CHAPTER 42

AutoSecure の使用

この章では、AutoSecure 機能を使用する手順について説明します。Release 12.2(33)SXH 以降のリリースでは、AutoSecure 機能がサポートされます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

この章で説明する内容は、次のとおりです。

AutoSecure の概要

AutoSecure 機能を使用すると、スイッチのセキュリティ機能すべてを理解しなくてもスイッチのセキュリティを簡単に保護できます。AutoSecure は簡単なセキュリティ設定プロセスです。不必要なシステム サービスをディセーブルにし、基本的な推奨セキュリティ ポリシーをイネーブルにすることで、セキュアなネットワーキング サービスを保証します。

注意 AutoSecure はスイッチのセキュリティ保護に役立ちますが、スイッチの完全なセキュリティを保証するものではありません。

ここでは、AutoSecure の機能について説明します。

AutoSecure の利点

AutoSecure は、スイッチのセキュリティを強化するための各種のメカニズムを提供します。

スイッチのセキュリティ設定の簡素化

AutoSecure は、スイッチのセキュリティ機能の設定を完全に自動化します。AutoSecure はセキュリティ ホールとして悪用されるおそれがある、デフォルトでイネーブルになっているある種の機能をディセーブルにします。

AutoSecure は、個々のニーズに応じて次の 2 つのモードで実行できます。

- インタラクティブ モード：サービスおよびその他のセキュリティ機能を指示に従ってイネーブルまたはディセーブルにするオプションです。各オプションのデフォルト設定が示されます。
- 非インタラクティブ モード：シスコの推奨するデフォルト設定を自動的に実行します。

パスワード セキュリティの強化

AutoSecure は、スイッチにアクセスする際のセキュリティを向上させるために次のメカニズムを提供します。

- 最低限必要なパスワード長を指定できます。これにより、ネットワーク上で広く使用されている「lab」や「cisco」などの脆弱なパスワードの使用を制限できます。

  最短パスワード長を設定するには、**security passwords min-length** コマンドを使用します。
- ログイン試行の失敗回数が設定したしきい値を超えると、Syslog メッセージが生成されるようにすることができます。

  ログイン試行の失敗許容回数（しきい値率）を設定するには、**security authentication failure rate** コマンドを使用します。

システム ロギング メッセージのサポート

システム ロギング メッセージは、実行コンフィギュレーションに適用されている AutoSecure 設定に対してあとから変更が行われた場合にその変更をキャプチャします。その結果、AutoSecure を実行するときにさらに詳細な監査証跡が可能になります。

マネジメント プレーンのセキュリティ保護

AutoSecure により、スイッチ管理インターフェイス（マネジメント プレーン）およびデータ ルーティングとスイッチングの機能（フォワーディング プレーン。「フォワーディング プレーンのセキュリティ保護」（P.42-6）を参照）を保護できます。マネジメント プレーンのセキュリティ保護は、セキュリティ攻撃で悪用される可能性のある特定のグローバル サービスおよびインターフェイス サービスをディセーブルにし、攻撃の脅威を最小限に抑える役に立つグローバル サービスをイネーブルにすることで実施されます。また、セキュア アクセスおよびセキュア ロギングをスイッチに設定します。

注意　使用している装置を Network Management（NM; ネットワーク管理）アプリケーションによって管理している場合は、マネジメント プレーンのセキュリティ保護によって HTTP サーバなどのいくつかのサービスがディセーブルになり、NM アプリケーションのサポートが中断されます。

次に、AutoSecure がマネジメント プレーンのセキュリティを保護する方法について説明します。

- 「グローバル サービスのディセーブル化」（P.42-3）
- 「インターフェイス単位のサービスのディセーブル化」（P.42-4）
- 「グローバル サービスのイネーブル化」（P.42-4）
- 「スイッチへのセキュアなアクセス」（P.42-4）
- 「セキュリティのためのロギングの強化」（P.42-5）

グローバル サービスのディセーブル化

AutoSecure は、スイッチの次のグローバル サービスを、ユーザにプロンプトを表示せずにディセーブルにします。

- Finger：攻撃前にシステムに関する情報を収集します（予備調査）。
- PAD：すべての Packet Assembler/Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）コマンドおよび PAD 装置とアクセス サーバの間の接続をイネーブルにします。
- スモール サーバ：TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）診断ポート攻撃を引き起こします。送信者は、スイッチの UDP 診断サービスに偽の要求を大量に送信して、すべての CPU リソースを消費させます。
- BOOTP サーバ：BOOTP はセキュアではないプロトコルです。攻撃で悪用されます。
- HTTP サーバ：Secure HTTP サーバを使用するか、関連する ACL を持つ HTTP サーバに組み込まれた認証を使用しなければ、HTTP サーバはセキュアではなく、攻撃で悪用されます（HTTP サーバをイネーブルにする必要がある場合は、適切な認証またはアクセス リストを要求されます）。

