Cisco IOS セキュリティ コマンド リファレンス：コマンド M ～ R、Cisco IOS XE リリース 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 11 日

最終更新：2013 年 01 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

目 次

mab ～ mime-type

mab

ポートで MAC ベースの認証を有効にするには、インターフェイス コンフィギュレーション モードまたはテンプレート コンフィギュレーション モードで **mab** コマンドを使用します。MAC ベースの認証を無効にするには、このコマンドの **no** 形式を使用します。

mab [eap]

no mab

構文の説明

eap	（オプション）Extensible Authentication Protocol（EAP）を使用するようにポートを設定します。

コマンド デフォルト

MAC ベースの認証は有効になっていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

テンプレート コンフィギュレーション（config-template）

コマンド履歴

リリース	変更内容
12.2(33)SXI	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。
15.2(2)E	このコマンドが、Cisco IOS リリース 15.2(2)E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。
Cisco IOS XE Release 3.6E	このコマンドが Cisco IOS XE Release 3.6E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。

使用上のガイドライン

ポートで MAC ベースの認証を有効にするには、**mab** コマンドを使用します。ポートで EAP を有効にするには、**mabeap** コマンドを使用します。

（注） MAB または MAB EAP がスイッチド ポート上で有効または無効のいずれであるかがわからない場合は、インターフェイス コンフィギュレーション モードで、**defaultmab** コマンドまたは **defaultmabeap** コマンドを使用して、MAB または MAB EAP をデフォルトに設定します。

例

次に、ギガビット イーサネット ポートで MAC ベースの認証を設定する例を示します。

```
Switch(config)# interface GigabitEthernet6/2
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# mab
Switch(config-if)# end
```

