IP サービスの設定

ここでは、オプションの IP サービスを設定する手順について説明します。この章で説明する IP サービス コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。この章で説明するその他のコマンドについて詳細が記載されている資料を探すには、コマンド リファレンス マスター インデックス、またはオンライン検索を使用してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IP サービスの機能情報」（P.21）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

IP サービスの概要

ここで説明する IP サービスを設定するには、次の概念を理解しておく必要があります。

IP ソース ルーティング

Cisco IOS ソフトウェアは、すべてのパケットの IP ヘッダー オプションを検査します。RFC 791 に定義されている IP ヘッダー オプションである Strict Source Route、Loose Source Route、Record Route、および Time Stamp をサポートします。これらのオプションのいずれかがイネーブルにされているパケットを検出すると、適切なアクションを実行します。無効なオプションが設定されたパケットを検出すると、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）パラメータの問題に関するメッセージをパケットの送信元に送信し、該当のパケットを破棄します。

IP は、送信元 IP ホストが IP ネットワーク上のルートを指定できるプロビジョニング（「ソース ルーティング」と呼ばれます）を提供します。ソース ルーティングは、IP ヘッダーのオプションとして指定されます。ソース ルーティングが指定されると、ソフトウェアは指定されたソース ルートに従ってパケットを転送します。IP ソース ルーティングは、ネットワーク上の特定のルートを通るようにパケットに強制したい場合に採用されます。デフォルトでは、ソース ルーティングが実行されます。IP ソース ルーティングがネットワークでの正規の目的に使用されることはめったにありません。古い IP 実装では、ソース - ルート パケットが適切に処理されないことがあり、ソース ルーティング オプションを指定してデータグラムに送信することで、これらの実装を実行するデバイスがクラッシュすることがあります。可能である限り、IP ソース ルーティングをディセーブルにします。IP ソース ルーティングをディセーブルにすると、Cisco ルータは、ソース ルーティング オプションを送受信する IP パケットの転送を行いません。

ICMP の概要

Internet Control Message Protocol（ICMP）は、元来、RFC 792 で TCP/IP スイート用に作成されたもので、少数のエラー状態を報告するように設計されました。ICMP は、さまざまなエラー状態を報告し、フィードバック機能やテスト機能を提供することもできます。各メッセージでは、共通のフォーマットが使用され、同じプロトコル ルールを使用して送受信されます。

ICMP により、カプセル化されたメッセージの IP デバイス間での送受信を許可することで、IP はアドレッシング、データグラム パッケージング、およびルーティングを実行できるようになります。これらのメッセージは、他の IP メッセージのように、IP データグラムにカプセル化されます。メッセージが生成されると、元の IP ヘッダーは ICMP メッセージにカプセル化され、これらの 2 つの情報は新しい IP ヘッダー内にカプセル化されて、エラー報告として送信元デバイスに返されます。

ICMP メッセージはさまざまな状況で送信されます。たとえば、データグラムが宛先に到達できない場合、ゲートウェイにデータグラムを転送するためのバッファリング機能がない場合、ゲートウェイが短いルート上でトラフィックを送信するホストを指定できる場合、などが挙げられます。メッセージに関するメッセージの無限後退を避けるため、ICMP メッセージに関する ICMP メッセージが送信されることはありません。

ICMP によって、IP の信頼性が高められることや、データグラム配信や制御メッセージが戻されることが確実になることはありません。一部のデータグラムは、データ損失が報告されることなく、ドロップされることがあります。IP を使用する上位レベルのプロトコルは、信頼性の高い通信が求められる場合、信頼性を高めるための独自の手順を実装する必要があります。

IPv6 および ICMP の詳細については、次の URL に掲載されている『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

ICMP 到達不能エラー メッセージ

宛先ホストのアプリケーションに対してメッセージを完全に配信できない場合は、タイプ 3 のエラー メッセージが送信されます。ICMP ヘッダーに含まれる 6 つのコードに、次のような到達不能条件が示されます。

- 0：ネットワーク到達不能
- 1：ホスト到達不能
- 2：プロトコル到達不能
- 3：ポート到達不能
- 4：フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されている
- 5：ソース ルート機能停止

Cisco IOS ソフトウェアは、ICMP 到達不能宛先エラー メッセージの生成を抑止できます。これは「レート制限」と呼ばれます。デフォルトでは、0.5 秒の間に 2 つ以上の到達不能メッセージが生成されないようにします。コード 4 やその他の到達不能宛先エラー メッセージがあるため、このように間隔を空けて設定できます。ただし、送信されていない ICMP メッセージの数を表示する方法はありません。

送信されていないタイプ 3 メッセージをカウントして表示する方法は、ICMP 到達不能宛先カウンタ機能によって提供されます。ルータに対する Denial of Service（DoS; サービス拒否）攻撃を示す過剰なレート制限が見られる期間が発生すると、この機能によりコンソール ロギングにもエラー メッセージが表示されます。

不明なプロトコルを使用した、自身に宛てた非ブロードキャスト パケットを受け取ると、Cisco IOS ソフトウェアは送信元に ICMP プロトコル 到達不能メッセージを送り返します。同様に、宛先アドレスへのルートがないことが明らかで最終的な宛先に配信できないパケットを受け取ったときも、Cisco IOS ソフトウェアは送信元に ICMP プロトコル 到達不能メッセージを送り返します。この機能はデフォルトでイネーブルになっています。

可能である限り、Internet Message Control Protocol（ICMP; インターネット制御メッセージ プロトコル）ホスト到達不能メッセージをディセーブルにします。ICMP は、パス、ルート、ネットワーク状態に関する情報をリレーする方法で、IP トラフィックをサポートします。これらのメッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。

