



## IPv6 ACL の設定

- 機能情報の確認, 1 ページ
- IPv6 ACL の概要, 1 ページ
- IPv6 ACL の制限, 3 ページ
- IPv6 ACL のデフォルト設定, 4 ページ
- IPv6 ACL の設定方法, 4 ページ
- インターフェイスへの IPv6 ACL の適用方法, 9 ページ
- IPv6 ACL のモニタリング, 10 ページ
- Additional References, 11 ページ

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## IPv6 ACL の概要

IP Version 6 (IPv6) アクセスコントロールリスト (ACL) を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4 (IPv4) の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN ベース フィーチャセットが稼働している場合、入ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。



(注) IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理 (SDM) テンプレートがスイッチに設定されている必要があります。テンプレートの選択は、`sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}` グローバル コンフィギュレーション コマンドで行います。

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス (SVI)、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンドトラフィックまたはインバウンドトラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、インバウンドおよびアウトバウンドのレイヤ 2 インターフェイスでトラフィックでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

スイッチは、IPv6 トラフィックの Virtual LAN (VLAN) ACL (VLAN マップ) をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

## スイッチ スタックおよび IPv6 ACL

アクティブ スイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバに配信します。

スタンバイ スイッチがアクティブ スイッチを引き継ぐと、ACL 設定がすべてのスタック メンバに配信されます。メンバ スイッチは、新しいスアクティブ スイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブ スイッチは変更内容をすべてのスタック メンバに配信します。

## 他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル (ICMP) キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラーメッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（たとえば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラーメッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェアメモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラーメッセージが記録されます。

## IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL (**reflect** キーワード) をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL (VLAN マップ) はサポートしていません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、スイッチスタックでだけサポートされています。スイッチは、コントロールプレーン (着信) IPv6 ACL だけをサポートします。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス (物理ポートまたは SVI) に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセスコントロールエントリ (ACE) を追加しようとする場合、スイッチは現在インターフェイスに接続されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム (IPv4 では **fragments** キーワード) がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。

- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ホップバイホップ オプションがあるルーテッド パケットまたはブリッジド パケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

## IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

## IPv6 ACL の設定方法

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

- 1 IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
- 2 IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。
- 3 インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

## 手順の概要

1. **configure terminal**
2. **[no]{ipv6 access-list list-name| client permit-control-packets| log-update threshold| role-based list-name}**
3. **[no]{deny | permit} protocol {source-ipv6-prefix/prefix-length|any threshold| host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]][dscp value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]**
4. **{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6- prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [rst] [routing] [sequence value] [syn] [time-range name] [urg]**
5. **{deny | permit} udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port | protocol}] [routing] [sequence value] [time-range name]**
6. **{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [icmp-type [icmp-code]] [icmp-message] [dscp value] [log] [log-input] [routing] [sequence value] [time-range name]**
7. **end**
8. **show ipv6 access-list**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>[no]{ipv6 access-list list-name  client permit-control-packets  log-update threshold  role-based list-name}</b>  例： Switch(config)# <b>ipv6 access-list example_acl_list</b>	IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 3	<b>[no]{deny   permit} protocol {source-ipv6-prefix/prefix-length any threshold  host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length   any   host destination-ipv6-address} [operator [port-number]][dscp value]</b>	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。  <ul style="list-style-type: none"> <li>• protocol には、インターネットプロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ~ 255 の整数を使用できます。</li> </ul>