次に、インターフェイス テンプレートで MAC ベースの認証を設定する例を示します。

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# mab
Device(config-template)# end
```

関連コマンド

コマンド	説明
showmab	MAB に関する情報を表示します。

mac access-group

MAC アクセス コントロール リスト（ACL）を使用して、ギガビット イーサネット インターフェイス、802.1Q VLAN サブインターフェイス、802.1Q-in-Q スタック VLAN サブインターフェイスでの着信トラフィックの受信を制御するには、インターフェイスまたはサブインターフェイス コンフィギュレーション モードで **macaccess-group** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac access-group *access-list-number* **in**

no mac access-group *access-list-number* **in**

構文の説明

access-list-number	インターフェイスまたはサブインターフェイスに適用する MAC ACL の番号（**access-list(MAC)** コマンドで指定された番号）。これは 10 進数の 700 ～ 799 です。
in	インバウンド パケットに対してフィルタリングします。

コマンド デフォルト

インターフェイスまたはサブインターフェイスにアクセス リストは適用されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）サブインターフェイス コンフィギュレーション（config-subif）

コマンド履歴

リリース	変更内容
12.0(32)S	このコマンドが Cisco 12000 シリーズ インターネット ルータに追加されました。
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

MAC ACL は、ギガビット イーサネット インターフェイスおよび VLAN サブインターフェイス上の着信トラフィックに対して適用されます。ネットワーキング デバイスでパケットを受信すると、Cisco IOS ソフトウェアはアクセス リストと、ギガビット イーサネット、802.1Q VLAN、ま

たは 802.1Q-in-Q のパケットの送信元 MAC アドレスを照合します。MAC アクセス リストでアドレスが許可されている場合、ソフトウェアはパケットの処理を続行します。アクセス リストでアドレスが拒否されている場合、ソフトウェアはパケットを廃棄し、インターネット制御メッセージ プロトコル（ICMP）ホスト到達不能メッセージを返します。

指定したMAC ACLがインターフェイスまたはサブインターフェイス上に存在しない場合、パケットはすべて通過します。

Catalyst 6500 シリーズ スイッチの場合、このコマンドをサポートするのはレイヤ 2 ポートだけです。

（注） VLANサブインターフェイス上で**macaccess-group** コマンドをサポートするのは、すでにVLANがサブインターフェイス上で設定済みの場合だけです。

例

次は、ギガビット イーサネット インターフェイス 0 で受信した着信トラフィックに対して MAC ACL 101 を適用する例です。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

関連コマンド

Command	Description
access-list(MAC)	MAC ACL を定義します。
clearmacaccess-listcounters	MAC ACL のカウンタをクリアします。
ipaccess-group	非同期ホストから送信されたパケットに対して使用する IP アクセス リストを設定します。
showaccess-groupmodeinterface	レイヤ2インターフェイスのACLコンフィギュレーションを表示します。
showmacaccess-list	1 つまたはすべての MAC ACL の内容を表示します。

mac-address (RITE)

宛先ホストのイーサネットアドレスを指定するには、ルータ IP トラフィック エクスポート（RITE）コンフィギュレーション モードで **mac-address** コマンドを使用します。宛先ホストの MAC アドレスを変更するには、このコマンドの **no** 形式を使用します。

mac-address *H.H.H*

nomac-address *H.H.H*

構文の説明

H.H.H	48 ビット MAC アドレス。

コマンド デフォルト

宛先ホストは不明です。

コマンド モード

RITE コンフィギュレーション

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。

使用上のガイドライン

mac-address コマンドは、エクスポートされたトラフィックを受信する宛先ホストを指定するコマンドであり、着信および発信の両方の IP トラフィック エクスポートの各種属性を制御する RITE コンフィギュレーション モード コマンド スイートの一部です。

iptraffic-exportprofile コマンドでは、選択したルータ入力インターフェイスで着信または発信される IP パケットをエクスポートするために設定できるプロファイルを開始できます。指定された出力インターフェイスは、キャプチャされた IP パケットをルータからエクスポートします。したがってルータは未変更の IP パケットを直接接続デバイスにエクスポートできます。

例

次に、プロファイル「corp1」を設定する例を示します。このプロファイルは、キャプチャされた IP トラフィックを、インターフェイス「FastEthernet 0/1」でホスト「00a.8aab.90a0」へ送信します。また、このプロファイルは 50 パケットごとに 1 つのパケットをエクスポートし、アクセス

コントロール リスト（ACL）「ham_ACL」からの着信トラフィックだけを許可するように設定されています。

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

関連コマンド

コマンド	説明
iptraffic-exportprofile	IP トラフィック エクスポート プロファイルを作成または編集し、入力インターフェイス上でこのプロファイルを有効にします。

match class-map

トラフィック クラスを分類ポリシーとして使用するには、クラス マップまたはポリシー インライン コンフィギュレーション モードで **match class-map** コマンドを使用します。一致基準としての特定のトラフィック クラスを削除するには、このコマンドの **no** 形式を使用します。

match class-map *class-map-nam e*

no match class-map *class-map-name*

構文の説明

class-map-name	一致基準として使用するトラフィック クラスの名前。

コマンド デフォルト

一致基準が指定されていません。

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更内容
12.0(5)XE	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。
12.4(6)T	このコマンドが拡張され、ゾーンベース ポリシー ファイアウォールをサポートするようになりました。
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(31)SB	このコマンドは、Cisco 10000 シリーズに実装されました。
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。
Cisco IOS XE Release 3.2S	このコマンドが、Cisco IOS XE Release 3.2S に統合されました。

使用上のガイドライン

1 つのトラフィック クラスに match-any 特性と match-all 特性の両方を使用する唯一の方法は、**match class-map** コマンドを使用する方法です。match-any 特性と match-all 特性を結合して 1 つのクラスにするには、次のいずれかを実行します。

- match-any 指示を使用してトラフィック クラスを作成し、一致基準として match-all 指示を使用して設定したクラスを使用します（**match class-map** コマンドを使用）。
- match-all 指示を使用してトラフィック クラスを作成し、一致基準として match-any 指示を使用して設定したクラスを使用します（**match class-map** コマンドを使用）。

また、**match class-map** コマンドを使用してトラフィック クラスを別のクラス内にネストすることもできます。これにより、以前に設定したトラフィック クラスにほとんどの情報が存在している場合に、ユーザが新しいトラフィック クラスを再作成するオーバーヘッドが削減されます。

パケットがクラス マップに一致すると、それらのパケットのトラフィック レートが生成されます。ゾーンベースファイアウォールポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

例

例

次の例で、トラフィック クラス class1 の特性は、トラフィック クラス class2 の特性とほぼ同じですが、トラフィック クラス class1 では、一致基準として宛先アドレスが追加されています。トラフィック クラス class1 をゼロから設定する代わりに、**match class-map class2** コマンドを使用できます。このコマンドを使用すると、トラフィック クラス class2 のすべての特性をトラフィック クラス class1 に取り込み、トラフィック クラスを再設定することなく、新しい宛先アドレスの一致条件を追加できます。

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

次に、2 つのトラフィック クラスの特性を組み合わせる例を示します。1 つは match-any 特性を使用し、1 つは match-all 特性を使用しています。これを、**match class-map** コマンドで 1 つのトラフィック クラスとして設定します。class4 というトラフィック クラスの場合、パケットが class4 トラフィック クラスのメンバーとして見なされるためには、3 つの一致基準（IP プロトコルかつ QoS グループ 4、宛先 MAC アドレス 1.1.1、またはアクセス グループ 2）のいずれかを満たしている必要があります。一致基準である IP プロトコルかつ QoS グループ 4 は、トラフィック クラス class3 の定義で必要であり、**match class-map class3** コマンドによって、トラフィック クラス class4 の定義に可能な一致として含まれています。

この例では、トラフィック クラス class4 だけがサービス ポリシー policy1 に使用されています。

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

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。

pac key ～ port-misuse

permit

名前付き IP アクセス リストでパケットを許可する条件を設定するには、該当するコンフィギュレーション モードで **permit** コマンドを使用します。IP アクセス リストから条件を削除するには、このコマンドの **no** 形式を使用します。

permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}} **[dscp** *dscp-value*| **precedence** *precedence-value*| **fragments** *fragment-value*| **option** *option-value*| **reflect** *access-list-name*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* **[ttl-value]**| **tos** *tos-value*| **timeout** *max-time*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit *protocol* [*source-addr source-wildcard*] {**any**| **host** {*address*| *name*}} {*destination-addr destination-wildcard*| **any**| **host** {*address*| *name*}}

permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*} {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*| *port-match-criteria* {*destination-addr destination-wildcard*| **any**| **host** *dest-addr*}} [*port-match-criteria port-number*| **fragments**| **ack**| **established**| **fin**| **psh**| **rst**| **syn**| **urg**| **match-all** *match-value*| **match-any** *match-value*| **dscp** *dscp-value*| **precedence** *precedence-value*| **option** *option-value*| **time-range** *time-range-value*| **ttl** *match-value ttl-value* [*ttl-value*]| **tos** *tos-value*| **log** [*log-value*]| **log-input** [*log-input-value*]]

no permit {**tcp**| **udp**} {*source-addr source-wildcard*| **any**| **host** *source-addr*} {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*| *port-match-criteria* {*destination-addr destination-wild-card*| **any**| **host** *dest-addr*}}

構文の説明

protocol	プロトコルの名前または番号。有効な値は、**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、、**tcp**、**pcp**、**pim**、**udp**、または IP プロトコル番号を表す 0 ～ 255 の範囲の整数です。任意のインターネットプロトコル（Internet Control Message Protocol（ICMP）、TCP、User Datagram Protocol（UDP）など）に一致するには、キーワード **ip** を使用します。その他の修飾子については、「使用上のガイドライン」を参照してください。
source-addr	（オプション）10 進表記の 4 つの部分をドットで区切った 32 ビット数として送信されるパケットの送信元ネットワークまたはホストの番号。
source-wildcard	（オプション）送信元に適用されるワイルドカード ビット。これは、10 進数の 4 つの部分をドットで区切ったものです。無視するビット位置に 1 を入れます。

any	送信元ホストまたは宛先ホストを、*source-addr* または *destination-addr value*、および *source-wildcard* または *destination-wildcard* の値（0.0.0.0 255.255.255.255）の短縮形として指定します。
host *address name*	1 つのホストの送信元アドレスまたは宛先アドレスおよび名前を指定します。
destination-addr	10 進表記の 4 つの部分をドットで区切った 32 ビット数として送信されるパケットの宛先ネットワークまたはホストの番号。
destination-wildcard	宛先に適用されるワイルドカードビット。これは、10 進数の 4 つの部分をドットで区切った 32 ビット数です。無視するビット位置に 1 を入れます。
dscp *dscp-value*	（オプション）特定の DiffServ コードポイント（DSCP）値が設定されているパケットと一致します。有効な値については、「使用上のガイドライン」を参照してください。
precedence *precedence-value*	（オプション）パケットの優先フィルタ レベルを指定します。有効な値は 0 ～ 7 の番号または名前です。有効な名前のリストについては、「使用上のガイドライン」を参照してください。
fragments *fragment-value*	（オプション）アクセス リスト エントリがパケットの先頭以外のフラグメントに適用され、フラグメントは許可または拒否されます。**fragments** キーワードの詳細については、「使用上のガイドライン」の「フラグメント」の「フラグメントのアクセス リストまたは OGACL 処理」と「フラグメントおよびポリシー ルーティング」を参照してください。
option *option-value*	（オプション）特定の IP オプション値番号を含むパケットに一致します。有効な値については、「使用上のガイドライン」を参照してください。
reflect *access-list-name*	（オプション）再帰的なアクセス リスト エントリを作成します。

time-range *time-range-value*	（オプション）時間範囲エントリ名を指定します。
ttl *match-value ttl-value*	（オプション）特定のTTL値を含むパケットに一致します。有効な値については、「使用上のガイドライン」を参照してください。
tos *tos-value*	（オプション）パケットのサービスフィルタリング レベルを指定します。有効な値は 0 ～ 15 の番号、または **access-list**（IP 拡張）コマンドの「使用上のガイドライン」にリストされている名前です。
timeout *max-time*	再帰 ACL の最大存続期間を指定します。有効な値は 1 ～ 2147483 秒です。

log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記録されるメッセージのレベルは **loggingconsole** コマンドで制御します）。 標準リストのメッセージには、アクセス リスト番号、パケットの許可/拒否、送信元アドレス、およびパケット数が含まれます。 拡張リストのメッセージには、アクセス リスト番号、パケットの許可/拒否、プロトコル（TCP、UDP、ICMP、または番号）が含まれます。また該当する場合には、送信元アドレスと宛先アドレス、ポート番号、およびユーザ定義 Cookie またはルータ生成ハッシュ値が含まれます。 標準リストと拡張リストの両方で、一致した最初のパケットに関するメッセージが生成され、その後 5 分間隔で、前の 5 分間で許可または拒否されたパケット数を含むメッセージが生成されます。 ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作により、ロギング パケットが多すぎるためにルータがリロードすることが防止されます。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。 **log** キーワード（および関連する *word* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。

log-value	（オプション）ログ メッセージに付加されるユーザ定義 Cookie。Cookie の条件は次のとおりです。 • 文字以内である必要があります。 • 16 進表記（0x など）で始めることはできません。 • **reflect**、**fragment** といったキーワードと同じであることはできません。また、これらのキーワードの一部を使用することはできません。 **time-range** • 英数字のみを使用する必要があります。 ユーザ定義 Cookie はアクセス コントロール エントリ（ACE）syslog エントリに付加され、アクセス コントロール リストでその syslog エントリを生成した ACE を一意に識別します。
log-input *log-input-value*	（オプション）このエントリ（入力インターフェイスなど）とログを照合します。 **log-input** キーワード（および関連する *log-input-value* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。
tcp	TCP プロトコルを指定します。
udp	UDP プロトコルを指定します。
port-match-criteria port-number	特定のポート番号を含むパケットのみに一致します。有効な値については、「使用上のガイドライン」を参照してください。

コマンド デフォルト　アクセス リストでパケットが許可される特定の条件はありません。

コマンド モード　標準アクセス リスト コンフィギュレーション（config-std-nacl） 拡張アクセス リスト コンフィギュレーション（config-ext-nacl）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.4(22)T	**log** キーワードと **log-input** キーワードに *word* 引数が追加されました。

使用上のガイドライン

パケットがアクセス リストで許可される条件を定義するには、**ipaccess-list** コマンドの後にこのコマンドを使用します。

Cisco IOS 15.0(1)M 以降のリリースでは、**permitipanyanylog** コマンドからログ エントリを削除するには **permitipanyany** コマンドを使用します。

Cisco IOS リリース 15.0(1)M より前のリリースでは、**log** オプションを **permitipanyanylog** コマンドから削除するには、**nopermitipanyanylog** コマンドと **permitipanyany** コマンドを使用します。

Cisco IOS リリース 15.0(1) M 以降のリリースでは、ログ エントリとユーザ定義 Cookie を削除するには **permitipanyany** [*log-value*] コマンドを使用します。

Cisco IOS リリース 15.0(1)M より前のリリースでは、ログ エントリとユーザ定義 Cookie を削除するには、**nopermitipanyanylog** [*log-value*] コマンドと **permitipanyany** コマンドを使用します。

フラグメントのアクセス リストまたは OGACL 処理

fragments キーワードを使用する場合と使用しない場合のアクセス リスト エントリの動作について、次の表で説明します。

表 *1*：フラグメントのアクセス リストまたは *OGACL* 処理

アクセス リスト エントリの状態...	結果

fragments キーワードが指定されておらず（デフォルトの動作）、すべてのアクセス リスト エントリ情報が一致している。	アクセス リスト エントリにレイヤ 3 情報のみが含まれている場合：
	• エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	
	アクセス リスト エントリにレイヤ 3 情報とレイヤ 4 情報が含まれている場合：
	• エントリは、非フラグメント パケットと先頭のフラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。先頭以外のフラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、先頭以外のフラグメントが許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

アクセス リスト エントリの状態...	結果
fragments キーワードが指定され、すべてのアクセス リスト エントリ情報が一致している	（注） アクセス リスト エントリは、先頭以外のフラグメントにのみ適用されます。レイヤ 4 情報を含むアクセス リスト エントリには **fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加しないでください。これは、IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。先頭フラグメントは、アクセス リストの **fragments** キーワードが設定されている **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリで許可または拒否されるまで、次のアクセス リスト エントリとの比較が続行されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには **fragments** キーワードは含まれず、このエントリは先頭フラグメントに適用されます。ペアの 2 番目の **deny** エントリは、**fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対する複数の **deny** アクセス リスト エントリがあるが、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

（注） アクセス リストおよび IP フラグメントに関するあらゆるケースを **fragments** キーワードで解決できるわけではありません。

フラグメントおよびポリシー ルーティング

ポリシー ルーティングが **matchipaddres** コマンドに基づくものであり、アクセス リストのエントリがレイヤ 4 ～ レイヤ 7 の情報に一致した場合、フラグメンテーションとフラグメント制御機能はポリシー ルーティングに影響を及ぼします。先頭フラグメントがポリシー ルーティングされなかった場合でも、先頭以外のフラグメントがアクセス リストを通過し、ポリシー ルーティングされることがあります。その逆もまた同じです。

前に説明したようにアクセス リスト エントリに **fragments** キーワードを使用すると、先頭フラグメントと先頭以外のフラグメントに対するアクションの照合を改善できるため、ポリシー ルーティングが想定どおりに機能する可能性が高くなります。

source-addr 引数と *destination-addr* 引数を使用すると、送信元グループと宛先グループを作成できます。次のキーワードおよび引数を使用できます。

- **dscp** *dscp-value*：（オプション）特定の DSCP 値を含むパケットと一致します。有効な値は次のとおりです。

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

- **fragments** ：（オプション）先頭以外のフラグメントをチェックします。前述の表を参照してください。
- **log** ：（オプション）このエントリとの一致をログに記録します。
- **log-input**（オプション）このエントリとの一致をログに記録します（入力インターフェイスなど）。
- **option** *option-value*：（オプション）特定の IP オプション値が設定されているパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 255：IP オプションの値。
  - **add-ext**：Address Extension Option（147）が設定されているパケットと一致します。

- **any-options**：任意のオプションが設定されているパケットと一致します。
- **com-security**：Commercial Security Option（134）が設定されているパケットと一致します。
- **dps**：Dynamic Packet State Option（151）が設定されているパケットと一致します。
- **encode**：Encode Option（15）が設定されているパケットと一致します。
- **eool**：End of Options（0）が設定されているパケットと一致します。
- **ext-ip**：Extended IP Option（145）が設定されているパケットと一致します。
- **ext-security**：Extended Security Option（133）が設定されているパケットと一致します。
- **finn**：Experimental Flow Control Option（205）が設定されているパケットと一致します。
- **imitd**：IMI Traffic Descriptor Option（144）が設定されているパケットと一致します。
- **lsr**：Loose Source Route Option（131）が設定されているパケットと一致します。
- **match-all**：指定されたフラグがすべて存在する場合にパケットと一致します。
- **match-any**：指定されたいずれかのフラグが存在する場合にパケットと一致します。
- **mtup**：MTU Probe Option（11）が設定されているパケットと一致します。
- **mtur**：MTU Reply Option（12）が設定されているパケットと一致します。
- **no-op**：No Operation Option（1）が設定されているパケットと一致します。
- **psh**：PSH ビットが設定されているパケットと一致します。
- **nsapa**：NSAP Addresses Option（150）が設定されているパケットと一致します。
- **reflect**：再帰的なアクセス リスト エントリを作成します。
- **record-route**：Record Route Option（7）が設定されているパケットと一致します。
- **rst**：RST ビットが設定されているパケットと一致します。
- **router-alert**：Router Alert Option（148）が設定されているパケットと一致します。
- **sdb**：Selective Directed Broadcast Option（149）が設定されているパケットと一致します。
- **security**：Basic Security Option（130）が設定されているパケットと一致します。
- **ssr**：Strict Source Route Option（137）が設定されているパケットと一致します。
- **stream-id**：Stream ID Option（136）が設定されているパケットと一致します。
- **syn**：SYN ビットが設定されているパケットと一致します。
- **timestamp**：Time Stamp Option（68）が設定されているパケットと一致します。
- **traceroute**：Trace Route Option（82）が設定されているパケットと一致します。
- **ump**：Upstream Multicast Packet Option（152）が設定されているパケットと一致します。

- **visa**：Experimental Access Control Option（142）が設定されているパケットと一致します。
- **zsu**：Experimental Measurement Option（10）が設定されているパケットと一致します。

- **precedence** *precedence-value*：（オプション）特定の precedence 値を持つパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 7：precedence 値。
  - **critical**：critical precedence（5）が設定されているパケットと一致します。