空のインターフェイスはパケット シンクであるため、ここで転送されたパケットは必ず破棄され、（機能がディセーブルになっていない限り）ホスト到達不能メッセージが生成されます。この場合、空のインターフェイスを使用して DoS 攻撃をブロックしていると、ローカル ネットワークではこれらのメッセージのフラッディングが発生します。このような状況に陥らないようにするためには、これらのメッセージをディセーブルにします。また、ブロックされたすべてのパケットは空のインターフェイスに転送されるため、ホスト到達不能メッセージを受信する攻撃者がそれらのメッセージを使用して Access Control List（ACL; アクセス コントロール リスト）設定を利用できるようになることがあります。ルータに「null 0」インターフェイスを設定している場合は、廃棄されたパケットや空のインターフェイスにルーティングされたパケットの ICMP ホスト到達不能メッセージをディセーブルにしてください。

ICMP マスク応答メッセージ

ネットワーク デバイスでは、インターネットワーク内の特定のサブネットワークのサブネット マスクを認識することが必要になる場合があります。このような場合、この情報を取得するため、デバイスは ICMP マスク要求メッセージを送信することができます。必要な情報を保有するデバイスからの応答として、ICMP マスク応答メッセージが送信されます。Cisco IOS ソフトウェアは、ICMP マスク要求メッセージに応答できます（この機能がイネーブルになっている場合）。

これらのメッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。

ICMP リダイレクト メッセージ

ルートは、最善ではないことがあります。たとえば、ルータは、パケットを受信したインターフェイスを通してパケットを再送信するように強制されることがあります。ルータが、パケットを受信したのと同じインターフェイスを通してパケットを再送信すると、Cisco IOS ソフトウェアはパケットの発信元に対して ICMP リダイレクト メッセージを送信し、ルータがサブネット上で受信デバイスに直接接続されていることと、パケットは同じサブネット上の別のシステムに転送する必要があることを知らせます。ソフトウェアがパケットの発信元に ICMP リダイレクト メッセージを送信するのは、送信元ホストは、このデバイスをまったく関与させることなく、パケットをネクストホップに送信できるからです。リダイレクト メッセージは、送信者に対し、ルートから受信デバイスを削除し、より具体的にパスを示すデバイスに置き換えるように指示します。この機能はデフォルトでイネーブルになっています。

適切に機能している IP ネットワークでは、ルータは独自のローカル サブネット上にあるホストにしかリダイレクトを送信しません。エンド ノードがリダイレクトを送信することはなく、またリダイレクトが複数のネットワーク ホップを通過することもありません。ただし、攻撃者がこれらのルールに違反することがあり、これに基づいた攻撃も見られます。ICMP リダイレクトをディセーブルにすると、ネットワークに運用上の影響を及ぼすことなく、この方法で攻撃される可能性を排除できます。

サービス拒否攻撃

サービス拒否は次第に懸念が高まってきている問題です。特に、このような攻撃に関連するコストには大きな関心が寄せられています。DoS 攻撃は、ネットワーク デバイスのパフォーマンス低下、デバイスのネットワークからの切断、システム クラッシュの発生、などの原因となります。ネットワーク サービスを利用できないと、企業やサービス プロバイダーは生産性低下や売上損失の損害を被ることになります。

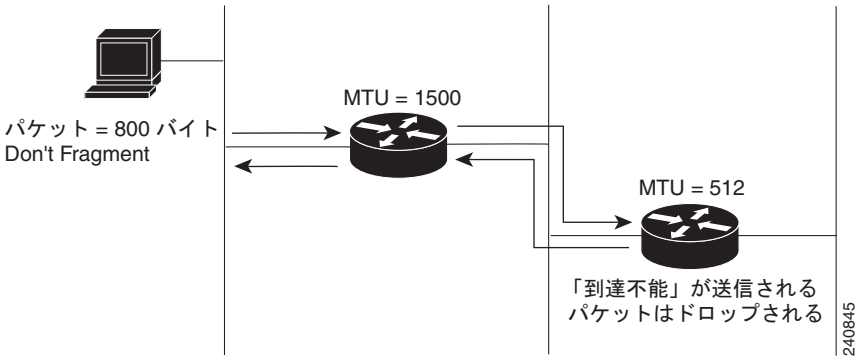
DoS 攻撃の目的は、ユーザや組織がサービスまたはリソースにアクセスできないようにすることです。Web サイトが DoS 攻撃の危険にさらされると、数百万のユーザのそのサイトへのアクセスが拒否されます。通常、DoS 攻撃によって情報が不正に盗み取られることはありません。DoS 攻撃では、不正なユーザがアクセスできるようにするのではなく、許可されたユーザのアクセスを妨害することで、苛立たせたり、コストを発生させたりします。Distributed DoS（DDoS; 分散型 DoS）攻撃は、危険にさらされたシステムで攻撃パケットのフラッディングを発生させるように DoS 攻撃を増幅させたもので、これにより、対象システムのユーザのサービス拒否が生じます。

DoS 攻撃は、ICMP エコー要求（ping）のストリームが宛先サブネットにブロードキャストされるときに発生します。これらの要求の送信元アドレスは、ターゲットの送信元アドレスに改ざんされます。攻撃者が要求を送信すると、その都度、サブネット上のホストはターゲット上でフラッディングを発生させ、帯域幅を浪費させます。大部分の DoS 攻撃は「Smurf」攻撃と呼ばれます。これは実行可能プログラムにちなんで名付けられたものです。ホストに対するネットワークレベル攻撃のカテゴリに該当します。ICMP 到達不能宛先カウンタ機能の error-message ロギングがイネーブルになっていると、DoS 攻撃を簡単に検出できます。