（注）　SDM を使用している場合は、**ip http server** コマンドを使用して、HTTP サーバを手動でイネーブルにする必要があります。

- 識別サービス：セキュアではないプロトコル（RFC 1413 で定義）です。外部ホストから TCP ポートに識別情報を照会できます。攻撃者は、ID サーバにあるユーザに関する個人的な情報にアクセスできます。
- CDP：大量の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）パケットがスイッチに送信されると、スイッチの利用可能なメモリが消費され、スイッチがクラッシュします。

（注）　CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を行うことができなくなります。

- NTP：認証またはアクセス制御を行っていない場合は、Network Time Protocol（NTP）はセキュアではありません。攻撃者は、このプロトコルを使用して NTP パケットを送信してスイッチをクラッシュまたは過負荷状態にさせます。

  NTP が必要な場合は、MD5 および **ntp access-group** コマンドを使用して、NTP 認証を設定する必要があります。NTP がグローバルでイネーブルになっている場合は、NTP を必要としないインターフェイスすべてでディセーブルにします。

- 送信元ルーティング：送信元ルーティングはデバッグ目的でだけ提供されており、それ以外の場合はディセーブルにする必要があります。そうしないと、パケットがスイッチのアクセス制御メカニズムのいくつかを回避する可能性があります。

インターフェイス単位のサービスのディセーブル化

AutoSecure は、スイッチの次のインターフェイス単位のサービスを、ユーザにプロンプトを表示せずにディセーブルにします。

- ICMP リダイレクト：すべてのインターフェイス上でディセーブルにします。機能が正しく設定されているネットワークにとっては特に有用というわけではなく、攻撃者はセキュリティ ホールを悪用するためにこの機能を使用することがあります。
- ICMP 到達不能：すべてのインターフェイス上でディセーブルにします。Internet Control Management Protocol（ICMP）到達不能は、ICMP ベースの DoS 攻撃（サービス拒絶攻撃）を可能にする方法の 1 つとして知られています。
- ICMP マスク応答メッセージ：すべてのインターフェイス上でディセーブルにします。ICMP マスク応答メッセージにより、攻撃者はインターネットワーク内の特定のサブネットワークのサブネット マスクを取得できます。
- プロキシ ARP：すべてのインターフェイス上でディセーブルにします。プロキシ ARP 要求は、DoS 攻撃を可能にする方法の 1 つとして知られています。これは、攻撃者が繰り返し送信した要求に応答しようとすることで、スイッチの利用可能な帯域幅およびリソースを消費するためです。
- ダイレクト ブロードキャスト：すべてのインターフェイス上でディセーブルにします。DoS のために SMURF アタックを引き起こす可能性があります。
- Maintenance Operations Protocol（MOP; メンテナンス オペレーション プロトコル）サービス：すべてのインターフェイス上でディセーブルにします。

グローバル サービスのイネーブル化

AutoSecure は、スイッチの次のグローバル サービスを、ユーザにプロンプトを表示せずにイネーブルにします。

- **service password-encryption** コマンド：パスワードが設定に表示されないようにします。
- **service tcp-keepalives-in** コマンド、**service tcp-keepalives-out** コマンド：異常終了した TCP セッションを確実に削除します。

スイッチへのセキュアなアクセス

注意　使用している装置を NM アプリケーションによって管理している場合は、スイッチへのアクセスのセキュリティを保護することで重要なサービスがオフになったり、NM アプリケーションのサポートが中断されたりする場合があります。

AutoSecure では、スイッチへのアクセスのセキュリティを保護するために次のオプションを利用できます。

- テキスト バナーがない場合は、バナーを追加するよう要求されます。この機能は、次のサンプル バナーを提供します。

```
Authorized access only
    This system is the property of ABC Enterprise
    Disconnect IMMEDIATELY if you are not an authorized user!
```

```
Contact abc@example.com +1 408 5551212 for help.
```

