例

次に、**show lpts bindings** コマンドで、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する例を示します。

```
RP/0/RSP0/CPU0:router# 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
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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 43 : *show lpts bindings* 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
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。

フィールド	説明
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)
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

次に、**show lpts bindings brief** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 44 : **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

フィールド	説明
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
Interface	インバウンドインターフェイス

## 関連コマンド

コマンド	説明
<a href="#">show lpts clients, (492 ページ)</a>	Port Arbitrator のクライアント情報を表示します。
<a href="#">show lpts flows, (495 ページ)</a>	LPTS フローに関する情報を表示します。

# show lpts clients

Port Arbitrator のクライアント情報を表示するには、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
lpts	読み取り

### 例

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

```
RP/0/RSP0/CPU0:router# show lpts clients
```

```

o flgs - open flags ; clid - client id
clid      loc      flags  o_flgs
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
MPA(7)    0/RP1/CPU0  0x3   0x0

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 45 : 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	rack/slot/module 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_flgs	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。

次に、**show lpts clients times** コマンドの出力例を示します。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/RSP0/CPU0:router# show lpts clients times

o flgs - open flags ; clid - client id
clid      loc      flags  o_flgs
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
MPA(7)    0/RP1/CPU0  0x3   0x0

```

## 関連コマンド

コマンド	説明
<a href="#">show lpts bindings</a> , (487 ページ)	Port Arbitrator でのバインディング情報を表示します。

コマンド	説明
show lpts flows, (495 ページ)	LPTS フローに関する情報を表示します。

# show lpts flows

Local Packet Transport Services (LPTS) フローに関する情報を表示するには、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
lpts	読み取り

### 例

次に、**show lpts flows** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts flows
```

```

-----
L3-proto      : IPV4 (2)
L4-proto      : ICMP (1)
VRF-ID        : * (000000000)
Local-IP      : any
Remote-IP     : any
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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 46 : 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 これより小さい TTL 値を持つ受信 パケットはドロップされます。
Slice	IFIB スライス



フィールド	説明
Flags	<ul style="list-style-type: none"> <li>• HasFGID : 複数の宛先に配信。</li> <li>• No IFIB entry : IFIB エントリを抑制。</li> <li>• Retrying FGID allocation。</li> <li>• InPre-IFIB : エントリは Pre-IFIB にも存在。</li> <li>• Deliver toone : 複数バインディングの場合、1 つだけに配信。</li> </ul>
Location	配信先の <i>rack/slot/module</i> 。
Element References	<ul style="list-style-type: none"> <li>• location : クライアントの <i>rack/slot/module</i>。</li> <li>• count : その場所にあるクライアントの数。</li> <li>• scope : バインディングスコープ (LR : 論理ルータ、LOCAL : ローカル)。</li> </ul>

次に、**show lpts flows brief** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 47 : **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"> <li>• <i>rack/slot/module</i> 個別の場所。</li> <li>• [0xNNNNN] 複数の場所 (プラットフォーム依存の値)。</li> <li>• (drop) どのアプリケーションにも配信しない。</li> </ul>
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

## 関連コマンド

コマンド	説明
<a href="#">show lpts bindings, (487 ページ)</a>	Port Arbitrator でのバインディング情報を表示します。
<a href="#">show lpts clients, (492 ページ)</a>	Port Arbitrator のクライアント情報を表示します。

## show lpts ifib

Internal Forwarding Information Base (IFIB) 内のエントリを表示するには、EXEC モードで **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"> <li>• <b>bgp4</b> : IPv4 ボーダー ゲートウェイ プロトコル (BGP) スライス</li> <li>• <b>bgp6</b> : IPv6 BGP スライス</li> <li>• <b>isis</b> : Intermediate System-to-Intermediate System (IS-IS) スライス</li> <li>• <b>mcast4</b> : IPv4 マルチキャスト スライス</li> <li>• <b>mcast6</b> : IPv6 マルチキャスト スライス</li> <li>• <b>ospf-mc4</b> : IPv4 Open Shortest Path First (OSPF) マルチキャスト スライス</li> <li>• <b>ospf-mc6</b> : IPv6 OSPF マルチキャスト スライス</li> <li>• <b>ospf4</b> : IPv4 OSPF スライス</li> <li>• <b>ospf6</b> : IPv6 OSPF スライス</li> <li>• <b>raw4</b> : IPv4 raw IP</li> <li>• <b>raw6</b> : IPv6 raw IP</li> <li>• <b>tcp4</b> : IPv4 伝送制御プロトコル (TCP) スライス</li> <li>• <b>tcp6</b> : IPv6 TCP スライス</li> <li>• <b>udp4</b> : IPv4 UDP スライス</li> <li>• <b>udp6</b> : IPv6 UDP スライス</li> </ul>
all	すべての IFIB タイプを表示します。
brief	(任意) IFIB エントリ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。

**location** *node-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** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドは、IFIB スライス内のエントリ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数、合計エントリ数の詳細な統計情報が表示されます。

タスク ID	タスク ID	操作
	lpts	読み取り

**例** 次に、**show lpts ifib** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
-----

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 48 : `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"> <li>• O : Opcode (DELIVER、DROP、REASSEMBLE のいずれか)</li> <li>• S : 統計カウンタ</li> <li>• 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)</li> <li>• R : レート制限 (LO、MED、HIGH のいずれか)</li> <li>• L : リスナー タグ (IPv4_STACK、IPv6_STACK、CLNL_STACK のいずれか)</li> <li>• I : ローカル関係フラグ (0 または 1)</li> <li>• Y : TCP SYN フラグ (0 または 1)</li> </ul>

フィールド	説明
Deliver List	<ul style="list-style-type: none"> <li>• (drop) : パケットをドロップ</li> <li>• rack/slot/module : 単一の宛先に配信</li> <li>• [0xNNNN] : 複数の宛先に配信 (プラットフォーム依存の形式)</li> </ul>

次に、**show lpts ifib brief** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts ifib brief
```

```

Slice      Local, Remote Address.Port          L4      Interface      Dlvr
-----
TCP4       any.7 any                            TCP     any            0/RP1/CPU0
TCP4       any.9 any                            TCP     any            0/RP1/CPU0

```

次に、**show lpts ifib brief statistics** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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

```

## 関連コマンド

コマンド	説明
<a href="#">show lpts ifib slices</a> , (503 ページ)	IFIB スライス情報を表示します。

## show lpts ifib slices

Internal Forwarding Information Base (IFIB) スライス情報を表示するには、EXEC モードで **show lpts ifib slices** コマンドを使用します。

```
show lpts ifib slices [type {bgp4|bgp6|isis|mcast4|mcast6|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"> <li>• <b>bgp4</b> : IPv4 ボーダー ゲートウェイ プロトコル (BGP) スライス</li> <li>• <b>bgp6</b> : IPv6 BGP スライス</li> <li>• <b>isis</b> : Intermediate System-to-Intermediate System (IS-IS) スライス</li> <li>• <b>mcast4</b> : IPv4 マルチキャスト スライス</li> <li>• <b>mcast6</b> : IPv6 マルチキャスト スライス</li> <li>• <b>ospf-mc4</b> : IPv4 Open Shortest Path First (OSPF) マルチキャスト スライス</li> <li>• <b>ospf-mc6</b> : IPv6 OSPF マルチキャスト スライス</li> <li>• <b>ospf4</b> : IPv4 OSPF スライス</li> <li>• <b>ospf6</b> : IPv6 OSPF スライス</li> <li>• <b>raw4</b> : IPv4 raw IP</li> <li>• <b>raw6</b> : IPv6 raw IP</li> <li>• <b>tcp4</b> : IPv4 伝送制御プロトコル (TCP) スライス</li> <li>• <b>tcp6</b> : IPv6 TCP スライス</li> <li>• <b>udp4</b> : IPv4 UDP スライス</li> <li>• <b>udp6</b> : IPv6 UDP スライス</li> </ul>
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 モード

EXEC モードの動作または値はありません。

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
lpts	読み取り

## 例

次に、**show lpts ifib slices** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts ifib slices
```

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

次に、**show lpts ifib slices times** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts ifib slices 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/RP1/CPU0:
total:5 tx 13 upd 1/-/1ms/tx

```

次に、**show lpts ifib slices statistics** コマンドの出力例を示します。

```

RP/0/RSP0/CPU0:router# 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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 49: **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

## 関連コマンド

コマンド	説明
<a href="#">show lpts ifib</a> , (499 ページ)	IFIB 内のエントリを表示します。

## show lpts ifib statistics

Internal Forwarding Information Base (IFIB) 統計情報を表示するには、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
lpts	読み取り

### 例

次に、**show lpts ifib statistics** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts ifib statistics
Flow Manager 0/RP1/CPU0:
Packets in:254
Packets delivered locally without lookups:0
Slice lookups:254
```

## show lpts ifib statistics

```

Post-lookup error drops:
  Failed ipv4_netio_input:1
  Rejects:254
Packets delivered locally:0
Packets delivered remotely:0

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 50 : 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。

## 関連コマンド

コマンド	説明
<a href="#">show lpts ifib</a> , (499 ページ)	IFIB スライス内のエントリを表示します。

## 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、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 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
lpts	読み取り

### 例

次に、**show lpts ifib times** コマンドの出力例を示します。

```
RP/0/RSP0/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
```

## show lpts ifib times

```

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/RP1/CPU0:
  total:5 tx 13 upd 1/-/lms/tx

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 51 : 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	rack/slot/module 形式のノードの場所

## 関連コマンド

コマンド	説明
<a href="#">show lpts ifib</a> , (499 ページ)	IFIB スライス内のエントリに関する詳細な情報を表示します。

## show lpts mpa groups

各グループのマルチキャスト バインディングに関する集計情報を表示するには、EXEC モードで `show lpts mpa groups` コマンドを使用します。

`show lpts mpa groups type interface-path-id`

### 構文の説明

`type` インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。

`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 カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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

デフォルトの動作または値はありません。

EXEC

### コマンド履歴

リリース

変更箇所

リリース 3.7.2

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show lpts mpa groups** コマンドは、指定したインターフェイスについてまとめられた、マルチキャストグループに関する情報を集計するために使用されます。このコマンドは、指定したインターフェイスについてまとめられたグループに関連付けられているフィルタモードとソースリストも表示します。

## タスク ID

タスク ID	操作
lpts	読み取り
network	読み取り

## 例

次に、**show lpts mpa groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts mpa groups gigabitethernet 0/0/0/0
 224.0.0.2 : includes 0, excludes 1, mode EXCLUDE
 <no source filter>
 224.0.0.13 : includes 0, excludes 1, mode EXCLUDE
 <no source filter>
 224.0.0.22 : includes 0, excludes 1, mode EXCLUDE
 <no source filter>
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 52 : **show lpts mpa groups** コマンドのフィールドの説明

フィールド	説明
Includes	そのグループに対して INCLUDE モードフィルタを設定したソケットの数と、ソース固有のフィルタがあるかどうかを表示します。
Excludes	そのグループに対して EXCLUDE モードフィルタを設定したソケットの数と、ソース固有のフィルタがあるかどうかを表示します。



## show lpts pifib

Pre-Internal Forwarding Information Base (Pre-IFIB) エントリを表示するには、EXEC モードで **show lpts pifib** コマンドを使用します。

```
show lpts pifib [entry] [hardware {entry | police}] [type {isis | ipv4 | ipv6}] {frag | ixmp | mcast | tcp | udp | ipsec | raw | all} [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。指定できる値は、 <b>frag</b> 、 <b>ixmp</b> 、 <b>mcast</b> 、 <b>tcp</b> 、 <b>udp</b> 、 <b>ipsec</b> 、および <b>raw</b> です。
ipv6	(任意) IPv6 サブ Pre-IFIB タイプ。指定できる値は、 <b>frag</b> 、 <b>icmp</b> 、 <b>ixmp</b> 、 <b>mcast</b> 、 <b>tcp</b> 、 <b>udp</b> 、 <b>ipsec</b> 、および <b>raw</b> です。
frag	(任意) IPv4 または IPv6 フラグメント。
icmp	(任意) IPv4 または IPv6 IXMP および Internet Group Management Protocol (IGMP)。
ixmp	(任意) IPv4 または IPv6 IXMP (ICMP および Internet Group Management Protocol [IGMP])。
mcast	(任意) IPv4 または IPv6 マルチキャスト。
tcp	(任意) IPv4 または IPv6 トランスミッション コントロール プロトコル (TCP)。
udp	(任意) IPv4 または IPv6 ユーザ データグラム プロトコル (UDP)。
ipsec	(任意) セキュア IP。
raw	(任意) IPv4 または IPv6 raw IP。

all	(任意) すべてのサブ Pre-IFIB。
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** EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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値が表示されます。

## タスク ID

タスク ID	操作
lpts	読み取り

## 例

次に、**show lpts pifib** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
```

次に、**show lpts pifib type** コマンドでキーワード **ipv4** および **tcp** を使用した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# 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/RSP0

/CPU0
Accepts/Drops    : 0/0
Is Stale         : 0
-----
```

次に、**show lpts pifib** コマンドに **entry** および **brief** キーワードを追加した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts pifib entry brief

* - Critical Flow; I - Local Interest;
```

## show lpts pifib

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

次に、**show lpts pifib** コマンドに **entry**、**brief**、および **entry brief statistics** キーワードを追加した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# 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、**show lpts pifib** コマンドで **brief** および **statistics** キーワードを使用した場合に表示される重要なフィールドを示します。

表 53 : **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

フィールド	説明
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 context

Local Packet Transport Services (LPTS) pre-IFIB ハードウェア関連のデータ構造のコンテキストを表示するには、EXEC モードで **show lpts pifib hardware context** コマンドを使用します。

**show lpts pifib hardware context** [**location** {**all**|*node-id*}]

### 構文の説明

<b>location</b> <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

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
lpts	読み取り

## 例

次に、**show lpts pifib hardware context** コマンドに **location** キーワードを指定した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware context location 0/1/0

Node: 0/1/CPU0:
-----
ACL ID for block 0: 3
Batching mode: No batching
TCAM Mgr ready: Yes
Mstats Mgr ready: Yes
Metro Driver ready: Yes
Resource sync: Yes
Sweep invoked: Yes
Initialization phase: Done
Queue for TCAM Batching:
  Size: 0 Head ptr: 0x0
Queue for Entry Processing:
  Size: 0 Head ptr: 0x0
Queue for Resources Releasing:
  Size: 0 Head ptr: 0x0
-----
IPv4 Region:
Block [0]:
  # of TCAM entries: 56 block created: Yes
  first entry in the block: 0x482a055c
Last non mandatory entry: 0x482c1a08
Queue for Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
Queue for Non Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
1st entry to be programmed: 0x0
Max. of entries: 15999
# of entries in shadow list: 54
1st entry in shadow list: 0x482a055c
last entry in shadow list: 0x48303534
-----
IPv6 Region:
Block [0]:
  # of TCAM entries: 20 block created: Yes
  first entry in the block: 0x482c1720
Last non mandatory entry: 0x482c1b00
Queue for Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
Queue for Non Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
1st entry to be programmed: 0x0
Max. of entries: 15999
# of entries in shadow list: 20
1st entry in shadow list: 0x482c1720
last entry in shadow list: 0x482e2344
-----
ISIS Region:
Block [0]:
  # of TCAM entries: 1 block created: Yes
  first entry in the block: 0x482e2cf4
Last non mandatory entry: 0xfd30d088
Queue for Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
Queue for Non Mandatory entries not in TCAM:
  Size: 0 Head ptr: 0x0
1st entry to be programmed: 0x0
Max. of entries: 15999
# of entries in shadow list: 1
1st entry in shadow list: 0x482e2cf4
last entry in shadow list: 0x482e2cf4
# of TCAM Insert: 0
```



```
# of TCAM Delete: 0  
# of TCAM Update: 0  
# of resource leaks: 0
```

## show lpts pifib hardware entry

Local Packet Transport Services (LPTS) pre-IFIB ハードウェア テーブルのエントリを表示するには、EXEC モードで **show lpts pifib hardware entry** コマンドを使用します。

**show lpts pifib hardware entry** [*type* {*ipv4*|*ipv6*|*isis*}] [*start-index number num-entries number*] [*brief* | *statistics*] [*location* {*all*|*node\_id*}]

### 構文の説明

<i>type</i>	(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"> <li>• <b>ipv4</b> : IPv4 エントリを指定します。</li> <li>• <b>ipv6</b> : IPv6 エントリを指定します。</li> <li>• <b>isis</b> : ISIS エントリを指定します。</li> </ul>
<i>start-index number</i>	(任意) 開始インデックス番号。
<i>num-entries number</i>	(任意) 最大許可エントリ。
<i>brief</i>	(任意) ハードウェア エントリの要約情報を表示します。
<i>statistics</i>	(任意) 各要約エントリの、ハードウェア エントリの許可またはドロップ統計情報を表示します。
<i>location all</i>	(任意) すべての場所を指定します。
<i>location 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。

**コマンド デフォルト**      ハードウェア エントリ情報の概要を表示します。

**コマンド モード**      EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID	タスク ID	操作
	lpts	読み取り

**例** 次に、**show lpts pifib hardware entry** コマンドに **location** キーワードを指定した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware entry location 0/1/CPU0
```

```
Node: 0/0/CPU0:
```

```
-----
M - Fabric Multicast;
L - Listener Tag; T - Min TTL;
F - Flow Type;
DestNode - Destination Node;
DestAddr - Destination Fabric queue;
SID - Stream ID;
Po - Policer; Ct - Stats Counter;
Lp - Lookup priority; Sp - Storage Priority;
Ar - Average rate limit; Bu - Burst;
HAr - Hardware Average rate limit; HBU - Hardware Burst;
Cir - Committed Information rate in HAL
Rsp - Relative sorting position;
Rtp - Relative TCAM position;
na - Not Applicable or Not Available
-----
```

```
VRF ID          : any
Destination IP   : any
Source IP        : any
Is Fragment      : 0
Interface        : any
M/L/T/F         : 0/ISIS_FM/0/ISIS-default
DestNode        : 48
DestAddr        : 48
SID             : 9
L4 Protocol      : -
Source port      : any
Destination Port : any
Ct               : 0xd84da
Accepted/Dropped : 0/0
Lp/Sp           : 0/0
# of TCAM entries : 1
HPo/HAr/HBU/Cir : 1879638/2000pps/2000ms/2000pps
State           : Entry in TCAM
Rsp/Rtp         : 0/2
```

```
Node: 0/1/CPU0:
```

```
-----
V - Vital; M - Fabric Multicast;
C - Moose Congestion Flag; L - Listener Tag; T - Min TTL;
F - Flow Type;
```

## show lpts pifib hardware entry

```

DestNode - Destination Node;
DestAddr - Destination Fabric Address;
Sq - Ingress Shaping Queue; Dq - Destination Queue;
Po - Policer; Ct - Stats Counter;
Lp - Lookup priority; Sp - Storage Priority;
Ar - Average rate limit; Bu - Burst;
Rsp - Relative sorting position;
-----

```

```

L4 Protocol      : any
VRF ID          : any
Source IP       : any
Port/Type       : any
Source Port     : any
Is Fragment     : 1
Is SYN         : any
Interface       : any
V/M/C/L/T/F    : 0/0/0/IPv4_REASS/0/Fragment
DestNode       : Local
DestAddr       : Punt
Sq/Dq/Ct       : 4/na/0x24400
Accepted/Dropped : 0/0
Lp/Sp          : 0/0
# of TCAM entries : 1
Po/Ar/Bu       : 101/1000pps/100ms
State          : Entry in TCAM
Rsp/Rtp        : 0/0
-----

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 54 : show lpts pifib hardware entry コマンドのフィールドの説明

フィールド	説明
L4 Protocol	エントリのレイヤ 4 プロトコル
VRF ID	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
Source IP	このエントリのソース IP アドレス
Port/Type	このエントリのポートまたはインターネット制御メッセージプロトコル (ICMP) タイプ
Source Port	このエントリのソース ポート
Is Fragment	このエントリが IP フラグメントに適用されるかどうか
Is SYN	このエントリが TCP SYN に適用されるかどうか
Interface	このエントリのインターフェイス

フィールド	説明
V/M/C/L/T/F	<ul style="list-style-type: none"><li>• V : vital</li><li>• M : ファブリック マルチキャスト</li><li>• C : Moose 輻輳フラグ</li><li>• L : リスナー フラグ</li><li>• T : 最小存続可能時間</li><li>• F : フロー タイプ</li></ul>
DestNode	パケットを送信する宛先ノード
DestAddr	パケットを送信する宛先アドレス
Sq/Dq/Ct	<ul style="list-style-type: none"><li>• Sq : 入力シェーピング キュー</li><li>• Dq : 宛先キュー</li><li>• Ct : 統計カウンタ</li></ul>
Accepted/Dropped	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

## show lpts pifib hardware police

ポリサー設定値セットを表示するには、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

<b>location</b> <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。
<b>all</b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
lpts	読み取り

例

次に、**show lpts pifib hardware police** コマンドに **location** キーワードと **0/2/CPU0** を指定した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router#show lpts pifib hardware police location 0/2/CPU0
```

```
-----
Node 0/2/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

## show lpts pifib hardware police

```

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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 55 : 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
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

## 関連コマンド

コマンド	説明
<a href="#">flow (LPTS)</a> , (478 ページ)	LPTS フロー タイプのポリサーを設定します。
<a href="#">lpts pifib hardware police</a> , (485 ページ)	入力ポリサーを設定し、 <code>pifib policer</code> グローバル コンフィギュレーションモードに移行します。





## 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、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

<b>type</b>	(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"> <li>• <b>ipv4</b> : IPv4 エントリを指定します。</li> <li>• <b>ipv6</b> : IPv6 エントリを指定します。</li> <li>• <b>isis</b> : ISIS エントリを指定します。</li> </ul>
<b>location</b> <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。
<b>all</b>	(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要約を表示します。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
lpts	読み取り

## 例

次に、**show lpts pifib hardware usage** コマンドに **location** キーワードを指定した場合の出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts pifib hardware usage location 0/1/cpu0
```

Type	Size	Used	Used(%)
ipv4	6000	21	0.35
ipv6	4000	15	0.38
isis	4000	1	0.03

次の表に、この出力で表示される重要なフィールドについて説明します。

表 56 : **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、EXEC モードで **show lpts pifib 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
lpts	読み取り

### 例

次に、**show lpts pifib statistics** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts pifib statistics
Packets into Pre-IFIB:80
Lookups:80
Packets delivered locally:80
Packets delivered remotely:0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 57 : *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

#### 関連コマンド

コマンド	説明
<a href="#">show lpts pifib</a> , (513 ページ)	pre-IFIB エントリに関する情報を表示します。

## show lpts port-arbitrator statistics

Local Packet Transport Services (LPTS) Port Arbitrator 統計情報を表示するには、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、キーワードと引数はありません。

#### 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

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
lpts	読み取り

#### 例

次に、**show lpts port-arbitrator statistics** コマンドの出力例を示します。

```
RP/0/RSP0/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 vrf

Local Packet Transport Services (LPTS) VPN ルーティング/転送 (VRF) インスタンスの識別番号と名前を表示するには、EXEC モードで **show lpts vrf** コマンドを使用します。

### show lpts vrf

#### 構文の説明

このコマンドには、キーワードと引数はありません。

#### 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

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
lpts	読み取り

#### 例

次に、**show lpts vrf** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show lpts vrf
```

```
VRF-ID      VRF-NAME
0x00000000  *
0x60000000  default
```

次の表に、この出力で表示される重要なフィールドについて説明します。



表 58 : show lpts vrf 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。
VRF-NAME	VRF に指定される名前

```
show lpts vrf
```



# 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 Version 4 (IPv4) および IP Version 6 (IPv6) に関連する機能を設定および監視するために、Cisco ASR 9000 シリーズ アグリゲーションサービスルータの Cisco IOS XR ソフトウェアで利用できる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、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』の「*Implementing Network Stack IPv4 and IPv6 on Cisco ASR 9000 Series Routers*」設定モジュールを参照してください。

- [clear ipv6 neighbors](#) , 542 ページ
- [icmp ipv4 rate-limit unreachable](#), 544 ページ
- [ipv4 address \(ネットワーク\)](#) , 546 ページ
- [ipv4 assembler max-packets](#), 549 ページ
- [ipv4 assembler timeout](#), 551 ページ
- [ipv4 conflict-policy](#), 553 ページ
- [ipv4 directed-broadcast](#), 555 ページ
- [ipv4 helper-address](#), 557 ページ
- [ipv4 mask-reply](#), 559 ページ
- [ipv4 mtu](#), 561 ページ
- [ipv4 redirects](#), 563 ページ
- [ipv4 source-route](#), 565 ページ
- [ipv4 unnumbered \(point-to-point\)](#) , 567 ページ
- [ipv4 unreachable disable](#), 570 ページ
- [ipv4 virtual address](#), 572 ページ
- [ipv6 address](#), 574 ページ

- [ipv6 address link-local, 576 ページ](#)
- [ipv6 assembler, 578 ページ](#)
- [ipv6 conflict-policy, 580 ページ](#)
- [ipv6 enable, 582 ページ](#)
- [ipv6 hop-limit, 584 ページ](#)
- [ipv6 icmp error-interval, 586 ページ](#)
- [ipv6 mtu, 588 ページ](#)
- [ipv6 nd dad attempts, 590 ページ](#)
- [ipv6 nd managed-config-flag, 593 ページ](#)
- [ipv6 nd ns-interval, 595 ページ](#)
- [ipv6 nd other-config-flag, 597 ページ](#)
- [ipv6 nd prefix, 599 ページ](#)
- [ipv6 nd ra-interval, 602 ページ](#)
- [ipv6 nd ra-lifetime, 604 ページ](#)
- [ipv6 nd reachable-time, 606 ページ](#)
- [ipv6 nd redirects, 608 ページ](#)
- [ipv6 nd scavenge-timeout, 610 ページ](#)
- [ipv6 nd suppress-ra, 612 ページ](#)
- [ipv6 neighbor, 614 ページ](#)
- [ipv6 source-route, 617 ページ](#)
- [ipv6 unreachable disable, 619 ページ](#)
- [local pool, 621 ページ](#)
- [show arm conflicts, 625 ページ](#)
- [show arm database, 628 ページ](#)
- [show arm router-ids, 631 ページ](#)
- [show arm registrations producers, 633 ページ](#)
- [show arm summary, 635 ページ](#)
- [show arm vrf-summary, 637 ページ](#)
- [show clns statistics, 639 ページ](#)
- [show ipv4 interface, 641 ページ](#)
- [show local pool, 645 ページ](#)

- [show ipv4 traffic, 647 ページ](#)
- [show ipv6 interface, 650 ページ](#)
- [show ipv6 neighbors, 654 ページ](#)
- [show ipv6 neighbors summary, 660 ページ](#)
- [show ipv6 traffic, 662 ページ](#)
- [show mpa client, 665 ページ](#)
- [show mpa groups, 667 ページ](#)
- [show mpa ipv4, 669 ページ](#)
- [show mpa ipv6, 671 ページ](#)
- [show vrf, 673 ページ](#)
- [vrf, 676 ページ](#)
- [vrf \(address-family\) , 678 ページ](#)
- [vrf \(description\) , 680 ページ](#)
- [vrf \(mhost\) , 682 ページ](#)
- [vrf mode, 684 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、EXEC モードで **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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

*location* オプションが指定されている場合、**location node-id** キーワードおよび引数で指定されている隣接エントリだけがクリアされます。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear ipv6 neighbors ?
location specify a node name

RP/0/RSP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH gigabitethernet
0/0/0/0
8888::8 - 1234.2345.9877 REACH gigabitethernet0
/0/0/0
fe80::205:1ff:fe9f:6400 1335 0005.019f.6400 STALE gigabitethernet
0/0/0/0
fe80::206:d6ff:fece:3808 1482 0006.d6ce.3808 STALE gigabitethernet
0/0/0/0
fe80::200:11ff:fe11:1112 1533 0000.1111.1112 STALE gigabitethernet
0/2/0/2

RP/0/RSP0/CPU0:router# clear ipv6 neighbors location 0/2/0
RP/0/RSP0/CPU0:router# show ipv6 neighbor

IPv6 Address Age Link-layer Addr State Interface
8888::3 - 1234.2345.9877 REACH gigabitethernet
0/0/0/0
8888::8 - 1234.2345.9877 REACH gigabitethernet
0/0/0/0
fe80::205:1ff:fe9f:6400 1387 0005.019f.6400 STALE gigabitethernet
0/0/0/0
fe80::206:d6ff:fece:3808 1534 0006.d6ce.3808 STALE gigabitethernet
0/0/0/0
```

## 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、グローバル コンフィギュレーション モードで **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

<b>DF</b>	(任意) コード 4 フラグメンテーションが必要で、Data Fragmentation (DF; データフラグメンテーション) 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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 つのタイマーを保守します。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 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無関係のままになります。



## タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、ICMP宛先到達不能メッセージが10ミリ秒に1件送信されるように設定する例を示します。

```
RP/0/RSP0/CPU0:router(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

<b>ipv4-address</b>	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"> <li>ネットワーク マスクには、4 分割ドット付き 10 進表記アドレスを使用できます。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。</li> <li>スラッシュ (/) と数字による表記。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。</li> </ul>
<b>secondary</b>	(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。
<b>route-tag</b>	(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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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クングデバイスは、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。ネットワークング 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、**no ipv4 address** コマンドを使用して 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 Address Resolution Protocol (ARP; アドレス解決プロトコル) 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、ネットワークング 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	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 でプライマリ アドレスを 192.168.1.27、セカンダリ アドレスを 192.168.7.17 および 192.168.8.17 に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.7.17 255.255.255.0 secondary
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.8.17 255.255.255.0 secondary
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv4 interface</a> , (641 ページ)	インターフェイスの IPv4 情報およびステータスのサマリー情報をリストします。

## ipv4 assembler max-packets

アセンブリ キューで許可されているパケットの最大数を設定するには、グローバルコンフィギュレーション モードで **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

<i>percentage value</i>	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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
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 packets 最大数を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 assembler max-packets 35
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 assembler timeout</a> , <a href="#">(551 ページ)</a>	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を設定します。

## ipv4 assembler timeout

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を設定するには、グローバル コンフィギュレーション モードで **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。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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 assembler timeout 88
```

---

**関連コマンド**

コマンド	説明
<a href="#">ipv4 assembler max-packets</a> , ( <a href="#">549 ページ</a> )	アセンブリ キューで許可されているパケットの最大数を設定します。



## ipv4 conflict-policy

IP Address Repository Manager (IPARM) 競合解決をイネーブルにするには、グローバル コンフィギュレーション モードで **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

<b>highest-ip</b>	競合セットの最も高い IP アドレスを保持します。
<b>longest-prefix</b>	競合セットの最長プレフィックス マッチを保持します。
<b>static</b>	新しいアドレス設定で稼動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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv4 conflict-policy** コマンドを使用して、設定されているアドレスで競合を解決する IPARM ポリシーを設定します。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	操作
ipv4	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/RSP0/CPU0:router(config)# ipv6 conflict-policy static
```

## 関連コマンド

コマンド	説明
<a href="#">show arm conflicts</a> , <a href="#">(625 ページ)</a>	IPv4 または IPv6 アドレス競合情報を表示します。

## ipv4 directed-broadcast

インターフェイスのIPv4ダイレクトブロードキャストの転送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 **ipv4 directed-broadcast** コマンドを使用します。インターフェイスのIPv4ダイレクトブロードキャストの転送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 directed-broadcast**

**no ipv4 directed-broadcast**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

デフォルトでは、ダイレクトブロードキャストはドロップされます。

### 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ダイレクトブロードキャストは、特定のネットワークに送信されるパケットです。IPv4ダイレクトブロードキャストは、ドロップされ、転送されません。IPv4ダイレクトブロードキャストをドロップすることで、ルータは、Denial-Of-Service (DoS; サービス拒絶) 攻撃の影響を受けづらくなります。

### タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 で IPv4 ダイレクトブロードキャストの転送をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 directed-broadcast
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 unnumbered (point-to-point)</a> , (567 ページ)	明示的な IP アドレスをインターフェイスに割り当てることなく、ポイントツーポイントインターフェイスの IP 処理をイネーブルにします。
<a href="#">show ipv4 interface</a> , (641 ページ)	インターフェイスの IPv4 情報およびステータスのサマリー情報をリストします。

## ipv4 helper-address

BOOTPなど、ソフトウェアがインターフェイスで受信したユーザデータグラムプロトコル (UDP) ブロードキャストを転送する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 helper-address** コマンドを使用します。IPv4 ヘルパー 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 helper-address [vrf vrf-name]] [ destination-address ]}
```

```
{no ipv4 helper-address [vrf vrf-name]] [ destination-address ]}
```

