



DHCP の概要

Dynamic Host Configuration Protocol (DHCP) は、*Bootstrap Protocol* (BOOTP; ブートストラッププロトコル) に基づいています。DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。DHCP により、再利用可能なネットワークアドレスおよび設定オプションをインターネットホストに自動的に割り当てられるようになります。DHCP は 2 つのコンポーネントで構成されます。1 つはホスト固有の設定パラメータを DHCP サーバからホストに配信するためのプロトコルで、もう 1 つはホストにネットワークアドレスを割り当てるためのメカニズムです。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 サーバホストが、ダイナミックに設定されるホストに対して、ネットワークアドレスを割り当て、設定パラメータを提供します。

このモジュールでは、Cisco IOS DHCP の理解に必要な概念について説明します。

変更履歴

このマニュアルの初版の発行は 2005 年 5 月 2 日 で、最終更新日は 2006 年 2 月 27 日 です。

目次

- [「DHCP について」 \(P.1\)](#)
- [「参考資料」 \(P.6\)](#)
- [「用語集」 \(P.8\)](#)

DHCP について

DHCP を設定するには、次の概念について理解しておく必要があります。

- [「DHCP の概要」 \(P.2\)](#)
- [「Cisco IOS DHCP を使用することの利点」 \(P.2\)](#)
- [「DHCP サーバ、リレー エージェント、およびクライアント動作」 \(P.3\)](#)
- [「DHCP データベース」 \(P.4\)](#)
- [「DHCP アトリビュートの継承」 \(P.4\)](#)
- [「DHCP オプションとサブオプション」 \(P.4\)](#)



- 「DHCP サーバ オンデマンドアドレス プール (ODAP) 管理の概要」 (P.5)
- 「アカウントリングとセキュリティ用 DHCP サービスの概要」 (P.6)

DHCP の概要

Cisco IOS ソフトウェアが稼動している Cisco ルータには、DHCP サーバとリレー エージェント ソフトウェアが含まれています。Cisco IOS DHCP サーバは、DHCP サーバの完全実装であり、ルータ内の特定のアドレスプールから IP アドレスを DHCP クライアントに割り当て、管理します。また、これらのアドレス プールは、DNS サーバの IP アドレス、デフォルト ルータ、その他の設定パラメータなどの詳細情報を要求元クライアントに提供するように設定できます。Cisco IOS DHCP サーバが自身のデータベースで DHCP 要求を実行できない場合、この要求をネットワーク管理者が定義した 1 つ以上のセカンダリ DHCP サーバに転送できます。

DHCP では、IP アドレス割り当ての次の 3 つのメカニズムをサポートします。

- 自動割り当て：DHCP は、無期限の IP アドレスをクライアントに割り当てます。
- ダイナミック割り当て：DHCP は、リースと呼ばれる限られた期間（またはクライアントがアドレスを明示的に放棄するまで）IP アドレスをクライアントに割り当てます。
DHCP は、On-Demand Address Pool (ODAP; オンデマンドアドレス プール) もサポートします。ODAP とは、アドレス利用水準に基づいて IP アドレスのプール サイズをダイナミックに拡大または縮小できる機能です。ODAP は、プライベート アドレスを使用するお客様のアドレス割り当てをサポートします。
- 手動割り当て：ネットワーク管理者が IP アドレスをクライアントに割り当てます。DHCP は、クライアントに割り当てられたアドレスを単に伝達するために使われます。

DHCP メッセージ形式は、BOOTP メッセージ形式に基づいています。これにより、BOOTP リレー エージェント機能および BOOTP クライアントと DHCP サーバ間の相互運用性が確実にサポートされます。BOOTP リレー エージェントにより、各物理ネットワーク セグメントに DHCP サーバを導入する必要がなくなります。BOOTP については、RFC 951 の『*Bootstrap Protocol (BOOTP)*』、および RFC 1542 の『*Clarifications and Extensions for the Bootstrap Protocol*』を参照してください。