PMTUD

Cisco IOS ソフトウェアは、RFC 1191 に定義されたとおりに、IP PMTUD メカニズムをサポートします。IP PMTUD を使用すると、ホストは経路上のさまざまなリンクで許容される Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズの差異をダイナミックに検出し、対処できます。（パケットが、**ip mtu** インターフェイス コンフィギュレーション コマンドでインターフェイスに設定した MTU よりも大きい場合など）フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されているため、ルータがデータグラムを転送できない場合もあります。Cisco IOS ソフトウェアは送信元ホストにメッセージを送信し、この問題を警告します。ホストは、パス沿いにあるすべてのリンクでの最小パケット サイズに合わせて、宛先に送信するパケットをフラグメンテーションすることが必要になります。この技術を図 1 に示します。

図 1　　IP PMTUD



IP PMTUD は、ネットワーク内のリンクが機能停止して別のリンクを使用しなければならないときに、MTU サイズのリンクが異なる場合（そしてルータが異なる場合）に役立ちます。図 1 に示すように、ルータはネットワーク上で IP パケットを送信していますが、1 台目のルータの MTU は 1500 バイトに設定され、2 台目のルータの MTU は 512 バイトに設定されています。データグラムの「Don't Fragment」ビットが設定されていると、512 バイトのルータはデータグラムを転送できないため、このデータグラムはドロップされます。この場合、512 バイトより大きいパケットはすべてドロップされます。2 台目のルータは、「フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されている」ことを示す Code フィールドとともに、ICMP 宛先到達不能メッセージをデータグラムの送信元に返します。IP PMTUD をサポートするため、未使用のヘッダー フィールドの下位ビットにはネクストホップ ネットワーク リンクの MTU が含まれます。

IP PMTUD は、接続が確立されているものの、送信者が介在するリンクに関する情報をまったく有していない場合にも役立ちます。リンクで生じる最大 MTU を使用できるようにすることが推奨されます。MTU が大きいほど、ホストが送信しなければならないパケット数が少なくなります。

（注） IP PMTUD は、エンド ホストによって開始されるプロセスです。エンド ホストが IP PMTUD をサポートしない場合、受信デバイスは、エンド ホストでのデータグラムのフラグメンテーションを回避するメカニズムを持たないことになります。

発信インターフェイス上で小さい MTU が設定されているルータが、大きい MTU が設定されているホストからパケットを受信すると（たとえば、トークンリング インターフェイスからパケットを受信し、発信イーサネット インターフェイスに転送する場合など）、このルータは、受信したパケットを、発信インターフェイスの MTU よりも大きいサイズにフラグメンテーションします。パケットをフラグメンテーションすると、ルータのパフォーマンスは低下します。ネットワーク内のルータで受信パケットの

フラグメンテーションを行わないようにするには、ネットワーク内のすべてのホストおよびルータで IP PMTUD を実行し、常に各ルータ インターフェイス タイプの MTU をできる限り大きく設定するようにします。

IP MAC アカウンティングと優先順位アカウンティング

Cisco IP アカウンティング サポートは、基本的な IP アカウンティング機能を提供します。IP アカウンティングをイネーブルにすると、ユーザが、送信元と宛先の IP アドレスに基づいて Cisco IOS ソフトウェアを介してスイッチングされたバイト数およびパケット数を参照できるようになります。中継 IP トラフィックだけが、発信ベースで測定されます。ソフトウェアが生成したトラフィックや、ソフトウェアで終了したトラフィックは、アカウンティング統計情報に含まれません。正確なアカウンティングの合計を得られるように、ソフトウェアは 2 つのアカウンティング データベース（アクティブ データベースとチェックポイント データベース）を維持します。

Cisco IP アカウンティング サポートは、IP アクセス リストに一致しなかった IP トラフィックを特定するための情報も提供します。IP アクセス リストに一致しなかった IP 送信元アドレスが特定されると、セキュリティ違反の可能性が警告されます。データでは、IP アクセス リスト コンフィギュレーションを確認する必要があることも通知されます。この機能をユーザが使用できるようにするには、**ip accounting access-violations** インターフェイス コンフィギュレーション コマンドを使用して、アクセス リストに一致しなかった IP アカウンティングをイネーブルにする必要があります。イネーブルにすると、ユーザは、送信元と宛先のペアのアクセス リストに対してセキュリティ違反を試みた送信元からのバイト数およびパケット数を表示できるようになります。デフォルトでは、IP アカウンティングは、アクセス リストに一致してルーティングされたパケット数を表示します。

MAC アドレス アカウンティング機能は、LAN インターフェイス上の送信元と宛先の MAC アドレスに基づいて IP トラフィックのアカウンティング情報を提供します。MAC アカウンティングは、一意の MAC アドレスとの間で IP パケットを送受信した、LAN インターフェイスの合計のパケット数とバイト数を計算します。また、最後に送受信したパケットのタイムスタンプも記録します。たとえば、IP MAC アカウンティングを使用して、Network Access Profile（NAPS; ネットワーク アクセス プロファイル）/ ピアリング ポイントでさまざまなピアとの間で送受信したトラフィック数を確認できます。IP MAC アカウンティングはイーサネット、ファスト イーサネット、FDDI インターフェイス上でサポートされ、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）、distributed CEF（dCEF）、フロー、および最適なスイッチングをサポートします。

優先順位アカウンティング機能は、任意のインターフェイスの優先順位に基づいて、IP トラフィックのアカウンティング情報を提供します。この機能は、IP パケットを送受信したインターフェイスの合計のパケット数とバイト数を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。

Show and Clear Commands for IOS Sockets

Show and Clear Commands for IOS Sockets 機能には、**show udp**、**show sockets**、and **clear sockets** コマンドが導入されました。これらの新しいコマンドは、Cisco IOS ソケット ライブラリのモニタリングや管理に役立ちます。

