基本ファイル転送サービスの設定

基本ファイル転送サービスを使用すると、ルータを簡易ファイル転送プロトコル（TFTP）または逆アドレス解決プロトコル（RARP）サーバーとして設定、そのルータが拡張 BOOTP 要求を非同期インターフェイス経由で転送するよう設定、および rcp、rsh、FTP を設定することが可能です。

基本ファイル転送サービスの前提条件

- ユーザーには、少なくとも Cisco IOS 環境とコマンドライン インターフェイスに関する基本的な知識が必要です。
- システムでは、少なくとも最小限の設定が実行されていることが必要です。

基本ファイル転送サービスに関する制約事項

- ネットワークが稼働していて、Cisco IOS リリース 12.2 以降のリリースがすでにインストールされている必要があります。
- Cisco IOS コンフィギュレーション コマンドのいくつかは、特定のルータ プラットフォームでのみ使用可能であり、コマンド構文はプラットフォームによって異なる可能性があります。

基本ファイル転送サービスに関する情報

TFTP または RARP サーバーとしてのルータの使用

サーバーとしてだけ機能するマシンをネットワークの各セグメントに配置するのは、コストがかかり、非効率的です。しかし、すべてのセグメントにサーバーがあるのではない場合、ネットワーク セグメントを超えたネットワークの操作によって相当の遅延が引き起こされることがあります。ルータを RARP または TFTP サーバーとして機能するよう設定することで、ルータの通常の機能を使用しながらコストと遅延時間を削減できます。

多くの場合、TFTP または RARP サーバーとして設定されたルータは、フラッシュ メモリから他のルータにシステム イメージまたはルータ コンフィギュレーション ファイルを提供します。リクエストのような他のタイプのサービス要求に応答するよう、ルータを設定することもできます。

TFTP サーバーとしてのルータの使用

TFTP サーバー ホストとして、ルータは TFTP 読み取り要求メッセージに応答し、ROM に含まれるシステム イメージのコピー、またはフラッシュ メモリに含まれるシステム イメージの 1 つを、要求したホストに送出します。TFTP 読み取り要求メッセージは、コンフィギュレーションで指定されたファイル名のいずれかを使用する必要があります。

（注） Cisco 7000 ファミリでは、使用されるファイル名はフラッシュ メモリ内に存在するソフトウェア イメージを表している必要があります。フラッシュ メモリ内にイメージが存在しない場合、クライアント ルータはデフォルトとしてサーバーの ROM イメージをブートします。

フラッシュ メモリは、ネットワーク内の他のネットワークの TFTP ファイル サーバーとして使用できます。この機能により、リモートのルータをフラッシュ サーバー メモリ内に存在するイメージを使用してブートすることが可能になります。

シスコ デバイスの中には、TFTP サーバーとして、さまざまなフラッシュ メモリ位置（**bootflash:**、**slot0:**、**slot1:**、**slavebootflash:**、**slaveslot0:**、または **slaveslot1:**）から 1 つを選択できるものもあります。

RARP サーバーとしてのルータの使用

逆アドレス解決プロトコル（RARP）は、MAC（物理）アドレスをもとに IP アドレスを検索する方法をそなえた、TCP/IP スタックのプロトコルです。ブロードキャスト Address Resolution Protocol（ARP）の逆であるこの機能により、ネットワーク層の特定の IP アドレスに対応する MAC レイヤ アドレスをホストが動的に検出できます。RARP はさまざまなシステムをディスクなしで起動させることを可能にします（たとえば、クライアントとサーバーが別のサブネットにあるネットワークの Sun ワークステーションや PC のように、起動時点では IP アドレスが

わからないディスクレス ワークステーション）。RARP は、MAC レイヤから IP アドレスへのマッピングのキャッシュされたエントリの表を持つRARPサーバーの存在に依存しています。

Cisco ルータは RARP サーバーとして設定できます。この機能で、Cisco IOS ソフトウェアは RARP 要求に応答することができます。

Rsh および rcp 用ルータの使用

リモート シェル（rsh）により、コマンドをリモートで実行できるようになります。リモート コピー（RCP）を使用すると、ユーザーはネットワーク上のリモート ホストやサーバーに存在するファイル システムへのファイル コピーや、ファイル システムからのコピーが行えます。シスコの rsh および rcp の実装は、業界標準の実装と相互運用できます。シスコでは、rsh と rcpの両方を示すために、省略形 RCMD（Remote Command、リモート コマンド）を使用します。

