



レイヤ 2 アクセス リストの実装

イーサネット サービス アクセス コントロール リスト (ACL) は、レイヤ 2 ネットワーク トラフィック プロファイルを集合的に定義する 1 つ以上のアクセス コントロール エントリ (ACE) で構成されます。このプロファイルは、Cisco IOS XR ソフトウェア機能によって参照できます。各イーサネット サービス ACL には、送信元および宛先アドレス、サービス クラス (CoS)、または VLAN ID などの基準に基づいたアクション要素 (許可または拒否) が含まれます。

このモジュールでは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータでのイーサネット サービス アクセス リストの実装に必要なタスクについて説明します。



(注)

このモジュールに記載されているイーサネット サービス アクセス リスト コマンドの詳細については、マニュアル『Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference』の「Ethernet Services (Layer 2) Access List Commands on Cisco ASR 9000 Series Routers」を参照してください。この章で使用される他のコマンドの説明については、コマンド リファレンスのマスター索引を参照するか、またはオンラインで検索してください。

Cisco ASR 9000 シリーズ ルータでのイーサネット サービス アクセス リスト実装の機能履歴

リリース	変更箇所
リリース 3.7.2	この機能が、Cisco ASR 9000 シリーズ ルータで導入されました。

内容

- 「レイヤ 2 アクセス リスト実装の前提条件」 (P.362)
- 「レイヤ 2 アクセス リストの実装に関する情報」 (P.362)
- 「レイヤ 2 アクセス リストの実装方法」 (P.364)
- 「レイヤ 2 アクセス リストを実装するための設定例」 (P.373)
- 「その他の参考資料」 (P.374)

レイヤ 2 アクセス リスト実装の前提条件

この前提条件は、アクセス リストおよびプレフィクス リストの実装に適用されます。

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。

ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

レイヤ 2 アクセス リストの実装に関する情報

イーサネット サービス アクセス リストを実装するには、次の概念を理解している必要があります。

- ・「イーサネット サービス アクセス リスト機能のハイライト」(P.362)
- ・「イーサネット サービス アクセス リストの目的」(P.362)
- ・「イーサネット サービス アクセス リストの機能」(P.362)
- ・「イーサネット サービス アクセス リスト エントリのシーケンス番号」(P.364)

イーサネット サービス アクセス リスト機能のハイライト

イーサネット サービス アクセス リストには、次の機能のハイライトがあります。

- ・ 特定のシーケンス番号を使用してアクセス リストのカウンタをクリアする機能。
- ・ 別のアクセス リストに既存のアクセス リストの内容をコピーする機能。
- ・ ユーザがシーケンス番号を `permit` または `deny` ステートメントに追加し、そのようなステートメントのシーケンスの再設定、追加、または名前付きアクセス リストからの削除を行うことができるようになります。
- ・ パケットを転送するためにインターフェイスでパケット フィルタリングを実行します。
- ・ イーサネット サービス ACL は、インターフェイス、VLAN サブインターフェイス、バンドルイーサネット インターフェイス、EFP、バンドルイーサネット インターフェイスを介した EFP で適用できます。イーサネット サービス ACL のアトミック置換は、これらの物理インターフェイスでサポートされています。

イーサネット サービス アクセス リストの目的

イーサネット サービス アクセス リストは、ACL ベースの転送 (ABF) を使用して、ネットワークを介して移動するパケットおよび場所を制御するパケット フィルタリングを実行します。そのような制御は、着信および発信ネットワーク トラフィックを制限し、ポート レベルでネットワークにユーザおよびデバイスのアクセスを制限するために役立ちます。

イーサネット サービス アクセス リストの機能

イーサネット サービス アクセス リストは、レイヤ 2 設定に適用される、`permit` および `deny` ステートメントで構成される順序付きリストです。アクセス リストには、参照に使用される名前があります。

アクセス リストを設定して名前を付けることは可能ですが、アクセス リストを受け取るコマンドによってアクセス リストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセス リストを参照できます。アクセス リストで、ルータに到達するレイヤ 2 トラフィック、またはルータ経由で送信されるレイヤ 2 トラフィックは制御できますが、ルータが送信元のトラフィックは制御できません。