Cisco IOS ソフトウェアでは、ソケットはプロセス単位のエンティティです。これは、ソケットの最大数がプロセス単位であり、すべてのソケットはプロセスベースに管理されることを意味します。たとえば、各 Cisco IOS プロセスには、ファイル記述子番号が 1 のソケットを持たせることができます。これは、システム単位にファイル記述子を割り当てる UNIX やその他のオペレーティング システムとは異なります。

show コマンドと **clear** コマンドは、現在の機能と一致するようにプロセス単位に動作します。このため、コマンドによるアクションは、CLI で入力したプロセス ID で指定された特定のプロセスにのみ適用されます。

多くのアプリケーションでは、主にデバッグ目的で **show** コマンドと **clear** コマンドが必要になります。次に、これらのコマンドが役に立つシナリオの例を示します。

- アプリケーション H.323 は、音声呼にソケットを使用しています。現在の呼数から考えると、より多くのソケットに対応できるスペースが残っているはずです。ただし、これ以上、ソケットを開くことができません。このような場合、**show sockets** コマンドを使用して、すべてのソケット スペースを実際に使用しているか、または（利用可能な）未使用のソケットがあるかどうかを調べることができます。
- アプリケーションは特定のソケット イベントが発生するのを待機しています。UDP セグメントが見つかりましたが、アプリケーションはアクティブになりません。このような場合、**show udp** コマンドを使用して、モニタされているイベントのリストを表示し、UDP ソケット イベントがモニタされているか、またはソケット ライブラリがアプリケーションのアクティブ化に失敗していないかを判断することができます。
- アプリケーションは、特定のプロセスに関するすべてのソケットを閉じようとしています。このような場合、**clear sockets** コマンドを使用して、ソケットと、その下位にある TCP/UDP 接続または Stream Control Transmission Protocol（SCTP）アソシエーションの両方を閉じることができます。

IP サービスの設定方法

ここでは、次の各手順について説明します。

- 「ネットワークの DoS 攻撃からの保護」（P.7）
- 「ICMP Unreachable Rate Limiting User Feedback の設定」（P.8）
- 「MTU パケット サイズの設定」（P.10）
- 「IP アカウンティングの設定」（P.11）
- 「IP ネットワークのモニタリングとメンテナンス」（P.13）

ネットワークの DoS 攻撃からの保護

ICMP は、パス、ルート、ネットワーク状態に関する情報をリレーする方法で、IP トラフィックをサポートします。ICMP メッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。IP ソース ルーティングを使用して、送信元 IP ホストは IP ネットワーク上のルートを指定することができます。IP ソース ルーティングがネットワークでの正規の目的に使用されることはめったにありません。古い IP 実装では、ソース - ルート パケットが適切に処理されないことがあり、ソース ルーティング オプションを指定してデータグラムに送信することで、これらの実装を実行するデバイスがクラッシュすることがあります。

可能である限り、ICMP メッセージと IP ソース ルーティングはディセーブルにしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip source-route**
4. **interface** *type/number*

5. **no ip unreachables**
6. **no ip redirects**
7. **no ip mask-reply**

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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `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 3	**no ip source-route** 例： `Router(config)# no ip source-route`	IP ソース ルーティングをディセーブルにします。
ステップ 4	**interface** *type*/*number* 例： `Router(config)# interface null 0`	設定するインターフェイスを指定し、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 5	**no ip unreachables** 例： `Router(config-if)# no ip unreachables`	到達不能な ICMP プロトコルとホスト到達不能メッセージの送信をディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。 **（注）** 到達不能メッセージをディセーブルにすると、IP PMTUD もディセーブルになります。パス ディスカバリが Cisco IOS ソフトウェアにより到達不能メッセージを送信するためです。
ステップ 6	**no ip redirects** 例： `Router(config-if)# no ip redirects`	ルートを学習するため、ICMP リダイレクト メッセージの送信をディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。
ステップ 7	**no ip mask-reply** 例： `Router(config-if)# no ip mask-reply`	ICMP マスク応答メッセージの送信をディセーブルにします。

ICMP Unreachable Rate Limiting User Feedback の設定

このタスクは、到達不能宛先パケットの統計情報をすべてクリアし、到達不能宛先メッセージの間隔を指定するために実行します。このタスクでは、パケット カウンタ（しきい値）と、コンソールへのロギング メッセージをトリガーする間隔も設定します。このタスクは、しきい値を設定した後に新しくロギングを開始する場合に有用です。

手順の概要

1. **enable**
2. **clear ip icmp rate-limit** [*interface-type interface-number*]
3. **configure terminal**
4. **ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]
5. **exit**
6. **show ip icmp rate-limit** [*interface-type interface-number*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ip icmp rate-limit** [*interface-type interface-number*] **例：** `Router# clear ip icmp rate-limit ethernet 2/3`	設定されたすべてのインターフェイスに関する、現在の ICMP 到達不能統計情報をすべてクリアします。オプションの *interface-type* 引数と *interface-number* 引数を使用すると、1 つのインターフェイスに関する統計情報のみがクリアされます。
ステップ 3	**configure terminal** **例：** `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 4	**ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]] **例：** `Router(config)# ip icmp rate-limit unreachable df log 1100 12000`	メッセージ生成について、ICMP 到達不能宛先メッセージのレート制限と、エラー メッセージ ログのしきい値を指定します。デフォルトでは、0.5 秒の間に 2 つ以上の到達不能メッセージが送信されないようにします。 引数およびキーワードは次のとおりです。 • **df**：（任意）ICMP ヘッダーに「Don't Fragment」（DF）ビットが設定されていると、データグラムのフラグメンテーションは行われません。**df** キーワードを指定しないと、その他のすべてのタイプの宛先到達不能メッセージが送信されます。 • *ms*：（任意）到達不能メッセージが生成される間隔。有効範囲は 1 ～ 4294967295 です。 • **log**：（任意）エラー メッセージのリスト。具体的な引数は次のとおりです。 – *packets*：（任意）ログ生成のしきい値を決定するパケット数。デフォルト値は 1000 です。 – *interval-ms*：（任意）ロギング メッセージがトリガーさえる間隔の時間制限。デフォルトは 60000（1 分）です。 **（注）** コマンドを設定するとすぐにカウントが開始します。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router# exit`	特権 EXEC モードに戻ります。
ステップ 6	**show ip icmp rate-limit** [*interface-type interface-number*] **例：** `Router# show ip icmp rate-limit ethernet 2/3`	（任意）設定されたすべてのインターフェイスに関する、現在の ICMP 到達不能統計情報をすべて表示します。オプションの *interface-type* 引数と *interface-number* 引数を使用すると、1 つのインターフェイスに関する統計情報のみが表示されます。