BOOTP と比較した DHCP の主な利点は、DHCP では DHCP サーバをすべてのクライアントのすべての MAC アドレスに設定する必要がないことです。DHCP は 1 つのプロセスを定義します。このプロセスにより、DHCP サーバは DHCP クライアントが存在する IP サブネットを認識し、サブネット内の有効な IP アドレスのプールから IP アドレスを割り当てることができます。DHCP が提供する可能性のあるデフォルト ルータ IP アドレスなどの他の情報の大半は、サブネット内のすべてのホストに共通しているため、DHCP サーバは通常ホストごとではなくサブネットごとに情報を設定できます。この機能により、ネットワーク管理作業が BOOTP より少なくなります。

Cisco IOS DHCP を使用することの利点

Cisco IOS DHCP 実装には次の利点があります。

- インターネット アクセス コストの削減
各リモートサイトで自動 IP アドレス割り当てを使用するとインターネット アクセス コストが大幅に削減されます。スタティック IP アドレスの購入は自動割り当て IP アドレスより非常に高価です。
- クライアント設定作業とコストの削減
DHCP の設定は簡単なため、運用上のオーバーヘッドおよびデバイス設定作業に関連するコストを最小限にし、技術者以外のユーザによる導入を容易にします。
- 中央集中型の管理

DHCP サーバは複数のサブネットの設定を保持するため、設定パラメータの変更時に管理者が更新する必要があるのは 1 台の中央サーバのみです。

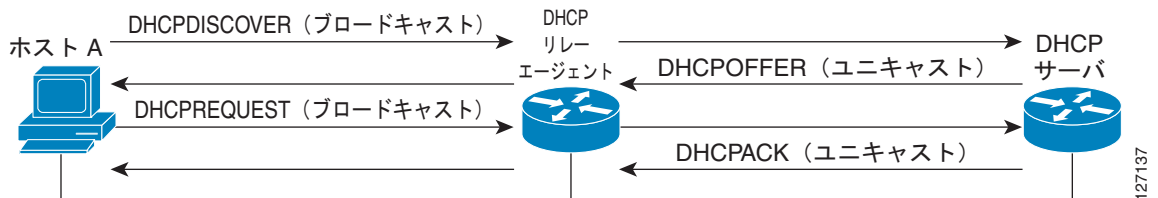
DHCP サーバ、リレー エージェント、およびクライアント動作

DHCP は、TCP/IP ネットワーク上のホストに設定情報をダイナミックに渡すフレームワークを提供します。DHCP クライアントは、DHCP を使用して IP アドレスなどの設定パラメータを取得するインターネット ホストです。

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するホストです。リレー エージェントは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送するために使用されます。リレー エージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間である程度透過的にスイッチングされます。これとは対照的に、リレー エージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して他のインターフェイスから送信します。

図 1 では、DHCP クライアントが DHCP サーバから IP アドレスを要求するときに発生する基本的な手順を示します。クライアントであるホスト A が DHCPDISCOVER ブロードキャストメッセージを送信して DHCP サーバの場所を特定します。リレー エージェントは、DHCP クライアントとサーバ間でパケットを転送します。DHCP サーバは、DHCPOFFER ユニキャストメッセージで、設定パラメータ (IP アドレス、MAC アドレス、ドメイン名、IP アドレスのリースなど) をクライアントに提示します。

図 1 DHCP サーバに対する IP アドレスの DHCP 要求



DHCP クライアントは、複数の DHCP サーバから提示を受ける場合があります。提示のうちの任意の 1 つを受け入れられます。通常、クライアントは最初に受け取った提示を受け入れます。また、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予約しておきます。

クライアントは、DHCPREQUEST ブロードキャストメッセージで、提示された IP アドレスの正式な要求を DHCP サーバに戻します。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知らせます。

