show auto discovery qos から show ip rsvp hello client lsp detail

show auto discovery qos

エンタープライズ機能用 AutoQoS の自動検出（データ収集）フェーズ中に収集したデータを表示するには、特権 EXEC モードで **showautodiscoveryqos** コマンドを使用します。

show auto discovery qos [**interface** [*type number*]]

構文の説明

interface	（任意）特定のインターフェイス タイプの設定が表示されることを示します。
type number	（オプション）インターフェイスのタイプおよび番号を指定します。

コマンド デフォルト

すべてのインターフェイス タイプ用に作成された設定を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.3(7)T	このコマンドが導入されました。
12.3(11)T	コマンド出力が変更され、推奨ポリシーマップ情報が追加されました。

使用上のガイドライン

推奨ポリシー出力（次の例に表示）を使用すると、**autoqos** コマンドをインターフェイスに実行する前にクラス マップとポリシー マップをプレビューできます。これにより、データを追加で収集するか、既存のデータをカット アンド ペーストして必要に応じて編集するまで、自動検出フェーズを継続できます。

例

次は、**showautodiscoveryqos** コマンドの出力例です。この例では、信頼モードで DSCP 分類を使用した自動検出（データ収集）フェーズ中に収集したデータを表示します。推奨ポリシー マップ情報も含まれます。

```
Router# show auto discovery qos
Serial2/1.1
 AutoQoS Discovery enabled for trusted DSCP
 Discovery up time: 2 hours, 42 minutes
 AutoQoS Class information:
 Class Voice:
  Recommended Minimum Bandwidth: 118 Kbps/1% (PeakRate)
  Detected DSCPs and data:
  DSCP value         AverageRate        PeakRate           Total
                     (kbps/%)           (kbps/%)           (bytes)
  -----------        -----------        --------           -------------
  46/ef              106/1              118/1              129510064
 Class Interactive Video:
  Recommended Minimum Bandwidth: 25 Kbps/<1% (AverageRate)
  Detected DSCPs and data:
  DSCP value         AverageRate        PeakRate           Total
```

```
                    (kbps/%)            (kbps/%)            (bytes)
  ------------      ------------        --------            ------------
   34/af41          25/<1               28/<1               31084292
  Class Signaling:
   Recommended Minimum Bandwidth: 50 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   24/cs3           50/<1               56/<1               61838040
  Class Streaming Video:
   Recommended Minimum Bandwidth: 79 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   32/cs4           79/<1               88/<1               96451788
  Class Transactional:
   Recommended Minimum Bandwidth: 105 Kbps/1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   18/af21          105/1               117/1               127798678
  Class Bulk:
   Recommended Minimum Bandwidth: 132 Kbps/1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   10/af11          132/1               147/1               160953984
  Class Scavenger:
   Recommended Minimum Bandwidth: 24 Kbps (AverageRate)/0% (fixed)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   8/cs1            24/<1               27/<1               30141238
  Class Management:
   Recommended Minimum Bandwidth: 34 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   16/cs2           34/<1               38/<1               41419740
  Class Routing:
   Recommended Minimum Bandwidth: 7 Kbps/<1% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   48/cs6           7/<1                7/<1                8634024
  Class Best Effort:
   Current Bandwidth Estimation: 820 Kbps/8% (AverageRate)
   Detected DSCPs and data:
   DSCP value       AverageRate         PeakRate            Total
                    (kbps/%)            (kbps/%)            (bytes)
   ------------     ------------        --------            ------------
   0/default        820/8               915/9               997576380
 Suggested AutoQoS Policy based on a discovery uptime of 2 hours, 42 minutes:
  !
  class-map match-any AutoQoS-Voice-Trust
   match ip dscp ef
  !
```

```
class-map match-any AutoQoS-Inter-Video-Trust
 match ip dscp af41
!
class-map match-any AutoQoS-Signaling-Trust
 match ip dscp cs3
!
class-map match-any AutoQoS-Stream-Video-Trust
 match ip dscp cs4
!
class-map match-any AutoQoS-Transactional-Trust
 match ip dscp af21
 match ip dscp af22
 match ip dscp af23
!
class-map match-any AutoQoS-Bulk-Trust
 match ip dscp af11
 match ip dscp af12
 match ip dscp af13
!
class-map match-any AutoQoS-Scavenger-Trust
 match ip dscp cs1
!
class-map match-any AutoQoS-Management-Trust
 match ip dscp cs2
!
class-map match-any AutoQoS-Routing-Trust
 match ip dscp cs6
!
policy-map AutoQoS-Policy-S2/1.1Trust
 class AutoQoS-Voice-Trust
  priority percent 1
 class AutoQoS-Inter-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Signaling-Trust
  bandwidth remaining percent 1
 class AutoQoS-Stream-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Transactional-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Bulk-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Scavenger-Trust
  bandwidth remaining percent 1
 class AutoQoS-Management-Trust
  bandwidth remaining percent 1
 class AutoQoS-Routing-Trust
  bandwidth remaining percent 1
 class class-default
  fair-queue
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *1 : show auto discovery qos* フィールドの説明

フィールド	説明
Serial2/1.1	データが収集されるインターフェイスまたはサブインターフェイス。

フィールド	説明
AutoQoS Discovery enabled for trusted DSCP	AutoQoSのデータ収集フェーズが有効であることを示します。
Discovery up time	データが収集された期間を示します。
AutoQoS Class information	各 AutoQoS クラスの情報を表示します。
Class Voice	指定されたクラスの情報。検出されたアプリケーションに関連するデータも含まれます。このデータには、DSCP値、平均レート（キロビット/秒（kbps））、ピーク レート（kbps）、および合計パケット（バイト）が含まれます。
Suggested AutoQoS Policy based on a discovery uptime of hours and minutes	指定された検出時間に基づいた、ポリシーマップとクラスマップの統計情報。

関連コマンド

コマンド	説明
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
autodiscoveryqos	エンタープライズ機能用 AutoQoS 設定に使用するデータの検出と収集を開始します。
showautoqos	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でAutoQoSによって作成されたインターフェイス コンフィギュレーション、ポリシーマップ、およびクラス マップを表示します。

show auto qos

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の AutoQoS で作成されるインターフェイス設定、ポリシー マップ、およびクラス マップを表示するには、特権 EXEC モードで **showautoqos** コマンドを使用します。

show auto qos [**interface** [*type slot/ port*]]

構文の説明

interface	（任意）AutoQoS--VoIP 機能が有効になっているすべてのインターフェイスまたは PVC の AutoQoS--VoIP 機能で作成された設定を表示します。 • **interface** キーワードを設定していても、インターフェイス タイプを指定していない場合、**showautoqosinterface** コマンドは AutoQoS--VoIP 機能が有効になっているすべてのインターフェイスまたは PVC の AutoQoS--VoIP 機能で作成された設定を表示します。
type	（任意）インターフェイス タイプ：有効な値は、**atm**、**ethernet**、**fastethernet**、**ge-wan**、**gigabitethernet**、**pos**、および **tengigabitethernet** です。
slot / port	（任意）スロットおよびポート番号。

コマンド デフォルト

引数またはキーワードを指定しない場合、すべてのインターフェイス タイプに作成された設定が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが、AutoQoS--VoIP 機能の一部として導入されました。
12.3(7)T	このコマンドが変更され、エンタープライズ機能の AutoQoS に対応しました。出力が変更され、エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータに基づいて作成されたクラス、クラス マップ、およびポリシー マップを表示するようになりました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.2(1)T	このコマンドが変更されました。出力に、フレーム リレー トラフィック シェーピング設定は表示されません。

使用上のガイドライン

showautoqosinterface コマンドは、フレーム リレー データリンク接続識別子（DLCI）と ATM PVC で使用できます。

AutoQoS--VoIP またはエンタープライズ機能用 AutoQos が有効になっていると、各インターフェイスまたはPVCに対応した設定が生成されます。これらの設定を使用して、インターフェイス設定、ポリシー マップ、クラス マップ、およびアクセス コントロール リスト（ACL）を作成し、ネットワークで使用します。**showautoqos** コマンドを使用して、インターフェイス設定、ポリシー マップ、クラス マップ、および ACL の内容を検証できます。

Catalyst 6500 シリーズ スイッチ

AutoQoS は次のモジュールでサポートされています。

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE-TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

例

show auto qos interface コマンド：AutoQoS--VoIP 機能に対応した設定

showautoqosinterface*typeslot/port* コマンドは、特定のインターフェイスの AutoQoS--VoIP 機能で作成された設定を表示します。

次の例では、シリアル サブインターフェイス 6/1.1 が指定されています。

```
Router# show auto qos interface serial 6/1.1
S6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

interface キーワードを設定していても、インターフェイス タイプを指定していない場合、**showautoqosinterface** コマンドはAutoQoS--VoIP機能が有効になっているすべてのインターフェイスまたはPVC の AutoQoS--VoIP 機能で作成された設定を表示します。

```
Router# show auto qos interface
```

```
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
ATM2/0.1: PVC 1/100 -
!
interface ATM2/0.1 point-to-point
 pvc 1/100
  tx-ring-limit 3
  encapsulation aal5mux ppp Virtual-Template200
!
interface Virtual-Template200
 bandwidth 512
 ip address 10.10.107.1 255.255.255.0
 service-policy output AutoQoS-Policy-UnTrust
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
```

次の例は、AutoQoS--VoIP 機能で作成されたすべての設定を表示します。

```
Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *2 : show auto qos* フィールドの説明（*AutoQoS--VoIP* 機能の設定）

フィールド	説明
class AutoQoS-VoIP-FR-Serial6/1-100	AutoQoS-VoIP 機能で作成されたクラスの名前。この例では、クラスの名前は AutoQoS-VoIP-FR-Serial6/1-100 です。
service-policy output AutoQoS-Policy-UnTrust	ポリシー マップ「AutoQoS-Policy-UnTrust」が、インターフェイスの発信方向のインターフェイスに適用されていることを示します。

show auto qos interface コマンド：エンタープライズ機能用 AutoQoS に対応した設定

次は、**showautoqos** コマンドの出力例です。この例では、エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータに基づいて作成されたクラス、クラス マップ、およびポリシー マップを表示します。

```
Router# show auto qos
 !
  policy-map AutoQoS-Policy-Se2/1.1
   class AutoQoS-Voice-Se2/1.1
    priority percent 70
    set dscp ef
   class AutoQoS-Inter-Video-Se2/1.1
    bandwidth remaining percent 10
    set dscp af41
   class AutoQoS-Stream-Video-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs4
   class AutoQoS-Transactional-Se2/1.1
    bandwidth remaining percent 1
    set dscp af21
   class AutoQoS-Scavenger-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs1
   class class-default
    fair-queue
 !
policy-map AutoQoS-Policy-Se2/1.1-Parent
   class class-default
    shape average 1024000
    service-policy AutoQoS-Policy-Se2/1.1
 !
 class-map match-any AutoQoS-Stream-Video-Se2/1.1
  match protocol cuseeme
 !
 class-map match-any AutoQoS-Transactional-Se2/1.1
  match protocol sqlnet
 !
class-map match-any AutoQoS-Voice-Se2/1.1
  match protocol rtp audio
 !
 class-map match-any AutoQoS-Inter-Video-Se2/1.1
  match protocol rtp video
 !
 rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner
 AutoQoS
Serial2/1.1: DLCI 58 -
 !
 interface Serial2/1.1 point-to-point
  frame-relay interface-dlci 58
   class AutoQoS-FR-Serial2/1-58
 !
 map-class frame-relay AutoQoS-FR-Serial2/1-58
  frame-relay cir 1024000
frame-relay bc 10240
  frame-relay be 0
  frame-relay mincir 1024000
  service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *3 : show auto qos* フィールドの説明（エンタープライズ機能用 *AutoQoS* の設定）

フィールド	説明
policy-map AutoQoS-Policy-Se2/1.1	AutoQoS 機能で作成されたポリシー マップの名前。この例では、ポリシー マップの名前は AutoQoS-Policy-Se2/1.1 です。
class AutoQoS-Voice-Se2/1.1 priority percent 70 set dscp ef	AutoQoS機能で作成されたクラスの名前。この例では、クラスの名前は AutoQoS-Voice-Se2/1.1 です。クラス名に続いて、クラスに設定された固有の QoS 機能が表示されます。
class-map match-any AutoQoS-Stream-Video-Se2/1.1 match protocol cuseeme	クラス マップの名前と指定されたパケット一致基準。

関連コマンド

コマンド	説明
autodiscoveryqos	エンタープライズ機能用 AutoQoS 設定に使用するデータの検出と収集を開始します。
autoqos	エンタープライズ機能の AutoQoS によって作成された QoS クラス マップおよびポリシー マップをインストールします。
autoqosvoip	インターフェイスに AutoQoS--VoIP 機能を設定します。
showautodiscoveryqos	エンタープライズ機能用 AutoQoS の自動検出フェーズ中に収集されたデータを表示します。

show class-map

クラス マップとその一致基準を表示するには、特権 EXEC モードで **showclass-map** コマンドを使用します。

Cisco 3660、3845、6500、7400、および 7500 シリーズ ルータ
show class-map [**type** {**stack**|**access-control**}] [*class-map-name*]

Cisco 7600 および ASR 1000 シリーズ ルータ
show class-map [*class-map-name*]

構文の説明

typestack	（任意）Flexible Packet Matching（FPM）で検査して正しいプロトコル スタックを決定するように設定されたクラス マップを表示します。
typeaccess-control	（任意）対象のプロトコル スタック内を検索するために正確なパターンを決定するように設定されたクラス マップを表示します。
class-map-name	（任意）クラス マップ名クラス マップ名には、最大 40 の英数字を使用できます。

コマンド デフォルト

すべてのクラス マップが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.2(13)T	このコマンドが変更され、クラス マップ内のトラフィックの一致基準として、フレーム リレー データ リンク接続識別子（DLCI）番号またはレイヤ 3 パケットの長さを表示するようになりました。
12.2(14)SX	このコマンドが Cisco 7600 シリーズ ルータに実装されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(4)T	**type**、**stack** および **access-control** キーワードが追加され、FPM がサポートされるようになりました。
Cisco IOS XE Release 2.2	このコマンドが Cisco ASR アグリゲーション サービス 1000 シリーズ ルータに実装されました。

リリース	変更箇所
15.0(1)M	このコマンドが変更されました。出力が変更され、暗号化フィルタ情報が表示されるようになりました。

使用上のガイドライン

すべてのクラス マップとその一致基準を表示するには、**showclass-map** コマンドを使用します。オプションの *class-map-name* 引数を入力すると、指定したクラス マップとその一致基準が表示されます。

例

次の例では、3 つのクラス マップが定義されます。アクセス リスト 103 に一致するパケットはクラス c3、IP パケットはクラス c2、イーサネット インターフェイス 1/0 経由で着信するパケットはクラス c1 に属します。**showclass-map** コマンドの出力には、3 つの定義されたクラス マップが表示されます。

```
Router# show class-map
 Class Map c3
 Match access-group 103
 Class Map c2
 Match protocol ip
 Class Map c1
 Match input-interface Ethernet1/0
```

次の例では、c1 クラス マップが定義され、一致基準としてフレーム リレー DLCI 番号が 500 に指定されます。

```
Router# show class-map
class map match-all c1
   match fr-dlci 500
```

次に、すべてのクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map
 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any class-simple (id 2)
   Match any
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
 Class Map match-all agg-2 (id 3)
```

次に、特定のクラス マップに関するクラス マップ情報を表示する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

次は、**showclass-maptypeaccess-control** コマンドを使用した、暗号化 FPM フィルタの出力例です。

```
Router# show class-map type access-control accesscontrol1
 Class Map type access-control match-all accesscontrol1 (id 4)
   Match encrypted FPM filter
            filter-hash   : FC50BED10521002B8A170F29AF059C53
```

```
          filter-version: 0.0_DummyVersion_20090101_1830
          filter-id     : cisco-sa-20090101-dummy_ddts_001
  Match start TCP payload-start offset 0 size 10 regex "abc.*def"
  Match field TCP source-port eq 1234
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *4: show class-map* フィールドの説明（カッコで囲んだ番号がクラス マップ名と一致基準情報の横に表示される場合があります）この番号は、*Cisco* 内部だけで使用されるものであり、無視できます。

フィールド	説明
Class Map	表示されるトラフィックのクラス。ポリシーに設定されているクラスマップごとに出力が表示されます。クラス一致の実装の選択（match-all、match-any など）もトラフィック クラスの横に表示されます。
Match	クラス マップに指定された一致基準。フレーム リレー DLCI 番号、レイヤ 3 パケット長、IP プレシデンス、IP Diffserv コードポイント（DSCP）値、マルチプロトコル ラベル スイッチング（MPLS）EXP 値、アクセス グループ、およびサービス品質（QoS）グループなどの基準があります。

関連コマンド

Command	Description
class-map	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
matchfr-dlci	クラス マップの一致基準としてフレームリレー DLCI 番号を指定します。
matchpacketlength(class-map)	IP ヘッダーのレイヤ 3 パケットの長さをクラスマップの一致基準として指定して、使用します。
showpolicy-map	指定されたサービス ポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
showpolicy-mapinterface	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

show class-map type nat

ネットワークアドレス変換（NAT）クラスマップとその一致基準を表示するには、特権EXECモードで **showclass-maptypenat** コマンドを使用します。

show class-map type nat [*class-map-name*]

構文の説明

class-map-name	（任意）NAT クラス マップの名前。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

すべての NAT クラス マップの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(11)T	このコマンドが導入されました。

使用上のガイドライン

showclass-maptypenat コマンドは、すべての NAT クラス マップとその一致基準を表示します。特定の NAT クラス マップとその一致基準を表示するには、クラス マップ名を指定します。

例

次は、**showclass-maptypenat** コマンドの出力例で、すべてのクラス マップを表示します。

```
Router# show class-map type nat
Class Map match-all ipnat-class-acl-we (id 5)
   Match access-group  0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 5 : show class-map type nat フィールドの説明

フィールド	説明
Class Map	クラスマップの名前と着信パケットに一致するクラスマップに適用する条件を表示します。
Match	クラス マップに指定された一致基準。

関連コマンド

コマンド	説明
showclass-maptypeinspect	レイヤ3とレイヤ4またはレイヤ7（用途別）検査タイプ クラスマップおよびその一致基準を表示します。
showclass-maptypeport-filter	ポートフィルタ クラスマップおよびその一致基準を表示します。

show class-map type port-filter

ポート フィルタのクラス マップとその一致基準を表示するには、特権 EXEC モードで **showclass-maptypeport-filter** コマンドを使用します。

show class-map type port-filter [*class-map-name*]

構文の説明

class-map-name	（任意）ポートフィルタ クラス マップの名前。名前には最大 40 文字までの英数字を指定できます。

コマンド デフォルト

引数を指定しないと、すべてのポートフィルタ クラス マップの情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(11)T	このコマンドが導入されました。

使用上のガイドライン

コントロール プレーン パケットの TCP/UDP ポート ポリシングを表示するには、**showclass-maptypeport-filter** コマンドを使用します。**showclass-maptypeport-filter** コマンドは、すべてのポートフィルタ クラス マップとその一致基準を表示します。特定のポートフィルタ クラス マップのクラス マップを表示するには、クラス マップ名を指定します。

例

次は、**showclass-maptypeport-filter** コマンドの出力例で、すべてのクラス マップを表示します。

```
Router# show class-map type port-filter
Class Map type port-filter match-all pf-policy (id 9)
   Match  port tcp 45 56
 Class Map type port-filter match-any cl1 (id 4)
   Match none
 Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

次は、**showclass-maptypeport-filter** コマンドの出力例で、クラス マップ pf-class を表示します。

```
Router# show class-map type port-filter pf-class
Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *6 : show class-map type port-filter* フィールドの説明

フィールド	説明
Class Map	表示されているポートフィルタ クラス マップ。出力は、設定されているクラス マップごとに表示されます。クラス一致の実装の選択（match-all、match-any など）はトラフィック クラスの横に表示されます。
Match	クラス マップに指定された一致基準。有効な一致基準は、**closed-ports**、**not**、および **port** です。

関連コマンド

コマンド	説明
class-map	指定したクラスへのパケットのマッチングに使用するクラスマップを作成します。

show control-plane cef-exception counters

コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planecef-exceptioncounters** コマンドを使用します。

show control-plane cef-exception counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planecef-exceptioncounters コマンドは、コントロール プレーン CEF 例外サブインターフェイスに設定された機能の次のパケット数を表示します。

- CEF 例外サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planecef-exceptioncounters** コマンドの出力例です。

```
Router# show control-plane cef-exception counters
 Control plane cef-exception path counters:
 Feature      Packets Processed/Dropped/Errors
 Control Plane Policing       63456/9273/0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *7 : show control-plane cef-exception counters* フィールドの説明

フィールド	説明
Feature	このサブインターフェイスに設定されている機能の名前。
Packets Processed	その機能で処理されたパケットの合計数。
Dropped	その機能でドロップされたパケットの合計数。
Errors	その機能で検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
show control-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
show control-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
show control-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehost open-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-plane transitcounters	コントロール プレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show control-plane cef-exception features

コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planecef-exceptionfeatures** コマンドを使用します。

show control-plane cef-exception features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planecef-exceptionfeatures コマンドは、コントロール プレーン CEF 例外サブインターフェイスの次の集約機能設定を表示します。

- コントロール プレーン CEF 例外サブインターフェイスに設定された機能の数。
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planecef-exceptionfeatures** コマンドの出力例です。

```
Router# show control-plane cef-exception features
 Total 1 features configure
  Control plane cef-exception path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *8 : show control-plane cef-exception features* フィールドの説明

フィールド	説明
Total features configured	設定された機能の数。
Feature Name	設定された機能の名前。
Activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-planecef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planefeatures	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show control-plane counters

すべてのコントロール プレーン インターフェイスのコントロール プレーン カウンタを表示するには、特権 EXEC モードで **showcontrol-planecounters** コマンドを使用します。

show control-plane counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planecounters コマンドは、すべてのコントロール プレーン インターフェイスおよびサブインターフェイスの次の集約パケット数を表示します。

- コントロール プレーン集約ホスト、トランジット、および CEF 例外サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次に、**showcontrol-planecounters** コマンドの出力例を示します。

```
Router# show control-plane counters
 Feature Path     Packets Processed/Dropped/Errors
  aggregate      43271/6759/0
  host      24536/4238/0
  transit      11972/2476/0
     cef-exception path       6345/0/0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *9 : show control-plane counters* フィールドの説明

フィールド	説明
Feature	表示されたインターフェイスまたはサブインターフェイスの名前。
Packets Processed	そのサブインターフェイスで処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数

フィールド	説明
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーン インターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
show control-planecef-exception features	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
show control-planehostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
show control-plane transitcounters	コントロール プレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane transitfeatures	コントロール プレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane features