RCMD 送信の発信元インターフェイス

RCMD（rsh と rcp）通信の発信元インターフェイスを指定できます。たとえば、RCMD接続でループバック インターフェイスをルータから送信されるすべてのパケットの送信元アドレスとして使用するように、ルータを設定できます。source-interface を指定するのは、ループバック インターフェイスの指定に最も一般的に使用される方法です。これにより、RCMD通信にパーマネント IP アドレスを関連付けることができます。パーマネント IP アドレスを持つことは、セッションの識別に役立ちます（リモートデバイスがセッションの間パケットの送信元を一貫して識別できます）。「既知の」IPアドレスも、アドレスを含めてリモートデバイスにアクセス リストを作成できるよう、セキュリティの目的で使用できます。

RCMD の DNS 逆引き参照について

基本的なセキュリティ チェックとして、Cisco IOS ソフトウェアでは、リモート コマンド（RCMD）アプリケーション（rsh および rcp）の DNS を使用してクライアント IP アドレスの逆引き参照を実行します。このチェックは、ホスト認証プロセスを使用して実行されます。

イネーブルにされている場合、システムは要求元のクライアントのアドレスを記録します。アドレスは、DNS を使用してホスト名にマッピングされます。次に、そのホスト名の IP アドレスに対する DNS リクエストが行われます。受け取った IP アドレスが、元の要求元アドレスと照合されます。そのアドレスが、DNS から受信したアドレスのいずれにも一致しない場合、RCMD 要求は処理されません。

この逆引き参照は、「スプーフィング」に対する保護を促進するためのものです。ただし、このプロセスでは当該 IP アドレスが有効かつルーティング可能なアドレスであることを確認するのみであり、ハッカーは引き続き既知のホストの有効な IP アドレスをスプーフィングできるということに注意してください。

rsh の導入

rsh（リモート シェル）を使用すると、アクセス可能なリモート システム上でコマンドを実行できます。**rsh** コマンドを発行すると、リモート システム上でシェルが起動します。シェルに

より、ターゲット ホストにログインすることなくリモート システム上でコマンドを実行できます。

そのシステムへの接続、ルータ、アクセス サーバー、さらにコマンド実行後の切断も、rsh を使えば必要ありません。たとえば、rsh を使用すれば、ターゲット デバイスへの接続やコマンドの実行、切断といった手順なしに、リモートで他のデバイスのステータスを見ることができます。この機能は、多数の異なるルータの統計情報を見る場合に役立ちます。rsh を有効化するコンフィギュレーション コマンドは、「remote command（リモート コマンド）」の略語である「rcmd」を使用します。

rsh セキュリティの維持

rshが動作しているリモートシステム（UNIXホストなど）にアクセスするためには、そのユーザーがリモートからそのシステムでコマンドを実行する権限を与えられていることを示すエントリが、システムの *.rhosts* ファイルまたはそれに相当するものに存在している必要があります。UNIX システムでは、*.rhosts* ファイルはシステムのコマンドをリモートで実行できるユーザーを特定します。

ルータ上の rsh サポートを有効化すると、リモート システム上のユーザーがコマンドを実行できるようになります。しかし、シスコの rsh の実装は、*.rhosts* ファイルをサポートしていません。その代わりに、rshを使用してリモートでコマンドを実行しようとするユーザーによるルータへのアクセスを制御するため、ローカルの認証データベースを設定する必要があります。ローカルの認証データベースは、UNIX *.rhosts* ファイルに似ています。認証データベースで設定する各エントリでは、ローカル ユーザー、リモート ホスト、およびリモート ユーザーを特定します。

rcp の導入

リモート コピー（rcp）コマンドは、リモート システムの rsh サーバー（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ーを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバーへのアクセスだけです（ほとんどの UNIX システムが rsh をサポートしています）。ある場所から別の場所にファイルをコピーするため、コピー元のファイルに対する読み取り権限とコピー先のディレクトリに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、rcp により作成されます。