イーサネット サービス アクセス リストのプロセスおよびルール

イーサネット サービス アクセス リストの設定時は、次のプロセスとルールを使用します。

- ソフトウェアは、アクセス リストの条件に対してフィルタされる各パケットの送信元アドレスや宛先アドレスをテストします。一度に 1 つの条件 (**permit** または **deny** ステートメント) がテストされます。
- パケットがアクセス リスト ステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リスト ステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。ソフトウェアがパケットを許可するか拒否するかは、パケットが一致する最初のエントリによって決定されます。つまり、一致すると、以降のエントリは考慮されません。
- アクセス リストがアドレスまたはプロトコルを拒否する場合は、ソフトウェアはパケットを廃棄します。
- いずれの条件とも一致しなかった場合、各アクセス リストは表記されないか暗黙の **deny** ステートメントで終了するため、ソフトウェアはパケットをドロップします。言い換えると、パケットが各ステートメントに対してテストされたときまでに許可または拒否されないと、このパケットは拒否されます。
- アクセス リストには **permit** ステートメントを 1 つ以上含める必要があります。そうしないと、パケットはすべて拒否されます。
- 最初に一致が見つかった後はソフトウェアによる条件のテストが終了するため、条件の順序は重要です。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- インバウンドアクセス リストは、ルータに到達するパケットを処理します。着信パケットの処理後に、アウトバウンド インターフェイスへのルーティングが行われます。インバウンドアクセス リストが効率的なのは、フィルタリング テストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。テストでパケットが許可される場合、ルーティングのために処理されます。インバウンド リストの場合、許可とは、インバウンド インターフェイスでパケットの受信後に処理が継続されることを示します。拒否とは、パケットが廃棄されることを示します。
- アウトバウンドアクセス リストの場合、パケットの処理後にルータから送信されます。着信パケットはアウトバウンド インターフェイスにルーティングされてから、アウトバウンドアクセス リストで処理されます。アウトバウンド リストの場合、許可とは、出力バッファに対して送信されることを示し、拒否とは、パケットが廃棄されることを示します。
- 使用中のアクセス グループによってアクセス リストが適用されている場合、そのアクセス リストは削除できません。アクセス リストを削除するには、アクセス リストを参照しているアクセス グループを削除してから、アクセス リストを削除します。
- アクセス リストは、**ethernet-services access-group** コマンドを使用する前に存在している必要があります。

イーサネット サービス アクセス リストを作成する際に役立つヒント

イーサネット サービス アクセス リストの作成時は、次の点に注意してください。

- アクセス リストは、インターフェイスに適用する前に作成します。
- より具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。

送信元アドレスおよび宛先アドレス

送信元 MAC アドレスと宛先 MAC アドレスの 2 つのフィールドは、アクセス リストの基礎として最も一般的なフィールドです。送信元 MAC アドレスを指定して、特定のネットワーク デバイスまたはホストからのパケットを制御します。宛先 MAC アドレスを指定して、特定のネットワーク デバイスまたはホストに送信されるパケットを制御します。

イーサネット サービス アクセス リスト エントリのシーケンス番号

イーサネット サービス アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡単になります。アクセス リスト エントリのシーケンス番号機能を使用すると、アクセス リスト エントリにシーケンス番号を追加して、シーケンス番号を再設定できます。新しいエントリを追加する場合、アクセス リストの目的の位置に挿入されるようにシーケンス番号を選択します。必要に応じて、アクセス リストの現在のエントリ順序を変更して、新しいエントリを挿入できる余地を作成します。

シーケンス番号の動作

次に、シーケンス番号の動作について詳細に説明します。

- シーケンス番号のないエントリが適用された場合、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は 10 ずつ増分されます。最大シーケンス番号は 2147483646 です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- ACL エントリは、トラフィック フローおよびハードウェア パフォーマンスに影響を与えることなく追加できます。
- ルート スイッチ プロセッサ (RSP) とインターフェイス カードにあるエントリのシーケンス番号が常に同期されるよう、分散サポートが提供されます。

レイヤ 2 アクセス リストの実装方法

この項では、次の手順について説明します。

- 「レイヤ 2 アクセス リスト実装の制約事項」 (P.365)
- 「イーサネット サービス アクセス リストの設定」 (P.366) (任意)
- 「イーサネット サービス アクセス リストの適用」 (P.367) (任意)