  - **flash**：flash precedence（3）が設定されているパケットと一致します。
  - **flash-override**：flash override precedence（4）が設定されているパケットと一致します。
  - **immediate**：immediate precedence（2）が設定されているパケットと一致します。
  - **internet**：internetwork control precedence（6）が設定されているパケットと一致します。
  - **network**：network control precedence（7）が設定されているパケットと一致します。
  - **priority**：priority precedence（1）が設定されているパケットと一致します。
  - **routine**：routine precedence（0）が設定されているパケットと一致します。
- **reflectacl-name** ：（オプション）再帰的なアクセス リスト エントリを作成します。
- **ttl** *match-value ttl-value*：（オプション）特定の TTL 値が設定されているパケットとの一致を指定します。有効な値は次のとおりです。
  - **eq**：指定された TTL 値が設定されているパケットと一致します。
  - **gt**：より大きい TTL 値が設定されているパケットと一致します。
  - **lt**：より小さい TTL 値が設定されているパケットと一致します。
  - **neq**：指定された TTL 値が設定されていないパケットと一致します。
  - **range**--TTL の範囲内のパケットと一致します。
- **time-range** *time-range-value*：（オプション）時間範囲エントリ名を指定します。
- **tos** ：指定された ToS 値を持つパケットと一致します。有効な値は次のとおりです。
  - 0 ～ 15：タイプ オブ サービス（ToS）値。
  - **max-reliability**：maximum reliable ToS（2）が設定されているパケットと一致します。
  - **max-throughput**：maximum throughput ToS（4）が設定されているパケットと一致します。
  - **min-delay**：minimum delay ToS（8）が設定されているパケットと一致します。
  - **min-monetary-cost**：minimum monetary cost ToS（1）が設定されているパケットと一致します。

- **normal**：normal ToS（0）が設定されているパケットと一致します。
- **timeout** *max-time*：（オプション）再帰 ACL の最大存続期間を指定します。有効な値は 1 ～ 2147483 秒です。

関連コマンド

Command	Description
deny	パケットを拒否する名前付き IP アクセス リストまたは OGACL の条件を設定します。
ipaccess-group	ACL または OGACL をインターフェイスまたはサービス ポリシー マップに適用します。
ipaccess-list	IP アクセス リストまたは OGACL を名前または番号で定義します。
ipaccess-listlogginghash-generation	ACE syslog エントリのハッシュ値の生成を有効にします。
showipaccess-list	IP アクセス リストまたは OGACL の内容を表示します。

permit (IP)

パケットが名前付き IP アクセス リストで許可される条件を設定するには、アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **permit** *source* [*source-wildcard*]

[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

no *sequence-number*

no permit *source* [*source-wildcard*]

no permit *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

インターネット制御メッセージ プロトコル（**ICMP**）

[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

インターネット グループ管理プロトコル（**IGMP**）

[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

伝送制御プロトコル（**TCP**）

[sequence-number] permit tcp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any**| **match-all**} {+-} *flag-name*| **precedence** *precedence*| **tos** *tos*| **ttl** *operator value*| **log**| **time-range** *time-range-name*| **fragments**| **log** | [*user-defined-cookie*]]

ユーザ データグラム プロトコル（**UDP**）

[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**time-range** *time-range-name*] **[fragments]** [**log** [*user-defined-cookie*]]

構文の説明

sequence-number	（オプション）permit ステートメントに割り当てられているシーケンス番号。システムはこのシーケンス番号に基づいて、ステートメントをアクセス リストのその番号の位置に挿入します。

source	パケットの送信元のネットワークまたはホストの番号。送信元を指定する場合、代わりに次の 3 つの方法を使用できます。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host** *source* を、*source* および *source* の *source-wildcard*（0.0.0.0）の短縮形として使用します。
source-wildcard	（オプション）送信元に適用されるワイルドカードビット。送信元のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。無視するビット位置には 1 を設定します。 • **any** キーワードを、*source* および *source-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host** *source* を、*source* および *source* の *source-wildcard*（0.0.0.0）の短縮形として使用します。

protocol	インターネットプロトコルの名前または番号。*protocol* 引数には、キーワード **eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **udp** のいずれか、あるいはインターネットプロトコル番号を表す 0 ～ 255 の範囲内の整数を設定できます。任意のインターネットプロトコル（ICMP、TCP、UDP など）と一致させるには、**ip** キーワードを使用します。 （注） **icmp**、**igmp**、**tcp,**および **udp** キーワードを入力するときには、**permit** コマンドの ICMP、IGMP、TCP、および UDP 形式で示されている特定のコマンド構文に従う必要があります。 （注） BGP トラフィックを許可するようにパケット フィルタを設定するには、プロトコル **tcp** を使用し、ポート番号 179 または bgp を指定します。 **bgp**
destination	パケットの宛先のネットワークまたはホストの番号。宛先を指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。 • **any** キーワードを、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host** *destination* を、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。

destination-wildcard	宛先に適用されるワイルドカードビット。宛先のワイルドカードを指定するには、次の 3 つの方法から選択します。 • 32 ビットの 4 分割ドット付き 10 進表記を使用する。無視するビット位置には 1 を設定します。 • **any** キーワードを、*destination* および *destination-wildcard*（0.0.0.0 255.255.255.255）の短縮形として使用します。 • **host** *destination* を、*destination* および *destination* の *destination-wildcard*（0.0.0.0）の短縮形として使用します。
option *option-name*	（オプション）パケットは IP オプション（0 ～ 255 の番号で指定）または対応する IP オプション名（「使用上のガイドライン」の表に記載）に基づいてフィルタリングできます。
precedence *precedence*	（オプション）パケットは、優先レベル（0 ～ 7 の番号で指定）または名前でフィルタリングできます。
tos *tos*	（オプション）パケットは、タイプ オブ サービス（ToS）レベル（0 ～ 15 の番号で指定）または名前（**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載）に基づいてフィルタリングできます。

ttl *operator-value*	（オプション）この **permit** ステートメントに指定されている TTL 値とパケットの TTL 値を比較します。 • *operator* は **lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、または **range**（包含範囲）のいずれかです。 • *value* は 0 ～ 255 の範囲で指定します。 • 演算子が **range** の場合、2 つの値を 1 つのスペースで区切って指定します。 • リリース 12.0S では、演算子が **eq** または **neq** の場合、1 つの TTL 値だけを指定できます。 • その他のすべてのリリースでは、演算子が **eq** または **neq** の場合、最大 10 個の TTL 値をスペースで区切って指定できます。
time-range *time-range-name*	（オプション）この **permit** ステートメントに適用する時間範囲の名前。時間範囲の名前は **time-range** コマンドにより指定され、時間範囲の制約は **absolute** または **periodic** コマンドにより指定されます。
fragments	（オプション）アクセス リスト エントリがパケットの先頭以外のフラグメントに適用され、フラグメントが許可または拒否されます。**fragments** キーワードの詳細については、「使用上のガイドライン」の「フラグメント」および「フラグメントおよびポリシー ルーティング」の「フラグメントのアクセスリスト処理」を参照してください。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記録されるメッセージのレベルは **loggingconsole** コマンドで制御します）。 **log** キーワード（および関連する *word* 引数）を指定した場合、このコマンドではその他のキーワードや設定は指定できません。

user-defined-cookie	（オプション）ログ メッセージに付加されるユーザ定義 Cookie。Cookie の条件は次のとおりです。 • 64 文字以内である必要があります。 • 16 進表記（0x など）で始めることはできません。 • **fragment,reflect** といったキーワードと同じであることはできません。また、これらのキーワードの一部を使用することはできません。 **time-range.** • 英数字のみを使用する必要があります。 ユーザ定義 Cookie は Allegro Crypto Engine（ACE）syslog エントリに付加され、アクセス コントロール リスト内でその syslog エントリを生成した ACE を一意に識別します。
icmp	ICMP パケットだけを許可します。**icmp** キーワードを入力するときには、**permit** コマンドの ICMP 形式で示されている特定のコマンド構文を使用する必要があります。
icmp-type	（オプション）ICMP パケットは、ICMP メッセージタイプでフィルタリングできます。メッセージ タイプの番号は 0 ～ 255 です。
icmp-code	（オプション）ICMP メッセージ タイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（オプション）ICMP パケットは、ICMP メッセージ タイプ名、または ICMP メッセージ タイプとコード名によってフィルタリングできます。有効な名前は、**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載されています。
igmp	IGMP パケットだけを許可します。**igmp** キーワードを入力するときには、**permit** コマンドの IGMP 形式で示されている特定のコマンド構文を使用する必要があります。

igmp-type	（オプション）IGMP パケットは、IGMP メッセージタイプまたはメッセージ名でフィルタリングできます。メッセージタイプの番号は 0 ～ 15 です。IGMP メッセージ名は、**access-list**（IP extended）コマンドの「使用上のガイドライン」に記載されています。
tcp	TCP パケットだけを許可します。**tcp** キーワードを入力するときには、**permit** コマンドの TCP 形式で示されている特定のコマンド構文を使用する必要があります。
operator	（オプション）発信元ポートまたは宛先ポートを比較します。演算子は **eq**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、および **range**（包含範囲）です。 演算子が source および source-wildcard 引数の後にある場合、送信元ポートに一致する必要があります。演算子が destination および destination-wildcard 引数の後にある場合、宛先ポートに一致する必要があります。 range 演算子には 2 つのポート番号が必要です。**eq**（等しい）および **neq**（等しくない）演算子に対し、最大 10 個のポート番号を入力できます。他のすべての演算子は 1 つのポート番号が必要です。
port	（オプション）TCP または UDP ポートの 10 進数の番号または名前。ポート番号の範囲は 0 ～ 65535 です。TCP ポート名と UDP ポート名は、**access-list(IPextended)** コマンドの「使用上のガイドライン」に記載されています。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
established	（任意）TCP プロトコルの場合にだけ、確立された接続を表示します。TCP データグラムに ACK または RST ビットが設定されている場合に一致します。接続するための初期 TCP データグラムの場合は照合しません。

match-any | **match-all**	（オプション）TCP プロトコルのみ：TCP データグラムで特定の TCP フラグの設定の有無に関係なく、一致します。指定した TCP フラグのいずれかが存在している場合に一致するようにするには、**match-any** キーワードを使用します。あるいは、指定した TCP フラグがすべて存在している場合に一致するようにするには、**match-all** キーワードを使用します。1 つ以上の TCP フラグを一致基準として使用するには、**match-any** および **match-all** キーワードの後に、**+** または **-** キーワードと *flag-name* 引数を指定する必要があります。
+ | **-** *flag-name*	（オプション）TCP プロトコルのみ：**+** キーワードを使用する場合、*flag-name* 引数に指定した TCP フラグが TCP ヘッダーに含まれている IP パケットが一致します。**-** キーワードを使用する場合、*flag-name* 引数に指定した TCP フラグが含まれていない IP パケットが一致します。**+** キーワードと **-** キーワードの後には *flag-name* 引数を指定する必要があります。TCP フラグ名は、TCP をフィルタリングする場合に限り使用できます。TCP フラグのフラグ名は、**ack**、**fin**、**psh**、**rst**、**syn**、および **urg** です。
udp	UDP パケットだけを許可します。**udp** キーワードを入力するときには、**permit** コマンドの UDP 形式で示されている特定のコマンド構文を使用する必要があります。

コマンド デフォルト

名前付きアクセス リストでパケットが許可される特定の条件はありません。

コマンド モード

アクセス リスト コンフィギュレーション（config-ext-nacl）

コマンド履歴

リリース	変更内容
11.2	このコマンドが導入されました。
12.0(1)T	**time-range** *time-range-name* キーワードおよび引数が追加されました。

リリース	変更内容
12.0(11)	**fragments** キーワードが追加されました。
12.2(13)T	Cisco IOS ソフトウェアで IGRP プロトコルが使用できなくなったため、igrp キーワードは削除されました。
12.2(14)S	*sequence-number* 引数が追加されました。
12.2(15)T	*sequence-number* 引数が追加されました。
12.3(4)T	**option** *option-name* キーワードおよび引数が追加されました。**match-any**、**match-all,+,**、および **-** キーワードと *flag-name* 引数が追加されました。
12.3(7)T	コマンド機能が変更され、**eq** 演算子と **neq** 演算子の後に最大 10 個のポート番号を追加できるようになりました。これにより、連続しないポートを使用してアクセス リスト エントリを作成できます。
12.4	**drip** キーワードが追加されました。このキーワードでは、Optimized Edge Routing（OER）通信に使用する TCP ポート番号を指定できます。
12.4(2)T	**ttl** *operator value* キーワードおよび引数が追加されました。
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(22)T	**log** キーワードに *word* 引数が追加されました。
Cisco IOS XE リリース 3.2	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 ルータに実装されました。

使用上のガイドライン

パケットが名前付きアクセス リストで許可される条件を定義するには、**ipaccess-list** コマンドの後に **permit** コマンドを使用します。

（注） Cisco IOS XE では、**permit** コマンドを使用して、ユーザがネットワークにアクセスするための包含ポート範囲を拡張 ACL で照合することはできません。

time-range キーワードでは、時間範囲を名前で指定できます。**time-range**、**absolute**、および **periodic** コマンドは、この **permit** ステートメントが有効になる時点を指定します。

log キーワード

ログ メッセージには、アクセス リスト番号またはアクセス リスト名、パケットの許可/拒否、プロトコル（TCP、UDP、ICMP、または番号）が含まれます。また該当する場合には、送信元アドレスと宛先アドレス、ポート番号、およびユーザ定義 Cookie またはルータ生成ハッシュ値も含まれます。一致した最初のパケットに関するメッセージが生成され、その後 5 分間隔で、前の 5 分間で許可または拒否されたパケット数を含むメッセージが生成されます。

5 分間の間隔が経過するまで待たずに、一致の数が設定可能なしきい値に到達した場合にロギング メッセージを生成するには、**ipaccess-listlog-update** コマンドを使用します。詳細については、**ipaccess-listlog-update** コマンドを参照してください。

ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作により、ロギング パケットが多すぎるためにルータがリロードすることが防止されます。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。

シスコ エクスプレス フォワーディングをイネーブルにしてから、**log** キーワードを使用するアクセス リストを作成した場合、アクセス リストと一致するパケットは、シスコ エクスプレス フォワーディングで交換されたものではありません。これらはファーストスイッチングで交換されたものです。ロギングにより、Cisco Express Forwarding が無効になります。

IP オプションのアクセス リスト フィルタリング

アクセス コントロール リストを使用して IP オプションを含むパケットをフィルタリングできます。これにより、IP オプションを含む偽のパケットでルータがいっぱいになることが防がれます。現在使用されていない IP オプションを含むすべての IP オプションが記載されている表を参照するには、Internet Assigned Numbers Authority（IANA）の最新情報（www.iana.org）を参照してください。

Cisco IOS ソフトウェアでは、パケットに 1 つ以上の正当な IP オプションが含まれているかどうかに基づいてパケットをフィルタリングできます。このためには、次の表に示すように、*option-name* 引数に IP オプション値または対応する名前を入力します。

表 *2*：*IP* オプションの値と名前

IP オプションの値と名前	説明
0 ～ 255	IP オプションの値。
add-ext	Address Extension Option（147）が設定されているパケットと一致します。
any-options	任意の IP オプションが設定されているパケットと一致します。

IP オプションの値と名前	説明
com-security	Commercial Security Option（134）が設定されているパケットと一致します。
dps	Dynamic Packet State Option（151）が設定されているパケットと一致します。
encode	Encode Option（15）が設定されているパケットと一致します。
eool	End of Options（0）が設定されているパケットと一致します。
ext-ip	Extended IP Options（145）が設定されているパケットと一致します。
ext-security	Extended Security Option（133）が設定されているパケットと一致します。
finn	Experimental Flow Control Option（205）が設定されているパケットと一致します。
imitd	IMI Traffic Descriptor Option（144）が設定されているパケットと一致します。
lsr	Loose Source Route Option（131）が設定されているパケットと一致します。
mtup	MTU Probe Option（11）が設定されているパケットと一致します。
mtur	MTU Reply Option（12）が設定されているパケットと一致します。
no-op	No Operation Option（1）が設定されているパケットと一致します。
nsapa	NSAP Addresses Option（150）が設定されているパケットと一致します。
psh	PSH ビットが設定されているパケットと一致します。
record-route	Router Record Route Option（7）が設定されているパケットと一致します。

IP オプションの値と名前	説明
reflect	再帰的なアクセス リスト エントリを作成します。
router-alert	Router Alert Option（148）が設定されているパケットと一致します。
rst	RST ビットが設定されているパケットと一致します。
sdb	Selective Directed Broadcast Option（149）が設定されているパケットと一致します。
security	Base Security Option（130）が設定されているパケットと一致します。
ssr	Strict Source Routing Option（137）が設定されているパケットと一致します。
stream-id	Stream ID Option（136）が設定されているパケットと一致します。
syn	SYN ビットが設定されているパケットと一致します。
timestamp	Time Stamp Option（68）が設定されているパケットと一致します。
traceroute	Trace Route Option（82）が設定されているパケットと一致します。
ump	Upstream Multicast Packet Option（152）が設定されているパケットと一致します。
visa	Experimental Access Control Option（142）が設定されているパケットと一致します。
zsu	Experimental Measurement Option（10）が設定されているパケットと一致します。

TCP フラグに基づく IP パケットのフィルタリング

特定の TCP フラグ グループが設定されているパケットのみ、または設定されていないパケットのみを許可することで、不正な TCP パケットを検出およびドロップするように、アクセスリストを構成するアクセス リスト エントリを設定できます。フィルタリングする TCP パケットについて、

TCP フラグの任意の組み合わせを選択できます。ユーザは、設定されているフラグと設定されていないフラグに基づいて照合できるようにアクセスリストエントリを設定できます。キーワード **+** および **-** とフラグ名を使用して、TCP ヘッダー フラグが設定されているかどうかに基づいて一致が決定することを指定します。キーワード **match-any** と **match-all** を使用し、キーワード **+** または **-** と *flag-name* 引数で指定されているフラグの一部またはすべてが設定されている場合または設定されていない場合に、パケットを許可することを指定します。

Optimized Edge Routing（OER）通信の許可

OER が設定されているネットワークでパケット フィルタリングをサポートするため、**drip** キーワードが **tcp** キーワードに導入されました。**drip** キーワードは、OER が内部通信に使用するポート 3949 を指定します。このオプションを使用して、OER マスタ コントローラと境界ルータ間での通信を許可するパケット フィルタを作成できます。**drip** キーワードは、TCP 送信元アドレス、宛先アドレス、および **eq** 演算子の後に入力されます。「例」に記載されている例を参照してください。

フラグメントのアクセス リスト処理

fragments キーワードを使用する場合と、使用しない場合に関するアクセス リスト エントリの動作は、次のようにまとめることができます。

アクセス リスト エントリの状態...	結果...

fragments キーワードが指定されておらず（デフォルトの動作）、すべてのアクセス リスト エントリ情報が一致している。	レイヤ 3 情報だけを含むアクセス リスト エントリの場合、このエントリは非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	レイヤ 3 およびレイヤ 4 情報を含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケットと先頭フラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。非初期フラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、先頭以外のフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

fragments キーワードが指定され、すべてのアクセス リスト エントリ情報が一致している。	アクセス リスト エントリは、非初期フラグメントにのみ適用されます。レイヤ 4 情報を含むアクセスリスト エントリには、**fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加することはできません。IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。先頭フラグメントは、アクセス リストの **fragments** キーワードが設定された **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリによって許可または拒否されるまで、次のアクセス リスト エントリと比較されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには、**fragments** キーワードは含まれず、初期フラグメントに適用されます。ペアの 2 番目の **deny** エントリは、**fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対する複数の **deny** アクセス リスト エントリがあるが、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

（注） アクセス リストおよび IP フラグメントに関するあらゆるケースを **fragments** キーワードで解決できるわけではありません。

フラグメントおよびポリシー ルーティング

ポリシー ルーティングが **matchipaddress** コマンドに基づくものであり、アクセス リストのエントリがレイヤ 4 ～ レイヤ 7 の情報に一致した場合、フラグメンテーションとフラグメント制御機能はポリシー ルーティングに影響を及ぼします。先頭フラグメントがポリシー ルーティングされなかった場合でも、先頭以外のフラグメントがアクセス リストで許可され、ポリシー ルーティングされることがあります。

アクセス リスト エントリに **fragments** キーワードを指定すると、先頭フラグメントと先頭以外のフラグメントに対するアクションの照合を改善できるため、ポリシー ルーティングが想定どおりに機能する可能性が高くなります。

非隣接ポートを使用するアクセス リスト エントリの作成

Cisco IOS リリース 12.3(7)T 以降では、1 つのアクセス コントロール エントリに複数の非隣接ポートを指定できます。これにより、同一の送信元アドレス、宛先アドレス、プロトコルの必要なアクセス リスト エントリの数が大幅に削減されます。多数のアクセス リスト エントリを管理している場合は、可能であれば非隣接ポートを使用してこれらのエントリを統合することを推奨します。**eq** 演算子と **neq** 演算子の後に最大 10 個のポート番号を指定できます。

例

次に、Internetfilter という名前の標準アクセス リストの条件を設定する例を示します。

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied).
```