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<i>vrf-name</i>	(任意) VRF の名前。
<i>destination-address</i>	UDP ブロードキャストが転送されるときに使用される宛先ブロードキャストまたはホストアドレス。インターフェイスごとに複数のヘルパー アドレスを使用できます。

### コマンド デフォルト

IPv4 ヘルパー アドレスはディセーブルです。VRF が指定されていない場合、デフォルトの VRF が使用されます。

### 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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドは、グローバル コンフィギュレーション モードで **forward-protocol udp** コマンドと使用します。これにより、転送されるブロードキャスト パケットをポート番号で指定できます。デフォルトでは、UDP は well-known ポートでイネーブルです。 **ipv4 helper-address** コマンドは、UDP パケットが転送される宛先を指定します。

IPv4 ヘルパー アドレスを必要とする 1 つのコモン アプリケーションは、RFC 1531 で定義されている Dynamic Host Configuration Protocol (DHCP) です。DHCP プロトコル情報は、BOOTP パケットの内部で転送されます。クライアントセットで BOOTP ブロードキャスト転送をイネーブルにするには、クライアントに物理的に最も近いネットワークングデバイス インターフェイスで IPv4 ヘルパー アドレスを設定します。IPv4 ヘルパー アドレスは、DHCP サーバのアドレスを指定しなければなりません。サーバが複数ある場合、各サーバに 1 つの IPv4 ヘルパー アドレスを設定できます。BOOTP パケットはデフォルトで転送されるため、DHCP 情報は、ネットワークングデバイスにより転送できます。DHCP サーバは、DHCP クライアントからブロードキャストを受信します。

DHCP リレー プロファイルは、DHCP リレーを実行するように設定する必要があります。 **ip helper-address** コマンドは、UDP ブロードキャスト (非 DHCP) パケットを転送する目的で使用されます。

---

**タスク ID**

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

---

**例**

次に、GigabitEthernet インターフェイス 0/1/1/0 で受信されるすべての UDP ブロードキャスト パケットが 192.168.1.0 に転送されるよう指定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 helper-address 192.168.1.0
```

---

**関連コマンド**

コマンド	説明
forward-protocol udp	ブロードキャスト パケットの転送時にネットワークングデバイスが転送するポートを指定します。

## 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 **ipv4 mask-reply** 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。

**ipv4 mask-reply**

**no ipv4 mask-reply**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

---

**例**

次に、GigabitEthernet インターフェイス 0/1/1/0 で ICMP マスク応答メッセージの送信をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0  
RP/0/RSP0/CPU0:router(config-if)# ipv4 mask-reply
```



## 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単位 (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 **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  
動的なテンプレート コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG の動的なテンプレートコンフィギュレーションモードでサポートされていました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータは、インターフェイスに設定されている MTU サイズを超えているすべての IPv4 パケットをフラグメントします。

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。

動的なテンプレート コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dynamic-template** コマンドを実行します。



- (注) MTU 値を変更すると (**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)、IPv4 MTU 値に影響を与えます。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、この逆の作用はなく、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	操作
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

次に、GigabitEthernet インターフェイス 0/1/1/0 の最大 IPv4 パケット サイズを 300 バイトに設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitEthernet0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 mtu 300
```

次に、動的なテンプレート コンフィギュレーション モードで IPv4 パケットの最大サイズを 300 バイトに設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 mtu 300
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv4 interface</a> , (641 ページ)	IPv4 に設定されているインターフェイスの MTU ステータスを表示します。

## ipv4 redirects

ソフトウェアが受信時と同じインターフェイスを介してパケットを強制的に再送する場合に IPv4 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の送信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 **ipv4 redirects** 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。

**ipv4 redirects**

**no ipv4 redirects**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

デフォルトでは、ICMP リダイレクトメッセージは、インターフェイスでディセーブルです。

### 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

デフォルトでは、ICMP リダイレクトメッセージは、インターフェイスでディセーブルです。

### タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 で ICMP IPv4 リダイレクト メッセージの送信をディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 redirects
```

## ipv4 source-route

source-route ヘッダー オプションを含む任意の IPv4 データグラムの処理を可能にするには、グローバル コンフィギュレーション モードで **ipv4 source-route** コマンドを使用します。source-route オプションを含むすべての IP データグラムを廃棄するようにソフトウェアを設定するには、このコマンドの **no** 形式を使用します。

**ipv4 source-route**

**no ipv4 source-route**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

ソフトウェアは、source-route ヘッダー オプションを含むすべての IPv4 データグラムを廃棄します。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

デフォルトでは、source-route ヘッダー オプションを含むすべての IPv4 データグラムが廃棄されます。

### タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
network	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 IPv4 データグラムの処理を可能にする例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 source-route
```

## 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、適切なコンフィギュレーションモードで **ipv4 unnumbered** 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 カード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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。

ルータ構文の詳細については、疑問符 (?) オンライン ヘルプ機能を使用します。

### 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

## 動的なテンプレート 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 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドは、BNGの動的なテンプレート コンフィギュレーション モードでサポートされていました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

動的なテンプレート コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **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。

- インターフェイスがアドレスを持たないため、インターフェイスがアップ状態かどうかを判断するために **ping EXEC** コマンドは使用できません。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は、イネーブルにされている必要があります (**show interfaces** コマンド出力に「up」と表示)。

## タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
ネットワーク	読み取り、書き込み
config-services	読み取り、書き込み

## 例

次の例では、GigabitEthernet インターフェイス 0/1/1/0 に、ループバック インターフェイス アドレス 5 が割り当てられます。

```
RP/0/RSP0/CPU0:router(config)# interface loopback 5
```



```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.6.6 255.255.255.0  
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0  
RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback 5
```

次の例では、Bundle-Ether インターフェイスに動的なテンプレート コンフィギュレーション モードのアドレス 100.10 が割り当てられます。

```
RP/0/RSP0/CPU0:router# configure  
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp p1  
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 unnumbered Bundle-Ether100.10
```

## ipv4 unreachable disable

IPv4 インターネット制御メッセージプロトコル (ICMP) 到達不能メッセージの生成をディセーブルにするには、適切なコンフィギュレーション モードで **ipv4 unreachable disable** コマンドを使用します。ICMP 到達不能メッセージの生成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。

**ipv4 unreachable disable**

**no ipv4 unreachable disable**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

IPv4 ICMP 到達不能メッセージが生成されます。

### コマンド モード

インターフェイス コンフィギュレーション  
動的なテンプレート コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.2.0	このコマンドは、BNG の動的なテンプレート コンフィギュレーション モードでサポートされていました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ソフトウェアが、それ自体を宛先とした、認識しないプロトコルを使用する非ブロードキャスト パケットを受信した場合、その送信元に ICMP プロトコル到達不能メッセージを送信します。

宛先アドレスまでのルートが不明なため最終的な宛先に配信できないデータグラムを受信した場合、ソフトウェアはそのデータグラムの発信者に ICMP ホスト到達不能メッセージで応答します。

このコマンドは、多くの ICMP 到達不能メッセージに影響を与えます。

動的なテンプレート コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dynamic-template** コマンドを実行します。

## タスク ID

タスク ID	操作
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

次に、GigabitEthernet インターフェイス 0/1/1/0 で ICMP 到達不能メッセージの生成をディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 unreachable disable
```

次に、動的なテンプレート コンフィギュレーションモードで ICMP 到達不能メッセージの生成をディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# dynamic-template type ppp foo
RP/0/RSP0/CPU0:router(config-dynamic-template-type)# ipv4 unreachable disable
```

## ipv4 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のIPv4仮想アドレスを定義するには、グローバルコンフィギュレーションモードで **ipv4 virtual interface** コマンドを使用します。設定からIPv4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。

**ipv4 virtual address** {[vrf vrf-name] ipv4-address/mask} **use-as-src-addr**}

**no ipv4 virtual address** {[vrf vrf-name] ipv4-address/mask} **use-as-src-addr**}

### 構文の説明

<b>vrf vrf-name</b>	(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) に基づいた仮想アドレスを設定します。 <i>vrf-name</i> 引数は、VRF の名前を指定します。
<b>ipv4 address</b>	設定されない仮想 IPv4 アドレスおよびマスク。
<b>mask</b>	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。 <ul style="list-style-type: none"> <li>• 4分割ドット付き 10進表記。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。</li> <li>• スラッシュ (/) と数字による表記。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。値の間のスラッシュ記号は表記の一部として必要です。</li> </ul>
<b>use-as-src-addr</b>	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

IPv4 仮想アドレスは設定に定義されません。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

IPv4 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。IPv4 仮想アドレスは、ルート プロセッサ (RP) フェールオーバー状況間で維持されます。

IPv4 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。IPv4 仮想アドレスは、RP フェールオーバー間で維持されます。このようにするには、仮想 IPv4 アドレスが、両方の RP の管理イーサネット インターフェイスで共通 IPv4 サブネットを共有する必要があります。

**vrf** キーワードで **ipv4 virtual address** コマンドをディセーブルにした場合、仮想 IP アドレスは、対応する VRF または VRF が指定されていない場合はデフォルト VRF で未設定になります。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** キーワードによって、管理アプリケーション用の送信元インターフェイス（つまり、更新送信元）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動作します。

**タスク ID**

タスク ID	操作
ipv4	読み取り、書き込み
network	読み取り、書き込み

**例**

次に、IPv4 仮想アドレスを定義する例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 virtual address 10.3.32.154/8
```

次に、VRF に基づいて管理インターフェイスの仮想 IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv4 virtual address vrf ppp 10.26.3.4/16
```

## ipv6 address

インターフェイスに IPv6 アドレスを設定し、アドレスの下位 64 ビットで EUI-64 インターフェイス ID を使用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 に記載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。
<b>eui-64</b>	(任意) IPv6 アドレスの下位 64 ビットのインターフェイス ID を指定します。
<b>route-tag</b>	(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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

*/prefix-length* 引数に指定される値が、64 ビットを超える場合、プレフィックスビットは、インターフェイス ID より優先されます。

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。

**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	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次に、IPv6 アドレス 2001:0DB8:0:1::/64 を GigabitEthernet インターフェイス 0/1/1/0 に割り当て、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を指定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

関連コマンド

コマンド	説明
<a href="#">ipv6 address link-local</a> , (576 ページ)	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 address link-local

インターフェイスの IPv6 リンクローカルアドレスを設定し、その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される *ipv6-address* 値は、インターフェイスに自動的に生成されるリンクローカルアドレスより優先されます。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 に記載されている形式にする必要があります。コロンの区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
<b>link-local</b>	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される <i>ipv6-address</i> 値は、インターフェイスに自動的に生成されるリンクローカルアドレスより優先されます。
<b>route-tag</b>	(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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。



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。

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	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、FE80::260:3EFF:FE11:6770 を GigabitEthernet インターフェイス 0/1/1/0 のリンクローカルアドレスとして割り当てる例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 address</a> , (574 ページ)	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 assembler

アセンブリ キューで許可されているパケットの最大数を設定するか、またはタイムアウトまでにアセンブリ キューが保持する秒数を設定するには、グローバル コンフィギュレーション モードで **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-packets value* | *timeout seconds*}

**no ipv6 assembler** {*max-packets value* | *timeout seconds*}

### 構文の説明

<b>max-packets</b>	アセンブリ キューで許可されるパケットの最大数。
<b>timeout</b>	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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ipv6 assembler max-packets 100
```

#### 関連コマンド

コマンド	説明
<a href="#">ipv4 assembler max-packets, (549 ページ)</a>	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ます。
<a href="#">ipv4 assembler max-packets, (549 ページ)</a>	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ます。

## ipv6 conflict-policy

IP Address Repository Manager (IPARM) 競合解決をイネーブルにするには、グローバル コンフィギュレーション モードで **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

<b>highest-ip</b>	競合セットの最も高い IP アドレスを保持します。
<b>longest-prefix</b>	競合セットの最長プレフィックス マッチを保持します。
<b>static</b>	新しいアドレス設定で稼動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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv6 conflict-policy longest-prefix
```

# 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上で 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 アドレスでまだ設定されていないインターフェイスで 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、キーワードと引数はありません。

## 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

## コマンド履歴

リリース

変更箇所

リリース 3.7.2

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 enable** コマンドは、インターフェイスの 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、その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。

## タスク ID

タスク ID

操作

ipv6

読み取り、書き込み

network

読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 での IPv6 処理をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 enable
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 address, (574 ページ)</a>	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">ipv6 address link-local, (576 ページ)</a>	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 hop-limit

ルータにより発信されるルータ アドバタイズメントおよびすべての IPv6 パケットで使用されるホップの最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6 hop-limit** コマンドを使用します。ホップ制限をその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。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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv6 hop-limit 15
```

## ipv6 icmp error-interval

すべてのノードの 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およびパケットサイズを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp error-interval** コマンドを使用します。間隔をその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

<i>milliseconds</i>	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。
<i>bucketsize</i>	(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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 icmp error-interval** コマンドをグローバル コンフィギュレーション モードで使用すると、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

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たびにバケットから削除されます。つまり、*bucketsize* 引数が 20 に設定されている場合、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	操作
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/RSP0/CPU0:router(config)# ipv6 icmp error-interval 50 20
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 neighbors</a> , (654 ページ)	IPv6 近隣探索キャッシュ情報を表示します。

## 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単位 (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

<i>bytes</i>	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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。



(注) MTU 値を変更すると (**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)、IPv6 MTU 値に影響を与えます。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、この逆の作用はなく、IPv6 MTU 値と変更しても、**mtu** コマンドの値には影響しません。

タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

例

次に、GigabitEthernet インターフェイス 0/1/1/0 の最大 IPv6 パケット サイズを 1350 バイトに設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 mtu 1350
```

関連コマンド

コマンド	説明
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd dad attempts

インターフェイスのユニキャスト 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、その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 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

<i>value</i>	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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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`（RFC 2461『*Neighbor Discovery for IP Version 6 [IPv6]*』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時、または隣接の到達可能性がプローブされる時に、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。



(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 gigabitethernet0
```

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	操作
ipv6	読み取り

## 例

次に、インターフェイス 0/2/0/1 で送信されるネイバー送信要求メッセージの連続数を 1 に設定し、インターフェイスで設定されているユニキャスト IPv6 アドレスの状態 (tentative または duplicate) を表示する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/1
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd dad attempts 1
RP/0/RSP0/CPU0:router(config-if)# Uncommitted changes found, commit them before
exiting(yes/no/cancel)? [cancel]:y

RP/0/RSP0/CPU0:router# show ipv6 interface
gigabitethernet0
/2/0/0 is Up, line protocol is Up
  IPv6 is disabled, link-local address unassigned
  No global unicast address is configured
gigabitethernet0
/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.
gigabitethernet0
/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.
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 nd ns-interval</a> , (595 ページ)	インターフェイスでIPv6 ネイバー送信要求メッセージが送信される時間間隔を設定します。
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。



## ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメントの managed address configuration フラグを設定するには、インターフェイス コンフィギュレーション モードで **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、キーワードと引数はありません。

### 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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み

タスク ID	操作
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 で IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd managed-config-flag
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd ns-interval

インターフェイスでの IPv6 ネイバー送信要求メッセージの再送信間隔を設定するには、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 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

*milliseconds* IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒）。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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 の IPv6 ネイバー送信要求メッセージの送信間隔を 9000 ミリ秒に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ns-interval 9000
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメントの **other stateful configuration** フラグを設定するには、インターフェイス コンフィギュレーションモードで **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、キーワードと引数はありません。

### 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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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** コマンドを使用するときに、**managed address configuration** フラグが設定された場合、接続ホストは、**other stateful configuration** フラグの設定に関係なく、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。

## タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 で IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd other-config-flag
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 nd managed-config-flag, (593 ページ)</a>	IPv6 ルータ アドバタイズメントに、managed address configuration フラグを設定します。
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd prefix

IPv6 プレフィックスが IPv6 ルータ アドバタイズメントでどのようにアドバタイズされるかを設定するには、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。プレフィックス (1つ以上) 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

<b>ipv6-prefix</b>	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、コロンの間で 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。
<b>/prefix-length</b>	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。
<b>default</b>	(任意) すべてのプレフィックスを指定します。
<b>valid-lifetime</b>	(任意) 指定された 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 (秒)。値の範囲は 0 ~ 4294967295 秒です。
<b>at</b>	(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> 形式で表現されます。
<b>infinite</b>	(任意) 有効なライフタイムが期限切れになりません。
<b>no-adv</b>	(任意) プレフィックスはアドバタイズされません。
<b>no-autoconfig</b>	(任意) ローカルリンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用できないことを示します。
<b>off-link</b>	(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せん。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****変更箇所**

リリース 3.7.2

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。

プレフィックスがアドバタイズされる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で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、指定したプレフィックスだけが、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を使用できます。

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	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、有効期間 1000 秒、推奨期間 900 秒で、GigabitEthernet 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 を含める例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 address, (574 ページ)</a>	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">ipv6 address link-local, (576 ページ)</a>	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
<a href="#">ipv6 nd managed-config-flag, (593 ページ)</a>	IPv6 ルータ アドバタイズメントに、managed address configuration フラグを設定します。
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## 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 転送の間隔を設定するには、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 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**

### 構文の説明

*seconds* 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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 nd ra-lifetime** コマンドを使用して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 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。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 での IPv6 ルータ アドバタイズメント間隔を 201 秒に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ra-interval 201
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 nd ra-lifetime, (604 ページ)</a>	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd ra-lifetime

インターフェイスの IPv6 ルータ アドバタイズメントの ルータ 有効期間の値を設定するには、インターフェイス コンフィギュレーション モードで **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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み

タスク ID	操作
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 での IPv6 ルータ アドバタイズメント有効期間を 1801 秒に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd ra-lifetime 1801
```

## 関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	インターフェイスで IPv6 ルータ アドバタイズメントメッセージが送信される時間間隔を設定します。
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd reachable-time

いくつかの到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能と見なされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

### 構文の説明

<i>milliseconds</i>	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

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。

## タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 の IPv6 到達可能時間を 1,700,000 ミリ秒に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd reachable-time 1700000
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## 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、キーワードと引数はありません。

### コマンド デフォルト

デフォルト値は、disabled 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	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 3.9.0	変更なし。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み



## 例

次に、GigabitEthernet インターフェイス 0/2/0/2 で IPv6 nd ダイレクトブロードキャストをリダイレクトする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd redirects
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## ipv6 nd scavenge-timeout

stale 状態の隣接エントリの有効期間を設定するには、グローバルコンフィギュレーションモードで **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

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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	操作
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/RSP0/CPU0:router(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送信をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスで 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、キーワードと引数はありません。

### 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、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

### コマンド履歴

リリース

変更箇所

リリース 3.7.2

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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（たとえば、シリアルまたはトンネル インターフェイス）での IPv6 ルータ アドバタイズメント送信をイネーブルにできます。

### タスク ID

タスク ID

操作

ipv6

読み取り、書き込み

network

読み取り、書き込み

## 例

次に、GigabitEthernet インターフェイス 0/1/1/0 での IPv6 ルータ アドバタイズメントをディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# ipv6 nd suppress-ra
```

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface</a> , (650 ページ)	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## 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、グローバルコンフィギュレーションモードで **ipv6 neighbor** コマンドを使用します。IPv6 近隣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 に記載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>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルート プロセッサ カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0/CPU0/0。</li> <li>• 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。</li> </ul> <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 モデル

このコマンドは、グローバルコンフィギュレーションモードで実行され、IPv6 ネイバー探索キャッシュに設定されません。

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**ipv6 neighbor** コマンドは、**arp** (グローバル) コマンドに似ています。

指定された IPv6 アドレスのエントリが (IPv6 ネイバー探索プロセスを通して学習された) ネイバー探索キャッシュ内にすでに存在する場合、その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す。

**show ipv6 neighbors** コマンドを使用すると、IPv6 近隣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状態の場合、**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)** 状態については、**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 エントリを除く、IPv6 近隣探索キャッシュ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。このコマンドは、IPv6 ネイバー探索プロセスから取得されたダイナミック エントリをキャッシュから削除しません。**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 エントリを除く、そのインターフェイスで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 (エントリの状態は **reach [reachable]** に変わります)。

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	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、イーサネット インターフェイス 0/RSP0/CPU0 の IPv6 アドレス 2001:0DB8::45A およびリンク層アドレス 0002.7D1A.9472 の隣接で、IPv6 ネイバー探索キャッシュのスタティック エントリを設定する例を示します。

```
RP/0/RSP0/CPU0:router (config)# ipv6 neighbor 2001:0DB8::45A 0002.7D1A.9472
```

## 関連コマンド

コマンド	説明
<a href="#">clear ipv6 neighbors</a> , (542 ページ)	スタティック エントリを除く、IPv6 近隣探索キャッシュのすべてのエントリを削除します。
<a href="#">ipv6 enable</a> , (582 ページ)	明示的な IPv6 アドレスで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します。
<a href="#">show ipv6 neighbors</a> , (654 ページ)	IPv6 近隣探索キャッシュ情報を表示します。



## ipv6 source-route

IPv6 タイプ送信元（タイプ 0）ルーティング ヘッダーの処理をイネーブルにするには、グローバル コンフィギュレーション モードで **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、キーワードと引数はありません。

### コマンド デフォルト

**ipv6 source-route** コマンドの **no** バージョンはデフォルトです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 4.2.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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。**ipv6 source-route** コマンドが設定され、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、ルータはパケットをドロップし、送信元に IPv6 ICMP エラー メッセージを送信し、適切なデバッグ メッセージをロギングします。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# ipv6 source-route
RP/0/RSP0/CPU0:router(config)#
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 source-route</a> , <a href="#">(565 ページ)</a>	source-route ヘッダー オプションを含むすべての IPv4 データグラムの処理を可能にします。

## ipv6 unreachable disable

IPv6 インターネット制御メッセージプロトコル (ICMP) 到達不能メッセージの生成をディセーブルにするには、適切なコンフィギュレーション モードで **ipv6 unreachable disable** コマンドを使用します。ICMP 到達不能メッセージの生成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 unreachable disable**

**no ipv6 unreachable disable**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

IPv6 ICMP 到達不能メッセージが生成されます。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ソフトウェアが、それ自体を宛先とした、認識しないプロトコルを使用する非ブロードキャスト パケットを受信した場合、その送信元に ICMP プロトコル到達不能メッセージを送信します。

宛先アドレスまでのルートが不明なため最終的な宛先に配信できないデータグラムを受信した場合、ソフトウェアはそのデータグラムの発信者に ICMP ホスト到達不能メッセージで応答します。

このコマンドは、多くの ICMP 到達不能メッセージに影響を与えます。

### タスク ID

タスク ID	操作
ipv6	読み取り、書き込み
network	読み取り、書き込み

---

**例**

次に、GigabitEthernet インターフェイス 0/6/0/0 で ICMP 到達不能メッセージの生成をディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/6/0/0  
RP/0/RSP0/CPU0:router(config-if)# ipv6 unreachable disable
```

## local pool

ピア接続時に割り当てられる IP アドレスの 1 つ以上のローカルアドレスプールを作成するには、グローバル コンフィギュレーション モードで **local pool** コマンドを使用します。デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

**local pool** [ipv4] [vrf vrf\_name] {poolname| default} first-ip-address [ last-ip-address ]

**no local pool** [ipv4] [vrf vrf\_name] {poolname| default} first-ip-address [ last-ip-address ]

### 構文の説明

<b>vrf</b>	VRF の名前が指定されることを示します。このパラメータが指定されない場合、デフォルトの VRF が割り当てられます。
<i>vrf_name</i>	プールのアドレスが属する VRF の名前を指定します。名前が指定されない場合、デフォルトの VRF が使用されます。
<b>default</b>	他のプールが指定されていない場合に使用されるデフォルトのローカル IPv4 アドレス プールを作成します。
<i>poolname</i>	ローカル IPv4 アドレス プールの名前を指定します。
<i>first-ip-address</i>	IPv4 アドレス範囲の最初のアドレスを指定します。high-IP-address が指定されない場合、アドレス範囲は、1 つだけのアドレスと見なされます。
<i>last-ip-address</i>	(任意) IPv4 アドレス範囲の最後のアドレスを指定します。high-IP-address が指定されない場合、アドレス範囲は、1 つだけのアドレスと見なされます。

### コマンド デフォルト

VRF が指定されない場合、特殊なデフォルトプール。デフォルトでは、この機能はディセーブルです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドを使用すると、ピア接続時の IP アドレスの割り当てに使用されるローカルアドレス プールを作成できます。また、既存のプールの IP アドレスの範囲を追加することもできます。プールの名前が指定されていない場合、「default」という名前のプールが使用されます。

オプションの **vrf** キーワードおよび関連する *vrfname* を使用すると、指定した VRF で IPv4 アドレス プールを割り当てることができます。 **vrf** キーワードを使用せずに作成された IPv4 はすべて、自動的にデフォルトの VRF のメンバになります。 IPv4 アドレス プール名に割り当てることができる VRF は 1 つだけです。それ以降、プール グループ内で、同じプール名を使用する場合、これは、そのプールの拡張として扱われます。また、既存のローカル IPv4 アドレス プール名を別の VRF に関連付けようとしても拒否されます。そのため、プール名を使用すると、毎回、関連する VRF を暗黙的に選択したことになります。



(注) 重複アドレスが誤って生成されるリスクを軽減するため、デフォルトプールの作成は、デフォルトの VRF だけで許可されます。

VRF 内のすべての IPv4 アドレス プールは、オーバーラップするアドレスを回避するためにチェックされますが、異なる VRF 間でアドレスがオーバーラップすることはあります。

## タスク ID

タスク ID	操作
ipv4	読み取り、書き込み
ipv6	読み取り、書き込み
network	読み取り、書き込み

## 例

次に、範囲 172.16.23.0 ~ 172.16.23.255 のすべての IPv4 アドレスを含む「pool2」という名前のローカル IPv4 アドレス プールを作成する例を示します。

```
RP/0/RSP0/CPU0:router (config)# local pool ipv4 pool2 172.16.23.0 172.16.23.255
```

次に、IP アドレス 1024 のプールを設定する例を示します。

```
RP/0/RSP0/CPU0:router (config)#no local pool ipv4 default
RP/0/RSP0/CPU0:router (config)#local pool ipv4 default 10.1.1.0 10.1.4.255
```



- (注) ローカルプールを定義する前に、このコマンドの **no** 形式を使用して、既存のプールを削除しておくことをお勧めします。これは、既存のプール名を指定すると、新しい IPv4 アドレスでそのプールを拡張する要求と見なされるからです。プール拡張には、このコマンドの **no** 形式は適用できません。

次に、IPv4 アドレスの複数の範囲を 1 つのプールに設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)#local pool ipv4 default 10.1.1.0 10.1.9.255
RP/0/RSP0/CPU0:router(config)#local pool ipv4 default 10.2.1.0 10.2.9.255
```

次に、基本システム グループで 2 つのプールグループおよび IPv4 アドレス プールを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)#local pool vrf grp1 ipv4 p1_g1 10.1.1.1 10.1.1.50
RP/0/RSP0/CPU0:router(config)#local pool vrf grp1 ipv4 p2_g1 10.1.1.100 10.1.1.110
RP/0/RSP0/CPU0:router(config)#local pool vrf grp2 ipv4 p1_g2 10.1.1.1 10.1.1.40
RP/0/RSP0/CPU0:router(config)#local pool ipv4 lp1 10.1.1.1 10.1.1.10
RP/0/RSP0/CPU0:router(config)#local pool vrf grp1 ipv4 p3_g1 10.1.2.1 10.1.2.30
RP/0/RSP0/CPU0:router(config)#local pool vrf grp2 ipv4 p2_g2 10.1.1.50 10.1.1.70
RP/0/RSP0/CPU0:router(config)#local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

この例では、次のようになります。

- VRF grp1 は、プール p1\_g1、p2\_g1、p3\_g1 で構成されています。
- VRF grp2 は、プール p1\_g2 および p2\_g2 で構成されています。
- プール lp1 および lp2 は、明示的に vrf に関連付けられていないため、デフォルト vrf のメンバーになります。



- (注) IPv4 アドレス 10.1.1.1 は、vrf grp1 および grp2 と、デフォルト vrf でオーバーラップしています。デフォルト vrf を含む vrf 内ではオーバーラップはありません。

次に、VPN および VRF で使用するための IP アドレス プールおよびグループを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p1_vpn1 10.1.1.1 10.1.1.50
RP/0/RSP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p2_vpn1 10.1.1.100 10.1.1.110
RP/0/RSP0/CPU0:router(config)# local pool vrf vpn2 ipv4 p1_vpn2 10.1.1.1 10.1.1.40
RP/0/RSP0/CPU0:router(config)# local pool ipv4 lp1 10.1.1.1 10.1.1.10
RP/0/RSP0/CPU0:router(config)# local pool vrf vpn1 ipv4 p3_vpn1 10.1.2.1 10.1.2.30
RP/0/RSP0/CPU0:router(config)# local pool vrf vpn2 ipv4 p2_vpn2 10.1.1.50 10.1.1.70 group
vpn2
RP/0/RSP0/CPU0:router(config)# local pool ipv4 lp2 10.1.2.1 10.1.2.10
```

次に、2 つの VRF およびデフォルト VRF でプールを設定する例を示します。

- VRF vpn1 は、プール p1\_vpn1、p2\_vpn1、p3\_vpn1 で構成されています。
- VRF vpn2 は、プール p1\_vpn2 および p2\_vpn2 で構成されています。
- プール lp1 および lp2 は、VRF に関連付けられていないため、デフォルト VRF に属します。



---

(注) IPv4 アドレス 10.1.1.1 は、VRF vpn1 および vpn2 と、デフォルト VRF でオーバーラップしています。VRF 内でのオーバーラップはありません。

---

VPN では、リモートユーザデータに基づいて正しいプールを選択することで正しい vrf を選択する設定が必要です。特定の VPN の各ユーザは、その VPN に適切なプールおよび関連する vrf を使用して、アドレス レンジを選択できます。他の VPN (他の vrf) との間でアドレスが重複していても問題ではありません。これは、VPN のアドレス レンジがその VPN に固有であるからです。この例では、VRF vpn1 のユーザには、プール p1\_vpn1、p2\_vpn1 および p3\_vpn1 の組み合わせが関連付けられ、そのアドレス レンジからアドレスが割り当てられます。アドレスは、そのアドレスがそこから割り当てられるプールと同じプールに戻されます。



## 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、EXEC モードで **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

<b>ipv4</b>	IPv4 アドレス競合を表示します。
<b>ipv6</b>	IPv6 アドレス競合を表示します。
<b>vrf</b>	(任意) VPN ルーティングおよび転送 (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。
<b>address</b>	(任意) アドレス競合情報を表示します。
<b>override</b>	(任意) アドレス競合上書き情報を表示します。
<b>unnumbered</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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。

任意のオプション キーワードを指定せずに **show arm conflicts** 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る出力が表示されます。

## タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show arm ipv4 conflicts** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm ipv4 conflicts

F Forced down
| Down interface & addr                Up interface & addr
F Lo2 10.1.1.2/24                       Lol 10.1.1.1/24

Forced down interface                Up interface
tu2->tu1                             tu1->Lol
```

次に、**address** キーワードを指定した **show arm ipv4 conflicts** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm ipv4 conflicts address

