CHAPTER 27

コンフィギュレーション ファイルの操作

この章では、Catalyst 6500 シリーズ スイッチ上でのスイッチ コンフィギュレーション ファイルの操作方法について説明します。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

（注） フラッシュ デバイス名（**slot0:** など）はスーパバイザ エンジンのタイプによって変わります。詳細については、「フラッシュ ファイル システムの機能」（p.25-2）を参照してください。

この章で説明する内容は、次のとおりです。

スイッチ上でのコンフィギュレーション ファイルの操作

ここでは、スイッチ上でのコンフィギュレーション ファイルの操作方法について説明します。

（注）　フラッシュ ファイル システムでのコンフィギュレーション ファイルの操作については、第 25 章「フラッシュ ファイル システムの使用」を参照してください。

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルを作成することにより、各スイッチの設定が容易になります。コンフィギュレーション ファイルには、1 台または複数のスイッチの設定に必要な一部またはすべてのコマンドを登録することができます。たとえば、同じハードウェア構成の複数のスイッチに同じコンフィギュレーション ファイルをダウンロードすることにより、モジュールおよびポートを同じ設定にすることができます。

ここでは、コンフィギュレーション ファイル作成時の注意事項について説明します。

- コンフィギュレーション ファイルを使用してスイッチを設定する場合、コンソール ポートから接続することを推奨します。Telnet セッションによる接続では、スイッチの設定時に IP アドレスを変更できません。また、ポートおよびモジュールをディセーブルにできません。
- スイッチにパスワードを設定していない場合、**set password** および **set enablepass** コマンドを入力して、各スイッチにパスワードを設定する必要があります。**set password** および **set enablepass** コマンドの後ろに空白行を作成してください。パスワードが空テキストとしてコンフィギュレーション ファイルに保存されます。

  すでにパスワードを設定している場合は、**set password** および **set enablepass** コマンドは入力できません。パスワード検証エラーになるためです。コンフィギュレーション ファイルにパスワードを入力すると、ファイルの実行時に、パスワードが誤ってコマンドとして実行されます。
- コンフィギュレーション ファイルに指定するコマンドによっては、コマンドの後ろに空白行を入力する必要があります。空白行を入力しないと、これらのコマンドによって Telnet セッションが切断される可能性があります。セッションを切断する前に、スイッチから確認を求めるプロンプトが出されます。空白行は、CR（復帰）の役割を果たすので、プロンプトに対する否定応答となり、Telnet セッションを継続することができます。

  コンフィギュレーション ファイルに次のコマンドを指定する場合は、各コマンドを入力するたびに、空白行を挿入してください。
  - **set interface sc0** *ip_addr netmask*
  - **set interface sc0 disable**
  - **set module disable** *mod*
  - **set port disable** *mod/port*

コンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成するときには、システムが正しく応答できるように、論理的な順序でコマンドを指定する必要があります。コンフィギュレーション ファイルを作成するには、次の手順を実行します。

ステップ 1　スイッチから既存の設定をダウンロードします。

ステップ 2　UNIX の vi または emacs、PC のメモ帳などのテキスト エディタで、コンフィギュレーション ファイルを開きます。

ステップ 3　コンフィギュレーション ファイルから必要なコマンドの部分を抜き出し、新しいファイルとして保存します。ファイルの先頭に独立した行として **begin**、ファイルの末尾に **end** を指定する必要があります。

ステップ 4　ワークステーションの適切な Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）ディレクトリ（UNIX ワークステーション上の /tftpboot）に、新しいコンフィギュレーション ファイルをコピーします。

ステップ 5　ファイルに対する許可が world-read に設定されていることを確認します。

次に、コンフィギュレーション ファイルの例を示します。このファイルを使用して、複数のスイッチに Domain Name System（DNS; ドメイン ネーム システム）を設定できます。

```
begin

!
#dns
set ip dns server 172.16.10.70 primary
set ip dns server 172.16.10.140
set ip dns enable
set ip dns domain corp.com
end
```

TFTP によるコンフィギュレーション ファイルのスイッチへのダウンロード

各スイッチは、作成したコンフィギュレーション ファイルを使用して設定することも、別のスイッチからコンフィギュレーション ファイルをダウンロードして設定することもできます。また、フラッシュ ファイル システムをサポートしているハードウェア上のフラッシュ デバイスにコンフィギュレーション ファイルを保存しておき、フラッシュ デバイス上のコンフィギュレーション ファイルを使用してスイッチを設定することもできます。

ここでは、TFTP サーバからダウンロードしたコンフィギュレーション ファイル、またはフラッシュ デバイス上のコンフィギュレーション ファイルを使用して、スイッチを設定する手順について説明します。

- TFTP によるコンフィギュレーション ファイルのダウンロードの準備（p.27-4）
- TFTP サーバ上のファイルを使用したスイッチの設定（p.27-4）
- フラッシュ デバイス上のファイルを使用したスイッチの設定（p.27-5）

