



基本ファイル転送サービスの設定

このモジュールでは、ルータを Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) または Reverse Address Resolution Protocol (RARP; 逆アドレス解決プロトコル) サーバとして設定する方法、非同期インターフェイスを通して拡張 BOOTP 要求を転送するようルータを設定する方法、および Cisco IOS Release 12.2 での rcp、rsh、FTP の設定方法について説明します。

この章で述べられているファイル転送機能コマンドについて、詳しくは、『[Cisco IOS Configuration Fundamentals Command Reference](#)』を参照してください。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。

基本ファイル転送サービスの設定作業リスト

基本ファイル転送サービスを設定するには、次の項で説明されている作業のいずれかを実行します。

- 「ルータを TFTP または RARP サーバとして設定」
- 「システム BOOTP パラメータの設定」
- 「rsh および rcp 使用時のルータ設定」
- 「FTP 接続使用時のルータ設定」

この章のすべての作業は任意です。

ルータを TFTP または RARP サーバとして設定

サーバ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。



ルータを TFTP サーバに設定

TFTP サーバ 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 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 サーバとしてさまざまなフラッシュ メモリ位置 (**bootflash:**、**slot0:**、**slot1:**、**slavebootflash:**、**slaveslot0:**、**slaveslot1:**) から 1 つを選ぶこともできます。

次の説明では、1 台の Cisco 7000 ルータがフラッシュ サーバと呼ばれ、他のルータはすべてクライアント ルータと呼ばれています。フラッシュ サーバとクライアント ルータのコンフィギュレーション例には、必要なだけのコマンドが含まれています。

TFTP ルータ設定の前提作業

TFTP 機能の実装前に、サーバとクライアント 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 コマンドの発行後、接続可能かどうかが一連の感嘆符 (!) 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、フラッシュ サーバとクライアント 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のイメージからブートした後にクライアントが X.25 の機能を持つようになることはありません。

TFTP サーバのイネーブル化

TFTP サーバの動作をオンにするには、次のコマンドを実行します。特権 EXEC モードで始めます。

	コマンド	目的
ステップ 1	Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Router(config)# tftp-server flash [partition-number:]filename1 [alias filename2] [access-list-number] または Router(config)# tftp-server flash device:filename (Cisco 7000 family only) または Router(config)# tftp-server flash [device:][partition-number:]filename (Cisco 1600 series and Cisco 3600 series only) または Router(config)# 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。
ステップ 3	Router(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 4	Router# 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。

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。

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 を使用してそ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* ファイルに対する 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* のコピーを送信する例です。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 内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
```

■ ルータを TFTP または RARP サーバとして設定

```

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#

```

クライアント ルータの設定作業

最初にサーバからシステム イメージをロードするよう、クライアント ルータを設定します。バックアップとして、サーバ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クライアント ルータを設定します。クライアント ルータを設定するには、次のコマンドを使用します。特権 EXEC モードで始めます。

	コマンド	目的
ステップ1	Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Router(config)# no boot system	(任意) これまでの boot system 文すべてを、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3	Router(config)# boot system [tftp] filename [ip-address]	クライアント ルータがサーバからシステム イメージをロードするよう指定します。
ステップ4	Router(config)# boot system rom	クライアント ルータがサーバ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指定します。
ステップ5	Router(config)# config-register value	クライアント ルータがネットワーク サーバからシステム 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6	Router(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7	Router# 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8	Router# reload	(任意) 変更を有効にするため、ルータをリロードします。

システムをリロードした後、**show version EXEC** モード コマンドを使用して、システムが希望のイメージで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、**no boot system** 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 サーバに保存するか（アップロードするか）を決定します。

次の例では、ルータは指定の TFTP サーバ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 172.16.111.111
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、**no boot system** 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 **boot system** 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 **boot system** 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 **boot system 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。これに失敗すると、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た **boot system rom** コマンドにตอบสนองして、自身のシステム ROM からブートします。**copy running-config startup-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)

サーバからブートするシステム ソフトウェアは、サーバのフラッシュ メモリ内に存在している必要があります。フラッシュ メモリでない場合、クライアント ルータはサーバのシステム ROM からブートします。

次の例に、ルータの再起動後に **show version** コマンドを実行したサンプル出力を示します。

```
Router> 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 内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。