設定されたコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planefeatures** コマンドを使用します。

show control-plane features

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planefeatures コマンドは、コントロール プレーン集約サブインターフェイスで有効になっているコントロール プレーン機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次に、**showcontrol-planefeatures** コマンドの出力例を示します。

```
Router# show control-plane features
 Total 1 features configured
  Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *10 : show control-plane features* フィールドの説明

フィールド	説明
Total features configured	設定された機能の数。
Feature Name	設定された機能の名前。
activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane host counters

コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planehostcounters** コマンドを使用します。

show control-plane host counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planehostcounters コマンドは、コントロール プレーン ホスト サブインターフェイスの次のパケット数を表示します。

- そのホスト サブインターフェイスに設定されている機能で処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planehostcounters** コマンドの出力例です。

```
Router# show control-plane host counters
 Control plane host path counters:
 Feature      Packets Processed/Dropped/Errors
 TCP/UDP portfilter       46/46/0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *11 : show control-plane host counters* フィールドの説明

フィールド	説明
Feature	ホストサブインターフェイスに設定された機能の名前。
Packets Processed	その機能で処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	ユーザが、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更が許可されるコントロールプレーン コンフィギュレーション モードを開始します。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planehostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロール プレーン トランジット サブインターフェイスに設定されている機能を表示します。

show control-plane host features

コントロール プレーン ホスト サブインターフェイスに設定されているコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planehostfeatures** コマンドを使用します。

show control-plane host features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planehostfeatures コマンドは、コントロール プレーン ホスト サブインターフェイスに設定されている機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planehostfeatures** コマンドの出力例です。

```
Router# show control-plane host features
   Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *12 : show control-plane host features* フィールドの説明

フィールド	説明
Feature Name	設定された機能の名前。
activated	機能が有効化された日時。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外のサブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane host open-ports

ポート フィルタ データベースに登録されたオープンな TCP/UDP ポートのリストを表示するには、特権 EXEC モードで **showcontrol-planehostopen-ports** コマンドを使用します。

show control-plane host open-ports

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planehostopen-ports コマンドは、ポート フィルタ データベースに登録されたオープンな TCP/UDP ポートのリストを表示します。

例

次に、**showcontrol-planehostopen-ports** コマンドの出力例を示します。

```
Router# show control-plane host open-ports

Active internet connections (servers and established)
Port        Local Address      Foreign Address                  Service    State
 tcp                *:23                *:0                    Telnet   LISTEN
 tcp                *:53                *:0                DNS Server   LISTEN
 tcp                *:80                *:0                 HTTP CORE   LISTEN
 tcp              *:1720                *:0                      H.225   LISTEN
 tcp              *:5060                *:0                       SIP   LISTEN
 tcp                *:23      192.0.2.18:58714              Telnet   ESTABLISHED
 udp                *:53                *:0                DNS Server   LISTEN
 udp                *:67                *:0             DHCPD Receive   LISTEN
 udp             *:52824                *:0                   IP SNMP   LISTEN
 udp               *:161                *:0                   IP SNMP   LISTEN
 udp               *:162                *:0                   IP SNMP   LISTEN
 udp              *:5060                *:0                       SIP   LISTEN
 udp              *:2517                *:0                 CCH323_CT   LISTEN
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *13 : show control-plane host open-ports* フィールドの説明

フィールド	説明
Port	ポート タイプ（TCP または UDP）。

フィールド	説明
Local Address	ローカルIPアドレスとポート番号。アスタリスク（*）は、サービスがすべての設定済みネットワーク インターフェイスでリッスンしていることを示します。
Foreign Address	リモートIPアドレスとポート番号。アスタリスク（*）は、サービスがすべての設定済みネットワーク インターフェイスでリッスンしていることを示します。
Service	ポートに設定された Cisco IOS サービス リスニングの名前。
State	Listen または Established。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-planetransitcounters	コントロール プレーン トランジット サブインターフェイスのコントロール プレーン パケット カウンタを表示します。

コマンド	Description
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane transit counters

コントロールプレーン トランジット サブインターフェイスのコントロールプレーン パケット カウンタを表示するには、特権 EXEC モードで **showcontrol-planetransitcounters** コマンドを使用します。

show control-plane transit counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planetransitcounters コマンドは、コントロール プレーン トランジット サブインターフェイスの次のパケット数を表示します。

- そのトランジット サブインターフェイスで処理されたパケットの合計数
- ドロップされたパケットの合計数
- エラーの合計数

例

次は、**showcontrol-planetransitcounters** コマンドの出力例です。

```
Router# show control-plane transit counters
 Control plane transit path counters:
 Feature      Packets Processed/Dropped/Errors
     Control Plane Policing       63456/2391/0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *14 : show control-plane transit counters* フィールドの説明

フィールド	説明
Feature	トランジットサブインターフェイスに設定された機能の名前。
Packets Processed	設定された機能で処理されたパケットの合計数。
Dropped	ドロップされたパケットの合計数
Errors	検出されたエラーの合計数。

関連コマンド

コマンド	Description
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外のサブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポートフィルタ データベースに登録されている、開いている TCP/UDP ポートのリストを表示します。
showcontrol-planetransitfeatures	コントロールプレーン中継サブインターフェイスに対して設定された機能を表示します。

show control-plane transit features

コントロール プレーン トランジット サブインターフェイスに設定されているコントロール プレーン機能を表示するには、特権 EXEC モードで **showcontrol-planetransitfeatures** コマンドを使用します。

show control-plane transit features

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.4(4)T	このコマンドが導入されました。

使用上のガイドライン

showcontrol-planetransitfeatures コマンドは、コントロール プレーン トランジット サブインターフェイスに設定されているコントロールプレーン機能を表示します。次の事項が表示されます。

- コントロール プレーンに設定された機能の数
- 機能の名前
- 機能が有効化された日時

例

次は、**showcontrol-planetransitfeatures** コマンドの出力例です。

```
Router# show control-plane transit features
  Control plane transit path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *15 : show control-plane transit features* フィールドの説明

フィールド	説明
Total Features Configured	設定された機能の数。
Feature Namef	設定された機能の名前。
Activated	機能が有効化された日時。

関連コマンド

コマンド	説明
clearcontrol-plane	コントロールプレーンインターフェイスおよびサブインターフェイスのパケット カウンタをクリアします。
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。このモードでは、デバイスのコントロールプレーンに関連付けられた属性またはパラメータの関連付けおよび変更ができます。
debugcontrol-plane	コントロール プレーン ルーチンからのデバッグ出力を表示します。
showcontrol-plane cef-exceptioncounters	コントロール プレーン CEF 例外サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-plane cef-exceptionfeatures	コントロール プレーン CEF 例外のサブインターフェイスに対して設定された機能を表示します。
showcontrol-plane counters	集約コントロール プレーン インターフェイスに対するコントロール プレーン パケット カウンタを表示します。
showcontrol-plane features	集約コントロール プレーン インターフェイスに対して設定された機能を表示します。
showcontrol-plane hostcounters	コントロール プレーン ホスト サブインターフェイスのコントロール プレーン パケット カウンタを表示します。
showcontrol-planehostfeatures	コントロール プレーン ホスト サブインターフェイスに対して設定された機能を表示します。
showcontrol-plane hostopen-ports	ポート フィルタ データベースに登録されたオープンなポートのリストを表示します。
showcontrol-planetransitcounters	コントロールプレーン中継サブインターフェイスに対するコントロール プレーン パケット カウンタを表示します。

show cops servers

ルータが設定されているポリシー サーバの IP アドレスと接続ステータスを表示するには、EXEC モードで **showcopsservers** コマンドを使用します。

show cops servers

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.1(1)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

show cops server コマンドを使用して、ルータの Common Open Policy Service（COPS）クライアントに関する情報を表示することもできます。

例

次の例では、現在のポリシーサーバとクライアントの情報が表示されます。Client Type の後に整数が表示される場合、1 はリソース予約プロトコル（RSVP）を意味し、2 は差別化サービス プロビジョニングを意味します。（0 はキープアライブを示します。）

```
Router# show cops servers
COPS SERVER: Address: 10.0.0.1. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
 COPS CLIENT: Client type: 1.  State: 0.
```

関連コマンド

Command	Description
showiprsvppolicycops	ポリシー サーバ アドレス、ACL ID、およびルータ サーバ接続の現在の状態を表示します。

show crypto eng qos

IPSec 暗号化エンジンの低遅延キューイング（LLQ）をモニタし、管理するには、特権 EXEC モードで show crypto eng qos コマンドを使用します。

show crypto eng qos

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T で導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS リリース 12(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

IPSec 暗号化エンジンの LLQ で QoS が有効になっているかどうかを確認するには、**show crypto eng qos** コマンドを使用します。

例

次の例では、IPSec 暗号化エンジンの LLQ が有効になっているかどうかを確認します。

```
Router# show crypto eng qos
crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                   llq size: 0
    default queue size/max: 0/64
      interface table size: 32
  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
    class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0
  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

この表示にはフィールドの説明がされています。

show crypto entropy status

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの暗号エントロピーの状態を表示するには、EXEC モードで **show crypto entropy status** コマンドを使用します。

show crypto entropy status

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC(#)

コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.7.3S	このコマンドが、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。
Cisco IOS XE Release 3.8S	コマンド出力が Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで変更されました。

例

次は、暗号エントロピーが有効になっている場合の **show crypto entropy status** コマンドの出力例です。

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128(*)
2 getrandombytes        SW  Working  160(*)
3 Nitrox / Octeon       HW  Working  256
(*) - The entropy collected from SW sources were not counted as a part of
      achieving the entropy target!
```

表 16 : 表 1 show crypto entropy status フィールドの説明に、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 : 表 1 show crypto entropy status フィールドの説明

フィールド	説明
Entropy source	暗号エントロピーのソース。

フィールド	説明
Type	暗号エントロピーのタイプ。次のいずれかの値を指定できます。 • ソフトウェアがソースの SW エントロピー。 ハードウェアがソースの HW エントロピー。
Status	暗号エントロピーの状態。次のいずれかの値を指定できます。 • Working エントロピーは動作中。 Offline エントロピーはオフライン。
Entropy Bits	暗号エントロピーのサイズ（ビット）

次は、暗号エントロピーが無効になっている場合の **show crypto entropy status** コマンドの出力例です。

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128
2 getrandombytes        SW  Working  160
3 Nitrox / Octeon       HW  Offline   --
```

（注） この表示内のフィールドは、表 16 : 表 1 show crypto entropy status フィールドの説明 で説明されています。

関連コマンド

コマンド	説明
platform ipsec fips-mode	

show frame-relay ip rtp header-compression

フレーム リレー Real-time Transport Protocol（RTP）ヘッダー圧縮統計情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showframe-relayiprtpheader-compression** コマンドを使用します。

show frame-relay ip rtp header-compression [**interface** *type number*] [*dlci*]

構文の説明

interface *type number*	（任意）情報を表示するインターフェイスを指定します。インターフェイスのタイプと番号の間のスペースは任意です。
dlci	（任意）情報を表示するデータ リンク接続識別子（DLCI）を指定します。範囲は 16 ～ 1022 です。

コマンド デフォルト

RTP ヘッダー圧縮が設定されたインターフェイスのすべての DLCI の RTP ヘッダー圧縮統計情報が表示されます。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
11.3	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。このコマンドの出力は変更され、フレーム リレー相手先固定接続（PVC）バンドルの RTP ヘッダー圧縮統計情報を表示するようになりました。
12.2(27)SBC	このコマンドが Cisco IOS Release 12.2(27)SBC に統合され、*dlci* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(9)T	*dlci* 引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(11)T	このコマンドの出力が変更され、フレームリレー相手先固定接続（PVC）バンドルの拡張圧縮 Real-Time Transport Protocol（ECRTP）ヘッダー圧縮統計情報を表示するようになりました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

例

次は、**showframe-relayiprtpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip rtp header-compression
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次は、ECRTP が有効になっている場合の **showframe-relayiprtpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip rtp header-compression
 DLCI 16         Link/Destination info: ip 10.0.0.1
  Interface Serial4/1 DLCI 16 (compression on, IETF, ECRTP)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 16 rx slots, 16 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 16 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで DLCI 21 に関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression 21
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
```

```
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで、シリアルインターフェイス 3/1 のすべての DLCI に関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface serial3/1
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の例では、**showframe-relayiprtpheader-compression** コマンドで、シリアルインターフェイス 3/1 の DLCI 21 のみに関する情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface serial3/1 21
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の出力例では、**showframe-relayiprtpheader-compression** コマンドで、MP-3-static という名前の PVC バンドルに関する統計情報を表示します。

```
Router# show frame-relay ip rtp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
```

```
          474 bytes saved, 119 bytes sent
          4.98 efficiency improvement factor
  Connect:256 rx slots, 256 tx slots,
          1 long searches, 1 misses 0 collisions, 0 negative cache hits
          93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

下の表で、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 frame-relay ip rtp header-compression* フィールドの説明

フィールド	説明
Interface	インターフェイスのタイプと番号、およびヘッダー圧縮のタイプ。
Rcvd:	受信パケットの詳細情報の表。
total	インターフェイスの受信パケット数。
compressed	圧縮されたヘッダーを持つパケット数
errors	エラー数。
dropped	ドロップされたパケット数
buffer copies	コピーされたバッファの数。
buffer failures	バッファの割り当てに失敗した回数。
Sent:	送信パケットの詳細情報の表。
total	送信されたパケットの合計数。
compressed	圧縮されたヘッダーを持つ送信パケット数
bytes saved	圧縮によって節約できた合計バイト数。
bytes sent	圧縮後に送信された合計バイト数
efficiency improvement factor	圧縮効率。
Connect:	接続の詳細情報の表。
rx slots	受信されたスロットの合計数。
tx slots	送信されたスロットの合計数。
long searches	複数のルックアップが必要だった検索。
misses	作成された新規ステート数。
hit ratio	既存のステートが修正された回数。

フィールド	説明
five minute miss rate	平均ミス レート。
max	最大ミス レート。

関連コマンド

Command	Description
frame-relayiprtpcompression-connections	フレーム リレー インターフェイスの RTP ヘッダー圧縮接続の最大数を指定します。
frame-relayiprtpheader-compression	物理インターフェイス上のすべてのフレームリレーマップについて RTP ヘッダー圧縮をイネーブルにします。
frame-relaymapipcompress	RTP と TCP の両方のヘッダー圧縮をリンクで有効にします。
frame-relaymapipnocompress	RTP と TCP の両方のヘッダー圧縮をリンクで無効にします。
frame-relaymapiprtpheader-compression	DLCI ごとに RTP ヘッダー圧縮を有効にします。
showiprpfevents	RTP ヘッダー圧縮の統計情報を表示します。

show frame-relay ip tcp header-compression

フレーム リレー Transmission Control Protocol（TCP）/IP ヘッダー圧縮統計情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showframe-relayiptcpheader-compression** コマンドを使用します。

show frame-relay ip tcp header-compression [**interface** *type number*] [*dlci*]

構文の説明

interface *type number*	（任意）情報を表示するインターフェイスを指定します。type と number の間のスペースは任意です。
dlci	（任意）情報を表示するデータ リンク接続識別子（DLCI）を指定します。範囲は 16 ～ 1022 です。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
10.3	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。このコマンドは変更され、フレーム リレー相手先固定接続（PVC）バンドルの RTP ヘッダー圧縮統計情報を表示するようになりました。
12.2(27)SBC	このコマンドが Cisco IOS Release 12.2(27)SBC に統合され、*dlci* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.4(9)T	*dlci* 引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

例

次は、**showframe-relayiptcpheader-compression** コマンドの出力例です。

```
Router# show frame-relay ip tcp header-compression
DLCI 200          Link/Destination info: ip 10.108.177.200
Interface Serial0:
Rcvd:     40 total, 36 compressed, 0 errors
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     0 total, 0 compressed
```

```
          0 bytes saved, 0 bytes sent
Connect:  16 rx slots, 16 tx slots, 0 long searches, 0 misses, 0% hit ratio
          Five minute miss rate 0 misses/sec, 0 max misses/sec
```

次の出力例では、**showframe-relayiptcpheader-compression** コマンドで「MP-3-static」という名前の PVC バンドルに関する統計情報を表示します。

```
Router# show frame-relay ip tcp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
             474 bytes saved, 119 bytes sent
             4.98 efficiency improvement factor
    Connect:256 rx slots, 256 tx slots,
             1 long searches, 1 misses 0 collisions, 0 negative cache hits
             93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

次の例では、**showframe-relayiptcpheader-compression** コマンドで DLCI 21 に関する情報を表示します。

```
Router# show frame-relay ip tcp header-compression 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の出力例では、**showframe-relayiptcpheader-compression** コマンドで、特定のインターフェイスの特定の DLCI を表示します。

```
Router# show frame-relay ip tcp header-compression pos2/0 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

次の表に、この出力で表示されるフィールドについて説明します。

表 *18 : show frame-relay ip tcp header-compression* フィールドの説明

フィールド	説明
Rcvd:	受信パケットの詳細情報の表。
total	受信した圧縮パケットと非圧縮パケットの合計数。
compressed	受信した圧縮パケットの数。
errors	ヘッダー フィールドのエラーが原因のエラー数（バージョン、全体の長さ、または IP チェックサム）。
dropped	廃棄されたパケット数。回線エラー後にのみ発生。
buffer failures	新しいバッファが必要な場合に取得できなかった回数。
Sent:	送信パケットの詳細情報の表。
total	送信した圧縮パケットと非圧縮パケットの合計数。
compressed	送信された圧縮パケットの数。
bytes saved	圧縮によって節約されたバイト数。
bytes sent	送信された実際のバイト数。
Connect:	接続の詳細情報の表。
rx slots、tx slots	1 回の TCP 接続で許可される状態の数。状態は、発信元アドレス、宛先アドレス、および IP ヘッダー長で認識されます。
long searches	着信パケットの接続 ID が処理済みの前回のものと異なる回数。
misses	一致するエントリが接続テーブル内に見つからず、新しいエントリを入力する必要があった回数。
hit ratio	一致するエントリが圧縮テーブル内で見つかり、ヘッダーが圧縮された回数のパーセンテージ。
Five minute miss rate	直近 5 分間で計算されたミス レート、およびこの期間の 1 秒あたりの最大ミス レート。

show interfaces fair-queue

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showinterfacesfair-queue** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showinterfacesfair-queue** コマンドは、モジュラ QoS CLI（MQC）コマンド（または MQC コマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Versatile Interface Processor（VIP）ベースのインターフェイスの重み付け均等化キューイング（WFQ）に関する詳細と統計情報を表示するには、EXEC モードで **showinterfacesfair-queue** コマンドを使用します。

show interfaces [*type number*] **fair-queue**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

例

次の出力例では、**showinterfacesfair-queue** コマンドで VIP 分散 WFQ（DWFQ）を表示します。

```
Router# show interfaces fair-queue
Hssi0/0/0 queue size 0
        packets output 1417079, drops 2
 WFQ: aggregate queue limit 54, individual queue limit 27
    max available buffers 54

     Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
     Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
     Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
     Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *19 : show interfaces fair-queue* フィールドの説明

フィールド	説明
queue size	このインターフェイスの現在の出力キュー サイズ。
packets output	このインタ フェースから送信されるパケット数またはインターフェイスから送信されるこのクラスのパケット数。
drops	ドロップされたパケットの数またはドロップされたこのクラスのパケットの数。
aggregate queue limit	集約制限（パケット数）。
individual queue limit	個別制限（パケット数）。
max available buffers	集約キュー制限（パケット数）に割り当てられた使用可能バッファ スペース。
Class	QoS グループまたはタイプ オブ サービス（ToS）クラス。

フィールド	説明
weight	輻輳期間中にこのクラスに割り当てられた帯域幅のパーセント。
limit	このクラスのキュー制限（パケット数）
qsize	このクラスの現在のキュー サイズ。

関連コマンド

Command	Description
showinterfaces	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。

show interfaces random-detect

（注） Cisco IOS XE Release 2.6、Cisco IOS Release 15.0(1)S、および Cisco IOS Release 15.1(3)T では、**showinterfacesrandom-detect** コマンドは非表示です。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンド ラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンド シーケンス）を使用する必要があります。代替コマンドのリストなど詳細については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントまたは『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

（注） Cisco IOS XE Release 3.2S では、**showinterfacesrandom-detect** コマンドは、モジュラ QoS CLI（MQC）コマンド（またはMQCコマンドのシーケンス）によって置き換えられます。適切な代替コマンド（またはコマンド シーケンス）については、『*Cisco IOS XE Quality of Service Solutions Configuration Guide*』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

Versatile Interface Processor（VIP）ベースのインターフェイスの重み付けランダム早期検出（WRED）に関する情報を表示するには、EXEC モードで **showinterfacesrandom-detect** コマンドを使用します。

show interfaces [*type number*] **random-detect**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドが非表示になりました。
15.0(1)S	このコマンドが変更されました。このコマンドが非表示になりました。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。
Cisco IOS XE Release 3.2S	このコマンドが、MQC コマンド（または MQC コマンドのシーケンス）に置き換えられました。

例

次の出力例では、**showinterfacesrandom-detect** コマンドで VIP 分散 WRED（DWRED）を表示します。

```
Router# show interfaces random-detect
 FastEthernet1/0/0 queue size 0
        packets output 29692, drops 0
 WRED: queue average 0
       weight 1/512
     Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
       1 packets output, drops: 0 random, 0 threshold
     Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
       14845 packets output, drops: 0 random, 0 threshold
     Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
     Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
       14846 packets output, drops: 0 random, 0 threshold
     Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
        (no traffic)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *20 : show interfaces random-detect* フィールドの説明

フィールド	説明
queue size	このインターフェイスの現在の出力キュー サイズ。
packets output	このインターフェイスから送信されるパケットの数。
drops	ドロップされたパケットの数
queue average	平均キューの長さ。

フィールド	説明
weight	平均キューの長さの決定に使用する重み係数。
Precedence	このプレシデンスの WRED パラメータ。
min threshold	このプレシデンスの最小しきい値。
max threshold	キューの最大長。平均キューがこの長さの場合、追加のパケットはドロップされます。
mark weight	平均キューが最大しきい値に達したときのパケットがドロップされる確率。
packets output	このプレシデンスが指定された送信済みパケットの数。
random	WRED プロセスによってランダムにドロップされたパケットの数。
threshold	平均キューが最大しきい値長に達したため自動的にドロップされるパケットの数。
(no traffic)	このプレシデンスが指定されたパケットはありません。

関連コマンド

Command	Description
random-detect(interface)	WRED または DWRED をイネーブルにします。
random-detectflow	フローベース WRED をイネーブルにします。
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。
showqueueing	すべてまたは選択した設定済みキューイング戦略を表示します。

show interfaces rate-limit

インターフェイスの専用アクセス レート（CAR）の情報を表示するには、EXEC モードで **showinterfacesrate-limit** コマンドを使用します。

show interfaces [*type number*] **rate-limit**

構文の説明

type	（任意）インターフェイスのタイプ。
number	（任意）インターフェイスの番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
11.1CC	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

例

次に、**showinterfacesrate-limit** コマンドの出力例を示します。

```
Router# show interfaces fddi2/1/0 rate-limit
Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-continue 1
   exceeded 0 packets, 0 bytes; action: set-prec-continue 0
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 101
   params: 80000000 bps, 56000 limit, 72000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 50000000 bps, 48000 limit, 64000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 80000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: transmit
   exceeded 0 packets, 0 bytes; action: drop
```