TFTP によるコンフィギュレーション ファイルのダウンロードの準備

TFTP を使用してコンフィギュレーション ファイルをダウンロードする前に、次の作業が必要です。

- TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注） /etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。TFTP デーモンの詳しい使用手順については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバに接続できるかどうかを確認してください。
- ダウンロードするコンフィギュレーション ファイルが、TFTP サーバの正しいディレクトリ（UNIX ワークステーションでは /tftpboot）に存在していることを確認します。
- ファイルに対する許可が正しく設定されていることを確認します。ファイルの許可は world-read に設定されていなければなりません。

TFTP サーバ上のファイルを使用したスイッチの設定

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーション上の適切な TFTP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 3　**copy tftp config** コマンドを入力し、TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定します。TFTP サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

コンフィギュレーション ファイルがダウンロードされ、ファイルの各行に指定されているコマンドが、順に実行されます。

次に、TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定する例を示します。

```
Console> (enable) copy tftp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using tftp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

フラッシュ デバイス上のファイルを使用したスイッチの設定

フラッシュ デバイス上のフラッシュ ファイル システムに保存されているコンフィギュレーション ファイルを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2　**cd** および **dir** コマンドを使用して、コンフィギュレーション ファイルを検索します（詳細については、第 25 章「フラッシュ ファイル システムの使用」を参照）。

ステップ 3　**copy** *file-id* **config** コマンドを使用し、フラッシュ デバイスに保存されているコンフィギュレーション ファイルを使用してスイッチを設定します。

ファイルが行単位で読み取られ、指定されているコマンドが実行されます。

次に、フラッシュ デバイスに保存されているコンフィギュレーション ファイルを使用してスイッチを設定する例を示します。

```
Console> (enable) copy slot0:dns-config.cfg config

Configure using slot0:dns-config.cfg (y/n) [n]? y

Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

TFTP サーバへのコンフィギュレーション ファイルのアップロード

ここでは、実行コンフィギュレーションまたはフラッシュ デバイスに保存されているコンフィギュレーション ファイルを、TFTP サーバにアップロードする手順について説明します。

TFTP サーバへのコンフィギュレーション ファイルのアップロードの準備

TFTP サーバにコンフィギュレーション ファイルをアップロードする前に、次の作業が必要です。

- TFTP サーバとして動作するワークステーションが、正しく設定されていることを確認します。Sun ワークステーション上で、/etc/inetd.conf ファイルに次の行が含まれていることを確認します。

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  /etc/services ファイルに次の行が含まれていることを確認します。

  ```
  tftp 69/udp
  ```

  （注） /etc/inetd.conf ファイルおよび /etc/services ファイルを変更したあとで、inetd デーモンを再起動する必要があります。デーモンを再起動するには、inetd プロセスをいったん中止してから再起動するか、**fastboot** コマンド（SunOS 4.x）または **reboot** コマンド（Solaris 2.x または SunOS 5.x）を入力します。TFTP デーモンの詳しい使用手順については、使用しているワークステーションのマニュアルを参照してください。

- スイッチに TFTP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチと TFTP サーバは同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、TFTP サーバに接続できるかどうかを確認してください。
- 必要に応じて、コンフィギュレーション ファイルをアップロードする前に、TFTP サーバ上に空のファイルを作成します。空のファイルを作成するには、**touch** *filename* コマンドを入力します。*filename* は、サーバにコンフィギュレーション ファイルをアップロードするときに使用するファイル名です。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。ファイルの許可は world-write に設定されていなければなりません。

TFTP サーバへのコンフィギュレーション ファイルのアップロード

スイッチから TFTP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。

ステップ 2　**copy config tftp** コマンドを使用して、TFTP にスイッチ コンフィギュレーションをアップロードします。TFTP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

TFTP サーバにファイルがアップロードされます。

次に、TFTP サーバに実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy config tftp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to tftp:cat6000_config.cfg, (y/n) [n]? y
.....
..........
.......