ルータを RARP サーバに設定

Reverse Address Resolution Protocol (RARP; 逆アドレス解決プロトコル) 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。この機能は、ホストがネットワーク レイヤの特定の IP アドレスに対応する物理レイヤの MAC アドレスをダイナミックに見つけるために使用される Address Resolution Protocols (ARP; アドレス解決プロトコル) のブロードキャストとちょうど逆の機能になります。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 サーバの存在に依存しています。

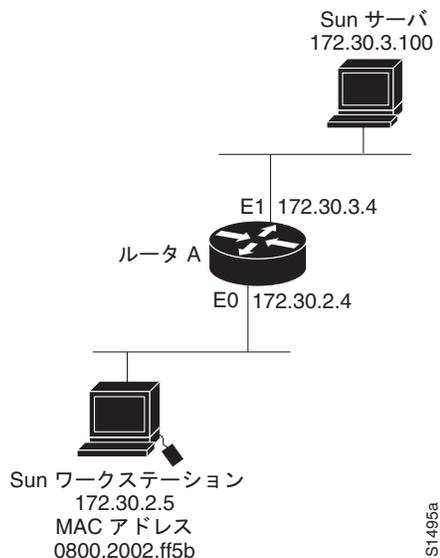
Cisco ルータは RARP サーバとして設定可能です。この機能により、Cisco IOS ソフトウェアが RARP 要求に応答できるようになります。

ルータを RARP サーバとして設定するには、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。

コマンド	目的
Router(config)# interface type [slot/]port	RARP サービスの設定を行うインターフェイスを指定し、その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 モードに入ります。
Router(config-if)# ip rarp-server ip-address	ルータで RARP サービスをイネーブルにします。

図 13 に、ルータをディスクレス ワークステーションの RARP サーバとして動作するよう設定するネットワーク設定を示します。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 サーバへ転送されます。

図 13 ルータを RARP サーバに設定



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 ethernet 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 クライアントとサーバの IP アドレスは、現行の SunOS *rpc.bootparamd* デーモンの制限により、同一のメジャー ネットワーク番号を使用している必要があります。

次の例では、アクセス サーバが RARP サーバとして動作するよう設定されます。

```
! 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 ethernet 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
```

システム BOOTP パラメータの設定

非同期インターフェイス用 Boot Protocol (BOOTP) サーバは、拡張された BOOTP 要求 (RFC 1084 で定義されたもの) をサポートしています。補助ポートを非同期インターフェイスとして使用する場合、次のコマンドが役立ちます。

非同期インターフェイス用拡張 BOOTP パラメータを設定するには、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。

コマンド	目的
Router(config)# async-bootp tag [:hostname] data	非同期インターフェイス用拡張 BOOTP 要求を設定します。

次のコマンドを EXEC モードで使用すると、BOOTP 応答内で送信される拡張されたデータを表示できます。

コマンド	目的
Router# show async bootp	BOOTP 応答のパラメータを表示します。

たとえば、DNS サーバのアドレスが BOOTP 応答の拡張データとして指定された場合、次のような出力が表示されます。

```
Router# show async bootp
The following extended data will be sent in BOOTP responses:

dns-server 172.22.53.210
```

ご使用のシスコ デバイスを BOOTP サーバとして設定することについて、詳しくは「[Using AutoInstall and Setup](#)」の章を参照してください。

rsh および rcp 使用時のルータ設定

Remote Shell (RSH; リモート シェル) を使用すると、ユーザはコマンドをリモートで実行できるようになります。Remote Copy (RCP; リモート コピー) を使用すると、ユーザはネットワーク上のリモート ホストやサーバ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、業界の標準的実装と相互運用できます。シスコは、rsh と rcp の両方を指すのに RCMD (リモート コマンド) という略語を使用しています。

この項は、次の各部にわかれています。

- 「[発信 RCMD コミュニケーションの発信元インターフェイス指定](#)」
- 「[RCMD のための DNS 逆ルックアップ](#)」
- 「[rsh の使用とイネーブル化](#)」
- 「[rcp のイネーブル化と使用](#)」

発信 RCMD コミュニケーションの発信元インターフェイス指定

RCMD (rsh および rcp) コミュニケーションの発信元インターフェイスを指定できます。たとえば、RCMD コネクションがループバック インターフェイスをルータから出て行くパケットすべての送信元アドレスとして使用するよう、ルータを設定できます。RCMD に関連付けるインターフェイスを指定するには、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。

コマンド	目的
Router(config)# <code>ip rcmd source-interface interface-id</code>	発信 rsh および rcp トラフィックすべてのラベルとして使用するインターフェイスのアドレスを指定します。

