CHAPTER 3

スイッチの初期設定

この章では、Catalyst 4500 シリーズ スイッチを初期設定する方法について説明します。

この章の情報は、次の URL の『*Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2SR』の管理情報と管理手順を補足するものです。

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frfabout.html

この章の主な内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

デフォルト スイッチ設定

ここでは、Catalyst 4500 シリーズ スイッチのデフォルト設定について説明します。表 3-1 に各機能のデフォルト設定を示します。

表 3-1　デフォルト スイッチ設定

機能	デフォルト設定
管理用接続	ユーザ モード
グローバル スイッチ情報	システム名、システムの連絡先、ロケーションにはデフォルト値が設定されていません。
システム クロック	システム クロック タイムには値が設定されていません。

表 3-1　デフォルト スイッチ設定 （続き）

機能	デフォルト設定
パスワード	ユーザ モードまたはイネーブル モードのパスワードは設定されていません（Return キーを押してください）。
スイッチ プロンプト	Switch>
インターフェイス	イネーブル。速度とフロー制御は自動ネゴシエーションで、Internet Protocol（IP; インターネット プロトコル）アドレスは指定されていません。

DHCP ベースの自動設定の設定

ここでは、DHCP ベースの自動設定を設定する手順について説明します。

DHCP サーバがシスコ デバイスの場合、またはスイッチを DHCP サーバとして設定している場合、DHCP の設定の詳細については、『*Cisco IOS IP and IP Routing Configuration Guide Cisco IOS Release 12.1*』の「*IP Addressing and Services*」を参照してください。

DHCP ベースの自動設定の概要

（注）　リリース 12.2(20)EW 以降では、**write erase** コマンドを入力することにより、DHCP の自動設定をイネーブルにできます。このコマンドにより、Non-Volatile Random Access Memory（NVRAM; 不揮発性 RAM）のスタートアップ コンフィギュレーションがクリアされます。Release 12.2(20)EW よりも前のイメージでは、このコマンドは自動設定をイネーブルにしません。

DHCP は、インターネットホストおよびインターネットワーキング デバイスに設定情報を提供します。このプロトコルには、2 つのコンポーネントが含まれます。1 つは DHCP サーバからデバイスにコンフィギュレーション パラメータを提供するコンポーネント、もう 1 つはデバイスにネットワーク アドレスを割り当てるコンポーネントです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバが、動的に設定されるデバイスに対して、ネットワーク アドレスを割り当て、コンフィギュレーション パラメータを提供します。スイッチは、DHCP クライアントおよび DHCP サーバとして機能できます。

DHCP ベースの自動設定により、スイッチ（DHCP クライアント）が起動時に IP アドレス情報およびコンフィギュレーション ファイルを使用して自動的に設定されるため、スイッチ上での DHCP クライアント側の設定は必要ありません。ただし、IP アドレスに関連付けられた各種のリース オプションに

対しては、DHCP サーバ、またはスイッチ上の DHCP サーバの機能を設定する必要があります。DHCP を使用してネットワーク上でコンフィギュレーション ファイルをリレーする場合は、TFTP サーバおよびドメイン ネーム システム（DNS）サーバの設定が必要なこともあります。

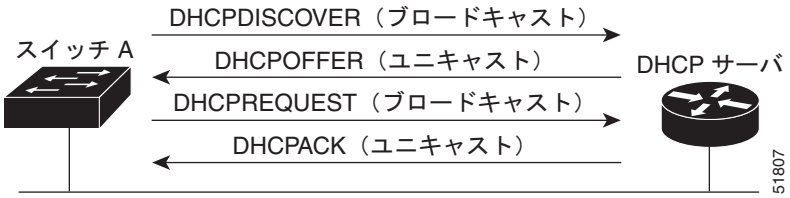
DHCP ベースの自動設定は、スイッチの BOOTP クライアント機能に代わるものです。

DHCP クライアント要求プロセス

起動時にスイッチ上にコンフィギュレーション ファイルがない場合は、スイッチは DHCP サーバに対して自動的に設定情報を要求します。

図 3-1 に、DHCP クライアントと DHCP サーバ間で交換される一連のメッセージを示します。

図 3-1　DHCP クライアント/サーバ間のメッセージ交換



クライアントであるスイッチ A は、DHCP サーバの場所を特定するために、DHCPDISCOVER メッセージをブロードキャストします。DHCP サーバは、コンフィギュレーション パラメータ（IP アドレス、サブネット マスク、ゲートウェイ IP アドレス、DNS IP アドレス、IP アドレス用のリースなど）を、DHCPOFFER ユニキャスト メッセージでクライアントに提示します。

DHCPREQUEST ブロードキャスト メッセージでは、クライアントは、提示された設定情報に対して、DHCP サーバに正式な要求を戻します。この正式な要求はブロードキャストされるため、クライアントから DHCPDISCOVER ブロードキャスト メッセージを受信した他のすべての DHCP サーバは、クライアントに提示した IP アドレスを再利用できます。

DHCP サーバは、DHCPACK ユニキャスト メッセージをクライアントに戻すことで、IP アドレスがクライアントに割り当てられたことを確認します。このメッセージによって、クライアントとサーバはバインドされ、クライアントはサーバから受信した設定情報を使用します。スイッチの受信する情報量は、DHCP サーバの設定方法によって異なります。詳細については、「DHCP サーバの設定」（P.3-4）を参照してください。

DHCPOFFER ユニキャスト メッセージでクライアントに送信されたコンフィギュレーション パラメータが無効である（コンフィギュレーション エラーがある）場合、クライアントは DHCP サーバに、DHCPDECLINE ブロードキャスト メッセージを戻します。

DHCP サーバはクライアントに、提示されたコンフィギュレーション パラメータが割り当てられていない、パラメータのネゴシエーション中にエラーが発生した、または DHCPOFFER メッセージに対するクライアントの応答が遅れているという意味の DHCPNAK 拒否ブロードキャスト メッセージを送信します （DHCP サーバが別のクライアントにパラメータを割り当てた可能性があります）。

DHCP クライアントは、複数の DHCP サーバから提示を受け取り、いずれも受け入れることができますが、通常は最初に受け取った提示を受け入れます。DHCP サーバから提示された IP アドレスが必ずしもクライアントに割り当てられるわけではありません。ただし、サーバは通常、クライアントが正式にアドレスを要求するまではアドレスを保管しておきます。

DHCP サーバの設定

スイッチは、DHCP クライアントとしても DHCP サーバとしても機能できます。デフォルトでは、スイッチの Cisco IOS DHCP サーバおよびリレー エージェント機能はイネーブルになっています。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能に、スイッチ ハードウェア アドレスによって各スイッチにバインドされた専用のリースを設定する必要があります。

スイッチに IP アドレス情報を受信させるには、DHCP サーバに次のリース オプションを設定する必要があります。

- クライアントの IP アドレス（必須）
- クライアントのサブネット マスク（必須）
- DNS サーバの IP アドレス（任意）
- ルータの IP アドレス（必須）

（注）　ルータの IP アドレスは、スイッチのデフォルト ゲートウェイ アドレスです。

スイッチに TFTP サーバからコンフィギュレーション ファイルを受信させる場合は、DHCP サーバに次のリース オプションを設定する必要があります。

- TFTP サーバの名前または IP アドレス（必須）
- ブート ファイル名（クライアントが必要とするコンフィギュレーション ファイル名）（推奨）
- ホスト名（任意）