..........
...........
..
/
Configuration has been copied successfully.
Console> (enable)
```

SCP または RCP を使用したコンフィギュレーションファイルのコピー

ここでは、SCP または RCP を使用してファイルをコピーする方法について説明します。

- RCP の概要（p.27-7）
- SCP の概要（p.27-7）

RCP の概要

Remote Copy Protocol（RCP）を使用して、リモート ホストとスイッチ間でコンフィギュレーションのダウンロード、アップロード、およびコピーを行うこともできます。UDP を使用する TFTP と異なり、コネクションレス プロトコルである RCP は、コネクション型の TCP を使用します。

RCP を使用してファイルをコピーするには、ファイルのコピー先またはコピー元となるサーバが RCP をサポートしていなければなりません。RCP の **copy** コマンドは、リモート システムの Remote Shell（RSH）サーバ（またはデーモン）に依存します。RCP を使用してファイルをコピーする場合、TFTP と異なり、ファイル配布用のサーバを作成する必要はありません。RSH をサポートするサーバにアクセスするだけです（大部分の UNIX システムは RSH をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在していない場合は、RCP がユーザに代わってファイルを作成します。

SCP の概要

Secure Copy（SCP; セキュア コピー）は、暗号化イメージ ファイルのコピーを安全に行います。SCP は Secure Shell（SSH; セキュア シェル）に依存していて、暗号化チャネルを使用してシステムで暗号化ファイルをコピーできます。

RCP または SCP サーバからのコンフィギュレーション ファイルのダウンロード

ここでは、RCP または SCP サーバから実行コンフィギュレーションまたはフラッシュ デバイスに、コンフィギュレーション ファイルをダウンロードする方法について説明します。

- RCP または SCP によるコンフィギュレーション ファイルのダウンロードの準備（p.27-8）
- RCP または SCP サーバ上のファイルを使用したスイッチの設定（p.27-8）

RCP または SCP によるコンフィギュレーション ファイルのダウンロードの準備

RCP または SCP を使用してコンフィギュレーション ファイルをダウンロードする前に、次の作業が必要です。

- RCP サーバとして動作するワークステーションが、RSH をサポートしていることを確認します。
- SCP サーバとして動作するワークステーションが、SSH をサポートしていることを確認します。
- スイッチに RCP または SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、スイッチとサーバが同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、RCP サーバに接続できるかどうかを確認してください。
- 有効なユーザ名を使用しないでコンソールまたは Telnet セッション経由でスイッチにアクセスしている場合、現在の RCP ユーザ名が RCP ダウンロードに使用する名前であることを確認してください。**show users** コマンドを入力すると、現在の有効なユーザ名を調べることができます。現在のユーザ名を使用しない場合は、**set rcp username** コマンドで新しいユーザ名を作成します。新しいユーザ名は NVRAM（不揮発性 RAM）に保存されます。有効なユーザ名を使用して Telnet セッション経由でスイッチにアクセスしている場合、このユーザ名が使用されるので、RCP ユーザ名を設定する必要はありません。

RCP または SCP サーバ上のファイルを使用したスイッチの設定

RCP または SCP サーバからダウンロードしたコンフィギュレーション ファイルを使用して、Catalyst 6500 シリーズ スイッチを設定するには、次の手順を実行します。

ステップ 1　コンフィギュレーション ファイルをワークステーション上の適切な RCP ディレクトリにコピーします。

ステップ 2　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。SCP を使用している場合、SSH セッションを使用してログインします。

ステップ 3　**copy rcp | scp config** コマンドを入力し、サーバからダウンロードしたコンフィギュレーション ファイルを使用してスイッチを設定します。サーバの IP アドレスまたはホスト名、およびダウンロードするファイル名を指定します。

コンフィギュレーション ファイルがダウンロードされ、ファイルの各行に指定されているコマンドが、順に実行されます。

次に、サーバからダウンロードしたコンフィギュレーション ファイルを使用して、Catalyst 6500 シリーズ スイッチを設定する例を示します。

```
Console> (enable) copy rcp config
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? dns-config.cfg

Configure using rcp:dns-config.cfg (y/n) [n]? y
/
Finished network download.  (134 bytes)
>>
>> set ip dns server 172.16.10.70 primary
172.16.10.70 added to DNS server table as primary server.
>> set ip dns server 172.16.10.140
172.16.10.140 added to DNS server table as backup server.
>> set ip dns enable
DNS is enabled
>> set ip dns domain corp.com
Default DNS domain name set to corp.com
Console> (enable)
```

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロード

ここでは、実行コンフィギュレーションまたはフラッシュ デバイスに保存されているコンフィギュレーション ファイルを、RCP または SCP サーバにアップロードする手順について説明します。

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロードの準備

RCP または SCP サーバにコンフィギュレーション ファイルをアップロードする前に、次の作業が必要です。

- RCP または SCP サーバとして動作するワークステーションが、正しく設定されていることを確認します。
- スイッチに RCP または SCP サーバへのルートが設定されていることを確認します。サブネット間でトラフィックをルーティングするルータを設定していない場合、システムとサーバが同じサブネットに置かれていなければなりません。**ping** コマンドを使用して、サーバに接続できるかどうかを確認してください。
- 既存ファイル（作成済みの空のファイルを含む）を上書きする場合は、ファイル許可が正しく設定されていることを確認します。ファイルの許可は user-write に設定されていなければなりません。

RCP または SCP サーバへのコンフィギュレーション ファイルのアップロード

スイッチから RCP または SCP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順を実行します。

ステップ 1　コンソール ポートまたは Telnet セッションを使用して、スイッチにログインします。SCP を使用している場合、SSH セッションを使用してスイッチにログインします。

ステップ 2　**copy config rcp | scp** コマンドを入力して、RCP サーバにスイッチの設定をアップロードします。RCP サーバの IP アドレスまたはホスト名、および宛先ファイル名を指定します。

サーバにファイルがアップロードされます。

次に、RCP サーバに Catalyst 6500 シリーズ スイッチの実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy config rcp
IP address or name of remote host []? 172.20.52.3
Name of file to copy to []? cat6000_config.cfg

Upload configuration to rcp:cat6000_config.cfg, (y/n) [n]? y
.....
.........
.......

.........
...........
..
/
Configuration has been copied successfully.
Console> (enable)
```