例

次に、インターフェイスに到達不能な宛先を表示する **show ip icmp rate-limit** コマンドの出力例を示します。

```
Router# show ip icmp rate-limit

                          DF bit unreachables       All other unreachables
Interval (millisecond)    500                       500

Interface                 # DF bit unreachables     # All other unreachables
---------                 ---------------------     ------------------------
Ethernet0/0               0                         0
Ethernet0/2               0                         0
Serial3/0/3               0                         19

The greatest number of unreachables is on serial interface 3/0/3.
```

MTU パケット サイズの設定

すべてのインターフェイスには、デフォルト MTU パケット サイズが設定されています。Cisco IOS ソフトウェアがインターフェイスに設定されている MTU サイズを超える IP パケットのフラグメンテーションを行うように、IP MTU サイズを調整することができます。

MTU 値を変更すると（**mtu** インターフェイス コンフィギュレーション コマンドを使用）、IP MTU 値に影響を及ぼします。現在の IP MTU 値が MTU 値と同じである場合に MTU 値を変更すると、IP MTU 値は新しい MTU に一致するように自動的に変更されます。ただし、その逆は当てはまりません。つまり、IP MTU 値を変更しても、**mtu** インターフェイス コンフィギュレーション コマンドの値には影響しません。

物理メディア上にあるデバイスでは、正常に動作させるためには同じプロトコル MTU を使用する必要があります。

このタスクは、指定インターフェイスの MTU パケット サイズを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **ip mtu** *bytes*
5. **exit**

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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `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 3	**interface** *type/number* 例： `Router(config)# interface ethernet1/1`	設定するインターフェイスを指定し、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 mtu** *bytes* 例： `Router(config-if)# ip mtu 300`	インターフェイスの IP MTU パケット サイズを設定します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。

IP アカウンティングの設定

IP アカウンティングをイネーブルにするため、このタスクはインターフェイスごとに実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip accounting-threshold** *threshold*
4. **ip accounting-list** *ip-address wildcard*
5. **ip accounting-transits** *count*
6. **interface** *type/number*
7. **ip accounting** [**access-violations**] [**output-packets**]
8. **ip accounting mac-address** {**input** | **output**}
   または
   ip accounting precedence {**input** | **output**}

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `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 3	**ip accounting-threshold** *threshold* **例：** `Router(config)# ip accounting-threshold 500`	（任意）作成するアカウンティング エントリの最大数を設定します。
ステップ 4	**ip accounting-list** *ip-address wildcard* **例：** `Router(config)# ip accounting-list 192.31.0.0 0.0.255.255`	（任意）ホストのアカウンティング情報をフィルタリングします。
ステップ 5	**ip accounting-transits** *count* **例：** `Router(config)# ip accounting-transits 100`	（任意）IP アカウンティング データベースに格納される中継レコードの数を制御します。
ステップ 6	**interface** *type*/*number* **例：** `Router(config)# interface ethernet1/1`	インターフェイスを指定し、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 7	**ip accounting** [**access-violations**] [**output-packets**] **例：** `Router(config-if)# ip accounting access-violations`	基本的な IP アカウンティングをイネーブルにします。 • オプションの **access-violations** キーワードを使用して、IP アクセス リストに一致しなかった IP トラフィックを特定するため IP アカウンティング機能をイネーブルにします。 • オプションの **output-packets** キーワードを使用して、インターフェイス上の IP パケット出力に基づいて IP アカウンティングをイネーブルにします。

ステップ 8	**ip accounting mac-address** {**input** | **output**}
	または
	ip accounting precedence {**input** | **output**}
	
	例：
	`Router(config-if)# ip accounting mac-address output`
	または
	
	例：
	`Router(config-if)# ip accounting precedence output`
		（任意）受信（入力）または送信（出力）パケットの MAC アドレスに基づいて IP アカウンティングを設定します。
		または
		（任意）受信（入力）または送信（出力）パケットの優先順位に基づいて IP アカウンティングを設定します。

IP ネットワークのモニタリングとメンテナンス

IP ルーティング テーブル、キャッシュ、データベース、ソケット プロセスの内容など、特定の統計情報を表示できます。結果の情報を使用して、リソースの活用法を判断したり、ネットワーク問題を解決したりできます。

IP ネットワークのモニタリングとメンテナンスを行うには、このタスクの任意の手順を実行してください。

手順の概要

1. **clear ip traffic**
2. **clear ip accounting** [**checkpoint**]
3. **clear sockets** *process-id*
4. **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]
5. **show interface** [*type number*] **mac**
6. **show interface** [*type number*] **precedence**
7. **show ip redirects**
8. **show ip sockets**
9. **show sockets** *process-id* [**detail**] [**events**]
10. **show udp** [**detail**]
11. **show ip traffic**