クライアントが送信する提示された IP アドレスに対する正式な要求 (DHCPREQUEST メッセージ) はブロードキャストのため、クライアントからの DHCPDISCOVER ブロードキャストメッセージを受信した他の DHCP サーバすべてがクライアントに提示された IP アドレスを再利用できます。

DHCP サーバから DHCPOFFER ユニキャストメッセージによってクライアントに送信された設定パラメータが無効である (誤設定エラーがある) 場合、クライアントは DHCPDECLINE ブロードキャストメッセージを DHCP サーバに戻します。

DHCP サーバは、DHCPNAK 拒否ブロードキャストメッセージをクライアントに送信します。これは、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 DHCP サーバの DHCPOFFER メッセージに対するクライアントの応答が遅い (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) 場合に、提示された設定パラメータが割り当てられなかったことを意味するメッセージです。

DHCP データベース

DHCP アドレス プールは、Non-Volatile RAM (NVRAM; 不揮発性 RAM) に格納されています。アドレス プール数に制限はありません。アドレス バインディングは、クライアントの IP アドレスとハードウェア アドレス間のマッピングです。クライアントの IP アドレスは、管理者が設定できます (手動アドレス割り当て)。また、DHCP サーバによりプールからも割り当てできます。

手動バインディングは、NVRAM に格納されます。手動バインディングは、ネットワーク管理者に設定される特別なアドレス プールにすぎません。手動バインディング数に制限はありません。

自動バインディングとは、DHCP データベースで検出されたホストの MAC アドレスに自動的にマッピングされた IP アドレスです。自動バインディングは、データベース エージェントと呼ばれるリモートホストに格納されます。DHCP データベース エージェントは、FTP、TFTP、または RCP サーバなどに対する DHCP バインディング データベースを格納する任意のホストです。バインディングはメンテナンスを簡単にするためにテキスト レコードとして保存されます。

複数の DHCP データベース エージェントを設定できます。また、各エージェントに対してデータベースの更新と転送の間隔を設定できます。

DHCP アトリビュートの継承

DHCP サーバ データベースはツリー構造になっています。ツリーのルートはナチュラル ネットワークのアドレス プール、ブランチはサブネットワークのアドレス プール、リーフはクライアントへの手動バインディングです。サブネットワークはネットワーク パラメータを継承し、クライアントはサブネットワーク パラメータを継承します。そのため、ドメイン名などの共通なパラメータはツリーの (ネットワークまたはサブネットワークの) 最上位レベルに設定する必要があります。

継承されたパラメータはオーバーライドできます。たとえば、パラメータがナチュラル ネットワークとサブネットワークの両方に定義されている場合は、サブネットワークの定義が使用されます。

アドレス リースは継承されません。IP アドレスにリースが指定されていない場合は、デフォルトで DHCP サーバがそのアドレスに 1 日リースを割り当てます。

DHCP オプションとサブオプション

設定パラメータと他の制御情報は、DHCP メッセージのオプション フィールドに格納されたタグ付きデータ項目で伝送されます。オプションにより、追加情報の付加方法が提供されます。プロトコルに設計されていないクライアントに追加情報を提供するベンダーはこのオプションを使用できます。

Cisco IOS DHCP 実装でも大半の DHCP サーバ オプションのカスタマイズが可能になります。たとえば、Cisco IOS イメージを格納する TFTP サーバは、Option 150 でインテリジェント IP Phone をサポートするようにカスタマイズできます。

Virtual Private Network (VPN; バーチャルプライベート ネットワーク) では、別々のネットワークの 2 つのプールが同じ DHCP サーバが使用する同じアドレス空間をプライベート ネットワーク アドレスを使用して保持できます。Cisco IOS ソフトウェアは、リレー エージェント情報オプションや VPN ID サブオプションなどの VPN-related オプションおよびサブオプションをサポートします。リレー エージェントは、これらの VPN-related オプションおよびサブオプションを認識してクライアントから発信された DHCP パケットを DHCP サーバに転送します。DHCP サーバはこの情報を使用して、VPN ID によって識別された IP アドレスや他のパラメータを割り当て、クライアントが属する VPN の選択に役立てられます。