F Forced down
| Down interface & addr                Up interface & addr
F Lo2 10.1.1.2/24                       Lol 10.1.1.1/24
```

次に、**unnumbered** キーワードを指定した **show arm ipv4 conflicts** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm ipv4 conflicts unnumbered

Forced down interface                Up interface                VRF
tu2->tu1                             tu1->Lol
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 59: **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。

フィールド	説明
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。
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 database

Address Repository Manager (ARM) データベースに保存されている IPv4 または IPv6 のアドレス情報を表示するには、EXEC モードで **show arm database** コマンドを使用します。

**show arm {ipv4|ipv6} [vrf {vrf-name?}] database [interface type interface-path-id] network prefix/length]**

### 構文の説明

<b>ipv4</b>	IPv4 アドレス情報を表示します。
<b>ipv6</b>	IPv6 アドレス情報を表示します。
<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<i>vrf-name</i>	(任意) VRF の名前。
<b>interface</b>	(任意) 指定されたインターフェイスで設定されている IPv4 または IPv6 アドレスを表示します。
<i>type</i>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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、 <b>show interfaces</b> 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。
<b>network</b>	(任意) プレフィックスと一致するアドレスを表示します。
<i>prefix / length</i>	(任意) ネットワークプレフィックスおよびマスク。指定するマスクの前にスラッシュ記号 (/) を付ける必要があります。範囲は 0 ~ 128 です。

コマンド デフォルト なし

コマンド モード EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show arm database** コマンドは、IP ARM データベース情報の表示に使用されます。データベース情報は、IPv4 または IPv6 アドレス、インターフェイス タイプおよび名前、プロデューサ情報で表示されます。

タスク ID

タスク ID	操作
network	読み取り

例

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

```
RP/0/RSP0/CPU0:router# show arm
ipv4 database interface loopback

Fri Jul 25 10:54:52.304 PST DST

P = Primary, S = Secondary address
|U = Unnumbered
|| Address                Interface                Producer
VRF: default
P 172.29.52.75/24         MgmtEth0/RP0/CPU0/0    ipv4_ma 0/RP0/CPU0      100
P 10.2.2.2/32            Loopback0                ipv4_ma 0/RP1/CPU0
P 10.12.24.2/24          Bundle-POS24             ipv4_ma 0/RP1/CPU0
P 10.12.28.2/24          Bundle-Ether28           ipv4_ma 0/RP1/CPU0
P 10.12.29.2/24          Bundle-Ether28.1        ipv4_ma 0/RP1/CPU0
P 10.12.30.2/24          Bundle-Ether28.2        ipv4_ma 0/RP1/CPU0
P 10.12.31.2/24          Bundle-Ether28.3        ipv4_ma 0/RP1/CPU0
P 10
.1
.1
.1
/24 Loopback1ipv4_io 0/0/0P 10.1
.1
.1
/24 Loopback1 ipv4_io 0/0/0

| Address                Interface                Producer
P 10.12.16.2/24          GigabitEthernet0/1/5/0  ipv4_ma 0/1/CPU0      1001
P 10.23.4.2/24           GigabitEthernet0/1/5/1  ipv4_ma 0/1/CPU0      1002
P 10.27.4.2/24           GigabitEthernet0/1/5/2  ipv4_ma 0/1/CPU0
P 10.12.8.2/24           POS0/1/0/1              ipv4_ma 0/1/CPU0
P 10.112.4.2/24          POS0/1/0/2              ipv4_ma 0/1/CPU0
```

## show arm database

```

P 10.112.8.2/24      POS0/1/0/3          ipv4_ma 0/1/CPU0
P 10.12.32.2/24     POS0/1/4/2          ipv4_ma 0/1/CPU0
P 10.12.32.2/24     POS0/1/4/3          ipv4_ma 0/1/CPU0
P 172.29.52.28/24   MgmtEth0/4/CPU1/0  ipv4_ma 0/4/CPU1
P 172.29.52.27/24   MgmtEth0/4/CPU0/0  ipv4_ma 0/4/CPU0
P 10.12.20.2/24     GigabitEthernet0/6/5/1  ipv4_ma 0/6/CPU0
P 10.4
.1
.4
/24 gigabitethernet 10/0 ipv4_io 1 10
S 10.4.2.4/24       gigabitethernet 10/0  ipv4_io 1 10
S 10.4.3.4/24       gigabitethernet 10/1  ipv4_io 1 10

```

P = Primary, S = Secondary address

|U = Unnumbered

```

|| Address          Interface          Producer
VRF: default
P 10.12.12.2/24     POS0/6/0/1        ipv4_ma 0/6/CPU0
P 10.23.8.2/24      POS0/6/4/4        ipv4_ma 0/6/CPU0
P 10.12.4.2/24      POS0/6/4/5        ipv4_ma 0/6/CPU0
P 10.24.4.2/24     POS0/6/4/6        ipv4_ma 0/6/CPU0
P 12
.25
.12
.10
/16

```

MgmtEth0/RSP0/CPU0/0 ipv4\_ma 0/RSP0/CPU0

次の表に、この出力で表示される重要なフィールドについて説明します。

表 60 : show arm database コマンドのフィールドの説明

フィールド	説明
Primary	プライマリ IP アドレス。
Secondary	セカンダリ IP アドレス。
Unnumbered Address	インターフェイスは unnumbered で、表示されるアドレスは、参照されるインターフェイスのアドレスです。
Interface	この IP アドレスを持つインターフェイス。
Producer	IP アドレスを ARM の提供するプロセス。

## show arm router-ids

ルータ ID 情報と Address Repository Manager (ARM) の VPN ルーティング/転送テーブル情報を表示するには、EXEC モードで **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

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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、ルータで選択されたルータ ID 情報を表示できます。

#### タスク ID

タスク ID	操作
network	読み取り

#### 例

次に、**show arm router-ids** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm router-ids
Router-ID          Interface
```

```
10.10.10.10      Loopback0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 61 : *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 registrations producers

Address Repository Manager (ARM) のプロデューサ登録情報を表示するには、EXEC モードで **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

<b>ipv4</b>	IPv4 プロデューサ登録情報を表示します。
<b>ipv6</b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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	操作
network	読み取り

### 例

次に、**show arm registrations producers** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm ipv4 registrations producers
```

## show arm 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
2       0/4/0         ipv4_io      1.1         Y
1       0/6/0         ipv4_io      1.1         Y

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 62 : *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 Address ARM (IP ARM; IP アドレス ARM) により使用される ID。
Node	プロデューサが稼動する物理ノード (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 <i>apis</i> 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 summary

IP Address Repository Manager (ARM) のサマリー情報を表示するには、EXEC モードで **show arm summary** コマンドを使用します。

**show arm {ipv4| ipv6} summary**

### 構文の説明

<b>ipv4</b>	IPv4 サマリー情報を表示します。
<b>ipv6</b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show arm summary** コマンドを使用すると、ルータのプロデューサ、アドレス競合、unnumbered インターフェイス競合の数に関するサマリー情報を表示できます。

### タスク ID

タスク ID	操作
network	読み取り

### 例

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

```
RP/0/RSP0/CPU0:router# show arm ipv4 summary
```

```
IPv4 Producers                : 5
IPv4 Router id consumers      : 7
IPv4 address conflicts        : 2
IPv4 unnumbered interface conflicts : 1
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 63: *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 Router id consumers	ルータの IPv4 ルータ ID コンシューマの数
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

## show arm vrf-summary

Address Repository Manager (ARM) により識別される VPN ルーティング/転送 (VRF) インスタンス情報のサマリー情報を表示するには、EXEC モードで **show arm vrf-summary** コマンドを使用します。

**show arm {ipv4| ipv6} vrf-summary**

### 構文の説明

<b>ipv4</b>	IPv4 アドレス情報を表示します。
<b>ipv6</b>	IPv6 アドレス情報を表示します。

### コマンド デフォルト

なし

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show arm vrf-summary** コマンドを使用すると、IPv4 VPN ルーティング/転送インスタンスに関する情報を表示できます。

### タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show arm vrf-summary** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show arm vrf-summary

VRF IDs:          VRF-Names:
0x60000000        default
0x60000001        vrf1
0x60000002        vrf2
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 64: **show arm vrf-summary** コマンドのフィールドの説明

フィールド	説明
VRF IDs	VPN ルーティング/転送 (VRF) ID (vrfid) 番号。
VRF-Names	VRF に指定される名前

## show clns statistics

コネクションレス型ネットワーク サービス (CLNS) プロトコル統計情報を表示するには、EXEC モードで **show clns statistics** コマンドを使用します。

### show clns statistics

#### 構文の説明

このコマンドには、キーワードと引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

EXEC

#### コマンド履歴

リリース

変更箇所

リリース 3.7.2

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドを使用すると、CLNS 統計情報を表示できます。

#### タスク ID

タスク ID

操作

isis

読み取り

#### 例

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

```
RP/0/RSP0/CPU0:router# show clns statistics
```

```
CLNS Statistics:
Last counter clear:                2868 seconds ago
Total number of packets sent:      0
Total number of packets received:  0
Send packets dropped, buffer overflow: 0
Send packets dropped, out of memory: 0
```

## show clns statistics

```

Send packets dropped, other:          0
Receive socket max queue size:       0
Class   Overflow/Max   Rate Limit/Max
IIH     0/0             0/0
LSP     0/0             0/0
SNP     0/0             0/0
OTHER   0/0             0/0
Total   0               0

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 65 : show clns traffic コマンドのフィールドの説明

フィールド	説明
Class	<p>パケットタイプを示します。パケットタイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• IIH : Intermediate System-to-Intermediate-System hello パケット</li> <li>• lsp : リンク ステート パケット</li> <li>• snp : パケットシーケンス番号</li> <li>• other</li> </ul>
Overflow/Max	<p>ソケット キューのオーバーフローのためにドロップされたパケット数を示します。この数値は、x/y フォーマットで表示されます。ここで、x は、パケットドロップの合計数を示し、y は、行の最大ドロップ数を示します。</p>
Rate Limit/Max	<p>レート制限のためにドロップされたパケット数を示します。この数値は、x/y フォーマットで表示されます。ここで、x は、パケットドロップの合計数を示し、y は、行の最大ドロップ数を示します。</p>



# show ipv4 interface

IPv4 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、EXEC モードで **show ipv4 interface** コマンドを使用します。

**show ipv4** [*vrf vrf-name*] **interface** [*type interface-path-id*] **brief** **summary**]

## 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ 機能を使用してください。
<b>interface-path-id</b>	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"> <li>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"> <li><i>rack</i> : ラックのシャーン番号。</li> <li><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。</li> <li><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。</li> <li><i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 /CPU0/0。</li> <li>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。</li> </ul> <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>
<b>brief</b>	(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。

## show ipv4 interface

**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** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	このコマンドが導入されました。
	リリース 4.2.0	このコマンドは、BNG でサポートされていました。

**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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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* が指定されない場合、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 に属する場合だけ表示されます。

タスク ID	タスク ID	操作
	ipv4	読み取り
	network	読み取り

**例** 次に、**show ipv4 interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
gigabitethernet0
/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
gigabitethernet0
/0/0/0 is Shutdown, line protocol is Down
Vrf is default (vrfid 0x60000000)
Internet protocol processing disabled
    
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 66 : 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、インターフェイスには「Up」マークが付けられます。インターフェイスが使用可能になるには、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ければなりません。
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、回線プロトコルには「UP」マークが付けられます。インターフェイスが使用可能になるには、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ければなりません。
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 値を表示します。 <a href="#">10</a>

## show ipv4 interface

フィールド	説明
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	インターフェイスでプロキシ ARP がイネーブルまたはディセーブルのいずれになっているかを示します。 <sup>11</sup>
ICMP redirects	ICMPv4 リダイレクトがこのインターフェイスに送信されるかどうかを指定します。 <sup>12</sup>
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。

<sup>10</sup> MTU = 最大伝送単位<sup>11</sup> ARP = アドレス解決プロトコル<sup>12</sup> 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

## 関連コマンド

コマンド	説明
<a href="#">show ipv6 interface, (650 ページ)</a>	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

## show local pool

IPv4 ローカル プールの詳細を表示するには、EXEC モードで **show local pool** コマンドを使用します。

```
show {local| other_pool_types} pool [vrf vrf_name] {ipv4| ipv6} {default| poolname}
```

### 構文の説明

<b>local</b>	アドレス プールがローカルであることを指定します。
<b>vrf</b>	VRF の名前が指定されることを示します。このパラメータが指定されない場合、デフォルトの VRF が割り当てられます。
<i>vrf_name</i>	プールのアドレスが属する VRF の名前を指定します。名前が指定されない場合、デフォルトの VRF が使用されます。
<b>default</b>	他のプールが指定されていない場合に使用されるデフォルトのローカル IPv4 アドレス プールを作成します。
<i>poolname</i>	ローカル IPv4 アドレス プー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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ipv4	読み取り

タスク ID	操作
network	読み取り

## 例

次に、poolname に P1 を指定した **show ipv4 local pool** の出力例を示します。

```
RP/0/RSP0/CPU0:router# show ipv4 local pool P1
```

```
Pool Begin End FreeInUse
P1 172.30.228.11172.30.228.1660
Available addresses:
172.30.228.11
172.30.228.12
172.30.228.13
172.30.228.14
172.30.228.15
172.30.228.16
Inuse addresses:
None
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 67: **show ipv4 local pool** コマンドのフィールドの説明

フィールド	説明
Pool	プールの名前
Begin	このプールで定義されているアドレス範囲の最初の IP アドレス
End	このプールで定義されているアドレス範囲の最後の IP アドレス
Free	使用できるアドレスの数
InUse	使用されているアドレスの数

## 関連コマンド

コマンド	説明
<a href="#">local pool</a> , (621 ページ)	ピア接続時に割り当てられる IP アドレスの 1 つ以上のローカル アドレス プールを作成します。

## show ipv4 traffic

IPv4 トラフィックに関する統計情報を表示するには、EXEC モードで **show ipv4 traffic** コマンドを使用します。

### show ipv4 traffic [brief]

#### 構文の説明

<b>brief</b>	(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

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

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドは、BNG でサポートされていました。

#### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show ipv4 traffic** コマンドの出力は、IPv4 に固有である点を除き、**show ipv6 traffic** コマンドの出力と似ています。

#### タスク ID

タスク ID	操作
ipv4	読み取り
network	読み取り

例

次に、**show ipv4 traffic** コマンドの出力例を示します。

```

RP/0/RSP0/CPU0:router# 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
        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
  Frags: 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

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 68 : 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 フィールドがゼロに減少されたためパケットが廃棄されるときに発生します。 <a href="#">13</a>
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。



フィールド	説明
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。
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	Cisco IOS XR ソフトウェアが送信方法を認識していなかったデータグラムを廃棄するときにカウントされます。

<sup>13</sup> TTL = 存続可能時間

#### 関連コマンド

コマンド	説明
<a href="#">show ipv6 traffic</a> , ( <a href="#">662 ページ</a> )	IPv6 トラフィックに関する統計情報を表示します。

## show ipv6 interface

IPv6 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、EXEC モードで **show ipv6 interface** コマンドを使用します。

**show ipv6 [vrf vrf-name] interface [type interface-path-id] [brief] [summary]**

### 構文の説明

<b>vrf</b>	(任意) VPN ルーティングおよび転送 (VRF) インスタンス情報を表示します。
<b>vrf-name</b>	(任意) VRF の名前。
<b>type</b>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	(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"> <li>• 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"> <li>◦ <i>rack</i> : ラックのシャーシ番号。</li> <li>◦ <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。</li> <li>◦ <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。</li> <li>◦ <i>port</i> : インターフェイスの物理ポート番号。</li> </ul> </li> <li>(注) ルートプロセッサカード上に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、モジュールは CPU0 です。例: インターフェイス MgmtEth0/RSP0 /CPU0/0。</li> <li>• 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。</li> </ul> <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>
<b>brief</b>	(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。

**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** 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** EXEC

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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。

タスク ID	タスク ID	操作
	ipv6	読み取り

**例** 次に、**show ipv6 interface** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show ipv6 interface
GigabitEthernet0/2/0/0 is Up, line protocol is Up, Vrfid is default (0x60000000)
IPv6 is enabled, link-local address is fe80::212:daff:fe62:c150
Global unicast address(es):
  202::1, subnet is 202::/64
Joined group address(es): ff02::1:ff00:1 ff02::1:ff62:c150 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 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.
```

## show ipv6 interface

```
Outgoing access list is not set
Inbound access list is not set
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 69 : show ipv6 interface コマンドのフィールドの説明

フィールド	説明
GigabitEthernet0 /3/0/0 is Shutdown, line protocol is Down	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、インターフェイスには「Up」マークが付けられます。インターフェイスが使用可能になるには、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ければなりません。
line protocol is Up (or 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、回線プロトコルには「UP」マークが付けられます。インターフェイスが使用可能になるには、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ければなりません。
IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)	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 がイネーブルの場合、インターフェイスには「enabled」マークが付けられます。重複アドレス検出処理がインターフェイスのリンクローカルアドレスを重複アドレスと識別した場合、IPv6 パケットは、そのインターフェイスでディセーブルであり、インターフェイスには「stalled」マークが付けられます。IPv6 がイネーブルでない場合、インターフェイスには「disabled」マークが付けられます。
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"> <li>• <b>duplicate</b> : 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。</li> <li>• <b>tentative</b> : 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。</li> </ul> <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。

関連コマンド

コマンド	説明
<a href="#">show ipv4 interface</a> , (641 ページ)	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します。

# show ipv6 neighbors

IPv6 ネイバー探索キャッシュ情報を表示するには、EXEC モードで **show ipv6 neighbors** 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

*type* (任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

*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。

- 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 カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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。

**location node-id** (任意) ノードを指定します。 *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 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 EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.3.0	このコマンドは、BNG でサポートされていました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

*interface-type* および *interface-number* 引数が指定されていない場合、すべての IPv6 隣接のキャッシュ情報が表示されます。*interface-type* および *interface-number* 引数を指定すると、指定して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	操作
ipv6	読み取り

## 例

次に、インターフェイス タイプおよび番号を指定して入力された **show ipv6 neighbors** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors
gigabitethernet
```

```
0/0/0/0
```

```
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e REACH gigabitethernet2
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e REACH gigabitethernet2
3001:1::45a                               - 0002.7d1a.9472 REACH gigabitethernet2
```

次に、IPv6 アドレスを指定して入力された **show ipv6 neighbors** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors 2000:0:0:4::2
```

```
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e REACH gigabitethernet2
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 70 : *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。
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。



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。次に、IPv6 ネイバー探索キャッシュのダイナミック エントリの状態を示します。</p> <ul style="list-style-type: none"> <li>• <b>INCMMP (incomplete)</b> : 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。</li> <li>• <b>reach (reachable)</b> : 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 <b>ReachableTime</b> ミリ秒内に受信されました。<b>reach</b> 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。</li> <li>• <b>stale</b> : 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、<b>ReachableTime</b> ミリ秒を超えています。<b>stale</b> 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。</li> <li>• <b>delay</b> : 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、<b>ReachableTime</b> ミリ秒を超えています。パケットは直近の <b>DELAY_FIRST_PROBE_TIME</b> 秒以内に送信されました。到達可能性確認が、<b>delay</b> 状態になってから <b>DELAY_FIRST_PROBE_TIME</b> 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 <b>probe</b> に変更します。</li> <li>• <b>probe</b> : 到達可能性確認が受信されるまで、<b>RetransTimer</b> 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。</li> </ul> <p>次に、IPv6 ネイバー探索キャッシュのスタティック エントリの可能な状態を示します。</p> <ul style="list-style-type: none"> <li>• <b>INCMMP (incomplete)</b> : このエントリのインターフェイスはダウン状態です。</li> </ul>

フィールド	説明
	<ul style="list-style-type: none"> <li>• reach (reachable) : このエントリのインターフェイスはアップ状態です。</li> </ul> <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であったインターフェイス。

---

**関連コマンド**

コマンド	説明
<a href="#">ipv6 neighbor, (614 ページ)</a>	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
<a href="#">show ipv6 neighbors summary, (660 ページ)</a>	近隣エントリのサマリー情報を表示します。

# show ipv6 neighbors summary

近隣エントリのサマリー情報を表示するには、EXEC モードで **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、キーワードと引数はありません。

### コマンド デフォルト

デフォルト値は、disabled です。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ipv6	読み取り

### 例

次に、近隣エントリのサマリー情報の出力例を示します。

```
RP/0/RSP0/CPU0:router# show ipv6 neighbors summary

Mcast nbr entries:
  Subtotal: 0
Static nbr entries:
  Subtotal: 0
Dynamic nbr entries:
  Subtotal: 0
```

```
Total nbr entries: 0
```

## 関連コマンド

コマンド	説明
<a href="#">ipv6 neighbor, (614 ページ)</a>	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
<a href="#">show ipv6 neighbors, (654 ページ)</a>	IPv6 ネイバー探索キャッシュ情報を表示します。

# show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、EXEC モードで **show traffic** コマンドを使用します。

## show ipv6 traffic [brief]

### 構文の説明

<b>brief</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show ipv6 traffic** コマンドの出力は、IPv6 に固有である点を除き、**show ipv4 traffic** コマンドの出力と似ています。

### タスク ID

タスク ID	操作
ipv6	読み取り
network	読み取り

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# 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
  unreach: 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
  unreach: 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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 71 : **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。

フィールド	説明
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。
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。

## 関連コマンド

コマンド	説明
<a href="#">show ipv4 traffic</a> , (647 ページ)	IPv4 トラフィックに関する統計情報を表示します。



# show mpa client

Multicast Port Arbitrator (MPA) クライアントについての情報を表示するには、EXEC モードで **show mpa client** コマンドを使用します。

**show mpa client {consumers| producers}**

## 構文の説明

<b>consumers</b>	コンシューマのクライアントを表示します。
<b>producers</b>	プロデューサのクライアントを表示します。

## コマンド デフォルト

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show mpa client** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show mpa client consumers
List of producer clients for ipv4 MPA
Location      Protocol      Process
```

## show mpa client

0/1/CPU0	255	raw
0/1/CPU0	17	udp
0/4/CPU0	17	udp
0/4/CPU0	255	raw
0/4/CPU1	17	udp
0/4/CPU1	255	raw
0/6/CPU0	17	udp
0/6/CPU0	255	raw
0/RP1/CPU0	17	udp
0/RP1/CPU0	255	raw

## show mpa groups

Multicast Port Arbitrator (MPA) マルチキャスト グループ情報を表示するには、EXEC モードで **show mpa groups** コマンドを使用します。

**show mpa groups** *type interface-path-id*

### 構文の説明

*type* インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。

*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 カード上に管理イーサネット インターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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 なし

コマンド モード EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show mpa groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show mpa groups gig 0/1/0/2
Mon Jul 27 04:07:19.802 DST
GigabitEthernet0/1/0/2 :-
  224.0.0.1 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.2 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.5 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.6 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.13 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
  224.0.0.22 : includes 0, excludes 1, mode EXCLUDE
    <no source filter>
```

## show mpa ipv4

IPv4 の Multicast Port Arbitrator (MPA) についての情報を表示するには、EXEC モードで **show mpa ipv4** コマンドを使用します。

```
show mpa ipv4 {client {consumers|producers}| groups type interface-path-id}
```

### 構文の説明

<b>client</b>	(任意) MPA クライアントに関する情報を表示します。
<b>consumers</b>	コンシューマのクライアントを表示します。
<b>producers</b>	プロデューサのクライアントを表示します。
<b>groups</b>	MPA マルチキャスト グループに関する情報を表示します。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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 モラボルト EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show mpa ipv4** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show mpa ipv4 client producers
List of producer clients for ipv4 MPA
Location      Protocol  Process
0/1/CPU0     17        udp
0/1/CPU0     255       raw
0/4/CPU0     17        udp
0/4/CPU0     255       raw
0/4/CPU1     17        udp
0/4/CPU1     255       raw
0/6/CPU0     17        udp
0/6/CPU0     255       raw
0/RP0/CPU0   17        udp
0/RP0/CPU0   255       raw
0/RP1/CPU0   255       raw
0/RP1/CPU0   17        udp
```

## show mpa ipv6

IPv6 の Multicast Port Arbitrator (MPA) についての情報を表示するには、EXEC モードで **show mpa ipv6** コマンドを使用します。

```
show mpa ipv6 {client {consumers|producers}| groups type interface-path-id}
```

### 構文の説明

<b>client</b>	(任意) MPA クライアントに関する情報を表示します。
<b>consumers</b>	コンシューマのクライアントを表示します。
<b>producers</b>	プロデューサのクライアントを表示します。
<b>groups</b>	MPA マルチキャスト グループに関する情報を表示します。
<b>type</b>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<b>interface-path-id</b>	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に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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 モデル **EXEC**

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
network	読み取り

## 例

次に、**show mpa ipv6** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show mpa ipv6 client producers
List of producer clients for ipv6 MPA
Location      Protocol  Process
0/1/CPU0     17       udp
0/1/CPU0     255     raw
0/4/CPU0     255     raw
0/4/CPU0     17       udp
0/4/CPU1     17       udp
0/4/CPU1     255     raw
0/6/CPU0     17       udp
0/6/CPU0     255     raw
0/RP0/CPU0   17       udp
0/RP0/CPU0   255     raw
0/RP1/CPU0   17       udp
0/RP1/CPU0   255     raw
```



# show vrf

VPN ルーティング/転送 (VRF) インスタンスのコンテンツを表示するには、EXEC モードで **show vrf** コマンドを使用します。

**show vrf {all| vrf-name} [detail]**

## 構文の説明

<b>all</b>	すべての VRF のコンテンツを表示します。
<b>vrf-name</b>	VRF を一意で識別する名前。
<b>detail</b>	(任意) 対応する VRF の詳細情報を表示します。

## 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.1.1	<b>detail</b> キーワードが追加されました。

## 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
network	読み取り、書き込み

## 例

次に、**show vrf** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router# show vrf all

VRF          RD          RT          AFI  SAFI
vpn_1        not set
              import 2:2    IPV4  Unicast
              export 2:2    IPV4  Unicast
vpn_2        not set
              import 3:3    IPV4  Unicast
              export 3:3    IPV4  Unicast
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 72: **show vrf** コマンドのフィールドの説明

フィールド	説明
VRF	ユーザが割り当てた VRF 名。
RD	各 VRF に関連付けられたルート識別子を表示します。
RT	インポートおよびエクスポートルートターゲット拡張コミュニティを表示します。
AFI	IP アドレス ファミリを表示します。
SAFI	VRF トポロジを表示します。

次に、**show vrf detail** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router# show v1 detail

V1; RD not set; VPN ID not set
VRF mode: Big
Description not set
Address family IPV4 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
Address family IPV6 Unicast
  No import VPN route-target communities
  No export VPN route-target communities
  No import route policy
  No export route policy
```

## 関連コマンド

コマンド	説明
<a href="#">vrf</a> , (676 ページ)	ルーティング プロトコルの VRF インスタンスを設定します。

# vrf

ルーティング プロトコルの VPN ルーティング/転送 (VRF) インスタンスを設定するには、ルータ コンフィギュレーション モードで **vrf** コマンドを使用します。VRF インスタン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。

**vrf** *vrf-name*

**no vrf** *vrf-name*

## 構文の説明

<i>vrf-name</i>	VRF インスタンスの名前。all、default、および global を名前に使用できません。
-----------------	---

## コマンド デフォルト

(注) サポートされる VRF の数はプラットフォームにより異なります。

すべてのルーティングプロトコルは、そのルートを VRF のルーティングテーブルに挿入します。

## コマンド モード

ルータ コンフィギュレーション

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
ip services	読み取り、書き込み

---

例

次に、**vrf** コマンドを使用して VRF を設定する例を示します。

```
RP/0/RSP0/CPU0:router# config  
RP/0/RSP0/CPU0:router(config)# vrf client
```

## vrf (address-family)

VRF インスタンスのアドレス ファミリを設定するには、VRF コンフィギュレーション モードで **vrf (address-family)** コマンドを使用します。アドレス ファミリ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。

**vrf** *vrf-name* [**address-family** {**ipv4**|**ipv6**} **unicast**]

**no vrf** *vrf-name* [**address-family** {**ipv4**|**ipv6**} **unicast**]

### 構文の説明

<b>vrf-name</b>	VRF インスタンスの名前。
<b>address-family</b>	(任意) AFI または SAFI 設定をイネーブルにします。
<b>ipv4</b>	IPv4 アドレスのアドレス ファミリ設定をイネーブルにします。
<b>ipv6</b>	IPv6 アドレスのアドレス ファミリ設定をイネーブルにします。
<b>unicast</b>	ユニキャスト トポロジを示します。

### コマンド デフォルト

なし

### コマンド モード

VRF コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
ip services	読み取り、書き込み

## 例

次に、**vrf (address-family)** コマンドを使用して VRF インスタンスのアドレス ファミリを設定する例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# vrf client
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)#
```

## 関連コマンド

コマンド	説明
<a href="#">vrf, (676 ページ)</a>	ルーティング プロトコルの VRF インスタンスを設定します。

## vrf (description)

設定される VRF インスタンスの簡単な説明を追加するには、VRF コンフィギュレーション モードで **vrf (description)** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

**vrf vrf-name [description]**

**no vrf vrf-name [description]**

### 構文の説明

<i>vrf-name</i>	VRF インスタンスの名前。
<b>description</b>	(任意) VRF インスタンスの説明を指定します。

### 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

VRF コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

説明行は最大 244 文字です。

### タスク ID

タスク ID	操作
ip services	読み取り、書き込み



## 例

次に、**vrf (description)** コマンドを使用して VRF インスタンスに説明を挿入する例を示します。

```
RP/0/RSP0/CPU0:router# config  
RP/0/RSP0/CPU0:router(config)# vrf v1  
RP/0/RSP0/CPU0:router(config-vrf)# description client
```

## 関連コマンド

コマンド	説明
<a href="#">vrf, (676 ページ)</a>	ルーティング プロトコルの VRF インスタンスを設定します。

## vrf (mhost)

特定の VRF のマルチキャストのデフォルト インターフェイスをホスト スタックからパケットを送受信するように設定するには、VRF コンフィギュレーションモードで **vrf (mhost)** コマンドを使用します。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。

**vrf** *vrf-name* [**mhost** {**ipv4** **ipv6**} **interface**]

**no vrf** *vrf-name* [**mhost** {**ipv4** **ipv6**} **interface**]

### 構文の説明

<i>vrf-name</i>	VRF インスタンスの名前。
<b>mhost</b>	(任意) マルチキャスト ホスト スタック オプションをイネーブルにします。
<b>ipv4</b>	IPv4 アドレスを指定します。
<b>ipv6</b>	IPv6 アドレスを指定します。
<b>interface</b>	デフォルトのマルチキャスト インターフェイスを指定します。

### コマンド デフォルト

なし

### コマンド モード

VRF コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

デフォルトのインターフェイスは、設定されている vrf に属する必要があります。

## タスク ID

タスク ID	操作
ip services	読み取り、書き込み

## 例

次に、**vrf (mhost)** コマンドを使用してVRFをマルチキャストのデフォルトインターフェイスとして設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# configvrf 101  
RP/0/RSP0/CPU0:router(config-vrf)# vrf clientmhost ipv4 default-interface loop101
```

## 関連コマンド

コマンド	説明
<a href="#">vrf, (676 ページ)</a>	ルーティング プロトコルの VRF インスタンスを設定します。

## vrf mode

VRF の **big** モードをイネーブルにするには、グローバル コンフィギュレーション モードで **vrf mode** コマンドを使用します。VRF の **big** モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

**mode big**

**no mode big**

### 構文の説明

<b>mode big</b>	VRF の <b>mode big</b> は、64 K を超えるプレフィックスの最大規模を設定します。
-----------------	--

### コマンド デフォルト

デフォルトでは、VRF の **big** モードはディセーブルになっています。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 4.1.1	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータが VRF の **big** モードに対して約 16 の VRF ID (デフォルトを含む) を保持します。既存のコミットされた **vrf** でのモード変更はお勧めできません。