（注） Cisco IOS リリース 12.4(11)T および以降のリリースでは、**show ip sockets** コマンドは **show udp**、**show sockets**、および **show ip sctp** コマンドに置き換えられました。**show ip sctp** コマンドの詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。

ステップ 1　clear ip traffic

すべてのインターフェイス上にあるすべての IP トラフィック統計カウンタをクリアするには、次のコマンドを使用します。

```
Router# clear ip traffic
```

ステップ 2　clear ip accounting [checkpoint]

特定のキャッシュ、テーブル、データベースのすべての内容を削除できます。キャッシュ、テーブル、またはデータベースは、特定の構造が無効になったり、無効になるおそれのあるときにクリアすることが必要になります。IP アカウンティングがイネーブルであるときにアクティブな IP アカウンティング データベースをクリアするには、次のコマンドを使用します。

```
Router# clear ip accounting
```

IP アカウンティングがイネーブルであるときにチェックポイントが作成された IP アカウンティング データベースをクリアするには、次のコマンドを使用します。

```
Router# clear ip accounting checkpoint
```

ステップ 3　clear sockets *process-id*

すべての IP ソケットを閉じ、その下位にあるトランスポート接続と特定のプロセスのデータ構造をクリアするには、次のコマンドを使用します。

```
Router# clear sockets 35

All sockets (TCP, UDP and SCTP) for this process will be cleared.
Do you want to proceed? [yes/no]: y
Cleared sockets for PID 35
```

ステップ 4 **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]

アクセス リストの不一致を表示するには、**show ip accounting** コマンドを使用します。このコマンドを使用するには、まず、インターフェイス ベースで IP アカウンティングをイネーブルにする必要があります。

チェックポイント データベースを表示するには、**checkpoint** キーワードを使用します。アクセス コントロールと一致し、ルーティングを表示する必要のあるパケットに関する情報を指定するには、**output-packets** キーワードを使用します。送信元と宛先のペアの最後のパケットで一致しなかったアクセス リストの数を表示するには、**access-violations** キーワードを使用します。パケット数により、特定の宛先に対する攻撃の状況（攻撃の強さなど）が明らかになります。**access-violations** キーワードを指定しないと、このコマンドでは、デフォルトで、アクセス リストに一致してルーティングされたパケット数が表示されます。

output-packets キーワードと **access-violations** キーワードのどちらも指定しない場合は、デフォルトで output-packets が使用されます。

次に、**show ip accounting** コマンドの出力例を示します。

```
Router# show ip accounting

   Source           Destination              Packets               Bytes
 172.16.19.40    192.168.67.20                  7                 306
 172.16.13.55    192.168.67.20                 67                2749
 172.16.2.50     192.168.33.51                 17                1111
 172.16.2.50     172.31.2.1                     5                 319
 172.16.2.50     172.31.1.2                   463               30991
 172.16.19.40    172.16.2.1                     4                 262
 172.16.19.40    172.16.1.2                    28                2552
 172.16.20.2     172.16.6.100                  39                2184
 172.16.13.55    172.16.1.2                    35                3020
 172.16.19.40    192.168.33.51               1986                95091
 172.16.2.50     192.168.67.20                233                14908
 172.16.13.28    192.168.67.53                390                24817
 172.16.13.55    192.168.33.51             214669              9806659
 172.16.13.111   172.16.6.23               27739              1126607
 172.16.13.44    192.168.33.51              35412              1523980
 192.168.7.21    172.163.1.2                   11                 824
 172.16.13.28    192.168.33.2                  21                1762
 172.16.2.166    192.168.7.130                797              141054
 172.16.3.11     192.168.67.53                  4                 246
 192.168.7.21    192.168.33.51              15696              695635
 192.168.7.24    192.168.67.20                 21                 916
 172.16.13.111   172.16.10.1                   16                1137
 accounting threshold exceeded for 7 packets and 433 bytes
```

次に、**show ip accounting access-violations** コマンドの出力例を示します。アクセス リストに一致せず、ルーティングされなかったパケットが出力されます。

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
172.16.19.40    192.168.67.20              7          306         77
172.16.13.55    192.168.67.20             67         2749        185
172.16.2.50     192.168.33.51             17         1111        140
172.16.2.50     172.16.2.1                 5          319        140
172.16.19.40    172.16.2.1                 4          262         77
```

```
Accounting data age is 41
```

ステップ 5 **show interface** [*type number*] **mac**

MAC アカウンティング用に設定されたインターフェイスの情報を表示するには、**show interface mac** コマンドを使用します。次に、**show interface mac** コマンドの出力例を示します。

```
Router# show interface ethernet 0/1 mac

Ethernet0/1
Input  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2684ms ago
Total:  4 packets, 456 bytes
Output  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2692ms ago
Total:  4 packets, 456 bytes
```

ステップ 6 **show interface** [*type number*] **precedence**

優先順位アカウンティング用に設定されたインターフェイスの情報を表示するには、**show interface precedence** コマンドを使用します。

次に、**show interface precedence** コマンドの出力例を示します。この例では、合計のパケット数とバイト数は IP パケットを受信（入力）または送信（出力）するインターフェイスについて算出され、結果は IP 優先順位に基づいてソートされます。

```
Router# show interface ethernet 0/1 precedence

Ethernet0/1
Input
Precedence 0:  4 packets, 456 bytes
Output
Precedence 0:  4 packets, 456 bytes
```

ステップ 7 **show ip redirects**

デフォルト ルータのアドレスおよび ICMP リダイレクト メッセージを受信するホストのアドレスを表示するには、**show ip redirects** コマンドを使用します。

次に、**show ip redirects** コマンドの出力例を示します。