シスコの rcp 実装は UNIX の rcp 実装（ネットワーク上のシステム間でファイルをコピー）の関数をエミュレートしたものですが、シスコのコマンド構文は UNIX の rcp コマンド構文とは異なります。Cisco IOS ソフトウェアには、rcpをトランスポートメカニズムとして使用する一群のコピー コマンドがあります。これらの rcp コピー コマンドは Cisco IOS TFTP コピー コマンドと類似していますが、より高速なパフォーマンスと信頼性の高いデータ配信を可能にする代替案になっています。このような改善が可能なのは、rcp トランスポート メカニズムが組み込まれており、Transmission Control Protocol/Internet Protocol（TCP/IP）スタックを使用しているためです。rcp コマンドを使用して、ルータからネットワークサーバー（またはその逆）へシステム イメージおよびコンフィギュレーション ファイルをコピーできます。

また、rcp サポートをイネーブルにすることで、リモート システムのユーザーによるルータへの、またはルータからのファイル コピーを許可できます。

/user キーワードおよび引数を指定しない場合、Cisco IOS ソフトウェアはデフォルトのリモートユーザー名を送信します。リモートユーザー名のデフォルト値として、現在の TTY プロセスと関連付けられたリモートユーザー名が有効である場合、ソフトウェアはそのユーザー名を送信します。TTY リモート ユーザー名が無効な場合、ソフトウェアはリモートとローカルのユーザー名の両方にルータのホスト名を使用します。

rcp 要求の送信側リモート クライアントの設定

rcp プロトコルでは、クライアントは rcp 要求ごとにリモート ユーザー名をサーバーに送信する必要があります。rcp を使用してコンフィギュレーション ファイルをサーバーからルータへコピーする場合、Cisco IOS ソフトウェアは次のリストから、最初の有効なユーザー名を送信します。

1. **ip rcmd remote-username** コマンドで設定されたユーザー名（このコマンドが設定されている場合）。
2. 現在の TTY（端末）プロセスに関連付けられているリモートユーザー名。たとえば、ユーザーが Telnet を介してルータに接続されており、**username** コマンドを介して認証された場合は、リモート ユーザー名として Telnet ユーザー名がルータ ソフトウェアによって送信されます。

（注） シスコ製品では、TTY がサーバーへのアクセスに広く使用されています。TTY の概念は、UNIX に由来します。UNIX システムでは、各物理デバイスがファイル システムで表現されます。端末は *tty* デバイスと呼ばれます（tty は、UNIX 端末の *teletype* が元になった省略形です）。

1. ルータのホスト名。

rcp を使用した **boot** コマンドで、ソフトウェアはルータ ホスト名を送信します。リモートユーザー名の明示的な設定はできません。

rcp コピー要求が正常に実行されるためには、ネットワーク サーバー上でリモート ユーザー名のアカウントが定義されている必要があります。

サーバーに書き込む場合、ルータ上のユーザーからの rcp 書き込み要求を受け入れるように、rcp サーバーを適切に設定する必要があります。UNIX システムの場合は、rcp サーバー上のリモートユーザーの *.rhosts* ファイルに対しエントリを追加する必要があります。たとえば、ルータに次の設定行が含まれているとします。

```
hostname Rtr1
ip rcmd remote-username User0
```

そのルータの IP アドレスを Router1.company.com と変換するとすれば、rcp サーバーの User0 の *.rhosts* ファイルは、次の行を含んでいる必要があります。

```
Router1.company.com Rtr1
```

詳細については、ご使用の RCP サーバーのマニュアルを参照してください。

このサーバーがディレクトリ構造をとっている場合、コンフィギュレーションファイルまたはイメージは、サーバー上のリモートユーザー名と関連付けられたディレクトリに関連して書き込まれるか、そのディレクトリからコピーされます。サーバー上で使用するディレクトリを指定するには、**iprcmdremote-username** コマンドを使用します。たとえば、システムイメージがサーバー上のあるユーザーのホーム ディレクトリに存在する場合、そのユーザーの名前をリモート ユーザー名として指定します。

