aaa nas port extended ～ address ipv6（TACACS+）

aaa nas port extended

NAS-Port 属性を RADIUS IETF 属性 26 で置換し、拡張フィールド情報を表示するには、グローバル コンフィギュレーション モードで **aaa nas port extended** コマンドを使用します。 拡張フィールド情報を表示しない場合は、このコマンドの **no** 形式を使用します。

aaa nas port extended

no aaa nas port extended

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド 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 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

各スロットに複数のインターフェイス（ポート）があるプラットフォームの場合、シスコ RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port 属性を提供しません。 たとえば、デュアル PRI インターフェイスがスロット 1 にある場合、Serial1/0:1 と Serial1/1:1 の両方のコールは、RADIUS IETF の NAS-Port 属性に関連付けられた 16 ビットのフィールド サイズ制限により、NAS-Port = 20101 として表示されます。

この場合の解決策は、ベンダー固有属性（RADIUS IETF 属性 26）で NAS-Port 属性を置換することです。 シスコのベンダー ID は 9 であり、Cisco-NAS-Port 属性はサブタイプ 2 です。 ベンダー固有属性（VSA）を有効にするには、**radius-server vsa send** コマンドを入力します。 ベンダー固有属性のポート情報を提供および設定するには、**aaa nas port extended** コマンドを使用します。

標準の NAS-Port 属性（RADIUS IETF 属性 5）は以降も送信されます。 この情報を送信しない場合、**no radius-server attribute nas-port** コマンドを使用して停止できます。 このコマンドを設定すると、標準の NAS-Port 属性は送信されなくなります。

例

次に、RADIUS が拡張インターフェイス情報を表示するように指定する例を示します。

```
radius-server vsa send
aaa nas port extended
```

関連コマンド

コマンド	説明
radius-server extended-portnames	NAS-Port 属性の拡張インターフェイス情報を表示します。
radius-server vsa send	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。

aaa new-model

認証、許可、アカウンティング（AAA）アクセス コントロール モデルをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを発行します。 AAA アクセス コントロール モデルをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa new-model

no aaa new-model

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

AAA がディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.4(4)T	IPv6 のサポ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(33)SXI	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 2.5	このコマンドが、Cisco IOS XE Release 2.5 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 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

このコマンドは、AAA アクセス コントロール システムをイネーブルにします。

例

次に、AAA を初期化する例を示します。

```
aaa new-model
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa authentication arap	TACACS+ を使用して ARAP の AAA 認証方式をイネーブルにします。
aaa authentication enable default	AAA 認証をイネーブルにして、ユーザが特権コマンドレベルにアクセスできるかどうかを確認します。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

aaa route download

スタティック ルート ダウンロード機能をイネーブルにし、ダウンロード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 **aaa route download** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

構文の説明

time	（任意）ダウンロード間隔（分単位）。 有効な範囲は 1 ～ 1440 分です。
authorization *method-list*	（任意）スタティック ルート ダウンロード用の RADIUS 許可要求が送信される名前付き方式リストを指定します。 これらの属性が設定されていない場合、すべての RADIUS 許可要求はデフォルトの方式リストで指定されたサーバに送信されます。

コマンド デフォルト

デフォルトのダウンロード（更新）間隔は 720 分です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.0(3)T	このコマンドが導入されました。
12.1	このコマンドが Cisco IOS Release 12.1 に統合されました。
12.2(8)T	**authorization** キーワードが追加されました。*method-list* 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。
12.2(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

このコマンドは、ルータの名前が *hostname* の場合に、許可、認証、アカウンティング（AAA）サーバからスタティック ルートの詳細をダウンロードするために使用されます。 スタティック ルートの AAA サーバに渡される名前は *hostname-1*、*hostname-2* ～ *hostname-n* です。ルータは、インデックスが失敗し、ルートがそれ以上ダウンロードできなくなるまで、スタティック ルートをダウンロードし続けます。

例

次に、AAA ルートの更新期間を 100 分に設定する例を示します。

```
aaa route download 100
```

次に、AAA ルートの更新期間を 10 分に設定し、方式リストの名前「list1」で指定されたサーバにスタティック ルート ダウンロード要求を送信する例を示します。