DHCP オプションおよびサブオプションの詳細については、『*Network Registrar User's Guide, Release 6.2*』の付録「[DHCP Options](#)」を参照してください。

リース ネゴシエーション中 DHCP サーバは、表 1 に示すオプションをクライアントに送信します。

表 1 デフォルト DHCP サーバオプション

DHCP オプション名	DHCP オプションコード	説明
Subnet mask オプション	1	RFC 950 に従ってクライアントのサブネット マスクを指定します。
Router オプション	3	クライアントのサブネット上にあるルータの IP アドレス リストを指定します。通常は、優先順位の高い順にリスト表示されます。
Domain name server オプション	6	クライアントが使用できる DNS ネーム サーバのリストを指定します。通常は、優先順位の高い順にリスト表示されます。
Hostname オプション	12	クライアントの名前を指定します。名前はローカル ドメイン名に制限することもしないことも可能です。
Domain name オプション	15	ドメイン ネーム システムを介してホスト名を解決するときにクライアントが使用するべきドメイン名を指定します。
NetBIOS over TCP/IP name server オプション	44	優先順位の高い順にリスト表示される RFC 1001/1002 NetBIOS ネーム サーバのリストを指定します。
NetBIOS over TCP/IP node type オプション	46	RFC 1001/1002 の説明に従って設定する設定可能な NetBIOS over TCP/IP クライアントをイネーブルにします。
IP address lease time オプション	51	クライアントが IP アドレスのリースを要求できるようにします。
DHCP message type オプション	53	DHCP メッセージのタイプを伝達します。
Server identifier オプション	54	選択された DHCP サーバの IP アドレスを識別します。
Renewal (T1) time オプション	58	アドレス割り当てからクライアントが更新ステートに移行するまでの時間間隔を指定します。
Rebinding (T2) time オプション	59	アドレス割り当てからクライアントが再バインディング ステートに移行するまでの時間間隔を指定します。

DHCP サーバ オンデマンド アドレス プール (ODAP) 管理の概要

Cisco IOS DHCP サーバ On-Demand Address Pool (ODAP; オンデマンド アドレス プール) マネージャは、大規模なアドレス プールを集中管理し、大規模ネットワークの設定を単純化するために使用されます。ODAP は、IP アドレス割り当ての集中管理ポイントを提供します。Cisco IOS ルータが ODAP マネージャとして設定されている場合、IP アドレスのプールのサイズは、アドレスの利用水準に応じてダイナミックに拡大/縮小されます。

ODAP は、プライベート アドレスを使用しているお客様のために、DHCP を使用したアドレスの割り当てをサポートします。各 ODAP は特定の Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) VPN に設定および関連付けられています。また、Cisco IOS ソフトウェアでは、非 MPLS VPN アドレス プールでも、プール名のサポートを `peer default ip address dhcp-pool pool name` コマンドに追加することにより、ODAP がサポートされます。

DHCP サーバのサブネット割り当ては、サブネット全体 (アドレスの範囲) をリレー エージェントに提示する方法の 1 つです。これにより、リモート アクセス デバイスは IP アドレスを DHCP クライアントにプロビジョニングできます。この機能は、個々のクライアント アドレスの管理とともに使用したり、その代わりに使用できます。サブネット割り当ては、DHCP インフラストラクチャによるサブネットのダイナミックな管理を使用することで、IP アドレスのプロビジョニング、集約、特性評価、配布を改善できます。

この機能により、ODAP クライアントへのリースを目的として、DHCP サーバにサブネットのプールを設定できるようになります。サブネット プールは、クライアントごとにグローバル ODAP クライアントに対してまたは MPLS VPN の ODAP クライアントに対して設定できます。DHCP サブネット割り当てサーバは、サブネットリースのバインディングを作成し、これらのリースを DHCP データベースに格納します。