### タスク ID

タスク ID	操作
ip-services	読み取り、書き込み

## 例

次に、big モードをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# vrf v1
RP/0/RSP0/CPU0:router(config-vrf)# mode big
RP/0/RSP0/CPU0:router(config-vrf)#
```

## 関連コマンド

コマンド	説明
<a href="#">show vrf</a> , ( <a href="#">673 ページ</a> )	VPN ルーティングおよび転送 (VRF) インスタンスのコンテンツを表示します。





## プレフィックス リスト コマンド

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ上で IP Version 4 (IPv4) および IP Version 6 (IPv6) のプレフィックス リストを設定するために使用する、Cisco IOS XR ソフトウェア コマンドについて説明します。

プレフィックスの概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』を参照してください。

- [clear prefix-list ipv4](#), 688 ページ
- [clear prefix-list ipv6](#), 690 ページ
- [copy prefix-list ipv4](#), 692 ページ
- [copy prefix-list ipv6](#), 694 ページ
- [deny \(プレフィックス リスト\)](#), 696 ページ
- [ipv4 prefix-list](#), 699 ページ
- [ipv6 prefix-list](#), 702 ページ
- [permit \(プレフィックス リスト\)](#), 704 ページ
- [remark \(プレフィックス リスト\)](#), 707 ページ
- [resequence prefix-list ipv4](#), 709 ページ
- [resequence prefix-list ipv6](#), 712 ページ
- [show prefix-list](#), 714 ページ
- [show prefix-list afi-all](#), 715 ページ
- [show prefix-list ipv4](#), 716 ページ
- [show prefix-list ipv4 standby](#), 718 ページ
- [show prefix-list ipv6](#), 720 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、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。 **clear prefix-list ipv4** コマンドは、指定した設定済みプレフィックスリストのカウントをクリアするために使用します。

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トをクリアするには、*sequence-number* 引数を使用します。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# 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/RSP0/CPU0:router# clear prefix-list ipv4 list3

RP/0/RSP0/CPU0:router# 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
```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696ページ)	IPv4 または IPv6 プレフィックスリストの拒否条件を設定します。
<a href="#">ipv4 prefix-list</a> , (699 ページ)	IPv4 プレフィックスリストを定義します。
<a href="#">permit (プレフィックスリスト)</a> , (704 ページ)	IPv4 または IPv6 プレフィックスリストの許可条件を設定します。
<a href="#">show prefix-list ipv4</a> , (716 ページ)	現在の IPv4 プレフィックスリストの設定を表示します。

## clear prefix-list ipv6

IP Version 6 (IPv6) 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、EXEC モードで **clear prefix-list ipv6** コマンドを使用します。

**clear prefix-list ipv6** *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) 特定のシーケンス番号のプレフィックスリストのカウンタをクリアします。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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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。指定した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 ipv6** 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	操作
acl	読み取り、書き込み

## 例

次に、IPv6 プレフィックスリストを表示し、プレフィックスリスト list3 上のシーケンス番号 60 のカウンタをクリアする例を示します。その後、再度 IPv6 プレフィックスリストを表示し、シーケンス番号 60 のカウンタがクリアされていることを確認します。

```
RP/0/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64 (5 matches)
 60 deny 3000:1::/64 (7 matches)

RP/0/RSP0/CPU0:router# clear prefix-list ipv6 list1 60
RP/0/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64 (5 matches)
 60 deny 3000:1::/64
```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696 ページ)	IPv4 または IPv6 プレフィックスリストの拒否条件を設定します。
<a href="#">ipv6 prefix-list</a> , (702 ページ)	IPv6 プレフィックスリストを定義します。
<a href="#">permit (プレフィックスリスト)</a> , (704 ページ)	IPv4 または IPv6 プレフィックスリストの許可条件を設定します。
<a href="#">show prefix-list ipv6</a> , (720 ページ)	現在の IPv6 プレフィックスリストの内容を表示します。

## copy prefix-list ipv4

既存の IP Version 4 (IPv4) プレフィックスリストのコピーを作成するには、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**copy prefix-list ipv4** コマンドは、設定済みプレフィックスリストをコピーするために使用します。*source-name* 引数でコピー対象のプレフィックスリストを指定し、*destination-name* 引数でコピー元プレフィックスリストの内容のコピー先を指定します。*destination-name* 引数は、一意の名前であることが必要です。*destination-name* 引数名がプレフィックスリストまたはアクセスリストに存在する場合、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、コピー元プレフィックスリストが存在することを確認した後、既存のプレフィックスリストが上書きされることを防ぐために、既存のリスト名をチェックします。

### タスク ID

タスク ID	操作
acl	読み取り、書き込み

タスク ID	操作
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/RSP0/CPU0:router# 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/RSP0/CPU0:router# copy prefix-list ipv4 list1 list4

RP/0/RSP0/CPU0:router# 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
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 prefix-list</a> , (699 ページ)	IPv4 プレフィックス リストを定義します。
<a href="#">show prefix-list ipv4</a> , (716 ページ)	現在の IPv4 プレフィックス リストの内容を表示します。

## copy prefix-list ipv6

既存の IP Version 6 (IPv6) プレフィックスリストのコピーを作成するには、EXEC モードで **copy prefix-list ipv6** コマンドを使用します。

**copy prefix-list ipv6** *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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**copy prefix-list ipv6** コマンドは、設定済みプレフィックスリストをコピーするために使用します。*source-name* 引数でコピー対象のプレフィックスリストを指定し、*destination-name* 引数でコピー元プレフィックスリストの内容のコピー先を指定します。*destination-name* 引数は、一意の名前であることが必要です。*destination-name* 引数名がプレフィックスリストまたはアクセスリストに存在する場合、プレフィックスリストはコピーされません。**copy prefix-list ipv6** コマンドは、コピー元プレフィックスリストが存在することを確認した後、既存のプレフィックスリストを上書きしないように、既存のリスト名を確認します。

### タスク ID

タスク ID	操作
acl	読み取り、書き込み

タスク ID	操作
filesystem	実行

例

次に、IPv6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、IPv6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/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
ipv6 prefix-list list2
 10 permit 5555::/24

RP/0/RSP0/CPU0:router# copy prefix-list ipv6 list1 list3

RP/0/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
ipv6 prefix-list list2
 10 permit 5555::/24
ipv6 prefix-list list3
 40 permit 2000:1::/64
 60 deny 3000:1::/6
```

関連コマンド

コマンド	説明
<a href="#">ipv6 prefix-list, (702 ページ)</a>	IPv6 プレフィックス リストを定義します。
<a href="#">show prefix-list ipv6, (720 ページ)</a>	現在の IPv6 プレフィックス リストの内容を表示します。

## deny (プレフィックスリスト)

IP Version 4 (IPv4) または IP Version 6 (IPv6) 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または IPv6 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 <b>sequence-number</b> 引数は、コマンドの <b>no</b> 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>ge value</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。 <i>length</i> の範囲の最小値です (長さの範囲の「から」の部分)。
<i>le value</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。 <i>length</i> の範囲の最大値です (長さの範囲の「まで」の部分)。
<i>eq value</i>	(任意) <i>length</i> の正確な値。

### コマンド デフォルト

IPv4 または IPv6 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  
IPv6 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**deny** コマンドは、パケットがプレフィックスリストに合格しない条件を指定するために使用します。

**ge**、**le**、**eq** の各キーワードを使用すると、照合するプレフィックス長の範囲を、*network/length* 引数よりも詳細に指定することができます。**ge** も **le** も指定しない場合、完全一致と見なされます。**ge** キーワードだけが指定されている場合、範囲は **ge value** から 32 と仮定されます。**le** 属性だけが指定されている場合、範囲は *length* から **le value** 引数までと見なされます。

指定する **ge value** または **le value** は、次の条件を満たしている必要があります。

*length* < **ge value** < **le value** <= 32 (IPv4 の場合)

*length* < **ge value** < **le value** <= 128 (IPv6 の場合)

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv6 prefix-list list2
RP/0/RSP0/CPU0:router(config-ipv6_pfx)#
70
```

## deny (プレフィックスリスト)

```
deny
2000:1::/64
ge 25
```

次に、list3 に拒否条件を追加し、**no** 形式のコマンドを使用して、シーケンス番号が 30 の条件を削除する例を示します。

```
RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list list3

RP/0/RSP0/CPU0:router(config-ipv6_pfx)# deny 2000:1::/64 ge 25
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# deny 3000:1::/64 le 32
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# deny 4000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP0/CPU0:router# 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

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list3
 10 deny 2000:1::/64 ge 25
 20 deny 3000:1::/64 le 32
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 prefix-list</a> , (699 ページ)	IPv4 プレフィックスリストを定義します。
<a href="#">ipv6 prefix-list</a> , (702 ページ)	IPv6 プレフィックスリストを定義します。
<a href="#">permit</a> (プレフィックスリスト), (704 ページ)	IPv4 または IPv6 プレフィックスリストの許可条件を設定します。
<a href="#">remark</a> (プレフィックスリスト), (707 ページ)	プレフィックスリストエン트리に関する有用な注釈を挿入します。
<a href="#">show prefix-list ipv4</a> , (716 ページ)	現在の IPv4 プレフィックスリストの内容を表示します。
<a href="#">show prefix-list ipv6</a> , (720 ページ)	現在の IPv6 プレフィックスリストの内容を表示します。

## ipv4 prefix-list

IP Version (IPv4) プレフィックス リストを名前で定義するには、グローバル コンフィギュレーション モードで **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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**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。このコマンドは、ルータをプレフィックス リスト コンフィギュレーション モードにします。このモードでは、**deny** または **permit** コマンドを使用して、許可または拒否アクセス条件を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。

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て、新しい IPv4 プレフィックス リスト ステートメント (**permit**、**deny**、**remark**) を追加できるようにするには、**resequence prefix-list ipv4** コマンドを使用します。最初のエン트리番号 (*base*) とステートメントのエン트리番号を分け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	操作
acl	読み取り、書き込み
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/RSP0/CPU0:router# 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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ipv4 prefix-list list2

RP/0/RSP0/CPU0:router(config-ipv4_pfx)#deny 172.18.30.154/16 ge 25
RP/0/RSP0/CPU0:router(config-ipv4_pfx)#
Uncommitted changes found, commit them? [yes]:
y

RP/0/RSP0/CPU0:router# 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
```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696 ページ)	IPv4 または IPv6 プレフィックスリストの拒否条件を設定します。
<a href="#">permit (プレフィックスリスト)</a> , (704 ページ)	IPv4 または IPv6 プレフィックスリストの許可条件を設定します。
<a href="#">remark (プレフィックスリスト)</a> , (707 ページ)	プレフィックスリスト エントリに関する有用な注釈を挿入します。
<a href="#">resequence prefix-list ipv4</a> , (709 ページ)	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。

コマンド	説明
<a href="#">show prefix-list ipv4</a> , (716 ページ)	現在の IPv4 プレフィックス リストの内容を表示します。

## ipv6 prefix-list

IP Version (IPv6) プレフィックス リストを名前で定義するには、グローバル コンフィギュレーション モードで **ipv6 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。

**ipv6 prefix-list name**

**no ipv6 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

IPv6 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。

### タスク ID

タスク ID	操作
acl	読み取り、書き込み
ipv6	読み取り、書き込み

### 例

次に、list-1 という名前のプレフィックス リストを作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router (config)# ipv6 prefix-list list-1
RP/0/RSP0/CPU0:router (config-ipv6-pfx)# 40 permit 2000:1::/64
RP/0/RSP0/CPU0:router (config-ipv6-pfx)# 60 deny 3000:1::/64
RP/0/RSP0/CPU0:router (config-ipv6-pfx)#
Uncommitted changes found, commit them? [yes]: y
```

```
RP/0/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64
RP/0/RSP0/CPU0:router#
```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696ページ)	IPv4 または IPv6 プレフィックス リストの拒否条件を設定します。
<a href="#">permit (プレフィックスリスト)</a> , (704 ページ)	IPv4 または IPv6 プレフィックス リストの許可条件を設定します。
<a href="#">remark (プレフィックスリスト)</a> , (707 ページ)	プレフィックス リスト エントリに関する有用な注釈を挿入します。
<a href="#">show prefix-list ipv6</a> , (720 ページ)	現在の IPv6 プレフィックス リストの内容を表示します。

## permit (プレフィックスリスト)

IP Version 4 (IPv4) または IP Version 6 (IPv6) 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または IPv6 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 <b>permit</b> 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)。
<i>ge value</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。 <i>length</i> の範囲の最小値です (長さの範囲の「から」の部分)。
<i>le value</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。 <i>length</i> の範囲の最大値です (長さの範囲の「まで」の部分)。
<i>eq value</i>	(任意) <i>length</i> の正確な値。

### 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

IPv6 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

パケットがプレフィックス リストに合格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、照合するプレフィックス長の範囲を、*network/length* 引数よりも詳細に指定することができます。**ge** も **le** も指定しない場合、完全一致と見なされます。**ge** キーワードだけが指定されている場合、範囲は **ge value** から 32 と仮定されます。**le** 属性だけが指定されている場合、範囲は *length* から **le value** 引数までと見なされます。

指定する **ge value** または **le value** は、次の条件を満たしている必要があります。

*length* < **ge value** < **le value** <= 32 (IPv4 の場合)

*length* < **ge value** < **le value** <= 128 (IPv6 の場合)

タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv4 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# permit 2000:1::/64 ge 25
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 le 32
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# permit 3000:1::/64 ge 25
Uncommitted changes found, commit them? [yes]: y
RP/0/RSP0/CPU0:router#show ipv6 prefix-list

ipv6 prefix-list list3
 10 permit 2000:1::/64 ge 25
```

## permit (プレフィックスリスト)

```

20 permit 3000:1::/64 le 32
30 permit 4000:1::/64 ge 25

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list list3
RP/0/RSP0/CPU0:router(config-ipv6_pfx)# no 30
Uncommitted changes found, commit them? [yes]: y
RP/0/RSP0/CPU0:router# 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

```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696 ページ)	IPv4 または IPv6 プレフィックス リストの拒否条件を設定します。
<a href="#">ipv4 prefix-list</a> , (699 ページ)	IPv4 プレフィックス リストを作成します。
<a href="#">ipv6 prefix-list</a> , (702 ページ)	IPv6 プレフィックス リストを作成します。
<a href="#">remark (プレフィックスリスト)</a> , (707 ページ)	プレフィックス リスト エントリに関する有用な注釈を挿入します。
<a href="#">show prefix-list ipv4</a> , (716 ページ)	現在の IPv4 プレフィックス リストの内容を表示します。
<a href="#">show prefix-list ipv6</a> , (720 ページ)	現在の IPv6 プレフィックス リストの内容を表示します。

## remark (プレフィックスリスト)

IP Version 4 (IPv4) または IP Version 6 (IPv6) プレフィックス リストに対して有用なコメント (注釈) を書き込むには、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またはIPv6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 リスト中の <b>remark</b> 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  
IPv6 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	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**remark** コマンドは、プレフィックス リストのエントリに対し有用なコメントを書き込むために使用します。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。

削除する注釈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せん。

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	操作
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/RSP0/CPU0:router(config)# ipv4 prefix-list deny-ten
RP/0/RSP0/CPU0:router(config-ipv4_pfx)# 10 remark Deny all routes with a prefix of 10/8
RP/0/RSP0/CPU0:router(config-ipv4_pfx)# 20 deny 10.0.0.0/8 le 32
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 40 permit 2000:1::/64
 60 deny 3000:1::/64

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ipv6 prefix-list list1
RP/0/RSP0/CPU0:router(config-ipv6-pfx)# 10 remark use from july23 forward
RP/0/RSP0/CPU0:router(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/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 remark use from july23 forward
 40 permit 2000:1::/64
 60 deny 3000:1::/64
```

## 関連コマンド

コマンド	説明
<a href="#">ipv4 prefix-list</a> , (699 ページ)	プレフィックスリストにエントリを作成します。
<a href="#">resequence prefix-list ipv4</a> , (709 ページ)	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。
<a href="#">show prefix-list ipv4</a> , (716 ページ)	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します。

## resequence prefix-list ipv4

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て、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、EXEC モードで **resequence prefix-list ipv4** を使用します。

**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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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するエントリの間には **permit**、**deny**、**remark** のいずれかの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。最初のエントリ番号 (*base*) とステートメントのエントリ番号を分け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	操作
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/RSP0/CPU0:router# 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/RSP0/CPU0:router# 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/RSP0/CPU0:router# 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
```

## 関連コマンド

コマンド	説明
<a href="#">deny (プレフィックスリスト)</a> , (696ページ)	IPv4 または IPv6 プレフィックスリストの拒否条件を設定します。
<a href="#">permit (プレフィックスリスト)</a> , (704ページ)	IPv4 または IPv6 プレフィックスリストの許可条件を設定します。

コマンド	説明
remark (プレフィックスリスト) , (707 ページ)	プレフィックスリスト エントリに関する有用な注釈を挿入します。
show prefix-list ipv4, (716 ページ)	現在の IPv4 プレフィックス リストの内容を表示します。

## resequence prefix-list ipv6

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て、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、EXEC モードで **resequence prefix-list ipv6** を使用します。

**resequence prefix-list ipv6** *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 2147483644 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。

### コマンド デフォルト

*base*: 10  
*increment*: 10

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

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 IPv6 プレフィックスリストの連続するエントリの間に **permit**、**deny**、**remark** のいずれかのステートメントを追加するには、**resequence prefix-list ipv6** コマンドを使用します。最初のエントリ番号 (*base*) とステートメントのエントリ番号を分け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**


---

**操作**


---

acl

---

読み取り、書き込み

---

**例**

次に、プレフィックスリスト 1 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/RSP0/CPU0:router# show prefix-list ipv6
ipv6
prefix-list list1
 10 permit 2000:1::
/16 le 24
 20 permit 3000:1::/16 le 32
 20 permit 172.18.0.0/16
 30 deny 3000:1::
/16 ge 25
ipv6
prefix-list list2
 10 deny 4000:1::
/16 ge 25

RP/0/RSP0/CPU0:router# resequence prefix-list ipv4 list1 10 30

RP/0/RSP0/CPU0:
Apr  4 02:29:39.513 : ipv6_acl_action_edm
[183]: %LIBTARCFG-6-COMMIT
: Configuration committed by user 'UNKNOWN'.  Use 'show commit changes 10000000
24' to view the changes.
```

## 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、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
acl	読み取り

### 例

次に、**show prefix-list** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list
```

## 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、EXECモードで**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、キーワードと引数はありません。

#### 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

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
acl	読み取り

#### 例

次に、**show prefix-list afi-all** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list afi-all
```

## show prefix-list ipv4

現在の IP Version 4 (IPv4) プレフィックスリストの内容を表示するには、EXEC モードで **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。
<b>summary</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

すべての IPv4 プレフィックスリストの内容を表示するには、**show prefix-list ipv4** コマンドを使用します。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要約を表示するには、**summary** キーワードを使用します。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# 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
```

次に、*list-name* 引数を使用して、プレフィックスリスト list1 を表示する例を示します。

```
RP/0/RSP0/CPU0:router# 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
```

次に、*list-name* 引数と *sequence-number* 引数を使用して、プレフィックスリスト list1 のシーケンス番号 10 を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list ipv4 list1 30

ipv4 prefix-list list1
 30 deny 172.24.20.164/16 ge 25
```

関連コマンド

コマンド	説明
<a href="#">clear prefix-list ipv4, (688 ページ)</a>	IPv4 プレフィックスリストに対するヒットカウントをリセットします。
<a href="#">ipv4 prefix-list, (699 ページ)</a>	IPv4 プレフィックスリストを定義します。
<a href="#">show prefix-list ipv6, (720 ページ)</a>	現在の IPv6 プレフィックスリストの内容を表示します。

## 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、EXEC モードで **show access-lists ipv4 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

<i>prefix-list name</i>	(任意) 特定の IPv4 プレフィックス リストの名前。 <b>prefix-list-name</b> 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。
<b>summary</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show prefix-list ipv4 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	操作
	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/RSP0/CPU0:router# show prefix-list ipv4 standby summary
Prefix List Summary:
  Total Prefix Lists configured:      2
  Total Prefix List entries configured : 6
```

## show prefix-list ipv6

現在の IP Version 6 (IPv6) プレフィックスリストの内容を表示するには、EXEC モードで **show prefix-list ipv6** コマンドを使用します。

**show prefix-list ipv6** [*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。
<b>summary</b>	(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 IPv6 プレフィックスリストが表示されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**show prefix-list ipv6** 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 IPv6 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要約を表示するには、**summary** キーワードを使用します。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# show prefix-list ipv6

ipv6 prefix-list list1
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
ipv6 prefix-list list2
 10 permit 2000::/24
```

次に、*list-name* 引数を使用して、プレフィックスリスト list1 を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list ipv6 list1

ipv6 prefix-list list1
 10 permit 5555::/24
 20 deny 3000::/24
 30 permit 2000::/24
```

次に、*list-name* 引数と *sequence-number* 引数を使用して、プレフィックスリスト list1 のシーケンス番号 10 を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list ipv6 list1 10

ipv6 prefix-list abc
 10 permit 5555::/24
```

次に、プレフィックスリストの内容の要約を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show prefix-list ipv6 summary

Prefix List Summary:
  Total Prefix Lists configured:      2
  Total Prefix List entries configured: 2
```

## 関連コマンド

コマンド	説明
<a href="#">clear prefix-list ipv6</a> , (690 ページ)	IPv4 プレフィックスリストに対するヒットカウントをリセットします。
<a href="#">copy prefix-list ipv6</a> , (694 ページ)	既存の IPv6 プレフィックスリストのコピーを作成します。
<a href="#">ipv6 prefix-list</a> , (702 ページ)	IPv6 プレフィックスリストを作成します。

■ `show prefix-list ipv6`



## トランスポート スタック コマンド

この章では、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータのトランスポート スタック（ノンストップルーティング（NSR）、TCP、ユーザデータグラムプロトコル（UDP）、RAW）に関する機能の設定とモニタに使用する Cisco IOS XR ソフトウェアコマンドを説明します。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、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*』の「*Configuring Transports on Cisco ASR 9000 Series Routers*」設定モジュールを参照してください。

- [clear nsr ncd client, 725 ページ](#)
- [clear nsr ncd queue, 727 ページ](#)
- [clear raw statistics pcb, 730 ページ](#)
- [clear tcp nsr client, 732 ページ](#)
- [clear tcp nsr pcb, 734 ページ](#)
- [clear tcp nsr session-set, 737 ページ](#)
- [clear tcp nsr statistics client, 739 ページ](#)
- [clear tcp nsr statistics pcb, 741 ページ](#)
- [clear tcp nsr statistics session-set, 744 ページ](#)
- [clear tcp nsr statistics summary, 746 ページ](#)
- [clear tcp pcb, 748 ページ](#)
- [clear tcp statistics, 750 ページ](#)
- [clear udp statistics, 752 ページ](#)
- [forward-protocol udp, 754 ページ](#)
- [nsr process-failures switchover, 756 ページ](#)
- [service tcp-small-servers, 757 ページ](#)

- [service udp-small-servers, 759 ページ](#)
- [show nsr ncd client, 761 ページ](#)
- [show nsr ncd queue, 764 ページ](#)
- [show raw brief, 766 ページ](#)
- [show raw detail pcb, 768 ページ](#)
- [show raw extended-filters, 770 ページ](#)
- [show raw statistics pcb, 773 ページ](#)
- [show tcp brief, 776 ページ](#)
- [show tcp detail, 778 ページ](#)
- [show tcp extended-filters, 780 ページ](#)
- [show tcp statistics, 782 ページ](#)
- [show tcp nsr brief, 784 ページ](#)
- [show tcp nsr client brief, 787 ページ](#)
- [show tcp nsr detail client, 789 ページ](#)
- [show tcp nsr detail pcb, 791 ページ](#)
- [show tcp nsr detail session-set, 794 ページ](#)
- [show tcp nsr session-set brief, 796 ページ](#)
- [show tcp nsr statistics client, 799 ページ](#)
- [show tcp nsr statistics pcb, 801 ページ](#)
- [show tcp nsr statistics session-set, 804 ページ](#)
- [show tcp nsr statistics summary, 806 ページ](#)
- [show udp brief, 808 ページ](#)
- [show udp detail pcb, 810 ページ](#)
- [show udp extended-filters, 812 ページ](#)
- [show udp statistics, 814 ページ](#)
- [tcp mss, 816 ページ](#)
- [tcp path-mtu-discovery, 818 ページ](#)
- [tcp selective-ack, 820 ページ](#)
- [tcp synwait-time, 822 ページ](#)
- [tcp timestamp, 823 ページ](#)
- [tcp window-size, 825 ページ](#)

## clear nsr ncd client

ノンストップルーティング (NSR) コンシューマデマルチプレクサ (NCD) の指定されたクライアントまたはすべてのクライアントのカウンタをクリアするには、EXEC モードで **clear nsr ncd client** コマンドを使用します。

**clear nsr ncd client** {*PID value*| **all**} [**location** *node-id*]

### 構文の説明

<i>PID value</i>	カウンタをクリアする必要があるクライアントのプロセス ID 値。範囲は 0 ~ 4294967295 です。
<b>all</b>	すべての NCD クライアントのカウンタをクリアします。
<b>location</b> <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

*node-id* 引数のデフォルト値は、コマンドを実行している現在のノードです。 *PID value* 引数にはデフォルト値はありません。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

一部の NSR 対応アプリケーションのアクティブインスタンスとスタンバイインスタンスは、2つのキューを使用して通信を行います。このようなアプリケーションは、このキューで多重化されます。NSR コンシューマデマルチプレクサ (NCD) は受信側で逆多重化サービスを提供するプロセスです。

**clear nsr ncd client** コマンドを使用して、トラフィック上の問題を解決できます。既存のカウンタをクリアする場合は、差分変更の監視に役立ちます。

## タスク ID

タスク ID	操作
transport	実行

## 例

次の例では、すべての NCD クライアントの全カウンタをクリアする方法を示しています。

```
RP/0/RSP0/CPU0:router# clear nsr ncd client all
RP/0/RSP0/CPU0:router# show nsr ncd client all

Client PID                : 3874979
Client Protocol           : TCP
Client Instance           : 1
Total packets received    : 0
Total acks received       : 0
Total packets/acks accepted : 0
Errors in changing packet ownership : 0
Errors in setting application offset : 0
Errors in enqueueing to client : 0
Time of last clear        : Sun Jun 10 14:43:44 20

RP/0/RSP0/CPU0:router# show nsr ncd client brief

Pid   Protocol  Instance  Total   Total   Accepted
      Packets Acks      Packets Acks      Packets/Acks
3874979 TCP        1         0     0         0
```

## 関連コマンド

コマンド	説明
<a href="#">clear nsr ncd queue, (727 ページ)</a>	NSR コンシューマ デマルチプレクサ (NCD) キューのカウンタをクリアします。
<a href="#">show nsr ncd client, (761 ページ)</a>	NSR コンシューマ デマルチプレクサ (NCD) のクライアントに関する情報を表示します。
<a href="#">show nsr ncd queue, (764 ページ)</a>	ノンストップルーティング (NSR) コンシューマ キューおよびディスパッチ (QAD) キューに関する情報を表示します。

## clear nsr ncd queue

ノンストップルーティング (NSR) コンシューマデマルチプレクサ (NCD) キューのカウンタをクリアするには、EXEC モードで **clear nsr ncd queue** コマンドを使用します。

**clear nsr ncd queue** {all| high| low} [**location** *node-id*]

### 構文の説明

<b>all</b>	すべての NCD キューのカウンタをクリアします。
<b>high</b>	優先度高の NCD キューのカウンタをクリアします。
<b>low</b>	優先度低の NCD キューのカウンタをクリアします。
<b>location</b> <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	実行

## 例

次の例では、すべての NCD キューのカウンタをクリアする方法を示しています。

```
RP/0/RSP0/CPU0:router# clear nsr ncd queue all
RP/0/RSP0/CPU0:router# show nsr ncd queue all

Queue Name                : NSR_LOW
Total packets received    : 0
Total packets accepted    : 0
Errors in getting datagram offset : 0
Errors in getting packet length : 0
Errors in calculating checksum : 0
Errors due to bad checksum : 0
Errors in reading packet data : 0
Errors due to bad NCD header : 0
Drops due to a non-existent client : 0
Errors in changing packet ownership : 0
Errors in setting application offset : 0
Errors in enqueueing to client : 0
Time of last clear        : Sun Jun 10 14:44:38 2007

Queue Name                : NSR_HIGH
Total packets received    : 0
Total packets accepted    : 0
Errors in getting datagram offset : 0
Errors in getting packet length : 0
Errors in calculating checksum : 0
Errors due to bad checksum : 0
Errors in reading packet data : 0
Errors due to bad NCD header : 0
Drops due to a non-existent client : 0
Errors in changing packet ownership : 0
Errors in setting application offset : 0
Errors in enqueueing to client : 0
Time of last clear        : Sun Jun 10 14:44:38 2007

RP/0/RSP0/CPU0:router# show nsr ncd queue brief

          Queue                Total      Accepted
          NSR_LOW              Packets      Packets
          NSR_HIGH              0          0
                                0          0
```

## 関連コマンド

コマンド	説明
<a href="#">clear nsr ncd client</a> , (725 ページ)	NSR コンシューマ デマルチプレクサ (NCD) クライアントのカウンタをクリアします。
<a href="#">nsr process-failures switchover</a> , (756 ページ)	リカバリアクションとしてフェールオーバーを構成し、アクティブインスタンスがスタンバイルートプロセッサ (RP) に切り替わるか、分散ルートプロセッサ (DRP) がノンストップルーティング (NSR) を維持するようにします。



コマンド	説明
<a href="#">show nsr ncd client</a> , (761 ページ)	NSR コンシューマ デマルチプレクサ (NCD) のクライアントに関する情報を表示します。
<a href="#">show nsr ncd queue</a> , (764 ページ)	ノンストップルーティング (NSR) コンシューマ キューおよびディスパッチ (QAD) キューに関する情報を表示します。

## clear raw statistics pcb

1つのRAW 接続あるいはすべてのRAW 接続の統計をクリアするには、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**} [**location node-id**]

### 構文の説明

<b>all</b>	すべてのRAW 接続の統計をクリアします。
<b>pcb-address</b>	特定のRAW 接続の統計をクリアします。
<b>location node-id</b>	(オプション) 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**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 Protocol Control Block (PCB; プロトコルコントロールブロック) アドレスを入力します。 **show raw brief** コマンドを使用すると、PCB アドレスを取得します。

**location** キーワードと *node-id* 引数を使用すると、指定されたノードのRAW 統計をクリアします。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear raw statistics pcb 0x80553b0
RP/0/RSP0/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/RSP0/CPU0:router# clear raw statistics pcb all
RP/0/RSP0/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
```

## 関連コマンド

コマンド	説明
<a href="#">show raw brief</a> , (766 ページ)	アクティブ RAW IP ソケットに関する情報を表示します。
<a href="#">show raw statistics pcb</a> , (773 ページ)	1 つの RAW 接続またはすべての RAW 接続の統計を表示します。

## clear tcp nsr client

指定されたクライアントが所有するすべてのセッション上のノンストップルーティング (NSR) を停止するには、EXEC モードで **clear tcp nsr client** コマンドを使用します。

**clear tcp nsr client** {*ccb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>ccb-address</i>	NSR クライアントの Client Control Block (CCB; クライアント コントロールブロック)。
<b>all</b>	すべてのクライアントを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのクライアント情報を表示します。 <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

ロケーションのデフォルト値は、コマンドを実行している現在のノードに設定されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

**show tcp nsr client** コマンドの出力を使用すると、任意のクライアントの CCB を検索します。

**clear tcp nsr client** コマンドを使用すると、1つのクライアントまたはすべてのクライアントが所有する NSR セッションを停止します。また、セッションのアクティビティがフリーズした場合は、**clear tcp nsr client** コマンドを使用して、状況を回避します。

## タスク ID

タスク ID	操作
transport	実行

## 例

次の例では、ノンストップルーティング（NSR）クライアントの 0x482afacc をクリアする例を示しています。2つのセッションですでにNSRを起動している状態で、**clear tcp nsr client** コマンドを実行しました。**clear tcp nsr client** コマンドの実行後は、NSRは起動していません。

```
RP/0/RSP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name      Instance      Sets          Sessions/NSR Up Sessions
0x482c10e0   mpls_ldap     1             2             3/1
0x482afacc   mpls_ldap     2             1             2/2