次に、月曜日、火曜日、金曜日の 9:00 a.m. から 5:00 p.m までの間に Telnet トラフィックを許可する例を示します。

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet0
 ip access-group legal in
```

次に、filter2 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、NSAP Addresses IP オプション（IP オプション値は nsapa）を含むパケットが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended filter2
 permit ip any any option nsapa
```

次に、kmdfilter1 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、RST IP フラグが設定されているパケットだけが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst
```

次に、kmdfilter1 という名前の拡張アクセス リストの許可条件を設定する例を示します。アクセス リスト エントリは、RST TCP フラグまたは FIN TCP フラグが設定されているパケットが名前付きアクセス リストで許可されることを指定します。

```
ip access-list extended kmdfilter1
 permit tcp any any match-any +rst +fin
```

次に、**show access-lists** コマンドを使用してアクセス リストを検証し、エントリを既存のアクセス リストに追加する例を示します。

```
Router# show access-lists
Standard IP access list 1
2 permit 10.0.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.255.255
10 permit 10.0.0.0, wildcard bits 0.0.255.255
20 permit 10.0.0.0, wildcard bits 0.0.255.255
ip access-list standard 1
 15 permit 10.0.0.0 0.0.255.255
```

次に、シーケンス番号が 20 のエントリをアクセス リストから削除する例を示します。

```
ip access-list standard 1
 no 20
!Verify that the list has been removed.
Router# show access-lists
Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.4.0.0, wildcard bits 0.0.0.255
```

次に、リストにすでに存在するエントリの重複エントリをユーザが入力すると、何も変更されない例を示します。ユーザが追加しようとしているエントリは、アクセス リストのシーケンス番号 20 のエントリと重複しています。

```
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.0.0.0 host 10.5.5.34
    20 permit icmp any any
```

```
    30 permit ip host 10.0.0.0 host 10.2.54.2
    40 permit ip host 10.0.0.0 host 10.3.32.3 log
ip access-list extended 101
 100 permit icmp any any
Router# show access-lists 101
Extended IP access list 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

次に、シーケンス番号20のエントリがすでにリストに存在しているために、ユーザがシーケンス番号 20 の新しいエントリを入力しようとすると発生する動作の例を示します。エラー メッセージが表示され、アクセス リストは変更されません。

```
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
ip access-lists extended 101
 20 permit udp host 10.1.1.1 host 10.2.2.2
%Duplicate sequence number.
Router# show access-lists 101
Extended IP access lists 101
    10 permit ip host 10.3.3.3 host 10.5.5.34
    20 permit icmp any any
    30 permit ip host 10.34.2.2 host 10.2.54.2
    40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

次に、非隣接ポートが設定されている 1 つのアクセス リスト エントリに統合可能ないくつかの **permit** ステートメントの例を示します。アクセス リスト aaa のアクセス リスト エントリのグループを表示するため、**showaccess-lists** コマンドが入力されます。

```
Router# show access-lists aaa
Extended IP access lists aaa
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

エントリはすべて同じ **permit** ステートメント用であり、ポートのみが異なるため、1 つの新しいアクセス リスト エントリに統合できます。次の例では、重複するアクセス リスト エントリを削除し、以前に表示されていたアクセス リスト エントリ グループを統合する新しいアクセス リスト エントリを作成します。

```
ip access-list extended aaa
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
```

次に、統合アクセス リスト エントリの作成例を示します。

```
Router# show access-lists aaa
Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 450 679
```

次のアクセス リストでは、TTL 値が 10 と 20 でタイプ オブ サービス（ToS）レベルが 3 の IP パケットをフィルタリングします。また、TTL が 154 を超える IP パケットをフィルタリングし、その規則を先頭以外のフラグメントにも適用します。フラッシュの優先レベルと 1 以外の TTL を持

つ IP パケットを許可し、そのようなパケットに関するログ メッセージをコンソールに送信します。他のすべてのパケットは拒否されます。

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

次に、すべての TCP 送信元と宛先に適用され、OER マスタ コントローラと境界ルータ間の通信を許可するパケット フィルタを設定する例を示します。

```
ip access-list extended 100
 permit any any tcp eq drip
 exit
```

次に、filter_logging という名前の拡張アクセス リストの許可条件を設定する例を示します。このアクセス リスト エントリは、TCP プロトコル タイプで宛先ホストが 10.5.5.5 であるパケットだけが名前付きアクセス リストで許可され、その他のパケットはすべて拒否されることを指定します。また、ロギング メカニズムが有効になり、ユーザ定義 Cookie（Permit_tcp_to_10.5.5.5 または Deny_all）が適切な syslog エントリに付加されます。

```
ip access-list extended filter_logging
 permit tcp any host 10.5.5.5 log Permit_tcp_to_10.5.5.5
 deny ip any any log Deny_all
```

次に、すべての TCP 送信元と宛先に適用され、インバウンドおよびアウトバウンド BGP トラフィックを許可するパケット フィルタを設定する例を示します。

```
ip access-list extended 100
 permit tcp any eq bgp any eq bgp
```

関連コマンド

Command	Description
absolute	時間範囲が有効なときの絶対時間を指定します。
access-list(IPextended)	拡張 IP アクセス リストを定義します。
access-list(IPstandard)	標準 IP アクセス リストを定義します。
deny(IP)	パケットが名前付き IP アクセス リストで許可されない条件を設定します。
ipaccess-group	インターフェイスへのアクセスを制御します。
ipaccess-listlog-update	ロギング メッセージが生成される条件となるパケット数のしきい値を設定します。
ipaccess-listlogginghash-generation	ACE syslog エントリのハッシュ値の生成を有効にします。