ファイル サーバーとして使用されているパーソナル コンピュータにコンフィギュレーションファイルをコピーする場合、このコンピュータではrshがサポートされている必要があります。

FTP 接続用ルータの使用

ネットワーク上のシステム間で File Transfer Protocol（FTP）を使用してファイルを転送するよう、ルータを設定できます。Cisco IOS に実装された FTP により、次の FTP 特性を設定できます。

- パッシブ モード FTP
- ユーザー名
- パスワード
- IP アドレス

基本ファイル転送サービスの設定方法

TFTP サーバーとしてのルータの使用の設定

ルータが TFTP サーバーとして使用されるよう設定するには、このセクションのタスクを実行します。

始める前に

TFTP 機能の実装前に、サーバーとクライアント ルータは互いに到達可能である必要があります。**ping***a.b.c.d* コマンドを使用して（*a.b.c.d* はクライアント デバイスのアドレス）サーバーとクライアント ルータとの接続をテストし（いずれかの方向で）、この接続を確認します。**ping** コマンドが発行されると、接続されたことが、一連の感嘆符（!）によって表示されます。接続に失敗した場合は、一連のピリオド（.）に加えて [timed out] または [failed] が表示されます。接続に失敗し、インターフェイスを再設定する場合は、フラッシュ サーバーとクライアント ルータとの間の物理的な接続をチェックし、ping を再実行します。

接続をチェックした後、TFTPブート可能イメージがサーバー上に存在することを確認します。これは、クライアント ルータがブートするシステム ソフトウェア イメージです。最初のクライアント ブートの後で確認できるように、そのソフトウェア イメージの名前を記録しておきます。

⚠

注意 すべての機能を使用するために、クライアントに送信されるソフトウェアイメージは、クライアントルータにインストールされたROMソフトウェアと同一のタイプのものである必要があります。たとえば、サーバーにはX.25ソフトウェアがあり、クライアントのROMにはX.25ソフトウェアがない場合、フラッシュメモリ内にあるサーバーのイメージからブートしてからも、クライアントにはX.25の機能がありません。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **tftp-server flash** [*partition-number*:]*filename1* [**alias***filename2*] [*access-list-number*]
   - **tftp-server flash** *device* **:** *filename*（Cisco 7000 ファミリのみ）
   - **tftp-server flash** [*device*:][*partition-number*:]*filename* （Cisco 1600 シリーズと Cisco 3600 シリーズのみ）
   - **tftp-server rom alias** *filename1* [*access-list-number*]
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	次のいずれかを実行します。 • **tftp-server flash** [*partition-number*:]*filename1* [**alias***filename2*] [*access-list-number*] • **tftp-server flash** *device* **:** *filename*（Cisco 7000 ファミリのみ） • **tftp-server flash** [*device*:][*partition-number*:]*filename* （Cisco 1600 シリーズと Cisco 3600 シリーズのみ） • **tftp-server rom alias** *filename1* [*access-list-number*]	読み取り要求の応答として送信されるシステム イメージを指定します。複数行を入力して複数のイメージを指定することができます。

	コマンドまたはアクション	目的
	例： `Device(config)# tftp-server flash version-10.3 22`	
ステップ 4	**end** 例： `Device(config)# end`	コンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

例

次の例では、フラッシュ メモリ ファイル *version-10.3* の TFTP 読み取りリクエストへの応答として、システムは TFTP を使用してこのファイルのコピーを送信できます。要求送出ホストはアクセス リスト 22 でチェックされます。

```
tftp-server flash version-10.3 22
```

次の例では、ROM イメージ *gs3-k.101* ファイルについての TFTP 読み取り要求への応答として、システムは TFTP を使用して *gs3-k.101* ファイルのコピーを送信できます。

```
tftp-server rom alias gs3-k.101
```

次の例では、TFTP 読み取り要求への応答として、ルータがフラッシュ メモリ内のファイル *gs7-k.9.17* のコピーを送信します。クライアント ルータはアクセス リスト 1 で指定されたネットワーク内に存在している必要があります。したがって、この例では、ネットワーク 172.16.101.0 にあるすべてのクライアントがファイルへのアクセスを許可されます。

```
Server# configure terminal

Enter configuration commands, one per line. End with CTRL/Z
Server(config)# tftp-server flash gs7-k.9.17 1

Server(config)# access-list 1 permit 172.16.101.0 0.0.0.255

Server(config)# end

Server# copy running-config startup-config

[ok]
Server#
```