コマンドまたはアクション	目的
<p>[fragments] [log] [log-input] [routing] [sequence value] [time-range name]</p>	<ul style="list-style-type: none"> <li>• <i>source-ipv6-prefix/prefix-length</i> または <i>destination-ipv6-prefix/prefix-length</i> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します (RFC 2373 を参照)。</li> <li>• IPv6 プレフィックス <i>::/0</i> の短縮形として、<i>any</i> を入力します。</li> <li>• <b>host</b> <i>source-ipv6-address</i> または <i>destination-ipv6-address</i> には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。</li> <li>• (任意) <b>operator</b> には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、<b>lt</b> (より小さい)、<b>gt</b> (より大きい)、<b>eq</b> (等しい)、<b>neq</b> (等しくない)、<b>range</b> (包含範囲) があります。 <i>source-ipv6-prefix/prefix-length</i> 引数のあとの <b>operator</b> は、送信元ポートに一致する必要があります。 <i>destination-ipv6-prefix/prefix-length</i> 引数のあとの <b>operator</b> は、宛先ポートに一致する必要があります。</li> <li>• (任意) <b>port-number</b> は、0 ~ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。</li> <li>• (任意) <b>dscp value</b> を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ~ 63 です。</li> <li>• (任意) <b>fragments</b> を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが <i>ipv6</i> の場合だけです。</li> <li>• (任意) <b>log</b> を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。<b>log-input</b> を指定すると、ログ エントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。</li> <li>• (任意) <b>routing</b> を入力して、IPv6 パケットのルーティングを指定します。</li> <li>• (任意) <b>sequence value</b> を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ~ 4,294,967,295 です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) <b>time-range name</b> を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。</li> </ul>
ステップ 4	<pre>{deny   permit} tcp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6- prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port   protocol}] [psh] [range {port   protocol}] [rst] [routing] [sequence value] [syn] [time-range name] [urg]</pre>	<p>(任意) TCP アクセス リストおよびアクセス条件を定義します。</p> <p>TCP の場合は <b>tcp</b> を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。</p> <ul style="list-style-type: none"> <li>• <b>ack</b> : 確認応答 (ACK) ビットセット</li> <li>• <b>established</b> : 確立された接続。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、照合が行われます。</li> <li>• <b>fin</b> : 終了ビットセット。送信元からのデータはそれ以上ありません。</li> <li>• <b>neq {port   protocol}</b> : 所定のポート番号上にないパケットだけを照合します。</li> <li>• <b>psh</b> : プッシュ機能ビットセット</li> <li>• <b>range {port   protocol}</b> : ポート番号の範囲内のパケットだけを照合します。</li> <li>• <b>rst</b> : リセットビットセット</li> <li>• <b>syn</b> : 同期ビットセット</li> <li>• <b>urg</b> : 緊急ポインタ ビットセット</li> </ul>
ステップ 5	<pre>{deny   permit} udp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port   protocol}] [range {port   protocol}] [routing] [sequence value] [time-range name]]</pre>	<p>(任意) UDP アクセス リストおよびアクセス条件を定義します。</p> <p>ユーザ データグラム プロトコルの場合は、<b>udp</b> を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前であればなりません。UDP の場合、established パラメータは無効です。</p>
ステップ 6	<pre>{deny   permit} icmp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]] [icmp-type [icmp-code]] [icmp-message] [dscp value]</pre>	<p>(任意) ICMP アクセス リストおよびアクセス条件を定義します。</p> <p>インターネット制御メッセージプロトコルの場合は、<b>icmp</b> を入力します。ICMP パラメータは手順 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。</p>

	コマンドまたはアクション	目的
	[log] [log-input] [routing] [sequence value] [time-range name]	<ul style="list-style-type: none"> <li>• <i>icmp-type</i> : ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。</li> <li>• <i>icmp-code</i> : ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。</li> <li>• <i>icmp-message</i> : ICMP パケットを 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でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。</li> </ul>
ステップ 7	end	特権 EXEC モードに戻ります。
ステップ 8	show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 9	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定のアクセス リストから拒否または許可条件を削除するには、キーワードを指定して **no {deny | permit} IPv6 access-list** コンフィギュレーション コマンドを使用します。

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番目の拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番目の拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番目の許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番目の許可エントリは必要です。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

### 次の作業

インターフェイスに IPv6 ACL をアタッチします。



# インターフェイスへの IPv6 ACL の適用方法

レイヤ 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **no switchport**
4. **ipv6 address pv6-address**
5. **ipv6 traffic-filter access-list-name {in | out}**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： Switch# <b>configure terminal</b>	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	<b>interface interface-id</b>	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を特定して、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。
ステップ 3	<b>no switchport</b>	ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変化します。
ステップ 4	<b>ipv6 address pv6-address</b>	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。
ステップ 5	<b>ipv6 traffic-filter access-list-name {in   out}</b>	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。  (注) out キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。スイッチで IP ベース フィーチャセットが稼働している場合、out キーワードはレイヤ 3 インターフェイスではサポートされません。

	コマンドまたはアクション	目的
ステップ 6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b>	アクセス リストの設定を確認します。
ステップ 8	<b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

インターフェイスからアクセス リストを削除するには、**no ipv6 traffic-filter access-list-name** インターフェイス コンフィギュレーション コマンドを使用します。

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

## IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

コマンド	目的
<b>show access-lists</b>	スイッチに設定されたすべてのアクセス リストを表示します。
<b>show ipv6 access-list</b> [ <i>access-list-name</i> ]	設定済みのすべての IPv6 アクセス リストまたは名前前で指定されたアクセス リストを表示します。

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
  10 permit ip any any
IPv6 access list ipv6
  permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
```

```
permit udp any any sequence 30
IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

## Additional References

### Related Documents

Related Topic	Document Title
IPv6 security configuration topics	IPv6 Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html">http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/xe-3se/3850/ipv6-xe-3se-3850-library.html</a>
IPv6 command reference	IPv6 Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) <a href="http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html">http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-xe-3se-3850-cr-book.html</a>

### MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></p>