- ログインおよびパスワード（サポートされている場合は、シークレット パスワードが望ましい）は、コンソール回線、AUX 回線、VTY 回線、および TTY 回線上で設定されます。**transport input** コマンドと **transport output** コマンドもまた、これらの回線上すべてで設定されます（有効な転送方法は、Telnet および Secure Shell（SSH; セキュア シェル）だけです）。**exec-timeout** コマンドは、コンソール回線および AUX 回線で 10 に設定されます。
- 装置上のイメージが暗号化イメージである場合、AutoSecure はスイッチにアクセスし、ファイル転送を行うために SSH および SCP をイネーブルにします。**ip ssh** コマンドの **timeout** *seconds* および **authentication-retries** *integer* オプションは最小数に設定されます（Telnet および FTP は、この操作による影響を受けずに引き続き動作します）。
- スイッチで Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用しないとユーザが指定する場合は、次の機能のいずれかが発生します。
  - インタラクティブ モードでは、ユーザはコミュニティ ストリングの値にかかわらず SNMP をディセーブルにするかどうか尋ねられます。コミュニティ ストリングはパスワードと同様に機能し、スイッチ上のエージェントへのアクセスを規制します。
  - 非インタラクティブ モードでは、コミュニティ ストリングが public または private である場合に、SNMP はディセーブルになります。

（注）　AutoSecure がイネーブルになると、装置の監視および設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。

- Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）が設定されていない場合は、AutoSecure はローカル AAA を設定します。AutoSecure はユーザにスイッチ上でローカル ユーザ名およびパスワードを設定するよう要求します。

セキュリティのためのロギングの強化

AutoSecure は次のロギング オプションを提供します。これにより、セキュリティ インシデントを特定し、それに対応できます。

- すべてのデバッグ メッセージおよびログ メッセージに対するシーケンス番号およびタイム スタンプ。このオプションは、ロギング メッセージの監査時に役立ちます。
- ログイン関連イベントに対するロギング メッセージ。たとえば、ログイン攻撃が検出され、スイッチが待機モードに入ると、メッセージ「Blocking Period when Login Attack Detected」が表示されます（待機モードでは、スイッチは Telnet、HTTP、または SSH を使用したログイン試行を許可しません）。
- **logging console critical** コマンド。システム ロギング（Syslog）メッセージをすべての利用可能な TTY 回線に送信し、メッセージを重大度に基づいて制限します。
- **logging buffered** コマンド。ロギング メッセージを内部バッファにコピーし、バッファに記録されるメッセージを重大度に基づいて制限します。
- **logging trap debugging** コマンド。重大度がデバッグよりも高いコマンドすべてをロギング サーバに送信できるようにします。

フォワーディング プレーンのセキュリティ保護

スイッチのフォワーディング プレーンに対する攻撃の危険を最小限に抑えるために、AutoSecure には次の機能があります。

- Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）: AutoSecure はスイッチ上の CEF または distributed CEF（dCEF; 分散 CEF）を可能なかぎりイネーブルにします。新しい宛先に対するトラフィックが到着し始めるとキャッシュ エントリを構築する必要がないため、大量のトラフィックに多くの宛先が指定されている場合でも CEF の動作は他のモードよりさらに予測可能になります。SYN 攻撃を受けている間も、CEF が設定されているスイッチの動作は、従来のキャッシュを使用するスイッチの動作よりもさらに優れています。

（注） CEF は従来のキャッシュよりも多くのメモリを消費します。

- 厳密な Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）が利用可能な場合は、偽装された（スプーフィングされた）送信元 IP アドレスが入ってくることで引き起こされる問題を軽減するためにスイッチ上で設定できます。uRPF は、確認可能な送信元 IP アドレスを持たない IP パケットを廃棄します。
- ハードウェアのレート制限：AutoSecure では、ユーザにプロンプトを表示することなく、次のトラフィック タイプのハードウェアのレート制限をイネーブルにします。
  - IP エラー
  - RPF 失敗
  - ICMP のルートなしメッセージ
  - ICMP の ACL ドロップ メッセージ
  - IPv4 マルチキャスト FIB 欠落メッセージ
  - 部分的にスイッチングされている IPv4 マルチキャスト フローのメッセージ

  AutoSecure では、次のトラフィック タイプについて、ハードウェアのレート制限のオプションが利用できます。
  - ICMP リダイレクト
  - TTL 失敗
  - MTU 失敗
  - IP ユニキャスト オプション
  - IP マルチキャスト オプション
  - 入力および出力 ACL ブリッジド パケット

（注） 入力および出力 ACL ブリッジド パケットのレート制限は、ACL ロギングの障害となることがあり、NAT、レイヤ 3 WCCP、TCP インターセプトなどのハードウェア加速機能のセッション セットアップ レートを増大させることがあります。