RP/0/RSP0/CPU0:router# clear tcp nsr client 0x482afacc
RP/0/RSP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name      Instance      Sets          Sessions/NSR Up Sessions
0x482c10e0   mpls_ldap     1             2             3/1
0x482afacc   mpls_ldap     2             1             2/0
```

## 関連コマンド

コマンド	説明
<a href="#">nsr process-failures switchover, (756 ページ)</a>	リカバリアクションとしてフェールオーバーを構成し、アクティブインスタンスがスタンバイルートプロセッサ（RP）に切り替わるか、分散ルートプロセッサ（DRP）がノンストップルーティング（NSR）を維持するようにします。
<a href="#">show tcp nsr client brief, (787 ページ)</a>	異なるノードのTCPクライアントのノンストップルーティング（NSR）状態に関する概要情報を表示します。

## clear tcp nsr pcb

指定された接続またはすべての接続でノンストップルーティング (NSR) を停止するには、EXEC モードで **clear tcp nsr pcb** コマンドを使用します。

**clear tcp nsr pcb** {*pcb-address* | **all**} [**location** *node-id*]

### 構文の説明

<b>pcb-address</b>	特定の接続情報の PCB アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべての接続を指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードの接続情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RSP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

**show tcp nsr brief** コマンドの出力を使用して、任意の接続のプロトコル コントロール ブロック (PCB) を検索できます。

タスク ID

タスク ID	操作
transport	実行

例

次の例は、TCP 接続情報をクリアする例を示しています。

```

RP/0/RSP0/CPU0:router# show tcp nsr brief
PCB          Local Address  Foreign Address      NSR   RcvOnly
0x482d7470 10
.1.1.1:646    10
.1.1.2:14142      Up    No
0x482d2844 10
.1.1.1:646    10
.1.1.2:15539     Up    No
0x482d3bc0 10
.1.1.1:646    10
.1.1.2:25671     Up    No
0x482d4f3c 10
.1.1.1:646    10
.1.1.2:32319     Up    No
0x482d87ec 10
.1.1.1:646    10
.1.1.2:39592     Up    No
0x482cd670 10
.1.1.1:646    10
.1.1.2:43447     Up    No
0x482d14c8 10
.1.1.1:646    10
.1.1.2:45803     Up    No
0x482bdee4 10
.1.1.1:646    10
.1.1.2:55844     Up    No
0x482d62b8 10
.1.1.1:646    10
.1.1.2:60695     Up    No
0x482d0310 10
.1.1.1:646    10
.1.1.2:63007     Up    No

RP/0/RSP0/CPU0:router# clear tcp nsr pcb 0x482d7470
RP/0/RSP0/CPU0:router# clear tcp nsr pcb 0x482d2844
RP/0/RSP0/CPU0:router# show tcp nsr brief
PCB          Local Address  Foreign Address      NSR   RcvOnly
0x482d7470 10
.1.1.1:646    10
.1.1.2:14142      Down  No
0x482d2844 10
.1.1.1:646    10
.1.1.2:15539     Down  No
0x482d3bc0 10
.1.1.1:646    10
.1.1.2:25671     Up    No
0x482d4f3c 10
.1.1.1:646    10
.1.1.2:32319     Up    No
0x482d87ec 10
.1.1.1:646    10
.1.1.2:39592     Up    No
0x482cd670 10
.1.1.1:646    10

```

## clear tcp nsr pcb

```

.1.1.2:43447          Up    No
0x482d14c8 10
.1.1.1:646           10    Up    No
.1.1.2:45803          Up    No
0x482bdee4 10
.1.1.1:646           10    Up    No
.1.1.2:55844          Up    No
0x482d62b8 10
.1.1.1:646           10    Up    No
.1.1.2:60695          Up    No
0x482d0310 10
.1.1.1:646           10    Up    No
.1.1.2:63007          Up    No

```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr brief</a> , (784 ページ)	異なるノードの TCP 接続のキー ノンストップルーティング (NSR) 状態を表示します。
<a href="#">show tcp nsr detail pcb</a> , (791 ページ)	TCP 接続のノンストップルーティング (NSR) 状態に関する詳細情報を表示します。



## clear tcp nsr session-set

指定されたセッションセットまたはすべてのセッションセットの全セッションのノンストップルーティング（NSR）をクリアするには、EXEC モードで **clear tcp nsr session-set** コマンドを使用します。

**clear tcp nsr session-set** { *sscb-address* | **all** } [*location node-id*]

### 構文の説明

<i>sscb-address</i>	特定のセッションセット情報のセッションセットコントロールブロック（SSCB）アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべてのセッションセットを指定します。
<i>location node-id</i>	（オプション）指定されたノードのセッションセット情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンドモード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

**show tcp nsr session-set brief** コマンドの出力を使用すると、任意のセッションセットの SSCB を検索します。

## タスク ID

タスク ID	操作
transport	実行

## 例

次の例では、セッション セット情報をクリアする例を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name      Instance  Sets      Sessions/NSR Up Sessions
0x482b5ee0   mpls_ldp       1         1         10/10

RP/0/RSP0/CPU0:router# clear tcp nsr client 0x482b5ee0
RP/0/RSP0/CPU0:router# show tcp nsr client brief

CCB          Proc Name      Instance  Sets      Sessions/NSR Up Sessions
0x482b5ee0   mpls_ldp       1         1         10/0
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr detail session-set, (794 ページ)</a>	異なるノードのセッションセットのノンストップルーティング (NSR) 状態に関する詳細情報を表示します。
<a href="#">show tcp nsr session-set brief, (796 ページ)</a>	異なるノードのノンストップルーティング (NSR) 状態のセッションセットに関する概要情報を表示します。

# clear tcp nsr statistics client

クライアントのノンストップルーティング (NSR) 統計をクリアするには、EXECモードで、**clear tcp nsr statistics client** コマンドを使用します。

**clear tcp nsr statistics client** {*ccb-address*| **all**} [**location** *node-id*]

## 構文の説明

<i>ccb-address</i>	任意のクライアントのクライアントコントロールブロック (CCB) たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべてのクライアントを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのクライアント情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

## タスク ID

タスク ID	操作
transport	実行

## 例

次の例では、NSR クライアントの統計をクリアする例を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics client all

=====
CCB: 0x482b5ee0
Name: mpls_ldp, Job ID: 365
Connected at: Thu Aug 16 18:20:32 2007

Notification Statistics :   Queued   Failed   Delivered Dropped
Init-Sync Done          :         2         0         2         0
Replicated Session Ready:         0         0         0         0
Operational Down       :        12         0        12         0
Last clear at: Never Cleared

RP/0/RSP0/CPU0:router# clear tcp nsr statistics client all

RP/0/RSP0/CPU0:router# show tcp nsr statistics client all

=====
CCB: 0x482b5ee0
Name: mpls_ldp, Job ID: 365
Connected at: Thu Aug 16 18:20:32 2007

Notification Statistics :   Queued   Failed   Delivered Dropped
Init-Sync Done          :         0         0         0         0
Replicated Session Ready:         0         0         0         0
Operational Down       :         0         0         0         0
Last clear at: Thu Aug 16 18:28:38 2007
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr statistics client</a> , ( <a href="#">799 ページ</a> )	クライアントのノンストップルーティング (NSR) 統計を表示します。

## clear tcp nsr statistics pcb

TCP 接続のノンストップルーティング (NSR) 統計をクリアするには、EXEC モードで **clear tcp nsr statistics pcb** コマンドを使用します。

**clear tcp nsr statistics pcb** {*pcb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>pcb-address</i>	特定の接続情報の PCB アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべての接続を指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードの接続情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	実行

例

次の例では、TCP 接続の NSR 統計をクリアする例を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics pcb 0x482d14c8

=====
PCB 0x482d14c8
Number of times NSR went up: 1
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times switch-over occurred : 0
IACK RX Message Statistics:
  Number of iACKs dropped because SSO is not up      : 0
  Number of stale iACKs dropped                     : 1070
  Number of iACKs not held because of an immediate match : 98
TX Message Statistics:
  Data transfer messages:
    Sent 317, Dropped 0, Data (Total/Avg.) 2282700/7200
    Rcvd 0
      Success      : 0
      Dropped (Trim) : 0
  Segmentation instructions:
    Sent 1163, Dropped 0, Units (Total/Avg.) 4978/4
    Rcvd 0
      Success      : 0
      Dropped (Trim) : 0
      Dropped (TCP) : 0
  NACK messages:
    Sent 0, Dropped 0
    Rcvd 0
      Success      : 0
      Dropped (Data snd): 0
  Cleanup instructions :
    Sent 8, Dropped 0
    Rcvd 0
      Success      : 0
      Dropped (Trim) : 0
Last clear at: Never cleared

RP/0/RSP0/CPU0:router# clear tcp nsr statistics pcb 0x482d14c8
RP/0/RSP0/CPU0:router# show tcp nsr statistics pcb 0x482d14c8

=====
PCB 0x482d14c8
Number of times NSR went up: 0
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times switch-over occurred : 0
IACK RX Message Statistics:
  Number of iACKs dropped because SSO is not up      : 0
  Number of stale iACKs dropped                     : 0
  Number of iACKs not held because of an immediate match : 0
TX Message Statistics:
  Data transfer messages:
    Sent 0, Dropped 0, Data (Total/Avg.) 0/0
    Rcvd 0
      Success      : 0
      Dropped (Trim) : 0
  Segmentation instructions:
    Sent 0, Dropped 0, Units (Total/Avg.) 0/0
    Rcvd 0
      Success      : 0
      Dropped (Trim) : 0
      Dropped (TCP) : 0
  NACK messages:
    Sent 0, Dropped 0
    Rcvd 0
      Success      : 0
      Dropped (Data snd): 0
```

```
Cleanup instructions      :
  Sent 0, Dropped 0
  Rcvd 0
    Success                : 0
    Dropped (Trim)        : 0
Last clear at: Thu Aug 16 18:32:12 2007
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr statistics pcb</a> , ( <a href="#">801 ページ</a> )	特定のプロトコル コントロール ブロック (PCB) のノンストップルーティング (NSR) 統計を表示します。

## clear tcp nsr statistics session-set

セッションセットのノンストップルーティング (NSR) 統計をクリアするには、EXEC モードで **clear tcp nsr statistics session-set** コマンドを使用します。

**clear tcp nsr statistics session-set** *{sscb-address| all}* [**location** *node-id*]

### 構文の説明

<i>sscb-address</i>	特定のセッションセット情報のセッションセットコントロールブロック (SSCB) アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべてのセッションセットを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのセッションセット情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	実行



例 次の例では、セッションセットの NSR 統計をクリアする例を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics session-set all

=====Session Set Stats =====
SSCB 0x482b6684, Set ID: 1
Number of times init-sync was attempted :3
Number of times init-sync was successful :3
Number of times init-sync failed       :0
Number of times switch-over occurred   :0
Last clear at: Never Cleared

RP/0/RSP0/CPU0:router# clear tcp nsr statistics session-set all
RP/0/RSP0/CPU0:router# show tcp nsr statistics session-set all

=====Session Set Stats =====
SSCB 0x482b6684, Set ID: 1
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed       :0
Number of times switch-over occurred   :0
Last clear at: Thu Aug 16 18:37:00 2007
```

#### 関連コマンド

コマンド	説明
<a href="#">show tcp nsr statistics session-set, (804 ページ)</a>	セッションセットのノンストップルーティング (NSR) 統計を表示します。

## clear tcp nsr statistics summary

ノンストップルーティング (NSR) 統計サマリーをクリアするには、EXEC モードで **clear tcp nsr statistics summary** コマンドを使用します。

**clear tcp nsr statistics summary** [*location node-id*]

### 構文の説明

**location node-id** (オプション) 指定されたノードの統計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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない可能性がある場合は、に問い合わせてください。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	実行

### 例

次の例では、サマリー統計をクリアする方法を示しています。

```
RP/0/RSP0/CPU0:router# clear tcp nsr statistics summary
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr statistics summary</a> , <a href="#">(806 ページ)</a>	すべての TCP セッションのノンストップルーティング (NSR) サマリー統計を表示します。

## 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、EXEC モードで **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。
<b>all</b>	開いている TCP 接続をすべてクリアします。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

ハングした TCP 接続をクリアする場合は、**clear tcp pcb** コマンドが便利です。 [show tcp brief](#) (776 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** コマンドを使用する場合は、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	操作
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/RSP0/CPU0:router# clear tcp pcb 60B75E48
```

#### 関連コマンド

コマンド	説明
<a href="#">show tcp brief</a> , ( <a href="#">776 ページ</a> )	TCP サマリー テーブルを表示します。

# clear tcp statistics

TCP 統計をクリアするには、EXEC モードで **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

<b>pcb all</b>	(オプション) すべての TCP 接続の統計をクリアします。
<b>pcb</b> <i>pcb-address</i>	(オプション) 特定の TCP 接続の統計をクリアします。
<b>summary</b>	(オプション) 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。
<b>location</b> <i>node-id</i>	(オプション) 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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**clear tcp statistics** コマンドを使用すると、TCP 統計をクリアします。 [show tcp statistics](#)、(782 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、指定されたノードの TCP 統計をクリアできます。

## タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear tcp statistics
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp statistics</a> , (782 ページ)	TCP 統計を表示します。

## 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、EXEC モードで **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

<b>pcb</b> <i>all</i>	すべての UDP 接続の統計をクリアします。
<b>pcb</b> <i>pcb-address</i>	特定の UDP 接続の統計をクリアします。
<b>summary</b>	UDP サマリー統計をクリアします。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**clear udp statistics** コマンドを使用すると、UDP 統計をクリアします。 [show udp statistics](#), (814 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、指定されたノードの UDP 統計をクリアできます。



## タスク ID

タスク ID	操作
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/RSP0/CPU0:router# clear udp statistics summary
```

## 関連コマンド

コマンド	説明
<a href="#">show udp statistics, (814 ページ)</a>	UDP 統計を表示します。

## forward-protocol udp

ブロードキャストパケットとして受信する任意のユーザ データグラム プロトコル (UDP) データグラムを指定されたヘルパー アドレスに転送するようにシステムを設定するには、グローバル コンフィギュレーション モードで **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状態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。

```
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。範囲は 1 ~ 65535 です。
<b>disable</b>	IP 転送プロトコル UDP をディセーブルにします。
<b>domain</b>	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。
<b>nameserver</b>	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。
<b>netbios-dgm</b>	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。
<b>netbios-ns</b>	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。
<b>tacacs</b>	UDP ブロードキャスト パケットを TACACS (49) に転送します。
<b>tftp</b>	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

ディセーブル

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**forward-protocol udp** コマンドを使用すると、受信インターフェイスで受信した UDP ブロードキャスト パケットを指定されたヘルパー 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。サービス処理の実行が可能なホストまたはネットワーク デバイスの IP アドレスを使用して、**helper-address** コマンドを設定します。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。

各転送する UDP ポートに対して、**forward-protocol udp** コマンドを 1 つ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**)、あるい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	操作
transport	読み取り、書き込み

## 例

次の例では、受信 MgmtEth インターフェイス 0/0/CPU0/0 で受信したポート 53 またはポート 69 を使用して、すべての UDP ブロードキャスト パケットを 172.16.0.1 に転送するように指定する方法を示しています。UDP ブロードキャストを受信する MgmtEth インターフェイス 0/0/CPU0/0 は、ヘルパー アドレス 172.16.0.1 に設定されています。これは、UDP データグラムの転送先アドレスです。

```
RP/0/RSP0/CPU0:router(config)# forward-protocol udp domain disable
RP/0/RSP0/CPU0:router(config)# forward-protocol udp tftp disable
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/0/CPU0/0
RP/0/RSP0/CPU0:router(config-if)# ipv4 helper-address 172.16.0.1
```

## nsr process-failures switchover

リカバリ アクションとしてフェールオーバーを構成し、アクティブ インスタンスがスタンバイ ルート プロセッサ (RP) に切り替わるか、分散ルート プロセッサ (DRP) がノンストップルー ティング (NSR) を維持するように設定するには、グローバル コンフィギュレーションで、**nsr process-failures switchover** 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。

**nsr process-failures switchover**

**no nsr process-failures switchover**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

設定していない場合は、アクティブ TCP あるいはアプリケーション (たとえば、LDP、BGP) のプロセス障害によって、セッションが停止し、NSR が提供されない可能性があります。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
transport	読み取り、書き込み

### 例

次の例では、**nsr process-failures switchover** コマンドを使用する方法を示しています。

```
RP/0/RSP0/CPU0:router (config)# nsr process-failures switchover
```

## 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、グローバル コンフィギュレーション モードで **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

<b>ip4</b>	IPv4 小規模サーバを指定します。
<b>ipv6</b>	IPv6 小規模サーバを指定します。
<b>max-servers</b>	(オプション) 許容 TCP 小規模サーバ数を設定します。
<b>number</b>	(オプション) 数値です。範囲は 1 ~ 2147483647 です。
<b>no-limit</b>	(オプション) 許容 TCP サーバ数を無制限に設定します。
<b>access-list-name</b>	(オプション) 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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	操作
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/RSP0/CPU0:router (config)# service ipv4 tcp-small-servers max-servers 5 acl100
```

## 関連コマンド

コマンド	説明
<a href="#">service udp-small-servers, (759 ページ)</a>	ECHO などの小規模 UDP サーバをイネーブルにします。
show cinetd services	cinetd でプロセスが生成されるサービスを表示します。

## 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、グローバル コンフィギュレーション モードで **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

<b>ip4</b>	IPv4 小規模サーバを指定します。
<b>ipv6</b>	IPv6 小規模サーバを指定します。
<b>max-servers</b>	(オプション) 許容 UDP 小規模サーバ数を設定します。
<b>number</b>	(オプション) 数値です。範囲は 1 ~ 2147483647 です。
<b>no-limit</b>	(オプション) 許容UDP小規模サーバ数を無制限に設定します。
<b>access-list-name</b>	(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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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	操作
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/RSP0/CPU0:router(config)# service ipv6 udp-small-servers max-servers 10
```

#### 関連コマンド

コマンド	説明
<a href="#">service tcp-small-servers, (757 ページ)</a>	ECHO などの小規模 TCP サーバをイネーブルにします。



## show nsr ncd client

クライアントのノンストップルーティング (NSR) コンシューマデマルチプレクサ (NCD) に関する情報を表示するには、EXEC モードで **show nsr ncd client** コマンドを使用します。

**show nsr ncd client** {*PID value*| **all**| **brief**} [**location** *node-id*]

### 構文の説明

<i>PID value</i>	特定のクライアントのプロセス ID (PID) 情報です。範囲は 0 ~ 4294967295 です。
<b>all</b>	すべてのクライアントに関する詳細情報を表示します。
<b>brief</b>	すべてのクライアントに関する概要情報を表示します。
<b>location</b> <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、すべてのクライアントに関する詳細情報を示しています。

```
RP/0/RSP0/CPU0:router# show nsr ncd client all

Client PID                : 3874979
Client Protocol           : TCP
Client Instance           : 1
Total packets received    : 28
Total acks received       : 0
Total packets/acks accepted : 28
Errors in changing packet ownership : 0
Errors in setting application offset : 0
Errors in enqueueing to client : 0
Time of last clear        : Never cleared
```

次のサンプル出力では、すべてのクライアントに関する概要情報を示しています。

```
RP/0/RSP0/CPU0:router# show nsr ncd client brief

Pid      Protocol  Instance  Total  Total  Accepted
3874979  TCP        1         28    0      28
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 73 : show nsr ncd client コマンドのフィールドの説明

フィールド	説明
Client PID	クライアントプロセスのプロセス ID です。
Client Protocol	クライアントプロセスのプロトコルです。プロトコルは TCP、Open Shortest Path First (OSPF; オープンショーテストパスファースト)、BGP のいずれかです。
Client Instance	クライアントプロセスのインスタンス数。OSPF など複数のルーティングプロトコルのインスタンスを含めることができます。
Total packets received	パートナー ルートプロセッサ (RP) のパートナー スタックから受信した合計パケット数。

フィールド	説明
Total acks received	パートナー スタックに送信されるパケットのパートナー RP のパートナー スタックから受信する合計応答数。
Total packets/acks accepted	パートナー RP のパートナー スタックから受信する合計パケット数および応答数。
Errors in changing packet ownership	クライアントでのパケット キューイングの前に、NCD はパケットの所有権をクライアントの所有権に変更します。このカウンタは所有権変更時のエラーがある場合、エラーを追跡します。
Errors in setting application offset	クライアントでのパケット キューイングの前に、NCD はパケットのアプリケーション データのオフセットを設定します。必要に応じて、このカウンタはオフセット変更時のエラーがある場合、エラーを追跡します。
Errors in enqueueing to client	カウンタはすべてのキューイングエラーを追跡します。
Time of last clear	ユーザが前回クリアした統計。

## 関連コマンド

コマンド	説明
<a href="#">clear nsr ncd client</a> , (725 ページ)	NSR コンシューマ デマルチプレクサ (NCD) クライアントのカウンタをクリアします。
<a href="#">clear nsr ncd queue</a> , (727 ページ)	NSR コンシューマ デマルチプレクサ (NCD) キューのカウンタをクリアします。
<a href="#">show nsr ncd queue</a> , (764 ページ)	ノンストップルーティング (NSR) コンシューマ キューおよびディスパッチ (QAD) キューに関する情報を表示します。

## show nsr ncd queue

パートナー ルート プロセッサ (RP) のパートナー スタックと通信を行うために、ノンストップ ルーティング (NSR) アプリケーションが使用するキューに関する情報を表示するには、EXEC モードで **show nsr ncd queue** コマンドを使用します。

**show nsr ncd queue** {**all**|**brief**|**high**|**low**} [**location** *node-id*]

### 構文の説明

<b>all</b>	すべてのコンシューマ キューに関する詳細情報を表示します。
<b>brief</b>	すべてのコンシューマ キューに関する概要情報を表示します。
<b>high</b>	優先度高キューとディスパッチ (QAD) キューに関する情報を表示します。
<b>low</b>	低優先 QAD キューに関する情報を表示します。
<b>location</b> <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

タスク ID

タスク ID	操作
transport	読み取り

例

次のサンプル出力では、すべてのコンシューマ キューに関する概要情報を示しています。

```
RP/0/RSP0/CPU0:router# show nsr ncd queue brief
      Queue           Total      Accepted
      NSR_LOW         992       992
      NSR_HIGH         0         0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 74 : show nsr ncd queue コマンドのフィールドの説明

フィールド	説明
Total Packets	パートナースタックから受信する合計パケット数。
Accepted Packets	一部の検証タスクの実行後に許可された受信パケット数。
Queue	キュー名。NSR_HIGH と NSR_LOW は 2 つのキューがあります。NSR_HIGH キューの高優先度パケットフロー。NSR_LOW キューの低優先度パケットフロー。

関連コマンド

コマンド	説明
<a href="#">clear nsr ncd client, (725 ページ)</a>	NSR コンシューマ デマルチプレクサ (NCD) クライアントのカウンタをクリアします。
<a href="#">clear nsr ncd queue, (727 ページ)</a>	NSR コンシューマ デマルチプレクサ (NCD) キューのカウンタをクリアします。
<a href="#">show nsr ncd client, (761 ページ)</a>	NSR コンシューマ デマルチプレクサ (NCD) のクライアントに関する情報を表示します。

## 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、EXEC モードで **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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

オープンショーテストパスファースト (OSPF) や Protocol Independent Multicast (PIM; プロトコル独立マルチキャスト) 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** コマンドは短寿命 RAW IP ソケットを使用します。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	操作
transport	読み取り

例

次は、**show raw brief** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# 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              0.0.0.0        255
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 75: **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 ソケットに関する詳細情報を表示するには、EXEC モードで **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。
<b>all</b>	すべての RAW 接続の統計を表示します。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**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を表示します。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	操作
transport	読み取り



例

次は、**show raw detail pcb** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show raw detail pcb 0x807e89c
```

```
=====
PCB is 0x807e89c, Family: 2, PROTO: 89, VRF: 0x0
  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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 76 : **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 RAWIP ソケットに関する情報を表示するには、EXEC モードで **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

<b>interface-filter</b>	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。
<b>location</b> <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。
<b>paktype-filter</b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**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を表示します。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	操作
transport	読み取り

## 例

次は、**show raw extended-filters** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show raw extended-filters 0/0/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: 0x3fff
LPTS socket options: 0x0020
Packet Type Filters:
0
[220 pkts in]
3
[0 pkts in]
4
[0 pkts in]
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 77: **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。

フィールド	説明
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、EXEC モードで **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

<b>all</b>	すべての RAW 接続の統計を表示します。
<b>pcb-address</b>	指定された RAW 接続の統計を表示します。
<b>location node-id</b>	(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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**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。

**show raw brief** コマンドを使用すると、PCB アドレスを取得します。

**location** キーワードと *node-id* 引数を使用すると、指定されたノードの RAW 統計を表示します。

### タスク ID

タスク ID	操作
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/RSP0/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
```

この例では、すべての RAW 接続の統計が表示されます。

```
RP/0/RSP0/CPU0:router# show raw statistics pcb all

Statistics for PCB 0x805484c, Vrfid: 0x60000000
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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 78 : 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。

## 関連コマンド

コマンド	説明
<a href="#">clear raw statistics pcb</a> , (730 ページ)	1 つの RAW 接続またはすべての RAW 接続の統計をクリアします。
<a href="#">show raw brief</a> , (766 ページ)	アクティブ RAW IP ソケットに関する情報を表示します。

# show tcp brief

TCP 接続テーブルのサマリーを表示するには、EXEC モードで **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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次は、**show tcp brief** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show tcp brief

TCPChB      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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 79 : *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

#### 関連コマンド

コマンド	説明
<a href="#">clear tcp pcb, (748 ページ)</a>	TCP 接続をクリアします。

# show tcp detail

TCP 接続テーブルの詳細を表示するには、EXEC モードで **show tcp detail** コマンドを使用します。

**show tcp detail pcb [value| all]**

## 構文の説明

<b>pcb</b>	TCP 接続情報を表示します。
<b>value</b>	特定の接続情報を表示します。範囲は 0 ~ ffffffff です。
<b>all</b>	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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次は、**show tcp detail pcb all** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# 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、EXEC モードで **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

<b>location node-id</b>	(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。
<b>peer-filter</b>	(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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次は、特定のロケーション (0/0/CPU0) での、**show tcp extended-filters** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show tcp extended-filters location 0/0/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、EXEC モードで **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

<b>pcb</b> <i>pcb-address</i>	(オプション) 指定された接続の詳細統計を表示します。
<b>pcb all</b>	(オプション) すべての接続の詳細統計を表示します。
<b>summary</b>	(オプション) 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。
<b>location</b> <i>node-id</i>	(オプション) 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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次は、**show tcp statistics** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show tcp statistics pcb 0x08091bc8

Statistics for PCB 0x8091bc8, vrfid 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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 80 : **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。

## 関連コマンド

コマンド	説明
<a href="#">clear tcp statistics</a> , ( <a href="#">750 ページ</a> )	TCP 統計をクリアします。

## show tcp nsr brief

異なるノードの TCP 接続のキー ノンストップルーティング (NSR) 状態を表示するには、EXEC モードで **show tcp nsr brief** コマンドを使用します。

**show tcp nsr brief** [*location node-id*]

### 構文の説明

**location node-id** (オプション) 指定されたノードのすべての TCP セッションに関する情報を表示します。 *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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り



## 例

次のサンプル出力では、NSR カラムの各 TCP セッションの管理上および動作上の NSR 状態を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr brief
```

```
PCB          Local Address      Foreign Address      NSR   RcvOnly
0x482c6b8c 10
.1.1.1:646          10
.1.1.2:23945        Down No
0x482db564 10
.1.1.1:646          10
.1.1.2:25398        Down No
0x482844e0 10
.1.1.1:646          10
.1.1.2:25430        Down No
0x482c9284 10
.1.1.1:646          10
.1.1.2:37434        Down No
0x482d98c8 10
.1.1.1:646          10
.1.1.2:37895        Down No
0x482d6018 10
.1.1.1:646          10
.1.1.2:50616        Down No
0x482c7f08 10
.1.1.1:646          10
.1.1.2:55860        Down No
0x482dbab0 10
.1.1.1:646          10
.1.1.2:56656        Down No
0x482d7394 10
.1.1.1:646          10
.1.1.2:57365        Down No
0x482d854c 10
.1.1.1:646          10
.1.1.2:59927        Down No
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 81 : show tcp nsr 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 (PCB)。
Local Address	TCP 接続のローカルアドレスとポート。
Foreign Address	TCP 接続の外部アドレスとポート。
NSR	この TCP 接続の現在の動作上の NSR 状態
RevOnly	yes に設定すると、TCP 接続は受信方向の場合に限り複製されます。一部のアプリケーションでは、受信方向に限定して TCP を複製しなければならない場合があります。

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr pcb, (734 ページ)</a>	指定された接続またはすべての接続の NSR を停止します。
<a href="#">show tcp nsr client brief, (787 ページ)</a>	異なるノードの TCP クライアントのノンストップルーティング (NSR) 状態に関する概要情報を表示します。

## show tcp nsr client brief

異なるノードのTCPクライアントのノンストップルーティング (NSR) 状態に関する概要情報を表示するには、EXEC モードで **show tcp nsr client brief** コマンドを使用します。

**show tcp nsr client brief** [*location node-id*]

### 構文の説明

**location node-id** (任意) 指定されたノードのクライアント概要情報を表示します。  
*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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

### 例

次は、**show tcp nsr client brief** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show tcp nsr client brief location 0/1/CPU0
```

## show tcp nsr client brief

```

CCB          Proc Name      Instance Sets Sessions/NSR Up Sessions
0x482bf378  mpls_ldp  1          1          1/1
0x482bd32c  mpls_ldp  2          1          0/0

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 82 : show tcp nsr client brief コマンドのフィールドの説明

フィールド	説明
CCB	クライアントコントロールブロック (CCB) 。クライアントを特定する一意の ID。
Proc Name	クライアントプロセスの名前。
Instance	ルーティングアプリケーションには複数のインスタンスが存在する可能性があるため、インスタンスはクライアントプロセスのインスタンス数と見なされます。
Sets	セット番号はセッションセットの ID として特定されます。
Sessions/NSR Up Sessions	セット内の合計セッション数と NSR が起動しているセッション数。

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr client</a> , (732 ページ)	ノンストップルーティング (NSR) クライアントに関する詳細情報をクリアします。
<a href="#">show tcp nsr brief</a> , (784 ページ)	異なるノードの TCP 接続のキー ノンストップルーティング (NSR) 状態を表示します。

## show tcp nsr detail client

ノンストップルーティング (NSR) クライアントに関する詳細情報を表示するには、EXEC モードで **show tcp nsr detail client** コマンドを使用します。

**show tcp nsr detail client** {*ccb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>ccb-address</i>	特定のクライアント情報のクライアントコントロールブロック (CCB) アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482a4e20 に設定できます。
<b>all</b>	すべてのクライアントを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのクライアント情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力は、すべてのクライアントの詳細情報を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr detail client all

=====
CCB 0x482b25d8, Proc Name mpls_ldap
Instance ID 1, Job ID 360
Number of session-sets 2
Number of sessions 3
Number of NSR Synced sessions 1
Connected at: Sun Jun 10 07:05:31 2007
Registered for notifications: Yes

=====
CCB 0x4827fd30, Proc Name mpls_ldap
Instance ID 2, Job ID 361
Number of session-sets 1
Number of sessions 2
Number of NSR Synced sessions 2
Connected at: Sun Jun 10 07:05:54 2007
Registered for notifications: Yes

=====
RP/0/RSP0/CPU0:router# show tcp nsr detail client all location 1
RP/0/RSP0/CPU0:router# show tcp nsr detail client all location 0/1/CPU0

=====
CCB 0x482bf378, Proc Name mpls_ldap
Instance ID 1, Job ID 360
Number of session-sets 1
Number of sessions 1
Number of NSR Synced sessions 1
Connected at: Sun Jun 10 07:05:41 2007
Registered for notifications: Yes

=====
CCB 0x482bd32c, Proc Name mpls_ldap
Instance ID 2, Job ID 361
Number of session-sets 1
Number of sessions 2
Number of NSR Synced sessions 2
Connected at: Sun Jun 10 07:06:01 2007
Registered for notifications: Yes
```

## 関連コマンド

コマンド	説明
<a href="#">show tcp nsr detail pcb, (791 ページ)</a>	TCP 接続のノンストップルーティング (NSR) 状態に関する詳細情報を表示します。
<a href="#">show tcp nsr detail session-set, (794 ページ)</a>	異なるノードのセッションセットのノンストップルーティング (NSR) 状態に関する詳細を表示します。

## show tcp nsr detail pcb

TCP接続のノンストップルーティング（NSR）状態に関する詳細情報を表示するには、EXECモードで **show tcp nsr detail pcb** コマンドを使用します。