Command	Description
ipaccess-listresequence	アクセス リストのアクセス リスト エントリにシーケンス番号を適用します。
ipoptions	ルータに送信された IP オプション パケットをドロップまたは無視します。
loggingconsole	システム ロギング（syslog）メッセージがすべての使用可能な TTY 回線に送信され、重大度に応じてメッセージが制限されます。
matchipaddress	標準アクセス リストまたは拡張アクセス リストで許可された宛先ネットワーク番号アドレスを含むすべてのルートを配するか、またはパケットに対してポリシー ルーティングを実行します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
showaccess-lists	アクセスリスト エントリ グループを表示します。
showipaccess-list	現在のすべての IP アクセス リストの内容を表示します。
time-range	アクセス リストまたはその他の機能が有効になる時点を指定します。

port

デバイスが設定されている RADIUS クライアントからの RADIUS 要求をリッスンするポートを指定するには、ダイナミック認証ローカル サーバ コンフィギュレーション モードで **port** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

port *port-number*

no port *port-number*

構文の説明

port-number	ポート番号。デフォルト値は、ポート 1700 です。

コマンド デフォルト

デバイスはデフォルト ポート（ポート 1700）で RADIUS 要求をリッスンします。

コマンド モード

ダイナミック認証サーバ コンフィギュレーション（config-locsvr-da-radius）

コマンド履歴

リリース	変更内容
12.2(28)SB	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

外部ポリシー サーバがルータにアップデートを動的に送信できるようにデバイス（ルータなど）を設定できるようになりました。この機能は CoA RADIUS 拡張により可能になりました。CoA によりピアツーピア機能が RADIUS に導入されました。この機能により、ルータと外部ポリシー サーバがそれぞれ RADIUS クライアントとサーバとして動作できます。ルータが RADIUS クライアントからの要求をリッスンするポートを指定するには、**port** コマンドを使用します。

例

次の例では、デバイスが RADIUS 要求をリッスンするポートとしてポート 1650 が指定されます。

```
aaa server radius dynamic-author
 client 10.0.0.1
 port 1650
```

関連コマンド

コマンド	説明
aaaserverradiusdynamic-author	デバイスを AAA サーバとして設定し、外部ポリシー サーバとの連携を容易にします。

port (TACACS+)

TACACS+ 接続に使用する TCP ポートを指定するには、TACACS+ サーバ コンフィギュレーション モードで **port** コマンドを使用します。TCP ポートを削除するには、このコマンドの **no** 形式を使用します。

port [*number*]

no port [*number*]

構文の説明

number	（オプション）TACACS+ サーバが Access-Request パケットの受信に使用するポートを指定します。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

ポートを設定しなかった場合は、ポート 49 が使用されます。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

port コマンドを使用するときに *number* 引数を使用しないと、TCP ポート 49 が使用されます。

例

次に、TCP ポート 12 を指定する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# port 12
```

関連コマンド

Command	Description
tacacsserver	TACACS+ サーバを IPv6 または IPv4 に対して設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。

ppp accounting ～ quit

プライマリ

指定されたトラストポイントをルータのプライマリ トラストポイントとして割り当てるには、ca-trustpoint コンフィギュレーション モードで **primary** コマンドを使用します。

primary *name*

構文の説明

name	ルータのプライマリ トラストポイントの名前。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

CA トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。
12.2(18)SXD	このコマンドが、Cisco IOS リリース 12.2(18)SXD 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。

使用上のガイドライン

特定のトラストポイントをプライマリとして指定するには、primary コマンドを使用します。

このコマンドを設定する前に、トラストポイントを定義して ca-trustpoint コンフィギュレーション モードを開始する **crypto ca trustpoint** コマンドを有効にしておく必要があります。

例

次に、トラストポイント「ka」をプライマリ トラストポイントとして設定する例を示します。

```
cr
ypto ca trustpoint ka
 enrollment url http://xxx
 primary
 crl option
al
```

関連コマンド

コマンド	説明
cryptocatrustpoint	ルータが使用する必要のある CA を宣言します。

privilege level

回線のデフォルト権限レベルを設定するには、ライン コンフィギュレーション モードで **privilege level** コマンドを使用します。回線のデフォルト ユーザ権限レベルに戻すには、このコマンドの **no** 形式を使用します。

privilege level *level*

no privilege level

構文の説明

level	指定された回線に関連付けられている権限レベル。

コマンド デフォルト

レベル 15 は、イネーブル パスワードによって許可されるアクセス レベルです。

レベル 1 は、通常の EXEC モード ユーザ権限です。

コマンド モード

ライン コンフィギュレーション

コマンド履歴

リリース	変更内容
10.3	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 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

ユーザは、回線にログインし、別の権限レベルを有効にすることで、このコマンドを使用して設定した権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっていれば、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。

特定のユーザまたは回線に対するコマンドのサブセットを指定するには、レベル 0 を使用できます。たとえば、ユーザ「guest」に対し **show users** コマンドと **exit** コマンドだけを使用することを許可できます。

回線の使用を制限するには、コンソール回線に高い権限レベルを指定してください。

（注） Cisco IOS リリース 12.2SXI 以前は、Webauth（Web 認証）を正常に実行するためには Access Control System（ACS）で権限レベル 15 を設定する必要がありました。このリリースより後では、ACS の権限設定は必須ではなくなりました。

（注） **privilege level** コマンドでは一部の CLI コマンドがサポートされていません。たとえば、**router bgp** や **default interface** などのコマンドには権限レベルを関連付けることができません。グローバル コンフィギュレーション CLI では、これらのサポートされていないコマンドに対する権限レベルの割り当てが許可されますが、これらのコマンドはルータの実行設定の一部にはなりません。

例

次の例では、補助回線での権限レベル 5 の設定が示されています。補助回線を使用するすべてのユーザには、デフォルトで権限レベル 5 が割り当てられます。

```
line aux 0
 privilege level 5
```

次の例では、すべての **show ip** コマンド（すべての **show** コマンドを含む）を権限レベル 7 に設定します。

```
privilege exec level 7 show ip route
```

これは、次のコマンドと同等です。

```
privilege exec level 7 show
```

次の例では、**show ip route** コマンドをレベル 7 に設定し、**show ip** コマンドをレベル 1 に設定します。

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

関連コマンド

Command	Description
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。

radius attribute nas-port-type ～ rd

radius-server attribute nas-port format

RADIUS アカウンティング機能に使用する NAS-Port 形式を設定し、デフォルトの NAS-port 形式を復元する場合、またはグローバル属性 61 セッション フォーマット e 文字列を設定するか、属性 61 サポートのための特定のサービス ポート タイプを設定する場合には、グローバル コンフィギュレーション モードで **radius-serverattributenas-portformat** コマンドを使用します。RADIUS サーバへの 属性 61 の送信を停止するには、このコマンドの **no** 形式を使用します。

RADIUS アカウンティング機能の NAS-Port およびデフォルト NAS-Port 形式の復元

radius-server attribute nas-port format 形式

no radius-server attribute nas-port format 形式

拡張 NAS-Port サポート

radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

no radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

構文の説明

形式	NAS-Port 形式。format 引数の有効な値は次のとおりです。 • a--標準 NAS-Port 形式。 • b--拡張 NAS-Port 形式。 • c：キャリア ベースの形式 • d：PPPoX（PPP over Ethernet または PPP over ATM）拡張 NAS-Port 形式 • e：設定可能な NAS-Port 形式。
string	（オプション）フォーマット e の特定ポート タイプをすべて表します。この引数には複数の値を指定できます。

type *nas-port-type*	（オプション）特定の物理ポートタイプを表すさまざまなフォーマット文字列をグローバルに指定できます。 いずれかの拡張 NAS-Port-Type 属性値を設定できます。 • **type30** ：PPP over ATM（PPPoA） • **type31** ：PPP over Ethernet（PPPoE）over ATM（PPPoEoA） • **type32** ：PPPoE over Ethernet（PPPoEoE） • **type33** ：PPPoE over VLAN（PPPoEoVLAN） • **type34** ：PPPoE over Q-in-Q（PPPoEoQinQ）

コマンド デフォルト

RADIUS アカウンティング機能の NAS-Port の標準 NAS-Port 形式と、デフォルト NAS-Port 形式または拡張 NAS-Port サポートの復元。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3(7)T	このコマンドが導入されました。
11.3(9)DB	PPP 拡張 NAS-Port 形式が追加されました。
12.1(5)T	PPP 拡張 NAS-Port 形式が拡張され、PPPoE over ATM と PPPoE over IEEE 802.1Q VLAN がサポートされました。
12.2(4)T	フォーマット e が導入されました。
12.2(11)T	フォーマット e が拡張され、PPPoX 情報がサポートされました。
12.3(3)	フォーマット e が拡張され、セッション ID U がサポートされました。
12.3(7)XI1	フォーマット e が拡張され、フォーマット文字列を NAS-Port-Type 属性固有にできるようになりました。次のキーワードと引数が追加されました：*string*、**type** *nas-port-type*。
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。

リリース	変更内容
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。
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

radius-serverattributenas-portformat コマンドは、NAS-Port 属性フィールド（RADIUS IETF 属性 5）のサイズとフォーマットを変更するように RADIUS を設定します。

次の NAS-Port 形式がサポートされています。

- 標準 NAS-Port 形式：この 16 ビット NAS-Port 形式は、制御インターフェイスのタイプ、ポート、およびチャネルを示します。これは Cisco IOS ソフトウェアが使用するデフォルトの形式です。
- 拡張 NAS-Port 形式：標準 NAS-Port 属性フィールドが 32 ビットに拡張されました。この NAS-Port 属性の上位 16 ビットは、制御インターフェイスの種類と番号を示します。下位 16 ビットは、インターフェイスで実行中の認証を示します。
- シェルフスロット NAS-Port 形式：この 16 ビット NAS-Port 形式では、シェルフ エントリとスロット エントリを必要とする拡張ハードウェア モデルがサポートされます。
- PPP 拡張 NAS-Port 形式：この NAS-Port 形式は 32 ビットであり、PPPoA と PPPoEoA のインターフェイス、仮想パス識別子（VPI）、仮想チャネル インジケータ（VCI）を示し、PPPoE over Institute of Electrical and Electronic Engineers（IEEE）標準 802.1Q VLAN のインターフェイスと VLAN ID を示します。

フォーマット e

Cisco IOS リリース 12.2(4)T 以前では、フォーマット a ～ c は、AS5400 などの Cisco プラットフォームでは機能しませんでした。このため、設定可能なフォーマット e が開発されました。フォーマット e では、属性 25（NAS-Port）の 32 ビットの用途を明示的に定義する必要があります。用途の定義では、特定のビット フィールドに対し、該当する各 NAS-Port フィールドに特定のパーサー文字を使用します。1 行に 1 文字（例：x）ずつ設定することで、その指定された値を格納するために 1 ビットだけが割り当てられます。同じタイプの文字（例：x）を追加すると、格納される有効な値の範囲が拡大します。次の表に、範囲の拡張方法を示します。

表 *3*：フォーマット *e* の範囲

文字	範囲
○	0 ～ 1

文字	範囲
xx	0-3
xxx	0 ～ 7
xxxx	0-F
xxxxx	0 ～ 1F

サポートするプラットフォームで、特定のパラメータの有効な範囲を把握しておく必要があります。Cisco IOS RADIUS クライアントは、設定に基づき許容可能な最大値まで、判別された値にビットマスクを適用します。したがって、パラメータに値8が指定されていることが判明するが、3 ビット（xxx）だけが設定されている場合、8 と 0x7 では結果は 0 になります。このため、必要な値を正しくキャプチャできるように、十分なビット数を常に設定する必要があります。ネットワーク環境内ですべてのNASポートタイプで適切に機能するようにフォーマットeが設定されていることを慎重に確認する必要があります。

次の表に、サポートされているパラメータとその文字を示します。

表 *4*：サポートされるパラメータと文字

サポートされるパラメータ	文字
0	0（このビットには常に 0 が設定されます）
1	1（このビットには常に 0 が設定されます）
DS0 shelf	f
DS0 slot	s
DS0 adaptor	a
DS0 port	p（物理ポート）
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L（モデム回線番号、つまり物理端末（TTY）番号）

サポートされるパラメータ	文字
PPPoX スロット	S
PPPoX adaptor	A
PPPoX port	P
PPPoX VLAN ID	V
PPPoX VPI	I
PPPoX VCI	C
Session ID	U

このフォーマットでは空のフィールドについては何も想定されないため、NAS-Portを表す32ビットすべてに、上記のいずれかの文字が設定されている必要があります。

アクセス ルータ

T1 ベース カードと T3 ベース カードの DS0 ポートでは異なる結果が得られます。T1 ベース カードでは、物理ポートと仮想ポートは等価です（これらのポートが同一であるため）。したがって、T1 カードでは **p** と **d** には同じ情報が含まれます。ただし T3 システムでは、ポートは物理ポート番号を示します（特定のプラットフォームではT3カードが複数存在する可能性があるため）。そのため、**d** は仮想 T1 回線を示します（T3 コントローラの設定に基づく）。T3 システムでは **p** と **d** は異なるため、物理デバイスを適切に識別するには両方をキャプチャする必要があります。Cisco AS5400 での実施例として、次の設定が推奨されます。