```
aaa route download 10 authorization list1
```

関連コマンド

コマンド	説明
aaa authorization configuration default	TACACS+ または RADIUS を使用して AAA サーバからスタティック ルート設定情報をダウンロードします。
clear ip route download	AAA サーバからダウンロードされたスタティック ルートをクリアします。
show ip route	すべてのスタティック IP ルート、または AAA ルート ダウンロード機能を使用してインストールされたスタティック IP ルートを表示します。

aaa server radius dynamic-author

デバイスを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシーサーバとの相互作用を実行するように設定するには、グローバル コンフィギュレーション モードで **aaa server radius dynamic-author** コマンドを使用します。 このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

aaa server radius dynamic-author

no aaa server radius dynamic-author

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デバイスは、外部ポリシー サーバとの相互作用を実行するときにサーバとして機能しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(28)SB	このコマンドが導入されました。
12.4	このコマンドが、Cisco IOS Release 12.4 に統合されました。
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。
12.2(5)SXI	このコマンドが、Cisco IOS Release 12.2(5)SXI に統合されました。
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

動的許可は、外部ポリシーサーバがデバイスに動的に更新情報を送信できます。 **aaa server radius dynamic-author** コマンドが設定されている場合は、動的許可ローカル サーバ コンフィギュレーション モードが開始されます。 このモードでは、RADIUS アプリケーション コマンドを設定できます。

Intelligent Services Gateway（ISG）用の動的許可

ISG は、加入者別およびサービス別の情報が格納されたポリシー サーバと呼ばれる外部デバイスと連携動作します。 ISG は、ISG デバイスと外部ポリシー サーバ間の相互作用の 2 つのモデル（初期許可と動的許可）をサポートしています。

動的許可モデルでは、外部ポリシー サーバは、ISG に対して動的にポリシーを送信できます。 これらの処理は、（サービスの選択を通じて）加入者がインバンド方式で開始することも、管理者の操作を通じて開始することもできます。また、アプリケーションはアルゴリズムに基づいてポリシーを変更できます（たとえば、1 日の特定の時間に、セッションの Quality of Service（QoS）を変更します）。 このモデルは、Change of Authorization（CoA）RADIUS 拡張によって容易になります。 CoA は、RADIUS にピアツーピア機能を導入しました。これにより、ISG と外部ポリシー サーバをそれぞれ RADIUS クライアントとサーバとして機能させることができます。

例

次に、IP アドレス 10.12.12.12 のクライアントと相互作用を実行する場合に、ISG が AAA サーバとして機能するように設定する例を示します。

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

関連コマンド

コマンド	説明
auth-type（ISG）	サーバの許可タイプを指定します。
client	デバイスに CoA および切断要求を送信する RADIUS クライアントを指定します。
default	RADIUS アプリケーション コマンドをデフォルトに設定します。
domain	ユーザ名のドメイン オプションを指定します。
ignore	特定のパラメータを無視するように動作を上書きします。
port	ローカル RADIUS サーバがリッスンするポートを指定します。
server-key	RADIUS クライアントと共有する暗号キーを指定します。

access-list（IP 標準）

標準 IP アクセス リストを定義するには、グローバル コンフィギュレーション モードで **access-list** コマンドの標準バージョンを使用します。標準アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *access-list-number* {**deny**| **permit**} *source* [*source-wildcard*] [**log** [*word*]]

no access-list *access-list-number*

構文の説明

access-list-number	アクセス リスト番号。 1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数です。
deny	条件に一致する場合、アクセスを拒否します。
permit	条件が一致した場合にアクセスを許可します。
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 2 つの方法を使用できます。 • 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用します。
source-wildcard	（任意）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場合、次の 2 つの方法を使用できます。 • 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。 無視するビット位置には 1 を入力します。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用します。

log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します）。 このログ メッセージに含まれるものには、アクセス リスト番号、パケットが許可されたか拒否されたか、送信元アドレス、パケット数、さらに、該当する場合は、ユーザ定義のクッキーまたはルータが生成したハッシュ値があります。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で許可または拒否されたパケット数を含めて生成されます。 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。 この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。 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。
word	（任意）ログ メッセージに追加されるユーザ定義のクッキー。 クッキーには次の制約があります。 • 文字以外は使用できません。 • 16進表記で開始することはできません（0x など）。 • **reflect**、**fragment**、**time-range** キーワード、およびこれらのキーワードのサブセットと同じにはできません。 • 英数字以外は使用できません。 ユーザ定義のクッキーはアクセス コントロール エントリ（ACE）の syslog エントリに加えられ、syslog エントリを生成したアクセス コントロール リスト内で ACE を一意に識別します。

コマンド デフォルト

アクセス リストは、デフォルトで、すべてに対する暗黙の拒否ステートメントです。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

コマンド モード

グローバル コンフィギュレーション（config）

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。
11.3(3)T	**log** 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。