```
show tcp nsr detail pcb {pcb-address| all} [location node-id]
```

### 構文の説明

<i>pcb-address</i>	特定の接続情報の PCB アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482c6b8c として設定できます。
<b>all</b>	すべての接続を指定します。
<b>location node-id</b>	(オプション) 指定されたノードの接続情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

例

次のサンプル出力では、すべてのロケーションのNSRの全詳細を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr detail pcb all location 0/0/cpu0
```

```
=====
PCB 0x482b6b0c, VRF Id 0x60000000, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 31466
SSCB 0x482bc80c, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Up, Rcv Path Replication only: No
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 3005097735, FSSN Offset: 0

Sequence number of last or current initial sync: 1181461961
Initial sync started at: Sun Jun 10 07:52:41 2007
Initial sync ended   at: Sun Jun 10 07:52:41 2007

Number of incoming packets currently held: 1
      Pak#      SeqNum      Len      AckNum
-----
      1      3005097735      0      1172387202

Number of iACKS currently held: 0

=====
PCB 0x482c2920, VRF Id 0x60000000, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 11229
SSCB 0x482bb3bc, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Down, Rcv Path Replication only: No
Replicated to standby: No
Synchronized with standby: No
NSR-Down Reason: Initial sync was aborted
NSR went down at: Sun Jun 10 11:55:38 2007

Initial sync in progress: No
Sequence number of last or current initial sync: 1181476338
Initial sync error, if any: 'ip-tcp' detected the 'warning' condition 'Initial sync operation
timed out'
Source of initial sync error: Local TCP
Initial sync started at: Sun Jun 10 11:52:18 2007
Initial sync ended   at: Sun Jun 10 11:55:38 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

=====
PCB 0x482baea0, VRF Id 0x60000000, Client PID: 2810078
Local host: 5.1.1.1, Local port: 646
Foreign host: 5.1.1.2, Foreign port: 41149
SSCB 0x482bb3bc, Client PID 2810078
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x00001000

NSR State: Down, Rcv Path Replication only: No
Replicated to standby: No
Synchronized with standby: No
NSR-Down Reason: Initial sync was aborted
NSR went down at: Sun Jun 10 11:55:38 2007

Initial sync in progress: No
Sequence number of last or current initial sync: 1181476338
```



```

Initial sync error, if any: 'ip-tcp' detected the 'warning' condition 'Initial sync operation
  timed out'
Source of initial sync error: Local TCP
Initial sync started at: Sun Jun 10 11:52:18 2007
Initial sync ended   at: Sun Jun 10 11:55:38 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

=====
PCB 0x482c35ac, VRF Id 0x60000000, Client PID: 2859233
Local host: 5:1::1, Local port: 8889
Foreign host: 5:1::2, Foreign port: 14008
SSCB 0x4827fea8, Client PID 2859233
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x0000001c

NSR State: Up, Rcv Path Replication only: No
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 2962722865, FSSN Offset: 0

Sequence number of last or current initial sync: 1181474373
Initial sync started at: Sun Jun 10 11:19:33 2007
Initial sync ended   at: Sun Jun 10 11:19:33 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

=====
PCB 0x482c2f10, VRF Id 0x60000000, Client PID: 2859233
Local host: 5:1::1, Local port: 8889
Foreign host: 5:1::2, Foreign port: 40522
SSCB 0x4827fea8, Client PID 2859233
Node Role: Active, Protected by: 0/1/CPU0, Cookie: 0x0000001b

NSR State: Up, Rcv Path Replication only: No
Replicated to standby: Yes
Synchronized with standby: Yes
FSSN: 3477316401, FSSN Offset: 0

Sequence number of last or current initial sync: 1181474373
Initial sync started at: Sun Jun 10 11:19:33 2007
Initial sync ended   at: Sun Jun 10 11:19:33 2007

Number of incoming packets currently held: 0

Number of iACKS currently held: 0

```

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr pcb, (734 ページ)</a>	指定された接続またはすべての接続の NSR を停止します。
<a href="#">show tcp nsr detail client, (789 ページ)</a>	ノンストップルーティング (NSR) クライアントに関する詳細情報を表示します。
<a href="#">show tcp nsr detail session-set, (794 ページ)</a>	異なるノードのセッションセットのノンストップルーティング (NSR) 状態に関する詳細を表示します。

## show tcp nsr detail session-set

異なるノードのセッションセットのノンストップルーティング (NSR) 状態に関する詳細情報を表示するには、EXEC モードで **show tcp nsr detail session-set** コマンドを使用します。

**show tcp nsr detail session-set** {*sscb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>sscb-address</i>	特定のセッションセット情報のセッションセットコントロールブロック (SSCB) アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482c6b8c として設定できます。
<b>all</b>	すべてのセッションセットを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのセッションセット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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、すべてのセッションセットを示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr detail session-set all

=====
SSCB 0x482bc80c, Client PID: 2810078
Set Id: 1, Addr Family: IPv4
Role: Active, Protected by: 0/1/CPU0, Well known port: 646
Sessions: total 1, synchronized 1
Initial sync in progress: No
  Sequence number of last or current initial sync: 1181461961
  Number of sessions in the initial sync: 1
  Number of sessions already synced: 1
  Number of sessions that failed to sync: 0
  Initial sync started at: Sun Jun 10 07:52:41 2007
  Initial sync ended   at: Sun Jun 10 07:52:41 2007

=====
SSCB 0x482bb3bc, Client PID: 2810078
Set Id: 2, Addr Family: IPv4
Role: Active, Protected by: 0/1/CPU0, Well known port: 646
Sessions: total 2, synchronized 0
Initial sync in progress: Yes
  Sequence number of last or current initial sync: 1181476338
  Initial sync timer expires in 438517602 msec
  Number of sessions in the initial sync: 2
  Number of sessions already synced: 0
  Number of sessions that failed to sync: 0
  Initial sync started at: Sun Jun 10 11:52:18 2007

=====
SSCB 0x4827fea8, Client PID: 2859233
Set Id: 1, Addr Family: IPv6
Role: Active, Protected by: 0/1/CPU0, Well known port: 8889
Sessions: total 2, synchronized 2
Initial sync in progress: No
  Sequence number of last or current initial sync: 1181474373
  Number of sessions in the initial sync: 2
  Number of sessions already synced: 2
  Number of sessions that failed to sync: 0
  Initial sync started at: Sun Jun 10 11:19:33 2007
  Initial sync ended   at: Sun Jun 10 11:19:33 2007
```

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr session-set</a> , (737 ページ)	セッションセットに関する情報をクリアします。
<a href="#">show tcp nsr detail client</a> , (789 ページ)	ノンストップルーティング (NSR) クライアントに関する詳細情報を表示します。
<a href="#">show tcp nsr detail pcb</a> , (791 ページ)	TCP 接続のノンストップルーティング (NSR) 状態に関する詳細情報を表示します。

# show tcp nsr session-set brief

異なるノードのノンストップルーティング (NSR) 状態のセッションセットに関する概要情報を表示するには、EXEC モードで **show tcp nsr session-set brief** コマンドを使用します。

**show tcp nsr session-set brief** [*location node-id*]

## 構文の説明

**location node-id** (オプション) 指定されたノードのセッションセット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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

セッションセットは、サブセットがただ1つのスタンバイ ノードによって保護されているアプリケーションセッションのサブセットから構成されます。TCP NSR 状態のコンピュータは、これらのセッションセットに応じて動作します。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、TCP インスタンスにとって既知のすべてのセッションセットを示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr session-set brief
```

```
SSCB      Client    LocalAPP Set-Id   Family  Role      Protect-Node  Total/Synced
0x482bc80c 2810078  mpls_ldp#1  1      IPv4     Active        0/1/CPU0     1/1
0x482bb3bc 2810078  mpls_ldp#1  2      IPv4     Active        0/1/CPU0     2/0
0x4827fea8 2859233  mpls_ldp#2  1      IPv6     Active        0/1/CPU0     2/2
```

次のサンプル出力では、ロケーション 0/1/CPU0 のセッションセットに関する概要情報を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr session-set brief location 0/1/CPU0
```

```
SSCB      Client    LocalAPP Set-Id   Family  Role      Protect-Node  Total/Synced
0x4827ff74 602319   mpls_ldp#1  1      IPv4     Stdbby       0/0/CPU0     1/1
0x482b8f54 602320   mpls_ldp#2  1      IPv6     Stdbby       0/0/CPU0     2/2
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 83 : show tcp nsr session-set brief コマンドのフィールドの説明

フィールド	説明
SSCB	クライアントのセッションセットを特定するセッションセットコントロールブロック (SSCB) の一意の ID。
Client	クライアントプロセスの PID。
LocalAPP	クライアントプロセス名とインスタンス数。
Set-Id	セッションセットの ID。
Family	IPv4 または IPv6 のセッションセットに追加されたセッションのアドレスファミリ。
Role	アクティブまたはスタンバイの TCP スタックのロール。
Protect-Node	パートナー ノードなどの保護を提供しているノード。
Total/Synced	セットの合計セッション数と同期化されたセッション数。

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr session-set, (737 ページ)</a>	セッションセットに関する情報をクリアします。
<a href="#">show tcp nsr detail session-set, (794 ページ)</a>	異なるノードのセッションセットのノンストップルーティング (NSR) 状態に関する詳細を表示します。

## show tcp nsr statistics client

クライアントのノンストップルーティング (NSR) 統計を表示するには、EXEC モードで **show tcp nsr statistics client** コマンドを使用します。

**show tcp nsr statistics client** {*ccb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>ccb-address</i>	クライアントの特定の統計情報のクライアントコントロールブロック (CCB) アドレス。0 ~ ffffffff。たとえば、アドレス範囲を 0x482c6b8c として設定できます。
<b>all</b>	クライアントのすべての統計を指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードのクライアント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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、クライアントのすべての統計を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics client all

=====
CCB: 0x482b25d8
Name: mpls_ldp, Job ID: 360
Connected at: Thu Jan 1 00:00:00 1970

Notification Stats      : Queued  Failed  Delivered  Dropped
Init-Sync Done          :      0      0           0         0
Replicated Session Ready:      0      0           0         0
Operational Down        :      0      0           0         0
Last clear at: Sun Jun 10 12:19:12 2007

=====
CCB: 0x4827fd30
Name: mpls_ldp, Job ID: 361
Connected at: Sun Jun 10 07:05:54 2007

Notification Stats      : Queued  Failed  Delivered  Dropped
Init-Sync Done          :      1      0           1         0
Replicated Session Ready:      0      0           0         0
Operational Down        :      0      0           0         0
Last clear at: Never Cleared
```

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr statistics client</a> , (739 ページ)	クライアントのノンストップルーティング (NSR) 統計をクリアします。
<a href="#">show tcp nsr statistics pcb</a> , (801 ページ)	特定のプロトコル コントロール ブロック (PCB) のノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics session-set</a> , (804 ページ)	セッションセットのノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics summary</a> , (806 ページ)	すべての TCP セッションのノンストップルーティング (NSR) サマリー統計を表示します。



## show tcp nsr statistics pcb

特定のプロトコルコントロールブロック (PCB) のノンストップルーティング (NSR) 統計を表示するには、EXEC モードで **show tcp nsr statistics pcb** コマンドを使用します。

```
show tcp nsr statistics pcb {pcb-address| all} [location node-id]
```

### 構文の説明

<i>pcb-address</i>	特定の接続情報の PCB アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482c6b8c として設定できます。
<b>all</b>	すべての接続統計を指定します。
<b>location node-id</b>	(オプション) 指定されたノードの接続統計を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、すべての NSR 統計を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics pcb all
```

```
=====
PCB 0x482b6b0c
Number of times NSR went up: 0
Number of times NSR went down: 0
Number of times NSR was disabled: 0
Number of times fail-over occurred : 0
Last clear at: Sun Jun 10 13:55:35 2007
```

```
=====
PCB 0x482c2920
Number of times NSR went up: 2
Number of times NSR went down: 2
Number of times NSR was disabled: 0
Number of times fail-over occurred : 0
Last clear at: Never Cleared
```

```
=====
PCB 0x482baea0
Number of times NSR went up: 2
Number of times NSR went down: 2
Number of times NSR was disabled: 0
Number of times fail-over occurred : 0
Last clear at: Never Cleared
```

```
=====
PCB 0x482c35ac
Number of times NSR went up: 4
Number of times NSR went down: 2
Number of times NSR was disabled: 1
Number of times fail-over occurred : 0
Last clear at: Never Cleared
```

```
=====
PCB 0x482c2f10
Number of times NSR went up: 4
Number of times NSR went down: 2
Number of times NSR was disabled: 1
Number of times fail-over occurred : 0
Last clear at: Never Cleared
```

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr statistics pcb, (741 ページ)</a>	TCP 接続のノンストップルーティング (NSR) 統計をクリアします。
<a href="#">show tcp nsr statistics client, (799 ページ)</a>	クライアントのノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics session-set, (804 ページ)</a>	セッションセットのノンストップルーティング (NSR) 統計を表示します。

コマンド	説明
<a href="#">show tcp nsr statistics summary</a> , <a href="#">(806 ページ)</a>	すべての TCP セッションのノンストップルーティング (NSR) サマリー統計を表示します。

## show tcp nsr statistics session-set

セッションセットのノンストップルーティング (NSR) 統計を表示するには、EXEC モードで **show tcp nsr statistics session-set** コマンドを使用します。

**show tcp nsr statistics session-set** {*sscb-address*| **all**} [**location** *node-id*]

### 構文の説明

<i>sscb-address</i>	特定の統計のセッションセット情報のセッションセット コントロール ブロック (SSCB) アドレス範囲。0 ~ ffffffff。たとえば、アドレス範囲を 0x482b3444 に設定できます。
<b>all</b>	統計のすべてのセッションセットを指定します。
<b>location</b> <i>node-id</i>	(オプション) 指定されたノードの統計のセッションセット情報を表示します。 <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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

### タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、統計のすべてのセッションセット情報を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics session-set all

=====Session Set Stats =====
SSCB 0x482bc80c, Set ID: 1
Number of times init-sync was attempted :1
Number of times init-sync was successful :1
Number of times init-sync failed       :0
Number of times switch-over occurred   :0
Last clear at: Never Cleared

=====Session Set Stats =====
SSCB 0x482bb3bc, Set ID: 2
Number of times init-sync was attempted :1
Number of times init-sync was successful :0
Number of times init-sync failed       :1
Number of times switch-over occurred   :0
Last clear at: Never Cleared

=====Session Set Stats =====
SSCB 0x4827fea8, Set ID: 1
Number of times init-sync was attempted :0
Number of times init-sync was successful :0
Number of times init-sync failed       :0
Number of times switch-over occurred   :0
Last clear at: Sun Jun 10 13:36:51 2007
```

## 関連コマンド

コマンド	説明
<a href="#">clear tcp nsr statistics session-set, (744 ページ)</a>	セッションセットのノンストップルーティング (NSR) 統計をクリアします。
<a href="#">show tcp nsr statistics client, (799 ページ)</a>	クライアントのノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics pcb, (801 ページ)</a>	特定のプロトコル コントロール ブロック (PCB) のノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics summary, (806 ページ)</a>	すべての TCP セッションのノンストップルーティング (NSR) サマリー統計を表示します。

# show tcp nsr statistics summary

すべての TCP セッションのノンストップルーティング (NSR) サマリー統計を表示するには、EXEC モードで **show tcp nsr statistics summary** コマンドを使用します。

**show tcp nsr statistics summary** [*location node-id*]

## 構文の説明

**location node-id** (オプション) 指定されたノードのサマリー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

値が指定されていない場合、コマンドを実行している現在の RP がロケーションとして使用されます。

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**location** キーワードを使用すると、アクティブおよびスタンバイ TCP インスタンスを個別に問い合わせることができます。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次のサンプル出力では、すべての TCP セッションのサマリー統計を示しています。

```
RP/0/RSP0/CPU0:router# show tcp nsr statistics summary
```

```

=====Summary Stats=====
The last clear at Thu Jan 1 00:00:00 1970

Notif Statistic:
                Queued  Failed  Delivered  Dropped
Init-sync Done      :      3      0          3         0
Replicated Session Ready:    0      0          0         0
Operational Down    :      8      0          8         0
QAD Msg Statistic:
Number of dropped messages from partner TCP stack(s)      : 0
Number of unknown messages from partner TCP stack(s)      : 0
Number of messages accepted from partner TCP stack(s)     : 31
Number of messages sent to partner TCP stack(s)           : 0
Number of messages failed to be sent to partner TCP stack(s): 0
IACK RX Msg Statistic:
Number of iACKs dropped because there is no PCB            : 0
Number of iACKs dropped because there is no datapath SCB  : 0
Number of iACKs dropped because SSO is not up              : 0
Number of stale iACKs dropped                              : 6
Number of iACKs not held because of an immediate match    : 0
Number of held packets dropped because of errors           : 0
    
```

関連コマンド

コマンド	説明
<a href="#">clear tcp nsr statistics summary, (746 ページ)</a>	統計サマリーをクリアします。
<a href="#">show tcp nsr statistics client, (799 ページ)</a>	クライアントのノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics pcb, (801 ページ)</a>	特定のプロトコル コントロール ブロック (PCB) のノンストップルーティング (NSR) 統計を表示します。
<a href="#">show tcp nsr statistics session-set, (804 ページ)</a>	セッションセットのノンストップルーティング (NSR) 統計を表示します。

# 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、EXEC モードで **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

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

## タスク ID

タスク ID	操作
transport	読み取り

## 例

次は、**show udp brief** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# 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
0x804fcb0      0      0 0.0.0.0:123     0.0.0.0:0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 84 : 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。

関連コマンド

コマンド	説明
<a href="#">show tcp brief</a> , (776 ページ)	TCP 接続の詳細を表示します。

## 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、EXEC モードで **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。
<b>all</b>	すべての UDP 接続の統計を提供します。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
transport	読み取り

例

次は、**show udp detail pcb all** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show udp detail pcb all location 0/3/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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 85: **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、EXEC モードで **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

<b>location</b> <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。
<b>peer-filter</b>	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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
transport	読み取り

### 例

次は、特定のロケーション (0/0/CPU0) での、**show udp extended-filters** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# show udp extended-filters location 0/0/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、EXEC モードで **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

<b>summary</b>	サマリー統計を表示します。
<b>pcb</b> <i>pcb-address</i>	各接続の詳細統計を表示します。
<b>pcb</b> <i>all</i>	すべての接続の詳細統計を表示します。
<b>location</b> <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

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

パケット受信に関係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	操作
transport	読み取り

## 例

次は、**show udp statistics summary** コマンドによるサンプル出力です。

```
RP/0/RSP0/CPU0:router# 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
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 86: **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

## 関連コマンド

コマンド	説明
<a href="#">clear udp statistics</a> , (752 ページ)	UDP 統計をクリアします。

## tcp mss

データ送信で TCP が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、グローバル コンフィギュレーション モードで **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 Maximum Transfer Unit (MTU; 最大転送ユニット)、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

グローバル コンフィギュレーション

#### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

#### タスク ID

タスク ID	操作
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.
RP/0/RSP0/CPU0:router:Sep  8 18:29:51.209 : config[65700]: %SYS-5-CONFIG_I : Configured from
console by lab
```

## tcp path-mtu-discovery

TCPによる接続に対する最大共通最大転送ユニット (MTU) の自動検出を許可するには、グローバル コンフィギュレーション モードで **tcp path-mtu-discovery** を使用します。デフォルト値をリセットするには、このコマンドの **no** 形式を使用します。

**tcp path-mtu-discovery** [*age-timer minutes*] **infinite**]

**no tcp path-mtu-discovery**

### 構文の説明

**age-timer** *minutes* (オプション) 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

ディセーブル

**age-timer** のデフォルト値は 10 分です。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース

変更箇所

リリース 3.7.2

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。

**tcp path-mtu-discovery** コマンドを使用すると、TCP による接続に対する最大共通 MTU の検出を許可し、パケットが送信ホストと受信ホストの間を通過するときに、パケットのフラグメント化と再構成を避けることができます。

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

## 操作

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/RSP0/CPU0:router(config)# tcp path-mtu-discovery age-timer 20
```

## tcp selective-ack

TCP 選択応答 (ACK) を有効化し、リモート TCP が受信した TCP パケット内のセグメントを特定するには、グローバル コンフィギュレーション モードで **tcp selective-ack** コマンドを使用します。デフォルト値をリセットするには、このコマンドの **no** 形式を使用します。

**tcp selective-ack**

**no tcp selective-ack**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

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回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 Long Fat Network (LFN; 高帯域遅延ネットワーク) の場合は、この方法は不十分です。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(config)# tcp selective-ack
```

## 関連コマンド

コマンド	説明
<a href="#">tcp timestamp</a> , ( <a href="#">823 ページ</a> )	パケットの往復時間を測定します。

## tcp synwait-time

TCP 接続の確立を試みながら、タイムアウトまで待機する時間を設定するには、グローバル コンフィギュレーション モードで **tcp synwait-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

**tcp synwait-time** *seconds*

**no tcp synwait-time** *seconds*

### 構文の説明

*seconds* 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

### タスク ID

タスク ID	操作
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/RSP0/CPU0:router(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、グローバル コンフィギュレーション モードで **tcp timestamp** コマンドを使用します。デフォルト値をリセットするには、このコマンドの **no** 形式を使用します。

**tcp timestamp**

**no tcp timestamp**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### 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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。

**tcp timestamp** コマンドを使用すると、より正確にパケットの往復時間を測定します。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	操作
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/RSP0/CPU0:router (config)# tcp timestamp
```

## 関連コマンド

コマンド	説明
<a href="#">tcp selective-ack</a> , ( <a href="#">820 ページ</a> )	TCP 選択応答機能をイネーブルにします。



## tcp window-size

TCP ウィンドウ サイズを変更するには、グローバル コンフィギュレーション モードで **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

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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。



(注) 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	操作
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/RSP0/CPU0:router (config)# tcp window-size 3000
```



## VRRP コマンド

---

このマニュアルでは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータの仮想ルータ冗長プロトコル (VRRP) の設定およびモニタに使用する Cisco IOS XR ソフトウェアコマンドについて説明します。

VRRP の概念、設定タスク、および例の詳細については、『*Cisco IOS XR IP Addresses and Services Configuration Guide*』を参照してください。

- [accept-mode, 829 ページ](#)
- [address-family, 831 ページ](#)
- [address \(VRRP\) , 833 ページ](#)
- [address global, 835 ページ](#)
- [address linklocal, 837 ページ](#)
- [address secondary, 839 ページ](#)
- [bfd minimum-interval \(VRRP\) , 841 ページ](#)
- [bfd multiplier \(VRRP\) , 843 ページ](#)
- [clear vrrp statistics, 845 ページ](#)
- [delay \(VRRP\) , 850 ページ](#)
- [interface \(VRRP\) , 852 ページ](#)
- [message state disable, 854 ページ](#)
- [router vrrp, 856 ページ](#)
- [show vrrp, 858 ページ](#)
- [snmp-server traps vrrp events, 864 ページ](#)
- [vrrp, 866 ページ](#)
- [vrrp assume-ownership disable, 868 ページ](#)
- [vrrp bfd fast-detect, 870 ページ](#)

- [vrrp bfd minimum-interval, 872 ページ](#)
- [vrrp bfd multiplier, 874 ページ](#)
- [vrrp delay, 876 ページ](#)
- [vrrp ipv4, 878 ページ](#)
- [vrrp preempt, 880 ページ](#)
- [vrrp priority, 882 ページ](#)
- [vrrp text-authentication, 884 ページ](#)
- [vrrp timer, 886 ページ](#)
- [vrrp track interface, 888 ページ](#)

## accept-mode

仮想ルータ冗長プロトコル（VRRP）仮想アドレスのルートのインストールをディセーブルにするには、VRRP 仮想ルータ サブモードで **accept-mode** コマンドを使用します。VRRP 仮想アドレスのルートのインストールをイネーブルにするには、このコマンドの **no** 形式を使用します。

**accept-mode disable**

**no accept-mode disable**

### 構文の説明

**disable** 受け入れモードをディセーブルにします。

### コマンド デフォルト

デフォルトでは、受け入れモードはイネーブルになっています。

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 4.1.0	このコマンドが導入されました。このコマンドは、 <b>vrrp assume-ownership disable</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

### 例

次に、VRRP 仮想アドレスのルートのインストールをディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```

RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# accept-mode disable
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#

```

## 関連コマンド

コマンド	説明
<a href="#">address (VRRP)</a> , (833 ページ)	仮想ルータのプライマリ仮想 IPv4 アドレスを設定します。
<a href="#">address global</a> , (835 ページ)	仮想ルータのグローバルな仮想 IPv6 アドレスを設定します。
<a href="#">address linklocal</a> , (837 ページ)	仮想ルータの仮想リンクローカル IPv6 アドレスを設定します。
<a href="#">address secondary</a> , (839 ページ)	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。
<a href="#">message state disable</a> , (854 ページ)	VRRP ステート変更イベントをロギングするタスクをディセーブルにします。

## address-family

アドレス ファミリ モードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **address-family** コマンドを使用します。アドレス ファミリ モードを終了するには、このコマンドの **no** 形式を使用します。

**address-family** {ipv4 | ipv6}

**no address-family** {ipv4 | ipv6}

### 構文の説明

**ipv4** IPv4 アドレス ファミリ。

**ipv6** IPv6 アドレス ファミリ。

### 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	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

### 例

次に、アドレス ファミリ モードをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router # config
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
```

## 関連コマンド

コマンド	説明
<a href="#">interface (VRRP)</a> , <a href="#">(852 ページ)</a>	VRRP インターフェイス コンフィギュレーション モードをイネーブルにします。



## address (VRRP)

仮想ルータのプライマリ仮想 IPv4 アドレスを設定するには、仮想ルータ冗長プロトコル (VRRP) 仮想ルータ サブモードで **address** コマンドを使用します。仮想ルータのプライマリ仮想 IPv4 アドレスの設定を解除するには、このコマンドの **no** 形式を使用します。

**address** *address*

**no address** *address*

### 構文の説明

*address* VRRP IPv4 アドレス。

### コマンド デフォルト

なし

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 4.1.0	このコマンドが導入されました。このコマンドは、 <b>vrrp ipv4</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

### 例

次に、仮想ルータのプライマリ仮想 IPv4 アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```

RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# address 10.20.30.1
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#

```

## 関連コマンド

コマンド	説明
<a href="#">accept-mode, (829 ページ)</a>	VRRP 仮想アドレスのルートのインストールをディセーブルにします。
<a href="#">address global, (835 ページ)</a>	仮想ルータのグローバルな仮想 IPv6 アドレスを設定します。
<a href="#">address linklocal, (837 ページ)</a>	仮想ルータの仮想リンクローカル IPv6 アドレスを設定します。
<a href="#">address secondary, (839 ページ)</a>	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。
<a href="#">message state disable, (854 ページ)</a>	VRRP ステート変更イベントをロギングするタスクをディセーブルにします。



```

RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv6
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# address global 4000::1000
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#

```

## 関連コマンド

コマンド	説明
<a href="#">address (VRRP)</a> , (833 ページ)	仮想ルータのプライマリ仮想 IPv4 アドレスを設定します。
<a href="#">accept-mode</a> , (829 ページ)	VRRP 仮想アドレスのルートのインストールをディセーブルにします。
<a href="#">address linklocal</a> , (837 ページ)	仮想ルータの仮想リンクローカル IPv6 アドレスを設定します。
<a href="#">address secondary</a> , (839 ページ)	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。
<a href="#">message state disable</a> , (854 ページ)	VRRP ステート変更イベントをロギングするタスクをディセーブルにします。

## address linklocal

仮想ルータの仮想リンクローカル IPv6 アドレスを設定するか、または仮想リンクローカル IPv6 アドレスが仮想ルータの仮想 Media Access Control (MAC) アドレスから自動的にイネーブルになり、計算されるように指定するには、仮想ルータ冗長プロトコル (VRRP) 仮想ルータ サブモードで **address linklocal** コマンドを使用します。仮想ルータの仮想リンクローカル IPv6 アドレスの設定を解除するには、このコマンドの **no** 形式を使用します。

**address linklocal** [*ipv6-address*] **autoconfig**

**no address linklocal** [*ipv6-address*] **autoconfig**

### 構文の説明

<i>ipv6-address</i>	VRRP IPv6 リンクローカル アドレス。
<b>autoconfig</b>	VRRP IPv6 リンクローカル アドレスを自動的に設定します。

### コマンド デフォルト

なし

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、VRRP IPv6 リンクローカルアドレスを自動的に設定する例を示します。

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)#interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)#address-family ipv6
RP/0/RSP0/CPU0:router(config-vrrp-address-family)#vrrp 3 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#address linklocal autoconfig
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

次に、仮想ルータの仮想 IPv6 リンクローカルアドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)#interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)#address-family ipv6
RP/0/RSP0/CPU0:router(config-vrrp-address-family)#vrrp 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#address linklocal FE80::260:3EFF:FE11:6770
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

## 関連コマンド

コマンド	説明
<a href="#">address (VRRP)</a> , (833 ページ)	仮想ルータのプライマリ仮想 IPv4 アドレスを設定します。
<a href="#">address global</a> , (835 ページ)	仮想ルータのグローバルな仮想 IPv6 アドレスを設定します。
<a href="#">accept-mode</a> , (829 ページ)	VRRP 仮想アドレスのルートのインストールをディセーブルにします。
<a href="#">address secondary</a> , (839 ページ)	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。
<a href="#">message state disable</a> , (854 ページ)	VRRP ステート変更イベントをロギングするタスクをディセーブルにします。

# address secondary

仮想ルータのセカンダリ仮想IPv4アドレスを設定するには、仮想ルータ冗長プロトコル (VRRP) 仮想ルータ サブモードで **address secondary** コマンドを使用します。仮想ルータのセカンダリ仮想 IPv4 アドレスの設定を解除するには、このコマンドの **no** 形式を使用します。

**address address secondary**

**no address address secondary**

## 構文の説明

<b>secondary</b>	セカンダリ VRRP IP アドレスを設定します。
<b>address</b>	VRRP IPv4 アドレス。

## コマンド デフォルト

なし

## コマンド モード

VRRP 仮想ルータ

## コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、仮想ルータのセカンダリ仮想 IPv4 アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# address 10.20.30.1 secondary
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

## 関連コマンド

コマンド	説明
<a href="#">address (VRRP)</a> , (833 ページ)	仮想ルータのプライマリ仮想 IPv4 アドレスを設定します。
<a href="#">address global</a> , (835 ページ)	仮想ルータのグローバルな仮想 IPv6 アドレスを設定します。
<a href="#">address linklocal</a> , (837 ページ)	仮想ルータの仮想リンクローカル IPv6 アドレスを設定します。
<a href="#">accept-mode</a> , (829 ページ)	VRRP 仮想アドレスのルートのインストールをディセーブルにします。
<a href="#">message state disable</a> , (854 ページ)	VRRP ステート変更イベントをロギングするタスクをディセーブルにします。



## bfd minimum-interval (VRRP)

BFD の最小間隔を特定のインターフェイス上のすべての VRRP BFD セッションで使用するよう設定するには、インターフェイス コンフィギュレーション モードで **bfd minimum-interval** コマンドを使用します。設定した最小期間を削除し、デフォルトの期間に設定するには、このコマンドの **no** 形式を使用します。

**bfd minimum-interval** *interval*

**no bfd minimum-interval** *interval*

### 構文の説明

*interval* ミリ秒単位で最小間隔を指定します。範囲は 15 ~ 30000 です。

### コマンド デフォルト

デフォルトの最小間隔は 15 ミリ秒です。

### コマンド モード

VRRP 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	変更箇所
リリース 4.1.0	このコマンドが導入されました。このコマンドは、 <b>vrrp bfd minimum-interval</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

