Novell IPX の設定

Configuring Novell IPX

Cisco IOS ソフトウェアは、さまざまなルーティング プロトコルをサポートしています。Novell Internetwork Packet Exchange（IPX）は、Xerox Network Services（XNS）Internet Datagram Protocol（IDP; インターネット データグラム プロトコル）から派生したものです。このマニュアルでは、IP および IP ルーティングのための Novell IPX ネットワーク プロトコルについて説明します。

このマニュアルでは、Novell Internetwork Packet Exchange（IPX）の設定方法について説明し、設定例を示します。この章に記載されている IPX コマンドの詳細については、『*Cisco IOS Novell IPX Command Reference*』を参照してください。この章で使用されたその他のコマンドの詳細については、コマンド リファレンス マスタ インデックスを使用するか、オンラインで検索してください。

機能情報の確認

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、「Novell IPX を設定するための機能情報」（P.126）を参照してください。

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、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。

目次

Novell IPX に関する情報

Novell Internetwork Packet Exchange（IPX）は、Xerox Network Services（XNS）Internet Datagram Protocol（IDP; インターネット データグラム プロトコル）から派生したものです。IPX と XNS には、次の相違点があります。

- IPX と XNS は、必ずしも同じ Ethernet カプセル化形式を使用するとは限りません。
- IPX では、Novell 専用の Service Advertising Protocol（SAP）を使用して、特別なネットワーク サービスをアドバタイズします。ファイル サーバとプリント サーバは、アドバタイズされる典型的なサービスの例です。

宛先への最良のパスを決定するためのプライマリ メトリックとして、IPX では遅延（ティックで測定）を使用するのに対し、XNS ではホップ カウントを使用します。

シスコによる Novell IPX プロトコルの実装では、完全な IPX ルーティング機能を提供することが保証されます。さまざまな IPX のサポートおよび IPX アドレスの詳細については、次の各項を参照してください。

- IPX MIB のサポート（P.2）
- IPX Enhanced IGRP のサポート（P.3）
- LANE のサポート（P.3）
- VLAN のサポート（P.3）
- マルチレイヤ スイッチングのサポート（P.3）
- IPX アドレス（P.4）

IPX MIB のサポート

シスコでは IPX MIB をサポートしています（現在は、読み取り専用アクセスをサポート）。IPX アカウンティング グループは、サポートするローカルのシスコ専用 IPX 変数のいずれかを表します。このグループによって、IPX アカウンティングがルータまたはアクセス サーバでイネーブルになっている場合に作成および維持される、アクティブなデータベースにアクセスできます。

IPX Enhanced IGRP のサポート

Cisco IOS ソフトウェアでは、次の機能を提供する IPX Enhanced IGRP がサポートされます。

- 自動再配布：IPX Routing Information Protocol（RIP）のルートは自動的に Enhanced IGRP に再配布され、Enhanced IGRP ルートは自動的に RIP に再配布されます。再配布は、必要に応じてオフにできます。また、デバイスまたは個々のインターフェイスで Enhanced IGRP および IPX RIP を完全にオフにすることもできます。
- ネットワーク規模の拡大：IPX RIP では、自分のネットワークで可能な最大規模が 15 ホップです。Enhanced IGRP がイネーブルになっている場合、最大規模は 224 ホップです。Enhanced IGRP メトリックは何千ものホップをサポートできるだけの大きさがあるため、ネットワークを拡張するうえでの唯一の障壁はトランスポート レイヤのホップ カウンタだけです。シスコは IPX パケットが 15 台のルータを通過し、宛先へのネクスト ホップが Enhanced IGRP を介して学習された場合にだけ、転送コントロール フィールドを増分することによって、この問題を回避しています。RIP ルートが宛先へのネクスト ホップとして使用される場合、転送コントロール フィールドが常に増分されます。
- インクリメンタル SAP 更新：Enhanced IGRP ネイバーが見つかり、その後 SAP テーブルに対して変更が行われた場合だけ、各インターフェイスで完全な SAP の更新が送信されます。この手順は、Enhanced IGRP 高信頼性転送メカニズムを利用して実行します。そのため、インクリメンタル SAP を送信するために、Enhanced IGRP ピアが存在する必要があります。特定のインターフェイスにピアが存在していない場合、ピアが見つかるまで、そのインターフェイスに SAP が定期的に送信されます。この機能はシリアル インターフェイスで自動的に行われ、LAN メディアで設定できます。

LANE のサポート

Cisco IOS ソフトウェアでは、イーサネット エミュレート LAN とトークン リング エミュレーション LAN の間での、IPX のルーティングがサポートされます。エミュレート LAN およびこれらの間での IPX のルーティングの詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Configuring LAN Emulation」の章を参照してください。

VLAN のサポート

Cisco IOS ソフトウェアでは、VLAN 間の IPX のルーティングがサポートされます。Novell NetWare 環境を使用しているユーザは、VLAN の境界を越えて ISL のカプセル化をルーティングする 4 つの IPX イーサネットのカプセル化のいずれかを使用できます。VLAN および ISL でのこれらの間での IPX のルーティングの詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Configuring Routing Between VLANs with ISL Encapsulation」の章を参照してください。

マルチレイヤ スイッチングのサポート

Cisco IOS ソフトウェアでは、IPX Multilayer Switching（MLS; マルチレイヤ スイッチング）がサポートされます。IPX MLS の詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Multilayer Switching」の章を参照してください。

IPX アドレス

IPX ネットワーク アドレスは、*network.node* の形式で表現されるネットワーク番号とノード番号で構成されます。

ネットワーク番号

ネットワーク番号は物理ネットワークを識別します。この番号は 4 バイト（32 ビット）で、IPX インターネットワーク全体で一意にする必要があります。ネットワーク番号は 16 進数で表現されます。指定できる最大桁数は 8 です。

Cisco IOS ソフトウェアでは、8 桁すべてを入力する必要はありません。先頭の 0 は省略できます。

ノード番号

ノード番号はネットワーク上のノードを識別します。この番号は 48 ビットで、4 桁の 16 進数のドット付き 3 ビット バイトで表現されます。

WAN リンクで使用されるルータのノード番号を指定しない場合、Cisco IOS ソフトウェアでは、ノード アドレスとして現在割り当てられているハードウェア MAC アドレスが使用されます。これは最初のイーサネット、トークン リング、または FDDI インターフェイス カードの MAC アドレスです。有効な IEEE インターフェイスがない場合、Cisco IOS ソフトウェアでは、システム クロックに基づく番号を使用してノード番号がランダムに割り当てられます。

IPX アドレスの例

次に、IPX ネットワーク アドレスを設定する例を示します。

```
4a.0000.0c00.23fe
```

この例では、ネットワーク番号が 4a（正確には 0000004a）で、ノード番号が 0000.0c00.23fe です。アドレスのすべての桁が 16 進数です。

Novell IPX の設定方法

IPX ルーティングを設定するには、ここで説明するタスクを実行します。

- IPX ルーティングの設定（P.5）（必須）
- IPX Enhanced IGRP の設定（P.12）（任意）
- WAN での IPX および SPX の設定（P.31）（任意）
- IPX ネットワークへのアクセスの制御（P.35）（任意）
- IPX ネットワーク パフォーマンスの調整（P.54）（任意）
- IPX ネットワークのシャットダウン（P.95）（任意）
- IPX アカウンティングの設定（P.98）（任意）
- LAN 間の IPX の設定（P.100）（任意）
- VLAN 間の IPX の設定（P.101）（任意）
- IPX マルチレイヤ スイッチングの設定（P.101）（任意）
- IPX ネットワークのモニタリングおよびメンテナンス（P.101）（任意）