トラブルシューティング

TFTP セッションには障害が発生することがあります。TFTP は TFTP セッション障害の原因判別のために、次の特別な文字を生成します。

- 文字「E」は、TFTP サーバーがエラーを含むパケットを受信したことを示します。
- 文字「O」は、TFTP サーバーがシーケンスに合わないパケットを受信したことを示します。
- ピリオド（.）はタイムアウトを示します。

転送中の不適当な遅延を診断するために、この出力が役立ちます。トラブルシューティングの手順については、マニュアル『*Internetwork Troubleshooting Guide*』を参照してください。

クライアント ルータの設定

最初にサーバーからシステムイメージをロードし、次にバックアップとして、サーバーからのロードに失敗した場合に自身の ROM イメージをロードするようクライアント ルータを設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no boot system**
4. **boot system** [**tftp**] *filename* [*ip-address*]
5. **boot system rom**
6. **config-register** *value*
7. **end**
8. **copy running-config startup-config**
9. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**no boot system** 例： `Device(config)# no boot system`	（任意）これまでの **bootsystem** 文をすべてコンフィギュレーション ファイルから削除します。
ステップ 4	**boot system** [**tftp**] *filename* [*ip-address*] 例： `Device(config)# boot system c5300-js-mz.121-5.T.bin 172.16.1.1`	クライアントルータがサーバーからシステムイメージをロードするよう指定します。
ステップ 5	**boot system rom** 例： `Device(config)# boot system rom`	クライアントルータがサーバーからのロードに失敗した場合に、自身の ROM イメージをロードするように指定します。
ステップ 6	**config-register** *value* 例： `Device(config)# config-register 0x010F`	クライアント ルータがネットワーク サーバーからシステム イメージをロードできるよう、コンフィギュレーション レジスタを設定します。
ステップ 7	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルをスタートアップコンフィギュレーションに保存します。
ステップ 9	**reload** 例： `Device# reload`	（任意）変更を有効にするため、ルータをリロードします。

例

次の例では、ルータは指定の TFTP サーバーからブートするよう設定されます。

```
Client# configure terminal

Enter configuration commands, one per line. End with CTRL/Z
Client(config)# no boot system

Client(config)# boot system c5300-js-mz.121-5.T.bin 172.16.1.1
```

```
Client(config)# boot system rom

Client(config)# config-register 0x010F

Client(config)# end

Client# copy running-config startup-config

[ok]
Client# reload
```

この例では、**nobootsystem** コマンドによって、現在コンフィギュレーション メモリ内にある他の **bootsystem** コマンドがすべて無効化され、このコマンドの後に入力される **bootsystem** コマンドが先に実行されるようになります。2 番目のコマンドである **bootsystem***filename address* は、クライアント ルータに対し、IP アドレスが 172.16.111.111 の TFTP サーバーにあるファイル c5300-js-mz.121-5.T.bin を探すよう指示しています。これが失敗した場合、クライアント ルータは、ネットワーク障害が生じた場合のバックアップとして含まれている **bootsystemrom** コマンドに応答して、自身のシステム ROM からブートします。**copyrunning-configstartup-config** コマンドは、コンフィギュレーションをスタートアップ コンフィギュレーションへコピーし、**reload** コマンドがシステムをブートします。

（注） サーバーからブートするためのシステム ソフトウェアは、サーバーのフラッシュ メモリ内に存在している必要があります。フラッシュ メモリにない場合、クライアント ルータはサーバーのシステム ROM からブートします。

次の例に、ルータの再起動後に **showversion** コマンドを実行した場合の出力例を示します。

```
Device> show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) 5300 Software (C5300-JS-M), Version 12.1(5)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Sat 11-Nov-00 03:03 by joe
Image text-base: 0x60008958, data-base: 0x611C6000
ROM: System Bootstrap, Version 11.2(9)XA, RELEASE SOFTWARE (fc2)
BOOTFLASH: 5300 Software (C5300-BOOT-M), Version 12.0(7)T,  RELEASE SOFTWARE (f)
Router uptime is 8 weeks, 4 days, 22 hours, 36 minutes
System returned to ROM by power-on
System restarted at 00:37:38 UTC Thu Feb 22 2001
System image file is "flash:c5300-js-mz.121-5.T.bin"
.
.
.
Configuration register is 0x010F
```