```
Router# show ip redirects

Default gateway is 172.16.80.29

Host               Gateway           Last Use    Total Uses  Interface
172.16.1.111      172.16.80.240        0:00             9  Ethernet0
172.16.1.4        172.16.80.240        0:00             4  Ethernet0
```

ステップ 8 **show ip sockets**

IP ソケット情報を表示し、使用しているソケットが正しく開いていることを確認するには、**show ip sockets** コマンドを使用します。ローカルとリモートのエンドポイントがある場合は、特定されたポートを使用して接続が確立されます。

次に、**show ip sockets** コマンドの出力例を示します。

```
Router# show ip sockets

Proto    Remote          Port      Local           Port  In Out Stat TTY OutputIF
 17      10.0.0.0          0       172.16.186.193  67    0   0    1   0
 17      172.16.191.135   514      172.16.191.129  1811  0   0    0   0
 17      172.16.135.20    514      172.16.191.1    4125  0   0    0   0
 17      172.16.207.163   49       172.16.186.193  49    0   0    9   0
 17      10.0.0.0         123      172.16.186.193  123   0   0    1   0
 88      10.0.0.0         0        172.16.186.193  202   0   0    0   0
```

```
 17      172.16.96.59     32856   172.16.191.1    161   0   0    1   0
 17     --listen--             --any--        496  0    0   1    0
```

ステップ 9 **show sockets** *process-id* [**detail**] [**events**]

現在開いているソケットの数を表示し、*process-id* 引数を指定してトランスポート プロトコル プロセスに関する配信状況を表示するには、**show sockets** コマンドを使用します。次に、指定したプロセスで開いているソケットの総数を示す **show sockets** コマンドの出力例を示します。

```
Router# show sockets 35

Total open sockets - TCP:7, UDP:0, SCTP:0
```

次に、開いている同じプロセスについて、**detail** キーワードを使用して情報を表示した場合の出力例を示します。

```
Router# show sockets 35 detail

   FD LPort FPort Proto Type    TransID

   0  5000  0     TCP   STREAM  0x6654DEBC
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   1  5001  0     TCP   STREAM  0x6654E494
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   2  5002  0     TCP   STREAM  0x656710B0
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   3  5003  0     TCP   STREAM  0x65671688
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   4  5004  0     TCP   STREAM  0x65671C60
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   5  5005  0     TCP   STREAM  0x65672238
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   6  5006  0     TCP   STREAM  0x64C7840C
State: SS_ISBOUND
Options: SO_ACCEPTCONN

Total open sockets - TCP:7, UDP:0, SCTP:0
```

次に、IP ソケット イベント情報を表示する例を示します。

```
Router# show sockets 35 events

Events watched for this process: READ
FD Watched Present Select Present

0 --- --- R-- R--
```

ステップ 10 **show udp** [**detail**]

UDP プロセスに関する IP ソケット情報を表示するには、**show udp** コマンドを使用します。次に、UDP ソケットに関する詳細情報を表示する例を示します。

```
Router# show udp detail

 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  67    0  0   2211 0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  2517  0   0  11   0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5000  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5001  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5002  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5003  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5004  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
```

（注） Cisco IOS リリース 12.4(11)T および以降のリリースでは、**show ip sockets** コマンドは **show udp**、**show sockets**、および **show ip sctp** コマンドに置き換えられました。**show ip sctp** コマンドの詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。

ステップ 11 show ip traffic

IP プロトコル統計情報を表示するには、**show ip traffic** コマンドを使用します。次に、**clear ip traffic** コマンドでクリアされた IP トラフィック統計情報の例を示します。

```
Router# clear ip traffic
Router# show ip traffic

IP statistics:
 Rcvd:  0 total, 0 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options, 0 with options
 Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
        0 timestamp, 0 extended security, 0 record route
        0 stream ID, 0 strict source route, 0 alert, 0 cipso
        0 other
 Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 couldn't fragment
 Bcast: 0 received, 0 sent
 Mcast: 0 received, 0 sent
 Sent: 0 generated, 0 forwarded
 Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 0 unicast RPF, 0 forced drop

ICMP statistics:
```

```
 Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
       0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
       0 parameter, 0 timestamp, 0 info request, 0 other
       0 irdp solicitations, 0 irdp advertisements
 Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
       0 mask requests, 0 mask replies, 0 quench, 0 timestamp
       0 info reply, 0 time exceeded, 0 parameter problem
       0 irdp solicitations, 0 irdp advertisements

UDP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total, 0 forwarded broadcasts

TCP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total

Probe statistics:
 Rcvd: 0 address requests, 0 address replies
       0 proxy name requests, 0 where-is requests, 0 other
 Sent: 0 address requests, 0 address replies (0 proxy)
       0 proxy name replies, 0 where-is replies

EGP statistics:
 Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
 Sent: 0 total

IGRP statistics:
 Rcvd: 0 total, 0 checksum errors
 Sent: 0 total

OSPF statistics:
 Rcvd: 0 total, 0 checksum errors
       0 hello, 0 database desc, 0 link state req
       0 link state updates, 0 link state acks

 Sent: 0 total

IP-IGRP2 statistics:
 Rcvd: 0 total
 Sent: 0 total

PIMv2 statistics: Sent/Received
 Total: 0/0, 0 checksum errors, 0 format errors
 Registers: 0/0, Register Stops: 0/0, Hellos: 0/0
 Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
 Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0