- 「アクセス リスト エントリの並べ替え」(P.371) (任意)

レイヤ 2 アクセス リスト実装の制約事項

次の制約事項が、イーサネット サービス アクセス リストの実装に適用されます。

- イーサネット アクセス リストは、レイヤ 2 インターフェイスだけでサポートされます。
- イーサネット サービス アクセス リストは、管理インターフェイスではサポートされていません。
- イーサネット サービス アクセス リストは、ルーテッドインターフェイスではサポートされていません。
- NetIO (ソフトウェア低速パス) は、イーサネット サービス アクセス リストではサポートされません。

イーサネット サービス アクセス リストの設定

このタスクでは、イーサネット サービス アクセス リストを設定します。

手順の概要

1. **configure**
2. **ethernet-service access-list name**
3. **[sequence-number] {permit | deny} {src-mac-address src-mac-mask | any | host} [{ethertype-number} | vlan min-vlan-ID [max-vlan-ID]] [cos cos-value] [dei] [inner-vlan min-vlan-ID [max-vlan-ID]] [inner-cos cos-value] [inner-dei]**
4. 必要に応じてステップ 3 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、**no sequence-number** コマンドを使用します。
5. **end**
または
commit
6. **show access-lists ethernet-services [access-list-name | maximum | standby | summary]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例 : RP/0/RSP0/CPU0:router# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ethernet-service access-list name 例 : RP/0/RSP0/CPU0:router(config)# ethernet-service access-list L2ACL2	イーサネット サービス アクセス リスト コンフィギュレーション モードを開始し、アクセス リスト L2ACL2 を設定します。
ステップ 3	[sequence-number] {permit deny} {src-mac-address src-mac-mask any host} [{ethertype-number} vlan min-vlan-ID [max-vlan-ID]] [cos cos-value] [dei] [inner-vlan min-vlan-ID [max-vlan-ID]] [inner-cos cos-value] [inner-dei] 例 : RP/0/RSP0/CPU0:router(config-es-al)# 20 permit 1.2.3 3.2.1 or RP/0/RSP0/CPU0:router(config-es-al)# 30 deny any dei	1 つ以上の許可条件または拒否条件を指定します。これによって、パケットが通過するかドロップされるかが決まります。
ステップ 4	必要に応じてステップ 3 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、 no sequence-number コマンドを使用します。	アクセス リストの変更を可能にします。

コマンドまたはアクション	目的
<p>ステップ 5</p> <pre>end または commit</pre> <p>例： RP/0/RSP0/CPU0:router(config-es-acl)# end または RP/0/RSP0/CPU0:router(config-es-acl)# commit </p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: – yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。 – no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、commit コマンドを使用します。
<p>ステップ 6</p> <pre>show access-lists ethernet-services [access-list-name maximum standby summary]</pre> <p>例： RP/0/RSP0/CPU0:router# show access-lists ethernet-services L2ACL1 </p>	<p>(任意) 指定されたイーサネット サービス アクセス リストの内容を表示します。</p> <ul style="list-style-type: none"> • デフォルトとして、すべてのイーサネット アクセス リストの内容が表示されます。

次の作業

イーサネット サービス アクセス リストの作成後に、インターフェイスに適用する必要があります。アクセス リストの適用方法の詳細については、[イーサネット サービス アクセス リストの適用](#)の項を参照してください。

イーサネット サービス アクセス リストの適用

アクセス リストを作成したら、動作するようにアクセス リストを参照する必要があります。アクセス リストは、発信または着信インターフェイスのいずれかに適用できます。この項では、端末回線およびネットワーク インターフェイスの両方に対してこのタスクを実行する方法のガイドラインについて説明します。

着信アクセス リストでは、パケットを受信した後で、Cisco IOS XR ソフトウェアは、アクセス リストに対してパケットの送信元 MAC アドレスを検査します。アクセス リストがアドレスを許可する場合は、ソフトウェアはパケットの処理を継続します。アクセス リストがアドレスを拒否する場合は、ソフトウェアはパケットを廃棄します。