この例の重要情報は、最初の行の「Cisco IOS (tm)..」と「System image file....」で始まる行とに含まれています。「Cisco IOS (tm)...」という行では、NVRAM のオペレーティングシステムのバージョンが表示されています。「System image file....」という行は、TFTP サーバからロードされたシステム イメージのファイル名を表示しています。

次の作業

システムをリロードしたら、**showversion** EXEC モードコマンドを使用して、目的とするイメージでシステムがブートしたことを確認する必要があります。

⚠

注意 次の例にあるとおり、**nobootsystem** コマンドを使用すると、現在クライアント ルータのシステム コンフィギュレーションにある他のブート システム コマンドがすべて無効化されます。次に進む前に、バックアップ コピーの目的でクライアント ルータに格納されたシステム コンフィギュレーションを先に TFTP ファイル サーバーに保存するか（アップロードするか）を決定します。

RARP サーバーとしてのルータの設定

ルータを RARP サーバーに設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type* [*slot*/]*port*
4. **ip rarp-server** *ip-address*

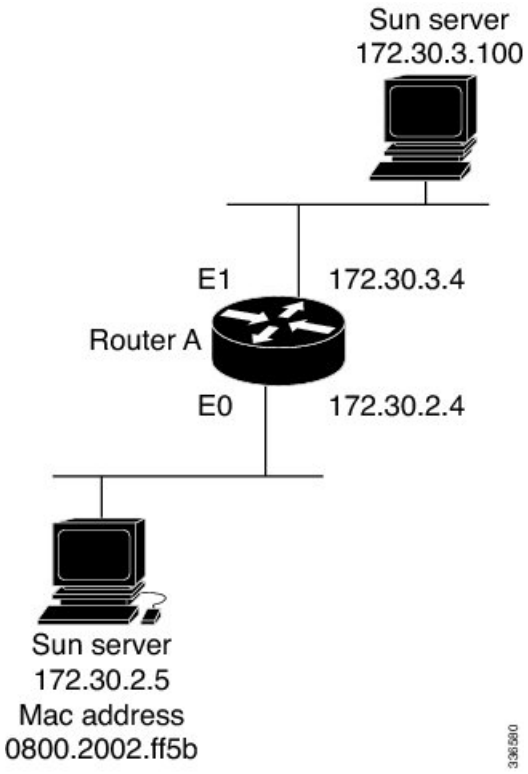
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** *type* [*slot*/]*port* 例： `Device(config)# interface Gigabitethernet 0/0`	RARP サービスを設定するインターフェイスを指定し、指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip rarp-server** *ip-address* 例： `Device(config-if)# ip rarp-server 172.30.3.100`	ルータの RARP サービスを有効化します。

例

以下の図は、ルータがディスクレス ワークステーションの RARP サーバーとして機能するネットワークの設定を示しています。この例では、Sun ワークステーションは自身の MAC（ハードウェア）アドレスを IP アドレスに解決するために SLARP 要求を送信し、要求はルータによって Sun サーバーへ転送されます。

図 *1 : RARP* サーバーとしてのルータの設定



ルータ A は次のように設定されています。

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface Gigabitethernet 0/0
! Configure the router to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100
```

Sun のクライアントとサーバーの IP アドレスには、現在の SunOS デーモン *rpc.bootparamd* での制限により、同じメジャー ネットワーク番号を使用する必要があります。

次の例では、アクセス サーバーが RARP サーバーとして機能するよう設定されています。