IGMP statistics: Sent/Received
 Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
 Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
DVMRP: 0/0, PIM: 0/0
```

IP サービスの設定例

ここでは、次の IP 設定例について説明します。

- 「ネットワークの DoS 攻撃からの保護：例」（P.19）
- 「ICMP 到達不能宛先カウンタの設定：例」（P.19）
- 「MTU パケット サイズの設定：例」（P.19）

ネットワークの DoS 攻撃からの保護：例

次に、ネットワーク マッピング情報を取得することを目的とした攻撃者によって利用されることがあるパス、ルート、ネットワーク状態に関する情報を ICMP がリレーしないようにするために、イーサネット インターフェイス 0/0 の ICMP のデフォルトの一部を変更する例を示します。

到達不能メッセージをディセーブルにすると、IP PMTUD もディセーブルになります。パス ディスカバリが Cisco IOS ソフトウェアにより到達不能メッセージを送信するためです。少数のデバイスのあるネットワーク セグメントがあり、絶対的な信頼性のあるトラフィック パターン（めったに使用されないユーザ デバイスが少数あるようなセグメントで発生しやすい）がある場合は、デバイスがどのような方法でも利用される可能性のなさそうなデバイス オプションを無効にします。

```
configure terminal
no ip source-route
interface ethernet 0/0
 no ip unreachables
 no ip redirects
 no ip mask-reply
```

ICMP 到達不能宛先カウンタの設定：例

次に、到達不能宛先パケット統計情報をすべてクリアし、到達不能宛先メッセージの間隔を指定する場合の例を示します。この例では、パケット カウンタのしきい値と、コンソールへのロギング メッセージをトリガーする間隔も設定します。

```
clear ip icmp rate-limit ethernet 0/0
configure terminal
 ip icmp rate-limit unreachable df log 1100 12000
```

MTU パケット サイズの設定：例

次に、イーサネット インターフェイス 0/0 のデフォルトの MTU パケット サイズを設定する例を示します。

```
configure terminal
interface ethernet 0/0
 ip mtu 300
```

IP アカウンティングの設定：例

次に、送信元と宛先の MAC アドレス、および送受信するパケットの IP 優先順位に基づいて IP アカウンティングをイネーブルにする例を示します。

```
configure terminal
 interface ethernet0/5
 ip accounting mac-address input
 ip accounting mac-address output
 ip accounting precedence input
 ip accounting precedence output
```

次に、アクセス リストに一致しない IP トラフィックを特定する機能を使用し、また IP アカウンティング データベースに格納される中継レコードの数を 100 に指定して、アカウンティングをイネーブルにする例を示します。

```
configure terminal
 ip accounting-transits 100
 interface ethernet0/5
  ip accounting output-packets
  ip accounting access-violations
```

その他の参考資料

IP サービスに関連する参考資料については、次の各項を参照してください。

関連資料

内容	参照先
IP アドレッシングとサービス設定作業	『*Cisco IOS IP Addressing Services Configuration Guide*』
IP アクセス リスト	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Access Control Lists (ACLs)」
IP アプリケーション サービス コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』

RFC

RFC	タイトル
RFC 791	「*Internet Protocol*」
RFC 792	「*Internet Control Message Protocol*」
RFC 1191	「*Path MTU discovery*」

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 登録ユーザの場合は、次のページからログインしてさらに多くのコンテンツにアクセスできます。	http://www.cisco.com/techsupport

IP サービスの機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

ここに記載のないテクノロジーの機能の詳細については、「Cisco IOS IP Application Services Features Roadmap」または「FHRP Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IP サービスの機能情報

機能名	リリース	機能情報
Clear IP Traffic CLI	12.4(2)T 12.2(31)SB2	Clear IP Traffic CLI 機能で、**clear ip traffic** コマンドが導入されました。これにより、ルータをリロードするのではなく、ルータ上のすべての IP トラフィック統計情報がクリアされるようになりました。安全性を高めるため、このコマンドを入力すると、ユーザに確認プロンプトが表示されます。 この機能は、Cisco IOS リリース 12.4(2)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 • 「IP ネットワークのモニタリングとメンテナンス」（P.13） コマンド **clear ip traffic** がこの機能により導入されました。

表 1　IP サービスの機能情報（続き）

機能名	リリース	機能情報
ICMP Unreachable Rate Limiting User Feedback	12.4(2)T 12.2(31)SB2	ICMP Unreachable Rate Limiting User Feedback 機能により、到達不能な宛先であるために破棄されたパケットをクリアして表示することができます。エラー メッセージをトリガーするしきい値の間隔を設定できます。メッセージ ロギングが生成されると、コンソールに表示されます。 この機能は、Cisco IOS リリース 12.4(2)T で導入されました。 この機能に関する詳細については、次の各項を参照してください。 • 「ICMP の概要」（P.2） • 「サービス拒否攻撃」（P.4） • 「ICMP Unreachable Rate Limiting User Feedback の設定」（P.8） • 「ネットワークの DoS 攻撃からの保護：例」（P.19） **clear ip icmp rate-limit**、**ip icmp rate-limit unreachable**、**show ip icmp rate-limit** の各コマンドがこの機能により導入または変更されました。
IP Precedence Accounting	12.2(21) 12.1(27b)E1 12.1(5)T15 12.2(25)S 12.2(33)SRA 12.2(18)SXF13 12.2(33)SXH1	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスの合計のパケット数とバイト数を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「IP MAC アカウンティングと優先順位アカウンティング」（P.6） • 「IP アカウンティングの設定：例」（P.19） **show interface precedence** および **ip accounting precedence** の各コマンドがこの機能により導入されました。

表 1　IP サービスの機能情報（続き）

機能名	リリース	機能情報
Show and Clear Commands for IOS Sockets	12.4(11)T	Show and Clear Commands for IOS Sockets 機能には、**show udp**、**show sockets**、and **clear sockets** コマンドが導入されました。これらの新しいコマンドは、Cisco IOS ソケット ライブラリのモニタリングや管理に役立ちます。 この機能に関する詳細については、次の各項を参照してください。 • 「Show and Clear Commands for IOS Sockets」（P.6） • 「IP ネットワークのモニタリングとメンテナンス」（P.13） **clear sockets**、**show sockets**、**show udp** の各コマンドがこの機能により導入または変更されました。 コマンド **show ip sockets** がこの機能により置換されました。