```
last packet: 4809528ms ago, current burst: 0 bytes
last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *21 : show interfaces rate-limit* フィールドの説明

フィールド	説明
Input	これらのレート制限はインターフェイスで受信したパケットに適用されます。
matches	このレート制限に一致するパケット。
params	**rate-limit** コマンドで設定した、このレート制限のパラメータ。
bps	平均レート（ビット/秒）です。
limit	バイト単位の通常バースト サイズ。
extended limit	バイト単位の超過バースト サイズ。
conformed	レート制限に一致したパケットの数。
action	Conform アクション。
exceeded	レート制限を超過したパケットの数。
アクション	Exceed アクション。
last packet	最後のパケットから経過した時間（ミリ秒）。
current burst	現時点のバースト サイズ。
last cleared	**clearcounters** コマンドでバースト カウンタをゼロに戻してから経過した時間。
conformed	一致したトラフィックの割合。
exceeded	超過したトラフィックの割合。
Output	これらのレート制限は、インターフェイスから送信されたパケットに適用されます。

関連コマンド

Command	Description
access-listrate-limit	CAR ポリシーで使用する場合のアクセス リストを設定します。
clearcounters	インターフェイス カウンタをクリアします。
shape	平均またはピーク レート トラフィック シェーピングを指定します。
showaccess-lists	現在の IP とレート制限アクセス リストの内容を表示します。

Command	Description
showinterfaces	ルータまたはアクセスサーバで設定されているすべてのインターフェイスの統計情報を表示します。

show iphc-profile

1 つ以上の IP ヘッダー圧縮（IPHC）プロファイルの設定情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiphc-profile** コマンドを使用します。

show iphc-profile [*profile-name*]

構文の説明

profile-name	（任意）表示する IPHC プロファイルの名前。

コマンド デフォルト

IPHC プロファイルの名前を指定しない場合は、すべての IPHC プロファイルが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(9)T	このコマンドが導入されました。
12.4(24)T	このコマンドが変更されました。出力は、EcRTP が設定されている場合に、回復可能な損失を表示するように拡張されました。

使用上のガイドライン

表示に含まれている情報

表示に含まれる情報には、プロファイル タイプ、有効なヘッダー圧縮のタイプ、コンテキストの数、更新間隔（Real-Time Transport [RTP] ヘッダー圧縮の場合）、フィードバック メッセージが無効になっているかどうか、IPHC プロファイルが添付されるインターフェイスなどがあります。

IPHC プロファイルの詳細について

IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

例

次は、**showiphc-profile** コマンドの出力例です。出力では、profile19 および profile20 という IPHC プロファイルの情報が表示されています。

```
Router# show iphc-profile
IPHC Profile "profile19"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 1
  Controlled interfaces: (0)
  Reference Count:  (1)
```

```
IPHC Profile "profile20"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 4 (dynamic)
  Controlled interfaces: (0)
  Reference Count:  (0)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *22 : show iphc-profile* フィールドの説明

フィールド	説明
IPHC Profile	IPHC プロファイル名。
Type	IPHC プロファイル タイプ：VJ（van-jacobson の場合）または IETF。
Compressing	TCP、TCP 以外、RTP など使用されたヘッダー圧縮のタイプ。
Contexts	コンテキスト番号の計算に使用されたコンテキストの数および設定。
Refresh	コンテキスト更新間のパケットの最大数または最大時間を示します。
EcRTP	回復可能損失が有効かどうか、および EcRTP 回復可能損失がダイナミックに設定されているかどうかを示します。
Controlled interfaces	IPHC プロファイルが添付されるインターフェイス。
Reference Count	アクティブな IPHC プロファイル サブモードの数を示します。

関連コマンド

コマンド	説明
iphc-profile	IPHCプロファイルを作成します。

show ip nat translations rsvp

リソース予約プロトコル（RSVP）メッセージのアクティブなネットワーク アドレス変換（NAT）を表示するには、特権 EXEC モードで **show ip nat translations rsvp** コマンドを使用します。

show ip nat translations rsvp［ **vrf** *vrf-name*］

構文の説明

vrf *vrf-name*	（任意）VPN ルーティングおよび転送（VRF）トラフィック関連の情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(2)T	このコマンドが導入されました。

使用上のガイドライン

RSVP パケットに RSVP-NAT アプリケーション レイヤ ゲートウェイ（ALG）によって実行された IP アドレス/ポート変換を表示するには、**show ip nat translations rsvp** コマンドを使用します。

例

次に、**show ip nat translations rsvp** コマンドの出力例を示します。

```
Router# show ip nat translations rsvp

RSVP-NAT-ALG:
 Inside Local: Address: <ip-address>, Port: <port-number>
 Outside Local: Address: <ip-address>, Port: <port-number>
 Inside Global: Address: <ip-address>, Port: <port-number>
 Outside Global: Address: <ip-address>, Port: <port-number>
 L4-Protocol: <protocol-number>
 Local Path Phop: <ip-address>
 Local Resv Phop: <ip-address>
 Local Resv Confirm: <ip-address>
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *23 : show ip nat translations rsvp* フィールドの説明

フィールド	説明
Inside Local	内部ネットワーク上のホストに割り当てられた IP アドレスおよびポート番号（多くの場合ネットワーク インターフェイス カード（NIC）やサービス プロバイダーにより割り当てられた正当なアドレスではありません）。

フィールド	説明
Outside Local	外部ホストが内部ネットワークに出現するときのIPアドレスおよびポート番号（多くの場合NICやサービスプロバイダーにより割り当てられた正当なアドレスではありません）。
Inside Global	1 つ以上の内部のローカル IP アドレスを外部に対して表す正当な IP アドレスおよびポート番号。
Outside Global	外部ネットワーク上のホストに、所有者が割り当てた IP アドレスおよびポート番号。
Address	変換の適切なカテゴリを表す IP アドレス。
Port	変換の適切なカテゴリを表すポート番号。
L4-Protocol	アドレスを識別するポートのレイヤ 4 プロトコル。
Local Path Phop	グローバルからローカルへ Resv メッセージを送信するために使用する前回のローカル ホップのアドレス。
Local Resv Phop	Resv メッセージがローカルからグローバルに着信したときに保存される前回のローカル ホップのアドレス。このアドレスは、Resv エラー メッセージの通過時に使用されます。
Local Resv Confirm	Resv メッセージの処理時に保存されるローカルホップのアドレスで、Resv 確認メッセージの通過に使用されます。

show ip nbar attribute

Network-Based Application Recognition（NBAR）で使用する設定属性を表示するには、特権 EXEC モードで **showipnbarattribute** コマンドを使用します。

show ip nbar attribute [{**application-group** |**business-relevance** |**category** |**encrypted** |**p2p-technology** |**sub-category** |**traffic-class** |**tunnel**}]

show ip nbar attribute *attribute-name attribute-value* [{*attribute-name attribute-value*}]

構文の説明

application-group	（任意）アプリケーション グループ属性を指定します。
business-relevance	（任意）ビジネス関連属性を指定します。
category	（任意）カテゴリ属性を指定します。
encrypted	（任意）暗号化アプリケーションを指定します。
p2p-technology	（任意）P2P アプリケーションを指定します。
sub-category	（任意）サブカテゴリ属性を指定します。
traffic-class	（任意）トラフィック クラス属性を指定します。
tunnel	（任意）トンネル アプリケーションを指定します。
attribute-name	（任意）プロトコル属性の名前。*attribute-value* を指定すると、コマンドには指定した属性値に一致するプロトコルのリストが表示されます。
attribute-value	（任意）*attribute-name* で指定した属性の値。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。
Cisco IOS XE Denali 16.4.1	2つの属性/属性値の組み合わせを照合する機能が追加されました。このモードでは、指定した属性の両方に一致するプロトコルのリストが表示されます。

使用上のガイドライン

showipnbarattribute コマンドは、複数のモードで動作します。

- 属性を指定せずに **showipnbarattribute** を実行すると、NBAR で使用するすべての属性のリストが表示されます。

- 属性（application-group、business-relevance、category、encrypted、p2p-technology、sub-category、traffic-class、tunnel）を指定して、**showipnbarattribute** *attribute-name* を実行すると、指定した属性のみ表示されます。
- 1 つまたは 2 つの属性と値を指定して **showipnbarattribute** *attribute-name attribute-value* [*attribute-name attribute-value*] を実行すると、指定した属性値に一致する、ルータにロードされたプロトコルのリストが表示されます。2 つの属性が指定されると、両方に一致するプロトコルのみが表示されます。

  たとえば、次のように「traffic-class voip-telephony」と「business-relevance business-relevant」を指定します。

  ```
  show ip nbar attribute traffic-class voip-telephony business-relevance
  business-relevant
  ```

  この場合、traffic-class の値は voip-telephony で、business-relevance の値は business-relevant のプロトコルのリストが表示されます。

  このリストには、ロードされたプロトコル パックまたはカスタム プロトコルによって定義されたプロトコルが含まれる場合があります。

例

次は、**showipnbarattribute** コマンドの出力例です。属性のリストが表示されます。

```
Router# show ip nbar attribute
      Name :  category
      Help :  category attribute
      Type :  group
    Groups :  email, newsgroup, location-based-services, instant-messaging, netg
      Need :  Mandatory
   Default :  other
      Name :  sub-category
      Help :  sub-category attribute
      Type :  group
    Groups :  routing-protocol, terminal, epayement, remote-access-terminal, nen
      Need :  Mandatory
   Default :  other
      Name :  application-group
      Help :  application-group attribute
      Type :  group
    Groups :  skype-group, wap-group, pop3-group, kerberos-group, tftp-group, bp
      Need :  Mandatory
   Default :  other
      Name :  tunnel
      Help :  Tunnelled applications
      Type :  group
    Groups :  tunnel-no, tunnel-yes, tunnel-unassigned
      Need :  Mandatory
   Default :  tunnel-unassigned
      Name :  encrypted
      Help :  Encrypted applications
      Type :  group
    Groups :  encrypted-yes, encrypted-no, encrypted-unassigned
      Need :  Mandatory
   Default :  encrypted-unassigned
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *24 : show ip nbar attribute* フィールドの説明

フィールド	説明
Name	属性の名前を示します。
Help	属性情報を表示します。
Type	属性のタイプを示します。
Groups	属性内のグループを指定します。
Need	属性の必要性を指定します。
Default	属性のデフォルト状態を表示します。

次は、属性と値が指定されたモードでこのコマンドを使用した場合の出力例です。一致するプロトコルのリストと各プロトコルの説明が表示されます。

```
Router# show ip nbar attribute traffic-class voip-telephony business-relevance
business-relevant
  cisco-collab-audio     Cisco Collaboration Voice by various Cisco unified communication
 clients.
  cisco-jabber-audio      Cisco Jabber Client; Audio Calls and Voice Mail
  cisco-media-audio       Cisco IP Phones and PC-based Unified Communicators
  cisco-phone-audio      Cisco IP Phones and PC-based Unified Communicators; Audio Calls

  citrix-audio            Citrix Audio Traffic
  ms-lync-audio           Skype provides cost effective and collaborative tools for
businesses
  rtp-audio               Real Time Protocol Audio
  telepresence-audio      Telepresentce Voice by various Cisco unified communication
clients.
```

関連コマンド

コマンド	説明
matchprotocolattributeapplication-group	アプリケーション グループに基づいてクラス マップの一致基準を設定します。
matchprotocolattributecategory	カテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributeencrypted	暗号化に基づいてクラス マップの一致基準を設定します。
matchprotocolattributesub-category	サブカテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributetunnel	トンネリングに基づいてクラス マップの一致基準を設定します。

show ip nbar classification auto-learn top-asymmetric-sockets

不明、HTTP および SSL トラフィックの非対称フローを表示するには、特権 EXEC モードで **showipnbarclassificationauto-learntop-asymmetric-sockets** コマンドを使用します。

show ip nbar classification auto-learn top-asymmetric-sockets *number-of-flows*[{**detailed**|**http**|**ssl**|**tcp**|**udp**|**unknown**}]

構文の説明

number-of-flows	表示するフロー数です。範囲：1 ～ 100
detailed	非対称フロー数が 0 のソケットも表示します。
http、**ssl**、**tcp**、**udp**、**unknown**	指定したタイプのソケットのみを含む出力をフィルタします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
Cisco IOS XE Releases 16.3.2 および 16.4.1	このコマンドが導入されました。

使用上のガイドライン

showipnbarclassificationauto-learn top-asymmetric-sockets コマンドは、不明、HTTP、または SSL に分類されたトラフィックの非対称フローを表示します。これは、非対称フローが NBAR2 分類に影響を与えているかどうかを判断する場合に役立つことがあります。

例

次は、**showipnbarclassificationauto-learn top-asymmetric-sockets** コマンドの出力例です。

```
Router# show ip nbar classification auto-learn top-asymmetric-sockets 100
Total tracked flows:               19.609 K
Asymmetric tracked flows:          19.609 K  (100%)
           Unknown TCP  asymmetric flows:         19.609 K (100%)
           Unknown UDP  asymmetric flows:          0       (0%)
          Generic HTTP asymmetric flows:         4.559 K (23%) -> percent are calculated
 from the total tracked flows.
           Generic SSL  asymmetric flows:         60       (0%)
DNS: Response without request (blocked by DNS guard): 100%

Asymmetric Tracked Flows Per Socket:
---|---------------
|--------|-----|---------------|---------|-----------|----|--------------|----|
#  |IP (*)          |Vrf name|Port |Classification |Transport|Asymmetric |Asym|Total
      |Host|
   |                |        |     |               |         |Flows      |%   |Flows
      |    |
---|---------------
|--------|-----|---------------|---------|-----------|----|--------------|----|
1  |171.71.196.84   |global  |4282 |unknown        |TCP      |  8.994 K  |100%|  8.994
K     |N/A |
2  |173.36.9.202    |global  |4282 |unknown        |TCP      |  2.998 K  |100%|  2.998
K     |N/A |
```

```
3  |171.71.196.85   |global  |4282 |unknown        |TCP      |  2.998 K  |100%|  2.998
K     |N/A |
4  |74.125.71.148   |global  |80   |http           |TCP      |600        |100%|600
      |N/A |
5  |54.246.114.214  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
6  |54.246.114.211  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
7  |54.246.114.212  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
8  |54.246.114.215  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
9  |54.246.114.213  |global  |80   |http           |TCP      |120        |100%|120
      |N/A |
10 |20.20.20.4      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
11 |20.20.20.8      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
12 |20.20.20.3      |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
13 |20.20.20.15     |global  |80   |http           |TCP      | 90        |100%| 90
      |N/A |
```

次は、**showipnbarclassificationauto-learn top-asymmetric-sockets** コマンドの出力例です。HTTP ソケットのみをフィルタするため、**http** キーワードを追加しています。Classification 列には「http」ソケットのみが表示されることに注意してください。

```
Router# show ip nbar classification auto-learn top-asymmetric-sockets 100 http
Total tracked flows:               24.912 M
Asymmetric tracked flows:          24.555 M  (98%)
           Unknown TCP  asymmetric flows:         19.934 M (80%)
           Unknown UDP  asymmetric flows:          4.620 M (18%)
           Generic HTTP asymmetric flows:          1.775 M (7%)
           Generic SSL  asymmetric flows:         17.405 M (69%)
DNS: Response without request (blocked by DNS guard): 3%


Asymmetric Tracked Flows Per Socket:
---|-----------------
|--------|-----|---------------|---------|-----------|----|----------|---------------|
#  |IP (*)            |Vrf name|Port |Classification |Transport|Asymmetric |Asym|Total
    |Host           |
   |                  |        |     |               |         |Flows      |%   |Flows
    |               |
---|-----------------
|--------|-----|---------------|---------|-----------|----|----------|---------------|
1  |10.42.9.30        |global  |80   |http           |TCP      |563.666 K  |100%|563.666
 K |N/A            |
2  |10.42.7.65        |global  |80   |http           |TCP      |446.010 K  |100%|446.010
 K |N/A            |
3  |10.42.23.213      |global  |80   |http           |TCP      |280.411 K  |100%|280.411
 K |N/A            |
4  |10.194.30.208     |global  |80   |http           |TCP      |163.195 K  |100%|163.195
 K |10.10.10.10    |
5  |10.42.5.71        |global  |80   |http           |TCP      | 57.136 K  |100%| 57.136
 K |N/A            |
6  |10.42.5.200       |global  |80   |http           |TCP      | 56.170 K  |100%| 56.170
 K |N/A            |
7  |172.19.137.134    |global  |80   |http           |TCP      | 49.931 K  |100%| 49.931
 K |test-test-test2|
8  |74.125.28.121     |global  |80   |http           |TCP      | 19.517 K  |100%| 19.517
 K |ip.kuku.com    |
```

```
9  |10.42.4.56        |global  |80   |http           |TCP      | 16.561 K  |100%| 16.561
 K |N/A            |
10 |10.34.161.43      |global  |80   |http           |TCP      | 15.036 K  |100%| 15.036
 K |10.34.161.43   |
11 |10.42.9.27        |global  |80   |http           |TCP      | 13.414 K  |100%| 13.414
 K |N/A            |
12 |10.35.45.42       |global  |80   |http           |TCP      |  6.169 K  |100%|  6.169
 K |N/A            |
13 |10.42.1.64        |global  |80   |http           |TCP      |  3.323 K  |100%|  3.323
 K |N/A            |
14 |10.42.38.81       |global  |80   |http           |TCP      |  3.100 K  |100%|  3.100
 K |N/A            |
15 |10.35.33.15       |global  |80   |http           |TCP      |  3.099 K  |98 %|  3.147
 K |N/A            |
16 |10.42.28.115      |global  |8081 |http           |TCP      |  3.047 K  |100%|  3.047
 K |N/A            |
17 |10.42.28.59       |global  |8081 |http           |TCP      |  2.993 K  |100%|  2.993
 K |N/A            |
18 |10.42.1.10        |global  |80   |http           |TCP      |  2.804 K  |100%|  2.804
 K |N/A            |
19 |10.42.28.59       |global  |80   |http           |TCP      |  2.472 K  |100%|  2.472
 K |N/A            |
20 |10.42.28.115      |global  |80   |http           |TCP      |  2.411 K  |100%|  2.411
 K |N/A            |
```

show ip nbar link-age

Network-Based Application Recognition（NBAR）ごとにプロトコルのリンク期限を表示するには、特権 EXEC モードで **showipnbarlink-age** コマンドを使用します。

show ip nbar link-age [*protocol-name*]

構文の説明

protocol-name	（任意）指定されたプロトコル名のリンク期限のみ表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.4(20)T	このコマンドが導入されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

showipnbarlink-age コマンドは、すべての NBAR プロトコルのリンク期限を表示します。特定のプロトコルの表示を制限するには、*protocol-name* 引数を使用します。

例

次は、**showipnbarlink-age** コマンドの出力例です。

```
Router# show ip nbar link-age

System Link Age: 30 seconds
No.  Protocol                  Link Age (seconds)
1    skype                        120
2  bittorrent                     120
3  winmx                          120
```

次は、特定のプロトコルについて表示する **showipnbarlink-age** コマンドの出力例です。

```
Router# show ip nbar link-age
 eigrp
System Link Age: 30 seconds
Protocol                  Link Age (seconds)
eigrp                        120
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *25 : show ip nbar link-age* フィールドの説明

フィールド	説明
No.	表示するプロトコル リストのシリアル番号です。
Protocol	NBAR プロトコルの名前です。

フィールド	説明
Link Age (seconds)	プロトコルのリンクが期限切れになる時間（秒）です。

関連コマンド

コマンド	説明
ipnbarresourcesprotocol	プロトコル ベースで、NBAR フロー リンク テーブルの有効期限を設定します。

show ip nbar classification auto-learn top-hosts

ジェネリックとして分類されたネットワーク トラフィックの上位ホストを示す Network Based Application Recognition（NBAR）の機能を有効にするには、**ip nbar classification auto-learn top-hosts** コマンドを使用します。

show ip nbar custom auto-learn top-hosts *number-of-hosts*［**details**］

構文の説明

number-of-hosts	上位ホストを自動学習するサンプル レートを設定します。
details	汎用に分類されたトップ ホストの統計情報とデータベースの詳細を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
15.5(2)T	このコマンドが導入されました。

例

次の例では、ネットワーク トラフィックの汎用に分類されたトップ ホストの統計情報とデータベースを表示します。

```
Device> show ip nbar classification auto-learn top-hosts 100
```

関連コマンド

コマンド	説明
ipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計およびデータベースを示す NBAR の機能を有効にします。
clearipnbarclassificationauto-learntop-hosts	ジェネリックとして分類されたネットワーク トラフィックの上位ホストの統計情報およびデータベースの表示をクリアします。

show ip nbar classification granularity

現在設定されている Network Based Application Recognition（NBAR）分類モードを表示するには、特権 EXEC モードで **show ip nbar classificationgranularity** コマンドを使用します。

show ip nbar classification granularity protocol *protocol-name*

構文の説明

protocol *protocol-name*	アプリケーションを示す指定されたプロトコルに対して、細粒分類を強制します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.14S	このコマンドが導入されました。
15.5(1)T	このコマンドが、15.5(1)T に統合されました。
15.5(2)T	このコマンドが変更されました。**protocol** *protocol-name* のキーワードと引数のペアが追加されました。
Cisco IOS XE Release 3.15S	このコマンドが、Cisco IOS XE Release 3.15S に統合されました。

例

次は、**show ip nbar granularity** コマンドの出力例です。この例では、現在設定されている NBAR 分類モード（粗粒）が表示されます。

```
Device#  show ip nbar classification granularity

NBAR classification granularity mode: coarse-grain
```

次は、**show ip nbar granularity** コマンドの出力例です。この例では、3pc プロトコルが細粒分類に強制設定されます。

```
Device# show ip nbar classification granularity protocol 3pc

Protocol                  Force mode
--------------------------------------
3pc                       fine-grain
```

関連コマンド

コマンド	説明
ipnbarclassificationgranularity	分類モード（細粒または粗粒）をNBARに設定します。

show ip nbar pdlm

Network-Based Application Recognition（NBAR）で使用する Packet Description Language Module（PDLM）を表示するには、特権 EXEC モードで **showipnbarpdlm** コマンドを使用します。

show ip nbar pdlm

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

ipnbarpdlm コマンドで NBAR にロードしたすべての PDLM のリストを表示するには、このコマンドを使用します。

例

この例では、**showipnbarpdlm** コマンドで、citrix.pdlm PDLM をフラッシュ メモリからロードします。

```
Router# show ip nbar pdlm

The following PDLMs have been loaded:
flash://citrix.pdlm
```

関連コマンド

コマンド	説明
ipnbarpdlm	シスコが提供する PDLM によって、NBAR が認識するプロトコルのリストを拡張および強化します。

show ip nbar port-map

このコマンドは廃止されました。

Network-Based Application Recognition（NBAR）で使用する現在のプロトコルからポートへのマッピングを表示するには、特権EXECモードで**showipnbarport-map**コマンドを使用します。

show ip nbar port-map [*protocol-name* [*protocol-type*]]