最小間隔は BFD ピアに BFD パケットを送信する頻度を決定します。これはセッションに送信される連続的な BFD パケット間の時間です。最小間隔はミリ秒単位で指定します。設定された最小間隔は、インターフェイス上のすべての BFD セッションに適用されます。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、100 ミリ秒の最小間隔を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp  
RP/0/RSP0/CPU0:router(config-vrrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-vrrp-if)# bfd minimum-interval 100
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp bfd fast-detect</a> , (870 ページ)	VRRP インターフェイスで BFD をイネーブルにします。

## bfd multiplier (VRRP)

BFD 乗数値を設定するには、インターフェイス コンフィギュレーション モードで **bfd multiplier** コマンドを使用します。設定した乗数値を削除し、乗数値をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**bfd multiplier multiplier**

**no bfd multiplier multiplier**

### 構文の説明

*multiplier* BFD 乗数値を指定します。範囲は 2 ～ 50 です。

### コマンド デフォルト

デフォルト値は 3 です。

### コマンド モード

VRRP 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	変更箇所
リリース 4.1.0	このコマンドが導入されました。このコマンドは、 <b>vrrp bfd multiplier</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

乗数値によって、期待どおりに受信していない場合に BFD セッションがダウンする連続 BFD パケットの数が指定されます。BFD 乗数値は、インターフェイス上に設定されたすべての BFD セッションに適用されます。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、乗数値 10 を使用して BFD 乗数値を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp  
RP/0/RSP0/CPU0:router(config-vrrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-vrrp-if)# bfd multiplier 10
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp bfd fast-detect, (870 ページ)</a>	VRRP インターフェイスで BFD をイネーブルにします。

## clear vrrp statistics

仮想ルータ冗長プロトコル（VRRP）統計情報を（ゼロまたはデフォルト値に）リセットするには、EXEC モードで **clear vrrp statistics** コマンドを使用します。

```
clear vrrp statistics [ipv4|ipv6][interface type interface-path-id [vrid]]
```

### 構文の説明

<b>ipv4</b>	（任意）IPv4 情報をリセットします。
<b>ipv6</b>	（任意）IPv6 情報をリセットします。
<b>interface type</b>	（任意）インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。

```
clear vrrp statistics
```

```
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。

- 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に管理イーサネットインターフェイスがある場合、物理スロット番号は英数字 (RSP0) で、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。

<b>vrid</b>	(任意) 仮想ルータ ID で、ステータスが表示される仮想ルータを識別する番号です。
-------------	--

**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** EXEC

<b>コマンド履歴</b>	<b>リリース</b>	<b>変更箇所</b>
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**interface** が指定されない場合、すべてのインターフェイス上のすべての仮想ルータの統計情報はクリアされます。

**vrid** の値が指定されない場合、指定されたインターフェイス上のすべての仮想ルータの統計情報はクリアされます。

<b>タスク ID</b>	<b>タスク ID</b>	<b>操作</b>
	vrrp	読み取り、書き込み

**例** 次に、vrrp 統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear vrrp statistics
```



## 関連コマンド

コマンド	説明
<a href="#">show vrrp</a> , (858 ページ)	1 つまたはすべての仮想ルータ冗長プロトコル (VRRP) 仮想ルータの要約ステータスまたは詳細ステータスを表示します。

## delay (VRRP)

VRRP ルータのアクティベーション遅延を設定するには、VRRP インターフェイス コンフィギュレーション モードで **delay** コマンドを使用します。アクティベーション遅延を削除するには、このコマンドの **no** 形式を使用します。

**delay minimum value reload value**

**no delay**

### 構文の説明

**minimum value** すべてのインターフェイス起動イベントの最小遅延（秒単位）を設定します。範囲は 0 ～ 10000 です。

**reload value** 最初のインターフェイス起動イベントのリロード遅延（秒単位）を設定します。範囲は 0 ～ 10000 です。

### コマンド デフォルト

**minimum value** : 1

**reload value** : 5

### コマンド モード

VRRP 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	変更箇所
リリース 4.1.0	このコマンドが導入されました。このコマンドは、 <b>vrrp delay</b> コマンドを置き換えました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**vrrp delay** コマンドは、インターフェイス起動イベントで VRRP Finite State Machine (FSM; 有限状態マシン) の開始を遅らせて、インターフェイスがトラフィックを通過する準備を整えます。これにより、**hello** パケットの損失によるエラー状態にならないようにします。最小遅延はすべてのインターフェイス起動イベントに適用され、リロード遅延は最初のインターフェイス起動イベントに適用されます。

この機能をオフにするには、ゼロの値を明示的に設定する必要があります。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、最小遅延を 10 秒にしてリロード遅延を 100 秒にする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface mgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# delay minimum 10 reload 100
```

## 関連コマンド

コマンド	説明
<a href="#">show vrrp</a> , (858 ページ)	1 つまたはすべての仮想ルータ冗長プロトコル (VRRP) 仮想ルータの要約ステータスまたは詳細ステータスを表示します。

## interface (VRRP)

VRRP インターフェイス コンフィギュレーション モードをイネーブルにするには、VRRP コンフィギュレーション モードで **interface (VRRP)** コマンドを使用します。VRRP インターフェイス コンフィギュレーション モードを終了するには、このコマンドの **no** 形式を使用します。

**interface** *type interface-path-id*

**no interface** *type interface-path-id*

### 構文の説明

<i>type</i>	インターフェイスのタイプ。詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。
<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、 <b>show interfaces</b> 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

VRRP はディセーブルです。

### コマンド モード

VRRP コンフィギュレーション

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**interface (VRRP)** コマンドを使用すると、VRRP インターフェイス コンフィギュレーション モードを開始することができます。

すべての VRRP コンフィギュレーション コマンドは VRRP インターフェイス コンフィギュレーション モードで設定する必要があります。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、10-ギガビットイーサネットインターフェイス 0/3/0/0 の VRRP および仮想ルータ 1 を設定する例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

## 関連コマンド

コマンド	説明
<a href="#">router vrrp</a> , <a href="#">(856 ページ)</a>	VRRP 冗長性プロセスを設定します。

## message state disable

syslog を介して仮想ルータ冗長プロトコル (VRRP) のステート変更イベントをロギングするタスクをディセーブルにするには、VRRP 仮想ルータ サブモードで **message state disable** コマンドを使用します。VRRP ステート変更イベントをロギングするタスクを再度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。

**message state disable**

**no message state disable**

### 構文の説明

このコマンドには、キーワードと引数はありません。

### コマンド デフォルト

デフォルトでは、VRRP ステート変更イベントをロギングするタスクはイネーブルになっています。

### コマンド モード

VRRP グローバル

### コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

### 例

次に、VRRP ステート変更イベントのロギングをディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#router vrrp
```

```
RP/0/RSP0/CPU0:router(config-vrrp)#message state disable
RP/0/RSP0/CPU0:router(config-vrrp)#
```

## 関連コマンド

コマンド	説明
<a href="#">address (VRRP)</a> , (833 ページ)	仮想ルータのプライマリ仮想 IPv4 アドレスを設定します。
<a href="#">address global</a> , (835 ページ)	仮想ルータのグローバルな仮想 IPv6 アドレスを設定します。
<a href="#">accept-mode</a> , (829 ページ)	VRRP 仮想アドレスのルートのインストールをディセーブルにします。
<a href="#">address secondary</a> , (839 ページ)	仮想ルータのセカンダリ仮想 IPv4 アドレスを設定します。
<a href="#">address linklocal</a> , (837 ページ)	仮想ルータの仮想リンクローカル IPv6 アドレスを設定します。

## router vrrp

仮想ルータ冗長プロトコル（VRRP）を設定するには、グローバル コンフィギュレーション モードで **router vrrp** コマンドを使用します。VRRP 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。

**router vrrp**

**no router vrrp**

**コマンド デフォルト** このコマンドには、キーワードと引数はありません。  
VRRP はディセーブルです。

**コマンド モード** グローバル コンフィギュレーション

コマンド履歴	リリース	変更箇所
	リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**router vrrp** コマンドを使用すると、VRRP コンフィギュレーション モードを開始することができます。

すべての VRRP コンフィギュレーション コマンドは VRRP インターフェイス コンフィギュレーション モードで設定する必要があります。

タスク ID	タスク ID	操作
	vrrp	読み取り、書き込み



## 例

次に、10-ギガビットイーサネットインターフェイス 0/3/0/0 の VRRP および仮想ルータ 1 を設定する例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

## 関連コマンド

コマンド	説明
<a href="#">interface (VRRP)</a> , (852 ページ)	VRRP インターフェイス コンフィギュレーション モードをイネーブルにします。

# show vrrp

1 つまたはすべての仮想ルータ冗長プロトコル (VRRP) 仮想ルータの要約ステータスまたは詳細ステータスを表示するには、EXEC モードで **show vrrp** コマンドを使用します。

**show vrrp [ipv4|ipv6] [interface type interface-path-id [vrid]] [brief|detail|statistics [all]]**

## 構文の説明

<b>ipv4</b>	(任意) IPv4 情報を表示します。
<b>ipv6</b>	(任意) IPv6 情報を表示します。
<b>interface</b>	(任意) 仮想ルータ インターフェイスのステータスを表示します。
<i>type</i>	(任意) インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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、 <b>show interfaces</b> 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>vrid</i>	(任意) 仮想ルータ ID で、ステータスが表示される仮想ルータを識別する番号です。  仮想ルータ ID は、 <b>vrrp ipv4</b> コマンドで設定されます。範囲は 1 ~ 255 です。

<b>brief</b>	(任意) 仮想ルータの情報の概要図を示します。
<b>detail</b>	(任意) 実行状態の詳細情報を表示します。
<b>statistics</b>	(任意) 統計情報を全部表示します。
<b>all</b>	(任意) 各仮想ルータの統計情報を表示します。

## コマンドモード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

インターフェイスを指定しない場合、すべてのインターフェイス上のすべての仮想ルータが表示されます。vrid が指定されていない場合は、特定インターフェイスのすべての vrid が表示されます。

## タスク ID

タスク ID	操作
vrrp	読み取り

## 例

次に、**show vrrp** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show vrrp
                                A indicates IP address owner
                                | P indicates configured to preempt
                                | |
Interface  vrID Prio A P State  Master addr  VRouter addr
Te0/3/0/0      1  100  P Init   unknown     10.0.1.20
```

```
Te0/3/0/2      7 100  P Init      unknown      10.1.13.0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 87: `show vrrp` コマンドのフィールドの説明

フィールド	説明
Interface	仮想ルータのインターフェイス。
vrID	仮想ルータの ID。
Prio	仮想ルータのプライオリティ。
A	VRRP ルータが IP アドレスのオーナーであることを示します。
P	VRRP ルータがプリエンプション (デフォルト) に設定されているかを示します。
State	仮想ルータの状態。
Master addr	マスター ルータの IP アドレス
VRouter addr	仮想ルータの仮想ルータ IP アドレス。

次に、`detail` キーワードを持つ `show vrrp` コマンドからの出力例を示します。

```
RP/0/RSP0/CPU0:router# show vrrp detail
GigabitEthernet0/4/0/0 - IPv4 vrID 1
  State is Master, IP address owner
    2 state changes, last state change 00:00:59
  Virtual IP address is 4.0.0.1
    Secondary Virtual IP address is 4.0.0.2
    Secondary Virtual IP address is 5.0.0.1
  Virtual MAC address is 0000.5E00.0101
  Master router is local
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + 156/256)
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 110, may preempt
    Minimum delay 0 secs
  Authentication enabled, string "myauth"
  BFD enabled: state Up, interval 15ms multiplier 3 remote IP 4.0.0.3
  Tracked items:
      Interface          State          Priority
      POS0/5/0/1        Down          Decrement    10

GigabitEthernet0/4/0/0 - IPv4 vrID 2
  State is Backup
    3 state changes, last state change 00:01:58
  Virtual IP address is 4.0.1.2
  Virtual MAC address is 0000.5E00.0102
  Master router is IP address owner (4.0.1.1), priority 200
```

```

Advertise time 1.500 secs (forced)
  Master Down Timer 5.109 (3 x 1 + 156/256)
Minimum delay 1 sec, reload delay 5 sec
Current priority 100
  Configured priority 100, may preempt
  Minimum delay 20 secs

Bundle-Ether1 - IPv4 vrID 5
  State is Init
    0 state changes, last state change never
  Virtual IP address is unknown
  Virtual MAC address is 0000.5E00.0100
  Master router is unknown
  Advertise time 1 secs
    Master Down Timer 3.500 (3 x 1 + 128/256)
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 128
    Configured priority 128

GigabitEthernet0/4/0/0 - IPv6 vrID 1
  State is Master
    2 state changes, last state change 00:10:01
  Virtual Linklocal address is FE80::100
    Global Virtual IPv6 address is 4000::100
    Global Virtual IPv6 address is 5000::100
  Virtual MAC address is 0000.5E00.0201
  Master router is local
  Advertise time 1 secs
    Master Down Timer 3.609 (3 x 1 + 156/256)
  Minimum delay 1 sec, reload delay 5 sec
  Current priority 100
    Configured priority 100, may preempt
    Minimum delay 0 secs

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 88 : `show vrrp detail` コマンドのフィールドの説明

フィールド	説明
TenGigE0/3/0/0 - vrID 1	インターフェイスのタイプと番号、およびVRRPグループ番号。
State is	このインターフェイスがVRRP（マスターまたはバックアップ）内で果たすロール。
Virtual IP address is	この仮想ルータの仮想 IP アドレス。
Virtual MAC address is	この仮想ルータの仮想 MAC アドレス。
Master router is	マスタールータの場所。
Advertise time	マスター仮想ルータの場合の、ルータがVRRPアドバタイズメントを送信するインターバル（秒単位）。この値は、 <code>vrrp timer</code> コマンドで設定されます。

フィールド	説明
Master Down Timer	バックアップルータが、マスタールータのロールを想定するまでのマスタールータのアドバタイズメントを待つ時間。
Minimum delay	インターフェイスが起動しネットワーク時間が安定するときの、ステートマシン開始の遅延時間。 <b>Minimum delay</b> は後続の（インターフェイスがフラップする場合の）インターフェイス起動イベントだけに適用される遅延で、リロード遅延は最初のインターフェイス起動イベント後に適用される遅延です。
Current priority	仮想ルータのプライオリティ。
Configured priority	仮想ルータで設定されるプライオリティ。
may preempt	プリエンプションがイネーブルされているかディセーブルされているかの表示。
minimum delay	プリエンプション（デフォルト）が発生するまでの遅延時間。
Tracked items	VRRP ルータがトラッキングしている項目を示すセクション。
Interface	トラッキングされているインターフェイス。
State	トラッキングされるインターフェイスの状態。
Priority Decrement	インターフェイスのダウン時に VRRP プライオリティから減少させるプライオリティ。

次に、10 ギガビットイーサネット インターフェイス 0/3/0/0 の **interface** キーワードを持つ **show vrrp** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show vrrp interface TenGigE 0/3/0/0

          A indicates IP address owner
          | P indicates configured to preempt
          | |
Interface  vrID Prio A P State   Master addr  VRouter addr
Te0/3/0/0      1  100 P Init   unknown    10.0.1.20
Te0/3/0/2      7  100 P Init   unknown    10.1.13.0
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , <a href="#">(878 ページ)</a>	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。

## snmp-server traps vrrp events

VRRP で使用可能な簡易ネットワーク管理プロトコル (SNMP) サーバ通知 (トラップ) をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server traps vrrp events command** コマンドを使用します。使用できるすべての VRRP SNMP 通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

**snmp-server traps vrrp events**

**no snmp-server traps vrrp events**

構文の説明	<b>events</b>	すべての VRRP SNMP サーバトラップを指定します。
-------	---------------	-------------------------------

コマンド デフォルト なし

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更箇所
	リリース 3.9.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID	タスク ID	操作
	snmp	読み取り、書き込み

**例** 次に、VRRP の snmpserver 通知をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:routerrouter(config)# snmp-server traps vrrp events
```



## 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , <a href="#">(878 ページ)</a>	インターフェイスの VRRP をイネーブルにします。

## vrrp

仮想ルータ冗長プロトコル (VRRP) 仮想ルータ モードをイネーブルにするには、アドレス ファミリ モードで **vrrp** コマンドを使用します。VRRP 仮想ルータ モードを終了するには、このコマンドの **no** 形式を使用します。

**vrrp** *vrid*

**no vrrp** *vrid*

### 構文の説明

*vrid* (任意) 仮想ルータ ID で、ステータスが表示される仮想ルータを識別する番号です。仮想ルータ ID は、**vrrp ipv4** コマンドで設定されます。範囲は 1 ~ 255 です。

### コマンド デフォルト

なし。

### コマンド モード

address-family

### コマンド履歴

リリース	変更箇所
リリース 4.1.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

### 例

次に、VRRP 仮想ルータ モードをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)#
```

## 関連コマンド

コマンド	説明
<a href="#">interface (VRRP)</a> , <a href="#">(852 ページ)</a>	VRRP インターフェイス コンフィギュレーション モードをイネーブルにします。

## vrrp assume-ownership disable

VRRPルータがマスター状態時に仮想IPアドレスの所有権を前提とするデフォルト設定をディセーブルにするにはをディセーブルにするには、VRRP インターフェイス コンフィギュレーション モードで、**vrrp assume-ownership** コマンドを使用します。デフォルト設定（所有権を前提とする）に戻すには、このコマンドの **no** 形式を使用します。

**vrrp vrid assume-ownership disable**

**no vrrp vrid assume-ownership disable**

### 構文の説明

<b>vrid</b>	仮想ルータ ID、つまり、仮想 IP アドレス所有権が設定される仮想ルータを識別する番号です。
<b>disable</b>	VRRP パケットを許可しません。

### コマンド デフォルト

VRRP パケット

### コマンド モード

VRRP 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	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.1.0	このコマンドはすでに廃止されています。このコマンドは、 <a href="#">accept-mode</a> 、(829 ページ) コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

デフォルトでは、マスター ルータの場合、IP アドレス オーナーであるかどうかにかかわらず、ルータは仮想 IP アドレスの所有権を前提とします。つまり、ネットワーク設定の検証中にルータは、その IP アドレスに送信されるパケットを許可します。**vrrp assume-ownership** のデフォルトが有効な場合、IP アドレスのオーナーではなくて他の IP アドレスのマスター ルータであるルータは、ping に対して受け入れと応答を行い、そのルータにへの Telnet を受け入れます。他の IP アドレスに送信されるパケットの受け入れは、

このコマンドは、ルータが IP アドレスのオーナーである場合に無視されます（無関係になります）（RFC 2338 の 6.4.3 項、「*Virtual Router Redundancy Protocol*」）。

---

**タスク ID**

タスク ID	操作
vrrp	読み取り、書き込み

---

**例**

次に、10-ギガビットイーサネットインターフェイス 0/3/0/0 上で **vrrp assume-ownership** コマンドをディセーブルにする設定の例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 10.0.0.101
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp 1 assume-ownership disable
```

---

**関連コマンド**

コマンド	説明
<a href="#">vrrp ipv4</a> , <a href="#">(878 ページ)</a>	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。

## vrrp bfd fast-detect

VRRP インターフェイスで双方向フォワーディング (BFD) 高速検出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 **vrrp bfd fast-detect** コマンドを使用します。これにより、仮想ルータ冗長プロトコル (VRRP) ルータとそのピアの間に BFD セッションが作成されます。VRRP がバックアップ状態のときにセッションがダウンすると、VRRP フェールオーバーが開始されます。BFD 高速検出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。

**vrrp vrid bfd fast-detect peer {ipv4 | ipv6} address**

**no vrrp vrid bfd fast-detect peer {ipv4 | ipv6} address**

### 構文の説明

<i>vrid</i>	仮想ルータ ID。
<b>peer</b>	BFD のモニタリング用の VRRP ピア。
<b>ipv4 address</b>	BFD ピア インターフェイスの IPv4 アドレス。
<b>ipv6 address</b>	BFD ピア インターフェイスの IPv6 アドレス。

### コマンド デフォルト

BFD はディセーブルです。

### コマンド モード

VRRP インターフェイス コンフィギュレーション

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.9.0	このコマンドが導入されました。
リリース 4.1.0	IPv6 キーワードが追加されました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

BFD は冗長 VRRP ルータを 2 つのみ搭載したシステムでのみサポートされます。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、IPv6 アドレスの **bfd fast-detect** をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface tenGigE 0/4/0/4
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv6
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 3 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# bfd fast-detect peer ipv6 10:20::10
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp bfd minimum-interval</a> , (872 ページ)	特定のインターフェイスの BFD 最小間隔値を設定します。
<a href="#">vrrp bfd multiplier</a> , (874 ページ)	特定のインターフェイスの BFD 乗数値を設定します。

## vrrp bfd minimum-interval

BFD の最小間隔を特定のインターフェイス上のすべての VRRP BFD セッションで使用するよう設定するには、インターフェイス コンフィギュレーション モードで **vrrp bfd minimum-interval** コマンドを使用します。設定した最小期間を削除し、デフォルトの期間に設定するには、このコマンドの **no** 形式を使用します。

**vrrp bfd minimum-interval** *interval*

**no vrrp bfd minimum-interval** *interval*

### 構文の説明

*interval* ミリ秒単位で最小間隔を指定します。範囲は 15 ~ 30000 です。

### コマンド デフォルト

デフォルトの最小間隔は 15 ミリ秒です。

### コマンド モード

VRRP 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	変更箇所
リリース 3.9.0	このコマンドが導入されました。
リリース 4.1.0	このコマンドはすでに廃止されています。このコマンドは、 <a href="#">bfd minimum-interval (VRRP)</a> 、 <a href="#">(841 ページ)</a> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

最小間隔は BFD ピアに BFD パケットを送信する頻度を決定します。これはセッションに送信される連続的な BFD パケット間の時間です。最小間隔はミリ秒単位で指定します。設定された最小間隔は、インターフェイス上のすべての BFD セッションに適用されます。



## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、100 ミリ秒の最小間隔を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp  
RP/0/RSP0/CPU0:router(config-vrrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp bfd minimum-interval 100
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp bfd fast-detect</a> , (870 ページ)	VRRP インターフェイスで BFD をイネーブルにします。

## vrrp bfd multiplier

BFD 乗数値を設定するには、インターフェイス コンフィギュレーション モードで **vrrp bfd multiplier** コマンドを使用します。設定した乗数値を削除し、乗数値をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

**vrrp bfd multiplier multiplier**

**no vrrp bfd multiplier multiplier**

### 構文の説明

*multiplier* BFD 乗数値を指定します。範囲は 2 ~ 50 です。

### コマンド デフォルト

デフォルト値は 3 です。

### コマンド モード

VRRP 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	変更箇所
リリース 3.9.0	このコマンドが導入されました。
リリース 4.1.0	このコマンドはすでに廃止されています。このコマンドは、 <a href="#">bfd multiplier (VRRP)</a> 、 <a href="#">(843 ページ)</a> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

乗数値によって、期待どおりに受信していない場合に BFD セッションがダウンする連続 BFD パケットの数が指定されます。BFD 乗数値は、インターフェイス上に設定されたすべての BFD セッションに適用されます。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、乗数値 10 を使用して BFD 乗数値を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp  
RP/0/RSP0/CPU0:router(config-vrrp)# interface gig 0/1/1/0  
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp bfd multiplier 10
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp bfd fast-detect</a> , (870 ページ)	VRRP インターフェイスで BFD をイネーブルにします。

## vrrp delay

VRRP ルータのアクティベーション遅延を設定するには、VRRP インターフェイス コンフィギュレーション モードで **vrrp delay** コマンドを使用します。アクティベーション遅延を削除するには、このコマンドの **no** 形式を使用します。

**vrrp delay minimum value reload value**

**no vrrp delay**

### 構文の説明

<b>minimum value</b>	すべてのインターフェイス起動イベントの最小遅延（秒単位）を設定します。範囲は 0 ～ 10000 です。
<b>reload value</b>	最初のインターフェイス起動イベントのリロード遅延（秒単位）を設定します。範囲は 0 ～ 10000 です。

### コマンド デフォルト

**minimum value** : 1

**reload value** : 5

### コマンド モード

VRRP 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	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.1.0	このコマンドはすでに廃止されています。このコマンドは、 <a href="#">delay (VRRP)</a> 、 <a href="#">(850ページ)</a> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**vrrp delay** コマンドは、インターフェイス起動イベントで VRRP Finite State Machine (FSM; 有限状態マシン) の開始を遅らせて、インターフェイスがトラフィックを通過する準備を整えます。これにより、hello パケットの損失によるエラー状態にならないようにします。最小遅延はすべての

インターフェイス起動イベントに適用され、リロード遅延は最初のインターフェイス起動イベントに適用されます。

この機能をオフにするには、ゼロの値を明示的に設定する必要があります。

#### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

#### 例

次に、最小遅延を 10 秒にしてリロード遅延を 100 秒にする例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface mgmtEth 0/RSP0/CPU0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp delay minimum 10 reload 100
```

#### 関連コマンド

コマンド	説明
<a href="#">show vrrp</a> , (858 ページ)	1 つまたはすべての仮想ルータ冗長プロトコル (VRRP) 仮想ルータの要約ステータスまたは詳細ステータスを表示します。

## vrrp ipv4

インターフェイス上の仮想ルータ冗長プロトコル (VRRP) をイネーブルにして、仮想ルータの IP アドレスを指定するには、VRRP インターフェイスコンフィギュレーションモードで **vrrp ipv4** コマンドを使用します。インターフェイス上の VRRP をディセーブルにして、仮想ルータの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

**vrrp vrid ipv4 ip-address [secondary]**

**no vrrp vrid ipv4 ip-address [secondary]**

### 構文の説明

<i>vrid</i>	仮想ルータ ID、つまり、仮想ルータを識別する番号です。範囲は 1 ~ 255 です。
<i>ip-address</i>	仮想ルータの IP アドレス
<b>secondary</b>	(任意) このグループがサポートする追加の IP アドレスを示します。

### コマンド デフォルト

VRRP はインターフェイスに設定されていません。

### コマンド モード

VRRP 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	変更箇所
リリース 3.7.2	このコマンドが導入されました。
リリース 4.1.0	このコマンドはすでに廃止されています。このコマンドは、 <a href="#">address (VRRP)</a> 、 <a href="#">(833 ページ)</a> コマンドに置き換えられました。

### 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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

仮想ルータ IP アドレスを示すには、**vrrp ipv4** コマンドを 1 回、**secondary** キーワードなしで設定します。仮想ルータがサポートする追加の IP アドレスを示したい場合、**secondary** キーワードを追加します。

VRRP 設定を IP アドレス オーナーから削除してインターフェイスの IP アドレスをアクティブなままにすることは、LAN 上に IP アドレスの重複コピーが作成されるため設定ミスと見なされま

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、10-ギガビットイーサネットインターフェイス 0/3/0/0 の VRRP をイネーブルにする例を示します。VRRP 仮想ルータ ID は 1 で、10.0.1.10 は仮想ルータの IP アドレスです。セカンダリ IP アドレスは 10.0.1.20 です。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0

RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp 1 ipv4 10.0.1.20 secondary
RP/0/RSP0/CPU0:router(config-vrrp-if)# vrrp ipv4 10.0.1.0
```

## 関連コマンド

コマンド	説明
<a href="#">show vrrp</a> , ( <a href="#">858 ページ</a> )	1 つまたはすべての仮想ルータ冗長プロトコル (VRRP) 仮想ルータの要約ステータスまたは詳細ステータスを表示します。

## vrrp preempt

VRRP プリエンプションはデフォルトでイネーブルです。つまり、マスター VRRP ルータよりもプライオリティが高い VRRP ルータがマスタールータとして引き継ぎます。この機能をディセーブルにするには、**preempt disable** コマンドを使用します。プライオリティの高いルータが引き継ぐ前にしばらく待つように、プリエンプレションを遅らせるには、**preempt delay** コマンドを使用します。デフォルトの動作（遅延なしでプリエンプレションがイネーブルになっている）に戻すには、このコマンドの **no** 形式を使用します。

**preempt** {*delay seconds*| **disable**}

**no preempt** {*delay seconds*| **disable**}

### 構文の説明

<b>delay seconds</b>	IP アドレス所有権を要求するアドバタイズメントをマスタールータに発行するまでルータが遅延する秒数を指定します。範囲は 1 ～ 3600 秒（1 時間）です。
<b>disable</b>	プリエンプレションをディセーブルにします。

### コマンド デフォルト

VRRP プリエンプションはイネーブルにされています。

*seconds* : 0（遅延なし）

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

デフォルトでは、このコマンドで設定されるルータは、現在のマスタールータよりも高いプライオリティを持つ場合、仮想ルータのマスタールータとしての機能を引き継ぎます。マスタールータになる仮想 IP アドレス所有権を要求するアドバタイズメントを発行するまで、VRRP ルータを指定された秒数だけ待機させる遅延を設定できます。





(注) 仮想 IP アドレスのオーナーであるルータは、このコマンドの設定に関係なく、プリエンプトします。

#### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

#### 例

次に、ルータの 200 のプライオリティが現在のマスタールータのプライオリティよりも高い場合にルータが現在のマスタールータをプリエンプトするように設定する例を示します。ルータは、現在のマスタールータをプリエンプトする場合、マスタールータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# preempt delay 15
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# priority 200
```

#### 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , (878 ページ)	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。
<a href="#">vrrp priority</a> , (882 ページ)	仮想ルータのプライオリティを設定します。

## vrrp priority

仮想ルータのプライオリティを設定するには、VRRP 仮想ルータ サブモードで **priority** コマンドを使用します。仮想ルータのプライオリティを削除するには、このコマンドの **no** 形式を使用します。

**priority** *priority*

**no**priority *priority*

### 構文の説明

*priority* 仮想ルータのプライオリティ。範囲は 1 ～ 254 です。

### コマンド デフォルト

*priority* : 100

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このコマンドを使用すると、どのルータをマスタールータにするかを制御できます。このコマンドは、ルータが仮想 IP アドレスのオーナーである間は無視されます。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、ルータを 254 のプライオリティに設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp  
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0  
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4  
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 3  
RP/0/RSP0/CPU0:router(config-vrrp-virtual router)# priority 254
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , ( <a href="#">878 ページ</a> )	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。
<a href="#">vrrp preempt</a> , ( <a href="#">880 ページ</a> )	どのルータをマスタールータにするかを制御します。

## vrrp text-authentication

VRRP を実行している他のルータから受信した仮想ルータ冗長プロトコル (VRRP) パケットに使用される簡易テキスト認証を設定するには、VRRP 仮想ルータ サブモードで **text-authentication** コマンドを使用します。VRRP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

**text-authentication** *string*

**no text-authentication** [ *string* ]

### 構文の説明

<i>string</i>	着信 VRRP パケットの検証に使用する認証ストリング (最大 8 字の英数字)。
---------------	---

### コマンド デフォルト

VRRP メッセージの認証を行いません。

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

VRRP パケットが別のルータから到着すると、その認証ストリングが、ローカル システムに設定されたストリングと比較されます。ストリングが一致する場合、そのメッセージが受け入れられます。一致しない場合、そのパケットは廃棄されます。

グループ内のすべてのルータは、同じ認証ストリングで設定される必要があります。



(注) プレーン テキスト認証は、セキュリティに使用されることになっていないではありません。それは、設定ミスのルータが VRRP に参加しないようにする方法を提供しているに過ぎません。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、x30dn78k の認証ストリングを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 2
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# text-authentication x30dn78k
```



(注) テキスト認証は VRRP バージョン 2 ルータでのみ有効です。

## 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , <a href="#">(878 ページ)</a>	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。

## vrrp timer

仮想ルータ冗長プロトコル（VRRP）仮想ルータ内のマスター ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP 仮想ルータサブモードで **timer** 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。

**timer [msec] interval [force]**

**no timer [msec] interval [force]**

### 構文の説明

<b>msec</b>	(任意) アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。範囲は 20 ～ 3000 ミリ秒です。
<b>interval</b>	マスタールータによる連続したアドバタイズメント間の時間間隔。 <b>msec</b> キーワードが指定されない限り、間隔の単位は秒です。範囲は 1 ～ 255 秒です。
<b>force</b>	(任意) 設定値を強制的に使用します。このキーワードは、ミリ秒を指定する場合に必須になります。

### コマンド デフォルト

*interval* : 1 秒

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

### タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次に、マスター ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# timer 4
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp ipv4</a> , ( <a href="#">878 ページ</a> )	インターフェイス上の VRRP をイネーブルにし、仮想ルータの IP アドレスを指定します。