アカウントिंगとセキュリティ用 DHCP サービスの概要

Cisco IOS ソフトウェアは、Public Wireless LAN (PWLAN; パブリック ワイヤレス LAN) における DHCP アカウントिंग、信頼性、セキュリティを強化する新しい機能を複数サポートしています。この機能は、他のネットワーク実装でも使用できます。

DHCP アカウントिंगは、DHCP に Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) および Remote Authentication Dial-In User Service (RADIUS) のサポートを提供します。AAA および RADIUS のサポートにより、セキュアな START および STOP アカウントिंग メッセージを送信することで、セキュリティが強化されます。DHCP アカウントिंगを設定すると、セキュリティ レイヤが追加され、適切な RADIUS START および STOP アカウントिंग レコードに対して DHCP リースの割り当てと終了をトリガーできるようになります。これにより、Service Selection Gateway (SSG) などのアップストリーム デバイスによりセッション ステートが適切に維持されます。このセキュリティ強化は、無許可のクライアントまたはハッカーが、許可された DHCP リースをスプーフィングしてネットワークに不正侵入することを防ぐのに役立ちます。

PWLAN のセキュリティ問題を解決するために、他に 3 つの機能が設計および実装されています。1 つめの機能では、DHCP データベース内の DHCP リースに対する ARP テーブル エントリを保護します。このセキュアな ARP 機能により、DHCP サーバのデータベースを ARP テーブルと同期させてアドレスのハイジャックを回避することで、IP スプーフィングを防止します。アドレスが割り当てられると、セキュア ARP により、クライアントの ARP テーブルにエントリが追加されます。バインディングが期限切れになった場合に限り、DHCP サーバはこれを削除できます。

2 つめの機能は DHCP 許可 ARP です。この機能では、DHCP が明示的にユーザ ログアウト時を認識する必要性に対応することで完全性の高いソリューションを提供します。DHCP 許可 ARP の導入前は、ユーザが不適切な方法でシステムを離れた場合に DHCP サーバに通知するメカニズムがありませんでした。このため、お客様がログアウトしてもシステムがログアウトを検出しなかった結果、過度の請求がされる可能性があります。この問題に対処するために、DHCP 許可 ARP は、1 分ごとに定期 ARP メッセージを送信して、ユーザが現在ログインしているかどうかを確認します。許可ユーザのみが ARP 要求に応答できます。無許可ユーザからの ARP 応答は DHCP サーバでブロックされるため、セキュリティ レベルがより強化されます。

さらに、DHCP 許可 ARP では、インターフェイスにおけるダイナミック ARP 学習がディセーブルになります。アドレス マッピングを組み込むことができるのは、**arp authorized** インターフェイス コンフィギュレーション コマンドで指定した許可コンポーネントのみです。現時点で ARP エントリのインストールができる許可コンポーネントは DHCP のみです。

3 つめの機能は ARP 自動ログオフです。この機能では、許可ユーザのログアウト時に、より緻密にプロービングを制御します。**arp probe interval** コマンドは、プローブの開始時点 (タイムアウト)、ピアのプローブ頻度 (間隔)、および最大試行回数 (カウント) を指定します。

参考資料

ここでは、DHCP に関する関連資料について説明します。

関連資料

関連項目	参照先
DHCP コマンド: コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『Cisco IOS IP Addressing Services Command Reference』
DHCP サーバ設定	『Configuring the Cisco IOS DHCP Server』 モジュール
DHCP リレー エージェント設定	『Configuring the Cisco IOS DHCP Relay Agent』 モジュール
DHCP クライアント設定	『Configuring the Cisco IOS DHCP Client』 モジュール
DHCP サーバ オンデマンドアドレス プール	『Configuring the DHCP Server On-Demand Address Pool Manager』 モジュール
DHCP 拡張機能	『Configuring DHCP Services for Accounting and Security』 モジュール
Edge-Session 管理用の DHCP 拡張機能	『Configuring DHCP Enhancements for Edge-Session Management』 モジュール
DHCP オプション	『Network Registrar User's Guide, Release 6.1.1』 の付録「DHCP Options」