```
Router (config)# radius-server attribute nas-port format e SSSSPPPPPPPPPssssppppppccccc
```

これにより、非同期スロット（0-16）、非同期ポート（0-512）、DS0 スロット（0-16）、DS0 物理ポート（0-32）、DS0 仮想ポート（0-32）、およびチャネル（0-32）が設定されます。パーサーが実装され、32 ビット サポートが明示的に必要となります。このサポートがない場合、エラーとなります。

最後に、フォーマット e は個別線信号方式（CAS）、PRI、および BRI ベースのインターフェイスでサポートされています。

（注） このコマンドは **radius-serverattributenas-portextended** コマンドを置き替えます。

拡張 NAS-Port-Type 属性のサポート

このコマンドでは、拡張属性61サポートのために特定のサービス ポート タイプを設定できます。これにより、デフォルトのグローバル設定が上書きされます。

例

次の例では、RADIUS サーバが指定されており、NAS-Port フィールドに PPP 拡張フォーマットが設定されています。

```
radius-server host 192.0.2.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

次に、拡張 NAS-Port-Type ポートのグローバル サポートを設定し、2 種類のポート タイプに対して 2 つの個別のフォーマット e 文字列をグローバルに指定する例を示します。

- type 30（PPPoA）
- type 33（PPPoEoVLAN）

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCCC
 type 30

Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVVV
 type 33
```

関連コマンド

コマンド	説明
radiusattributenas-port-type	サブインターフェイス（イーサネット、vLAN、スタック VLAN（Q-inQ）、仮想回線（VC）、および VC 範囲など）を設定します。
radius-serverattribute61extended	非 RFC 準拠の拡張 NAS-Port-Type 属性（RADIUS 属性 61）を有効にします。
vpdnaaaattribute	LNS が PPP 拡張 NAS-Port 形式値をアカウンティングのために RADIUS サーバに送信できるようにします。

radius-server configure-nas

ベンダー固有のRADIUSサーバに対し、デバイスの起動時にドメイン全体で使用されるスタティック ルートとIPプール定義を照会するようにCiscoルータまたはアクセス サーバを設定するには、グローバル コンフィギュレーション モードで**radius-server configure-nas**コマンドを使用します。RADIUS サーバの照会を中止するには、このコマンドの no 形式を使用します。

radius-server configure-nas

no radius-server configure-nas

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3	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 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

Ciscoルータが初回起動時にスタティック ルートとIPプール定義をベンダー固有のRADIUSサーバに照会できるようにするには、**radius-server configure-nas**コマンドを使用します。RADIUS のベンダー固有実装の一部では、ネットワーク内にある個々のネットワーク アクセス サーバの代わりに、ユーザがRADIUSサーバのスタティック ルートおよびIPプールを定義できます。各ネットワーク アクセス サーバは、起動時にスタティック ルートとIPプール情報についてRADIUSサーバに照会します。このコマンドにより、CiscoルータはRADIUSサーバからスタティック ルートとIPプール定義情報を取得できます。

（注） **radius-server configure-nas** コマンドは Cisco ルータの起動時に実行されるため、これは **copy system:running-config nvram:startup-config** コマンドを実行するまでは有効ではありません。

例

次に、Cisco ルータまたはアクセス サーバに対し、デバイスの初回起動時に既に定義されているスタティック ルートと IP プール定義をベンダー固有の RADIUS サーバに照会するように指示する例を示します。

```
radius-server configure-nas
```

関連コマンド

Command	Description
radius-serverhostnon-standard	セキュリティ サーバが RADIUS のベンダー独自の実装を使用していることを示します。

radius-server dead-criteria

RADIUS サーバをデッド状態としてマークするための条件のいずれかまたは両方を、示されている定数に強制的に設定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria** コマンドを使用します。設定されていた基準をディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

no radius-server dead-criteria [**time** *seconds*| **tries** *number-of-tries*]

構文の説明

time *seconds*	（オプション）ルータがRADIUSサーバから有効なパケットを最後に受信してから、サーバがデッド状態としてマークされるまでに経過する必要のある最小時間（秒単位）。ルータの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。この時間は 1 ～ 120 秒に設定できます。 • *seconds* 引数を設定しない場合、この秒数はサーバのトランザクション レートに応じて 10 ～ 60 秒になります。 （注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

tries *number-of-tries*	（オプション）RADIUS サーバがデッド状態としてマークされるまでにルータで発生する必要がある連続タイムアウト回数。サーバが認証とアカウンティングの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。最初の送信と再送信を含むすべての送信がカウントされます。タイムアウト回数は 1 ～ 100 に設定できます。 • *number-of-tries* 引数を設定しない場合は、サーバのトランザクション レートと設定されている再送信回数に基づいて、連続タイムタウト回数は 10 ～ 100 となります。 （注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

コマンド デフォルト

RADIUS サーバがデッド状態としてマークされるまでに発生する連続タイムアウトの回数と秒数は、サーバのトランザクション レートと設定されている再送信回数に応じて異なります。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
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。
12.2SX	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

（注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

このコマンドの **no** 形式では、次のようになります。

- 引数 *seconds* または *number-of-tries* のいずれも **no radius-server dead-criteria** コマンドに指定されていない場合、時間と試行回数の両方がデフォルトにリセットされます。
- 最初に設定されていた値を使用して *seconds* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 60）にリセットされます。
- 最初に設定されていた値を使用して *number-of-tries* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 100）にリセットされます。

例

次に、5 秒経過後および 4 回の試行後にルータがデッド状態と見なされるようにルータを設定する例を示します。

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

次に、**radius-server dead-criteria** コマンドに設定された時間と試行回数の条件を無効にする例を示します。

```
Router (config)# no radius-server dead-criteria
```

次に、**radius-server dead-criteria** コマンドに設定された時間の条件を無効にする例を示します。

```
Router (config)# no radius-server dead-criteria time 5
```

次に、**radius-server dead-criteria** コマンドに設定された試行回数の条件を無効にする例を示します。

```
Router (config)# no radius-server dead-criteria tries 4
```

関連コマンド

Command	Description
debugaaadead-criteriatransactions	デッド条件の AAA トランザクションの値を表示します。
showaaadead-criteria	AAA サーバのデッド条件に関する情報を表示します。
show aaa server-private	すべてのプライベート RADIUS サーバのステータスを表示します。

Command	Description
show aaa servers	AAA サーバとの間で送受信されたパケットの数に関する情報を表示します。

radius-server deadtime

一部のサーバが使用不能な場合の RADIUS 応答時間を改善し、使用不能なサーバを即時にスキップするには、グローバル コンフィギュレーション モードで **radius-server deadtime** コマンドを使用します。deadtime を 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime 分

no radius-server deadtime

構文の説明

分	トランザクション要求が RADIUS サーバをスキップする期間（分単位、最大 1440 分（24 時間））。

コマンド デフォルト

デッド タイムは 0 に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
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

このコマンドは、Cisco IOS ソフトウェアが認証要求に応答しない RADIUS サーバを「デッド」状態とマークできるようにします。これにより、設定されている次のサーバを試行する前に要求の待機がタイムアウトになることが防止されます。「デッド」状態としてマークされた RADIUS サーバは、指定された期間（分数）、その他の要求でスキップされます。ただし、「デッド」状態としてマークされていないサーバが他にない場合を除きます。

（注） 「デッド」状態としてマークされたRADIUSサーバがダイレクト要求を受信する場合、そのダイレクト要求はRADIUSサーバで省略されません。ダイレクト要求はRADIUSサーバに直接送信されるため、RADIUSサーバはダイレクト要求の処理を続行します。

RADIUSサーバがデッド状態としてマークされている場合

12.2(13.7)T以前のバージョンのCisco IOSでは、設定されている再送信回数までパケットの送信が行われ、RADIUSパケット送信に設定されているタイムアウトに達するまでにサーバから有効な応答を受信しなかった場合に、RADIUSサーバがデッド状態としてマークされました。

Cisco IOSバージョン12.2(13.7)T以降の場合、次の両方の条件を満たした場合にRADIUSサーバがデッド状態としてマークされます。

1. サーバへ再送信するかどうかを決定するために使用される最小限のタイムアウト期間内に、未処理のトランザクションに対する有効な応答をRADIUSサーバから受信しなかった。
2. 最小限必要な再送信回数に1（初回送信分）を加算した回数だけ、パケットがすべてのトランザクションで連続してRADIUSサーバに送信されたが、必要なタイムアウト期間内にサーバから有効な応答を受信しなかった。

例

次に、認証要求への応答に失敗したRADIUSサーバのデッドタイムを5分に指定する例を示します。