## vrrp track interface

仮想ルータ冗長プロトコル（VRRP）がインターフェイスをトラッキングするように設定するには、VRRP 仮想ルータ サブモードで **track interface** コマンドを使用します。トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

**track interface** *type interface-path-id* [ *priority-decrement* ]

**no track interface** *type interface-path-id* [ *priority-decrement* ]

### 構文の説明

<i>vrid</i>	仮想ルータ ID、つまり、トラッキングが適用される仮想ルータを識別する番号です。
<i>type</i>	インターフェイスのタイプ。詳細については、疑問符 (?) オンラインヘルプ機能を使用してください。
<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、 <b>show interfaces</b> 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>priority-decrement</i>	(任意) トラッキングされたインターフェイスがダウンした場合のルータのプライオリティの減少数（または増加数）。減少分は、1 ~ 254 の任意の値に設定できます。デフォルト値は 10 です。

### コマンド デフォルト

デフォルトの減少値は 10 です。範囲は 1 ~ 254 です。

### コマンド モード

VRRP 仮想ルータ

### コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが導入されました。



## コマンド履歴

リリース	変更箇所
リリース 3.2	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

**vrrp track interface** コマンドは、ルータのプライオリティを、そのインターフェイスのアベイラビリティに結合します。これは、VRRP に設定されていないインターフェイスをトラッキングする場合に便利です。IP インターフェイスだけがトラッキングされます。トラッキングされるインターフェイスは、そのインターフェイス上の IP が立ち上がると起動します。IP が立ち上がらないと、トラッキングされるインターフェイスはダウンします。

VRRP 仮想ルータの仮想ルータのプライオリティ レベルを VRRP が変更できるように設定できます。インターフェイスの IP プロトコル状態がダウンした場合、またはインターフェイスがルータから削除された場合、バックアップ仮想ルータのプライオリティは、*priority-decrement* 引数内に指定された値により減少します。インターフェイスの IP プロトコル状態が起動状態になると、プライオリティが元に戻ります。

## タスク ID

タスク ID	操作
vrrp	読み取り、書き込み

## 例

次の例では、10 ギガビットイーサネットインターフェイス 0/3/0/0 がインターフェイス 0/3/0/3 および 0/3/0/2 をトラッキングしています。これらの 2 つのインターフェイスのいずれか、または両方がダウンすると、ルータのプライオリティが各インターフェイスに対して 10（デフォルトのプライオリティ減少数）だけ減少します。デフォルトのプライオリティ減少数は、*priority-decrement* 引数を使用して変更します。この例では、仮想ルータのデフォルトのプライオリティが 100 であるため、トラッキングされるインターフェイスのうちの 1 つがダウンするとプライオリティが 90 になり、両方のインターフェイスがダウンするとプライオリティが 80 になります。仮想ルータのプライオリティ設定の詳細については、**priority** コマンドを参照してください。

```
RP/0/RSP0/CPU0:router(config)# router vrrp
RP/0/RSP0/CPU0:router(config-vrrp)# interface TenGigE 0/3/0/0
RP/0/RSP0/CPU0:router(config-vrrp-if)# address-family ipv4
RP/0/RSP0/CPU0:router(config-vrrp-address-family)# vrrp 1 version 3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# track interface TenGigE 0/3/0/3
RP/0/RSP0/CPU0:router(config-vrrp-virtual-router)# track interface TenGigE 0/3/0/2
```

## 関連コマンド

コマンド	説明
<a href="#">vrrp priority</a> , (882 ページ)	仮想ルータのプライオリティを設定します。



# Cisco ASR 9000 シリーズ ルータでのビデオ モニタリング コマンド

---

この章では、Cisco ASR 9000 シリーズ ルータのビデオ モニタリング サービスを設定および監視するために使用するコマンドについて説明します。

ビデオ モニタリング の概念、設定作業、および例については、『*Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide*』の「*Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers*」の章を参照してください。

- [clear performance traffic clone profile](#), 892 ページ
- [clear performance traffic statistics](#), 893 ページ
- [show performance traffic alerts](#), 895 ページ
- [show performance traffic clone profile](#), 897 ページ
- [show policy-map type performance-traffic](#), 899 ページ

# clear performance traffic clone profile

宛先にクローンされたすべてのパケットをクリアするには、EXEC モードで **clear performance traffic clone profile** コマンドを使用します。

**clear performance traffic clone profile** *profile name*

## 構文の説明

*profile name* パケットをクリアする必要のあるクローンのプロファイル名。

## コマンド デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

リリース

変更箇所

リリース 4.0.1

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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID

操作

netflow

読み取り、書き込み

## 例

次に、コマンドライン インターフェイスから **clear performance traffic clone profile** コマンドを実行する例を示します。

```
RP/0/RSP0/CPU0:router#clear performance traffic clone
profile
```

# clear performance traffic statistics

すべてのポリシー マップ統計情報をクリアするには、EXEC モードで **clear performance traffic statistics** コマンドを使用します。このコマンドは、集約統計情報を除くすべての間隔統計情報をクリアします。

**clear performance traffic statistics interface type instance input**

## 構文の説明

<b>interface</b>	統計情報をクリアする必要があるすべてのインターフェイスまたは特定のインターフェイスを指定します。
<b>input</b>	トラフィックの方向を指定します。

## コマンド デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 3.9.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
netflow	読み取り、書き込み

## 例

次に、コマンドライン インターフェイスから **clear performance traffic statistics** コマンドを実行する例を示します。

```
RP/0/RSP0/CPU0:router clear performance traffic statistics interface gigabitEthernet  
0/0/0/8 input
```

## show performance traffic alerts

アクティブ TCA（しきい値超過アラート）を表示するには、EXEC モードで **show performance traffic alerts** コマンドを使用します。TCA は、設定されたパラメータが満たされる場合に設定されます。TCA は、設定されたパラメータが **true** でない場合にクリアされます。イベントは、設定およびクリアの両方について生成されます。

### show performance traffic alerts interface *type instance* input

#### 構文の説明

**interface** パフォーマンス トラフィック アラートが設定される特定のインターフェイスまたはすべてのインターフェイスを指定します。

#### コマンド デフォルト

なし

#### コマンド モード

EXEC

#### コマンド履歴

リリース	変更箇所
リリース 3.9.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

#### タスク ID

タスク ID	操作
netflow	読み取り

#### 例

これは、**show performance traffic alerts** コマンドの出力例です。

```
RP/0/RSP0/CPU0:router# show performance traffic alerts interface ten0/6/0/0 input
Interface: TenGigE0/6/0/0 Direction: input
```

## show performance traffic alerts

```

GROUP Alerts
Class: class1
Num Flows: 1
Num Grouped Alerts: 1
Highest Alert Severity: Warning
React ID      Severity      Metric
-----      -
          4      Critical      Flow Count

FLOW Alerts
Flow ID: 3496 Class: class1
Num Alerts: 3
Highest Alert Severity: Warning
React ID      Severity      Metric
-----      -
          1      Critical
          2      Critical      Media Rate Variation
          5      Critical      Delay Factor

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 89 : show performance traffic alerts のフィールドの説明

フィールド	説明
Group/Flow Alerts	このアラートは、グループ化されるか、または単一フローに適用されます。
Class	ポリシーで使用されるクラス マップ名。
Flow ID	フローの固有識別子。 (注) フロー ID 番号はアンバインドおよび再バインドごとに異なるものになります。
Num Flows	このグループアラートで設定されたフロー数。
Num Grouped Alerts	グループ化されたアラートの合計数。
Num Alerts	フローにより設定されたアラートの合計数。
Severity	設定された重大度を示します。
Highest Alert Severity	設定されたアラートの最も高い重大度を示します。
React ID	設定された反応 ID を指定します。
Metric	設定されたアラートのタイプを示します。



# show performance traffic clone profile

設定されたトラップ、クローンプロファイル、および関連付けられたクローンフローを表示するには、EXEC モードで **show performance traffic clone profile** コマンドを使用します。

**show performance traffic clone profile** *profile name*

## 構文の説明

*profile name* クローンのプロファイル名。

## コマンド デフォルト

なし

## コマンド モード

EXEC

## コマンド履歴

リリース	変更箇所
リリース 4.0.1	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
netflow	読み取り

## 例

次に、コマンドライン インターフェイスから **show performance traffic clone profile** コマンドを実行する例を示します。

```
RP/0/RSP0/CPU0:router#show performance traffic clone
profile
```

```
-----
Total number of trap and clone profiles: 3
-----
```

```
Profile Name: profile1                               ID: 1
-----
```

## show performance traffic clone profile

```

description:          new_profile
egress interface:    GigabitEthernet0_0_0_8
total number of clone flows: 2
-----
clone  id      source      destination
     1      2.2.2.2    229.1.1.1
     2      2.2.2.2    229.1.1.2
-----
Profile Name: profile2                               ID: 2
-----
description:          second profile
egress interface:    GigabitEthernet0_0_0_19
total number of clone flows: 5
-----
clone  id      source      destination
     1      1.1.1.1    229.1.1.10
     2      1.1.1.1    229.1.1.11
     3      1.1.1.1    229.1.1.12
     4      1.1.1.1    229.1.1.14
     5      1.1.1.1    229.1.1.15
-----
Profile Name: profile3                               ID: 3
-----
description:          third profile
egress interface:    TenGigE0_2_0_1
total number of clone flows: 13
-----
clone  id      source      destination
     1      12.12.12.12 233.1.1.1
     2      12.12.12.12 233.1.1.2
     3      12.12.12.12 233.1.1.3
     4      12.12.12.12 233.1.1.4
     5      12.12.12.12 233.1.1.5
     6      12.12.12.12 233.1.1.6
     7      12.12.12.12 233.1.1.7
     8      12.12.12.12 233.1.1.8
     9      12.12.12.12 233.1.1.10
    10      12.12.12.12 233.1.1.11
    11      12.12.12.12 233.1.1.12
    12      12.12.12.12 233.1.1.16
    13      12.12.12.12 233.1.1.18

```

## show policy-map type performance-traffic

ビデオ モニタリング機能のポリシー マップ統計情報を表示するには、EXEC モードで **show policy-map type performance-traffic** コマンドを使用します。このコマンドにより、サービス プロバイダーのビデオ フローの Quality of Experience (QoE) を監視できます。

**show policy-map type performance-traffic interface *type instance* [aggregate| brief| cumulative| detail| input| last| match]**

### 構文の説明

<b>interface</b> <i>type instance</i>	表示する特定のインターフェイスを指定します。
<b>aggregate</b>	(任意) フローの合計数と最終変更時刻を表示します。
<b>brief</b>	(任意) キー メトリックだけを表示します。
<b>cumulative</b>	(任意) フローのライフタイムにおける累積統計情報を表示します。
<b>detail</b>	(任意) 詳細なメトリックを表示します。
<b>input</b>	(任意) 入力トラフィック ポリシーを表示します。
<b>last</b>	(任意) 最後の <i>n</i> 個の間隔を表示します。
<b>match</b>	(任意) フィルタリングする一致基準を指定します。

### コマンド デフォルト

コマンドのデフォルト値は 1 です。

### コマンド モード

EXEC

### コマンド履歴

リリース	変更箇所
リリース 3.9.0	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のためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

## タスク ID

タスク ID	操作
netflow	読み取り

## 例

次に、**show policy-map type performance-traffic** コマンドのさまざまな出力例を示します。

```
RP/0/RSP0/CPU0:router# show policy-map type performance-traffic interface tenGigE 0/6/0/0
brief
```

```
-----
Interface:      TenGigE0/6/0/0      Direction: input
Service-Policy: policy1
-----
Total Num Flows: 2
FlowID   Flow Key                               MRV(%)  DF (ms)
-----
   3528   6.1.1.2:4000      -> 225.0.0.1:4000   UDP      0.000    3.337
   3496   6.1.1.2:4000      -> 225.0.0.101:4000  UDP      50.000   2502.220
-----

Class Name                               Num-Flows
-----
class1                                    2
-----
```

```
RP/0/RSP0/CPU0:router#show policy-map type performance-traffic interface tenGigE0/6/0/0
aggregate brief
```

```
Interface: TenGigE0/6/0/0 Direction: input

Number of flows      : 2
Last flow add/delete : Tue Nov  3 13:46:56 2009
```

```
RP/0/RSP0/CPU0:ios#show policy-map type performance-traffic interface ten0/6/0/0 detail
Tue Nov  3 13:52:02.046 EST
```

```
-----
Interface:      TenGigE0/6/0/0      Direction: input
Service-Policy: policy1
-----
Total Num Flows: 2

Flow: 3528      Key: 6.1.1.2:4000 -> 225.0.0.1:4000 UDP
Class: class1                                     Total Intvls: 1
Intvl# 1, Updated at: Tue Nov  3 13:51:56 2009, Duration: 10 s
Metric type:   IP-CBR
MRV:           0.000 %                               DF:           3.338 ms
Avg Packet Rate: 300.00 pps                           Total Packets: 3000
Avg Bit Rate:   3158 kbps                               Total Bytes:   3948000
Avg Packet Len: 1316.00 B
IPv4 TTL:      63

Flow: 3496      Key: 6.1.1.2:4000 -> 225.0.0.101:4000 UDP
Class: class1                                     Total Intvls: 1
Intvl# 1, Updated at: Tue Nov  3 13:51:54 2009, Duration: 10 s
Metric type:   IP-CBR
MRV:           50.000 %                               DF:           2502.220 ms
Avg Packet Rate: 450.00 pps                           Total Packets: 4500
Avg Bit Rate:   4737 kbps                               Total Bytes:   5922000
Avg Packet Len: 1316.00 B
IPv4 TTL:      63
-----
```

```

-----
Class Name                               Num-Flows
-----
class1                                    2
-----

RP/0/RSP0/CPU0:router#show policy-map type performance-traffic interface tenGigE0/6/0/0
last 5

-----
Interface:      TenGigE0/6/0/0      Direction: input
Service-Policy: policy1
-----

Total Num Flows: 2

Flow: 3528      Key: 6.1.1.2:4000 -> 225.0.0.1:4000 UDP
Class: class1
-----
Intvl#  Updated at                Durn  MRV(%)  DF (ms)
-----
1      Tue Nov 3 13:53:26 2009    10     0.000   3.337
2      Tue Nov 3 13:53:16 2009    10     0.000   3.337
3      Tue Nov 3 13:53:06 2009    10     0.000   3.337
4      Tue Nov 3 13:52:56 2009    10     0.000   3.337
5      Tue Nov 3 13:52:46 2009    10     0.000   3.337
-----

Flow: 3496      Key: 6.1.1.2:4000 -> 225.0.0.101:4000 UDP
Class: class1
-----
Intvl#  Updated at                Durn  MRV(%)  DF (ms)
-----
1      Tue Nov 3 13:53:24 2009    10    50.000  2502.220
2      Tue Nov 3 13:53:14 2009    10    50.000  2502.220
3      Tue Nov 3 13:53:04 2009    10    50.000  2502.220
4      Tue Nov 3 13:52:54 2009    10    50.000  2502.220
5      Tue Nov 3 13:52:44 2009    10    50.000  2502.220
-----

-----
Class Name                               Num-Flows
-----
class1                                    2
-----

RP/0/RSP0/CPU0:router#show policy-map type performance-traffic interface tenGigE0/6/0/0
match flow-id 3496

-----
Interface:      TenGigE0/6/0/0      Direction: input
Service-Policy: policy1
-----

Total Num Flows: 2
FlowID  Flow Key                               MRV(%)  DF (ms)
-----
3496    6.1.1.2:4000      -> 225.0.0.101:4000  UDP    50.000  2502.220
-----

Num Flows Displayed: 1
-----

```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 90 : show policy-map type performance traffic コマンドの説明

フィールド	説明
DF	遅延係数。
Mrv	メディア レート変動。
Total intvls	ユーザ定義間隔の数。

## show policy-map type performance-traffic

フィールド	説明
Service-policy	このフローのサービス ポリシーの名前。
Duration	間隔の長さ。
Num-flows	このポリシーに一致するフローの合計数。
Flow	一意のフロー ID。



## 索引

### A

accept-mode コマンド [829](#)  
address-family コマンド [831](#)  
address (hsrp) コマンド [391](#)  
address global コマンド [835](#)  
address linklocal コマンド [837](#)  
address secondary (hsrp) コマンド [393](#)  
address secondary コマンド [839](#)  
address コマンド [833](#)  
arp dagr コマンド [107](#)  
arp purge-delay コマンド [109](#)  
arp timeout コマンド [111](#)  
arp コマンド [104](#)  
authentication (hsrp) コマンド [395](#)

### B

bfd fast-detect (hsrp) コマンド [397](#)

### C

cinetd rate-limit コマンド [327](#)  
clear access-list ipv4 コマンド [3](#)  
clear access-list ipv6 コマンド [6](#)  
clear adjacency statistics コマンド [140](#)  
clear arp-cache コマンド [113](#)  
clear cef ipv4 drops コマンド [142](#)  
clear cef ipv4 exceptions コマンド [144](#)  
clear cef ipv4 interface bgp-policy-statistics コマンド [146](#)  
clear cef ipv4 interface rpf-statistics コマンド [148](#)  
clear cef ipv6 drops コマンド [150](#)  
clear cef ipv6 exceptions コマンド [152](#)  
clear cef ipv6 interface bgp-policy-statistics コマンド [154](#)  
clear dhcp ipv4 snoop binding コマンド [265](#)  
clear host コマンド [329](#)

clear hsrp statistics コマンド [399](#)  
clear ipv6 neighbors コマンド [542](#)  
clear lpts ifib statistics コマンド [471](#)  
clear lpts pifib hardware statistics コマンド [473](#)  
clear lpts pifib statistics コマンド [476](#)  
clear nsr ncd client コマンド [725](#)  
clear nsr ncd queue コマンド [727](#)  
clear performance traffic clone profile コマンド [892](#)  
clear performance traffic statistics コマンド [893](#)  
clear prefix-list ipv4 コマンド [688](#)  
clear prefix-list ipv6 コマンド [690](#)  
clear raw statistics pcb コマンド [730](#)  
clear tcp nsr client コマンド [732](#)  
clear tcp nsr pcb コマンド [734](#)  
clear tcp nsr session-set コマンド [737](#)  
clear tcp nsr statistics client コマンド [739](#)  
clear tcp nsr statistics pcb コマンド [741](#)  
clear tcp nsr statistics session-set コマンド [744](#)  
clear tcp nsr statistics summary コマンド [746](#)  
clear tcp pcb コマンド [748](#)  
clear tcp statistics コマンド [750](#)  
clear udp statistics コマンド [752](#)  
clear vrrp statistics コマンド [845](#)  
copy access-list ipv4 コマンド [9](#)  
copy access-list ipv6 コマンド [11](#)  
copy prefix-list ipv4 コマンド [692](#)  
copy prefix-list ipv6 コマンド [694](#)

### D

delay コマンド [850](#)  
deny (IPv4) コマンド [13](#)  
deny (プレフィックスリスト) コマンド [696](#)  
deny (IPv6) コマンド [25](#)  
destination (DHCP IPv6) コマンド [269](#)  
dhcp ipv4 none コマンド [276](#)

dhcp ipv4 コマンド [272](#)  
 dhcp ipv6 コマンド [274](#)  
 domain ipv4 host コマンド [331](#)  
 domain ipv6 host コマンド [333](#)  
 domain list コマンド [335](#)  
 domain lookup disable コマンド [337](#)  
 domain name-server コマンド [341](#)  
 domain name (グローバル) コマンド [339](#)

## F

flow (LPTS) コマンド [478](#)  
 forward-protocol udp コマンド [754](#)  
 ftp client anonymous-password コマンド [343](#)  
 ftp client passive コマンド [345](#)  
 ftp client password コマンド [347](#)  
 ftp client source-interface コマンド [349](#)  
 ftp client username コマンド [351](#)

## G

giaddr policy コマンド [278](#)

## H

helper-address (IPv6) コマンド [282](#)  
 helper-address コマンド [280](#)  
 hsrp authentication コマンド [401](#)  
 hsrp bfd fast-detect コマンド [403](#)  
 hsrp bfd minimum-interval コマンド [405](#)  
 hsrp bfd multiplier コマンド [407](#)  
 hsrp delay コマンド [409](#)  
 hsrp ipv4 コマンド [411](#)  
 hsrp mac-address コマンド [413](#)  
 hsrp preempt コマンド [416](#)  
 hsrp priority コマンド [418](#)  
 hsrp redirects コマンド [420](#)  
 hsrp timers コマンド [422](#)  
 hsrp track コマンド [425](#)  
 hsrp use-bia コマンド [428](#)

## I

icmp ipv4 rate-limit unreachable コマンド [544](#)

interface (DHCP) コマンド [285](#)  
 interface (HSRP) コマンド [430](#)  
 interface (VRRP) コマンド [852](#)  
 ipv4 access-group コマンド [31](#)  
 ipv4 access-list log-update rate コマンド [36](#)  
 ipv4 access-list log-update threshold コマンド [38](#)  
 ipv4 access-list コマンド [34](#)  
 ipv4 address (ネットワーク) コマンド [546](#)  
 ipv4 assembler max-packets コマンド [549](#)  
 ipv4 assembler timeout コマンド [551](#)  
 ipv4 bgp policy accounting コマンド [156](#)  
 ipv4 bgp policy propagation コマンド [159](#)  
 ipv4 conflict-policy コマンド [553](#)  
 ipv4 directed-broadcast コマンド [555](#)  
 ipv4 helper-address コマンド [557](#)  
 ipv4 mask-reply コマンド [559](#)  
 ipv4 mtu コマンド [561](#)  
 ipv4 prefix-list コマンド [699](#)  
 ipv4 redirects コマンド [563](#)  
 ipv4 source-route コマンド [565](#)  
 ipv4 unnumbered (point-to-point) コマンド [567](#)  
 ipv4 unreachable disable コマンド [570](#)  
 ipv4 verify unicast source reachable-via コマンド [161](#)  
 ipv4 virtual address コマンド [572](#)  
 ipv6 access-group コマンド [40](#)  
 ipv6 access-list log-update rate コマンド [47](#)  
 ipv6 access-list log-update threshold コマンド [49](#)  
 ipv6 access-list maximum ace threshold コマンド [51](#)  
 ipv6 access-list maximum acl threshold コマンド [53](#)  
 ipv6 access-list コマンド [43](#)  
 ipv6 address link-local コマンド [576](#)  
 ipv6 address コマンド [574](#)  
 ipv6 assembler コマンド [578](#)  
 ipv6 conflict-policy コマンド [580](#)  
 ipv6 enable コマンド [582](#)  
 ipv6 hop-limit コマンド [584](#)  
 ipv6 icmp error-interval コマンド [586](#)  
 ipv6 mtu コマンド [588](#)  
 ipv6 nd dad attempts コマンド [590](#)  
 ipv6 nd managed-config-flag コマンド [593](#)  
 ipv6 nd ns-interval コマンド [595](#)  
 ipv6 nd other-config-flag コマンド [597](#)  
 ipv6 nd prefix コマンド [599](#)  
 ipv6 nd ra-interval コマンド [602](#)  
 ipv6 nd ra-lifetime コマンド [604](#)  
 ipv6 nd reachable-time コマンド [606](#)  
 ipv6 nd redirects コマンド [608](#)



ipv6 nd scavenge-timeout コマンド 610  
 ipv6 nd suppress-ra コマンド 612  
 ipv6 neighbor コマンド 614  
 ipv6 prefix-list コマンド 702  
 ipv6 source-route コマンド 617  
 ipv6 unreachable disable コマンド 619  
 ipv6 verify unicast source reachable-via コマンド 164

## L

local pool コマンド 621  
 lpts pifib hardware police コマンド 485

## M

mac-address (hsrp) コマンド 432  
 message state disable コマンド 854

## N

nsr process-failures switchover コマンド 756

## P

peer (DAGR) コマンド 115  
 permit (IPv4) コマンド 55  
 permit (プレフィックス リスト) コマンド 704  
 permit (IPv6) コマンド 75  
 ping (ネットワーク) コマンド 353  
 ping bulk (ネットワーク) コマンド 357  
 preempt (hsrp) コマンド 434  
 priority-timeout コマンド 117  
 priority (hsrp) コマンド 436  
 profile コマンド 287  
 proxy-arp コマンド 119

## R

rcp client source-interface コマンド 360  
 rcp client username コマンド 362  
 relay information check コマンド 291  
 relay information option allow-untrusted コマンド 296  
 relay information option コマンド 293  
 relay information policy コマンド 299

remark (IPv4) コマンド 81  
 remark (IPv6) コマンド 83  
 remark (プレフィックス リスト) コマンド 707  
 resequence access-list ipv4 コマンド 85  
 resequence access-list ipv6 コマンド 88  
 resequence prefix-list ipv4 コマンド 709  
 resequence prefix-list ipv6 コマンド 712  
 route distance コマンド 121  
 route metric コマンド 123  
 router hsrp コマンド 438  
 router vrrp コマンド 856  
 rp mgmtethernet forwarding コマンド 166

## S

service tcp-small-servers コマンド 757  
 service udp-small-servers コマンド 759  
 session name コマンド 440  
 show access-lists afi-all コマンド 91  
 show access-lists ipv4 コマンド 92  
 show access-lists ipv6 コマンド 98  
 show adjacency コマンド 168  
 show arm conflicts コマンド 625  
 show arm database コマンド 628  
 show arm registrations producers コマンド 633  
 show arm router-ids コマンド 631  
 show arm summary コマンド 635  
 show arm vrf-summary コマンド 637  
 show arp dagr コマンド 130  
 show arp traffic コマンド 132  
 show arp コマンド 125  
 show cef bgp-attribute コマンド 173  
 show cef external コマンド 175  
 show cef ipv4 adjacency hardware コマンド 189  
 show cef ipv4 adjacency コマンド 186  
 show cef ipv4 drops コマンド 192  
 show cef ipv4 exact-route コマンド 195  
 show cef ipv4 exceptions コマンド 198  
 show cef ipv4 hardware コマンド 201  
 show cef ipv4 interface bgp-policy-statistics コマンド 206  
 show cef ipv4 interface コマンド 203  
 show cef ipv4 non-recursive コマンド 209  
 show cef ipv4 resource コマンド 213  
 show cef ipv4 summary コマンド 215  
 show cef ipv4 unresolved コマンド 218  
 show cef ipv4 コマンド 183

- show cef ipv6 adjacency hardware コマンド 226
- show cef ipv6 adjacency コマンド 224
- show cef ipv6 drops コマンド 228
- show cef ipv6 exact-route コマンド 232
- show cef ipv6 exceptions コマンド 234
- show cef ipv6 hardware コマンド 237
- show cef ipv6 interface コマンド 239
- show cef ipv6 non-recursive コマンド 241
- show cef ipv6 resource コマンド 244
- show cef ipv6 summary コマンド 246
- show cef ipv6 unresolved コマンド 249
- show cef ipv6 コマンド 220
- show cef mpls adjacency hardware コマンド 254
- show cef mpls adjacency コマンド 251
- show cef mpls interface コマンド 256
- show cef mpls unresolved コマンド 258
- show cef recursive-nexthop コマンド 178
- show cef summary コマンド 180
- show cef vrf コマンド 260
- show cef コマンド 171
- show cinetd services コマンド 364
- show elns statistics コマンド 639
- show dhcp ipv4 relay profile name コマンド 304
- show dhcp ipv4 relay profile コマンド 302
- show dhcp ipv4 relay statistics コマンド 306
- show dhcp ipv4 snoop binding コマンド 308
- show dhcp ipv4 snoop statistics コマンド 313
- show dhcp ipv6 interface コマンド 310
- show dhcp ipv6 proxy binding コマンド 315
- show hosts コマンド 366
- show hsrp bfd コマンド 447
- show hsrp mgo コマンド 449
- show hsrp statistics コマンド 451
- show hsrp summary 453
- show hsrp コマンド 442
- show ipv4 interface コマンド 641
- show ipv4 traffic コマンド 647
- show ipv6 interface コマンド 650
- show ipv6 neighbors summary コマンド 660
- show ipv6 neighbors コマンド 654
- show ipv6 traffic コマンド 662
- show local pool コマンド 645
- show lpts bindings コマンド 487
- show lpts clients コマンド 492
- show lpts flows コマンド 495
- show lpts ifib slices コマンド 503
- show lpts ifib statistics コマンド 507
- show lpts ifib times コマンド 509
- show lpts ifib コマンド 499
- show lpts mpa groups コマンド 511
- show lpts pifib hardware context コマンド 519
- show lpts pifib hardware entry コマンド 522
- show lpts pifib hardware police コマンド 526
- show lpts pifib hardware usage コマンド 530
- show lpts pifib statistics コマンド 532
- show lpts pifib コマンド 513
- show lpts port-arbitrator statistics コマンド 534
- show lpts vrf コマンド 536
- show mpa client コマンド 665
- show mpa groups コマンド 667
- show mpa ipv4 コマンド 669
- show mpa ipv6 コマンド 671
- show nsr ncd client コマンド 761
- show nsr ncd queue コマンド 764
- show performance traffic alerts コマンド 895
- show policy-map type performance-traffic コマンド 899
- show prefix-list afi-all コマンド 715
- show prefix-list ipv4 standby コマンド 718
- show prefix-list ipv4 コマンド 716
- show prefix-list ipv6 コマンド 720
- show prefix-list コマンド 714
- show raw brief コマンド 766
- show raw detail pcb コマンド 768
- show raw extended-filters コマンド 770
- show raw statistics pcb コマンド 773
- show tcp brief コマンド 776
- show tcp detail コマンド 778
- show tcp extended-filters コマンド 780
- show tcp nsr brief コマンド 784
- show tcp nsr client brief コマンド 787
- show tcp nsr detail client コマンド 789
- show tcp nsr detail pcb コマンド 791
- show tcp nsr detail session-set コマンド 794
- show tcp nsr session-set brief コマンド 796
- show tcp nsr statistics client コマンド 799
- show tcp nsr statistics pcb コマンド 801
- show tcp nsr statistics session-set コマンド 804
- show tcp nsr statistics summary コマンド 806
- show tcp statistics コマンド 782
- show udp brief コマンド 808
- show udp detail pcb コマンド 810
- show udp extended-filters コマンド 812
- show udp statistics コマンド 814
- show vrf コマンド 673

show vrrp コマンド [858](#)  
slave follow コマンド [455](#)  
slave primary virtual IPv4 address コマンド [457](#)  
slave secondary virtual IPv4 address コマンド [459](#)  
slave virtual mac address コマンド [461](#)  
snmp-server traps vrrp events コマンド [864](#)

## T

tcp mss コマンド [816](#)  
tcp path-mtu-discovery コマンド [818](#)  
tcp selective-ack コマンド [820](#)  
tcp synwait-time コマンド [822](#)  
tcp timestamp コマンド [823](#)  
tcp window-size コマンド [825](#)  
telnet client source-interface コマンド [373](#)  
telnet dscp コマンド [375](#)  
telnet server コマンド [377](#)  
telnet transparent コマンド [379](#)  
telnet コマンド [369](#)  
tftp client source-interface コマンド [381](#)  
tftp server コマンド [383](#)  
timers (DAGR) コマンド [135](#)  
timers (hsrp) コマンド [463](#)  
traceroute コマンド [385](#)

track (hsrp) コマンド [466](#)  
trusted コマンド [319](#)  
trust relay-reply コマンド [317](#)

## V

vrf (address-family) コマンド [678](#)  
vrf (description) コマンド [680](#)  
vrf (mhost) コマンド [682](#)  
vrf (relay profile) コマンド [321](#)  
vrf mode コマンド [684](#)  
vrf コマンド [676](#)  
vrrp assume-ownership disable コマンド [868](#)  
vrrp bfd fast-detect コマンド [870](#)  
vrrp bfd minimum-interval コマンド [841, 872](#)  
vrrp bfd multiplier コマンド [843, 874](#)  
vrrp delay コマンド [876](#)  
vrrp ipv4 コマンド [878](#)  
vrrp preempt コマンド [880](#)  
vrrp priority コマンド [882](#)  
vrrp text-authentication コマンド [884](#)  
vrrp timer コマンド [886](#)  
vrrp track interface コマンド [888](#)  
vrrp コマンド [866](#)