```
! Allow the access server to forward broadcast portmapper requests
 ip forward-protocol udp 111
! Provide the access server with the IP address of the diskless sun
 arp 172.30.2.5 0800.2002.ff5b arpa
 interface Gigabitethernet 0/0
! Configure the access server to act as a RARP server, using the Sun Server's
! IP address in the RARP response packet.
 ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
 ip helper-address 172.30.3.100
```

rsh および rcp を使用するためのルータの設定

RCMD 送信での送信元インターフェイスの指定

RCMD 接続でルータから送信されるすべてのパケットの送信元アドレスとしてループバック インターフェイスを使用するようにルータを設定するには、このセクションのタスクを実行することにより、RCMD 通信に関連付けられているインターフェイスを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd source-interface** *interface-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip rcmd source-interface** *interface-id* 例： `Device(config)# ip rcmd source-interface`	rsh と rcp のすべての送信トラフィックにラベル付けするために使用するインターフェイス アドレスを指定します。

RCMD の DNS 逆引き参照の無効化

rcmd の DNS 逆引き参照はデフォルトで有効化されています。このセクションのタスクを実行することにより、RCMD（rsh および rcp）アクセスの DNS チェックを無効化できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip rcmd domain-lookup**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**no ip rcmd domain-lookup** 例： `Device(config)# no ip rcmd domain-lookup`	リモート コマンド（RCMP）アプリケーション（rsh および rcp）の Domain Name Service（DNS）逆ルックアップ機能をディセーブルにします。

リモート ユーザーが rsh を使用してコマンドを実行できるようにするためのルータの設定

リモート ユーザーが rsh を使用してコマンドを実行できるようにルータを設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]]
4. **ip rcmd rsh-enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]] 例： `Device(config)# ip rcmd remote-host Router1 172.16.101.101 netadmin4 enable`	ローカル認証データベースで、rsh コマンド実行を許可するリモートユーザーそれぞれにエントリを作成します。
ステップ 4	**ip rcmd rsh-enable** 例： `Device(config)# ip rcmd rsh-enable`	ソフトウェアの受信 rsh コマンドのサポートをイネーブルにします。 （注） ソフトウェアの受信 rsh コマンドのサポートを無効化するには、**noiprcmdrsh-enable** コマンドを使用します。 （注） 受信 rsh コマンドのサポートがディセーブルにされた場合でも、リモート シェル プロトコルをサポートする他のルータおよびネットワーク上の UNIX ホストで実行される rsh コマンドを発行することができます。

例

次に、リモート ユーザーのために 2 つのエントリを認証データベースに追加し、リモート ユーザーからの rsh コマンドをサポートするようルータをイネーブルにする例を示します。

```
ip rcmd remote-host Router1 172.16.101.101 rmtnetad1
ip rcmd remote-host Router1 172.16.101.101 netadmin4 enable
ip rcmd rsh-enable
```

名前が *rmtnetad1* というユーザーと *netadmin4* というユーザーはいずれも、リモート ホストの IP アドレス 172.16.101.101 に存在します。ユーザーはいずれも同じリモート ホスト上にいますが、各ユーザーに対して一意のエントリを含める必要があります。ルータを rsh に対して有効化すると、いずれのユーザーも、そのルータに接続してリモートで rsh コマンドを実行できるようになります。*netadmin4* という名前のユーザーは、ルータ上での特権 EXEC モード コマンドの実行を許可されます。認証データベース上のいずれのエントリも、ローカルのユーザー名として、ルータのホスト名 *Router1* を使用します。最後のコマンドで、リモート ユーザーが発行した rsh コマンドのルータでのサポートを有効化します。

rsh を使用したリモートでのコマンド実行

rshを使用してリモートからネットワーク サーバーでコマンドを実行するには、ユーザーEXEC モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **rsh** {*ip-address* | *host* } [**/user***username*] *remote-command*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**rsh** {*ip-address* | *host* } [**/user***username*] *remote-command* 例： `Device# rsh mysys.cisco.com /user sharon ls -a`	rshを使用してリモートからコマンドを実行します。

例

次の例では、mysys.cisco.com 上で、ユーザー sharon のホーム ディレクトリから rsh を使用して「ls -a」コマンドを実行します。

```
Device# enable
Device# rsh mysys.cisco.com /user sharon ls -a
.
..
.alias
.cshrc
.emacs
.exrc
```