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 951	『Bootstrap Protocol (BOOTP)』
RFC 2131	『Dynamic Host Configuration Protocol』
RFC 2132	『DHCP Options and BOOTP Vendor Extensions』
RFC 1542	『Clarifications and Extensions for the Bootstrap Protocol』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポートおよびドキュメンテーション Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

用語集

BOOTP : Bootstrap Protocol (ブートストラップ プロトコル)。起動中のコンピュータが自分の IP アドレスおよび残りのパラメータが格納されたブート ファイルの場所を見つける方法を提供するプロトコル。

DHCP : Dynamic Host Configuration Protocol。ホストに IP アドレスが不要になったときに、IP アドレスを再利用できるようにダイナミックに IP アドレス割り当てるメカニズムを提供するプロトコル。

DNS : Domain Name System (ドメイン ネーム システム)。ネットワーク ノードの名前をアドレスに変換するためにインターネットで使用されるシステム。

PWLAN : Public Wireless Local Area Network (パブリック ワイヤレス ローカル エリア ネットワーク)。ワイヤレス LAN の 1 種類で、ホットスポットとも呼ばれます。PWLAN には、適切に設定されているコンピュータ デバイスがあれば誰でもアクセスできます。

SSG : Service Selection Gateway。シスコ ネットワーク内でオンデマンド サービス拡張機能を提供する Cisco IOS 機能セットです。

アドレス バインディング : クライアントの IP アドレスとハードウェア (MAC) アドレス間のマッピング。クライアントの IP アドレスは、管理者が設定できます (手動アドレス割り当て)。または、DHCP サーバによりプールから割り当てできます (自動アドレス割り当て)。バインディングには、リースの有効期限日も含まれます。リースの有効期限日のデフォルトは 1 日です。

アドレス プール : DHCP サーバによって割り当てられる IP アドレスの範囲。アドレス プールはサブネット番号によって索引付けされています。

アドレスの競合 : 2 つのホストで同じ IP アドレスを使用することによる重複。アドレスの割り当て中、DHCP は ping および gratuitous (ARP) を使用して競合がないか確認します。競合が検出されると、そのアドレスはプールから削除されます。そのアドレスは、管理者が競合を解決するまで割り当てられません。

クライアント : 設定パラメータを要求する任意のホスト。

サーバ : 設定パラメータを提供する任意のホスト。

自動アドレス割り当て : 限定された期間またはクライアントが IP アドレスを明示的に放棄するまでの間のクライアントの IP アドレスをネットワーク管理者が取得するためのアドレス割り当て方法。自動割り当ては、ネットワークに一時的にのみ接続するクライアントにアドレスを割り当てる場合、または無期限の IP アドレスが必要ではないクライアント グループ間で IP アドレスの限られたプールを共有する場合に特に有用です。自動割り当ては、IP アドレスが十分に足りていないために、古いクライアントが廃棄された際の IP アドレスの再利用が重要なネットワークに無期限に接続する新しいクライアントに対して IP アドレスを割り当てる場合にも最適です。

手動アドレス割り当て : 管理的に割り当てられた IP アドレスをホストに割り当てるアドレスの割り当て方法。手動割り当てでは、DHCP を使用して IP アドレスをホストに手動設定するときにエラーを起しやすいうプロセスを排除できます。

データベース：アドレス プールおよびバインディングの集合。

データベース エージェント：DHCP バインディング データベースを格納する任意のホスト。たとえば、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバ。

リレー エージェント：異なるサブネット上のサーバとクライアント間で DHCP メッセージおよび BOOTP メッセージを転送するルータ。



(注) この用語集に記載されていない用語については、『[Internetworking Terms and Acronyms](#)』を参照してください。

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。

© 2007 Cisco Systems, Inc.
All rights reserved.

Copyright © 2007–2011, シスコシステムズ合同会社.
All rights reserved.