`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、パーマネント IP アドレスを RCMD コミュニケーションと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)。セキュリティ上の理由から、「既知の」IP アドレスが使用されることもあります。そうすることで、リモート デバイスにそのアドレスを含むアクセス リストを作成できます。

RCMD のための DNS 逆ルックアップ

Cisco IOS ソフトウェアは、基本的なセキュリティ チェックとして、リモート コマンド (RCMD) アプリケーション (rsh および rcp) のために、DNS を使用してクライアント IP アドレスの逆ルックアップを行います。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。その後、そのホスト名の IP アドレスの DNS 要求が行われます。受取った IP アドレスが、元の要求元アドレスと照合されます。アドレスが DNS から受け取ったどのアドレスとも一致しない場合、rcmd 要求は実行されません。

この逆ルックアップは、「スプーフィング」の防止策とされています。ただし、このプロセスで確認できるのは、IP アドレスがルーティングできる有効なアドレスかどうかだけである点に注意してください。ハッカーが既知のホストの有効な IP アドレスでスプーフする可能性は残っています。

この機能は、デフォルトでイネーブルにされています。次のコマンドをグローバル コンフィギュレーション モードで実行して、RCMD (rsh および rcp) アクセスの DNS チェックをディセーブルにできます。

コマンド	目的
Router(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。

rsh の使用とイネーブル化

rsh (リモート シェル) を使用して、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スタートします。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、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 をイネーブル化するコンフィギュレーション コマンドは、「remote command」の略語である「rcmd」を使用します。

rsh セキュリティの維持

UNIX ホストのように rsh が動作しているリモート システムにアクセスするためには、そのユーザがリモートからそのシステムでコマンドを実行させ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する必要があります。UNIX システムでは *rhosts* ファイルによってそのシステムでリモートからコマンドを実行可能なユーザを識別します。

ルータで rsh サポートをイネーブルにすることで、リモート システムのユーザがコマンドを実行することを可能にできます。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するユーザによるルータへのアクセスを制御するために、ローカル認証データベースを設定する必要があります。ローカル認証データベースは、UNIX の *.rhosts* ファイルに類似しています。認証データベースで設定する各エントリで、ローカル ユーザ、リモート ホスト、リモート ユーザを識別します。

リモート ユーザによる rsh を使用したコマンド実行を許可するルータ設定

ルータを rsh サーバとして設定するには、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実行します。

	コマンド	目的
ステップ 1	Router(config)# ip rcmd remote-host local-username {ip-address host} remote-username [enable [level]]	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 ユーザそれぞれにエントリを作成します。
ステップ 2	Router(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。

ソフトウェアの受信 rsh コマンドのサポートをディセーブルにするには、**no ip rcmd rsh-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。

次に、リモート ユーザのために 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
```

rmtnetad1 および *netadmin4* という名前のユーザは、両者とも IP アドレス 172.16.101.101 のリモート ホスト上にいます。ユーザは両方とも同じリモート ホスト上にいますが、それぞれのユーザのために専用のエントリを含める必要があります。ユーザは両方とも、ルータへの接続と、ルータが rsh をイネーブル化した後にリモートからルータ上で rsh コマンドを実行することを許可されます。*netadmin4* という名前のユーザは、ルータ上で特権 EXEC モード 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 2 つのエントリは、ローカルのユーザ名として、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 ユーザが発行した rsh コマンドのルータでのサポートをイネーブルにします。

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 シェル プロトコルをサポートするネットワーク サーバ上で、リモートからコマンドを実行させることができます。このコマンドを使用するには、ネットワーク サーバの *rhosts* ファイル（または同等のファイル）に、そのホスト上でのリモートからのコマンド実行を許可するエントリが含まれている必要があります。

UNIX システムのようにリモート サーバがディレクトリ構造を有している場合、発行した rsh コマンドは */user username* というキーワードと引数のペアで指定したリモート ユーザ アカウントのディレクトリから、リモートで実行されます。

/user キーワードと引数を指定しなかった場合、Cisco IOS ソフトウェアはデフォルトのリモート ユーザ名を送信します。リモート ユーザ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 ユーザ名が有効である場合、ソフトウェアはそのユーザ名を送信します。TTY リモート ユーザ名が無効な場合、ソフトウェアはリモートとローカルのユーザ名の両方にルータのホスト名を使用します。

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

	コマンド	目的
ステップ 1	Router> enable [<i>password</i>]	特権 EXEC モードを開始します。
ステップ 2	Router# rsh { <i>ip-address</i> <i>host</i> } [<i>/user username</i>] <i>remote-command</i>	rsh を使用してリモートからコマンドを実行します。

次の例では、*mysys.cisco.com* 上で、ユーザ *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。