```
.history
.login
.mailrc
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
jazz
Device#
```

リモート ユーザーからの rcp 要求受け入れのためのルータ設定

Cisco IOS ソフトウェアが受信 rcp 要求をサポートするよう設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]]
4. **ip rcmd rcp-enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]] 例： `Device(config)# ip rcmd remote-host Router1 172.16.101.101 netadmin3`	ローカルの認証データベースで、rcp コマンドの実行を許可されているリモートユーザーそれぞれにエントリを作成します。 （注） ソフトウェアの受信 rcp 要求のサポートを無効化するには、**noiprcmdrcp-enable** コマンドを使用します。

	コマンドまたはアクション	目的
		（注） 受信 rcp 要求のサポートをディセーブルにした場合でも、rcp コマンドを使用してリモートサーバーへイメージをコピーできます。受信 rcp 要求のサポートは、発信 rcp 要求を扱う際の機能とは異なっています。
ステップ 4	**ip rcmd rcp-enable** 例： `Device(config)# ip rcmd rcp-enable`	ソフトウェアの受信 rcp 要求のサポートをイネーブルにします。

例

次の例に、認証データベースにリモート ユーザー用の 2 つのエントリを追加してから、ソフトウェアでリモートユーザーからのリモートコピー要求のサポートを有効化する方法を示します。IP アドレス 172.16.15.55 のリモート ホストの *netadmin1* というユーザーと、IP アドレス 172.16.101.101 のリモート ホストの *netadmin3* というユーザーは両方とも、ルータへの接続、およびルータが rcp サポートをイネーブル化した後にリモートから rcp コマンドを実行することを許可されます。認証データベース上のいずれのエントリも、ローカルのユーザー名として、ホスト名 *Router1* を使用します。最後のコマンドで、リモート ユーザーからの rcp 要求のルータでのサポートをイネーブルにします。

```
ip rcmd remote-host Router1 172.16.15.55 netadmin1
ip rcmd remote-host Router1 172.16.101.101 netadmin3
ip rcmd rcp-enable
```

rcp 要求の送信側リモートの設定

rcp 要求で送信されるデフォルトのリモート ユーザー名を上書きするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip rcmd remote-username** *username* 例： `Device(config)# ip rcmd remote-username sharon`	リモート ユーザー名を指定します。 （注） リモート ユーザー名を削除してデフォルト値に戻すには、**noiprcmdremote-username** コマンドを使用します。

FTP 接続使用時のルータ設定

ネットワークのシステム間で File Transfer Protocol（FTP）を使用してファイルを転送するようルータを設定して、このセクションのタスクである FTP 特性の設定を完了するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ftp username** *string*
4. **ip ftp password** [*type*] *password*
5. 次のいずれかを実行します。
   - **ip ftp passive**
   -
   -
   - **no ip ftp passive**
6. **ip ftp source-interface** *interface*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip ftp username** *string* 例： `Device(config)# ip ftp username zorro`	FTP 接続で使用されるユーザー名を指定します。
ステップ 4	**ip ftp password** [*type*] *password* 例： `Device(config)# ip ftp password sword`	FTP 接続で使用されるパスワードを指定します。
ステップ 5	次のいずれかを実行します。 • **ip ftp passive** • • • **no ip ftp passive** 例： `Device(config)# ip ftp passive`	パッシブ モード FTP 接続のみを使用するようルータを設定します。 または すべてのタイプのFTP 接続（デフォルト）を許可します。
ステップ 6	**ip ftp source-interface** *interface* 例： `Device(config)# ip ftp source-interface to1`	FTP 接続の発信元 IP アドレスを指定します。

例

次の例に、Cisco IOS の FTP 機能を使用してコア ダンプを取り込む方法を示します。ルータはログイン名 zorro とパスワード sword により IP アドレス 192.168.10.3 でサーバーにアクセスします。デフォルトのパッシブ モード FTP が使用され、コア ダンプが発生するルータ上のトークン リング インターフェイス to1 を使用してサーバーへのアクセスが行われます。

```
ip ftp username zorro
ip ftp password sword
ip ftp passive
ip ftp source-interface to1
! The following command allows the core-dump code to use FTP rather than TFTP or RCP
exception protocol ftp
```

```
! The following command identifies the FTP server
! 192.168.10.3 crashes
exception dump 192.168.10.3
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。