構文の説明

protocol-name	（任意）プロトコルの名前。使用可能なプロトコルの詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。
protocol-type	（任意）プロトコルのタイプ。2 つのタイプのプロトコルを指定できます。 • **tcp**：Transmission Control Protocol（TCP）ポートに関する情報を表示します。 • **udp**：User Datagram Protocol（UDP）ポートに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(13)E	このコマンドがCatalyst 6000 ファミリ スイッチに実装されました。FlexWAN モジュールが削除されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(22)T	このコマンドが Cisco IOS Release 12.4(22)T に統合されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
Cisco IOS XE Release 3.10S	このコマンドは廃止されました。

使用上のガイドライン

showipnbarport-map コマンドは、NBAR プロトコルのポート割り当てを表示します。

NBAR で使用する現在のプロトコルからポートへのマッピングを表示するには、**showipnbarport-map** コマンドを使用します。**ipnbarport-map** コマンドを使用すると、**showipnbarport-map** コマンドでは、プロトコルに割り当てたポートが表示されます。プロトコルの設定に **ipnbarport-map** コマンドを使用しないと、**showipnbarport-map** コマンドでは、デフォルトのポートが表示されます。特定のプロトコルの表示を制限するには、*protocol-name* 引数を使用します。*protocol-type* 引数タイプには、UDP または TCP を使用できます。

例

次は、**showipnbarport-map** コマンドの出力例です。

```
Router# show ip nbar port-map
port-map    cuseeme    udp    7648    7649    24032
port-map    cuseeme    tcp    7648    7649
port-map    dhcp       udp    67      68
port-map    dhcp       tcp    67      68
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *26 : show ip route track-table* フィールドの説明

フィールド	説明
port-map	割り当てられたポートを示します。
cuseeme	CU-SeeMe プロトコルが使用されていることを示します。
udp	User Datagram Protocol タイプが使用されていることを示します。
tcp	Transmission Control Protocol タイプが使用されていることを示します。
dhcp	Dynamic Host Configuration Protocol タイプが使用されていることを示します。

関連コマンド

コマンド	説明
ipnbarport-map	ウェルノウン ポート番号以外のポート番号を使用して、プロトコルまたはプロトコル名を検索するように NBAR を設定します。

show ip nbar protocol activated

デバイスのアクティブ化された Network-Based Application Recognition（NBAR）プロトコルをすべて表示するには、特権 EXEC モードで **show ip nbar protocol activated** コマンドを使用します。

show ip nbar protocol activated

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

使用上のガイドライン

デバッグには NBAR を有効にする必要があります。

例

次は、**show ip nbar protocol activated** コマンドの出力例です。

```
Device# show ip nbar protocol activated

Following Protocol are enabled
 Feature:PD
       Hwidb:Ethernet0/0 MI:1 SI:0 FR:0 PVC:0
All iana protocols
```

次の表で、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ています。

表 *27 : show ip nbar protocol activated* フィールドの説明

フィールド	説明
Hwidb	設定されたハードウェア IDB を表示します。
MT1	設定されたメインインターフェイスを表示します。
SI	設定されたサブインターフェイスを表示します。
FR	設定されたフレーム リレーを表示します。
PVC	設定された ATM PVC を表示します。

show ip nbar protocol-attribute

Network-Based Application Recognition（NBAR）で使用するプロトコル属性を表示するには、特権 EXEC モードで **showipnbarprotocol-attribute** コマンドを使用します。

show ip nbar protocol-attribute [*protocol-name*]

構文の説明

protocol-name	（任意）属性を表示するプロトコルの名前です。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。

使用上のガイドライン

すべてのプロトコルの属性を表示するには、**showipnbarprotocol-attribute** コマンドを使用します。特定のプロトコルの属性を表示するには、プロトコル名を指定します。

例

次は、**showipnbarprotocol-attribute** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Router# show ip nbar protocol-attribute ospf
    Protocol Name :  ospf
                category :  net-admin
            sub-category :  routing-protocol
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

Router# show ip nbar protocol-attribute
           Protocol Name :  ftp
                category :  file-sharing
            sub-category :  client-server
       application-group :  ftp-group
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  http
                category :  browsing
            sub-category :  other
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  egp
                category :  net-admin
            sub-category :  routing-protocol
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no
```

```
    Protocol Name :  gre
         category :  net-admin
     sub-category :  tunneling-protocols
application-group :  other
           tunnel :  tunnel-yes
        encrypted :  encrypted-no

    Protocol Name :  icmp
         category :  net-admin
     sub-category :  network-management
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no

    Protocol Name :  eigrp
         category :  net-admin
     sub-category :  routing-protocol
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no
```

関連コマンド

コマンド	説明
matchprotocolattributeapplication-group	アプリケーション グループに基づいてクラス マップの一致基準を設定します。
matchprotocolattributecategory	カテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributeencrypted	暗号化に基づいてクラス マップの一致基準を設定します。
matchprotocolattributesub-category	サブカテゴリに基づいてクラス マップの一致基準を設定します。
matchprotocolattributetunnel	トンネリングに基づいてクラス マップの一致基準を設定します。

show ip nbar protocol-discovery

Network-Based Application Recognition（NBAR）Protocol Discovery 機能で収集された統計情報を表示するには、**showipnbarprotocol-discoverycommandinprivilegedEXEC**モードを使用します。

show ip nbar protocol-discovery [**interface** *type number*] [**stats** {**byte-count**|**bit-rate**|**packet-count**|**max-bit-rate**}] [**protocol** *protocol-name*] [**top-n** *number*]

構文の説明

interface	（任意）このインターフェイスの Protocol Discovery 統計情報が表示されることを示します。
type	ポリシー設定が表示されるサブインターフェイスのインターフェイス タイプ。
number	ポート、コネクタ、VLAN、またはインターフェイス カードの番号です。
stats	（任意）バイト カウント、バイト レート、またはパケット カウントが表示されることを示します。
byte-count	（任意）バイト カウントが表示されることを示します。
max-bit-rate	（任意）最大ビット レートが表示されることを示します。
packet-count	（任意）パケット カウントが表示されることを示します。
protocol	（任意）特定のプロトコルの統計情報が表示されることを示します。
protocol-name	（任意）統計情報を表示するユーザ指定のプロトコル名です。
top-n	（任意）top-n が表示されることを示します。top-n はアクティブな NBAR サポート プロトコルのなかの上位プロトコル数です。n は表示するプロトコル数を表します。たとえば、top-n 3 と入力すると、アクティブな NBAR サポート プロトコルの上位 3 つが表示されます。
number	（任意）表示するアクティブな NBAR サポート プロトコルの上位の数を指定します。

コマンド デフォルト

NBAR Protocol Discovery 機能が有効になっているすべてのインターフェイスの統計情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。

リリース	変更箇所
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.1(13)E	このコマンドが、FlexWAN モジュールを備えていない Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.3(7)T	このコマンド出力が変更され、最大ビット レートが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(18)ZYA	このコマンドが、Cisco IOS Release 12.2(18)ZYA に統合されました。このコマンドが変更され、VLAN に関する情報表示（必要に応じて）、およびレイヤ 2 とレイヤ 3 両方の EtherChannel のサポート（Catalyst スイッチのみ）が追加されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。

使用上のガイドライン

NBAR Protocol Discovery 機能で収集した統計情報を表示するには、**showipnbarprotocol-discovery** コマンドを使用します。このコマンドのデフォルトでは、Protocol Discovery が現在有効になっているすべてのインターフェイスの統計情報を表示します。デフォルトの出力では、入力ビットレート（bps）、入力バイトカウント、入力パケットカウント、およびプロトコル名が、この順番で表示されます。

プロトコルディスカバリは、入力トラフィックと出力トラフィックの両方をモニタするために使用でき、有効なサービスポリシーがあってもなくても適用できます。NBAR Protocol Discovery によって、出力インターフェイスへスイッチされたパケットの統計情報が収集されます。パケットはさまざまな理由（出力インターフェイス、アクセス リスト、またはキュー ドロップでのポリシングなど）でスイッチング後にドロップされた可能性があるため、これらの統計情報は、出力インターフェイスのルータから出たパケットに関するものとは限りません。

レイヤ 2/3 Etherchannel サポート

Cisco IOS Release 12.2(18)ZYA は、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）搭載の Cisco 6500 シリーズ スイッチ用に設計されているため、**showipnbarprotocol-discovery** コマンドは、レイヤ 2 およびレイヤ 3 EtherChannel の両方でサポートされます。

例

次の例では、イーサネット インターフェイスのアクティブなプロトコルの上位 5 つについて、**showipnbarprotocol-discovery** コマンドの出力を表示する例を示します。

```
Router# show ip nbar protocol-discovery top-n 5

 Ethernet2/0
                              Input                     Output
```

```
                                -----                     ------
  Protocol                      Packet Count              Packet Count
                                Byte Count                Byte Count
                                30sec Bit Rate (bps)      30sec Bit Rate (bps)
                                30sec Max Bit Rate (bps)  30sec Max Bit Rate (bps)
--------------------------- ------------------------- -------------------------
   rtp                          3272685                   3272685
                                                242050604                 242050604

                                768000                    768000
                                2002000                   2002000
   gnutella                     513574                    513574
                                118779716                 118779716
                                383000                    383000
                                987000                    987000
   ftp                          482183                    482183
                                37606237                  37606237
                                121000                    121000
                                312000                    312000
   http                         144709                    144709
                                32351383                  32351383
                                105000                    105000
                                269000                    269000
   netbios                      96606                     96606
                                10627650                  10627650
                                36000                     36000
                                88000                     88000
   unknown                      1724428                   1724428
                                534038683                 534038683
                                2754000                   2754000
                                4405000                   4405000
   Total                        6298724                   6298724
                                989303872                 989303872
                                4213000                   4213000
                                8177000                   8177000
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *28 : show ip nbar protocol-discovery* フィールドの説明

フィールド	説明
Interface	インターフェイスのタイプと番号です。
Input	インターフェイスの着信トラフィックです。
Output	インターフェイスの発信トラフィックです。
Protocol	使用されているプロトコルです。unknown は、何らかの理由で NBAR が分類できなかったプロトコルすべての合計です。
Packet Count	インターフェイスで送受信されるパケットの数です。
Byte Count	インターフェイスで送受信されるバイト数です。
30sec Bit Rate	Protocol Discovery 有効化後のビット/秒（bps）単位でのプロトコルごとのビット レートの平均値です（直近 30 秒間）。

フィールド	説明
30sec Max Bit Rate	Protocol Discovery 有効化後のビット/秒（bps）単位でのプロトコルごとのビット レートの最大値です（直近 30 秒間）。
Total	入出力トラフィックの合計です。

関連コマンド

コマンド	説明
ipnbarprotocol-discovery	特定のインターフェイス上で NBAR が認識するすべてのプロトコルについて、トラフィックを検出するように NBAR を設定します。

show ip nbar protocol-id

Network Based Application Recognition（NBAR）プロトコル ID の情報を表示するには、特権 EXEC モードで **showipnbarprotocol-id** コマンドを使用します。

show ip nbar protocol-id [*protocol-name*]

構文の説明

protocol-name	（任意）プロトコルの名前。

コマンド デフォルト

オプションの引数を指定しないと、すべてのプロトコルの NBAR プロトコル ID が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.0(1)M	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)S	このコマンドが、Cisco IOS Release 15.1(1)S に統合されました。
Cisco IOS Release XE 3.2S	このコマンドが変更されました。追加 IANA プロトコルのサポートが追加されました。

例

次は、**showipnbarprotocol-id** コマンドの出力例です。

```
Router# show ip nbar protocol-id
Protocol Name              id             type
-----------------------------------------------
ftp                        2           Standard
http                       3           Standard
egp                        8           L3 IANA
gre                        47          L3 IANA
icmp                       1           L3 IANA
eigrp                      88          L3 IANA
ipinip                     4           L3 IANA
ipsec                      9           Standard
ospf                       89          L3 IANA
bgp                        179         L4 IANA
cuseeme                    12          Standard
dhcp                       13          Standard
finger                     79          L4 IANA
gopher                     70          L4 IANA
secure-http                16          Standard
imap                       17          Standard
secure-imap                18          Standard
irc                        194         L4 IANA
secure-irc                 994         L4 IANA
kerberos                   21          Standard
```

```
l2tp                          1701          L4 IANA
ldap                          389           L4 IANA
secure-ldap                   636           L4 IANA
sqlserver                     1433          L4 IANA
netbios                       26            Standard
nfs                           2049          L4 IANA
nntp                          28            Standard
secure-nntp                   563           L4 IANA
notes                         1352          L4 IANA
ntp                           123           L4 IANA
pcanywhere                    32            Standard
pop3                          110           L4 IANA
secure-pop3                   995           L4 IANA
pptp                          1723          L4 IANA
rip                           520           L4 IANA
rsvp                          37            Standard
snmp                          38            Standard
socks                         39            Standard
ssh                           22            L4 IANA
syslog                        41            Standard
telnet                        23            L4 IANA
secure-telnet                 992           L4 IANA
secure-ftp                    990           L4 IANA
xwindows                      45            Standard
printer                       515           L4 IANA
novadigm                      47            Standard
tftp                          48            Standard
exchange                      49            Standard
vdolive                       50            Standard
sqlnet                        51            Standard
rcmd                          52            Standard
netshow                       53            Standard
sunrpc                        54            Standard
streamwork                    55            Standard
citrix                        56            Standard
fasttrack                     57            Standard
gnutella                      58            Standard
kazaa2                        59            Standard
rtsp                          60            Standard
rtp                           61            Standard
mgcp                          62            Standard
skinny                        63            Standard
h323                          64            Standard
sip                           65            Standard
rtcp                          66            Standard
winmx                         68            Standard
bittorrent                    69            Standard
directconnect                 70            Standard
smtp                          71            Standard
dns                           72            Standard
hl7                           73            Standard
fix                           74            Standard
msn-messenger                 75            Standard
dicom                         76            Standard
yahoo-messenger               77            Standard
mapi                          78            Standard
aol-messenger                 79            Standard
cifs                          80            Standard
cisco-phone                   81            Standard
youtube                       82            Standard
skype                         83            Standard
sap                           84            Standard
blizwow                       85            Standard
whois++                       63            L4 IANA
```

```
klogin                    543         L4 IANA
kshell                    544         L4 IANA
ora-srv                   1525         L4 IANA
sqlexec                   9088         L4 IANA
clearcase                 371         L4 IANA
appleqtc                  458         L4 IANA
rcp                       469         L4 IANA
isakmp                    500         L4 IANA
ibm-db2                   523         L4 IANA
lockd                     4045         L4 IANA
npp                       92          L4 IANA
microsoftds               98          Standard
doom                      666         L4 IANA
vnc                       100         Standard
echo                      7           L4 IANA
systat                    11          L4 IANA
daytime                   13          L4 IANA
chargen                   19          L4 IANA
time                      37          L4 IANA
isi-gl                    55          L4 IANA
rtelnet                   107         L4 IANA
server-ipx                213         L4 IANA
xdmcp                     177         L4 IANA
nicname                   43          L4 IANA
corba-iiop                111         Standard
tacacs                    112         Standard
telepresence-media        113         Standard
telepresence-control      114         Standard
edonkey                   243         Custom
custom-10                 244         Custom
custom-09                 245         Custom
custom-08                 246         Custom
custom-07                 247         Custom
custom-06                 248         Custom
custom-05                 249         Custom
custom-04                 250         Custom
custom-03                 251         Custom
custom-02                 252         Custom
custom-01                 253         Custom
mftp                      349         L4 IANA
matip-type-a              350         L4 IANA
matip-type-b              351         L4 IANA
dtag-ste-sb               352         L4 IANA
ndsauth                   353         L4 IANA
datex-asn                 355         L4 IANA
cloanto-net-1             356         L4 IANA
bhevent                   357         L4 IANA
shrinkwrap                358         L4 IANA
nsrmp                     359         L4 IANA
scoi2odialog              360         L4 IANA
semantix                  361         L4 IANA
srssend                   362         L4 IANA
rsvp_tunnel               363         L4 IANA
aurora-cmgr               364         L4 IANA
dtk                       365         L4 IANA
odmr                      366         L4 IANA
mortgageware              367         L4 IANA
qbikgdp                   368         L4 IANA
rpc2portmap               369         L4 IANA
codaauth2                 370         L4 IANA
ulistproc                 372         L4 IANA
legent-1                  373         L4 IANA
legent-2                  374         L4 IANA
hassle                    375         L4 IANA
```

```
tnETOS                   377         L4 IANA
is99c                    379         L4 IANA
is99s                    380         L4 IANA
hp-collector             381         L4 IANA
hp-managed-node          382         L4 IANA
hp-alarm-mgr             383         L4 IANA
arns                     384         L4 IANA
ibm-app                  385         L4 IANA
asa                      386         L4 IANA
aurp                     387         L4 IANA
unidata-ldm              388         L4 IANA
fatserv                  347         L4 IANA
uis                      390         L4 IANA
synotics-relay           391         L4 IANA
synotics-broker          392         L4 IANA
meta5                    393         L4 IANA
embl-ndt                 394         L4 IANA
netware-ip               396         L4 IANA
mptn                     397         L4 IANA
kryptolan                398         L4 IANA
iso-tsap-c2              399         L4 IANA
ups                      401         L4 IANA
genie                    402         L4 IANA
decap                    403         L4 IANA
nced                     404         L4 IANA
ncld                     405         L4 IANA
imsp                     406         L4 IANA
timbuktu                 407         L4 IANA
prm-sm                   408         L4 IANA
prm-nm                   409         L4 IANA
decladebug               410         L4 IANA
rmt                      411         L4 IANA
synoptics-trap           412         L4 IANA
smsp                     413         L4 IANA
infoseek                 414         L4 IANA
bnet                     415         L4 IANA
onmux                    417         L4 IANA
hyper-g                  418         L4 IANA
ariel1                   419         L4 IANA
ariel2                   421         L4 IANA
ariel3                   422         L4 IANA
opc-job-start            423         L4 IANA
opc-job-track            424         L4 IANA
smartsdp                 426         L4 IANA
svrloc                   427         L4 IANA
ocs_cmu                  428         L4 IANA
ocs_amu                  429         L4 IANA
utmpsd                   430         L4 IANA
utmpcd                   431         L4 IANA
iasd                     432         L4 IANA
nnsp                     433         L4 IANA
mobileip-agent           434         L4 IANA
mobilip-mn               435         L4 IANA
dna-cml                  436         L4 IANA
comscm                   437         L4 IANA
dsfgw                    438         L4 IANA
dasp                     439         L4 IANA
sgcp                     440         L4 IANA
decvms-sysmgt            441         L4 IANA
cvc_hostd                442         L4 IANA
snpp                     444         L4 IANA
ddm-rdb                  446         L4 IANA
ddm-dfm                  447         L4 IANA
ddm-ssl                  448         L4 IANA
```

```
as-servermap              449         L4 IANA
tserver                   450         L4 IANA
sfs-smp-net               451         L4 IANA
sfs-config                452         L4 IANA
creativeserver            453         L4 IANA
contentserver             3365         L4 IANA
creativepartnr            455         L4 IANA
scohelp                   457         L4 IANA
skronk                    460         L4 IANA
datasurfsrv               461         L4 IANA
datasurfsrvsec            462         L4 IANA
alpes                     463         L4 IANA
kpasswd                   464         L4 IANA
digital-vrc               466         L4 IANA
mylex-mapd                467         L4 IANA
photuris                  468         L4 IANA
scx-proxy                 470         L4 IANA
mondex                    471         L4 IANA
ljk-login                 472         L4 IANA
hybrid-pop                473         L4 IANA
tn-tl-fd1                 476         L4 IANA
ss7ns                     477         L4 IANA
spsc                      478         L4 IANA
iafserver                 479         L4 IANA
iafdbase                  480         L4 IANA
bgs-nsi                   482         L4 IANA
ulpnet                    483         L4 IANA
integra-sme               484         L4 IANA
powerburst                485         L4 IANA
avian                     486         L4 IANA
saft                      487         L4 IANA
gss-http                  488         L4 IANA
nest-protocol             489         L4 IANA
micom-pfs                 490         L4 IANA
go-login                  491         L4 IANA
ticf-1                    492         L4 IANA
ticf-2                    493         L4 IANA
pov-ray                   494         L4 IANA
intecourier               495         L4 IANA
pim-rp-disc               496         L4 IANA
dantz                     497         L4 IANA
siam                      498         L4 IANA
iso-ill                   499         L4 IANA
stmf                      501         L4 IANA
asa-appl-proto            502         L4 IANA
intrinsa                  503         L4 IANA
mailbox-lm                505         L4 IANA
ohimsrv                   506         L4 IANA
crs                       507         L4 IANA
xvttp                     508         L4 IANA
snare                     509         L4 IANA
fcp                       510         L4 IANA
passgo                    511         L4 IANA
exec                      512         L4 IANA
shell                     430         Standard
videotex                  516         L4 IANA
talk                      517         L4 IANA
ntalk                     518         L4 IANA
utime                     519         L4 IANA
ripng                     521         L4 IANA
ulp                       522         L4 IANA
pdap                      344         L4 IANA
ncp                       524         L4 IANA
timed                     525         L4 IANA
```

```
tempo                          526          L4 IANA
stx                            527          L4 IANA
custix                         528          L4 IANA
irc-serv                       529          L4 IANA
courier                        530          L4 IANA
conference                     531          L4 IANA
netnews                        532          L4 IANA
netwall                        533          L4 IANA
iiop                           535          L4 IANA
opalis-rdv                     536          L4 IANA
nmsp                           537          L4 IANA
gdomap                         538          L4 IANA
apertus-ldp                    539          L4 IANA
uucp                           540          L4 IANA
uucp-rlogin                    541          L4 IANA
commerce                       542          L4 IANA
appleqtcsrvr                   545          L4 IANA
dhcpv6-client                  546          L4 IANA
dhcpv6-server                  547          L4 IANA
idfp                           549          L4 IANA
new-rwho                       550          L4 IANA
cybercash                      551          L4 IANA
pirp                           553          L4 IANA
remotefs                       556          L4 IANA
openvms-sysipc                 557          L4 IANA
sdnskmp                        558          L4 IANA
teedtap                        559          L4 IANA
rmonitor                       560          L4 IANA
monitor                        561          L4 IANA
chshell                        562          L4 IANA
9pfs                           564          L4 IANA
whoami                         565          L4 IANA
streettalk                     566          L4 IANA
banyan-rpc                     567          L4 IANA
ms-shuttle                     568          L4 IANA
ms-rome                        569          L4 IANA
meter                          570          L4 IANA
sonar                          572          L4 IANA
banyan-vip                     573          L4 IANA
ftp-agent                      574          L4 IANA
vemmi                          575          L4 IANA
ipcd                           576          L4 IANA
vnas                           577          L4 IANA
ipdd                           578          L4 IANA
decbsrv                        579          L4 IANA
sntp-heartbeat                 580          L4 IANA
bdp                            581          L4 IANA
scc-security                   582          L4 IANA
philips-vc                     583          L4 IANA
keyserver                      584          L4 IANA
password-chg                   586          L4 IANA
submission                     587          L4 IANA
tns-cml                        590          L4 IANA
http-alt                       8008          L4 IANA
eudora-set                     592          L4 IANA
http-rpc-epmap                 593          L4 IANA
tpip                           594          L4 IANA
cab-protocol                   595          L4 IANA
smsd                           596          L4 IANA
ptcnameservice                 597          L4 IANA
sco-websrvrmg3                 598          L4 IANA
acp                            599          L4 IANA
ipcserver                      600          L4 IANA
urm                            606          L4 IANA
```