AutoSecure に関する注意事項および制約事項

AutoSecure を設定する際に、以下の注意事項と制約事項に従ってください。

- AutoSecure によって行われた設定変更を元に戻すコマンドがないため、AutoSecure の設定を行う前に実行コンフィギュレーションを必ず保存してください。
- AutoSecure 設定は実行時またはセットアップ時に行うことができます。AutoSecure をイネーブルにしたあとで関連する設定が変更されると、AutoSecure 設定が一部有効にならないことがあります。
- AutoSecure がイネーブルになると、装置の監視および設定のために SNMP を使用するツールは、SNMP を使用する装置との通信を行うことができなくなります。
- 使用している装置を NM アプリケーションによって管理している場合は、マネジメント プレーンのセキュリティ保護によって HTTP サーバなどのいくつかのサービスがディセーブルになり、NM アプリケーションのサポートが中断されます。
- SDM を使用している場合は、**ip http server** コマンドを使用して、HTTP サーバを手動でイネーブルにする必要があります。
- CDP を使用してネットワーク トポロジを検出する NM アプリケーションは、検出を行うことができなくなります。

AutoSecure の設定

ここでは、AutoSecure の設定手順について説明します。

- 「AutoSecure コマンドの使用」（P.42-7）
- 「セキュリティの追加設定」（P.42-8）
- 「AutoSecure の確認」（P.42-9）

AutoSecure コマンドの使用

auto secure コマンドを使用すると、マネジメント プレーンおよびフォワーディング プレーンのセキュリティを保護するための半インタラクティブなセッション（別名 AutoSecure セッション）を実行できます。このコマンドは、マネジメント プレーンまたはフォワーディング プレーンのセキュリティを保護するだけです。コマンド ラインでどちらのオプションも選択されていない場合は、セッション中にどちらかのプレーンまたは両方のプレーンを選択して設定できます。

またこのコマンドでは、セッションの非インタラクティブな部分の設定をすべて行ってから、インタラクティブな部分の設定を行います。セッションの非インタラクティブな部分は、任意で **no-interact** キーワードを選択することでイネーブルにできます。

AutoSecure セッションでは、次の情報が必要になります。

- 装置はインターネットに接続する予定かどうか。
- いくつのインターフェイスをインターネットに接続するか。
- インターネットに接続するインターフェイスの名前は何か。
- どのようなローカル ユーザ名およびパスワードを使用するか。
- スイッチのホスト名およびドメイン名は何か。

プロンプトが表示されているときに疑問符（**?**）を入力するとヘルプが表示され、Ctrl+C を押すとセッションが中断されます。

インタラクティブ モードでは、セッション終了時に、生成された設定をスイッチの実行コンフィギュレーションにコミットするかどうか尋ねられます。非インタラクティブ モードでは、変更は実行コンフィギュレーションに自動的に適用されます。

（注）　AutoSecure により行われた設定変更を元に戻すコマンドはありません。**auto secure** コマンドを実行する前に実行コンフィギュレーションを必ず保存する必要があります。

AutoSecure 設定プロセスを実行するには、特権 EXEC モードを開始して、次の作業を行います。

コマンド	目的
`Router# auto secure [management | forwarding] [no-interact | full]`	スイッチのどちらかのプレーンか両方のプレーンを設定するために AutoSecure セッションを実行します。 • **management**：マネジメント プレーンだけ、セキュリティを保護します。 • **forwarding**：フォワーディング プレーンだけ、セキュリティを保護します。 • **no-interact**：インタラクティブな設定について入力を要求しません。 • **full**：すべてのインタラクティブな設定について入力を要求します。これがデフォルトです。

AutoSecure セッションの例については、「AutoSecure 設定例」（P.42-9）を参照してください。

セキュリティの追加設定

AutoSecure 設定が終わってから、次の作業を行うことでスイッチへの管理アクセスのセキュリティをさらに強化できます。

	コマンドまたはアクション	目的
ステップ 1	`Router# configure terminal`	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	`Router(config)# security passwords min-length` *length*	すべての設定されたパスワードが、指定長よりも長いことを確認します。 • *length*：設定されるパスワードの最短長。範囲は 0 ～ 16 文字です。