IPX ルーティングの設定

IPX ルーティングを設定するには、最初にルータでイネーブルにしてから、各インターフェイスで設定します。

必要に応じて、一部のインターフェイスで IPX をルーティングし、他のインターフェイスに透過的にブリッジすることもできます。また、ルーティングされるインターフェイスとブリッジ グループの間で IPX トラフィックをルーティングすることや、ブリッジ グループ間で IPX トラフィックをルーティングすることもできます。

IPX ルーティングを設定するには、ここで説明するタスクを実行します。最初の 2 つの作業は必須で、残りの作業は任意です。

- IPX ルーティングのイネーブル化（P.5）（必須）
- 個々のインターフェイスへのネットワーク番号の割り当て（P.6）（必須）
- ルーティングとブリッジングの同時イネーブル化（P.11）（任意）
- Integrated Routing and Bridging の設定（P.12）（任意）

IPX デフォルト ルート

IPX では、*デフォルト ルート*とは、宛先アドレスへのルートが不明なすべてのパケットが転送されるネットワークです。

元の Routing Information Protocol（RIP）の実装では、ネットワーク内の通常のネットワーク番号として、ネットワーク -2（0xFFFFFFFE）の使用が許可されていました。NetWare Link Services Protocol（NLSP; NetWare リンク サービス プロトコル）の開始時に、ネットワーク -2 が NLSP および RIP のデフォルト ルートとして予約されます。NLSP ルータと RIP ルータの両方で、ネットワーク -2 がデフォルト ルートとして扱われている必要があります。したがって、IPX ネットワークで NLSP を設定しているかどうかに関係なく、ネットワーク -2 をデフォルト ルートとして実装する必要があります。

デフォルトでは、Cisco IOS ソフトウェアでネットワーク -2 がデフォルト ルートとして扱われます。IPX ネットワークで、ネットワーク -2 が通常のネットワークとして使用されないことを確認する必要があります。何らかの理由で、ネットワーク -2 を通常のネットワークとして使用する必要がある場合、デフォルトの動作をディセーブルにすることができます。方法については、この章の「デフォルト ルートの調整」を参照してください。

IPX のデフォルトのルートを処理する方法に関する詳細な背景情報については、Novell の『*NetWare Link Services Protocol（NLSP）Specification, Revision 1.1*』を参照してください。

IPX ルーティングのイネーブル化

IPX ルーティングをイネーブルにするための最初の手順は、ルータをイネーブルにすることです。WAN リンクで使用されるルータのノード番号を指定しない場合、Cisco IOS ソフトウェアでは、ノード アドレスとして現在割り当てられているハードウェア MAC アドレスが使用されます。これは最初のイーサネット、トークン リング、または FDDI インターフェイス カードの MAC アドレスです。有効な IEEE インターフェイスがない場合、Cisco IOS ソフトウェアでは、システム クロックに基づく番号を使用してノード番号がランダムに割り当てられます。

次の手順では、グローバル コンフィギュレーション モードで IPX ルーティング コマンドをイネーブルにする方法を説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx routing** [*node*]
4. **end**

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。 • 必要に応じて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	**ipx routing** [*node*] **例：** `Router(config)# ipx routing node1`	IPX ルーティングをイネーブルにします。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IPX ルーティングをイネーブルにする方法の例については、この章の最後にある「IPX ルーティングの例」の項を参照してください。

注意 DECnet と IPX ルーティングを同じインターフェイスで同時に使用するように計画する場合、まず DECnet ルーティングをイネーブルにして、その後、オプションの MAC ノード番号を指定せずに IPX ルーティングをイネーブルにする必要があります。DECnet ルーティングをイネーブルにする前に IPX をイネーブルにした場合は、MAC レベルのノード番号の変更が強制されるため、IPX のルーティングが妨害されます。

個々のインターフェイスへのネットワーク番号の割り当て

IPX ルーティングをイネーブルにした後、個々のインターフェイスにネットワーク番号を割り当てることによって、インターフェイスごとに IPX ルーティングをイネーブルにします。

IPX ルーティングは、単一のネットワークまたは複数のネットワークがサポートされるインターフェイスでイネーブルにします。

インターフェイスで IPX ルーティングをイネーブルにすると、ネットワーク上で送信されるパケットに使用するカプセル化（フレーム タイプ）を指定することもできます。表 1 に、IEEE インターフェイスで使用できるカプセル化のタイプ、およびカプセル化のタイプのためのシスコの命名規則と Novell の命名規則の間の対応を示します。

表 1　Cisco と Novell IPX の IEEE インターフェイスでのカプセル化の名前

インターフェイス タイプ	シスコの名前	Novell の名前
イーサネット	novell-ether（Cisco IOS のデフォルト） arpa sap snap	Ethernet_802.3 Ethernet_II Ethernet_802.2 Ethernet_Snap
トークンリング	sap（Cisco IOS のデフォルト） snap	Token-Ring Token-Ring_Snap
FDDI	snap（Cisco IOS のデフォルト） sap novell-fddi	Fddi_Snap Fddi_802.2 Fddi_Raw

（注）SNAP カプセル化タイプはサポートされません。FDDI-Ethernet ブリッジに接続された IPX インターフェイスでは設定しないでください。

個々のインターフェイス タスク リストへのネットワーク番号の割り当て

ここでは、単一のネットワークがサポートされるインターフェイスおよび複数のネットワークがサポートされるインターフェイスで、IPX ルーティングをイネーブルにする方法を説明します。インターフェイスで IPX ルーティングをイネーブルにするには、次のタスクのいずれかを実行する必要があります。

- 単一のネットワークがサポートされるインターフェイスへのネットワーク番号の割り当て（P.7）（必須）
- 複数のネットワークがサポートされるインターフェイスへのネットワーク番号の割り当て（P.8）（必須）
- サブインターフェイスのカプセル化のタイプの設定（P.9）（必須）

単一のネットワークがサポートされるインターフェイスへのネットワーク番号の割り当て

単一のインターフェイスで、単一のネットワークまたは複数の論理ネットワークをサポートできます。単一のネットワークの場合、カプセル化のタイプを設定できます。当然ながら、ネットワーク番号を使用するサーバとクライアントのカプセル化のタイプと一致している必要があります。

単一のネットワークがサポートされるインターフェイスにネットワーク番号を割り当てるには、インターフェイス 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. **interface** *type number*
4. **ipx network** *network* [**encapsulation** *encapsulation-type*]
5. **end**

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。 • 必要に応じて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 POS3/0`	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 4	**ipx network** *network* [**encapsulation** encapsulation-type] **例：** `Router(config-if)# ipx network 4325 encapsulation hdlc`	IPX ルーティングをイネーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

カプセル化のタイプを指定する場合、ネットワーク上のサーバおよびクライアントで使用されるものと同じタイプを選択してください。Novell-ether または ARPA のカプセル化は、FDDI-Ethernet でブリッジされた IPX トラフィックには使用できません。FDDI-Ethernet ブリッジに接続されている発信元および宛先の IPX インターフェイスでは、SAP カプセル化を使用します。IEEE インターフェイスで使用できるカプセル化のタイプのリストについては、表 1 を参照してください。

IPX ルーティングをイネーブルにする方法の例については、この章の「IPX ルーティング：例」の項を参照してください。

複数のネットワークがサポートされるインターフェイスへのネットワーク番号の割り当て

複数のネットワークがサポートされるインターフェイスにネットワーク番号を割り当てる場合、各ネットワークに異なるカプセル化のタイプを指定する必要があります。複数のネットワークが物理メディアを共有するため、Cisco IOS ソフトウェアで各ネットワークに属しているパケットを識別できます。たとえば、イーサネットでは 4 つのカプセル化のタイプがサポートされるため、1 本のイーサネット ケーブルで最大 4 つの IPX ネットワークを設定できます。同じネットワーク番号を使用するサーバとクライアントのカプセル化のタイプと一致している必要があります。IEEE インターフェイスで使用できるカプセル化のタイプのリストについては、表 1 を参照してください。