次に、SCP サーバに Catalyst 6500 シリーズ スイッチの実行コンフィギュレーションをアップロードして保存する例を示します。

```
Console> (enable) copy scp flash scp
IP address or name of remote host []? 172.20.52.3
Name of file to copy from []? cat6000-sup720cvk9.8-3-1.bin
Username for scp[bob]?
Password for User bob[]:
CCC/
File has been copied successfully.
```

設定の消去

スイッチ全体の設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
スイッチの設定を消去します。	**clear config all**

次に、スイッチ全体の設定を消去する例を示します。

```
Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
........
.............................

System configuration cleared.
Console> (enable)
```

個々のモジュールの設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
個々のモジュールの設定を消去します。	**clear config** *mod*

（注） モジュールを取り外して、異なるタイプのモジュールに交換すると（10/100 イーサネット モジュールからギガビット イーサネット モジュールに交換する場合など）、モジュールの設定の不一致が生じます。**show module** コマンドを実行すると、出力結果から問題がわかります。この不一致を解消するには、モジュール上の設定を消去する必要があります。

次に、個々のモジュールの設定を消去する例を示します。

```
Console> (enable) clear config 2
This command will clear module 2 configuration.
Do you want to continue (y/n) [n]? y
.............................
Module 2 configuration cleared.
Console> (enable)
```

個々のモジュール ポートの設定を消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
個々のモジュール ポートの設定を消去します。	**clear config** {*mod* | *mod/port*}

コンフィギュレーション ファイルの比較

コンフィギュレーション ファイル間の違いを判断したり、システム コンフィギュレーションが変更されたかどうかをチェックするために、システムに保存されているコンフィギュレーション ファイルを比較できます。コンフィギュレーション ファイルを比較するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション ファイル間の違いを比較します。	**show config differences** {**all** *file* | **context** *val* | *file* | **ignorecase**}

次に、2 つの異なるコンフィギュレーション ファイルの違いを比較する例を示します。

```
Console> (enable) show config differences 1.cfg 2.cfg
--- bootflash:1.cfg
+++ bootflash:2.cfg
@@ -8,1 +8,1 @@
-#version 8.2(0.11-Eng)DEL
+#VERSION 8.2(0.11-eNG)del
@@ -11,1 +11,1 @@
-set config mode text auto-save interval 1
+SET CONFIG MODE TEXT AUTO-SAVE INTERVAL 1
Console> (enable)
```

次に、大文字と小文字の違いは無視してコンフィギュレーション ファイルの違いを比較する例を示します。

```
Console> (enable) show config differences ignorecase 1.cfg 2.cfg
Files bootflash:1.cfg and bootflash:2.cfg are identical
Console> (enable)
```

コンフィギュレーション ロールバック用のコンフィギュレーション チェックポイント ファイルの作成

現在のファイルによって望ましくない結果がシステムで生じる場合、現在のスイッチ コンフィギュレーション ファイルを前に保存したコンフィギュレーション ファイル（別名「チェックポイント」ファイル）にロール バックできます。このロールバック機能によって、1 つのコマンドに複数のコンフィギュレーション「チェックポイント」ファイルを設定できます。現在のコンフィギュレーション ファイルをスイッチ上で実行したくない場合、速やかにコンフィギュレーション チェックポイント ファイルのいずれかに戻し、スイッチ機能への障害をできるだけ少なくすることができます。

コンフィギュレーション チェックポイント ファイルの作成時には、次の注意事項に従ってください。

- コンフィギュレーション チェックポイント ファイルは、ファイルの作成時に指定する名前によって特定されます。コンフィギュレーション チェックポイント ファイル名は、15 文字以内にする必要があります。名前を指定しない場合、システムによって名前が生成されます。システムによって生成される名前は、CKPi_MMDDYYHHMM の形式になります。「i」はチェックポイント番号を表します。
- チェックポイント ファイルは、ブートフラッシュまたは slotX/diskX に保存されます。装置を指定しない場合、ファイルは現在のデフォルト装置に保存されます。
- コンフィギュレーション チェックポイント ファイルは、読み取りおよび編集が可能なテキスト ファイルに保存されます。ファイルを編集しないことを強く推奨します。

- チェックポイント ファイル名がシステムから消去されると、関連するコンフィギュレーション チェックポイント ファイルが削除されます。スペースを確保するために装置をスクイーズする必要があります。
- システム上に最大 5 つのコンフィギュレーション チェックポイント ファイルを作成できます。保存されたすべてのコンフィギュレーション チェックポイント ファイルに任意の順序でロール バックできます。これらのファイルは完全なコンフィギュレーションを使用して生成されるので、相互に独立しています。
- チェックポイント コンフィギュレーションは NVRAM に保存されます。**clear config all** コマンドを入力した場合、コンフィギュレーションは消去されません。
- この機能は、冗長スーパバイザ エンジンを搭載したシステムでサポートされています。チェックポイント コンフィギュレーション ファイルおよび関連するファイルはスタンバイ スーパバイザ エンジンに同期化されます。