```
nqs                         607         L4 IANA
sift-uft                    608         L4 IANA
npmp-trap                   609         L4 IANA
npmp-local                  610         L4 IANA
npmp-gui                    611         L4 IANA
hmmp-ind                    612         L4 IANA
hmmp-op                     613         L4 IANA
sshell                      614         L4 IANA
sco-inetmgr                 615         L4 IANA
sco-sysmgr                  616         L4 IANA
sco-dtmgr                   617         L4 IANA
dei-icda                    618         L4 IANA
sco-websrvrmgr              620         L4 IANA
escp-ip                     621         L4 IANA
collaborator                622         L4 IANA
cryptoadmin                 624         L4 IANA
dec_dlm                     625         L4 IANA
passgo-tivoli               627         L4 IANA
qmqp                        628         L4 IANA
3com-amp3                   629         L4 IANA
rda                         630         L4 IANA
ipp                         631         L4 IANA
bmpp                        632         L4 IANA
servstat                    633         L4 IANA
ginad                       634         L4 IANA
rlzdbase                    635         L4 IANA
lanserver                   637         L4 IANA
mcns-sec                    638         L4 IANA
msdp                        639         L4 IANA
entrust-sps                 640         L4 IANA
repcmd                      641         L4 IANA
esro-emsdp                  642         L4 IANA
sanity                      643         L4 IANA
dwr                         644         L4 IANA
ldp                         646         L4 IANA
dhcp-failover               647         L4 IANA
rrp                         648         L4 IANA
aminet                      2639         L4 IANA
obex                        650         L4 IANA
ieee-mms                    651         L4 IANA
hello-port                  652         L4 IANA
repscmd                     653         L4 IANA
aodv                        654         L4 IANA
tinc                        655         L4 IANA
spmp                        656         L4 IANA
rmc                         657         L4 IANA
tenfold                     658         L4 IANA
mac-srvr-admin              660         L4 IANA
hap                         661         L4 IANA
pftp                        662         L4 IANA
purenoise                   663         L4 IANA
sun-dr                      665         L4 IANA
disclose                    667         L4 IANA
mecomm                      668         L4 IANA
meregister                  669         L4 IANA
vacdsm-sws                  670         L4 IANA
vacdsm-app                  671         L4 IANA
vpps-qua                    672         L4 IANA
cimplex                     673         L4 IANA
acap                        674         L4 IANA
dctp                        675         L4 IANA
vpps-via                    676         L4 IANA
vpp                         677         L4 IANA
ggf-ncp                     678         L4 IANA
```

```
mrm                          679         L4 IANA
entrust-aaas                 680         L4 IANA
entrust-aams                 681         L4 IANA
mdc-portmapper               685         L4 IANA
hcp-wismar                   686         L4 IANA
asipregistry                 687         L4 IANA
realm-rusd                   688         L4 IANA
nmap                         689         L4 IANA
vatp                         690         L4 IANA
msexch-routing               691         L4 IANA
hyperwave-isp                692         L4 IANA
connendp                     693         L4 IANA
ha-cluster                   694         L4 IANA
ieee-mms-ssl                 695         L4 IANA
rushd                        696         L4 IANA
uuidgen                      697         L4 IANA
olsr                         698         L4 IANA
accessnetwork                699         L4 IANA
elcsd                        704         L4 IANA
agentx                       705         L4 IANA
silc                         706         L4 IANA
borland-dsj                  707         L4 IANA
entrust-kmsh                 709         L4 IANA
entrust-ash                  710         L4 IANA
cisco-tdp                    711         L4 IANA
netviewdm1                   729         L4 IANA
netviewdm2                   730         L4 IANA
netviewdm3                   731         L4 IANA
netgw                        741         L4 IANA
netrcs                       742         L4 IANA
flexlm                       744         L4 IANA
fujitsu-dev                  747         L4 IANA
ris-cm                       748         L4 IANA
pump                         751         L4 IANA
qrh                          752         L4 IANA
rrh                          753         L4 IANA
tell                         754         L4 IANA
nlogin                       758         L4 IANA
con                          759         L4 IANA
ns                           760         L4 IANA
rxe                          761         L4 IANA
quotad                       762         L4 IANA
cycleserv                    763         L4 IANA
omserv                       764         L4 IANA
webster                      765         L4 IANA
phonebook                    767         L4 IANA
vid                          769         L4 IANA
cadlock                      770         L4 IANA
rtip                         771         L4 IANA
cycleserv2                   772         L4 IANA
submit                       643         Standard
entomb                       775         L4 IANA
multiling-http               777         L4 IANA
wpgs                         780         L4 IANA
device                       801         L4 IANA
itm-mcell-s                  828         L4 IANA
pkix-3-ca-ra                 829         L4 IANA
dhcp-failover2               847         L4 IANA
rsync                        873         L4 IANA
iclcnet-locate               886         L4 IANA
iclcnet_svinfo               887         L4 IANA
accessbuilder                888         L4 IANA
omginitialrefs               900         L4 IANA
smpnameres                   901         L4 IANA
```

```
xact-backup                   911          L4 IANA
ftps-data                     989          L4 IANA
nas                           991          L4 IANA
vsinet                        996          L4 IANA
maitrd                        997          L4 IANA
applix                        999          L4 IANA
surf                          1010          L4 IANA
rmiactivation                 1098          L4 IANA
rmiregistry                   1099          L4 IANA
ms-sql-m                      1434          L4 IANA
ms-olap                       2393          L4 IANA
msft-gc                       3268          L4 IANA
msft-gc-ssl                   3269          L4 IANA
tlisrv                        1527          L4 IANA
coauthor                      1529          L4 IANA
rdb-dbs-disp                  1571          L4 IANA
oraclenames                   1575          L4 IANA
oraclenet8cman                1630          L4 IANA
net8-cman                     1830          L4 IANA
micromuse-lm                  1534          L4 IANA
orbix-locator                 3075          L4 IANA
orbix-config                  3076          L4 IANA
orbix-loc-ssl                 3077          L4 IANA
shockwave                     1626          L4 IANA
sitaraserver                  2629          L4 IANA
sitaramgmt                    2630          L4 IANA
sitaradir                     2631          L4 IANA
mysql                         3306          L4 IANA
net-assistant                 3283          L4 IANA
msnp                          1863          L4 IANA
groove                        2492          L4 IANA
directplay                    2234          L4 IANA
directplay8                   6073          L4 IANA
kali                          2213          L4 IANA
worldfusion                   2595          L4 IANA
directv-web                   3334          L4 IANA
directv-soft                  3335          L4 IANA
directv-tick                  3336          L4 IANA
directv-catlg                 3337          L4 IANA
wap-push                      2948          L4 IANA
wap-pushsecure                2949          L4 IANA
wap-push-http                 4035          L4 IANA
wap-push-https                4036          L4 IANA
wap-wsp                       9200          L4 IANA
wap-wsp-wtp                   9201          L4 IANA
wap-wsp-s                     9202          L4 IANA
wap-wsp-wtp-s                 9203          L4 IANA
wap-vcard                     9204          L4 IANA
wap-vcal                      9205          L4 IANA
wap-vcard-s                   9206          L4 IANA
wap-vcal-s                    9207          L4 IANA
ibprotocol                    6714          L4 IANA
gtp-user                      2152          L4 IANA
xdtp                          3088          L4 IANA
parsec-game                   6582          L4 IANA
hopopt                        0            L3 IANA
ggp                           3            L3 IANA
st                            5            L3 IANA
cbt                           7            L3 IANA
zserv                         346          L4 IANA
igrp                          9            L3 IANA
bbnrccmon                     10           L3 IANA
pawserv                       345          L4 IANA
texar                         333          L4 IANA
```

```
rtsps                    322         L4 IANA
pip                      1321         L4 IANA
ptp-general              320         L4 IANA
nat-stun                 3478         L4 IANA
compressnet              2           L4 IANA
rje                      5           L4 IANA
discard                  9           L4 IANA
qotd                     17          L4 IANA
msp                      18          L4 IANA
ftp-data                 20          L4 IANA
nsw-fe                   27          L4 IANA
msg-icp                  29          L4 IANA
csi-sgwp                 348         L4 IANA
msg-auth                 31          L4 IANA
dsp                      33          L4 IANA
rap                      38          L4 IANA
rlp                      39          L4 IANA
graphics                 41          L4 IANA
name                     42          L4 IANA
profile                  136         L4 IANA
mpm-flags                44          L4 IANA
mpm                      45          L4 IANA
mpm-snd                  46          L4 IANA
ni-ftp                   47          L4 IANA
auditd                   48          L4 IANA
emfis-data               140         L4 IANA
re-mail-ck               50          L4 IANA
la-maint                 51          L4 IANA
xns-time                 52          L4 IANA
emfis-cntl               141         L4 IANA
xns-ch                   54          L4 IANA
bl-idm                   142         L4 IANA
xns-auth                 56          L4 IANA
xns-mail                 58          L4 IANA
ni-mail                  61          L4 IANA
acas                     62          L4 IANA
covia                    64          L4 IANA
sql*net                  66          L4 IANA
bootps                   67          L4 IANA
bootpc                   68          L4 IANA
uaac                     145         L4 IANA
iso-tp0                  146         L4 IANA
netrjs-1                 71          L4 IANA
netrjs-2                 72          L4 IANA
netrjs-3                 73          L4 IANA
netrjs-4                 74          L4 IANA
deos                     76          L4 IANA
iso-ip                   147         L4 IANA
xfer                     82          L4 IANA
mit-ml-dev               83          L4 IANA
ctf                      84          L4 IANA
mfcobol                  86          L4 IANA
jargon                   148         L4 IANA
su-mit-tg                89          L4 IANA
dnsix                    90          L4 IANA
mit-dov                  91          L4 IANA
aed-512                  149         L4 IANA
dcp                      93          L4 IANA
objcall                  94          L4 IANA
supdup                   95          L4 IANA
dixie                    96          L4 IANA
swift-rvf                97          L4 IANA
tacnews                  98          L4 IANA
metagram                 99          L4 IANA
```

```
hostname                 101         L4 IANA
iso-tsap                 102         L4 IANA
acr-nema                 104         L4 IANA
csnet-ns                 105         L4 IANA
3com-tsmux               106         L4 IANA
sql-net                  150         L4 IANA
snagas                   108         L4 IANA
pop2                     109         L4 IANA
hems                     151         L4 IANA
mcidas                   112         L4 IANA
auth                     113         L4 IANA
sftp                     115         L4 IANA
ansanotify               116         L4 IANA
uucp-path                117         L4 IANA
sqlserv                  118         L4 IANA
cfdptkt                  120         L4 IANA
erpc                     121         L4 IANA
smakynet                 122         L4 IANA
bftp                     152         L4 IANA
ansatrader               124         L4 IANA
locus-map                125         L4 IANA
nxedit                   126         L4 IANA
locus-con                127         L4 IANA
gss-xlicen               128         L4 IANA
pwdgen                   129         L4 IANA
cisco-fna                130         L4 IANA
sgmp                     153         L4 IANA
netsc-prod               154         L4 IANA
netsc-dev                155         L4 IANA
knet-cmp                 157         L4 IANA
pcmail-srv               158         L4 IANA
nss-routing              159         L4 IANA
sgmp-traps               160         L4 IANA
cmip-man                 163         L4 IANA
cmip-agent               164         L4 IANA
xns-courier              165         L4 IANA
s-net                    166         L4 IANA
namp                     167         L4 IANA
rsvd                     168         L4 IANA
send                     169         L4 IANA
print-srv                170         L4 IANA
multiplex                171         L4 IANA
xyplex-mux               173         L4 IANA
mailq                    174         L4 IANA
vmnet                    175         L4 IANA
genrad-mux               176         L4 IANA
nextstep                 178         L4 IANA
ris                      180         L4 IANA
unify                    181         L4 IANA
audit                    182         L4 IANA
ocbinder                 183         L4 IANA
ocserver                 184         L4 IANA
remote-kis               185         L4 IANA
kis                      186         L4 IANA
mumps                    188         L4 IANA
qft                      189         L4 IANA
gacp                     190         L4 IANA
prospero                 191         L4 IANA
osu-nms                  192         L4 IANA
srmp                     193         L4 IANA
dn6-nlm-aud              195         L4 IANA
dls                      197         L4 IANA
dls-mon                  198         L4 IANA
smux                     199         L4 IANA
```

```
src                            200          L4 IANA
at-rtmp                        201          L4 IANA
at-nbp                         202          L4 IANA
at-3                           203          L4 IANA
at-echo                        204          L4 IANA
at-5                           205          L4 IANA
at-zis                         206          L4 IANA
at-7                           207          L4 IANA
at-8                           208          L4 IANA
qmtp                           209          L4 IANA
z39.50                         210          L4 IANA
914c/g                         211          L4 IANA
anet                           212          L4 IANA
vmpwscs                        214          L4 IANA
softpc                         215          L4 IANA
CAIlic                         216          L4 IANA
dbase                          217          L4 IANA
mpp                            218          L4 IANA
uarps                          219          L4 IANA
fln-spx                        221          L4 IANA
rsh-spx                        222          L4 IANA
cdc                            223          L4 IANA
masqdialer                     224          L4 IANA
sur-meas                       243          L4 IANA
inbusiness                     244          L4 IANA
dsp3270                        246          L4 IANA
subntbcst_tftp                 247          L4 IANA
bhfhs                          248          L4 IANA
set                            257          L4 IANA
esro-gen                       259          L4 IANA
openport                       260          L4 IANA
nsiiops                        261          L4 IANA
arcisdms                       262          L4 IANA
hdap                           263          L4 IANA
bgmp                           264          L4 IANA
x-bone-ctl                     265          L4 IANA
sst                            266          L4 IANA
td-service                     267          L4 IANA
td-replica                     268          L4 IANA
http-mgmt                      280          L4 IANA
personal-link                  281          L4 IANA
cableport-ax                   282          L4 IANA
rescap                         283          L4 IANA
corerjd                        284          L4 IANA
k-block                        287          L4 IANA
novastorbakcup                 308          L4 IANA
bhmds                          310          L4 IANA
asip-webadmin                  311          L4 IANA
vslmp                          312          L4 IANA
magenta-logic                  313          L4 IANA
opalis-robot                   314          L4 IANA
dpsi                           315          L4 IANA
decauth                        316          L4 IANA
zannet                         317          L4 IANA
pkix-timestamp                 318          L4 IANA
ptp-event                      319          L4 IANA
cisco-tna                      131          L4 IANA
cisco-sys                      132          L4 IANA
statsrv                        133          L4 IANA
ingres-net                     134          L4 IANA
Konspire2b                     6085          L4 IANA
Total protocols:               721
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *29 : show ip nbar protocol-id* フィールドの説明

フィールド	説明
Protocol Name	NBAR プロトコルの名前です。
id	NBAR プロトコルに割り当てられている固有識別子です。
type	プロトコルが標準かカスタマイズされているかを示します。

関連コマンド

コマンド	説明
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポート アプリケーションを分類および監視できます。または、NBAR はサポートしていないスタティック ポート トラフィックを分類できるようになります。

show ip nbar protocol-pack

プロトコル パック情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip nbar protocol-pack** コマンドを使用します。

show ip nbar protocol-pack {*protocol-pack*|**active**} **[detail]**

構文の説明

protocol-pack	プロトコル パック ファイルのパスおよび名前です。
active	アクティブなプロトコル パック情報を表示します。
detail	（任意）詳細なプロトコルパック情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

プロトコル パックは、複数のプロトコル記述言語（PDL）ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。このプロトコルパックが導入される前は、PDL を個別にロードする必要がありました。Network-Based Application Recognition（NBAR）プロトコル パックを使用すると、必須のプロトコル セットをロードでき、ご使用のネットワークでの分類で、NBAR が認識可能なプロトコルを追加できます。

例

次の **show ip nbar protocol-pack** コマンドからの出力例では、アクティブなプロトコル パックの情報が表示されています。

```
Router# show ip nbar protocol-pack active
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

次の **show ip nbar protocol-pack** コマンドからの出力例では、アクティブなプロトコル パックの詳細情報が表示されています。

```
Router# show ip nbar protocol-pack active detail
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

```
Protocols:
base                                Mv: 4
ftp                                 Mv: 5
http                                Mv: 18
static                              Mv: 6
socks                               Mv: 2
nntp                                Mv: 2
tftp                                Mv: 2
exchange                            Mv: 3
vdolive                             Mv: 1
sqlnet                              Mv: 2
netshow                             Mv: 3
sunrpc                              Mv: 3
streamwork                          Mv: 2
citrix                              Mv: 11
fasttrack                           Mv: 3
gnutella                            Mv: 7
kazaa2                              Mv: 11
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *30 : show ip nbar protocol-pack* フィールドの説明

フィールド	説明
Name	プロトコル パックの名前です。
Version	プロトコル パックのバージョンです。
Publisher	プロトコル パックのパブリッシャの名前です。
Protocols	プロトコルパックに含まれるプロトコルのリストです。

関連コマンド

コマンド	説明
defaultipnbarprotocol-pack	プロトコル パックのベース バージョンをロードし、ロード済みのその他のすべてのプロトコル パックを削除します。
ipnbarprotocol-pack	プロトコル パックをロードします。

show ip nbar resources flow

Network-Based Application Recognition（NBAR）の現在の設定およびリソースの使用率を表示するには、特権 EXEC モードで **showipnbarresourcesflow** コマンドを使用します。

show ip nbar resources flow

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.4S	このコマンドが導入されました。

例

次は、**showipnbarresourcesflow** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Router# show ip nbar resources flow

NBAR flow statistics
        Maximum no of sessions allowed : 3500000
        Maximum memory usage allowed   : 734003 KBytes
        Active sessions                : 3499950
        Active memory usage            : 665364 KBytes
        Peak session                   : 3499950
        Peak memory usage              : 672396 KBytes
```

関連コマンド

コマンド	説明
ipnbarresourcesflowmax-session	最大フローセッションが、フローテーブルで使用できるように設定します。

show ip nbar statistics

Network-Based Application Recognition（NBAR）が動作するデバイスの障害統計情報、フローごとのパケット数、および異なるタイプの分類を表示するには、特権 EXEC モードで **show ip nbar statistics** コマンドを使用します。

show ip nbar statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

例

次は、**show ip nbar statistics** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar statistics

Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
```

show ip nbar trace

データ プレーンのパケットが通過するパスを表示するには、特権 EXEC モードで **show ip nbar trace** コマンドを使用します。

show ip nbar trace{**detail**|**summary**}[{**config**}]

構文の説明

detail	分類トレースの詳細を表示します。
summary	分類トレースの概要を表示します。
config	（任意）状態グラフのトレースの設定情報を表示します。

コマンド デフォルト

パケットが通過するすべてのパスに関する情報が表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.2(4)M	このコマンドが導入されました。

使用上のガイドライン

トレースおよびサマリー デバッグを有効にする必要があります。

例

次は、**show ip nbar trace summary** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar trace summary

Classification: 76, flag: 163
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE

Classification: 1, flag: 160
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE
```

次は、**show ip nbar trace detail** コマンドの出力例です。出力にはフィールドの説明も表示されます。

```
Device# show ip nbar trace detail

Graph Id 1
Classification: 82, flag: 163
Packet No: 1
```

```
String: Searching Source V4 WKP
String: Searching Destination V4 WKP
String: Entering loop core from Heuristic Regex
State Node:http-verify-heuristic-entry-point-get
State Node:http-verify-heuristic-entry-point-get
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:youtube-found-url
State Node:http-check-url-fe
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-end-of-request-check
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-headers-parser
State Node:HTTP-request-headers-parser
Graph Id 1
```

関連コマンド

コマンド	説明
clear ip nbar trace summary	分類モジュールをクリアします。
debug ip nbar config	NBAR の有効化および無効化で設定するすべてのコマンドのデバッグを有効にします。

show ip nbar unclassified-port-stats

未分類パケットの Network-Based Application Recognition（NBAR）ポート統計情報を表示するには、特権 EXEC モードで **showipnbarunclassified-port-stats** コマンドを使用します。

show ip nbar unclassified-port-stats [{*top-talkers*|**ip** [{*protocol-number* [*number-protocols*]|**top** *top-talkers*}]|[{**tcp**|**udp**}] [{*port-number* [*number-ports*]|**top** *top-talkers*|**bottom** *bottom-talkers*}]}]

構文の説明

top-talkers	（任意）表示するトップ トーカーの数です。
ip	（任意）TCP 以外/UDP 以外の未分類パケットのポート統計情報を表示します。
protocol-number	（任意）開始 IP プロトコル番号です。
number-protocols	（任意）表示するプロトコルの数です。
top	（任意）top-n が表示されることを示します。top-n はアクティブな NBAR サポート プロトコルのなかの上位プロトコル数です。n は表示するプロトコル数を表します。たとえば、top-n 3 と入力すると、アクティブな NBAR サポート プロトコルの上位 3 つが表示されます。
tcp	（任意）未分類 TCP パケットのポート統計情報を表示します。
udp	（任意）未分類 UDP パケットのポート統計情報を表示します。
port-number	（任意）開始 TCP または UDP ポート番号です。
number-ports	（任意）表示するポートの数です。
bottom	（任意）bottom-n が表示されることを示します。bottom-n はアクティブな NBAR サポート プロトコルのなかの下位プロトコル数です。n は表示するプロトコル数を表します。たとえば、bottom-n 3 と入力すると、アクティブな NBAR サポート プロトコルの下位 3 つが表示されます。
bottom-talkers	（任意）表示するボトム トーカーの数です。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(5)XE2	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。

リリース	変更箇所
12.1(13)E	このコマンドが、FlexWAN モジュール非搭載の Cisco Catalyst 6000 ファミリ スイッチに実装されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(18)ZYA	このコマンドが、Cisco IOS Release 12.2(18)ZYA に統合されました。このコマンドが変更され、VLAN に関する情報表示（必要に応じて）、およびレイヤ 2 とレイヤ 3 両方の EtherChannel のサポート（Cisco Catalyst スイッチのみ）が追加されました。

使用上のガイドライン

デフォルトでは、NBAR未分類メカニズムは無効です。ルータを設定してパケットが着信するポートのトラッキングを開始するには、**debugipnbarunclassified-port-stats** コマンドを使用します。次に **showipnbarunclassified-port-stats** コマンドを使用して、収集した情報を確認します。