複数のネットワークがサポートされるインターフェイスにネットワーク番号を割り当てる方法は 2 とおりあります。サブインターフェイスまたは、プライマリネットワークおよびセカンダリ ネットワークを使用できます。

サブインターフェイスのカプセル化のタイプの設定

通常、複数のネットワークがサポートされるインターフェイスにネットワーク番号を割り当てるには、サブインターフェイスを使用します。

*サブインターフェイス*とは、単一の物理インターフェイスで複数の論理インターフェイスまたは複数の論理ネットワークをサポートできるようにするためのメカニズムです。つまり、複数の論理インターフェイスまたは複数の論理ネットワークを、単一のハードウェア インターフェイスに関連付けることができます。各サブインターフェイスで個別カプセル化を使用する必要があり、カプセル化が同じネットワーク番号を使用するクライアントおよびサーバのカプセル化と一致している必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number subinterface-number*
4. **ipx network** *network* [**encapsulation** *encapsulation-type*]
5. **end**

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。 • 必要に応じて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 subinterface-number* **例：** `Router(config)# interface ethernet 0.2`	サブインターフェイスを指定します。
ステップ 4	**ipx network** *network* [**encapsulation** encapsulation-type] **例：** `Router(config-if)# ipx network 4325 encapsulation hdlc`	IPX ルーティングをイネーブルにして、最初のカプセル化のタイプを指定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

（注） **ipx network** コマンドを使用して、1 台のルータで 200 を超える IPX インターフェイスを設定することはできません。

複数のサブインターフェイスを設定するには、この 2 つの手順を繰り返します。IEEE インターフェイスで使用できるカプセル化のタイプのリストについては、表 1 を参照してください。

インターフェイスで複数の IPX ネットワークを設定する例については、この章の「複数ネットワークでの IPX ルーティング：例」の項を参照してください。

プライマリ ネットワークとセカンダリ ネットワーク

複数のネットワークがサポートされるインターフェイスにネットワーク番号を割り当てる場合、プライマリ ネットワークとセカンダリ ネットワークも設定できます。

インターフェイス上で設定する最初の論理ネットワークが、*プライマリ ネットワーク*として認識されます。その他のネットワークは*セカンダリ ネットワーク*として認識されます。ここでも、インターフェイス上の各ネットワークで個別カプセル化を使用する必要があり、同じネットワーク番号を使用するクライアントおよびサーバのカプセル化と一致している必要があります。

このインターフェイスで指定するインターフェイス設定パラメータは、すべての論理ネットワークに適用されます。たとえば、ルーティング アップデート タイマーを 120 秒に設定した場合、この値は 4 つのネットワークすべてに使用されます。

プライマリ ネットワークとセカンダリ ネットワークを使用して、インターフェイスで複数の IPX ネットワークを設定するには、インターフェイス 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. **interface** *type number*
4. **ipx network** *network* [**encapsulation** *encapsulation-type*]
5. **ipx network** *network* [**encapsulation** *encapsulation-type*] [**secondary**]
6. **end**

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。 • 必要に応じて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 POS3/0`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipx network** *network* [**encapsulation** *encapsulation-type*] **例：** `Router(config-if)# ipx network 4325 encapsulation hdlc`	プライマリ ネットワークで IPX ルーティングをイネーブルにします。
ステップ 5	**ipx network** *network* [**encapsulation** *encapsulation-type*] [**secondary**] **例：** `Router(config-if)# ipx network 4325 encapsulation hdlc secondary`	セカンダリ ネットワークで IPX ルーティングをイネーブルにします。
ステップ 6	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

複数のセカンダリ ネットワークを設定するには、必要に応じて、これらの手順を繰り返します。IEEE インターフェイスで使用できるカプセル化のタイプのリストについては、表 1 を参照してください。

（注） NLSP をイネーブルにして複数のカプセル化を同じ物理 LAN インターフェイスで設定するには、サブインターフェイスを使用する必要があります。セカンダリ ネットワークは使用できません。

ルーティングとブリッジングの同時イネーブル化

一部のインターフェイスで IPX をルーティングし、他のインターフェイスに透過的にブリッジすることもできます。このタイプのルーティングをイネーブルにするには、同時ルーティングとブリッジングをイネーブルにする必要があります。同時ルーティングとブリッジングをイネーブルにするには、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. **bridge crb**
4. **end**

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。 • 必要に応じて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	**bridge crb** **例：** `Router(config)# bridge crb`	Cisco IOS ソフトウェアで、単一のルータ内の個々のインターフェイスで特定のプロトコルのルーティングとブリッジングの両方をイネーブルにします。
ステップ 4	**end** **例：** `Router(configf)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Integrated Routing and Bridging の設定

Integrated Routing and Bridging（IRB）によって、ユーザはルーティングされるインターフェイスとブリッジ グループの間で IPX トラフィックをルーティングするか、またはブリッジ グループ間で IPX トラフィックをルーティングできます。特に、ローカル トラフィックまたはルーティングできないトラフィックは、同じブリッジ グループ内のブリッジされたインターフェイスの間でブリッジされます。ルーティング可能なトラフィックは、他のルーティングされたインターフェイスまたはブリッジ グループにルーティングされます。IRB を使用すると、次のことを実行できます。

- ブリッジされたインターフェイスからルーティングされたインターフェイスへのパケットのスイッチ
- ルーティングされたインターフェイスからブリッジされたインターフェイスへのパケットのスイッチ
- 同じブリッジ グループ内でのパケットのスイッチ

Integrated Routing and Bridging の設定の詳細については、『*Cisco IOS Bridging and IBM Networking Configuration Guide*』の「Configuring Transparent Bridging」の章を参照してください。

IPX Enhanced IGRP の設定

Enhanced IGRP は、シスコによって開発された Interior Gateway ルーティング Protocol（IGRP）の拡張バージョンです。Enhanced IGRP は、IGRP と同じ距離ベクトル型アルゴリズムおよび距離情報を使用します。ただし、Enhanced IGRP のコンバージェンス プロパティおよび処理効率は、IGRP よりも大幅に改善されています。

コンバージェンス テクノロジーは、SRII International で行われた調査に基づいており、Diffusing Update Algorithm（DUAL）と呼ばれるアルゴリズムを採用しています。このアルゴリズムはルート計算の中で、すべてのインスタンスでのループフリー動作を保証しており、これによって、1 つのトポロ

ジに含まれているすべてのルータの変更を、一度に同期することができます。トポロジの変更によって影響を受けないルータは、再計算で考慮されません。DUAL でのコンバージェンス時間は、他の既存のルーティング プロトコルでのコンバージェンス時間に匹敵します。

Enhanced IGRP 機能

Enhanced IGRP は次の機能を提供します。

- コンバージェンス：DUAL アルゴリズムにより、現在利用可能なルーティング プロトコルと同様にルーティング情報を迅速にコンバージできます。
- 部分的なアップデート：宛先の状態が変わったときに、ルーティング テーブル全体の内容を送信するのではなく、Enhanced EIGRP では変更分のアップデートだけが送信されます。この機能により、Enhanced IGRP パケットに必要な帯域幅が抑制されます。
- IGRP よりも少ない CPU 使用率：更新パケットを受信するたびに、更新パケット全体を処理する必要がありません。
- ネイバー検出メカニズム：この機能は簡単な hello メカニズムで、隣接するルータについて学習する場合に使用します。これはプロトコルに依存します。
- スケーリング：Enhanced EIGRP は大規模なネットワークに合わせてスケーリングできます。