コンフィギュレーション チェックポイント ファイルを作成するには、イネーブル モードで次の作業を行います。

作業	コマンド
コンフィギュレーション チェックポイント ファイルを作成します。	**set config checkpoint** [**name** *name*] [**device** *device*]
コンフィギュレーション チェックポイント ファイル名を確認します。	**show config checkpoints**

次に、コンフィギュレーション チェックポイント ファイルを作成し、作成されたことを確認する例を示します。

```
Console> (enable) set config checkpoint
Configuration checkpoint CKP0_0722040905 creation successful.
Console> (enable) show config checkpoints
Checkpoint          File id                                  Date
==========          =======                                  ====
CKP0_0722040905     bootflash:CKP0_07220409058.4(0.79)COC    Thu Jul 22 2000, 09:05:31
Console> (enable)
```

現在のコンフィギュレーション ファイルを前に作成されたコンフィギュレーション チェックポイント ファイルにロール バックするには、イネーブル モードで次の作業を行います。

作業	コマンド
現在のコンフィギュレーション ファイルをコンフィギュレーション チェックポイント ファイルにロール バックします。	**set config rollback** *name*

すべてのコンフィギュレーション チェックポイント ファイルまたは特定のコンフィギュレーション チェックポイント ファイルを消去するには、イネーブル モードで次の作業を行います。

作業	コマンド
すべてのコンフィギュレーション チェックポイント ファイルまたは特定のコンフィギュレーション チェックポイント ファイルを消去します。	**clear config checkpoint** {**all** | *name*}
コンフィギュレーション チェックポイント ファイル名を確認します。	**show config checkpoints**

次に、すべてのコンフィギュレーション チェックポイント ファイルを消去し、消去されたことを確認する例を示します。

```
Console> (enable) clear config checkpoint all
All configuration checkpoints cleared.
Console> (enable) show config checkpoints
No Checkpoints defined.
Console> (enable)
```

MSFC 上でのコンフィギュレーション ファイルの操作

ここでは、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）上のコンフィギュレーション ファイルの操作について説明します。

MSFC の稼働時は、設定情報は 2 つの場所にあります。NVRAM 内のデフォルト（永続的）設定と RAM 内の実行（一時的）メモリです。NVRAM の情報は電源を切断しても保持されるので、デフォルト設定は常時、使用できます。現在の実行メモリは、システムの電源を切断すると失われます。現在の設定には、**configure** または **setup** コマンドを入力することにより、またはコンフィギュレーション ファイルを編集することにより追加された、デフォルト以外のすべての設定情報が含まれています。

電源を切断しても現在の設定が失われないようにするには、**copy running-config startup-config** コマンドを使用して現在の設定を NVRAM のデフォルト設定に追加します。システムの設定を変更する場合は、必ず **copy running-config startup-config** コマンドを実行し、新しい設定を保存してください。

MSFC を交換する場合には、設定全体を交換する必要があります。MSFC を取り外す前にコンフィギュレーション ファイルをリモート サーバにアップロード（コピー）しておけば、新しい MSFC を取り付けたあと、元の設定を NVRAM に戻すことができます。コンフィギュレーション ファイルをアップロードしない場合には、新しい MSFC を取り付けたあと、**configure** コマンドを入力して設定情報を再入力する必要があります。

MSFC を一時的に取り外して再び取り付ける場合には、コンフィギュレーション ファイルを保存して戻す必要はありません。リチウム電池により、設定情報がメモリに保存されています。この作業では、EXEC コマンド インタープリタのイネーブル レベルにアクセスする必要があり、通常、パスワードが必要になります。

TFTP サーバへのコンフィギュレーション ファイルのアップロード

TFTP ファイル サーバに実行コンフィギュレーションをアップロードする前に、次のことを確認してください。

- コンソール端末から、または Telnet セッションによりリモートで MSFC に接続できること。
- MSFC がファイル サーバ（リモート ホスト）をサポートしているネットワークに接続していること。
- リモート ホストが TFTP アプリケーションをサポートしていること。
- 使用できるリモート ホストの IP アドレスまたはホスト名がわかっていること。

リモート ホストに情報を保存するには、**write network** イネーブル EXEC コマンドを使用します。このコマンドに、宛先ホストのアドレスおよびファイル名を入力し、指示した情報を確認します。情報を確認すると、MSFC により、現在の実行コンフィギュレーションがリモート ホストに送信されます。システムのデフォルトでは、設定は MSFC の名前に *-confg* が付加されたファイル名で保存されます。**Return** キーを押してデフォルト ファイル名を使用するか、別のファイル名を入力して **Return** キーを押します。

現在の実行コンフィギュレーションをリモート ホストにアップロードするには、次の手順を実行します。

ステップ 1　システム プロンプトに、EXEC コマンド インタープリタのイネーブル レベルを示すポンド記号（#）が表示されていることを確認します。

ステップ 2　**ping** コマンドを入力して、MSFC とリモート ホストとの接続を確認します。

ステップ 3　**write term** コマンドを入力して、現在の実行コンフィギュレーションを端末に表示し、設定情報が完全で正しいことを確認します。情報が正しくない場合には、**configure** コマンドを使用して既存の設定に追加または変更を行います。