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能の設定によっては、スイッチは IP アドレス情報またはコンフィギュレーション ファイル、あるいはその両方を受信できます。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能に、上記のリース オプションを設定しない場合は、スイッチはクライアントの要求に対して、設定されているパラメータだけで応答します。IP アドレスおよびサブネット マスクが応答に含まれていないと、スイッチは設定されません。ルータの IP アドレスまたは TFTP のサーバ名（または IP アドレス）が見つからなかった場合、スイッチは TFTP 要求をユニキャストしないでブロードキャストする場合があります。その他のリース オプションは、使用できなくても自動設定には影響しません。

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能は、同じ Local Area Network（LAN; ローカル エリア ネットワーク）上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが別の LAN 上で稼働している場合は、2 つの直接接続された LAN 間のブロードキャスト トラフィックを転送する DHCP リレーを設定する必要があります。ルータはブロードキャスト パケットを転送しませんが、受信したパケットの宛先 IP アドレスに基づいてパケットを転送します。リレー装置の詳細については、「リレー デバイスの設定」（P.3-5）を参照してください。

TFTP サーバの設定

DHCP サーバの設定に基づいて、スイッチは TFTP サーバから 1 つまたは複数のコンフィギュレーション ファイルをダウンロードしようとします。TFTP サーバへの IP 接続に必要なすべてのオプションについてスイッチに応答するよう DHCP を設定している場合で、なおかつ、TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を指定して DHCP サーバを設定している場合、スイッチは指定された TFTP サーバから指定されたコンフィギュレーション ファイルをダウンロードしようとします。

コンフィギュレーション ファイル名、および TFTP サーバを指定しなかった場合、またはコンフィギュレーション ファイルをダウンロードできなかった場合は、スイッチはファイル名と TFTP サーバ アドレスをさまざまに組み合わせてコンフィギュレーション ファイルをダウンロードしようとします。ファイルには、（ある場合）特定のコンフィギュレーション ファイル名と次のファイルが指定されています。network-confg、cisconet.cfg、*hostname*.confg、または *hostname*.cfg です。この場合、*hostname* はスイッチおよび router-confg と ciscortr.cfg の現在のホスト名です。使用される TFTP サーバアドレスには、（存在する場合）指定された TFTP サーバのアドレス、およびブロードキャスト アドレス（255.255.255.255）が含まれています。

スイッチが正常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には、TFTP サーバのベース ディレクトリに 1 つまたは複数のコンフィギュレーション ファイルが含まれていなければなりません。設定できるファイルは、次のとおりです。

- DHCP 応答で指定されているコンフィギュレーション ファイル（実際のスイッチ コンフィギュレーション ファイル）
- network-confg または cisconet.cfg ファイル（デフォルトのコンフィギュレーション ファイル）
- router-confg または ciscortr.cfg ファイル （これらのファイルには、すべてのスイッチに共通のコマンドが含まれています。通常、DHCP および TFTP サーバが適切に設定されていれば、これらのファイルはアクセスされません）

DHCP サーバ リース データベースに TFTP サーバ名を指定する場合は、DNS サーバのデータベースに TFTP サーバ名と IP アドレスのマッピングを設定することも必要です。

使用する TFTP サーバが、スイッチとは異なる LAN 上にある場合、またはスイッチがブロードキャスト アドレスを使用してアクセスした場合（前述のすべての必須情報が DHCP サーバの応答に含まれていない場合に発生）は、リレーを設定して TFTP サーバに TFTP パケットを転送する必要があります。詳細については、「リレー デバイスの設定」（P.3-5）を参照してください。DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能のいずれかに、すべての必須情報を使用して設定することを推奨します。

DNS サーバの設定

DHCP サーバ、またはスイッチ上で実行される DHCP サーバの機能は、DNS サーバを使用して TFTP サーバ名を IP アドレスに変換します。DNS サーバ上で、TFTP サーバ名から IP アドレスへのマッピングを設定する必要があります。TFTP サーバには、スイッチのコンフィギュレーション ファイルが存在します。

DNS サーバの IP アドレスを、DHCP 応答が IP アドレスを取得する DHCP サーバのリース データベースに設定できます。リース データベースには、DNS サーバの IP アドレスを 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に配置することも、そのスイッチとは別の LAN 上に配置することもできます。DHCP サーバが別の LAN 上に存在する場合、スイッチはルータを介して DHCP サーバにアクセスできなければなりません。

リレー デバイスの設定

スイッチが、別の LAN 上のホストからの応答を必要とするブロードキャスト パケットを送信する場合は常に、受信されるブロードキャスト パケットを宛先ホストに転送するようリレー装置を設定する必要があります。このようなブロードキャスト パケットの例として DHCP パケット、DNS パケット、場合によっては TFTP パケットが挙げられます。

リレー装置が Cisco ルータである場合、IP ルーティングをイネーブルにし（**ip routing** グローバル コンフィギュレーション コマンド）、ヘルパー アドレスを設定します（**ip helper-address** インターフェイス コンフィギュレーション コマンド）。図 3-2 では、ルータ インターフェイスを次のように設定しています。

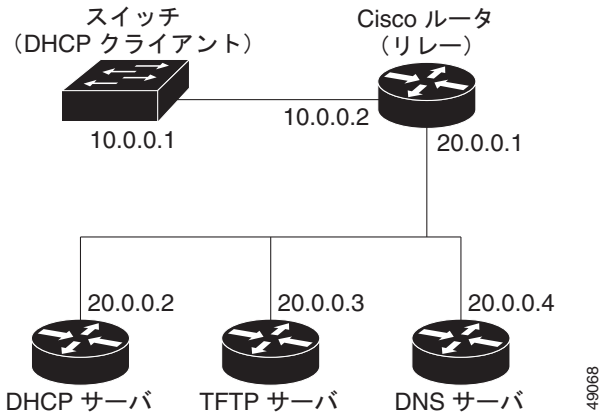
インターフェイス 10.0.0.2 の場合

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

インターフェイス 20.0.0.1 の場合

```
router(config-if)# ip helper-address 10.0.0.1
```

図 3-2　自動設定でのリレー デバイスの使用



コンフィギュレーション ファイルの入手方法

IP アドレスおよびコンフィギュレーション ファイル名が DHCP で専用のリースとして取得できるかどうかに応じて、スイッチは次の方法で設定情報を入手します。

- IP アドレスおよびコンフィギュレーション ファイル名が、スイッチ用に予約され、DHCP 応答（1 ファイル読み込み方式）で提供されます。

  スイッチは、DHCP サーバまたはスイッチ上で実行される DHCP サーバ機能のいずれかから、IP アドレス、サブネット マスク、TFTP サーバ アドレス、およびコンフィギュレーション ファイル名を受信します。スイッチは、TFTP サーバにユニキャスト メッセージを送信して、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、受信後、ブートアップ プロセスを完了します。

- スイッチの IP アドレスおよびコンフィギュレーション ファイル名が予約されているが、DHCP 応答に TFTP サーバ アドレスが含まれていない場合（1 ファイル読み込み方式）

  スイッチは、DHCP サーバから IP アドレス、サブネット マスク、およびコンフィギュレーション ファイル名を DHCP サーバまたはスイッチ上で実行される DHCP サーバ機能のいずれかから受信します。スイッチは、TFTP サーバにブロードキャスト メッセージを送信して、名前付きコンフィギュレーション ファイルをサーバのベース ディレクトリから取得して、受信後、ブートアップ プロセスを完了します。

- IP アドレスだけがスイッチ用に予約され、DHCP 応答で提供されており、コンフィギュレーション ファイル名は提供されない場合（2 ファイル読み込み方式）

スイッチは、DHCP サーバ、またはスイッチ上で実行される DHCP サーバ機能のいずれかから IP アドレス、サブネット マスク、および TFTP サーバ アドレスを受信します。スイッチは、TFTP サーバにユニキャストメッセージを送信し、network-confg または cisconet.cfg のデフォルト コンフィギュレーション ファイルを取得します （network-confg ファイルが読み込めない場合、スイッチは cisconet.cfg ファイルを読み込みます）。

デフォルトのコンフィギュレーション ファイルには、スイッチのホスト名から IP アドレスへのマッピングが含まれています。スイッチは、ファイルの情報をホスト テーブルに書き込み、ホスト名を入手します。ファイルでホスト名が見つからない場合、スイッチは DHCP 応答のホスト名を使用します。DHCP 応答でホスト名が指定されていない場合、スイッチはデフォルトの *Switch* をホスト名として使用します。

デフォルトのコンフィギュレーション ファイルまたは DHCP 応答からホスト名を入手したあと、スイッチはホスト名と同じ名前のコンフィギュレーション ファイル（network-confg または cisconet.cfg のどちらが先に読み込まれたかに応じて、*hostname*-confg または *hostname*.cfg）を TFTP サーバから読み込みます。cisconet.cfg ファイルが読み込まれている場合は、ホストのファイル名は 8 文字に切り捨てられます。

network-confg、cisconet.cfg、またはホスト名と同じ名前のファイルを読み込むことができない場合、スイッチは router-confg ファイルを読み込みます。router-confg ファイルを読み込むことができない場合、スイッチは ciscortr.cfg ファイルを読み込みます。

（注） 次のいずれかの場合に、スイッチは TFTP サーバ要求をブロードキャストします。1）DHCP 応答から TFTP サーバを入手できなかった場合、2）ユニキャスト伝送によるコンフィギュレーション ファイルの読み込みに失敗した場合、3）TFTP サーバ名を IP アドレスに変換できない場合

構成例

図 3-3 に、DHCP ベースの自動設定を使用して IP 情報を取得するネットワークの例を示します。

図 3-3　DHCP ベースの自動設定を使用するネットワークの構成例

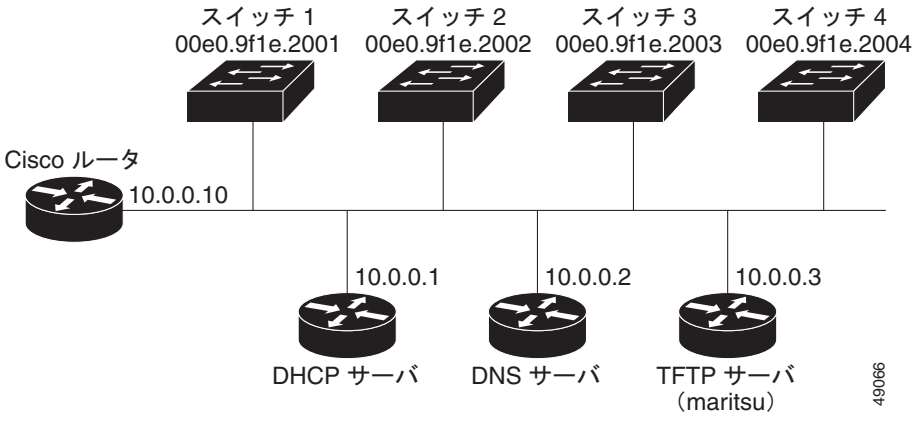


表 3-2 に、DHCP サーバ、またはスイッチ上で実行される DHCP サーバ機能の専用のリースのコンフィギュレーションを示します。

表 3-2　DHCP サーバ コンフィギュレーション

	スイッチ 1	スイッチ 2	スイッチ 3	スイッチ 4
バインディング キー（ハードウェア アドレス）	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP アドレス	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
ルータ アドレス	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS サーバ アドレス	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP サーバ名	*maritsu* または *10.0.0.3*	*maritsu* または *10.0.0.3*	*maritsu* または *10.0.0.3*	*maritsu* または *10.0.0.3*
ブート ファイル名（コンフィギュレーション ファイル）（任意）	switch1-confg	switch2-confg	switch3-confg	switch4-confg
ホスト名（任意）	switch 1	switch 2	switch 3	switch 4

DNS サーバの設定

DNS サーバは、TFTP サーバ名 *maritsu* を IP アドレス 10.0.0.3 にマッピングします。

TFTP サーバ コンフィギュレーション（UNIX）

TFTP サーバのベース ディレクトリは、/tftpserver/work/ に設定されています。このディレクトリには、2 ファイル読み込み方式で使用される network-confg ファイルがあります。このファイルには、IP アドレスに基づいてスイッチに割り当てられるホスト名が含まれています。ベース ディレクトリには、次に示すように、各スイッチのコンフィギュレーション ファイル（*switch1-confg*、*switch2-confg* など）も含まれています。

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switch1-confg
switch2-confg
switch3-confg
switch4-confg
prompt> cat network-confg
ip host switch1 10.0.0.21
ip host switch2 10.0.0.22
ip host switch3 10.0.0.23
ip host switch4 10.0.0.24
```

DHCP クライアント コンフィギュレーション

スイッチ 1 ～ 4 には、コンフィギュレーション ファイルは存在しません。

コンフィギュレーションの説明

図 3-3 の場合、スイッチ 1 はコンフィギュレーション ファイルを次のようにして読み込みます。

- スイッチ 1 は、DHCP サーバから IP アドレス 10.0.0.21 を入手します。
- DHCP サーバの応答でコンフィギュレーション ファイル名が提供されない場合、スイッチ 1 は TFTP サーバのベース ディレクトリから network-confg ファイルを読み込みます。
- スイッチ 1 は、ホスト テーブルに network-confg ファイルの内容を追加します。

- スイッチ 1 は、IP アドレス 10.0.0.21 を基にホスト テーブルを検索し、ホスト名（switch1）を取得します。
- スイッチ 1 は、ホスト名に対応するコンフィギュレーション ファイルを読み込みます。たとえば、TFTP サーバから *switch1-confg* を読み込みます。

スイッチ 2 ～ 4 も、同様にコンフィギュレーション ファイルおよび IP アドレスを取得します。

スイッチの設定

ここではスイッチの設定方法について説明します。

コンフィギュレーション モードによるスイッチの設定

コンフィギュレーション モードからスイッチを設定する手順は、次のとおりです。

ステップ 1　スーパーバイザ エンジンのコンソール インターフェイスに、コンソール端末を接続します。

ステップ 2　数秒後に、ユーザ EXEC プロンプト（Switch>）が表示されます。このあと、特権 EXEC モード（別名、イネーブル モード）を開始できます。**enable** と入力して、イネーブル モードを開始します。

```
Switch> enable
```

（注）　コンフィギュレーションを変更する場合は、イネーブル モードを開始している必要があります。

プロンプトがイネーブル プロンプト（#）に変わります。

```
Switch#
```

ステップ 3　イネーブル プロンプト（#）に、**configure terminal** コマンドを入力して、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。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

ステップ 4　グローバル コンフィギュレーション モード プロンプトに、**interface** *type slot/interface* コマンドを入力して、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。

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)#
```

ステップ 5　これらのコンフィギュレーション モードのいずれかで、スイッチ設定の変更を行います。

ステップ 6　コンフィギュレーション モードを終了するには、**end** コマンドを入力します。

ステップ 7　設定を保存します。（「実行コンフィギュレーション設定値の起動ファイルへの保存」（P.3-10）を参照）。

これで最小限のスイッチ設定が完了し、入力した設定を使用してルータを起動できるようになりました。コンフィギュレーション コマンドのリストを確認するには、プロンプトで **?** を入力するか、またはコンフィギュレーション モードで **help** キーを押します。

実行コンフィギュレーション設定の確認

入力したコンフィギュレーションまたは変更を確認するには、次の例に示すように、イネーブルプロンプト（#）で **show running-config** コマンドを入力します。

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch

<...output truncated...>

!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end
Switch#
```

実行コンフィギュレーション設定値の起動ファイルへの保存

注意　このコマンドは、コンフィギュレーション モードで入力した設定値を保存します。この作業を行わないと、次回システムをリロードするときに設定が失われます。

コンフィギュレーション、コンフィギュレーションへの変更内容、またはスタートアップ コンフィギュレーションへの変更を NVRAM に保存するには、イネーブル プロンプト（#）で **copy running-config startup-config** コマンドを入力します。

```
Switch# copy running-config startup-config
```

NVRAM での設定の確認

NVRAM に保存されている情報を表示するには、**show startup-config** EXEC コマンドを入力します。

次に、一般的なシステム設定の例を示します。

```
Switch# show startup-config
Using 1579 out of 491500 bytes, uncompressed size = 7372 bytes
Uncompressed configuration from 1579 bytes to 7372 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service compress-config
!
hostname Switch
!
!
ip subnet-zero
!
!
!
!
interface GigabitEthernet1/1
 no snmp trap link-status
!
interface GigabitEthernet1/2
 no snmp trap link-status
!--More--

<...output truncated...>

!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

デフォルト ゲートウェイの設定

（注） スイッチがデフォルト ゲートウェイを使用するのは、ルーティング プロトコルが設定されていない場合に限られます。

スイッチにルーティング プロトコルが設定されていない場合、他のサブネットにデータを送信するデフォルト ゲートウェイを設定します。デフォルト ゲートウェイには、スイッチに直接接続するルータ上のインターフェイスの IP アドレスを指定する必要があります。

デフォルト ゲートウェイを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip default-gateway IP-address`	デフォルト ゲートウェイを設定します。
ステップ 2	`Switch# show ip route`	デフォルト ゲートウェイが IP ルーティング テーブルに正しく表示されることを確認します。

次に、デフォルト ゲートウェイを設定し、その設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip default-gateway 172.20.52.35
Switch(config)# end
3d17h: %SYS-5-CONFIG_I: Configured from console by console
Switch# show ip route
Default gateway is 172.20.52.35

Host               Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty
Switch#
```

スタティック ルートの設定

Telnet ステーションまたは SNMP ネットワーク管理ワークステーションが、スイッチと異なるネットワークに存在し、ルーティング プロトコルが設定されていない場合、使用しているエンド ステーションが存在するネットワークに対応するスタティック ルーティング テーブル エントリを追加しなければならない場合があります。

スタティック ルートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# ip route dest_IP_address mask {forwarding_IP | vlan vlan_ID}`	リモート ネットワークへのスタティック ルートを設定します。
ステップ 2	`Switch# show running-config`	スタティック ルートが正しく表示されることを確認します。

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.10.5.10 のワークステーションへのスタティック ルートを設定する例を示します。この場合、サブネット マスクと転送ルータの IP アドレス 172.20.3.35 を用います。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip route 171.10.5.10 255.255.255.255 172.20.3.35
Switch(config)# end
Switch#
```

次に、**show running-config** コマンドを使用して、スタティック ルートの設定を確認する例を示します。

```
Switch# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
```

```
ip route 171.10.5.10 255.255.255.255 172.20.3.35
no ip http server
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

次に、スイッチ上で **ip route** コマンドを使用して、IP アドレス 171.20.5.3 のワークステーションへのスタティック ルートを設定する例を示します。この場合、サブネット マスクと接続されている Virtual Local Area Network（VLAN; 仮想 LAN）1 を用います。

```
Switch# configure terminal
Switch(config)# ip route 171.20.5.3 255.255.255.255 vlan 1
Switch(config)# end
Switch#
```

次に、**show running-config** コマンドを使用して、スタティック ルートの設定を確認する例を示します。

```
Switch# show running-config
Building configuration...
.
<...output truncated...>
.
ip default-gateway 172.20.52.35
ip classless
ip route 171.20.5.3 255.255.255.255 Vlan1
no ip http server
!
!
x25 host z
!
line con 0
 transport input none
line vty 0 4
 exec-timeout 0 0
 password lab
 login
 transport input lat pad dsipcon mop telnet rlogin udptn nasi
!
end

Switch#
```

特権 EXEC コマンドへのアクセス コントロール

次の手順に従って、システム コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御します。

- 「スタティック イネーブル パスワードの設定または変更」（P.3-14）
- 「enable password コマンドおよび enable secret コマンドの使用」（P.3-14）
- 「イネーブル パスワードの設定または変更」（P.3-15）

- 「パスワードの暗号化」（P.3-22）
- 「複数の特権レベルの設定」（P.3-23）

スタティック イネーブル パスワードの設定または変更

イネーブル モードへのアクセスを制御するスタティック パスワードを設定または変更するには、次の作業を行います。

表 3-1

コマンド	目的
`Switch(config)# enable password password`	特権 EXEC モードの新しいパスワードを設定するか、または既存のパスワードを変更します。

次に、特権 EXEC モードでイネーブル パスワードを「lab」に設定する例を示します。

```
Switch# configure terminal
Switch(config)# enable password lab
Switch(config)#
```

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

enable password コマンドおよび enable secret コマンドの使用

ネットワークで送受信されるパスワードまたは TFTP サーバに保存されるパスワードについて、セキュリティをさらに強化するには、**enable password** コマンドまたは **enable secret** コマンドを使用します。どちらのコマンドも、イネーブル モード（デフォルト）または指定したその他の特権レベルにアクセスするために、ユーザが入力しなければならない暗号化パスワードを設定します。

enable secret コマンドの使用を推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

スイッチがイネーブル パスワードを要求するように設定するには、次のいずれかの作業を行います。

コマンド	目的
`Switch(config)# enable password [level level] {password | encryption-type encrypted-password}`	特権 EXEC モードを開始するためのパスワードを設定します。
`Switch(config)# enable secret [level level] {password | encryption-type encrypted-password}`	不可逆的な暗号化方式を使用して保存されるシークレット パスワードを設定します（**enable password** コマンドおよび **enable secret** コマンドを両方とも設定した場合、ユーザはイネーブル シークレット パスワードを入力しなければなりません）。

level オプションを使用してどちらかのパスワード コマンドを入力すると、特定の特権レベルにアクセスするためのパスワードを定義できます。レベルを指定してパスワードを設定したあと、特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

service password-encryption コマンドをイネーブルにしている場合は、入力したパスワードが暗号化されます。**more system:running-config** コマンドを使用してパスワードを表示すると、パスワードは暗号化形式で表示されます。

暗号化タイプを指定する場合は、暗号化パスワード（別の Catalyst 4500 シリーズ スイッチの設定からコピーした暗号化パスワード）を入力する必要があります。

（注）　暗号化パスワードを忘れた場合、回復はできません。NVRAM を消去し、新しいパスワードを設定する必要があります。詳細については、「イネーブル パスワードを忘れた場合の回復方法」（P.3-25）を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

イネーブル パスワードの設定または変更

イネーブル パスワードを設定または変更するには、次の作業を行います。

表 3-2

コマンド	目的
`Switch(config-line)# password password`	特権レベルの新しいパスワードを設定するか、既存のパスワードを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

TACACS+ によるスイッチ アクセスの制御

ここでは、詳細なアカウンティング情報を提供し、認証および許可プロセスを柔軟に管理できるようにするために、TACACS+ をイネーブルにして設定する方法について説明します。TACACS+ は、認証、許可、アカウンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

（注）　ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」（P.3-16）
- 「TACACS+ の動作」（P.3-17）
- 「TACACS+ の設定」（P.3-18）
- 「TACACS+ 設定の表示」（P.3-22）

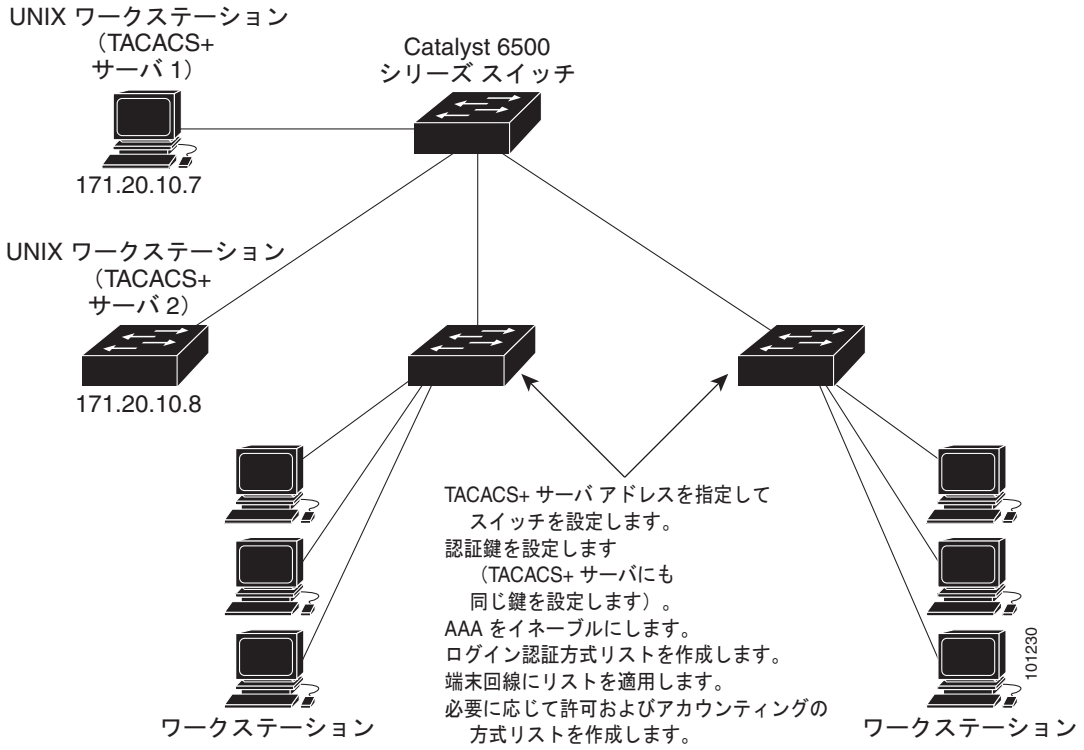
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ は、個別のモジュール式 AAA 機能を備えています。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスは固有のデータベースに組み込まれるため、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスも利用できます。

TACACS+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。ネットワーク アクセス サーバは、個々のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークとの接続を実現します（図 3-4 を参照）。

図 3-4　一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号など、複数の質問でユーザの身元を確認します）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード エージング ポリシーのため、パスワードを変更する必要があることをメッセージでユーザに通知することができます。

- 許可：ユーザのセッション期間中の管理機能を詳細に制御します。これには自動コマンドの設定、アクセス コントロール、セッション期間、またはプロトコル サポートなどが含まれますが、それに限定されません。また、TACACS+ 許可機能によってユーザが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立すると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、ユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワード プロンプトを取得します。スイッチによってパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

   TACACS+ によって、デーモンはユーザを認証するのに十分な情報を取得するまで、デーモンとユーザの間で対話が可能になります。デーモンはユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
   - ACCEPT：ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
   - REJECT：ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログイン シーケンスを再試行するように求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
   - CONTINUE：ユーザは、さらに認証情報の入力を求められます。

   認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。
   - Telnet、Secure Shell（SSH; セキュア シェル）、rlogin、または特権 EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。方式リストでは、ユーザの認証、許可、およびアカウントの記録を行うための順序と方式を定義します。方式リストを使用すると、1 つまたは複数のセキュリティ プロトコルを指定し、最初の方式が失敗した場合のバックアップ システムを確保できます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」（P.3-18）
- 「TACACS+ サーバ ホストの特定および認証キーの設定」（P.3-18）
- 「TACACS+ ログイン認証の設定」（P.3-19）
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」（P.3-21）
- 「TACACS+ アカウンティングの起動」（P.3-22）

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

（注）　TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定および認証キーの設定

認証用に単一サーバを使用する、または既存のサーバ ホストをグループ化するために AAA サーバ グループを使用するようスイッチを設定できます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを維持する IP ホスト（1 つまたは複数）を特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • （任意）**port** *integer* には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**timeout** *integer* には、スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチはタイムアウトしてエラーを宣言します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**key** *string* には、スイッチと TACACS+ デーモン間のすべてのトラフィックを暗号化および暗号解除するための暗号キーを指定します。暗号化が正しく機能するには、TACACS+ デーモンに同じキーを設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）AAA サーバ グループを、特定のグループ名で定義します。 このコマンドによって、スイッチはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	入力内容を確認します。
ステップ 8	**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。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *hostname* グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server tacacs+** *group-name* グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義してから、さまざまなポートにそのリストを適用します。方式リストには実行する認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義した認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証のために 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証し

ます。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルトの状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ **enable** *password* グローバル コンフィギュレーション コマンドを使用してイネーブル パスワードを定義しておく必要があります。 • **group tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの特定および認証キーの設定」（P.3-18）を参照してください。 • **line**：回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *name* **password** グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンド	目的
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**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。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、スイッチはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドに **tacacs+** キーワードを付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可を、スイッチに設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ TACACS+ 許可をスイッチに設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**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。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**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。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

パスワードの暗号化

プロトコル アナライザでパケットを調べる（パスワードを読み取る）ことができるので、パスワードを暗号化するように Cisco IOS ソフトウェアを設定することによって、アクセス セキュリティを強化することができます。暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。

パスワードを暗号化するように Cisco IOS ソフトウェアを設定するには、次の作業を行います。

表 3-3

コマンド	目的
`Switch(config)# service password-encryption`	パスワードを暗号化します。

暗号化は、現在の設定が保存されるとき、またはパスワードが設定されるときに行われます。パスワードの暗号化は、認証キー パスワード、特権コマンド パスワード、コンソールおよび仮想端末回線アクセス パスワード、およびボーダー ゲートウェイ プロトコル（BGP）ネイバー パスワードを含む、すべてのパスワードに適用されます。**service password-encryption** コマンドを使用すると、許可されていないユーザがコンフィギュレーション ファイルのパスワードを表示できなくなります。

注意　**service password-encryption** コマンドでは、高度なネットワーク セキュリティは提供されません。このコマンドを使用する場合は、その他のネットワーク セキュリティ手段も講じる必要があります。

暗号化パスワードを忘れた場合、パスワードの回復はできません（元のパスワードを取り戻すことはできません）。ただし、暗号化パスワードを忘れても、スイッチの制御を取り戻すことはできます。詳細については、「イネーブル パスワードを忘れた場合の回復方法」（P.3-25）を参照してください。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

複数の特権レベルの設定

Cisco IOS ソフトウェアには、パスワード セキュリティのモードがデフォルトで 2 つあります。ユーザ EXEC モードと特権 EXEC モードです。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザが **clear line** コマンドにアクセスできるようにするには、このコマンドにレベル 2 セキュリティを割り当て、レベル 2 パスワードを広範囲に配布します。一方、**configure** コマンドにアクセスできるユーザを限定する場合には、このコマンドにレベル 3 セキュリティを割り当て、そのパスワードを配布するユーザ数を減らします。

ここでは、追加レベルのセキュリティを設定する手順について説明します。

- 「コマンドの特権レベルの設定」（P.3-23）
- 「回線のデフォルト特権レベルの変更」（P.3-24）
- 「特権レベルへのログイン」（P.3-24）
- 「特権レベルの終了」（P.3-24）
- 「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）

コマンドの特権レベルの設定

コマンドの特権レベルを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# privilege mode level level command`	コマンドの特権レベルを設定します。
ステップ 2	`Switch(config)# enable password level level [encryption-type] password`	特権レベルにアクセスするためのイネーブル パスワードを指定します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

回線のデフォルト特権レベルの変更

特定の回線または回線グループのデフォルト特権レベルを変更するには、次の作業を行います。

表 3-4

コマンド	目的
`Switch(config-line)# privilege level level`	回線のデフォルト特権レベルを変更します。

パスワードまたはアクセス レベルの設定を表示する方法については、「パスワード、アクセス レベル、および特権レベルの設定の表示」（P.3-24）を参照してください。

特権レベルへのログイン

特定の特権レベルにログインするには、次の作業を行います。

表 3-5

コマンド	目的
`Switch# enable level`	指定された特権レベルにログインします。

特権レベルの終了

特定の特権レベルを終了するには、次の作業を行います。

表 3-6

コマンド	目的
`Switch# disable level`	指定した特権レベルを終了します。

パスワード、アクセス レベル、および特権レベルの設定の表示

詳細なパスワード情報を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# show running-config`	パスワードおよびアクセス レベルの設定を表示します。
ステップ 2	`Switch# show privilege`	特権レベルの設定を表示します。

次に、パスワードおよびアクセス レベルの設定を表示する例を示します。

```
Switch# show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Switch
!
boot system flash sup-bootflash
enable password lab
!
<...output truncated...>
```

次に、特権レベルの設定を表示する例を示します。

```
Switch# show privilege
Current privilege level is 15
Switch#
```

イネーブル パスワードを忘れた場合の回復方法

（注） NVRAM にあらかじめ設定されているコンフィギュレーション レジスタについては、「ソフトウェア コンフィギュレーション レジスタの設定」（P.3-27）を参照してください。

イネーブル パスワードを忘れた場合の回復手順は、次のとおりです。

ステップ 1　コンソール インターフェイスに接続します。

ステップ 2　起動後 5 秒以内に Ctrl を押した状態で C を押して、ブート シーケンスを停止し、ROM モニタを開始します。

ステップ 3　コンフィギュレーション メモリ（NVRAM）を読み込まずに起動するように、スイッチを設定します。

ステップ 4　システムをリブートします。

ステップ 5　イネーブル モードにアクセスします（パスワードが設定されていない場合は、パスワードを指定しません）。

ステップ 6　パスワードを表示または変更するか、または設定を消去します。

ステップ 7　通常どおり NVRAM を読み込んで起動するように、スイッチを再設定します。

ステップ 8　システムをリブートします。

スーパーバイザ エンジンのスタートアップ コンフィギュレーションの変更

ここでは、スーパーバイザ エンジンのスタートアップ コンフィギュレーションの機能と、BOOT 変数およびコンフィギュレーション レジスタを変更する手順について説明します。

スーパーバイザ エンジンのブート コンフィギュレーションの概要

スーパーバイザ エンジンの起動プロセスには、2 種類のソフトウェア イメージが関係します。ROM モニタとスーパーバイザ エンジン ソフトウェアです。スイッチを起動またはリセットすると、Random Access Memory Monitor（ROMmon; ランダム アクセス メモリ モニタ）コードが実行されます。NVRAM に保存されている設定に応じて、スーパーバイザ エンジンは ROMmon モードを継続するか、またはスーパーバイザ エンジン ソフトウェアをロードします。

ユーザ側で設定できる 2 つのパラメータによって、スイッチの起動方法が決まります。コンフィギュレーション レジスタと BOOT 環境変数です。コンフィギュレーション レジスタについては、「ブート フィールドの変更および boot コマンドの使用」（P.3-28）を参照してください。BOOT 環境変数については、「スタートアップ システム イメージの指定」（P.3-31）を参照してください。

ROM モニタの概要

ROM モニタ（ROMmon）はスイッチの起動時、リセット時、または致命的な例外が発生した場合に呼び出されます。スイッチで ROMmon モードが開始されるのは、スイッチが有効なソフトウェア イメージを見つけることができなかった場合、NVRAM 内の設定が壊れていた場合、またはコンフィギュレーション レジスタが ROMmon モードを開始するように設定されていた場合です。ROMmon モードでは、ブートフラッシュまたはフラッシュ ディスクからソフトウェア イメージを手動でロードできます。また、管理インターフェイスから起動することもできます。ROMmon モードはプライマリ イメージをロードします。このプライマリ イメージで、BOOTLDR 環境変数を使用してローカルに、またはネットワークを通じて、指定されたソースから起動するセカンダリ イメージを設定できます。この変数については、「スイッチの出荷時のデフォルト設定へのリセット」（P.3-32）を参照してください。

また、スイッチを再起動して、起動後の最初の 5 秒間に Ctrl を押した状態で C を押しても、ROMmon モードを開始できます。端末サーバから接続している場合は、エスケープによって Telnet プロンプトを表示し、**send break** コマンドを入力すると、ROMmon モードが開始されます。

（注）　コンフィギュレーションレジスタで Ctrl を押した状態で C を押す機能がディセーブルに設定されているかどうかにかかわらず、スイッチの再起動後 5 秒間は常に Ctrl を押した状態で C を押す機能がイネーブルになります。

ROM モニタの機能は、次のとおりです。

- 電源投入時の信頼性テスト
- ハードウェアの初期化

- 起動能力（手動による起動および自動起動が可能）
- ファイル システム（ROMmon の実行時は読み取り専用）

ソフトウェア コンフィギュレーション レジスタの設定

スイッチは 16 ビットのソフトウェア コンフィギュレーション レジスタを使用します。このコンフィギュレーション レジスタに特定のシステム パラメータを設定できます。ソフトウェア コンフィギュレーション レジスタの設定は、NVRAM にあらかじめ設定されています。

次の場合は、ソフトウェア コンフィギュレーション レジスタの設定値を変更する必要があります。

- 起動元およびデフォルトのブート ファイル名を選択する場合
- ブロードキャスト アドレスを制御する場合
- コンソール端末のボーレートを設定する場合
- フラッシュ メモリからオペレーティング ソフトウェアをロードする場合
- 忘れたパスワードを回復する場合
- ブートストラップ プログラム プロンプトで **boot** コマンドを使用し、手動でシステムを起動する場合
- システム ブートストラップ ソフトウェア（ブート イメージ）またはオンボード フラッシュ メモリ上のデフォルトのシステム イメージから自動的に起動し、NVRAM 上のコンフィギュレーション ファイル内の **boot system** コマンドを読み取るように強制的に設定する場合

注意　誤って Catalyst 4500 シリーズ スイッチのスイッチが停止するような事態を避けるために、コンフィギュレーション レジスタ設定を有効にするには、表 3-3 に記載されている個々の設定値を使用するのではなく、設定値を組み合わせる必要があります。たとえば、出荷時のデフォルトである 0x2101 という値は、3 つの設定値の組み合わせです。

表 3-3 に、各ソフトウェア コンフィギュレーション メモリ ビットの意味を示します。表 3-4 にブート *フィールド*の定義を示します。

表 3-3　ソフトウェア コンフィギュレーション レジスタ ビット

ビット番号[1]	16 進数	意味
00 ～ 03	0x0000 ～ 0x000F	ブート フィールド（表 3-4 を参照）
04	0x0010	未使用
05	0x0020	ビット 2 はコンソール回線速度
06	0x0040	システム ソフトウェアに NVRAM の内容を無視させます。
07	0x0080	OEM[2] ビットをイネーブルにします。
08	0x0100	未使用
09	0x0200	未使用
10	0x0400	すべて 0 の IP ブロードキャスト
11 ～ 12	0x0800 ～ 0x1000	コンソール回線速度のビット 1 と 0（デフォルトは 9600 ボー）
13	0x2000	ネットブートの失敗後に ROM モニタをロードします。
14	0x4000	IP ブロードキャストでネットワーク番号を使用しません。

1. コンフィギュレーション レジスタの出荷時のデフォルト値は 0x2101 です。この値は、次の設定値を組み合わせたものです。バイナリ ビット 13、ビット 8 = 0x0100、およびバイナリ ビット 00 ～ 03 = 0x0001（表 3-4 を参照）。
2. OEM = Original Equipment Manufacturer（相手先商標製造会社）

表 3-4　ブート フィールド（コンフィギュレーション レジスタ ビット 00 ～ 03）の説明

ブート フィールド	意味
00	システム ブートストラップ プロンプトの状態（自動起動しません）
01	オンボード フラッシュ メモリ上で最初に検出されたシステム イメージを起動します。
02 ～ 0F	BOOT 環境変数で指定されたイメージを使用して自動起動します。複数のイメージが指定されている場合、スイッチは BOOT 変数で最初に指定されたイメージの起動を試みます。スイッチがこのイメージからの起動に成功すると、再起動時に同じイメージが使用されます。スイッチが BOOT 変数で最初に指定されたイメージからの起動に失敗すると、スイッチは BOOT 変数の次のイメージからの起動を試みます。BOOT 変数の最後のイメージからスイッチが起動できない場合、スイッチは BOOT 変数の最初に戻って起動を試みます。自動起動は、スイッチが BOOT 変数で指定されたいずれかのイメージからの起動に成功するまで続きます。

ブート フィールドの変更および boot コマンドの使用

コンフィギュレーション レジスタのブート フィールドにより、スイッチはオペレーティング システム イメージをロードするかどうかを決定し、ロードする場合はシステム イメージをどの位置から取得するかを決定します。ここでは、コンフィギュレーション レジスタのブート フィールドの使用方法および設定手順と、コンフィギュレーション レジスタのブート フィールドを変更する場合の手順について説明します。ROMmon では、コンフィギュレーション レジスタの変更とブート設定の変更に **confreg** コマンドを使用できます。

ソフトウェア コンフィギュレーション レジスタのビット 0 ～ 3 が、ブート フィールドを形成します。

（注） システムおよびスペア製品のコンフィギュレーション レジスタの出荷時のデフォルト値は、0x2101 です。ただし、推奨値は 0x0102 です。

ブート フィールドを 00 または 01（0-0-0-0 または 0-0-0-1）に設定すると、システムはシステム コンフィギュレーション ファイルの起動命令を無視して、次の動作を行います。

- ブート フィールドが 00 に設定されている場合は、システム ブートストラップまたは ROMmon プロンプトで **boot** コマンドを入力し、手動でオペレーティング システムを起動する必要があります。
- ブート フィールドが 01 に設定されている場合は、ブートフラッシュ Single In-line Memory Module（SIMM; シングル インライン メモリ モジュール）で最初に検出されたイメージを起動します。
- ブート フィールド全体が 0-0-1-0 ～ 1-1-1-1 の範囲の値である場合、スイッチはスタートアップ コンフィギュレーション ファイルの **boot system** コマンドで指定されるシステム イメージをロードします。

注意 ブートフィールドを 0-0-1-0 ～ 1-1-1-1 の範囲の値に設定する場合は、**boot system** コマンドで値を指定する必要があります。値を指定しないと、スイッチは起動できず ROMmon のままになります。

boot コマンドは単独でも入力できますが、フラッシュ メモリに保存されたファイル名、ネットワーク サーバからの起動を指定するファイル名など、追加の起動命令を含めることもできます。ファイル名または他の起動命令を指定せずに **boot** コマンドを使用すると、システムはデフォルトのフラッシュ イメージ（オンボード フラッシュ メモリ上の最初のイメージ）から起動します。また、特定のフラッシュ イメージから起動するように指定することもできます（**boot system flash** *filename* コマンドを使用）。

また、**boot** コマンドを使用して、スーパーバイザ エンジン上のスロット 0 にあるコンパクト フラッシュ カードに保存されたイメージを起動することもできます。

ブート フィールドの変更

ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更します。ソフトウェア コンフィギュレーション レジスタのブート フィールドを変更するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# show version`	現在のコンフィギュレーション レジスタ設定値を判別します。
ステップ 2	`Switch# configure terminal`	コンフィギュレーション モードを開始し、**terminal** オプションを指定します。
ステップ 3	`Switch(config)# config-register` *value*	スイッチへの希望するシステム イメージのロード方法に応じて、既存のコンフィギュレーション レジスタ設定値を変更します。
ステップ 4	`Switch(config)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Switch# reload`	スイッチを再起動して、変更を有効にします。

スイッチが Cisco IOS ソフトウェアを実行している場合にコンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ 1　**enable** コマンドおよびパスワードを入力して、特権レベルを開始します。

```
Switch> enable
Password:
Switch#
```

ステップ 2　EXEC モード プロンプト（#）で、**configure terminal** コマンドを次のように入力します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

ステップ 3　コンフィギュレーション レジスタを 0x102 に設定します。

```
Switch(config)# config-register 0x102
```

value コマンド変数を指定して、コンフィギュレーション レジスタの内容を設定します。*value* は、先頭が 0x の 16 進数です（表 3-3（P.3-27）を参照）。

ステップ 4　コンフィギュレーション モードを終了するには、**end** コマンドを入力します。新しい設定値がメモリに保存されます。ただし、システムを再起動するまで新しい設定値は有効になりません。

ステップ 5　**show version** EXEC コマンドを入力して、現在有効なコンフィギュレーション レジスタ値を表示します。これは次回のリロード時に使用されます。この値は次の出力例のように、画面の最後の行に表示されます。

```
Configuration register is 0x141 (will be 0x102 at next reload)
```

ステップ 6　設定を保存します。（「実行コンフィギュレーション設定値の起動ファイルへの保存」（P.3-10）を参照してください）。コンソールから **reload** コマンドを入力するなどの方法でシステムをリロードしないかぎり、コンフィギュレーション レジスタの変更は有効になりません）。

ステップ 7　システムをリブートします。システムを再起動した時点で、新しいコンフィギュレーション レジスタ値が有効になります。

コンフィギュレーション レジスタ設定値の確認

現在のコンフィギュレーション レジスタ設定値を確認するには、**show version** EXEC コマンドを使用します。コンフィギュレーション レジスタの設定を確認するには、ROMmon モードで **show version** コマンドを使用します。

スイッチのコンフィギュレーション レジスタ設定値を確認するには、次の作業を行います。

表 3-7

コマンド	目的
Switch# **show version**	コンフィギュレーション レジスタの設定値を表示します。

次に示す **show version** コマンドの出力例では、現在のコンフィギュレーション レジスタは、スイッチがオペレーティング システム イメージを自動的にロードしないように設定されています。レジスタは ROMmon モードを開始し、ユーザによる ROM モニタ コマンドの入力を待機します。

```
Switch# show version
Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-ENTSERVICES-M), Version
12.2(40)SG, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 07-Nov-07 19:16 by prod_rel_team
Image text-base: 0x10000000, data-base: 0x11992640

ROM: 12.2(31r)SGA4
Pod Revision 0, Force Revision 31, Gill Revision 19

Switch uptime is 2 minutes
System returned to ROM by reload
System image file is
"tftp://172.25.60.31/release/122/bin/122-40.SG/cat4500-entservices-mz.122-40.SG"

cisco WS-C4948-10GE (MPC8540) processor (revision 5) with 262144K bytes of memory.
Processor board ID FOX095107K6
MPC8540 CPU at 667Mhz, Fixed Module
Last reset from Reload
1 Virtual Ethernet interface
48 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x860
```

スタートアップ システム イメージの指定

スタートアップ コンフィギュレーション ファイルまたは BOOT 環境変数に複数のブート コマンドを入力して、システム イメージをロードするバックアップ方法を提供することができます。

BOOT 環境変数については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Loading and Maintaining System Images and Microcode」の章の「Specify the Startup System Image in the Configuration File」でも説明されています。

次の項目に従って、フラッシュ メモリから起動するようにスイッチを設定してください。フラッシュ メモリは Single In-Line Memory Module（SIMM; シングル インライン メモリ モジュール）またはフラッシュ ディスクのいずれかになります。フラッシュ メモリのタイプについては、適切なハードウェアのインストールおよびメンテナンス マニュアルを確認してください。

フラッシュ メモリの使用

フラッシュ メモリを使用すると、次の作業が可能になります。

- TFTP を使用したシステム イメージのフラッシュ メモリへのコピー
- フラッシュ メモリからの自動または手動によるシステムの起動
- TFTP または RCP を使用したフラッシュ メモリ イメージのネットワーク サーバへのコピー

フラッシュ メモリの機能

フラッシュ メモリを使用すると、次の作業が可能になります。

- TFTP または RCP 転送による複数のシステム ソフトウェア イメージのリモートでのロード（ファイルのロードごとに 1 回の転送）
- フラッシュ メモリに保存されたシステム ソフトウェア イメージからの、手動または自動によるスイッチの起動（ROM からの直接起動も可能）

セキュリティ対策

フラッシュ メモリからロードする場合、次のセキュリティ上の注意を参照してください。

注意　フラッシュ メモリに保存されたシステム イメージを変更できるのは、コンソール端末の特権 EXEC レベルからにかぎられます。

フラッシュ メモリの設定

スイッチがフラッシュ メモリから起動するように設定する手順は、次のとおりです。ハードウェアのインストール方法については、適切なハードウェアのインストールおよびメンテナンス マニュアルを参照してください。

ステップ 1　TFTP またはその他のプロトコルでシステム イメージをフラッシュ メモリにコピーします。次の URL の『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』の「Cisco IOS File Management」および「Loading and Maintaining System Images」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_2sr/cf_12_2sr_book.html

ステップ 2　フラッシュ メモリ内の必要なファイルからシステムが自動的に起動するように設定します。コンフィギュレーション レジスタ値を変更しなければならない場合があります。コンフィギュレーション レジスタを変更する方法については、「ブート フィールドの変更および boot コマンドの使用」（P.3-28）を参照してください。

ステップ 3　設定を保存します。

ステップ 4　システムの電源をオフにしてから再びオンにしてシステムを再起動し、すべて正常に動作しているかどうかを確認します。

環境変数の制御

環境変数の制御は ROM モニタが行いますが、特定のコマンドを使用して環境変数を作成、変更、または表示することができます。BOOT 変数と BOOTLDR 変数を作成または変更するには、それぞれ **boot system** と **boot bootldr** グローバル コンフィギュレーション コマンドを使用します。BOOT 環境変数の設定の詳細については、『*Configuration Fundamentals Configuration Guide*』の「Loading and Maintaining System Images and Microcode」の章の「Specify the Startup System Image in the Configuration File」を参照してください。

（注）　**boot system** と **boot bootldr** グローバル コンフィギュレーション コマンドが有効なのは、実行コンフィギュレーションだけです。あとで使用できるようにコンフィギュレーションを保存する場合は、ROM モニタ制御下に情報を置くスタートアップ コンフィギュレーションに環境変数の設定を保存する必要があります。環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、**copy system:running-config nvram:startup-config** コマンドを使用します。

BOOT 変数および BOOTLDR 変数の内容を表示するには、**show bootvar** コマンドを使用します。このコマンドは、スタートアップ コンフィギュレーション内のこれらの変数の設定値を表示しますが、実行コンフィギュレーションの設定値がスタートアップ コンフィギュレーションの設定値と異なっている場合には、実行コンフィギュレーション内の設定値も表示します。次に、スイッチ上の BOOT 変数と BOOTLDR 変数を確認する例を示します。

```
Switch# show bootvar
BOOTLDR variable = bootflash:cat4000-is-mz,1;
Configuration register is 0x0
Switch#
```

スイッチの出荷時のデフォルト設定へのリセット

製造元およびリペア センターでは、**erase /all non-default** コマンドを使用して次の作業を実行できます。

- ローカルのスーパーバイザ エンジンの不揮発設定および状態（NVRAM およびフラッシュ）をクリアします。
- カスタマーへ出荷する前に、Catalyst 4500 シリーズ スイッチ上で出荷時のデフォルト パラメータを設定します。

次に、このコマンドの出力例を示します。

```
Switch# erase /all non-default
Erase and format operation will destroy all data in non-volatile storage.  Continue?
[confirm]
Formatting bootflash: ...
```

```
Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
     ConfigReg=0x2101
     PS1=rommon ! >
     EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

Catalyst 4500 シリーズ スイッチが TFTP サーバにアクセス可能な場合は、tftp コマンドを使用してブートフラッシュ メモリにイメージをコピーできます。

```
Switch# copy tftp://192.20.3.123/tftpboot/abc/cat4500-entservices-mz.bin bootflash:
```

コピーが完了すると、**reload** コマンドによりブートフラッシュ メモリに格納されたイメージにコピーされたばかりの Catalyst 4500 シリーズ スイッチのイメージを再起動できます。

```
Switch# reload

 System configuration has been modified. Save? [yes/no]: no
 Proceed with reload? [confirm]

 00:06:17: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

erase /all non-default コマンドによって設定されるデフォルト パラメータの詳細については、『*Catalyst 4500 Series Switch Command Reference*』の **erase** コマンド ページの使用上のガイドラインを参照してください。