例

次は、**showipnbarunclassified-port-stats** コマンドの出力例です。

```
Router# show ip nbar unclassified-port-stats

-tcp-
      80/tcp:48
    1443/tcp:3
    1423/tcp:2
    1424/tcp:2
    1425/tcp:2
-udp-
    1985/udp:158
    1029/udp:13
     496/udp:4
    1445/udp:3
    1449/udp:2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *31 : show ip nbar unclassified-port-stats* フィールドの説明

フィールド	説明
-tcp-	TCP プロトコルです。
80/tcp:48	80 はポート番号、tcp はプロトコル、48 はパケット数を示します。
-udp-	UDP プロトコルです。
1985/udp:158	1855 はポート番号、udp はプロトコル、158 はパケット数を示します。

出力には、ポート番号、プロトコル、およびパケット数が表示されます。たとえば、80/tcp:48 において 80 はポート番号、tcp はプロトコル、48 はパケット数を示します。

関連コマンド

コマンド	説明
ipnbarcustom	NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポートアプリケーションを分類および監視できます。または、NBARはサポートしていないスタティック ポート トラフィックを分類できるようになります。
ipnbarpdlm	シスコが提供する PDLM によって、NBAR が認識するプロトコルのリストを拡張および強化します。
ipnbarport-map	ウェルノウン ポート番号以外のポート番号を使用して、プロトコルまたはプロトコル名を検索するように NBAR を設定します。
ipnbarprotocol-discovery	特定のインターフェイス上で NBAR が認識するすべてのプロトコルについて、トラフィックを検出するように NBAR を設定します。
ipnbarresourcesprotocol	プロトコル ベースで、NBAR フロー リンク テーブルの有効期限を設定します。
ipnbarresourcessystem	システム全体で、NBAR フローリンク テーブルの有効期限とメモリ要件を設定します。
showipnbarpdlm	NBAR で使用されている PDLM を表示します。
showipnbarport-map	NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。
showipnbarprotocol-discovery	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。
showipnbarversion	Cisco IOS リリースの NBAR ソフトウェア バージョンまたは Cisco IOS ルータの NBAR PDLM のバージョンに関する情報を表示します。

show ip nbar version

Cisco IOS リリースの Network-Based Application Recognition（NBAR）ソフトウェア バージョンまたは Cisco IOS ルータの NBAR Packet Description Language Module（PDLM）のバージョンに関する情報を表示するには、特権 EXEC モードで **showipnbarversion** コマンドを使用します。
rivilegedEXEC

show ip nbar version [*PDLM-name*]

構文の説明

PDLM-name	（任意）情報を表示する特定の PDLM の名前を指定します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.3(4)T	このコマンドが導入されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX1	このコマンドが、Cisco IOS Release 12.2(17a)SX1 に統合されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。

使用上のガイドライン

showipnbarversion コマンドは、最初の NBAR リリース後に NBAR に追加されたすべてのプロトコル（ユーザが Cisco.com から PDLM をダウンロードせずに Cisco IOS ソフトウェアに追加されたプロトコルを含む）を PDLM として処理します。ユーザが Cisco.com からダウンロードし NBAR に追加した PDLM も、**showipnbarversion** コマンドを入力すると、表示されます。

NBAR を使用すると、NBAR 内の各種の要素にバージョン番号が割り当てられます。これらのバージョン番号は、PDLM をダウンロードするときに必要です。PDLM（これもバージョン付けされます）は、PDLM バージョン番号が Cisco IOS ソフトウェアの NBAR バージョン番号と互換性がある場合、特定の Cisco IOS リリースの NBAR のみにダウンロードできます。

次の NBAR 関連のバージョン情報が入手できます。

- NBAR Software Version：現在のバージョンの Cisco IOS ソフトウェアで動作している NBAR ソフトウェアのバージョン。
- Resident Module Version：NBAR がサポートする PDLM プロトコルのバージョン。

次のバージョン番号が PDLM に保持されています。

- NBAR Software Version：この PDLM をロードする場合に必要な NBAR ソフトウェアの最小バージョン。

showipnbarversion コマンドを使用すると、Cisco IOS ソフトウェアにロード済みの PDLM のバージョン情報を表示できます。

例

次に、show ip nbar version コマンドの出力例を示します。

```
Router# show ip nbar version
NBAR software version:  3
1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
4   static-port          Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 5
14  fasttrack            Mv: 2
15  gnutella             Mv: 1
16 kazaa                Mv: 6, Nv: 3; slot1:kazaa2_vers.pdlm
17 custom-protocols     Mv: 1
18 rtsp                 Mv: 1
19  rtp                  Mv: 2
20  mgcp                 Mv: 1
21  skinny               Mv: 1
22 h323                 Mv: 1
23 sip                  Mv: 1
24 rtcp                 Mv: 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *32 : show ip nbar version* コマンドのフィールドの説明

フィールド	説明
NBAR Software Version	現在の Cisco IOS ソフトウェアで動作している NBAR ソフトウェア バージョン。この例では、Cisco IOS ソフトウェアの現在のバージョンで動作している NBAR ソフトウェアは、バージョン 3 です。
Mv	Resident Module Version。Resident Module Version は NBAR がサポートする PDLM プロトコルのバージョンなので、プロトコルによって異なります。たとえば、TFTP の Resident Module Version は 1 です。
Nv	非ネイティブ PDLM のロードに必要な NBAR ソフトウェアの最小バージョン。この番号は、Kazaa PDLM（プロトコル 17）など、ルータにロードされている非ネイティブ PDLM にのみ使用できます。この場合、Nv バージョンは 3 です。

同じネットワーク設定の場合、次の例は、**showipnbarversion** CLI で PDLM の特定のプロトコルを指定して出力します。

```
Router# show ip nbar version http
http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
```

関連コマンド

コマンド	説明
ipnbarpdlm	NBAR でサポートするプロトコルを追加するために、ルータへ PDLM をダウンロードします。

show ip rsvp

リソース予約プロトコル（RSVP）に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvp** コマンドを使用します。

show ip rsvp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.2(13)T	このコマンドが変更されました。**listeners** キーワードおよび **policy** キーワードが追加され、このコマンドはキーワードや引数が入力されていないときには RSVP グローバル設定を表示するように変更されました。
12.2(33)SRB	このコマンドが変更されました。コマンド出力が高速ローカル修復（FLR）情報を表示するように変更されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.2(33)SRC	このコマンドが変更されました。コマンド出力は、次の情報を表示するように変更されました。 • RSVP Quality of Service（QoS）およびマルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）情報。 • RSVP 集約情報。
15.0(1)M	このコマンドが変更されました。 [**atm-peak-rate-limit** | **counters** | **host** | **installed** | **interface** | **listeners** | **neighbor** | **policy** | **precedence** | **request** | **reservation** | **sbm** | **sender** | **signalling** | **tos**] 構文は、コマンドから削除されました。キーワード オプションは、次の個別のコマンド ファイルで表されます。show ip rsvp **atm-peak-rate-limit,**show ip rsvp **counters,**show ip rsvp **host,**show ip rsvp installed、show ip rsvp interface、show ip rsvp listeners、show ip rsvp neighbor、show ip rsvp policy、show ip rsvp precedence、show ip rsvp request、show ip rsvp reservation、show ip rsvp sbm、show ip rsvp sender、show ip rsvp signalling、show ip rsvp tos の各コマンドです。

リリース	変更箇所
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

例

次に、**showiprsvp** コマンドの出力例を示します。

```
Router# show ip rsvp
RSVP: enabled (on 1 interface(s))
   RSVP QoS signalling enabled
   MPLS/TE signalling enabled
Signalling:
   Refresh interval (msec): 30000
   Refresh misses: 4
Rate Limiting: enabled
   Burst: 8
   Limit: 37
   Maxsize: 2000
   Period (msec): 20
   Max rate (msgs/sec): 400
Refresh Reduction: disabled
   ACK delay (msec): 250
   Initial retransmit delay (msec): 1000
   Local epoch: 0xCE969B
   Message IDs: in use 0, total allocated 0, total freed 0
Neighbors: 0
   Raw IP encap: 0  UDP encap: 0  Raw IP, UDP encap: 0
RFC 3175 Aggregation: Enabled
   Level: 1
   Default QoS service: Controlled-Load
   Router ID: 10.22.22.22
   Number of signaled aggregate reservations:     0
   Number of signaled E2E reservation:            0
   Number of configured map commands:             0
   Number of configured reservation commands:     0
Hello:
   RSVP Hello for Fast-Reroute/Reroute: Disabled
     Statistics: Disabled
   BFD for Fast-Reroute/Reroute: Disabled
   RSVP Hello for Graceful Restart: Disabled
Graceful Restart: Disabled
   Refresh interval: 10000 msecs
   Refresh misses: 4
   DSCP: 0x30
   Advertised restart time: 5 msecs
   Advertised recovery time: 0 msecs
   Maximum wait for recovery: 3600000 msecs
Fast-Reroute:
   PSBs w/ Local protection desired
     Yes: 0
     No:  0
Fast Local Repair: enabled
   Max repair rate (paths/sec): 400
   Max processed   (paths/run): 1000
Local policy:
COPS:
Generic policy settings:
     Default policy: Accept all
     Preemption:     Disabled
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *33 : show ip rsvp* フィールドの説明

フィールド	説明
RSVP	RSVP、QoS、および MPLS TE シグナリングの状態。値は、[有効（アクティブ化）（enabled (activated)）] または [無効（非アクティブ化）（disabled (deactivated)）] です。 （注） このフィールドが無効になるのは、RIB に登録するときに内部エラーが発生した場合のみです。
Signalling	有効な RSVP シグナリング パラメータは次のとおりです。 • [更新間隔（Refresh interval）] : RSVP 状態ごとの更新送信間の時間（ミリ秒（ms））。 • [更新ミス（Refresh misses）] : RSVP が状態の期限切れと見なし、ティアダウンするまでに、未受信の可能性がある連続した更新メッセージの数。
Rate Limiting: enabled or disabled	有効な RSVP レート制限パラメータは次のとおりです。 • [バースト（Burst）] : インターバル中に隣接ルータへの送信が許可された RSVP メッセージの最大数。 • [制限（Limit）] : キュー間隔あたりの最大送信 RSVP メッセージ数。 • [最大サイズ（Maxsize）] : メッセージ キューの最大サイズ（バイト）。 • [期間（Period）] : 間隔（時間枠）の長さ（ミリ秒（ms））。 • [最大レート（Max rate）] : 送信が許可された 1 秒あたりのメッセージの最大数。
Refresh Reduction: enabled or disabled	有効な RSVP 更新削減パラメータは次のとおりです。 • [ACK 遅延（ミリ秒）（ACK delay (msec)）] : 受信側ルータが確認応答（ACK）を送信するまでの期間（ミリ秒）。 • [初期再送信遅延（ミリ秒）（Initial retransmit delay (msec)）] : ルータがメッセージを再送信するまでの期間（ミリ秒）。 • [ローカル エポック（Local epoch）] : RSVP プロセス識別子（ID）。ノードが再起動するか、または RSVP プロセスが再実行されるたびにランダムに生成されます。 • [メッセージ ID（Message IDs）] : 使用中のメッセージ ID の数、割り当て済みの合計数、および使用可能な（解放された）合計数。

フィールド	説明
Neighbors	使用中のネイバーの合計数およびカプセル化の種類。RSVP や User Datagram Protocol（UDP）などがあります。
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。
show ip rsvp Field Descriptions	予約の集約レベル。一般的な値は次のとおりです。 • 0：エンドツーエンド（E2E）予約。 • 1：集約予約。 レベル x 予約を集約して、レベル *x* +1 で予約を形成できます。
Default QoS service	設定された QoS のタイプ。値は次のとおりです。 • Controlled-Load：アプリケーションはその要件を満足する帯域幅を予約できます。たとえば、重み付けランダム早期検出（WRED）を使用した RSVP では、このタイプのサービスが提供されます。 • Guaranteed-Rate：アプリケーションには、輻輳発生時でも低遅延かつ高スループットが保証されます。たとえば、RSVP を使用した重み付け均等化キューイング（WFQ）では、このタイプのサービスが提供されます。
Number of signaled aggregate reservations	シグナル集約予約の累積数。
Number of signaled E2E reservations	シグナル E2E 予約の累積数。
Number of configured map commands	設定された map コマンドの累積数。
Number of configured reservation commands	設定された reservation コマンドの累積数。
Hello	後続のフィールドは、hello が有効または無効になっているプロセスについて説明したものです。選択肢は、Fast Reroute、再ルーティング（hello ステート タイマー）、双方向フォワーディング検出（BFD）、およびグレースフル リスタート（リスタート機能を備えたノードの場合）です。

フィールド	説明
Statistics	hello 統計のステータス。有効な値は、次のとおりです。 • Enabled：統計が設定されています。helloパケットは、helloインプットキューに到着すると、その処理にかかる時間を記録する目的でタイムスタンプが付けられます。 • Disabled：hello 統計は設定されていません。 • [シャットダウン（Shutdown）]：hello 統計は設定されていますが、動作していません。インプットキューが長すぎです（つまり、10,000を超えるパケットがキュー内に滞留しています）。
Graceful Restart: Enabled or Disabled	有効な RSVP グレースフル リスタート パラメータは次のとおりです。 • [更新間隔（Refresh interval）]：ノードがそのネイバーに hello メッセージを送信する頻度（ミリ秒（ms））。 • [更新ミス（Refresh misses）]：ネイバー ダウン イベントをトリガーしてステートフル スイッチオーバー（SSO）プロシージャを起動させた、未受信の hello メッセージの数。 • [DSCP]：hello メッセージの IP ヘッダーにある DiffServ コード ポイント（DSCP）値。 • [再起動時刻のアドバタイズ（Advertised restart time）]：障害発生後に送信者がRSVP トラフィック エンジニアリング コンポーネントを再起動し、helloメッセージを交換するのに必要な時間（ミリ秒）。 • [リカバリ時間のアドバタイズ（Advertised recovery time）]：リカバリしているノードがそのネイバー ルータに対し、SSO 後に RSVP またはMPLS フォワーディング ステートの再同期を求める期限（ミリ秒）。ゼロ値は、RSVP または MPLS 転送状態が SSO 後に保持されないことを示します。 • [リカバリの最大待機（Maximum wait for recovery）]：ルータがネイバーのリカバリを待機する最大時間（ミリ秒）。
Fast-Reroute	有効な Fast Reroute パラメータは次のとおりです。 • [必要なローカル保護を備えたPSB（PSBs w/ Local protection desired）]：[はい（Yes）] にすると、トンネルが停止したときに、パケット フローが中断していなければ、パス ステート ブロック（PSB）が再ルーティングされます。PSB が再ルーティングされないという意味ではありません。

フィールド	説明
Fast Local Repair: enabled or disabled	有効な高速ローカル修復パラメータは次のとおりです。 • [最大修復レート（パス/秒）（Max repair rate (paths/sec)）]：最大修復レート（1 秒あたりのパス数）。 • [最大処理（パス/実行）（Max processed (paths/run)）]：処理する最大通知要素（1 回の実行あたりのパス数）。
Local policy	現在設定されているローカル ポリシー。
COPS	現在有効な Common Open Policy Service（COPS）。
Generic policy settings	COPS またはローカル ポリシーに固有ではないポリシー設定。 • Default policy：「Accept all」は、すべての RSVP メッセージが受け入れられ、転送されることを意味します。[すべて拒否（Reject all）] とは、すべての RSVP メッセージを拒否するということです。 • [プリエンプション（Preemption）]：[無効（Disabled）] にすると、RSVP は予約の優先順位付けとそれに応じた帯域幅の割り当てを行いません。[有効（Enabled）] にすると、RSVP は予約に優先順位を付けて、最も優先順位の高い予約により多くの帯域幅を割り当てます。

関連コマンド

Command	Description
debugiprsvp	RSVP カテゴリのデバッグ メッセージを表示します。
showiprsvpatm-peak-rate-limit	あるインターフェイスまたはすべてのインターフェイスに対して設定された現在のピーク レート制限を表示します。
showiprsvpcounters	各インターフェイスで送受信した RSVP メッセージの数を表示します。
showiprsvphost	RSVP ホストに固有の情報を表示します。
showiprsvpinstalled	RSVP 関連のインストールされているフィルタと対応する帯域幅情報を表示します。
showiprsvpinterface	RSVP が有効になっているインターフェイスの情報を表示します。
show iprsvplisteners	指定したポートまたはプロトコルの RSVP リスナーを表示します。
showiprsvpneighbor	現在の RSVP ネイバーに関する情報を表示します。

Command	Description
showiprsvppolicy	現在設定されている RSVP ポリシーに関する情報を表示します。
showiprsvpprecedence	RSVP が有効になっているインターフェイスに関する IP プレシデンス情報を表示します。
showiprsvprequest	現在の RSVP 関連の要求情報を表示します。
showiprsvpreservation	現在の RSVP 関連の受信側情報を表示します。
showiprsvpsbm	RSVP 対応のインターフェイスに関する SBM 設定情報を表示します。
showiprsvpsender	RSVP PATH 関連の送信側情報を表示します。
showiprsvpsignalling	RSVP シグナリング情報を表示します。
showiprsvptos	RSVP が有効になっているインターフェイスに関する IP ToS 情報を表示します。

show ip rsvp aggregation ip

リソース予約プロトコル（RSVP）の要約集約情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpaggregationip** コマンドを使用します。

show ip rsvp aggregation ip [{**endpoints [detail]** [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**|**deaggregator**}]|**interface** [*if-name*]|**map** [**dscp** *value*]|**reservation** [**dscp** *value* [**aggregator** *ip-address*]]}]

構文の説明

endpoints	（任意）集約領域のアグリゲータとデアグリゲータを指定します。
interface *if-name*	（任意）インターフェイス名を指定します。
map	（任意）マップ コンフィギュレーション ルールを表示します。
dscp *value*	（任意）**map** キーワードに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
reservation	（任意）予約設定を表示します。
dscp *value*	（任意）**reservation** キーワードに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
aggregator *ip-address*	（任意）アグリゲータの IP アドレスを指定します。

コマンド デフォルト

showiprsvpaggregationip コマンドをオプション キーワードを指定せずに入力すると、すべての集約予約の概要情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

集約、マップ、および予約の設定の数を含む、集約に関する概要情報を表示するには、**showiprsvpaggregationip** コマンドを使用します。

例

show ip rsvp aggregation ip コマンドの出力例

次は、**showiprsvpaggregationip** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip
RFC 3175 Aggregation:  Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Number of signaled aggregate reservations:  2
  Number of signaled E2E reservations:        8
  Number of configured map commands:          4
  Number of configured reservation commands:  1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *34 : show ip rsvp aggregation ip* フィールドの説明

フィールド	説明
RFC 3175 Aggregation	RFC 3175（*AggregationofRSVPforIPv4andIPv6Reservations*）に定義された集約の状態。値は次のとおりです。 • Enabled：アクティブ。 • Disabled：非アクティブ。
Level	予約の集約レベル。一般的な値は次のとおりです。 • 0：エンドツーエンド（E2E）予約。 • 1：集約予約。 （注） レベル x 予約を集約すると、次の高いレベルの予約を作成できます。たとえばレベル x+1 などです。

フィールド	説明
Default QoS service	設定されているサービス品質（QoS）のタイプ。値は次のとおりです。 • Controlled-Load：アプリケーションはその要件を満足する帯域幅を予約できます。たとえば、重み付けランダム早期検出（WRED）を使用した RSVP では、このタイプのサービスが提供されます。 • Guaranteed-Rate：アプリケーションには、輻輳発生時でも低遅延かつ高スループットが保証されます。たとえば、RSVP を使用した重み付け均等化キューイング（WFQ）では、このタイプのサービスが提供されます。
Number of signaled aggregate reservations	シグナル集約予約の累積数。
Number of signaled E2E reservations	シグナル E2E 予約の累積数。
Number of configured map commands	設定された map コマンドの累積数。
Number of configured reservation commands	設定された reservation コマンドの累積数。

show ip rsvp aggregation ip interface の出力例

次は、**showiprsvpaggregationipinterface** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip interface
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
Serial2/0            exterior
Serial3/0            exterior
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *35 : show ip rsvp aggregation ip interface* フィールドの説明

フィールド	説明
Interface Name	インターフェイスの名前および番号。
Role	ルータのインターフェイスの設定。値は、interior または exterior。

次は、インターフェイスを指定した場合の **showiprsvpaggregationipinterface** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip interface Ethernet0/0
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
```

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータでRSVP集約を有効にします。

show ip rsvp aggregation ip endpoints

アグリゲータおよびデアグリゲータ ルータに関するリソース予約プロトコル（RSVP）情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpaggregationipendpoints** コマンドを使用します。

show ip rsvp aggregation ip endpoints [detail] [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**|**deaggregator**}]

構文の説明

detail	（任意）アグリゲータおよびデアグリゲータに関する追加情報を表示します。
dscp *value*	（任意）アグリゲータおよびデアグリゲータ ルータに DiffServ コード ポイント（DSCP）を指定します。有効な値は次のとおりです。 • 0 ～ 63：DSCP の数値。デフォルト値は 0 です。 • af11 ～ af43：相対的優先転送（AF）DSCP 値。 • cs1 ～ cs7：タイプ オブ サービス（ToS）プレシデンス値。 • default：デフォルト DSCP 値。 • ef：Expedited Forwarding（EF; 完全優先転送）DSCP 値。
remote	（任意）リモート デアグリゲータを指定します。
ip-address	リモート デアグリゲータの IP アドレスです。
role	（任意）集約領域でのルータの位置を指定します。
aggregator	（任意）集約領域の始点のルータを指定します。
deaggregator	（任意）集約領域の終点のルータを指定します。

コマンド デフォルト

showiprsvpaggregationipendpoints コマンドをオプション キーワードを指定せずに入力すると、すべての集約予約の情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(33)SRC	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

アグリゲータおよびデアグリゲータ ルータにおける次の出力のいずれかを表示するには、**showiprsvpaggregationipendpoints** コマンドを使用します。

- すべての集約予約。
- ノードがアグリゲータのすべての集約予約。
- ノードがデアグリゲータのすべての集約予約。
- リモート ノードが IP アドレスで指定されるすべての集約予約。
- 指定した DSCP のすべての集約予約。
- 上記オプションの組み合わせ。ノードがアグリゲータで、リモート ノードが IP アドレスで指定される、DSCP 指定のすべての集約などがあります。
- 詳細情報付きの上記オプションのいずれか。