Enhanced IGRP のコンポーネント

Enhanced IGRP には、ここで説明する 4 つの基本的なコンポーネントがあります。

- ネイバー ディスカバリ / 復帰（P.13）
- 高信頼性転送プロトコル（P.13）
- DUAL 有限状態マシン（P.14）
- プロトコル依存モジュール（P.14）

ネイバー ディスカバリ / 復帰

ネイバー ディスカバリ / 復帰とは、ルータが直接接続されているネットワーク上で他のルータを動的に学習するために使用するプロセスです。ルータは、自身のネイバーが到達不可能または動作しなくなった場合も、検出する必要があります。ルータは、定期的に送信することによって、少ないオーバーヘッドでネイバー ディスカバリ / 復帰を行います。

高信頼性転送プロトコル

高信頼性転送プロトコルは、すべてのネイバーに対して Enhanced IGRP パケットを、正しい順序で確実に配信します。このプロトコルは、マルチキャスト パケットおよびユニキャスト パケットのインターミックス送信をサポートしています。Enhanced IGRP パケットの中には、高信頼性で送信する必要があるものと、必要がないものがあります。効率の点から、高信頼性は必要な場合だけ使用してください。たとえば、マルチキャスト機能を備えているマルチアクセス ネットワーク（イーサネットなど）では、すべてのネイバーに対して個別に hello を高信頼性で送信する必要はありません。したがって、Enhanced IGRP はパケット内に、受信者はこのパケットに確認応答する必要がないことを示すともに、単一のマルチキャスト hello を送信します。その他のタイプのパケット（アップデートなど）では、確認応答が必要ですが、このことはパケット内に示されています。非確認応答パケットが保留中の場合、高信頼性転送は、マルチキャスト パケットをすぐに送信するための機能を備えています。この機能により、さまざまな速度のリンクが存在している場合でも、コンバージェンス時間が短く保たれます。

DUAL 有限状態マシン

DUAL 有限状態マシンは、すべてのルート計算に対する決定プロセスを実現します。このマシンは、すべてのネイバーからアドバタイズされたルートをすべて追跡します。DUAL では、ディスタンス情報（メトリックと呼ばれる）を使用して、効率よい、ループフリーのパスを選択します。DUAL はフィージブル サクセサに基づいて、ルーティング テーブルへ挿入するルートを選択します。*サクセサ*は、パケットのフォワーディングに使用するネイバー ルータであり、ルーティング ループに含まれないことが保証された、宛先に対して最もコストの少ないパスを持っています。フィージブル サクセサがないが、宛先をアドバタイズするネイバーが存在する場合は、再計算が行われます。これは、新しいサクセサを定義するためのプロセスです。ルートの再計算に必要な時間は、コンバージェンス時間に影響を与えます。再計算ではプロセッサに負荷がかかります。不要な再計算はしないようにしてください。トポロジ変更が発生すると、DUAL はフィージブル サクセサをテストします。フィージブル サクセサがある場合、検出されたいずれかのフィージブル サクセサを使用して、不要な再計算を防止します。

プロトコル依存モジュール

プロトコル依存モジュールは、ネットワークレイヤのプロトコル特有のタスクを処理します。また、このモジュールは、Enhanced IGRP パケットの解析を行い、新しい情報を受け取ったことを DUAL に通知します。Enhanced IGRP は DUAL にルーティングを決定するよう依頼しますが、結果は IPX ルーティング テーブルに保存されます。また、Enhanced IGRP は他の IPX ルーティング プロトコルによって学習されたルートの再配布も行います。

IPX Enhanced IGRP 設定タスク リスト

IPX Enhanced IGRP をイネーブルにするには、ここで説明するタスクを実行します。最初のタスクのみが必須で、残りの作業は任意です。

- IPX Enhanced IGRP のイネーブル化（P.14）（必須）
- リンク特性のカスタマイズ（P.15）（任意）
- ルーティングとサービス情報の交換のカスタマイズ（P.19）（任意）
- バックアップ サーバの照会（P.30）（任意）

IPX Enhanced IGRP のイネーブル化

IPX Enhanced IGRP ルーティング プロセスを作成するには、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードをそれぞれ開始し、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx router eigrp** *autonomous-system-number*
4. **interface** *type number*
5. **ipx network** {*network-number* | **all**}
6. **end**

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。 • 必要に応じて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	**ipx router eigrp** *autonomous-system-number* **例：** `Router(config)# ipx router eigrp 2345`	Enhanced IGRP ルーティング プロセスをイネーブルにします。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface ethernet0/1`	インターフェイスのタイプを指定し、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	**ipx network** {*network-number* | **all**} **例：** `Router(config-if)# ipx network 234`	ネットワーク上で Enhanced IGRP をイネーブルにします。
ステップ 6	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

複数のネットワークを Enhanced IGRP ルーティング プロセスに関連付けるには、この 2 つの手順を繰り返します。

Enhanced IGRP をイネーブルにする方法の例については、この章の最後にある「IPX Enhanced IGRP の例」の項を参照してください。

リンク特性のカスタマイズ

Enhanced IGRP のリンク特性をカスタマイズできます。ここでは、このようなカスタマイゼーションのタスクについて説明します。

- Enhanced IGRP によって使用されるリンク帯域幅のパーセンテージの設定（P.15）（任意）
- 最大ホップ カウントの設定（P.16）（任意）
- hello パケットとホールド タイムの間隔調整（P.17）（任意）

Enhanced IGRP によって使用されるリンク帯域幅のパーセンテージの設定

デフォルトでは、Enhanced IGRP パケットは、**bandwidth** インターフェイス サブコマンドで設定されたリンク帯域幅の最大 50% を消費します。複数の値が必要な場合、**ipx bandwidth-percent** コマンドを使用します。このコマンドは、別のレベルのリンク使用率が必要な場合、または設定していた帯域幅が実際のリンク帯域幅に合わない（ルート メトリックの計算に影響を与えるように設定されていた可能性がある）場合などに役立ちます。

インターフェイス上で Enhanced IGRP で使用される可能性ある帯域幅の割合を設定するには、インターフェイス 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. **interface** *type number*
4. **ipx bandwidth-percent eigrp** *as-number percent*
5. **end**

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。 • 必要に応じて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# interface ethernet0/1`	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 4	**ipx bandwidth-percent eigrp** *as-number percent* **例：** `Router(config-if)# ipx bandwidth-percent eigrp 2344 456`	インターフェイス上で Enhanced IGRP が使用可能な帯域幅のパーセンテージを設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Enhanced IGRP の帯域幅のパーセンテージを設定する方法の例については、この章の最後にある「IPX Enhanced IGRP の帯域幅の設定例」の項を参照してください。

最大ホップ カウントの設定

（注） 最大ホップ カウント数は調整できますが、Enhanced IGRP の場合はお勧めしません。Enhanced IGRP の最大ホップ数のデフォルト値を使用するようにしてください。

デフォルトでは、ホップ数が 15 を超える IPX パケットは破棄されます。大規模なインターネットワークでは、この最大ホップ数では不十分な場合があります。Enhanced IGRP では最大ホップ数を 254 ホップに増やすことができます。最大ホップ数を変更するには、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. **ipx maximum-hops** *hops*
4. **end**