	コマンドまたはアクション	目的
ステップ 3	`Router(config)# enable password {password | [encryption-type] password}`	さまざまな特権レベルへのアクセスを制御するためにローカル パスワードを設定します。 • *encryption-type*：値が 0 である場合は、暗号化されないパスワードを指定することを示します。値が 7 である場合は、隠しパスワードを指定することを示します。 **（注）** シスコのルータまたはスイッチにより暗号化されているパスワードを入力する場合を除いて、暗号化タイプを入力することは通常ありません。
ステップ 4	`Router(config)# security authentication failure rate threshold-rate log`	ログイン試行の失敗許容回数を設定します。 • *threshold-rate*：ログイン試行の失敗許容回数。範囲は 1 ～ 1024 です。 • **log**：1 分間に失敗回数がしきい値を超える場合の Syslog 認証失敗

次に、スイッチで最短パスワード長を 10 文字に、パスワードの失敗の許容しきい値を 1 分間に 3 回に設定する例を示します。また、非表示ローカル パスワードを設定する例も示します。

```
Router# configure terminal
Router(config)# security passwords min-length 10
Router(config)# security authentication failure rate 3
Router(config)# enable password 7 elephant123
```

AutoSecure の確認

AutoSecure 機能の実行に成功していることを確認するには、次の作業を行います。

コマンド	目的
`Router# show auto secure config`	AutoSecure 設定の一部として追加されているすべてのコンフィギュレーション コマンドを表示します。出力はコンフィギュレーションにより生成される出力と同じです。

AutoSecure 設定例

次に、AutoSecure セッションの例を示します。**auto secure** コマンドを実行すると、AutoSecure は **no-interact** キーワードをイネーブルにしている場合を除いて、これと同様の応答が自動的に表示されます（ディセーブルにする機能とイネーブルにする機能の詳細については、「マネジメント プレーンのセキュリティ保護」（P.42-2）および「フォワーディング プレーンのセキュリティ保護」（P.42-6）を参照してください）。

```
Router# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
```

```
 AutoSecure will modify the configuration of your device.

All the configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
AutoSecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]: y

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: y
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan77                 77.1.1.4        YES NVRAM  down                  down
GigabitEthernet6/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet6/2     21.30.30.1      YES NVRAM  up                    up
Loopback0              3.3.3.3         YES NVRAM  up                    up
Tunnel1                unassigned      YES NVRAM  up                    up
Enter the interface name that is facing the internet: Vlan77

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of <Name of Enterprise>.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k
banner
k
Enter the new enable secret:
Confirm the enable secret :
Enable password is not configured or its length
is less than minimum no. of charactersconfigured
Enter the new enable password:
```

```
Confirm the enable password:

Configuration of local user database
Enter the username: cisco
Enter the password:
Confirm the password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected (in seconds): 5

Maximum Login failures with the device: 3

Maximum time period for crossing the failed login attempts (in seconds): ?
% A decimal number between 1 and 32767.

Maximum time period for crossing the failed login attempts (in seconds): 5

Configure SSH server? [yes]: no

Configuring interface specific AutoSecure services
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected
to internet

The following rate-limiters are enabled by default:
  mls rate-limit unicast ip errors 100 10
  mls rate-limit unicast ip rpf-failure 100 10
  mls rate-limit unicast ip icmp unreachable no-route 100 10
  mls rate-limit unicast ip icmp unreachable acl-drop 100 10
  mls rate-limit multicast ipv4 fib-miss 100000 100
  mls rate-limit multicast ipv4 partial 100000 100

Would you like to enable the following rate-limiters also?
mls rate-limit unicast ip icmp redirect 100 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
mls rate-limit unicast ip options 100 10
mls rate-limit multicast ipv4 ip-options 100 10

Enable the above rate-limiters also? [yes/no]: yes

Would you like to enable the rate-limiters for Ingress/EgressACL bridged packets also?
NOTE: Enabling the ACL in/out rate-limiters can affect ACL logging
      and session setup rate for hardware accelerated features such
      as NAT, Layer 3 WCCP and TCP Intercept
mls rate-limit unicast acl input 100 10
mls rate-limit unicast acl output 100 10

Enable the ACL in/out rate-limiters also? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
```

```
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner k
banner
k
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$30kP$f.KDndYPz/Hv/.yTlJStN/
enable password 7 08204E4D0D48574446
username cisco password 7 08204E4D0D48574446
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line vty 0 15
 login authentication local_auth
 transport input telnet
login block-for 5 attempts 3 within 5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int Vlan1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int Vlan77
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int GigabitEthernet6/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Vlan77
 ip verify unicast source reachable-via rx
```

```
mls rate-limit unicast ip icmp redirect 100 10
mls rate-limit all ttl-failure 100 10
mls rate-limit all mtu-failure 100 10
mls rate-limit unicast ip options 100 10
mls rate-limit multicast ipv4 ip-options 100 10
!
end


Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config

Router#
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント