



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。

- 「デフォルト スイッチ設定」 (P.3-1)
- 「DHCP ベースの自動設定の設定」 (P.3-2)
- 「スイッチの設定」 (P.3-9)
- 「特権 EXEC コマンドへのアクセス制御」 (P.3-13)
- 「イネーブル パスワードを忘れた場合の回復方法」 (P.3-25)
- 「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」 (P.3-25)
- 「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)



(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	通常モード
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、Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) 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 ベースの自動設定の概要」(P.3-2)
- 「DHCP クライアントの要求プロセス」(P.3-3)
- 「DHCP サーバの設定」(P.3-4)
- 「TFTP サーバの設定」(P.3-4)
- 「DNS サーバの設定」(P.3-5)
- 「リレー装置の設定」(P.3-5)
- 「コンフィギュレーション ファイルの入手方法」(P.3-6)
- 「構成例」(P.3-7)

DHCP サーバがシスコ製デバイスの場合、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)

Release 12.2(20)EW 以降では、**write erase** コマンドを発行することにより、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 クライアントとしても DHCP サーバとしても機能できます。

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、ネットワーク上のコンフィギュレーション ファイルの位置をリレーする場合は、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバおよび Domain Name System (DNS; ドメイン ネーム システム) サーバの設定が必要な場合があります。

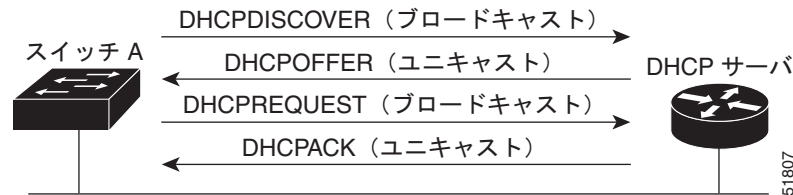
DHCP ベースの自動設定は、スイッチの BOOTstrap Protocol (BOOTP) クライアント機能に代わるものです。

DHCP クライアントの要求プロセス

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。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 DHCP サーバはすべて、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 (DHCP サーバがパラメータを別のクライアントに割り当てた) 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 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 Internetwork Operating System (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。

- 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な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 上で稼動している場合は、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、受信されるパケットの宛先 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、「[リレー装置の設定](#)」(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 ファイルのダウンロードを試行します。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、および TFTP サーバ名、アドレス、およびコンフィギュレーション ファイル名を使用して DHCP サーバを設定した場合、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-config、cisco.net.cfg、hostname.config、または hostname.cfg です。この場合、hostname はスイッチおよび router-config と ciscotr.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、(ある場合) 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 サーバは、そのベース 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を含んでいる必要があります。設定できるファイルは、次のとおりです。

- DHCP 応答の名前付き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-config または cisco.net.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-config または ciscotr.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必要があります。

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、「[リレー装置の設定](#)」(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含まれます。

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 アドレスを最大 2 つまで入力できます。

DNS サーバは、スイッチと同じ LAN 上に存在しても、またスイッチとは別の LAN 上に存在していてもかまいません。DNS 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 DNS サーバにアクセス可能である必要があります。

リレー装置の設定

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。

リレー装置がシスコ製 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。

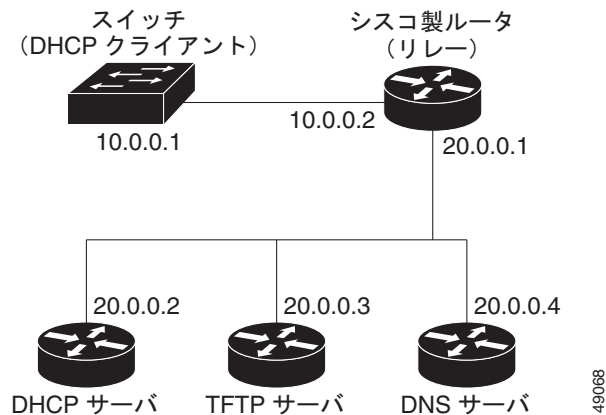
インターフェイス 10.0.0.2 では、

```
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 では、

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

図 3-2 自動設定でのリレー装置の使用



コンフィギュレーション ファイルの入手方法

DHCP 予約リースの IP アドレスおよびコンフィギュレーション ファイル名のアベイラビリティに応じて、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。

- 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ます。

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 応答で提供されます。コンフィギュレーション ファイル名は提供されません (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 メッセージを送り、`network-config` または `cisconet.cfg` のデフォルトのコンフィギュレーション ファイルを取得します (`network-config` 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-config` または `cisconet.cfg` のどちらが先に読み込まれたかに応じて、`hostname-config` 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-config`、`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-config` ファイルを読み込みます。スイッチが `router-config` ファイルを読み込めない場合は、`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。DHCP 応答から TFTP サーバを入手できなかった場合、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、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

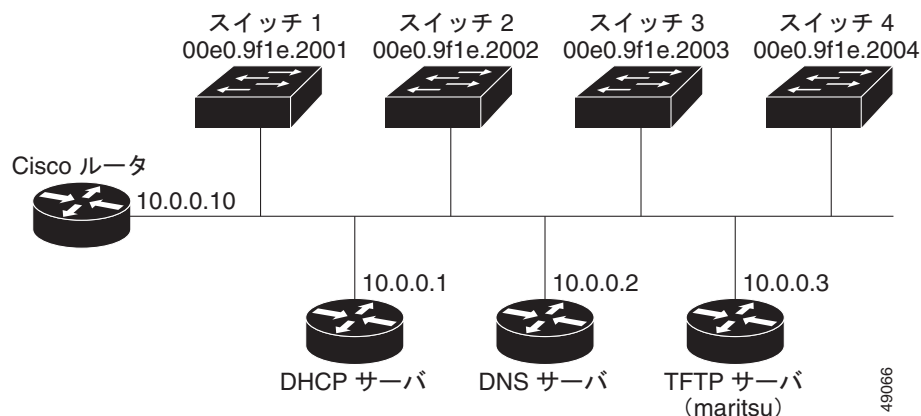


表 3-2 に、DHCP サーバ、またはスイッチ上で実行される DHCP サーバ機能の専用のリースのコンフィギュレーションを示します。

表 3-2 DHCP サーバの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	<i>maritsu</i> または <i>10.0.0.3</i>	<i>maritsu</i> または <i>10.0.0.3</i>	<i>maritsu</i> または <i>10.0.0.3</i>	<i>maritsu</i> または <i>10.0.0.3</i>
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-config	switch2-config	switch3-config	switch4-config
ホスト名 (任意)	switch 1	switch 2	switch 3	switch 4

DNS サーバ コンフィギュレーション

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-config` 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-config`、`switch2-config` など) も含まれています。

```
prompt> cd /tftpserver/work/
prompt> ls
network-config
switch1-config
switch2-config
switch3-config
switch4-config
prompt> cat network-config
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-config` 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-config` 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-config* 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」(P.3-9)
- 「実行コンフィギュレーション設定の確認」(P.3-10)
- 「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)
- 「NVRAM での設定の確認」(P.3-11)
- 「デフォルト ゲートウェイの設定」(P.3-11)
- 「スタティック ルートの設定」(P.3-12)

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** 設定値を保存します（「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

次のコマンドで、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 <i>IP-address</i>	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 Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 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 <i>dest_IP_address mask {forwarding_IP vlan vlan_ID}</i>	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。

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# **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#

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制御

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)
- 「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。

コマンド	目的
Switch(config)# enable password <i>password</i>	特権 EXEC モード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。

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せん。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 <i>level</i>] { <i>password</i> <i>encryption-type</i> <i>encrypted-password</i> }	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 <i>level</i>] { <i>password</i> <i>encryption-type</i> <i>encrypted-password</i> }	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 コマンドの両方を設定した場合は、イネーブル シークレットパスワードを入力する必要があります)。

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、その特権レベルにアクセスする必要があるユーザだけに、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。

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。

Terminal Access Controller Access Control System Plus (TACACS+) によるスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus (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、詳細なアカウント情報収集、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication、Authorization、Accounting (AAA; 認証、認可、アカウント管理) を通じて機能し、AAA コマンドによってだけイネーブルにできます。



(注)

この章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。

ここで説明する設定内容は次のとおりです。

- 「[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)

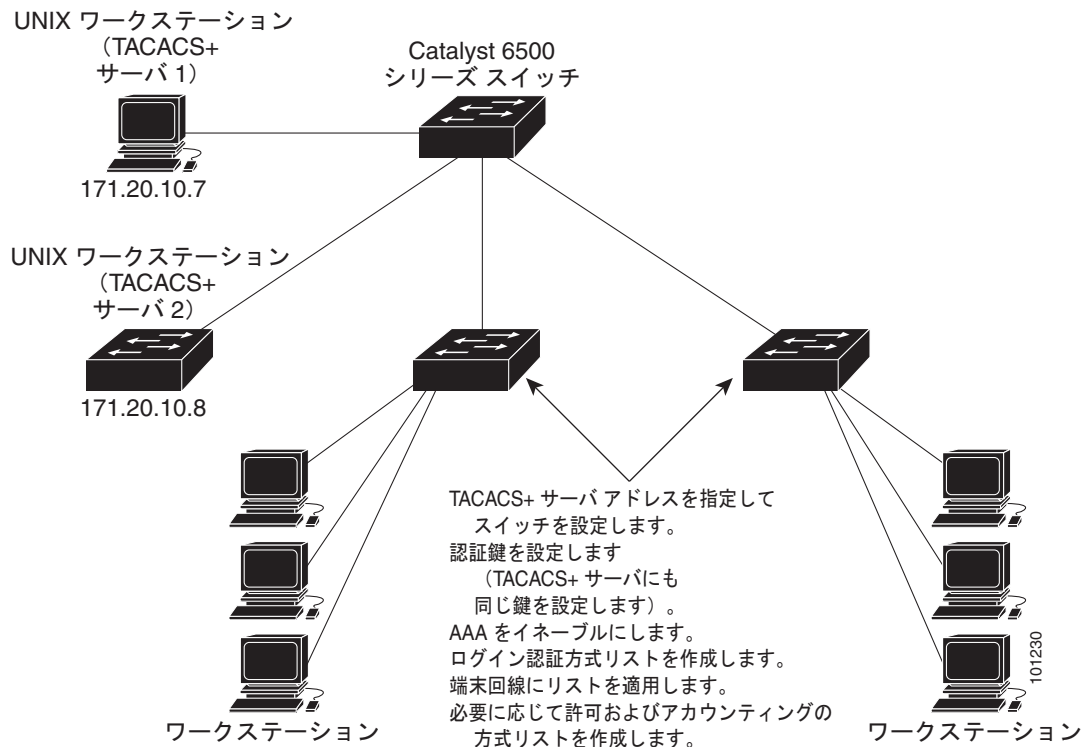
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの評価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動する TACACS+ デーモンのデータベースで維持されます。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、単一のアクセス制御サーバ (TACACS+ デーモン) が各サービス (認証、認可、アカウントिंग) を個別に提供します。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、単一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、他のシスコ ルータおよびアクセス 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、単一のユーザ、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、メッセージング サポートによって認証をフル制御します。

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あと、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを確認します)。TACACS+ 認証サービスにより、ユーザ画面にメッセージを表示することもできます。たとえば、会社のパスワード有効期間ポリシーにより、パスワードを変更する必要があることをユーザに通知します。

- 認可：自動コマンド、アクセス制御、セッション期間、またはプロトコルサポートの設定を含む（ただし、これらに限定されない）ユーザ機能をユーザセッション期間内で厳しく制限します。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アクティビティを追跡したり、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 [ポイントツーポイントプロトコル] など）、パケット数、バイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間の認証を行います。スイッチと TACACS+ デーモンの間のプロトコル交換はすべて暗号化されるため、機密は保持されます。

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動するシステムが必要です。

TACACS+ の動作

ユーザが TACACS+ を使用してスイッチを認証することで、簡易 ASCII ログインを試行すると、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。スイッチがパスワードプロンプトを表示し、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受信します。
 - ACCEPT：ユーザが認証され、サービスを開始できます。認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、この時点で認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求められます。
 - ERROR：デーモンを使用した認証のある時点で、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 応答を受信した場合、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、スイッチで許可機能がイネーブルになっている場合、ユーザは追加の認可フェーズに入ります。ユーザは TACACS+ 認可に進む前にまず、TACACS+ 認証を正常に終了する必要があります。

3. TACACS+ 認可が必要な場合、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、その応答にユーザおよびサービスの EXEC または NETWORK セッションを指示するデータが属性の形式で含まれており、ユーザがアクセスできるサービスが決まります。
 - 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、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スイッチを設定する方法を説明します。少なくとも、TACACS+ デーモンを維持するホストを特定し、TACACS+ 認証の方式リストを定義する必要があります。さらに、任意で TACACS+ 認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、認可、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、リストされた最初の方式を使用してユーザの認証、認可、およびアカウントの記録を行います。その方式が応答しない場合、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、方式リストをすべて試行し終わるまで続きます。

ここで説明する設定内容は次のとおりです。

- 「TACACS+ のデフォルト設定」(P.3-18)
- 「TACACS+ サーバ ホストの特定と認証キーの設定」(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+ 認可の設定」(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+ と AAA は、デフォルトではディセーブルです。

セキュリティ上の理由により、ネットワーク管理アプリケーションを使用して TACACS+ を設定できません。イネーブルに設定されている場合、TACACS+ は Command Line Interface (CLI; コマンドライン インターフェイス) を介し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 を介して実行しますが、TACACS+ サーバは特権レベル 15 に設定された Hypertext Transfer Protocol (HTTP; ハイパーテキスト トランスファ プロトコル) 接続を認証します。

TACACS+ サーバ ホストの特定と認証キーの設定

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れら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 リストと一緒に使用され、選択したサーバ ホストの IP アドレスのリストを含んでいます。

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 モードを開始して次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>tacacs-server host hostname [port integer] [timeout integer] [key string]</code>	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力すると、優先ホストのリストを作成できます。ソフトウェアは、指定された順序でホストを検索します。 <ul style="list-style-type: none"> • <i>hostname</i> には、ホスト名または 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単位で指定します。この時間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+ デーモンの間のすべてのトラフィックを暗号化および復号化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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa group server tacacs+ group-name</code>	(任意) グループ名で AAA サーバグループを定義します。 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	<code>server ip-address</code>	(任意) 特定の TACACS+ サーバを定義済みサーバグループに関連付けます。AAA サーバグループの各 TACACS+ サーバに対してこの手順を繰り返します。 グループの各サーバは、ステップ 2 で事前に定義する必要があります。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show tacacs</code>	入力を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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。設定リストからサーバグループを削除するには、**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 (*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、明示的に定義された名前付き方式リストを持つポート以外の、すべてのポートに自動的に適用されます。定義された方式リストは、デフォルトの方式リストを上書きします。

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、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内の次の認証方式を選択します。このプ

■ 特権 EXEC コマンドへのアクセス制御

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、定義された方式を使い果たすまで続きます。このサイクル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、それ以上他の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 モードを開始して次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • <code>login authentication</code> 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。 • <code>list-name</code> には、作成するリストの名前に使用する文字列を指定します。 • <code>method1...</code> 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戻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。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • 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前に、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 パスワードを定義する必要があります。 • group tacacs+ : TACACS+ 認証を使用します。この認証方式を使用する前に、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 ホストの特定と認証キーの設定」(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前に、回線パスワードを設定しておく必要があります。それには、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する必要があります。それには、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たローカル ユーザ名データベースを認証に使用します。それには、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	<code>line [console tty vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。

	コマンド	目的
ステップ5	<code>login authentication {default list-name}</code>	回線または回線セットに、認証リストを適用します。 <ul style="list-style-type: none"> default を指定する場合、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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ7	<code>show running-config</code>	入力を確認します。
ステップ8	<code>copy running-config startup-config</code>	(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。ログインの TACACS+ 認証をディセーブルにする、また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+ 認可の設定