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。 • 必要に応じて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	**ipx maximum-hops** *hops* **例：** `Router(config)# ipx maximum-hops 134`	RIP 以外のルーティング プロトコルによって到達可能な IPX パケットの最大ホップ数を設定します。また、IPX パケットが廃棄される前に通過できるルータの最大数も設定します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

hello パケットとホールド タイムの間隔調整

hello パケットとホールド タイムの間隔は調整することができます。

ルータは定期的に hello パケットを互いに送信し、直接接続されているネットワーク上の他のデバイスを動的に学習します。ルータはこの情報を使用して、ネイバーを検出し、ネイバーがいつ到達不可能または無効になるかを検出します。

デフォルトでは、hello パケットは 5 秒間隔で送信されます。例外は、低速の非ブロードキャスト マルチアクセス（NBMA）メディアで、デフォルトの hello 間隔は 60 秒です。低速とは、**bandwidth** インターフェイス コンフィギュレーション コマンドで指定されているように、T1 以下のレートのことを指します。高速の NBMA ネットワークに対しては、デフォルトの hello 間隔は 5 秒のままです。

（注） Enhanced IGRP の目的のため、フレーム リレーおよび SMDS ネットワークは NBMA と見なされることもあれば、見なされないこともあります。これらのネットワークは、インターフェイスで物理マルチキャストを使用するように設定されていない場合 NBMA と見なされ、それ以外の場合、NBMA とは見なされません。

自律システム番号によって指定されている、特定の Enhanced IGRP ルーティング プロセスについて、指定のインターフェイス上に、ホールド タイムを設定することができます。ホールド タイムは hello パケット内でアドバタイズされ、ネイバーに対して、送信者が有効であるとみなす期間を示します。デフォルトのホールド タイムは、hello 間隔の 3 倍、つまり 15 秒です。

非常に輻輳した大規模なネットワークでは、すべてのルータがネイバーから hello パケットを受信するには、15 秒では十分ではないことがあります。この場合、ホールド タイムを増やすこともできます。ホールド タイムを増やすには、インターフェイス 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. **interface** *type number*
4. **ipx hold-time eigrp** *autonomous-system-number seconds*
5. **end**

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。 • 必要に応じて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 etherenet0/1`	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 4	**ipx hold-time eigrp** *autonomous-system-number seconds* 例： `Router(config-if)# ipx hold-time eigrp 234 22`	ホールド タイムを設定します。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

hello パケットの間隔を変更するには、インターフェイス 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. **interface** *type number*
4. **ipx hello-interval eigrp** *autonomous-system-number seconds*
5. **end**

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。 • 必要に応じて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 etherenet0/1`	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 4	**ipx hello-interval eigrp** *autonomous-system-number seconds* **例：** `Router(config-if)# ipx hello-interval eigrp 234 22`	hello パケットの間隔を設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

（注） シスコのテクニカル サポート担当者に問い合わせずに、ホールド タイムを調整しないでください。

ルーティングとサービス情報の交換のカスタマイズ

ルーティングとサービス情報の交換をカスタマイズする場合があります。ここでは、このようなカスタマイゼーションのタスクについて説明します。

- ルーティング情報の再配布（P.20）（任意）
- スプリット ホライズンのディセーブル化（P.21）（任意）
- ルーティング アップデートでのルートのアドバタイジングの制御（P.22）（任意）
- ルーティング アップデートの処理の制御（P.23）（任意）

- SAP アップデートの制御（P.24）（任意）
- SAP アップデートでのサービスのアドバタイジングの制御（P.28）（任意）
- SAP アップデートの処理の制御（P.29）（任意）

ルーティング情報の再配布

デフォルトでは、Cisco IOS ソフトウェアが IPX RIP ルートを Enhanced IGRP に、またはその逆方向に再配布します。ルート再配布をディセーブルにするには、IPX ルータ 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. **ipx router eigrp** *number*
4. **no redistribute** {**connected** | **eigrp** *autonomous-system-number* | **rip** | **static** | **floating-static**}
5. **end**

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。 • 必要に応じて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	**ipx router eigrp** *autonomous-system-number* **例：** `Router(config)# ipx router eigrp 2345`	EIGRP の自律番号を指定し、IPX ルータ 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	**no redistribute** {**connected** | **eigrp** autonomous-*system-number* | **rip** | **static** | **floating-static**} `Router(config-ipx-router)# no redistribute eigrp 234`	RIP ルートの Enhanced IGRP への再配布、および Enhanced IGRP ルートの RIP への再配布をディセーブルにします。
ステップ 5	**end** **例：** `Router(config-ipx-router)# end`	IPX ルータ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スプリット ホライズンのディセーブル化

スプリット ホライズンは、Enhanced IGRP アップデートおよびクエリー パケットの送信を制御します。インターフェイス上でスプリット ホライズンがイネーブルになっていると、このインターフェイスが宛先へのネクスト ホップである場合、これらのパケットが宛先に送信されません。

デフォルトでは、すべてのインターフェイス上でスプリット ホライズンがイネーブルになっています。

スプリット ホライズンでは、情報が発生したインターフェイス外部の Cisco IOS ソフトウェアによって、ルートについての情報がアドバタイズされることが防止されます。通常、この動作は、複数のルータの（特にリンクが破損した場合の）通信を最適化します。ただし、非ブロードキャスト ネットワーク（フレーム リレーや SMDS など）では、この動作が適さない状況が発生することがあります。このような状況では、スプリット ホライズンをディセーブルにできます。

スプリット ホライズンをディセーブルにするには、インターフェイス 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. **interface** *type number*
4. **no ipx split-horizon eigrp** *autonomous-system-number*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx split-horizon eigrp** *autonomous-system-number* **例：** `Router(config-if)# no ipx split-horizon eigrp 234`	スプリット ホライズンをディセーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

（注） スプリット ホライズンは RIP または SAP に対してディセーブルにすることはできず、Enhanced IGRP に対してのみディセーブルにすることができます。

ルーティング アップデートでのルートのアドバタイジングの制御

ルートを学習するデバイスを制御するには、ルーティング アップデートでのルートのアドバタイジングを制御できます。このアドバタイジングを制御するには、ルータ 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. **router** *routing-type number*
4. **distribute-list** *access-list-number* **out** [*interface-name* | *routing-process*]
5. **end**

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。 • 必要に応じて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	**router** *routing-type number* **例：** `Router(config)# router eigrp 234`	ルーティングの詳細を指定し、ルータ 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	**distribute-list** *access-list-number* **out** [*interface-name* | *routing-process*] **例：** `Router(config-router)# distribute-list 55 out ehternet`	ルーティング アップデートでのルートのアドバタイジングを制御します。
ステップ 5	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

（注） スプリット ホライズンは RIP または SAP に対してディセーブルにすることはできず、Enhanced IGRP に対してのみディセーブルにすることができます。

ルーティング アップデートの処理の制御

受信アップデートに表示されているルートの処理を制御するには、ルータ 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. **router** *routing-type number*
4. **distribute-list** *access-list-number* **in** [*interface-name*]
5. **end**

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。 • 必要に応じて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	**router** *routing-type number* **例：** `Router(config)# router eigrp 234`	ルーティングの詳細を指定し、ルータ 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	**distribute-list** *access-list-number* **in** [*interface-name*] **例：** `Router(config-router)# distribute-list 22 in ethernet`	処理される受信ルート アップデートを制御します。
ステップ 5	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

SAP アップデートの制御

インターフェイス上に IPX Enhanced IGRP ピアが見つかった場合、Cisco IOS ソフトウェアで SAP アップデートを定期的に送信するか、SAP テーブルで変更が発生したときに送信するように設定できます。インターフェイス上に IPX Enhanced IGRP ピアが存在していない場合、SAP が常に定期的に送信されます。