ステップ 4　**write net** コマンドを入力します。EXEC コマンド インタープリタによって、コンフィギュレーション ファイルを受信するリモート ホストの名前または IP アドレスの入力を求めるプロンプトが表示されます（プロンプトにデフォルトのファイル サーバの名前またはアドレスが示されていることもあります）。

```
Router# write net
Remote host []?
```

ステップ 5　リモート ホストの名前または IP アドレスを入力します。次の例では、リモート サーバ名 *servername* を入力しています。

```
Router# write net
Remote host []? servername
Translating "servername"...domain server (1.1.1.1) [OK]
```

ステップ 6　設定を保存するファイル名を指定するように要求されます。デフォルトでは、MSFC 名に *-confg* を付加した新しいファイル名が作成されます。**Return** キーを押してデフォルト ファイル名を使用するか、別のファイル名を入力して **Return** を押します。次の例ではデフォルトがそのまま使用されています。

```
Name of configuration file to write [Router-confg]?
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg .....
```

ステップ 7　MSFC によりコピー処理が開始される前に、指定した情報が表示されるので確認します。指定した内容が正しくない場合には、**n**（no）を入力し、**Return** キーを押して処理を中止します。指定した内容を確定するには、**Return** キーを押すか、**y**（yes）を入力して **Return** キーを押します。コピー処理が開始されます。次の例ではデフォルトがそのまま使用されています。

```
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg: !!!! [ok]
```

MSFC がリモート ホストに設定をコピーしている間、一連の感嘆符（!!!）またはピリオド（...）を表示します。!!! および [ok] は、処理が成功したことを示しています。失敗すると、ピリオドの連続（...）と [timed out] または [failed] が表示されます。この場合、ネットワークに障害があるか、リモート ファイル サーバ上に読み書き可能なファイルが存在しない可能性があります。

ステップ 8　処理が成功していれば（!!! および [ok] が表示されている状態）、アップロードは完了です。設定は、リモート ファイル サーバ上の一時ファイルに保存されます。

処理が失敗すると、次の例のようにピリオドの連続（...）が表示されます。

```
Writing Router-confg .....
```

この場合、設定は保存されていません。上記の手順を再度実行するか、別のリモート ファイル サーバを選択して同じ手順を繰り返してください。

リモート ホストに設定を正常にコピーできない場合には、ネットワーク管理者に連絡してください。

スーパバイザ エンジンのフラッシュ PC カードへのコンフィギュレーション ファイルのアップロード

スーパバイザ エンジンのフラッシュ PC カードにコンフィギュレーション ファイルをアップロードするには、次の作業を行います。

	作業	コマンド
ステップ 1	EXEC プロンプトで、イネーブル モードを開始します。	Router> **enable**
ステップ 2	スタートアップ コンフィギュレーション ファイルをスロット 0 にコピーします。	Router# **copy startup-config sup-slot0:***file_name*
ステップ 3	実行コンフィギュレーション ファイルをスロット 0 にコピーします。	Router# **copy running-config sup-slot0:***file_name*

リモート ホストからのコンフィギュレーション ファイルのダウンロード

新しい MSFC を搭載したあと、保存した設定を検索して、NVRAM にコピーすることができます。コンフィギュレーション モードを開始し、ネットワーク経由で MSFC の設定を行います。システム プロンプトにホスト名、アドレス、およびホストに保存されているコンフィギュレーション ファイル名を入力し、リモート ファイルを使用した再起動を指示します。

リモート ホストから現在の実行コンフィギュレーションをダウンロードするには、次の手順を実行します。

ステップ 1　システム プロンプトに、EXEC コマンド インタープリタのイネーブル レベルを示すポンド記号 (#) が表示されていることを確認します。

（注）　元の設定を検索して戻すまで、MSFC は NVRAM 上のデフォルト設定を実行します。設定を戻すまでは、システムに設定していたパスワードは無効になります。

ステップ 2　**ping** コマンドを入力して、ルータとリモート ホストとの接続を確認します。

ステップ 3　システム プロンプトに **configure network** コマンドを入力し、**Return** キーを押してコンフィギュレーション モードを開始します。(デフォルトのコンソール端末を使用するのではなく)ネットワーク装置からシステムの設定を行うことを指定します。

```
Router# configure network
```

ステップ 4　ホストまたはネットワーク上のコンフィギュレーション ファイルを選択するように要求されます。デフォルトはホスト上のファイルです。デフォルトを確定するには、**Return** キーを押します。

```
Host or network configuration file [host]?
```

ステップ 5　ホストの IP アドレスを入力するように要求されます。リモート ホスト（コンフィギュレーション ファイルをアップロードしたリモート ファイル サーバ）の IP アドレスまたは名前を入力します。

```
IP address of remote host [255.255.255.255]? 1.1.1.1
```

ステップ 6　コンフィギュレーション ファイル名を入力します。ファイルのアップロード時のデフォルト名は、MSFC 名に *-confg* を付けたファイル名（次の例では *router-confg*）です。設定のアップロード時にデフォルト以外のファイル名を指定した場合は、そのファイル名を入力します。デフォルト名を使用した場合には、**Return** キーを押します。

```
Name of configuration file [router-confg]?
```