発信アクセス リストでは、パケットを受信して制御インターフェイスにルーティングした後で、ソフトウェアは、アクセス リストに対してパケットの送信元 MAC アドレスを検査します。アクセス リストがアドレスを許可した場合、ソフトウェアはパケットを送信します。アクセス リストがアドレスを拒否する場合は、ソフトウェアはパケットを廃棄します。



(注)

空のアクセス リスト（アクセス コントロール エLEMENTが含まれていない）は、インターフェイスに適用できません。

インターフェイスへのアクセスの制御

ここでは、インターフェイスへのアクセスを制限するためにアクセス リストをそのインターフェイスに適用します。アクセス リストは、発信または着信インターフェイスのいずれかに適用できます。

手順の概要

1. **configure**
2. **interface type instance**
3. **ethernet-service access-group access-list-name {ingress | egress}**
4. **end**
または
commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例 : RP/0/RSP0/CPU0:router# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type instance 例 : RP/0/RSP0/CPU0:router(config)# interface gigabitethernet 0/2/0/2	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • <i>type</i> 引数は、インターフェイス タイプを指定します。インターフェイス タイプの詳細については、疑問符 (?) オンライン ヘルプ機能を使用してください。 • <i>instance</i> 引数は、物理インターフェイス インスタンスまたは仮想インスタンスのいずれかを指定します。 <ul style="list-style-type: none"> – 物理インターフェイス インスタンスの名前の表記は <i>rack/slot/module/port</i> です。値を区切るスラッシュ (/) は、表記の一部として必須です。 – 仮想インターフェイス インスタンスの番号の範囲は、インターフェイス タイプによって異なります。

コマンドまたはアクション	目的
<p>ステップ 3 <code>ethernet-services access-group access-list-name {ingress egress}</code></p> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# ethernet-services access-group p-in-filter ingress</pre> <pre>RP/0/RSP0/CPU0:router(config-if)# ethernet-services access-group p-out-filter egress</pre>	<p>インターフェイスへのアクセスを制御します。</p> <ul style="list-style-type: none">• <code>access-list-name</code> 引数を使用して、特定のイーサネット サービス アクセス リストを指定します。• ingress キーワードを使用すると着信パケットをフィルタリングでき、または egress キーワードを使用すると発信パケットをフィルタリングできます。 <p>次の例では、GigabitEthernet インターフェイス 0/2/0/2 からの受信および送信パケットにフィルタを適用します。</p>

コマンドまたはアクション	目的
<p>ステップ 4</p> <pre>end または commit</pre> <p>例 :</p> <pre>RP/0/RSP0/CPU0:router(config-if)# end または RP/0/RSP0/CPU0:router(config-if)# commit</pre>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> • end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> - yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。 - no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 - cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、commit コマンドを使用します。

イーサネット サービス アクセス リストのコピー

このタスクでは、イーサネット サービス アクセス リストをコピーします。

手順の概要

1. `copy access-list ethernet-service source-acl destination-acl`
2. `show access-lists ethernet-services [access-list-name | maximum | standby | summary]`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<pre>copy access-list ethernet-service source-acl destination-acl</pre> <p>例:</p> <pre>RP/0/RSP0/CPU0:router# copy access-list ethernet-service list-1 list-2</pre>	<p>既存のイーサネット サービス アクセス リストのコピーを作成します。</p> <ul style="list-style-type: none"> • コピー元のアクセス リストの名前を指定するには、<i>source-acl</i> 引数を使用します。 • コピー元アクセス リストの内容のコピー先を指定するには、<i>destination-acl</i> 引数を使用します。 <ul style="list-style-type: none"> – <i>destination-acl</i> 引数は一意な名前である必要があり、アクセス リストに <i>destination-acl</i> 引数名が存在する場合は、そのアクセス リストはコピーされません。
ステップ2	<pre>show access-lists ethernet-services [access-list-name maximum standby summary]</pre> <p>例:</p> <pre>RP/0/RSP0/CPU0:router# show access-lists ethernet-services list-2</pre>	<p>(任意) 指定されたイーサネット サービス アクセス リストの内容を表示します。たとえば、出力を確認して、コピー先アクセス リスト <i>list-2</i> に、コピー元アクセス リスト <i>list-1</i> のすべての情報が含まれていることを調べます。</p>