デフォルトでは、シリアル回線に Enhanced IGRP ネイバーが存在している場合、SAP テーブルで変更が発生した場合にだけ、Cisco IOS ソフトウェアで SAP アップデートが送信されます。デフォルトでは、イーサネット、トークン リング、および FDDI インターフェイスで、Cisco IOS ソフトウェアで SAP アップデートが定期的に送信されます。SAP アップデートを送信するために必要な帯域幅を減らすため、LAN インターフェイスで SAP アップデートの定期的な送信をディセーブルにする場合があります。この機能は、このインターフェイス外のすべてのノードが Enhanced IGRP ピアの場合にだけディセーブルにする必要があります。そうしないと、その他のノードでの SAP 情報が消失します。

SAP テーブルで変更が生じたときのみに SAP アップデートを送信するには、インターフェイス 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. **interface** *type number*
4. **ipx sap-incremental eigrp** *autonomous-system-number*

5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx sap-incremental eigrp** *autonomous-system-number* **例：** `Router(config-if)# ipx sap-incremental eigrp 312`	SAP テーブルで変更が生じたときのみ、SAP アップデートを送信します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP テーブルで変更が生じたときのみに SAP アップデートを送信し、SAP の変更点のみを送信するには、インターフェイス 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. **interface** *type number*
4. **ipx sap-incremental eigrp** *autonomous-system-number* **rsup-only**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx sap-incremental eigrp** *autonomous-system-number* **rsup-only** **例：** `Router(config-if)# ipx sap-incremental eigrp 311 rsup-only`	SAP テーブルで変更が生じたときのみに SAP アップデートを送信し、SAP での変更点のみを送信します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ipx sap-incremental eigrp rsup-only コマンドを使用してインクリメンタル SAP をイネーブルにする場合、Cisco IOS ソフトウェアでは、インターフェイスに対して Enhanced IGRP を介したルート情報の交換がディセーブルになります。

定期的に SAP アップデートを送信するには、インターフェイス 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. **interface** *type number*
4. **no ipx sap-incremental eigrp** *autonomous-system-number*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx sap-incremental eigrp** *autonomous-system-number* **例：** `Router(config-if)# no ipx sap-incremental eigrp 112`	SAP アップデートを定期的に送信します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP アップデートを設定する方法の例については、この章の最後にある「Enhanced IGRP SAP アップデートの例」の項を参照してください。

インクリメンタル SAP のスプリット ホライズンをディセーブルにするには、インターフェイス 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. **interface** *type number*
4. **no ipx sap-incremental split-horizon**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx sap-incremental split-horizon** **例：** `Router(config-if)# no ipx sap-incremental split-horizon`	SAP のスプリット ホライズンをディセーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP アップデートでのサービスのアドバタイジングの制御

サービスを学習するデバイスを制御するには、SAP アップデートでのこれらのサービスのアドバタイジングを制御できます。このアドバタイジングを制御するには、IPX ルータ 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. **ipx router** *routing-type number*
4. **distribute-sap-list** *access-list-number* **out** [*interface-name* | *routing-process*]
5. **end**

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。 • 必要に応じて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	**ipx router** *routing-type number* **例：** `Router(config)# ipx router eigrp 234`	ルーティングの詳細を指定し、ルータ 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	**distribute-sap-list** *access-list-number* **out** [*interface-name* | *routing-process*] **例：** `Router(config-ipx-router)# distribute-sap-list 22 out ethernet`	ルーティング プロセス間で配布された SAP アップデートでサービスのアドバタイジングを制御します。
ステップ 5	**end** **例：** `Router(config-ipx-router)# end`	IPX ルータ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP アップデートのアドバタイズメントの制御の設定例については、この章の最後にある「SAP アップデートのアドバタイズメントと処理の例」の項を参照してください。

SAP アップデートの処理の制御

受信アップデートに表示されているルートの処理を制御するには、IPX ルータ 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. **ipx router** *routing-type number*
4. **distribute-sap-list** *access-list-number* **in** [*interface-name*]
5. **end**

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。 • 必要に応じて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	**router** *routing-type number* **例：** `Router(config)# router eigrp 234`	ルーティングの詳細を指定し、ルータ 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	**distribute-sap-list** *access-list-number* **in** [*interface-name*] **例：** `Router(config-ipx-router)# distribute-sap-list 22 out ethernet`	処理される受信 SAP アップデートを制御します。
ステップ 5	**end** **例：** `Router(config-ipx-router)# end`	IPX ルータ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP アップデートの処理の制御の設定例については、この章の最後にある「SAP アップデートのアドバタイズメントと処理の例」の項を参照してください。

バックアップ サーバの照会

バックアップ サーバ テーブルは、各 Enhanced IGRP ピアのために維持されるテーブルです。そのピアによってアドバタイズされた IPX サーバのリストが表示されます。サーバが何らかの理由でメイン サーバ テーブルから削除された場合、Cisco IOS ソフトウェアではバックアップ サーバ テーブルを調べて、この削除されたばかりのサーバが Enhanced IGRP ピアのいずれかによって認識されるかどうかを学習します。認識される場合、ピアがサーバ情報をこのルータに再アドバタイズされたのと同様に、そのピアからの情報はメイン サーバ テーブルに再びアドバタイズされます。この方法を使用して、バックアップ サーバ テーブルと各ピアによってアドバタイズされる内容との整合性を維持できるようにすると、テーブルへの変更内容のみを Enhanced IGRP ルータ間でアドバタイズする必要があります。定期的なアップデート全体を送信する必要はありません。

Cisco IOS ソフトウェアのデフォルトでは、各 Enhanced IGRP ネイバーのバックアップ サーバ テーブルの独自のコピーを 60 秒ごとに照会します。この間隔を変更するには、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. **ipx backup-server-query-interval** *interval*
4. **end**

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。 • 必要に応じて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	**ipx backup-server-query-interval** *interval* **例：** `Router(config-router)# ipx back-up-server-query-interval 234`	ネイバーのバックアップ サーバ テーブルの連続する照会の最短間隔を指定します。
ステップ 4	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

WAN での IPX および SPX の設定

Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）、フレーム リレー、PPP、SMDS、および X.25 ネットワークで IPX を設定できます。Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）の詳細については、『*Cisco IOS Dial Technologies Configuration Guide*』を参照してください。フレーム リレー、SMDS、および X.25 の詳細については、『*Cisco IOS Wide-Area Networking Configuration Guide*』を参照してください。

PPP で IPX を設定する場合、このプロトコルにはアドレス マップは不要です。また、ポイントツーポイント リンクによって IPX ヘッダーの圧縮をイネーブルにして、リンクの利用可能な有効帯域幅を増やし、リンクの相互利用のための応答時間を減らすことができます。

フレーム リレーおよび SMDS に設定されたファースト スイッチング IPX シリアル インターフェイスを使用でき、ATM に設定されたインターフェイスで、ファースト スイッチング Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）でカプセル化されたパケットを使用できます。

さらに、IPXWAN プロトコルを設定できます。

WAN インターフェイスで IPX ルーティングを設定する方法の例については、この章の最後にある「WAN インターフェイスでの IPX の例」の項を参照してください。

IPX over DDR の設定

クライアント セッションが約 5 分間アイドル状態になった後、IPX はサーバからクライアントに定期的にウォッチドッグ キープアライブ パケットを送信します。DDR リンクで、送信するデータ パケットがあるかどうかに関係なく、5 分間ごとにコールが発信されます。このようなコールが発信されないように Cisco IOS ソフトウェアを設定して、リモート クライアントの代わりにサーバのウォッチドッグ キープアライブ パケットに応答することができます。これは、*サーバのスプーフィング*とも呼ばれます。スプーフィングによって、サーバでクライアントが常に接続されているように表示されるため（接続されていない場合でも）、使用できるライセンスの数が減少します。Novelle NetWare サーバで非アクティブな接続をクリーン アップできるように、ユーザが IPX ウォッチドッグ スプーフィングの期間を設定して、定期的にディセーブルにすることができます。