ステップ 7　新しい設定でシステムを再起動する前に、指定した情報が表示されるので確認します。指定した内容が正しくない場合には、**n**（no）を入力し、**Return** キーを押して処理を中止します。指定した内容を確定するには、**Return** キーを押すか、**y** を入力して **Return** キーを押します。

```
Configure using router-confg from 1.1.1.1? [confirm]
Booting router-confg from 1.1.1.1: ! ! [OK - 874/16000 bytes]
```

MSFC がリモート ホスト上の設定の検索およびシステム再起動を開始すると、コンソールに処理が成功したかどうかが示されます。一連の !!! および [ok]（前述の例を参照）は、処理が成功したことを示します。ピリオドの連続（ . . .）と [timed out] または [failed] は、処理が失敗したことを示します（ネットワークに障害があるか、指定したサーバ名、アドレス、またはファイル名が間違っている可能性があります)。次に、リモート サーバからのシステム再起動に失敗した例を示します。

```
Booting Router-confg ..... [timed out]
```

ステップ 8　処理に成功した場合は、次の手順に進みます。

処理に失敗した場合は、リモート サーバの名前またはアドレスおよびファイル名が正しいかどうか確認し、前の手順を繰り返してください。設定を正常に検索できない場合には、ネットワーク管理者に連絡してください。

ステップ 9　**write term** コマンドを入力して、現在の実行コンフィギュレーションを端末に表示します。表示されたコンフィギュレーション情報が完全で、正しいことを確認します。正しくない場合は、ファイル名を確認してから前の手順を繰り返して正しいファイルを検索するか、**configure** コマンドを入力して既存の設定に追加または変更を行います（システム、各インターフェイス、特定の設定手順で利用できる設定オプションについては、該当するソフトウェアのマニュアルを参照してください）。

ステップ 10　現在の実行コンフィギュレーションが正しいことを確認したら、**copy running-config startup-config** コマンドを入力して、検索した設定を NVRAM に保存します。保存しないと、システムを再起動した場合に、検索した設定は失われます。

スーパバイザ エンジンのフラッシュ PC カードからのコンフィギュレーション ファイルのダウンロード

スーパバイザ エンジンのフラッシュ PC カードからコンフィギュレーション ファイルをダウンロードするには、次の作業を行います。

	作業	コマンド
ステップ 1	EXEC プロンプトで、イネーブル モードを開始します。	Router> **enable**
ステップ 2	保存されている実行コンフィギュレーション ファイルを、MSFC 実行コンフィギュレーションにコピーします。	Router# **copy sup-slot0:***file_name* **running-config**
ステップ 3	保存されているスタートアップ コンフィギュレーション ファイルを、MSFC 実行コンフィギュレーションにコピーします。	Router# **copy sup-slot0:***file_name* **startup-config**

プロファイル ファイルの操作

プロファイル ファイルによって、スイッチのデフォルト コンフィギュレーションとしてカスタマイズされたコンフィギュレーションを持つことができます。また、起動時または新規のモジュールが搭載された場合に、特定の機能をイネーブルまたはディセーブルにするカスタム デフォルト コンフィギュレーションをロードすることができます。プロファイル ファイルを使用すれば、スイッチにセキュリティ リスク（たとえば、CDP のディセーブル化またはポート上の自動トランキングの切断）をもたらす可能性がある機能または処理を排除できます。

セキュリティ リスクのほとんどを無効にしたプロファイル ファイルは、「ロックダウン」プロファイルともいいます。ロックダウン プロファイルは、デフォルトでスイッチの機能をアクセスのイネーブルからアクセスの阻止に変更します。ロックダウン プロファイルが適用されている場合、プロファイル ファイルによってディセーブルにされた機能を手動でイネーブルにする必要があります。

プロファイル ファイルの作成

プロファイル ファイル形式は、コンフィギュレーション ファイル形式と類似しています。新規のプロファイル ファイルを作成することもできますし、システムによって生成されたコンフィギュレーション ファイルを編集することもできます。

注意　要素を失ったり、置き違えるとコンフィギュレーションが失敗する原因になるので、コンフィギュレーション ファイルに不慣れな場合は新規のプロファイル ファイルを作成しないことを推奨します。

システムによって生成されたコンフィギュレーション ファイルを編集してプロファイル ファイルを作成する場合、必須の表記のほとんどがすでにファイルに存在します。現在サポートされているキーワードは、ALL_MODULES、ALL_PORTS、ALL_MODULE_PORTS、および ALL_VLANS です。**copy config all** コマンドを入力した結果生じた出力をテンプレートとして使用してプロファイル ファイルを作成しないでください。出力には、ファイルのサイズと処理時間を増やすデフォルトのコンフィギュレーション情報が含まれているからです。