```
Router# enable
```

```
Router# rsh mysys.cisco.com /user sharon ls -a
.
..
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
.newsrc
.oldnewsr
.rhosts
.twmrc
.xsession
jazz
Router#
```

rcp のイネーブル化と使用

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 (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 サーバのようにファイル配布用のサーバ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へのアクセスだけです (ほとんどの UNIX システムは rsh をサポートしています)。ある場所から別の場所へファイルをコピーする以上、コピー元ファイルの読み取り権限と、コピー先ディレクトリの書き込み権限が必要になります。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 実装機能をエミュレートした、ファイルをネットワーク上のシステム間でコピーするものですが、シスコのコマンド構文は UNIX の rcp コマンド構文と異なっています。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。これらの改善は、rcp のトランスポートメカニズムがコネクション型の Transmission Control Protocol/Internet Protocol (TCP/IP) スタック上に構築されており、これを使用しているために可能になりました。rcp コマンドを使用して、ルータからネットワークサーバ (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。

リモートユーザからの 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。

	コマンド	目的
ステップ1	Router(config)# ip rcmd remote-host local-username {ip-address host} remote-username [enable [level]]	ローカル認証データベースで、rcp コマンド実行を許可するリモートユーザそれぞれにエントリを作成します。
ステップ2	Router(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。

ソフトウェアの受信 rcp 要求のサポートをディセーブルにするには、**no ip rcmd rcp-enable** コマンドを使用します。



(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。

次の例に、リモート ユーザ用に認証データベースに 2 つのエントリを追加し、ソフトウェアでリモート ユーザからのリモート コピー要求のサポートをイネーブルに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 2 つのエントリは、ローカルのユーザ名として、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` プロトコルでは、クライアントは `rcp` 要求ごとにリモート ユーザ名をサーバ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名 (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 ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続しており、`username` コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。



(注)

シスコ製品では、TTY がサーバ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、元の UNIX の端末だった *teletype* を表す *TTY* デバイスと呼ばれています。

3. 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 サーバ上でリモート ユーザ名のアカウントが定義されている必要があります。

サーバに書き込む場合、ルータ上のユーザからの `rcp` 書き込み要求を受け入れるように、`rcp` サーバ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` サーバ上のリモート ユーザの `.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
```

ルータの IP アドレスを `Router1.company.com` と変換するとすれば、`rcp` サーバの `User0` のための `.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 サーバのマニュアルを参照してください。

このサーバ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、サーバ上のリモート ユーザ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。サーバ上で使用するディレクトリを指定するには、**ip rcmd remote-username** コマンドを使用します。たとえば、システム イメージがサーバ上のあるユーザのホーム ディレクトリに存在する場合、そのユーザの名前をリモート ユーザ名として指定できます。

ファイル サーバ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。

rcp 要求で送信されるデフォルトのリモート ユーザ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。

コマンド	目的
Router(config)# ip rcmd remote-username username	リモート ユーザ名を指定します。

リモート ユーザ名を削除してデフォルト値に戻す場合、**no ip rcmd remote-username** コマンドを使用します。

FTP 接続使用時のルータ設定

File Transfer Protocol (FTP; ファイル転送プロトコル) を使用してネットワーク上のシステム間でファイルを転送するようルータを設定します。Cisco IOS の FTP 実装では、次の FTP 特性を設定できます。

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

FTP 特性を設定するには、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のいずれかを使用します。

コマンド	目的
Router(config)# ip ftp username string	FTP 接続で使用されるユーザ名を指定します。
Router(config)# ip ftp password [type] password	FTP 接続で使用されるパスワードを指定します。
Router(config)# ip ftp passive	パッシブ モード FTP 接続だけを使用するよう、ルータを設定します。
または Router(config)# no ip ftp passive	または すべての種類の FTP 接続を許可します (デフォルト)。
Router(config)# ip ftp source-interface interface	FTP 接続の発信元 IP アドレスを指定します。

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**、パスワード **sword** を使用して、IP アドレス **192.168.10.3** のサーバにアクセスします。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 creates the core dump in the event the system at IP address
! 192.168.10.3 crashes
exception dump 192.168.10.3
```

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2008 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2011, シスコシステムズ合同会社.
All rights reserved.