DDR で IPX を設定する場合、コールが 5 分間ごとに発信されないように、このようなパケットの生成をディセーブルにすることもできます。他の WAN プロトコルでは、必要なときだけ接続を確立するのではなく、専用の接続が確立されるため、コールが 5 分間ごとに発信されることは問題になりません。

ipx watchdog-spoof コマンドを使用して、ウォッチドッグ スプーフィングの期間をイネーブルにして設定します。スプーフィングが何時間連続してイネーブルになるかと、スプーフィングが何分間ディセーブルになるかを指定できます。スプーフィングがディセーブルになっている場合に、サーバで非アクティブな接続をクリーンアップできます。このコマンドを使用する前に、シリアル インターフェイスでファースト スイッチングとオートノマス スイッチングがディセーブルになっていることを確認します。

ウォッチドッグ スプーフィングをイネーブルにするには、インターフェイス 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. **interface** *type number*
4. **ipx watchdog-spoof** [*enable-time-hours disable-time-minutes*]
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipx watchdog-spoof** [*enable-time-hours disable-time-minutes*] **例：** `Router(config-if)# ipx watchdog-proof 3 45`	ウォッチドッグ スプーフィングをイネーブルにして期間を設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ウォッチドッグ パケットのみが送信される場合にシリアル インターフェイスをアイドル状態にするには、『*Cisco IOS Dial Technologies Configuration Guide*』にある「Deciding and Preparing to Configure DDR」の章で説明されているタスクを参照してください。DR で IPX を設定する方法の例については、この章の最後にある「IPX over DDR の例」の項を参照してください。

DDR での SPX スプーフィングの設定

Sequenced Packet Exchange（SPX）では、クライアントとサーバの間で定期的にキープアライブ パケットを送信します。IPX ウォッチドッグ パケットと同様に、データの転送が停止された後で、サーバとクライアントの間で送信されるキープアライブ パケットがあります。パケット単位またはバイト単位で課金されるネットワークでは、アイドル時間のこれらのパケットのために、顧客の電話接続料金が高額になる可能性があります。このようなコールが発信されないように Cisco IOS ソフトウェアを設定して、リモート システムの代わりにキープアライブ パケットに応答することができます。

DDR で SPX を設定する場合、コールがアイドル状態にならないように、このようなパケットの生成をディセーブルにすることもできます。他の WAN プロトコルでは、必要なときだけ接続を確立するのではなく、専用の接続が確立されるため、パケットの生成をディセーブルにすることは問題ありません。

キープアライブ パケットのみが送信される場合にシリアル インターフェイスをアイドル状態にするには、『*Cisco IOS Dial Technologies Configuration Guide*』にある「Deciding and Preparing to Configure DDR」の章で説明されているタスクを参照してください。

DDR で SPX スプーフィングを設定する方法の例については、この章の最後にある「IPX over DDR の例」の項を参照してください。

IPX ヘッダー圧縮の設定

ポイントツーポイント リンクでの IPX ヘッダー圧縮を設定できます。IPX ヘッダー圧縮を使用すると、ポイントツーポイント リンクで IPX ヘッダーのみを圧縮することも、IPX と NetWare コア プロトコル ヘッダーの組み合わせを圧縮することもできます。現在、ポイントツーポイント リンクでは最初に IPXCP または IXPWAN によって IPX ヘッダー圧縮のネゴシエーションを行う必要があります。Cisco IOS ソフトウェアでは、RFC 1553 で定義されているように、IPX ヘッダー圧縮がサポートされます。

IPX ヘッダー圧縮の設定の詳細については、『*Cisco IOS Dial Technologies Configuration Guide*』にある「Configuring Medial-Independent PPP and Multilink PPP」の章を参照してください。

IPXWAN プロトコルの設定

Cisco IOS ソフトウェアでは、RFC 1634 で定義されているように、IPXWAN プロトコルがサポートされます。IPXWAN を使用すると、IPX ルーティングを実行しているルータでシリアル リンクを介して、IPX ルーティングを実行していて IPXWAN を使用している別のルータ（別の製造元のルータでも可能）に接続できます。

IPXWAN は接続開始プロトコルです。リンクが確立されると、IPXWAN のオーバーヘッドがほとんどなくなります。

PPP で IPXWAN プロトコルを使用できます。また、HDLC で IPXWAN プロトコルを使用することもできますが、シリアル リンクの両端のデバイスを Cisco ルータにする必要があります。

シリアル インターフェイスで IPXWAN を設定するには、インターフェイス 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. **interface** *type number*
4. **no ipx network** [***number***]
5. **encapsulation ppp**
6. **ipx ipxwan** [*local-node* {*network-number* | **unnumbered**} *local-server-name retry-interval retry-limit*]
7. **ipx ipxwan error** [**reset** | **resume** | **shutdown**]
8. **ipx ipxwan static**
9. **end**

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。 • 必要に応じて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	**configure terminal** **例：** `Router(config)# interface ethernet0/1`	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 4	**no ipx network** [*number*] **例：** `Router(config-if)# no ipx network 45`	インターフェイスで IPX ネットワーク番号を設定していないことを確認します。

	コマンドまたはアクション	目的
ステップ 5	**encapsulation ppp** **例：** `Router(config-if)# encapsulation ppp`	PPP をイネーブルにします。
ステップ 6	**ipx ipxwan** [*local-node* {*network-number* | **unnumbered**} *local-server-name retry-interval retry-limit*] **例：** `Router(config-if)# ipx ipxwan 234 342 samp 22 4`	IPXWAN をイネーブルにします。
ステップ 7	**ipx ipxwan error** [**reset** | **resume** | **shutdown**] **例：** `Router(config-if)# ipx ipxwan error reset`	必要に応じて、シリアル リンクに障害が発生した場合に IPXWAN を処理する方法を定義します。
ステップ 8	**ipx ipxwan static** **例：** `Router(config-if)# ipx ipxwan static`	必要に応じて、IPXWAN でスタティック ルーティングをイネーブルにします。リモート サイトでもスタティック ルーティングを使用する必要があることに注意してください。
ステップ 9	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPX ネットワークへのアクセスの制御

IPX ネットワークへのアクセスを制御するには、まずアクセス リストを作成し、次にフィルタを使用して個々のインターフェイスに適用します。

アクセス リストのタイプ

さまざまな種類のトラフィックにフィルタを適用する、次の IPX アクセス リストを作成できます。

- 標準アクセス リスト：発信元ネットワーク番号に基づいてトラフィックを制限します。宛先アドレスおよび発信元と宛先のアドレス マスクを指定することによって、さらにトラフィックを制限することができます。標準 IPX アクセス リストでは、800 ～ 899 の番号または識別名を使用します。
- 拡張アクセス リスト：IPX プロトコル タイプに基づいてトラフィックを制限します。発信元と宛先のアドレスとアドレス マスク、および発信元と宛先のソケットを指定することによって、さらにトラフィックを制限することができます。拡張 IPX アクセス リストでは、900 ～ 999 の番号または識別名を使用します。
- SAP アクセス リスト：IPX SAP タイプに基づいてトラフィックを制限します。これらのリストは SAP フィルタおよび GNS 応答フィルタに使用されます。Novell SAP アクセス リストでは、1000 ～ 1099 の番号または識別名を使用します。
- IPX NetBIOS アクセス リスト：番号ではなく、NetBIOS 名に基づいて IPX NetBIOS トラフィックを制限します。