12.2SX	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。

使用上のガイドライン

アクセス条件を慎重に計画し、アクセス リストの末尾にある暗黙の拒否ステートメントに注意してください。

アクセス リストは、インターフェイスでのパケット送信の制御、vty アクセスの制御、ルーティング アップデートの内容の制限に使用できます。

すべてのアクセス リストの内容を表示するには、**show access-lists** EXEC コマンドを使用します。

1 つのアクセス リストの内容を表示するには、**show ip access-list** EXEC コマンドを使用します。

注意

このコマンドの拡張には下位互換性があります。Cisco IOS Release 10.3 以前のリリースからの移行ではアクセス リストが自動的に変換されます。 ただし、Release 10.3 以前のリリースでは、これらの拡張との上位互換性はありません。 そのため、アクセス リストをこれらのイメージに保存してから、Release 10.3 以前のソフトウェアを使用すると、そのアクセス リストは正しく解釈されません。 **この状態は、深刻なセキュリティ上の問題が発生する可能性があります。** これらのイメージをブートする前に、以前のコンフィギュレーション ファイルを保存してください。

例

次に、標準アクセス リストで、3 つの特定のネットワーク上のホストだけにアクセスを許可する例を示します。 ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リスト ステートメントに一致しない送信元アドレスのホストはすべて拒否されます。

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

ワイルドカードがすべてゼロの場合、ワイルドカードを省略することで、大量の個別アドレスを簡単に指定できます。 したがって、次の 2 つのコンフィギュレーション コマンドは実質的に同一です。

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。 また、ロギング メカニズムがイネーブルになり、各 syslog エントリに SampleUserValue という語句が追加されます。

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

関連コマンド

コマンド	説明
access-list	着信接続および発信接続を特定の（シスコデバイスへの）vty とアクセス リスト内のアドレスとの間に制限します。
access-list（IP 拡張）	拡張 IP アクセス リストを定義します。
access-list remark	番号付き IP アクセス リスト内のエントリに有益なコメント（注釈）を書き込みます。
deny（IP）	パケットが名前付きアクセス リストを渡さない条件を設定します。

コマンド	説明
distribute-list in（IP）	アップデートで受信するネットワークをフィルタリングします。
distribute-list out（IP）	更新でのネットワークのアドバタイズを抑制します。
ip access-group	インターフェイスへのアクセスを制御します。
ip access-list logging hash-generation	ACE syslog エントリのハッシュ値の生成をイネーブルにします。
permit（IP）	パケットが名前付きアクセスリストを渡す条件を設定します。
remark（IP）	名前付き IP アクセス リスト内のエントリに有益なコメント（注釈）を書き込みます。
show access-lists	現在の IP およびレート制限アクセス リストの内容を表示します。
show ip access-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。

address ipv6（config-radius-server）

RADIUS サーバのアカウンティングおよび認証パラメータの IPv6 アドレスを設定するには、RADIUS サーバ コンフィギュレーション モードで **address ipv6** コマンドを使用します。 指定した RADIUS サーバのアカウンティングおよび認証パラメータを削除するには、このコマンドの **no** 形式を使用します。

address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

no address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

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。
ipv6address	RADIUS サーバの IPv6 アドレス。
acct-port *port*	（任意）アカウンティング要求の RADIUS アカウンティング サーバにユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトのポートは 1646 です。
alias {*hostname* | *ipv6address*}	（任意）このサーバにエイリアスを指定します。 エイリアスは IPv6 アドレスまたはホスト名を指定できます。エイリアスはこのサーバに 8 つまで設定できます。
auth-port *port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。デフォルトのポートは 1645 です。

コマンド デフォルト

RADIUS サーバのアカウンティングおよび認証パラメータは設定されていません。

コマンド モード

RADIUS サーバ コンフィギュレーション（config-radius-server）

コマンド履歴

リリース	変更内容
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

このコマンドにアクセスする前に、**aaa new-model** コマンドを設定する必要があります。

Cisco TrustSec（CTS）機能は、Secure RADIUS を使用して、認証、許可、セッション アソシエーション、暗号化、およびトラフィック フィルタリングの処理を規定します。

エイリアスを RADIUS サーバに設定する前に、サーバの IPv6 アドレスまたは DNS 名を設定する必要があります。 これは、**address ipv6** コマンドおよび *hostname* 引数を使用して行います。 その後、**address ipv6** コマンド、**alias** キーワードおよび *hostname* 引数を使用してエイリアスを設定できます。

例

次に、RADIUS サーバのアカウンティングおよび認証パラメータを設定する例を示します。

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812
```

関連コマンド

コマンド	説明
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。
address ipv4	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
radius server	RADIUS サーバ コンフィギュレーションの名前を指定し、RADIUS サーバ コンフィギュレーション モードを開始します。

address ipv6（TACACS+）

TACACS+ サーバの IPv6 アドレスを設定するには、TACACS+ サーバ コンフィギュレーション モードで **address ipv6** コマンドを使用します。 IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

address ipv6 *ipv6-address*

no address ipv6 *ipv6-address*

構文の説明

ipv6-address	秘密 TACACS+ サーバ ホスト。

コマンド デフォルト

TACACS+ サーバは設定されていません。

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

tacacs server コマンドを使用して TACACS+ サーバをイネーブルにした後で、address ipv6（TACACS+）コマンドを使用します。

例

次に、server1 という名前の TACACS+ サーバの IPv6 アドレスを指定する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。

address ipv6（TACACS+）