```
radius-server deadtime 5
```

関連コマンド

Command	Description
deadtime(server-groupconfiguration)	RADIUSサーバ グループのコンテキスト内でデッドタイムを設定します。
radius-serverhost	RADIUSサーバ ホストを指定します。
radius-serverretransmit	Cisco IOSソフトウェアがRADIUSサーバ ホストのリストを検索する回数の最大値を指定します。
radius-servertimeout	サーバホストが応答するまでルータが待機する間隔を設定します。

radius-server host

（注） **radius-server host** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバを設定するには、**radius server** *name* コマンドを使用します。**radius server** コマンドの詳細については、『Cisco IOS Security Command Reference: Commands M to R』を参照してください。

RADIUS サーバ ホストを指定するには、グローバル コンフィギュレーション モードで **radius-server host** コマンドを使用します。指定した RADIUS ホストを削除するには、このコマンドの **no** 形式を使用します。

Cisco IOS リリース 12.4T 以降

radius-server host {*hostname*| *ip-address*} [**alias** {*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**backoff exponential** [**max-delay** 分] [**backoff-retry** *number-of-retransmits*]] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

その他のすべてのリリース

radius-server host {*hostname*| *ip-address*} [**alias** {*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** 分]] [**backoff exponential** [**max-delay** 分] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

構文の説明

hostname	RADIUS サーバ ホストのドメイン ネーム システム（DNS）名です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
alias	（任意）指定した RADIUS サーバについて、1 行につき最大 8 つのエイリアスを許可します。
acct-port *port-number*	（オプション）アカウンティング要求の UDP 宛先ポート。 • ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。ポート番号が指定されていない場合に割り当てられるデフォルトのポート番号は 1646 です。

auth-port *port-number*	（オプション）認証要求の UDP 宛先ポート。 • ポート番号が 0 に設定されている場合、そのホストは認証に使用されません。ポート番号が指定されていない場合に割り当てられるデフォルトのポート番号は 1645 です。
non-standard	RADIUS 標準に違反する属性を解析します。
timeout *seconds*	（オプション）デバイスが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）。 • timeout キーワードは、**radius-server timeout** コマンドのグローバル値を上書きします。 • タイムアウト値が指定されない場合はグローバル値が使用されます。範囲は 1 ～ 1000 です。
retransmit *retries*	（オプション）サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数です。 • retransmit キーワードは、**radius-server retransmit** コマンドのグローバル設定値を上書きします。 • 再送信値が指定されない場合はグローバル値が使用されます。範囲は 1 ～ 100 です。
test username *user-name*	（オプション）RADIUS サーバ ロード バランシングの自動テスト機能のテスト ユーザ名を設定します。
ignore-acct-port	（オプション）アカウンティング ポートでの RADIUS サーバ ロード バランシングの自動テスト機能を無効にします。
ignore-auth-port	（オプション）認証ポートでの RADIUS サーバ ロードバランシングの自動テスト機能を無効にします。

idle-time 分	（オプション）サーバが隔離され、テスト パケットが送信されるまでのサーバのアイドル時間（分単位）。範囲は 1 ～ 35791 です。デフォルトは 60 です。
backoff exponential	（オプション）指数再送信バックアップ モードを設定します。
max-delay 分	（オプション）再送信間の最大遅延（分単位）を設定します。 • **max-delay** 分 *minutes*：範囲は 1 ～ 120 です。デフォルト値は 3 です。
key-wrap encryption-key	（オプション）キーラップ暗号キーを指定します。
message-auth-code-key	キーラップ メッセージ認証コード キーを指定します。
format	（オプション）メッセージ オーセンティケータ コード キーの形式を指定します。 • 有効な値は次のとおりです。 ◦ **ascii**：キーを ASCII 形式で設定します。 ◦ **hex**：キーを 16 進数形式で設定します。
backoff-retry *number-of-retransmits*	（オプション）指数バックオフ再試行回数を指定します。 • *number-of-retransmits*：バックオフ再試行回数。範囲は 1 ～ 50 です。デフォルト値は 8 です。
pac	（オプション）サーバ別の Protected Access Credential（PAC）キーを生成します。

key	（オプション）このRADIUSサーバで実行されるRADIUSデーモンとデバイスの間で使用される暗号キー。 • この **key** キーワードは、**radius-server key** コマンドのグローバル設定値を上書きします。キー文字列を指定しない場合、グローバル値が使用されます。 （注） **key** キーワードは、RADIUSサーバで使用する暗号キーに一致するテキスト文字列でなければなりません。キーの先行スペースは無視されますが、途中および末尾のスペースは有効なので、キーは必ず **radius-server host** コマンド構文の最後の項目として設定してください。キーにスペースを使用する場合は、引用符自体がキーの一部でない限り、そのキーを引用符で囲まないでください。
encryption-key	暗号キーを指定します。 • *encryption-key* の有効な値を次に示します。 ◦ **0**：暗号化されていないキーが続くことを示します。 ◦ **7**：非公開のキーが続くことを示します。 ◦暗号化されていない（クリアテキスト）サーバ キーを指定する文字列。

コマンド デフォルト

デフォルトでは、RADIUSホストは指定されず、RADIUSサーバ ロード バランシング自動テストは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。

リリース	変更内容
12.0(5)T	このコマンドが変更され、タイムアウト、再送信およびキー値を RADIUS サーバごとに設定できるオプションが追加されました。
12.1(3)T	このコマンドが変更されました。**alias** キーワードが追加されました。
12.2(15)B	このコマンドが、Cisco IOS リリース 12.2(15)B に統合されました。**backoffexponential**、**backoff-retry**、**key**、および **max-delay** キーワードと、*number-of-retransmits*、*encryption-key*、および *minutes* 引数が追加されました。
12.2(28)SB	このコマンドが Cisco IOS リリース 12.2(28)SB に統合されました。RADIUS サーバ ロード バランシング自動テスト機能を設定するためのキーワードおよび引数 **test username** *user-name*、**ignore-auth-port**、**ignore-acct-port**、および **idle-time** *seconds* 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。Cisco IOS リリース 12.2(28)SB で追加されたキーワードと引数は、Cisco IOS リリース 12.2(33)SRA およびこれ以降の 12.2SR リリースに適用されます。
12.4(11)T	このコマンドが変更されました。 （注） Cisco IOS リリース 12.2(28)SB で追加されたキーワードと引数は、Cisco IOS リリース 12.4(11)T およびこれ以降の 12.4T リリースには適用されません。
12.2 SX	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。 （注） Cisco IOS リリース 12.2(28)SB で追加されたキーワードと引数は、Cisco IOS リリース 12.2SX には適用されません。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
15.3(1)S	このコマンドが変更されました。**key-wrap encryption-key**、**message-auth-code-key**、**format**、**ascii**、および **hex** キーワードが追加されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。
15.4(2)S	このコマンドが、Cisco IOS リリース 15.4(2)S に統合されました。

使用上のガイドライン

複数の **radius-server host** コマンドを使用して、複数のホストを指定できます。ソフトウェアは、指定された順序でホストを検索します。

ホスト固有のタイムアウト値、再送信値、またはキー値が指定されていない場合は、グローバル値が各ホストに適用されます。

RADIUS サーバで RADIUS サーバの自動テスト用に定義されていないテスト ユーザを使用することが推奨されます。これにより、テスト ユーザが正しく設定されていない場合に発生する可能性のあるセキュリティの問題から保護されます。

非標準のオプションを使用して RADIUS サーバを設定し、非標準のオプションを使用せずに別の RADIUS サーバを設定すると、非標準のオプションを使用する RADIUS サーバ ホストでは事前定義されたホストが受け入れられません。ただし、複数の異なる宛先 UDP ポートに同じ RADIUS サーバ ホスト IP アドレスを設定している場合、つまり（アカウンティング要求用の）UDP 宛先ポートが **acct-port** キーワードを使用して設定されており、非標準オプションの有無に関係なく（認証要求用の）別の UDP 宛先ポートが **auth-port** キーワードを使用して設定されている場合、RADIUS サーバは非標準オプションを受け入れません。これにより、すべてのポート番号がリセットされます。ホストの指定と、アカウンティング ポートと認証ポートの設定を 1 行で入力します。

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

RADIUS サーバ自動テスト

radius-server host コマンドを使用して RADIUS サーバ ロード バランシングの自動テストを有効にすると、次のようになります。

- デフォルトでは、認証ポートが有効になります。ポート番号が指定されていない場合にはデフォルトのポート番号（1645）が使用されます。認証ポートを無効にするには、**ignore-auth-port** キーワードを指定します。
- デフォルトでは、アカウンティング ポートが有効になります。ポート番号が指定されていない場合にはデフォルトのポート番号（1645）が使用されます。アカウンティング ポートを無効にするには、**ignore-acct-port** キーワードを指定します。

例

次に、host1 を RADIUS サーバとして指定し、使用している Cisco リリースに基づいてアカウンティングと認証の両方にデフォルト ポートを使用する例を示します。

```
radius-server host host1
```

次に、host1 という RADIUS ホストで認証要求の宛先ポートとしてポート 1612 を指定し、アカウンティング要求の宛先ポートとしてポート 1616 を設定する例を示します。

```
radius-server host host1 auth-port 1612 acct-port 1616
```

新しい行を開始するとすべてのポート番号がリセットされるため、ホストの指定とアカウンティング ポートおよび認証ポートの設定を 1 つの行に入力する必要があります。

次に、RADIUS サーバとして IP アドレス 192.0.2.46 のホストを指定し、認証ポートおよびアカウンティング ポートとしてポート 1612 と 1616 を使用し、タイムアウト値を 6、再送信値を 5 にそ

れぞれ設定して、さらに RADIUS サーバのキーと一致する暗号キーとして「rad123」を設定する例を示します。

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

次に、RADIUS サーバ host1 を認証には使用せずにアカウンティングに使用するように指定し、RADIUS サーバ host2 をアカウンティングには使用せずに認証に使用するように指定する例を示します。

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

次に、IP アドレスが 192.0.2.1 の RADIUS サーバの 4 つのエイリアスを指定する例を示します。

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

次に、サーバ単位で指数バックオフ再送信を有効化する例を示します。次の例では、再送信に 3 回の再試行回数が設定され、タイムアウトは 5 秒に設定されると想定します。つまり、RADIUS 要求は 5 秒間の遅延で 3 回送信されます。 その後デバイスは、再試行回数が 32 回に達するまで、各再試行時に遅延間隔を 2 倍にして RADIUS 要求の再送信を継続します。 デバイスは、再送信間隔が設定された 60 分を超えると、間隔を 2 倍にする操作を中止し、その後は 60 分ごとに送信します。

pac キーワードを指定すると、PAC-Opaque が許可されます。これは、Transport Layer Security（TLS）トンネルの確立フェーズでサーバに送信される可変長フィールドです。 PAC-Opaque はサーバだけが解釈でき、ピアのアイデンティティと認証を検証するために必要な情報がサーバで復元されます。 たとえば、PAC-Opaque には PAC-Key と PAC のピア アイデンティティが含まれていることがあります。PAC-Opaque の形式と内容は、発行元 PAC サーバによって異なります。

次に、デバイスで自動 PAC プロビジョニングを設定する例を示します。シード デバイスでは PAC-Opaque をプロビジョニングする必要があります。これにより、すべての RADIUS 交換で、この PAC-Opaque を使用して使用中サーバの自動 PAC プロビジョニングを有効にできます。すべての非シード デバイスは、リンク初期化の認証フェーズで PAC-Opaque を取得します。

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

例

次に、ご使用の Cisco リリースに基づいて指定された認証ポートとアカウンティング ポートを使用した、RADIUS サーバのロード バランシング自動テストを有効にする例を示します。

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

関連コマンド

コマンド	説明
aaaaccounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。

コマンド	説明
aaaauthenticationppp	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaaauthorization	ネットワーク アクセスをユーザに制限するパラメータを設定します。
debugaaatest	RADIUS サーバ ロード バランシングのアイドル タイマーまたは dead タイマーが満了になった時点を示します。
load-balance	名前付き RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。
ppp	PPP を使用して非同期接続を開始します。
pppauthentication	CHAP または PAP、またはその両方を有効にし、インターフェイスで CHAP および PAP 認証が選択される順序を指定します。
radius-serverkey	デバイスおよびRADIUSデーモン間のすべてのRADIUS通信の認証キーおよび暗号キーを指定します。
radius-serverload-balance	グローバル RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。
radius-serverretransmit	Cisco ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。
radius-servertimeout	サーバホストが応答するまでデバイスが待機する間隔を設定します。
testaaagroup	RADIUS ロード バランシング サーバ応答を手動でテストします。
username	PPP CHAP や PAP などのユーザ名ベースの認証システムを確立します。

radius-server key

（注） **radius-server key** コマンドは、Cisco IOS リリース 15.4(2)S 以降では廃止されています。IPv4 または IPv6 RADIUS サーバを設定するには、**radius server** *name***key** コマンドを使用します。**key (config-radius-server)** コマンドの詳細については、『*Cisco IOS Security Command Reference: Commands D to L*』を参照してください。

ルータと RADIUS デーモン間のすべての RADIUS 通信に認証および暗号キーを設定するには、**radius-server key** コマンドを使用します。キーをディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server key {**0** *string*| **7** *string*} *string*

no radius-server key

構文の説明

0 *string*	暗号化されていないキーが続くことを示します。 暗号化されていない（クリアテキスト）共有キー。
7 *string*	非公開のキーが続くことを示します。 非公開の共有キー。
string	暗号化されていない（クリアテキスト）共有キー。

コマンド デフォルト

認証および暗号キーはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。

リリース	変更内容
12.1(3)T	このコマンドが変更されました。*string* 引数が次のように変更されました。 • **0** *string* • **7** *string* • *string*
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。
Cisco IOS XE リリース 3.3S	このコマンドが、Cisco IOS XE リリース 3.3S に統合されました。
15.4(2)S	このコマンドが、Cisco IOS リリース 15.4(2)S に統合されました。

使用上のガイドライン

aaanew-model コマンドを使用して認証、認可、およびアカウンティング（AAA）の認証を有効にした後で、**radius-server key** コマンドを使用して認証と暗号キーを設定する必要があります。

（注） **aaanew-model** コマンドの発行後に RADIUS キーを指定します。

入力するキーは、RADIUS デーモンで使用されるキーと一致する必要があります。先頭のスペースはすべて無視されますが、キーの中間および末尾のスペースは使用できます。キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

例

次に、認証および暗号キーを「key1」に設定する例を示します。

```
Device(config)# radius-server key key1
```

次に、認証および暗号キーを「anykey」に設定する例を示します。7は、非公開のキーが続くことを指定します。

```
service password-encryption
radius-server key 7 anykey
```

設定を保存し、show-running config コマンドを使用すると、暗号キーが次のように表示されます。

```
Device# show running-config
!
!
```

```
 radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

関連コマンド

Command	Description
aaaaccounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaaauthenticationppp	PPPを実行しているシリアルインターフェイス上で使用する1つまたは複数のAAA認証方式を指定します。
aaaauthorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa new-model	AAAアクセス コントロール モデルを有効にします。
ppp	PPPを使用して非同期接続を開始します。
pppauthentication	CHAPまたはPAP、またはその両方をイネーブルにし、インターフェイスでCHAPおよびPAP認証が選択される順番を指定します。
radius-serverhost	RADIUSサーバ ホストを指定します。
servicepassword-encryption	パスワードを暗号化します。
username	PPP CHAPやPAPなどのユーザ名ベースの認証システムを確立します。

radius-server load-balance

認証、許可、およびアカウンティング（AAA）メソッドリストで「radius」と示されているグローバル RADIUS サーバ グループの RADIUS サーバ ロード バランシングを有効にするには、グローバル コンフィギュレーション モードで radius-server load-balance コマンドを使用します。RADIUS サーバ ロード バランシングを無効にするには、このコマンドの **no** 形式を使用します。

radius-server load-balance method least-outstanding [**batch-size** *number*] **[ignore-preferred-server]**

no radius-server load-balance

構文の説明

methodleast-outstanding	ロードバランシングの最小未解決モードを有効にします。
batch-size	（任意）バッチごとに割り当てられるトランザクションの数。
number	（オプション）バッチのトランザクションの数。 • デフォルトは 25 です。 • 範囲は 1 ～ 2147483647 です。 （注） バッチ サイズがスループットと CPU の負荷に影響する場合があります。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。
ignore-preferred-server	（オプション）1 つの AAA セッションに関連付けられているトランザクションが、同じサーバを使用する必要があるかどうかを指定します。 • 設定されている場合、優先サーバ設定は使用されません。 • デフォルトでは優先サーバが使用されます。