例

次は、**showiprsvpaggregationipendpointsdetail** コマンドの出力例です。

```
Router# show ip rsvp aggregation ip endpoints detail
Role  DSCP Aggregator      Deaggregator    State  Rate    Used    QBM PoolID
----- ---- --------------- --------------- ------ ------- ------- ----------
Agg   46   10.3.3.3         10.4.4.4         ESTABL 100K    100K    0x00000003
   Aggregate Reservation for the following E2E Flows (PSBs):
To             From          Pro DPort Sport  Prev Hop       I/F      BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    100K
   Aggregate Reservation for the following E2E Flows (RSBs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.4.4.4       Se2/0    FF RATE 100K
   Aggregate Reservation for the following E2E Flows (Reqs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    FF RATE 100K
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *36 : show ip rsvp aggregation ip endpoints detail* フィールドの説明

フィールド	説明
Role	ルータの機能。値は、aggregator または deaggregator です。
DSCP	DSCP 値。
Aggregator	アグリゲータの IP アドレスです。
Deaggregator	デアグリゲータの IP アドレスです。

フィールド	説明
State	予約の状態です。各集約予約は、次のいずれかの状態になります。 • PATH_WAIT：デアグリゲータのみで有効。デアグリゲータの集約予約が、必要な新しい集約を要求する PATHERROR メッセージをデアグリゲータが送信後に、この状態になります。 • RESV_WAIT：アグリゲータのみで有効。アグリゲータの集約予約が、集約予約の PATH メッセージをアグリゲータが送信後に、この状態になります。 • RESVCONF_WAIT：デアグリゲータのみで有効。デアグリゲータの集約予約が、集約予約の RESV メッセージをデアグリゲータが送信後に、この状態になります。 • ESTABLISHED：アグリゲータおよびデアグリゲータ両方で有効。アグリゲータは、RESVCONF メッセージを送信後に、この状態になります。デアグリゲータは、集約予約の RESVCONF メッセージの受信後に、この状態になります。 • SHUT_DELAY：アグリゲータおよびデアグリゲータ両方で有効。アグリゲータおよびデアグリゲータは、最後のエンドツーエンド（E2E）予約が削除された後に、この状態になります。
Rate	ビット/秒（bps）単位での割り当てられた帯域幅です。
Used	ビット/秒（bps）単位で使用された帯域幅量です。
QBM Pool ID	予約の Quality of Service（QoS）帯域幅マネージャ（QBM）ID です。
Aggregate Reservation for the following E2E Flows	予約に関する情報： PSB：パス ステート ブロック。PATH メッセージ ダウンストリームの転送に使用するデータが含まれます。 RSB：予約ステートブロック。着信RESV メッセージのデータが含まれます。 Reqs：要求。PATH メッセージを送信したノードへ RESV メッセージ アップストリームを転送するために必要なデータが含まれます。
To	受信者の IP アドレス。
From	送信元の IP アドレス。
Pro	プロトコル コード。コードは、TCP、User Datagram Protocol（UDP）などの IP プロトコルを示します。
DPort	宛先ポート番号。

フィールド	説明
Sport	送信元ポート番号です。
Prev Hop or Next Hop	前のホップまたはネクスト ホップの IP アドレスです。
I/F	前のホップまたは ネクスト ホップのインターフェイスです。
Fi	フィルタです（Wildcard Filter、Shared-Explicit、または Fixed-Filter）。
Serv	サービスです（RATE または LOAD）。
BPS	ビット/秒（bps）単位での集約予約で使用された帯域幅です。

関連コマンド

コマンド	説明
iprsvpaggregationip	ルータでRSVP集約を有効にします。

show ip rsvp atm-peak-rate-limit

インターフェイスまたはすべてのインターフェイス（該当する場合）に設定された現在のピーク レート制限を表示するには、EXEC モードで **showiprsvpatm-peak-rate-limit** コマンドを使用します。

show ip rsvp atm-peak-rate-limit [*interface-type interface-number*]

構文の説明

interface-type interface-number	（任意）インターフェイス タイプおよびインターフェイス番号。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

showiprsvpatm-peak-rate-limit コマンドは、省略形として次の表記を使用して、設定済みのピーク レートを表示します。

- キロバイトは、K bytes と表示されます。たとえば、1200 キロバイトは 1200K bytes と表示されます。
- 1000 キロバイトは、1M bytes と表示されます。

インターフェイス名が指定されないと、すべてのリソース予約プロトコル（RSVP）対応インターフェイスの設定済みピーク レートが表示されます。

例

次の例は、**showiprsvpatm-peak-rate-limit** コマンドの結果です。この例では、**iprsvpatm-peak-rate-limit** コマンドを使用して ATM サブインターフェイス 2/0/0.1 の予約ピーク レート制限が 100 KB に設定済みです。

次は、**showiprsvpatm-peak-rate-limit** コマンドの出力例です。*interface-type interface-number* 引数を使用しています。

```
Router# show ip rsvp atm-peak-rate-limit atm2/0/0.1
RSVP: Peak rate limit for ATM2/0/0.1 is 100K bytes
```

次は、インターフェイス名を指定しない場合の **showiprsvpatm-peak-rate-limit** コマンドの出力例です。

```
Router# show ip rsvp atm-peak-rate-limit


Interface name         Peak rate limit
Ethernet0/1/1         not set
```

```
ATM2/0/0              not set
ATM2/0/0.1            100K
Router# show ip rsvp atm-peak-rate-limit
Interface name       Peak rate limit
Ethernet0/1          not set
ATM2/1/0             1M
ATM2/1/0.10          not set
ATM2/1/0.11          not set
ATM2/1/0.12          not set
```

関連コマンド

Command	Description
iprsvpatm-peak-rate-limit	現在のインターフェイスまたはそのサブインターフェイス上に確立された、すべての新しく作成されたRSVP SVCの予約のピーク セルレートに制限を設定します。

show ip rsvp authentication

リソース予約プロトコル（RSVP）が他の RSVP ネイバーと確立したセキュリティ アソシエーションを表示するには、ユーザ EXEC または特権 EXEC モードで show **iprsvpauthentication** コマンドを使用します。

show ip rsvp authentication [detail] [from {*ip-addresshostname*}] [**to** {*ip-addresshostname*}]

構文の説明

detail	（任意）RSVPセキュリティ アソシエーションの追加情報を表示します。
from	（任意）セキュリティ アソシエーションの始点を指定します。
to	（任意）セキュリティ アソシエーションの終点を指定します。
ip-address	（任意）IP アドレスを指定したネイバーに関する情報。
hostname	（任意）特定のホストに関する情報。

コマンド モード

ユーザ EXEC（<）
特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.2(15)T	このコマンドが導入されました。
12.0(29)S	オプションの **from** および **to** キーワードが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

RSVP が他の RSVP ネイバーと確立したセキュリティ アソシエーションを表示するには、show ip rsvp authentication コマンドを使用します。すべてのセキュリティ アソシエーションを表示するか、特定の RSVP ネイバーの IP アドレスまたはホスト名を指定できます。表示サイズには制限があります。

ip-address と *hostname* 引数の違いは、IP アドレスまたは名前でネイバーを指定することです。

例

次に、**showiprsvpauthenticationcommand** の出力例を示します。

```
Router# show ip rsvp authentication
Codes: S - static, D - dynamic, N - neighbor, I -interface, C - chain
From            To              I/F      Mode    Key-Source Key-ID       Code
192.168.102.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
```

```
192.168.106.1   192.168.106.2   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.2   192.168.104.1   AT1/0.1  Receive RSVPKey    1            DNC
192.168.106.2   192.168.106.1   AT1/0.1  Receive RSVPKey    1            DNC
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *37 : show ip rsvp authentication* フィールドの説明

フィールド	説明
Codes	キーは、static（手動設定）または dynamic（ACL 単位キーから作成、または Kerberos などのキー管理サーバから取得）です。Cisco IOS ソフトウェアでは、キー管理サーバからのダイナミック キーは現在サポートされていません。このフィールドに文字列 per-neighbor が含まれている場合、セキュリティ アソシエーションではネイバー単位キーが使用されています。このフィールドに文字列 per-interface が含まれている場合、セキュリティ アソシエーションではインターフェイス単位キーが使用されています。このフィールドに文字列 chain が含まれている場合、セキュリティアソシエーションのキーは Key Source に指定されたキー チェーンから取得されます。
From	セキュリティ アソシエーションの始点。
To	セキュリティ アソシエーションの終点。
I/F	セキュリティアソシエーションが保持されているインターフェイスの名前および番号。
Mode	特定の RSVP ネイバーの RSVP メッセージを送受信するために保持されている個別のアソシエーション。有効な値は、**Send** または **Receive** です。
Key-Source	キーが設定されている場所を示します。
Key-ID	IP アドレスと組み合わせて、セキュリティアソシエーションを一意に識別するための文字列。per-interface **iprsvpauthenticationkey** コマンドを使用すれば、Cisco IOS ソフトウェアで自動的にキー ID が生成されますが、ネイバー単位またはインターフェイス単位 RSVP キーのキー チェーンを使用する場合、Cisco IOS ソフトウェアでキー ID が設定されます。キー ID は、他の RSVP プラットフォームで設定可能です。送信元が送信した RSVP 認証済みメッセージすべてにキー ID が割り当てられ、すべての受信者がこれを保存します。 （注） **KeyExpired** ：このフィールド内では、このネイバーに使用可能なキーがすべて期限切れになっていることを意味します。
コード（Code）	使用するキー ID のタイプを示します。

次は、s**howiprsvpauthentication** detail コマンドの出力例です。

```
Router# show ip rsvp authentication detail
From:                   192.168.102.1
```

```
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000411
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:17:08
Challenge:              Supported
Window size:            1
Last seq # sent:        14167519095569779135
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 0400040F
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:22:06
Challenge:              Supported
Window size:            1
Last seq # sent:        14167520384059965440
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 02000404
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:16:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167518979605659648
From:                   192.168.106.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000408
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:11:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167517691115473376
From:                   192.168.106.1
```

```
To:                     192.168.106.2
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 8D00040E
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:29
Challenge:              Supported
Window size:            1
Last seq # sent:        14167808344437293057
From:                   192.168.106.2
To:                     192.168.104.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 CD00040A
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783626
From:                   192.168.106.2
To:                     192.168.106.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 C0000412
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783619
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *38 : show ip rsvp authentication detail* フィールドの説明

フィールド	説明
From	セキュリティ アソシエーションの始点。
To	セキュリティ アソシエーションの終点。
Neighbor	セキュリティ アソシエーションが保持されている RSVP ネイバーの IP アドレス。

フィールド	説明
Interface	セキュリティ アソシエーションが保持されているインターフェイスの名前および番号。
Mode	特定の RSVP ネイバーの RSVP メッセージを送受信するために保持されている個別のアソシエーション。有効な値は、Send または Receive です。
Key ID	IP アドレスと組み合わせて、セキュリティ アソシエーションを一意に識別するための文字列。per-interface **iprsvpauthenticationkey** コマンドを使用すれば、Cisco IOS ソフトウェアで自動的にキー ID が生成されますが、ネイバー単位またはインターフェイス単位 RSVP キーのキー チェーンを使用する場合、Cisco IOS ソフトウェアでキー ID が設定されます。キー ID は、他の RSVP プラットフォームで設定可能です。送信元が送信した RSVP 認証済みメッセージすべてにキー ID が割り当てられ、すべての受信者がこれを保存します。 （注） **KeyExpired** ：このフィールド内では、このネイバーに使用可能なキーがすべて期限切れになっていることを意味します。
Key ACL	dynamic、chain などのキー タイプの場合、このフィールドはネイバーに一致した ACL を示します。つまり、使用するキー チェーンを示します。有効な値は次のとおりです。 • **populated**：ACL のエントリが存在します。 • **removed** ：設定から ACL が削除されています。
Key Source	キーが設定済みかどうか、有効かどうかを示します。キーチェーンの場合、キー チェーンの名前を示します。Key ID フィールドはチェーン内の現在使用中のキーを示します。インターフェイス単位キーの場合、このキーで設定されたインターフェイスの名前を示します。
Key Type	static（手動設定）または dynamic（ACL 単位キーから作成、または Kerberos などのキー管理サーバから取得）。 （注） Cisco IOS ソフトウェアでは、キー管理サーバからのダイナミック キーは現在サポートされていません。
Handle	経理目的でRSVPによってセキュリティ アソシエーションに割り当てられた内部データ ベース ID。
Hash Type	ネイバーで使用するセキュア ハッシュ アルゴリズムのタイプ。
Lifetime	セキュリティ アソシエーションが期限切れになるまでの最大時間（時間、分、および秒単位）。 （注） これはキーの有効期間ではありません。キーの有効期間を取得するには、**showkeychain** コマンドを使用します。

フィールド	説明
Expires	セキュリティ アソシエーションが期限切れになるまでの残り時間（日、時間、分、および秒単位）。 （注） これは現在のキーの期限ではありません。キーの期限を取得するには、**showkeychain** コマンドを使用します。
Challenge	receive タイプのセキュリティ アソシエーションの場合、有効な値は **NotConfigured**、**Completed**、**InProgress**、および **Failed** です。send タイプのセキュリティ アソシエーションの場合、値は **Supported** です。Cisco IOS ソフトウェアは常にチャレンジに応答できますが、シスコ以外のネイバーではチャレンジが実装されていない場合があります。
Window size	receive タイプのセキュリティ アソシエーションのウィンドウ サイズ、およびリプレイ アタックを疑うまでに、順序が不正であっても受信することを許容する認証済み RSVP メッセージの最大数を示します。
Last seq # sent	send タイプのセキュリティ アソシエーションにのみ表示されます。最後の認証済みメッセージを RSVP ネイバーに送信するために使用するシーケンス番号を示します。この情報を使用して、特定タイプの認証問題をトラブルシューティングします。
Last valid seq # rcvd	receive タイプのセキュリティ アソシエーションにのみ表示されます。ネイバーから受信した最後の有効な RSVP メッセージの認証シーケンス番号を示します。デフォルトでは、1 つのシーケンス番号が表示されます。ただし、ip rsvp authentication window-size コマンドを使用して、認証ウィンドウ サイズを n に増やす場合、最後から n 個の有効な受信シーケンス番号が表示されます。この情報を使用して、特定タイプの認証問題をトラブルシューティングします。

関連コマンド

コマンド	説明
cleariprsvpauthentication	ライフタイムの期限が切れる前に RSVP セキュリティ アソシエーションを削除します。

show ip rsvp counters

各インターフェイスで送受信されたリソース予約プロトコル（RSVP）メッセージ数を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpcounters** コマンドを使用します。

show ip rsvp counters [authentication] [{**interface** *type number*|**neighbor** [**vrf** {******vrf-name*}]|**state teardown|summary**}]

構文の説明

authentication	（任意）RSVP 認証カウンタのリストを表示します。
interface *type number*	（任意）指定したインターフェイス名の送受信 RSVP メッセージの数を表示します。
neighbor	（任意）指定したネイバーの送受信 RSVP メッセージの数を表示します。
vrf *	（任意）設定された Virtual Routing and Forwarding（VRF）インスタンスをすべて表示します。
vrf *vrf-name*	（任意）指定した VRF の名前を表示します。
stateteardown	（任意）RSVP メッセージ状態の数とティアダウンの理由を表示します。
summary	（任意）すべてのインターフェイス上でルータによって送受信された RSVP メッセージの累積数を表示します。

コマンド デフォルト

showiprsvpcounters コマンドをオプションのキーワードを指定せずに入力すると、RSVP が設定された各インターフェイスで送受信された RSVP メッセージの数が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(14)ST	このコマンドが導入されました。
12.2(13)T	**neighbor** キーワードが追加され、このコマンドが Cisco IOS Release 12.2(13)T に統合されました。
12.2(15)T	コマンド出力が変更され、RSVP 認証が有効なインターフェイスに RSVP メッセージが着信し、そのメッセージの認証チェックに失敗するとエラー数が増えるエラー カウンタを表示するようになりました。
12.2(11)S	このコマンドが、Cisco IOS Release 12.2(11)S に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。

リリース	変更箇所
12.0(29)S	**authentication** キーワードが追加されました。コマンド出力が変更され、Hello およびメッセージ キュー情報も表示されるようになりました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.0(1)M	このコマンドが変更されました。**vrf** および ***** キーワードと *vrf-name* 引数が追加されました。

例

Summary の例

次の例では、すべてのインターフェイスのルータで送受信された各タイプの RSVP メッセージ数を、Hello およびメッセージ キュー情報とともに表示します。

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit                        Recv      Xmit
    Path                  110        15    Resv                  50        28
    PathError               0         0    ResvError              0         0
    PathTear                0         0    ResvTear               0         0
    ResvConf                0         0    RTearConf              0         0
    Ack                     0         0    Srefresh               0         0
    Hello                5555      5554    IntegrityChalle        0         0
    IntegrityRespon         0         0    DSBM_WILLING           0         0
    I_AM_DSBM               0         0
    Unknown                 0         0    Errors                 0         0
Recv Msg Queues                 Current       Max
    RSVP                              0         2
    Hello (per-I/F)                   0         1
    Awaiting Authentication           0         0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *39 : show ip rsvp counters summary* フィールドの説明

フィールド	説明
All Interfaces	すべてのインターフェイスについて表示されるメッセージのタイプ。 （注） Hello はグレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute メッセージのサマリーです。
Recv	指定したインターフェイスまたはすべてのインターフェイスで受信されたメッセージの数。

フィールド	説明
Xmit	指定したインターフェイスまたはすべてのインターフェイスから送信されたメッセージの数。
Recv Msg Queues	RSVP、インターフェイスごとのHello、および待機中の認証向けの受信メッセージ キュー。 • Current：キューイング中のメッセージの数。 • Max：過去にキューイングされたメッセージの最大数。

VRF の例

次の例では、VRF名がmyvrfの指定したネイバーのRSVPメッセージ数を表示します。

```
Router# show ip rsvp counters neighbor vrf myvrf
VRF: myvrf
Neighbor: 10.10.15.13
      Rate-Limiting:
        Output queue overflow, number of dropped RSVP messages: 0
      Refresh-Reduction:
        Number of RSVP messages received out of order: 0
        Number of retransmitted RSVP messages: 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *40 : show ip rsvp counters neighbor vrf* フィールドの説明

フィールド	説明
VRF	VRF の名前。
Neighbor	ネイバーの IP アドレス。
Rate-Limiting	有効な rate-limiting パラメータは次のとおりです。 • Output queue overflow, number of dropped RVSP messages：キューのオーバーフロー時にネイバーによってドロップされたメッセージの数。
Refresh-Reduction	有効な refresh-reduction パラメータは次のとおりです。 • Number of RSVP messages received out of order：シーケンシャルな順番ではないためドロップされたメッセージの数。 • Number of retransmitted RSVP messages：ネイバーに再送信されたメッセージの数。

関連コマンド

コマンド	説明
clearipsvpcounters	保持されている IP RSVP カウンタをすべてクリア（0 に設定）します。

show ip rsvp counters state teardown

ティアダウン状態の原因になったリソース予約プロトコル（RSVP）イベントのカウンタを表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpcountersstateteardown** コマンドを使用します。

show ip rsvp counters state teardown

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC
特権 EXEC

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ラベルスイッチドパス（LSP）がダウン状態の場合は **showiprsvpcountersstateteardown** コマンドを使用します。グレースフル リスタートでティアダウン状態がトリガーされた場合、「例」セクションの Path、Resv-In、および Resv-Out 列の数値は 0 より大きくなります。

例

次は、**showiprsvpcountersstateteardown** コマンドの出力例です。

```
Router# show ip rsvp counters state teardown
States
  Reason for Teardown                          State torn down
                                                 Path    Resv-In   Resv-Out
  PathTear arrival                                  0          0          0
  ResvTear arrival                                  0          0          0
  Local application requested tear                  0          0          0
  Output or Input I/F went down                     0          0          0
  Missed refreshes                                  0          0          0
  Preemption                                        0          0          0
  Backup tunnel failed for FRR Active LSP           0          0          0
  Reroutabilty changed for FRR Active LSP           0          0          0
  Hello RR Client (HST) requested tear              0          0          0
  Graceful Restart (GR) requested tear              0          0          0
  Downstream neighbor SSO-restarting                0          0          0
  Resource unavailable                              0          0          0
  Policy rejection                                  0          0          0
  Policy server sync failed                         0          0          0
  Traffic control error                             0          0          0
  Error in received message                         0          0          0
```

```
Non RSVP HOP upstream, TE LSP                    0          0          0
Other                                            0          0          0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *41 : show ip rsvp counters state teardown* フィールドの説明

フィールド	説明
States	パス ステート ブロック（PSB）および予約ステート ブロック（RSB）情報を含む RSVP 状態。
Reason for Teardown	ティアダウンをトリガーしたイベント。

関連コマンド

コマンド	説明
cleariprsvpcounters	保持されている IP RSVP カウンタをクリア（0 に設定）します。

show ip rsvp fast bw-protect

バックアップ帯域幅保護が有効かどうか、その保護を提供するために使用するバックアップ トンネルの状態を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfastbw-protect** コマンドを使用します。

show ip rsvp fast bw-protect [detail] [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

バックアップ帯域幅保護およびバックアップ トンネル状態の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました

例

次は、**showiprsvpfastbw-protect** コマンドの出力例です。

```
Router# show ip rsvp fast bw-protect
```

```
Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
---------------  -------  --------   ----------    -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *42 : show ip rsvp fast bw-protect* フィールドの説明

フィールド	説明
Primary Tunnel	保護されているトンネルの ID。
Protect I/F	インターフェイス名。
BW BPS:Type	帯域幅（bps）および帯域幅のタイプ。可能な値は次のとおりです。 • S：サブプール • G：グローバル プール
Backup Tunnel:Label	バックアップ トンネルの ID。
State	バックアップ トンネルの状態有効な値は次のとおりです。 • Ready：データはプライマリ トンネルを通過していますが、プライマリ トンネルがダウンした場合はバックアップ トンネルに切り替わります。 • Active：プライマリ トンネルがダウンしたため、バックアップ トンネルがトラフィックに使用されています。 • None：バックアップ トンネルはありません。
BW-P	バックアップ帯域幅保護の状態。有効な値は、ON または OFF です。
Type	バックアップ トンネルのタイプ。可能な値は次のとおりです。 • Nhop：ネクスト ホップ • NNHOP：ネクスト ネクスト ホップ

関連コマンド

コマンド	説明
tunnelmplstraffic-engfast-reroutebw-protect	MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。

show ip rsvp fast detail

リソース予約プロトコル（RSVP）カテゴリ固有の情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfastdetail** コマンドを使用します。

show ip rsvp fast detail [**filter** [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

filter	（任意）表示する受信者のサブネットを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

RSVP カテゴリ固有の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(24)S	このコマンドが導入されました。
12.0(29)S	必要な Bandwidth Prot がコマンド出力の Flag フィールドに追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

例

次に、**show ip rsvp fast detail** コマンドの出力例を示します。

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
```

```
  Setup Prio: 7, Holding Prio: 7
  Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: PRAB-72-5_t500
ERO: (incoming)
  10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound  FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
    Backup Tunnel: Tu501      (label 19)
    Bkup Sender Template:
      Tun Sender: 10.5.6.5  LSP ID: 8
    Bkup FilerSpec:
      Tun Sender: 10.5.6.5, LSP ID: 8
Path ID handle: 04000405.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *43 : show ip rsvp fast detail* フィールドの説明

フィールド	説明
Tun Dest	受信者の IP アドレス。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベルスイッチド パス ID 番号。
Setup Prio	確立プライオリティ。
Holding Prio	ホールディング プライオリティ。
Flags	バックアップ帯域幅保護がラベルスイッチド パス（LSP）に設定されています。
Session Name	セッションの名前を指定します。
ERO (incoming)	着信 path メッセージの EXPLICIT_ROUTE オブジェクト。
ERO (outgoing)	発信 path メッセージの EXPLICIT_ROUTE オブジェクト。
Traffic params Rate	平均レート（ビット/秒）です。