AAA 認可によってユーザが利用できるサービスが制限されます。AAA 認可がイネーブルである場合、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、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。

tacacs+ キーワードを指定して **aaa authorization** グローバル コンフィギュレーション コマンドを使用すると、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、次の認可パラメータを設定します。

- 認証に TACACS+ を使用した場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 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) 認可が設定されていても、CLI を介してログインし、認証されたユーザに対しては、認可は省略されません。

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+ 認可を指定するには、特権 EXEC モードを開始して、次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	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	<code>aaa authorization network tacacs+</code>	ネットワーク 関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ3	<code>aaa authorization exec tacacs+</code>	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 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) が返されることがあります。
ステップ4	<code>end</code>	特権 EXEC モードに戻ります。

■ 特権 EXEC コマンドへのアクセス制御

	コマンド	目的
ステップ 5	<code>show running-config</code>	入力を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

認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 リソース量を追跡します。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アクティビティをアカウンティング レコード形式で 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 レコードは、アカウンティングの AV のペアを含み、セキュリティ サーバに保存されます。このデータは、ネットワーク管理、クライアントへの課金、または監査用に分析できます。

各 Cisco IOS 特権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 モードを開始して、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>aaa accounting network start-stop tacacs+</code>	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	<code>aaa accounting exec start-stop tacacs+</code>	TACACS+ アカウンティングをイネーブルにして、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します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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）ことができるため、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 ファイル内でのパスワード読み取りを不可能にできます。

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。

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時、またはパスワードが設定される時に行われます。パスワードの暗号化は、認証キー パスワード、イネーブル 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 Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) 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、認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構成され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と、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。

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。

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。

コマンド	目的
Switch# disable level	特定の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.3-26) 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は、次の作業を行い回復します。

-
- 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** キーを押した状態で **C** キーを押して、ブートシーケンスを停止し、Read Only Memory (ROM; リードオンリーメモリ) 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** システムを再起動します。
 - 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、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** システムを再起動します。
-

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](#)」(P.3-26)

- ・ 「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.3-26)
- ・ 「スタートアップ システム イメージの指定」 (P.3-30)
- ・ 「環境変数の制御」 (P.3-32)

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 エンジンのブート プロセスには、2つのソフトウェア イメージが関与します。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 コマンドの実行」 (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.3-30) 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、「Switch#」 (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** キーを押した状態で **C** キーを押しても、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** キーを押した状態で **C** キー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** キーを押した状態で **C** キー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 4006 switch with Supervisor Engine III 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

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)

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 (続き)

ブートフィールド	意味
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 コマンドの実行

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)

システムおよびスベ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 レジスタ設定値を確認します。
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 設定値を保存します

「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限り、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** システムを再起動します。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。

コマンド	目的
Switch# show version	コンフィギュレーション レジスタ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 Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Experimental
Version 12.1(20010828:211314) [cisco 105]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 06-Sep-01 15:40 by
Image text-base:0x00000000, data-base:0x00ADF444

ROM:1.15
Switch uptime is 10 minutes
System returned to ROM by reload
Running default software

cisco Catalyst 4000 (MPC8240) processor (revision 3) with 262144K bytes
of memory.
Processor board ID Ask SN 12345
Last reset from Reload
Bridging software.
49 FastEthernet/IEEE 802.3 interface(s)
20 Gigabit Ethernet/IEEE 802.3 interface(s)
271K bytes of non-volatile configuration memory.

Configuration register is 0xEC60

Switch#
```

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ためのバックアップ手段を得ることができます。

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」でも説明しています。

以下の項目に従って、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 **Remote Copy Protocol (RCP; リモート コピー プロトコル)** 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)
- TFTP によるシステム 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 によるフラッシュ 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 メモリの詳細については、

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/OL_2788.html を参照してください。

セキュリティ上の注意

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 レベルからに限られます。

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もあります。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 コマンドの実行」(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 環境変数の詳しい設定手順については、『*Configuration Fundamentals Configuration Guide*』の「Loading and Maintaining System Images and Microcode」の章にある「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
  PSl=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 コマンドにより設定されたデフォルト パラメータの詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』の **erase** コマンドの使用上の注意事項を参照してください。

■ スイッチの出荷時のデフォルト設定へのリセット