アクセス リスト エントリの並べ替え

ここでは、名前付きアクセス リストのエントリにシーケンス番号を再割り当てする例を示します。アクセス リストの並べ替えは任意です。

手順の概要

1. `resequence access-list ethernet-service access-list-name [starting-sequence-number [increment]]`
2. `end`
または
`commit`
3. `show access-lists ethernet-services [access-list-name | maximum | standby | summary]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<pre>resequence access-list ethernet-service access-list-name [starting-sequence-number [increment]]</pre> <p>例 : RP/0/RSP0/CPU0:router# resequence access-list ethernet-service L2ACL2 20 10</p>	<p>(任意) 目的の開始シーケンス番号およびシーケンス番号の増分を使用して、指定されたイーサネット サービス アクセス リストを並べ替えます。</p> <ul style="list-style-type: none"> 次の例では、L2ACL2 という名前のイーサネット サービス アクセス リストを並べ替えます。開始シーケンス番号は 20、増分は 10 です。増分を選択しない場合、デフォルトの増分 10 が使用されます。 <p>(注) 並べ替えプロセス中に終了番号が許可された最大シーケンス番号を超えることがわかった場合、設定は無効になり、拒否されます。シーケンス番号は変更されません。</p>
ステップ 2	<pre>end または commit</pre> <p>例 : RP/0/RSP0/CPU0:router# end または RP/0/RSP0/CPU0:router# commit</p>	<p>設定変更を保存します。</p> <ul style="list-style-type: none"> end コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、commit コマンドを使用します。
ステップ 3	<pre>show access-lists ethernet-services [access-list-name maximum standby summary]</pre> <p>例 : RP/0/RSP0/CPU0:router# show access-lists ethernet-services L2ACL2</p>	<p>(任意) 指定されたイーサネット サービス アクセス リストの内容を表示します。</p> <ul style="list-style-type: none"> 出力を確認し、アクセス リストに更新された情報が含まれることを確認します。

レイヤ 2 アクセス リストを実装するための設定例

ここでは、次の設定例を示します。

- 「アクセス リストのエントリの並べ替え : 例」 (P.373)
- 「シーケンス番号を指定したエントリの追加 : 例」 (P.373)

アクセス リストのエントリの並べ替え : 例

次に、アクセス リストの並べ替え例を示します。並べ替えられたアクセス リストの先頭の値は 1、増分値は 2 です。後続のエントリはユーザ指定の増分値に基づいて並べられています。範囲は 1 ~ 2147483646 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
ethernet service access-list acl_1
10 permit 1.2.3 4.5.6
20 deny 2.3.4 5.4.3
30 permit 3.1.2 5.3.4 cos 5

resequence access-list ethernet service acl_1 10 20

show access-list ethernet-service acl1_1

ipv4 access-list acl_1
 10 permit 1.2.3 4.5.6
 30 deny 2.3.4 5.4.3
 50 permit 3.1.2 5.3.4 cos 5
```

シーケンス番号を指定したエントリの追加 : 例

この例では、新しいエントリをイーサネット サービス アクセス リスト acl_5 に追加します。

```
ethernet-service access-list acl_5
2 permit 1.2.3 5.4.3
5 permit 2.3.4. 6.5.4 cos 3
10 permit any dei
20 permit 6.5.4 1.3.5 VLAN vlan3

configure
  ethernet-service access-list acl_5
  15 permit 1.5.7 7.5.1
end

ethernet-service access-list acl_5
2 permit 1.2.3 5.4.3
5 permit 2.3.4. 6.5.4 cos 3
10 permit any dei
15 permit 1.5.7 7.5.1
20 permit 6.5.4 1.3.5 VLAN vlan3
```

その他の参考資料

ここでは、Cisco ASR 9000 シリーズ ルータでのイーサネット サービス アクセス リストの実装に関する参考資料を紹介します。

関連資料

関連項目	ドキュメント名
イーサネット サービス アクセス リスト コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドラインおよび例	『Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference』の「Ethernet Services (Layer 2) Access List Commands on Cisco ASR 9000 Series Routers」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用している MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
<p>シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