使用するシステム プロファイル ファイルを指定するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	装置および使用するプロファイル ファイル名を指定します。	**set system profile** *device*:*filename*
ステップ 2	指定したモジュールのシステム プロファイル ファイルをイネーブルまたはディセーブルにします。	**set system profile** {**enable** | **disable**} *mod_list*

次に、装置名およびプロファイル ファイル名を指定する例を示します。

```
Console> (enable) set system profile bootflash:test.cfg
System is set to be configured with profile file bootflash:test.cfg.
Console> (enable)
```

次に、指定されたモジュールのシステム プロファイルのロードをディセーブルにする例を示します。

```
Console> (enable) set system profile disable 2
System profile loading is disabled for module 2.
Console> (enable)
```

次に、ロックダウン プロファイル ファイルの例を示します。一般的であると考えられるロックダウン プロファイル ファイルをデフォルト コンフィギュレーションとして使用する場合、このファイルのコピーをそのまま使用できます。このロックダウン プロファイル ファイルのパラメータがニーズに合わない場合は、ファイルを変更し、ファイルを変更したものを使用することもできます。

```
begin
!
# ***** DEFAULT PROFILE *****
!
!
###################################
# Lockdown Profile version 1.0.3 #
###################################
!
# set system prompt (edit as needed)
set prompt locked_down>
!
# system attributes to be customized (edit as needed)
set system name locked_down
set system contact locked_down
set system location locked_down
!
# set a strong banner (edit as needed)
set banner motd ^
Access to this device or the attached networks is prohibited
without express permission from the network administrator.

Violators will be prosecuted to the fullest extent of both civil
and criminal law.

^
!
!
#
# vtp mode off, enable password and dummy domain (edit as needed)
set vtp domain locked_down
set vtp mode off
set vtp passwd locked_down
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 name Quarantine
!
# Management VLAN is "Management" (edit as needed)
set vlan 1000 name Management
# Alternate management vlan is "OtherMgmt" (edit as needed)
set vlan 1001 name OtherMgmt
!
# sc0 and sc1 off (edit as needed)
set interface sc0 down
set interface sc0 1000
set interface sc1 down
set interface sc1 1001
!
# default port status is disabled
set port disable ALL_PORTS
!
# default cdp status is disabled
set cdp disable ALL_PORTS
!
# default STP status is with BPDU guard enabled
set spantree portfast bpdu-guard ALL_PORTS enable
!
# default PAgP/LACP status is disabled
set port channel ALL_PORTS mode off
!
# Default DTP status is disabled, no allowed vlans and dot1q-all-tagged mode on.
# Warning: A max of 128 trunks can have non-default configuration in CatOS 8.4
# Warning: Edit port list as needed.
```

```
set trunk ALL_PORTS off none
set dot1q-all-tagged enable
!
# default is CPU rate limiters enabled
set rate-limit l2pdu enable
!
# default SSH version is 2
set ssh mode v2
!
# default VLAN is "Quarantine" (edit as needed)
set vlan 999 ALL_PORTS
!
# Enable image checksum verification by default
set image-verification enable
!
# Set a more aggressive default logout timeout
set logout 10
#
#
# Anti-spoofing ACL
#
!
! Deny any packets from the RFC 1918, IANA reserved, ranges,
! multicast as a source, and loopback netblocks to block
! attacks from commonly spoofed IP addresses.
!
! Bogons
!
set security acl ip Anti-spoofing deny ip 0.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 1.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 2.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 5.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 7.0.0.0 0.255.255.255  any log
set security acl ip Anti-spoofing deny ip 10.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 23.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 27.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 31.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 36.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 37.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 39.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 41.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 42.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 49.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 50.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 73.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 74.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 75.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 76.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 77.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 78.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 79.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 89.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 90.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 91.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 92.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 93.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 94.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 95.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 96.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 97.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 98.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 99.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 100.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 101.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 102.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 103.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 104.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 105.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 106.0.0.0 0.255.255.255 any log
```

```
set security acl ip Anti-spoofing deny ip 107.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 108.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 109.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 110.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 111.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 112.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 113.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 114.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 115.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 116.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 117.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 118.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 119.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 120.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 121.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 122.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 123.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 124.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 125.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 126.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 127.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 169.254.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 172.16.0.0 0.15.255.255 any log
set security acl ip Anti-spoofing deny ip 173.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 174.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 175.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 176.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 177.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 178.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 179.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 180.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 181.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 182.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 183.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 184.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 185.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 186.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 187.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 189.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 190.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 192.0.2.0 0.0.0.255     any log
set security acl ip Anti-spoofing deny ip 192.168.0.0 0.0.255.255 any log
set security acl ip Anti-spoofing deny ip 197.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 223.0.0.0 0.255.255.255 any log
set security acl ip Anti-spoofing deny ip 224.0.0.0 31.255.255.255 any log
# Add here a specific list of permits as needed
set security acl ip Anti-spoofing deny any any log
!
# Set protection to VLAN list (edit as needed)
# You can use ALL_VLANS but that will
# take some time to finish.
# Use the "show security acl" cmd to verify when
# the ACL mapping process is completed.
commit security acl all
set security acl map Anti-spoofing ALL_VLANS
!
!
end
```