コマンド デフォルト

このコマンドが設定されていない場合、グローバル RADIUS サーバ ロード バランシングは行われません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(28)SB	このコマンドが導入されました。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T に統合されました。
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。

例

次の例は、グローバル RADIUS サーバ グループに対してロード バランシングを有効にする方法を示しています。この例は、RADIUS コマンド出力の現在の設定、デバッグ出力、および AAA サーバ ステータス情報の 3 つの部分からなります。デリミタを使用して関連する設定部分だけを表示できます。

例

次に、関連する RADIUS 設定を示します。

```
Router# show running-config | inc radius
aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

上記 RADIUS コマンド出力の現行設定内の行は、次のように定義されています。

- **aaa authentication ppp** コマンドは、RADIUS を使用してすべての PPP ユーザを認証します。
- **aaa accounting** コマンドは、クライアントの認証後、および start-stop キーワードを使用した切断の後に、AAA サーバにすべてのアカウンティング要求を送信できるようにします。
- **radius-server host** コマンドは、指定された認証ポートおよびアカウンティング ポートと、特定された認証および暗号キーを使用して、RADIUS サーバ ホストの IP アドレスを定義します。
- **radius-server load-balance** コマンドは、バッチ サイズが指定されたグローバル RADIUS サーバ グループに対してロード バランシングを有効化します。

例

下のデバッグ出力は、上の設定に関する優先サーバの選択と要求の処理を示しています。

```
Router# show debug
General OS:
  AAA server group server selection debugging is on
Router#
<sending 10 pppoe requests>
Router#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(0000001A):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001A):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001D):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server
.
.
.
```

グローバル RADIUS サーバ グループのサーバ ステータス情報の例

下の出力は、グローバル RADIUS サーバ グループ設定例の AAA サーバ ステータスを示しています。

```
Router# show aaa server
RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3247ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
Router#
```

この出力は、2 つの RADIUS サーバのステータスを示しています。両方のサーバが動作中であり、最後の 2 分間で次の処理に成功しています。

- 6 つの認証要求のうち 5 つ
- 5 つのアカウンティング要求のうち 5 つ

関連コマンド

コマンド	説明
debugaaasg-serverselection	ルータ内の RADIUS および TACACS+ サーバ グループ システムが特定のサーバを選択している理由を示します。

コマンド	説明
debugaaatest	RADIUS サーバ ロード バランシングのアイドル タイマーまたは dead タイマーが満了になった時点を示します。
load-balance	名前付き RADIUS サーバ グループに対して RADIUS サーバ ロード バランシングを有効にします。
radius-serverhost	ロード バランシングの RADIUS 自動テストを有効にします。
testaaagroup	RADIUS ロード バランシング サーバ応答を手動でテストします。

radius-server retransmit

Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する最大回数を指定するには、グローバル コンフィギュレーション モードで **radius-server retransmit** コマンドを使用します。再送信を無効にするには、このコマンドの **no** 形式を使用します。

radius-server retransmit *retries*

no radius-server retransmit

構文の説明

retries	再送信の最大試行回数です。範囲は 0 ～ 100 です。

コマンド デフォルト

デフォルトの再送信試行回数は 3 回です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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。
Cisco IOS XE リリース 3.3S	このコマンドが、Cisco IOS XE リリース 3.3S に統合されました。

使用上のガイドライン

Cisco IOS ソフトウェアでは、すべてのサーバに対して再送信が試みられ、それぞれがタイムアウトになってから再送信カウントが増加します。

RADIUS サーバとルータの間の距離が数ホップの場合は、RADIUS サーバの再試行レートを 5 に設定することが推奨されます。

例

次に、再送信カウンタ値を 5 回に指定する例を示します。

```
Router(config)# radius-server retransmit 5
```

関連コマンド

Command	Description
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
radius-serverhost	RADIUS サーバ ホストを指定します。
radius-serverkey	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
radius-servertimeout	サーバホストが応答するまでルータが待機する間隔を設定します。
showradiusstatistics	アカウンティング パケットと認証パケットについての RADIUS 統計情報を示します。

radius-server timeout

ルータがサーバホストの応答を待機する間隔を設定するには、グローバル コンフィギュレーション モードで **radius-servertimeout** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout

構文の説明

seconds	タイムアウトの間隔を指定する秒数です。指定できる範囲は 1 ～ 1000 です。デフォルト値は 5 秒です。

コマンド デフォルト

5 秒

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.1	このコマンドが導入されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB 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

タイムアウトになるまでルータがサーバ ホストの応答を待機する秒数を設定するには、このコマンドを使用します。

RADIUS サーバとルータの間の距離が数ホップの場合は、RADIUS サーバのタイムアウトを 15 秒に設定することが推奨されます。

例

次に、インターバル タイマーを 10 秒に設定する例を示します。

```
radius-server timeout 10
```

関連コマンド

Command	Description
radius-serverhost	RADIUS サーバ ホストを指定します。
radius-serverkey	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
radius-serverretransmit	Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。
showradiusstatistics	アカウンティング パケットと認証パケットについての RADIUS 統計情報を示します。

radius-server vsa send

ベンダー固有の属性（VSA）を認識して使用するようにネットワークアクセスサーバ（NAS）を設定するには、グローバル コンフィギュレーション モードで **radius-server vsa send** コマンドを使用します。NAS が VSA を使用できないようにするには、このコマンドの **no** 形式を使用します。

radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] **[3gpp2]**

no radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] **[3gpp2]**

構文の説明

accounting	（オプション）認識されるVSAをアカウンティング属性のみに制限します。
authentication	（オプション）認識される VSA を認証属性のみに制限します。
cisco-nas-port	（オプション）Cisco NAS ポート VSA を返します。 （注） 属性 87（Attr87）に NAS ポート情報を指定するという IETF の要件に基づき、Cisco NAS ポートはデフォルトでは無効です。
3gpp2	（オプション）Third Generation Partnership Project 2（3GPP2）Cisco VSA を 3GPP2 パケット タイプに追加します。

コマンド デフォルト

NAS は VSA を認識して使用するように設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
11.3T	このコマンドが導入されました。
12.2(27)SBA	このコマンドが、Cisco IOS リリース 12.2(27)SBA に統合されました。
12.2(33)SRA	このコマンドが変更されました。Cisco VSA との後方互換性のために、**cisco-nas-port** キーワードと **3gpp2** キーワードが追加されました。

リリース	変更内容
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。
Cisco IOS XE リリース 3.3S	このコマンドが、Cisco IOS XE リリース 3.3S に統合されました。
Cisco IOS XE Release 3.8S	このコマンドが変更されました。NASがアカウンティング要求と認証要求で VSA を使用できるようにするため、**accounting** キーワードと **authentication** キーワードがデフォルトで有効になりました。

使用上のガイドライン

IETF のドラフト規格では、NAS と RADIUS サーバ間で、VSA（属性 26）を使用してベンダー固有情報を受け渡す方法が定められています。ベンダーはVSAを使用して、一般的な用途には適さない独自の拡張属性をサポートできます。**radius-servervsasend** コマンドは、NASがアカウンティングと認証の両方の VSA を認識して使用できるようにします。認識される VSA をアカウンティング属性だけに制限するには、**accounting** キーワードを **radius-servervsasend** コマンドに使用します。認識される VSA を認証属性だけに制限するには、**authentication** キーワードを **radius-servervsasend** コマンドに使用します。デフォルトの **radius-servervsasendaccounting** コマンドと **radius-servervsasendauthentication** コマンドを参照するには、**show running-config all** コマンドを使用します。

シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は cisco-avpair）です。値は次の形式のストリングです。

```
"protocol : attribute separator value"
```

前述の例では、*protocol* は特定の認証タイプの Cisco プロトコル属性の値、*attribute* と *value* は、Cisco TACACS+ の仕様で定義されている適切な属性と値（AV）のペア、*separator* は必須属性では = です。このソリューションでは、TACACS+ 許可で使用できるすべての機能を RADIUS にも使用できるようになります。

たとえば、次の AV ペアにより、IP 認証中（PPP Internet Protocol Control Protocol（IPCP）アドレス割り当て中）に、Multiple Named IP Address Pools 機能がアクティブになります。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例では、NAS Prompt ユーザが EXEC コマンドに即時にアクセスできるようになります。

```
cisco-avpair= "shell:priv-lvl=15"
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『*Remote Authentication Dial-In User Service*（*RADIUS*）』を参照してください。

例

次に、NAS がベンダー固有のアカウンティング属性を認識して使用するように設定する例を示します。

```
Device(config)# radius-server vsa send accounting
```

関連コマンド

Command	Description
aaanasportextended	NAS-Port 属性を RADIUS IETF 属性 26 に置き換え、拡張フィールド情報を表示します。
show running-config all	設定情報全体（デフォルト設定および値を含む）を表示します。

rd

VPNルーティングおよび転送（VRF）インスタンスのルート識別子（RD）を指定するには、VRFコンフィギュレーション モードで **rd** コマンドを使用します。ルート識別子を削除するには、このコマンドの **no** 形式を使用します。

rd *route-distinguisher*

no rd *route-distinguisher*

構文の説明

route-distinguisher	VPN IPv4 プレフィックスを作成するために、IPv4プレフィックスに追加される8バイト値。

コマンド デフォルト

RD は指定されません。

コマンド モード

VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
12.0(5)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが Cisco IOS 12.0(22)S に統合されました。
12.2(13)T	このコマンドが Cisco IOS 12.2(13)T に統合されました。
12.2(14)S	このコマンドが Cisco IOS 12.2(14)S 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。
12.2(33)SRB	IPv6 のサポートが追加されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

リリース	変更内容
12.2(54)SG	このコマンドが、Cisco IOS Release 12.2(54)SG に統合されました。
Cisco IOS XE Release 3.1S	このコマンドが、Cisco IOS XE リリース 3.1S に統合されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

RD はルーティング テーブルと転送テーブルを作成し、VPN のデフォルト ルート識別子を指定します。RD は顧客の IPv4 プレフィックスの先頭に追加され、その IPv4 プレフィックスはグローバルに一意の VPN-IPv4 プレフィックスになります。

RD は次のいずれかです。

- ASN-related：自律システム番号と任意の番号で構成されます。
- IP-address-related：IP アドレスと任意の番号で構成されます。

RD は、次のいずれかの形式で入力できます。

16-bit autonomous-system-number **:** *your 32-bit number* 例：101:3。

32-bit IP address **:** *your 16-bit number* 例：192.168.122.15:1。

例

次に、2 つの VRF のデフォルト RD を設定する例を示します。これは、autonomous-system-number-relative RD と IP-address-relative RD の両方の使用法を示しています。

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

次に、VRF 設定のグローバル部分に共通ポリシーが定義されている IPv4 および IPv6 用の VRF の例を示します。

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

関連コマンド

Command	Description
ipvrf	VRF ルーティング テーブルを設定します。
showipvrf	一連の定義された VRF および関連付けられているインターフェイスを表示します。
vrfdefinition	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。

reauthentication time ～ rsa-pubkey

remark

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

remark *remark*

no remark *remark*

構文の説明

remark	アクセス リスト エントリを記述するコメント。最大 100 文字です。

コマンド デフォルト

アクセス リスト エントリには注釈はありません。

コマンド モード

標準名前付きアクセス リスト コンフィギュレーションまたは拡張名前付きアクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
12.0(2)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

注釈は最大 100 文字まで可能で、これより長い文字は切り捨てられます。

番号付き IP アクセス リストのエントリに関するコメントを記入するには、**access-list remark** コマンドを使用します。

例

次の例では、host1 サブネットに対しアウトバウンド Telnet の使用が許可されていません。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.69.2.88 any eq telnet
```

関連コマンド

Command	Description
access-listremark	番号付き IP アクセス リストのエントリに有益なコメント（注釈）を指定します。
deny(IP)	パケットが名前付き IP アクセス リストで許可されない条件を設定します。
ipaccess-list	IP アクセス リストを名前で定義します。
permit(IP)	パケットが名前付き IP アクセス リストで許可される条件を設定します。