フィールド	説明
Max. burst	最大バースト サイズ（バイト）。
Min Policed Unit	最小ポリシング単位（バイト）。
Max Pkt Size	最大パケット サイズ（バイト）。
Inbound FRR	着信 Fast Reroute（FRR）バックアップ トンネルの状態。このノードが再ルーティングされた LSP の下流にある（この LSP のマージ ポイントなど）場合、状態はアクティブです。
Outbound FRR	発信 FRR バックアップ トンネルの状態。このノードが、LSP のローカル修復点（PLR）である場合、次の 3 つの状態があります。 • Active：おそらくダウンストリーム障害があったため、この LSP はアクティブにバックアップ トンネルを使用しています。 • No Backup：この LSP にはローカルの（Fast Reroute）保護がありません。障害時に使用するためのバックアップ トンネルが選択されていません。 • Ready：この LSP は、ダウンストリーム リンクまたはノードの障害発生時にバックアップ トンネルが使用できます。障害時に使用するためのバックアップ トンネルが選択されています。
Backup Tunnel	発信 FRR 状態が Ready または Active の場合、このフィールドには次の内容が表示されます。 • 障害時に使用するためこの LSP に選択されているバックアップ トンネル。 • バックアップ トンネルテール（マージポイント）で受信するため、LSP のデータ パケットの先頭に追加される着信ラベル。
Bkup Sender Template	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path メッセージおよび pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv メッセージおよび resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。

フィールド	説明
Bkup FilerSpec	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Path ID handle	保護スイッチ バイト（PSB）の識別子。
Incoming policy	LSP のポリシー判定。トンネルの着信 path メッセージに RSVP ポリシーが許可されていなかった場合、LSP はアップになりません。Accepted が表示されます。
Policy source(s)	FRR LSP の場合、ポリシー ソースの値は常に MPLS/TE です。
Status	FRR LSP の場合、有効な値は次のとおりです。 • Proxied：ヘッドエンド ルータ。 • Proxied Terminated：テールエンド ルータ。 ミッドポイント ルータの場合、このフィールドは常に空白です。

関連コマンド

コマンド	説明
mplstraffic-engfast-reroutebackup-prot-preemption	バックアップ保護プリエンプション アルゴリズムを変更して、有効に使用されていない帯域幅量を最小化します。

show ip rsvp fast-reroute

高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroute** コマンドを使用します。

show ip rsvp fast-reroute [**filter** [**session-type** {*session-type-number*|**all**}]]

構文の説明

filter	（任意）表示するトンネルのサブネットを指定します。
session-type *session-type-number*	（任意）表示するトンネルのタイプを指定します。有効な値は次のとおりです。 • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合）。 • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
session-typeall	（任意）トンネル セッションのすべてのタイプを指定します。

コマンド デフォルト

引数を指定しない場合は、すべての高速再ルーティング プライマリ トンネルの情報が表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(27)S	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
12.2(33)SRE	このコマンドが変更されました。**filter** キーワードが追加され、ポイントツーポイントとポイントツーマルチポイント別にトンネル情報が表示されるようになりました。出力が更新され、マルチプロトコル ラベル スイッチング（MPLS）TE P2MP の情報が表示されるようになりました。
15.0(1)M	このコマンドが変更されました。クラシック IP RSVP（セッション タイプ 1）のサポートが削除されました。

例

次は、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの出力例です。

```
Router# show ip rsvp fast-reroute
Primary                 Protect BW         Backup
Tunnel                  I/F     BPS:Type   Tunnel:Label  State  Level  Type
------                  ------- --------   ------------- ------ -----  ---
GSR1---R2---_t65336     PO1/0   0:G        Tu1002:0      Ready  any-unl Nhop
GSR1---R2---_t65338     PO4/0   0:G        Tu1004:0      Ready  any-unl Nhop
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *44 : show ip rsvp fast-reroute* フィールドの説明

フィールド	説明
Primary Tunnel	ホスト名とトンネル ID。
Protect I/F	保護されているインターフェイス。
BW BPS:Type	帯域幅（bps）と帯域幅を供給するプール。有効な値は、G（グローバル プール）と S（サブプール）です。
Backup Tunnel:Label	バックアップ トンネル ID とラベル。
State	保護の状態。有効な値は、Ready、Active、および None です。
Level	帯域幅のレベル。有効な値は、any と unl（無制限）です。
Type	バックアップ トンネルのタイプ：Nhop（ネクスト ホップ）または NNhop（ネクスト ネクスト ホップ）。

次の例では、高速再ルーティング プライマリ トンネルと、これに対応するバックアップ トンネルを表示します。この情報は、P2P LSP と P2MP サブ LSP に分類されます。次の例では、6 つのサブ LSP（イーサネット インターフェイス 0/0 で保護される 3 つとイーサネット インターフェイス 0/1 で保護される 3 つ）が含まれる Tunnel 22 を表示します。

```
Router# show ip rsvp fast-reroute
P2P                         Protect BW         Backup
Protected LSP               I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------               ------- --------   ------------- ------ -----   ------
R201_t1                     Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
P2MP
Protected Sub-LSP                           Protect BW         Backup
src_lspid[subid]->dst_tunid                 I/F     BPS:Type   Tunnel:Label  State
---------------------------                 ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22                Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22                Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22                Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22                Et0/1   500K:G     None          None
```

次の例では、Cisco IOS Release 12.4(24)T 以前のリリースで、高速再ルーティング プライマリ トンネルと、これに対応するバックアップ トンネルの情報を表示します。出力は、セッション タイプ別に表示されます。

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 1 (rsvp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
R201_t1                   Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
Protected Sub-LSP                          Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22               Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22               Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22               Et0/1   500K:G     None          None
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *45 : show ip rsvp fast-reroute Point-to-Multipoint* フィールドの説明

フィールド	説明
Protected LSP	保護されている LSP とトンネル ID。
Protected Sub-LSP src_lspid[subid]->dst_tunid	保護されているサブ LSP の送信元と宛先アドレス。P2MP ID は、送信元アドレスに追加されます。トンネル ID は、宛先アドレスに追加されます。

次の例では、Cisco IOS Release 15.0(1)M 以降のリリースで、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルの情報を表示します。

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
p2mp-2_t12                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
p2mp-2_t13                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
*Protected Sub-LSP                         Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.2.0.1_12[1]->10.1.0.1_1                 Se5/0   1M:G       None          None
```

```
10.2.0.1_12[3]->10.2.3.3_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[5]->10.3.0.1_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[6]->10.3.4.3_1              Se3/0   1M:G        Tu700:16      Ready
10.2.0.1_12[8]->10.2.5.3_1              Se6/0   1M:G        Tu100:17      Ready
```

関連コマンド

コマンド	説明
mplstraffic-engauto-tunnelprimaryconfig	明示的なアドレスを使用せずに IP 処理を有効にします。
mplstraffic-engauto-tunnelprimaryconfigmplsip	プライマリ自動トンネルで LDP をイネーブルにします。
mplstraffic-engauto-tunnelprimaryonehop	すべてのネクストホップへのプライマリ トンネルを自動的に作成します。
mplstraffic-engauto-tunnelprimarytimers	障害の発生したプライマリ自動トンネルの削除後の秒数を設定します。
mplstraffic-engauto-tunnelprimarytunnel-num	プライマリ自動トンネル用のトンネルインターフェイス番号の範囲を設定します。

show ip rsvp fast-reroute bw-protect

バックアップ帯域幅保護が有効かどうか、その保護を提供するために使用するバックアップ トンネルの状態を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroutebw-protect** コマンドを使用します。

show ip rsvp fast-reroute bw-protect [detail] [**filter** [**session-type** {*session-type-number*|**all**}] [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

detail	（任意）追加の受信者情報を指定します。
filter	（任意）表示する受信者のサブネットを指定します。
session-type *session-type-number*	（任意）表示するリソース予約プロトコル（RSVP）セッションのタイプを指定します。有効な値は次のとおりです。 • **1**（IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13**（IPv4 ポイントツーマルチポイント TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド デフォルト

バックアップ帯域幅保護およびバックアップ トンネル状態の情報は表示されません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(29)S	このコマンドが導入されました。

リリース	変更箇所
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）ポイントツーマルチポイント（P2MP）の情報が表示されるようになりました。

例

次は、**showiprsvpfast-reroutebw-protect** コマンドの出力例です。

```
Router# show ip rsvp fast-reroute bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
---------------  -------  ---------  -----------   -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *46 : show ip rsvp fast-reroute bw-protect* フィールドの説明

フィールド	説明
Primary Tunnel	保護されているトンネルの ID。
Protect I/F	インターフェイス名。
BW BPS:Type	帯域幅（bps）および帯域幅のタイプ。可能な値は次のとおりです。 • S：サブプール • G：グローバル プール
Backup Tunnel:Label	バックアップ トンネルの ID。

フィールド	説明
State	バックアップ トンネルの状態有効な値は次のとおりです。 • Ready：データはプライマリ トンネルを通過していますが、プライマリ トンネルがダウンした場合はバックアップ トンネルに切り替わります。 • Active：プライマリ トンネルがダウンしたため、バックアップ トンネルがトラフィックに使用されています。 • None：バックアップ トンネルはありません。
BW-P	バックアップ帯域幅保護の状態。有効な値は、ON または OFF です。
Type	バックアップ トンネルのタイプ。有効な値は次のとおりです。 • Nhop：ネクスト ホップ • NNHOP：ネクスト ネクスト ホップ

次の例では、高速再ルーティング プライマリ トンネルと、これに対応して保護を提供するバックアップ トンネルを表示します。この情報は、ポイントツーポイント（P2P）ラベル スイッチド パス（LSP）と P2MP サブ LSP に分類されます。次の例では、6 つのサブ LSP（イーサネット インターフェイス 0/0 で保護される 3 つとイーサネット インターフェイス 0/1 で保護される 3 つ）が含まれる Tunnel 22 を表示します。

```
Router# show ip rsvp fast-reroute bw-protect

P2P                          Protect BW          Backup
Protected LSP                I/F     BPS:Type    Tunnel:Label  State  BW-P    Type
-------------                ------- --------    ------------- ------ -----   ------
R201_t1                      Et0/1   500K:G      Tu777:16      Ready  ON      Nhop
P2MP
Protected Sub-LSP                              Protect BW          Backup
src_lspid[subid]->dst_tunid                    I/F     BPS:Type    Tunnel:Label  BW-P
---------------------------                    ------- --------    ------------- ------
10.1.1.201_1[1]->10.1.1.203_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[2]->10.1.1.206_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[3]->10.1.1.213_22                   Et0/0   500K:G      Tu666:20      ON
10.1.1.201_1[4]->10.1.1.214_22                   Et0/1   500K:G      None          None
10.1.1.201_1[5]->10.1.1.216_22                   Et0/1   500K:G      None          None
10.1.1.201_1[6]->10.1.1.217_22                   Et0/1   500K:G      None          None
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *47 : show ip rsvp fast-reroute bw-protect Point-to-Multipoint* フィールドの説明

フィールド	説明
Protected LSP	保護されている LSP とトンネル ID。

フィールド	説明
Protected Sub-LSP src_lspid[subid]->dst_tunid	保護されているサブ LSP の送信元と宛先アドレス。P2MP ID は、送信元アドレスに追加されます。トンネル ID は、宛先アドレスに追加されます。

関連コマンド

コマンド	説明
tunnelmplstraffic-engfast-reroutebw-protect	MPLS TE トンネルが、リンクまたはノードの障害発生時に、確立されたバックアップ トンネルを使用できるようにします。

show ip rsvp fast-reroute detail

リソース予約プロトコル（RSVP）カテゴリ固有の情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvpfast-reroutedetail** コマンドを使用します。

show ip rsvp fast-reroute detail [**filter** [**session-type** {*session-type-number*|**all**}] [{**destination** *ip-addresshostname*}] [**dst-port** *port-number*] [{**source** *ip-addresshostname*}] [**src-port** *port-number*]]

構文の説明

filter	（任意）表示する受信者のサブネットを指定します。
session-type *session-type-number*	（任意）表示する RSVP セッションのタイプを指定します。有効な値は次のとおりです。 • **1**（IPv4 セッションの場合） • **7**（IPv4 ポイントツーポイント（P2P）トラフィック エンジニアリング（TE）ラベル スイッチド パス（LSP）トンネル セッションの場合） • **13**（IPv4 ポイントツーマルチポイント（P2MP）TE LSP トンネル セッションの場合）
all	（任意）RSVP セッションのすべてのタイプを指定します。
destination *ip-address*	（任意）受信者の宛先 IP アドレスを指定します。
hostname	（任意）受信者のホスト名を指定します。
dst-port *port-number*	（任意）宛先ポート番号を指定します。有効な宛先ポート番号は、0 ～ 65535 の範囲内の値です。
source *ip-address*	（任意）受信者の送信元 IP アドレスを指定します。
src-port *port-number*	（任意）送信元ポートの番号を指定します。有効な送信元ポート番号は、0 ～ 65535 の範囲内の値です。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(24)S	このコマンドが導入されました。
12.0(29)S	必要な Bandwidth Prot がコマンド出力の Flag フィールドに追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。

リリース	変更箇所
12.2(33)SRE	このコマンドが変更されました。**session-type** キーワードが追加され、指定したタイプのトンネルが表示されるようになりました。出力が変更され、MPLS TE P2MP の情報が表示されるようになりました。

例

次に、**show ip rsvp fast-reroute detail** コマンドの出力例を示します。

```
Router# show ip rsvp fast-reroute detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 10.5.6.5  LSP ID: 8
      Bkup FilerSpec:
        Tun Sender: 10.5.6.5, LSP ID: 8
  Path ID handle: 04000405.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxied
  Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *48 : show ip rsvp fast-reroute detail* フィールドの説明

フィールド	説明
Tun Dest	受信者の IP アドレス。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。

フィールド	説明
LSP ID	ラベル スイッチド パス ID 番号。
Setup Prio	確立プライオリティ。
Holding Prio	ホールディング プライオリティ。
Flags	バックアップ帯域幅保護がラベル スイッチドパスに設定されています。
Session Name	セッションの名前を指定します。
ERO (incoming)	着信 path メッセージの EXPLICIT_ROUTE オブジェクト。
ERO (outgoing)	発信 path メッセージの EXPLICIT_ROUTE オブジェクト。
Traffic params Rate	平均レート（ビット/秒）です。
Max. burst	最大バースト サイズ（バイト）。
Min Policed Unit	最小ポリシング単位（バイト）。
Max Pkt Size	最大パケット サイズ（バイト）。
Inbound FRR	着信 Fast Reroute（FRR）バックアップ トンネルの状態。このノードが再ルーティングされた LSP の下流にある（この LSP のマージ ポイントなど）場合、状態はアクティブです。
Outbound FRR	発信 FRR バックアップ トンネルの状態。このノードが、LSP のローカル修復点（PLR）である場合、次の 3 つの状態があります。 • Active：おそらくダウンストリーム障害があったため、この LSP はアクティブにバックアップ トンネルを使用しています。 • No Backup：この LSP にはローカルの（Fast Reroute）保護がありません。障害時に使用するためのバックアップ トンネルが選択されていません。 • Ready：この LSP は、ダウンストリーム リンクまたはノードの障害発生時にバックアップ トンネルが使用できます。障害時に使用するためのバックアップ トンネルが選択されています。
Backup Tunnel	発信 FRR 状態が Ready または Active の場合、このフィールドには次の内容が表示されます。 • 障害時に使用するためこの LSP に選択されているバックアップ トンネル。 • バックアップ トンネルテール（マージポイント）で受信するため、LSP のデータ パケットの先頭に追加される着信ラベル。

フィールド	説明
Bkup Sender Template	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Bkup FilerSpec	発信 FRR 状態が Ready または Active の場合、SENDER_TEMPLATE および FILTERSPEC オブジェクトが表示されます。LSP がアクティブにバックアップ トンネルの使用を開始すると、これらのオブジェクトは、バックアップ トンネルから送信される RSVP メッセージ内で使用されます。ノード（PLR）はオリジナルの発信元ではなく、それ自身の IP アドレスを使用するという点のみが、これらのオブジェクトとオリジナル（障害前）のオブジェクトとは異なります。たとえば、path および pathTear メッセージには、新しい SENDER_TEMPLATE が含まれます。Resv および resvTear メッセージには、新しい FILTERSPEC オブジェクトが含まれます。この LSP がアクティブにバックアップ トンネルの使用を開始する場合、表示が変化します。
Path ID handle	保護スイッチ バイト（PSB）の識別子。
Incoming policy	LSP のポリシー判定。トンネルの着信 path メッセージに RSVP ポリシーが許可されていなかった場合、LSP はアップになりません。Accepted が表示されます。
Policy source(s)	FRR LSP の場合、ポリシー ソースの値は常に MPLS/TE です。
Status	FRR LSP の場合、有効な値は次のとおりです。 • Proxied：ヘッドエンド ルータ。 • Proxied Terminated：テールエンド ルータ。 ミッドポイント ルータの場合、このフィールドは常に空白です。

次の例では、P2MP データを表示します。

```
Router# show ip rsvp fast-reroute detail

PATH:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
```

```
SubGroup ID: 2
S2L Destination : 10.1.1.206
Path refreshes:
  sent:     to   NHOP 10.0.0.205 on Ethernet0/0
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: R201_t22
ERO: (incoming)
  10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
  1o.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
Fast-Reroute Backup info:
  Inbound  FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
    Backup Tunnel: Tu666      (label 20)
    Bkup Sender Template:
      Tun Sender: 10.0.2.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
    Bkup FilerSpec:
      Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
Path ID handle: 01000417.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *49 : show ip rsvp fast-reroute detail P2MP* フィールドの説明

フィールド	説明
P2MP ID	P2MP トンネルの宛先セットを指定する 32 ビットの番号。
Tun ID	トンネル ID 番号。
Ext Tun ID	拡張トンネル ID 番号。
Tun Sender	送信元の IP アドレス。
LSP ID	ラベル スイッチド パス ID 番号。
SubGroup Orig	LSP ヘッドエンド ルータ ID アドレス。
SubGroup ID	ヘッドエンド ルータからのシグナルを受ける各サブ LSP に割り当てられる増分番号。
S2L Destination	LSP テールエンド ルータ ID アドレス。

関連コマンド

コマンド	説明
mplstraffic-engfast-reroutebackup-prot-preemption	バックアップ保護プリエンプションアルゴリズムを変更して、有効に使用されていない帯域幅量を最小化します。

show ip rsvp hello

高速再ルーティング、再ルーティング（Hello ステート タイマー）、グレースフル リスタートに関する hello の状態および統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showiprsvphello** コマンドを使用します。

show ip rsvp hello

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(22)S	このコマンドが導入されました。
12.0(29)S	コマンド出力が変更され、グレースフル リスタート、再ルーティング（Hello ステート タイマー）、および Fast Reroute の情報が追加されました。
12.2(18)SXD1	このコマンドが、Cisco IOS Release 12.2(18)SXD1 に統合されました。
12.2(33)SRA	コマンド出力が変更され、グレースフル リスタートが設定されているかどうか、フル モードが追加されているかどうかが表示されるようになりました。
12.2(31)SB2	このコマンドは、Cisco IOS Release 12.2(31)SB2 に統合されました。
12.2(33)SRC	コマンドの出力が、双方向フォワーディング検出（BFD）プロトコル情報も含むように変更されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

例

次は、**showiprsvphello** コマンドの出力例です。

```
Router# show ip rsvp hello
Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

次の表で、この出力に表示される重要なフィールドを説明します。これらのフィールドは、hello が有効化または無効化されているプロセスに関する情報を表示します。

表 *50 : show ip rsvp hello* フィールドの説明

フィールド	説明
RSVP Hello for Fast-Reroute/Reroute	高速再ルーティング/再ルーティングの状態。 • Disabled：高速再ルーティングおよび再ルーティング（Hello ステート タイマー）は非アクティブ（無効）です。 • Enabled：高速再ルーティングおよび再ルーティング（Hello ステート タイマー）はアクティブ（有効）です。
Statistics	hello 統計の状態。 • Disabled：hello 統計は設定されていません。 • Enabled：統計が設定されています。hello パケットは、Hello インプット キューに到達すると、処理されるまでに要した時間を記録するためにタイムスタンプが付加されます。 • Shutdown：hello 統計は設定されていますが、動作していません。インプット キューが長すぎです（つまり、10,000 を超えるパケットがキュー内に滞留しています）。
BFD for Fast-Reroute/Reroute	高速再ルーティング/再ルーティングの BFD の状態。 • Disabled：BFD は設定されていません。 • Enabled：BFD が設定されています。
Graceful Restart	リスタート機能： • Disabled：リスタート機能は非アクティブです。 • Enabled：リスタート機能は、ルータ（フル モード）またはネイバー（ヘルプ ネイバー）でアクティブです。

関連コマンド

コマンド	説明
iprsvpsignallinghello(configuration)	ルータで Hello をグローバルに有効にします。
iprsvpsignallinghellostatistics	ルータで Hello 統計情報を有効にします。
showiprsvphellostatistics	hello パケットが hello 入力キューに入っていた時間を表示します。

show ip rsvp hello client lsp detail

ラベルスイッチド パス（LSP）のリソース予約プロトコル（RSVP）トラフィック エンジニアリング（TE）クライアント Hello に関する詳細情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showiprsvphelloclientlspdetail** コマンドを使用します。

show ip rsvp hello client lsp detail [**filter** [**destination** *hostname*]]

構文の説明

filter	（任意）出力表示を限定するフィルタを指定します。
destination	（任意）接続先（トンネルテール）に設定されたフィルタを表示します。
hostname	（任意）接続先（トンネル テール）の IP アドレスまたは名前。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更箇所
12.0(33)S	このコマンドが導入されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

LSP に関する情報（IP アドレス、タイプなど）を表示するには、**showiprsvphelloclientlspdetail** コマンドを使用します。

例

次は、**showiprsvphelloclientlspdetail** コマンドの出力例です。

```
Router# show ip rsvp hello client lsp detail
Hello Client LSPs (all lsp tree)
  Tun Dest: 10.0.1.1  Tun ID: 14  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 31
    Lsp flags: 0x32
    Lsp GR DN nbr: 192.168.1.1
    Lsp RR DN nbr: 10.0.0.3 HST
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *51 : show ip rsvp hello client lsp detail* フィールドの説明

フィールド	説明
Hello Client LSPs	現在のクライアントには、グレースフル リスタート（GR）、再ルーティング（RR）（Hello ステート タイマー）、および Fast Reroute（FRR）が含まれます。
Tun Dest	宛先トンネルの IP アドレス。

フィールド	説明
Tun ID	トンネルの ID 番号。
Ext Tun ID	トンネルの拡張 ID 番号。通常、発信元アドレスと同じです。
Tun Sender	トンネル送信元の IP アドレス。
LSP ID	LSP の ID 番号。
Lsp flags	LSP データベースの情報。
Lsp GR DN nbr	LSP グレースフル リスタート ダウンストリーム ネイバーの IP アドレス。
Lsp RR DN nbr	LSP 再ルーティング ダウンストリーム ネイバーの IP アドレス（HST：Hello ステート タイマー）。

関連コマンド

コマンド	説明
showiprsvphello	Fast Reroute、再ルーティング（Hello ステート タイマー）、およびグレースフル リスタートについて、Hello の状態と統計情報を表示します。