フィルタのタイプ

IPX インターフェイスに定義できる IPX フィルタは 14 種類以上あります。これらは次の 6 つのグループに分類されます。

- 汎用フィルタ：発信元および宛先のアドレスとパケットの IPX プロトコル タイプに基づいて、インターフェイスの内外でルーティングされるデータ パケットを制御します。
- ルーティング テーブル フィルタ：Cisco IOS ソフトウェアで受け入れられ、アドバタイズされる RIP アップデートと、ローカル ルータが RIP アップデートを受け入れるデバイスを制御します。
- SAP フィルタ：Cisco IOS ソフトウェアで受け入れ、アドバタイズする SAP サービスと、送信する GNS 応答メッセージを制御します。
- IPX NetBIOS フィルタ：着信および発信 IPX NetBIOS パケットを制御します。
- ブロードキャスト フィルタ：転送されるブロードキャスト パケットを制御します。

表 2 に、フィルタ、使用するアクセス リスト、最初の 5 つのグループでフィルタを定義するために使用されるコマンドについてまとめます。**show ipx interfaces** コマンドを使用して、インターフェイスで定義されたフィルタを表示します。

表 2　　フィルタ

フィルタ タイプ	フィルタで使用されるアクセス リスト	フィルタを定義するコマンド
汎用フィルタ		
IPX ネットワーク ヘッダーの内容に基づいて、インバウンドまたはアウトバウンドのパケットにフィルタを適用します。	標準または拡張	**ipx access-group** {*access-list-number* | *name*} [**in** | **out**]
ルーティング テーブル フィルタ		
ルーティング テーブルに追加されるネットワークを制御します。	標準または拡張	**ipx input-network-filter** {*access-list-number* | *name*}
ルーティング アップデートでアドバタイズされるネットワークを制御します。	標準または拡張	**ipx output-network-filter** {*access-list-number* | *name*}
Cisco IOS ソフトウェアによって送信される Enhanced IGRP ルーティング アップデートでアドバタイズされるネットワークを制御します。	標準または拡張	**distribute-list** {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]
アップデートが受け入れられるルータを制御します。	標準または拡張	**ipx router-filter** {*access-list-number* | *name*}
SAP フィルタ		
着信サービス アドバタイズメントにフィルタを適用します。	SAP	**ipx input-sap-filter** {*access-list-number* | *name*}
発信サービス アドバタイズメントにフィルタを適用します。	SAP	**ipx output-sap-filter** {*access-list-number* | *name*}
SAP アップデートが受け入れられるルータを制御します。	SAP	**ipx router-sap-filter** {*access-list-number* | *name*}
GNS 応答メッセージでサーバのリストにフィルタを適用します。	SAP	**ipx output-gns-filter** {*access-list-number* | *name*}

表 2　　フィルタ（続き）

フィルタ タイプ	フィルタで使用されるアクセス リスト	フィルタを定義するコマンド
IPX NetBIOS フィルタ		
着信パケットをノード名ごとにフィルタを適用します。	IPX NetBIOS	**ipx netbios input-access-filter host** *name*
着信パケットをバイト パターンごとにフィルタを適用します。	IPX NetBIOS	**ipx netbios input-access-filter bytes** *name*
発信パケットをノード名ごとにフィルタを適用します。	IPX NetBIOS	**ipx netbios output-access-filter host** *name*
発信パケットをバイト パターンごとにフィルタを適用します。	IPX NetBIOS	**ipx netbios output-access-filter bytes** *name*
ブロードキャスト フィルタ		
転送されるブロードキャスト パケットを制御します。	標準または拡張	**ipx helper-list** {*access-list-number* | *name*}

実装の注意事項

IPX ネットワーク アクセス コントロールを設定する場合、次の点に注意してください。

- アクセス リスト エントリは入力順にスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを高めるには、アクセス リストの初めの方に、最もよく使用されるエントリを置くことをお勧めします。
- アクセス リストの最後に明示的な *permit everything* エントリを定義しないかぎり、このリストの最後には暗示的な *deny everything* エントリが存在します。
- 番号付きアクセス リストの場合、新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することはできません。この結果、以前に明示的に *permit everything* エントリを含めた場合、新しいエントリはスキャンされません。解決方法は、アクセス リストを削除し、新しいエントリを再入力することです。

名前付きアクセス リストの場合、新しいエントリはすべて既存のリストの最後に置かれます。リストの中間にエントリを追加することはできません。ただし、アクセス リスト全体を削除する代わりに、**no deny** コマンドと **no permit** コマンドを使用して、特定のエントリを削除できます。

- 条件は設定しないでください。設定するとパケットが失われます。パケットが失われる可能性がある 1 つの方法は、これらのパケットを拒否するアクセス リストが含まれるネットワーク上でサービスをアドバタイズするようにデバイスまたはインターフェイスが設定される場合です。

IPX ネットワークへのアクセス制御タスク リスト

IPX ネットワークへのアクセスを制御するには、ここで説明する必須タスクを実行します。

- アクセス リストの作成（P.38）（必須）
- フィルタの作成（P.45）（必須）

アクセス リストの作成

番号または名前を使用してアクセス リストを作成できます。任意の方法を選択できます。番号を使用してアクセス リストを識別する場合、フィルタ タイプごとにアクセス リストが 100 に制限されます。名前を使用してアクセス リストを識別する場合は、フィルタ タイプごとにアクセス リストが制限されません。

ここでは、このようなタスクの実行方法について説明します。

- 番号を使用したアクセス リストの作成（P.38）（任意）
- 名前を使用したアクセス リストの作成（P.39）（任意）

番号を使用したアクセス リストの作成

番号を使用してアクセス リストを作成するには、グローバル コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source-network* [*source-node* [*source-node-mask*]] [*destination-network* [*destination-node* [*destination-node-mask*]]]
4. **access-list** *access-list-number* {**deny** | **permit**} *protocol* [*source-network* [*source-node* [*source-network-mask.source-node-mask*]] *source-socket* [*destination-network* [*destination-node* [*destination-network-mask.destination-node-mask*] *destination-socket*] [**log**] [**time-range time-range-name**]
5. **access-list** *access-list-number* {**deny** | **permit**} *network* [*.node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]
6. **end**

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。 • 必要に応じて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	**access-list** *access-list-number* {**deny** | **permit**} *source-network* [*.source-node* [*source-node-mask*]][*destination-network* [*.destination-node* [*destination-node-mask*]]] **例：** `Router(config)# access-list 234 permit source-network 0x22 destination-network 0x10 0x1`	番号を使用して標準 IPX アクセス リストを定義します（汎用、ルーティング、およびブロードキャスト フィルタでこのタイプのアクセス リストを使用します）。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol* [*source-network* [.*source-node* [*source-network-mask.source-node-mask*]] *source-socket* [*destination-network* [.*destination-node* [*destination-network-mask.destination-node-mask*] *destination-socket*] [**log**] [**time-range time-range-name**] **例：** `Router# access-list 432 permit protocol1 source-network 0x1 0x22 source-socket 0x3 0x333`	番号を使用して、拡張 IPX アクセス リストを定義します（汎用、ルーティング、およびブロードキャスト フィルタでこのタイプのアクセス リストを使用します）。**log** キーワードを使用して、違反も含めて、アクセス リストのロギング メッセージを取得します。**permit** 文または **deny** 文が有効な場合、制限する時間範囲を指定します。
ステップ 5	`Router(config)#` **access-list** *access-list-number* {**deny** | **permit**} *network* [.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]] **例：** `Router# access-list 123 permit network 0x1`	番号を使用して SAP フィルタリング アクセス リストを定義します（SAP 応答フィルタおよび GNS 応答フィルタでこのタイプのアクセス リストを使用します）。
ステップ 6	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

番号を使用してアクセス リストを作成したら、この章の「フィルタの作成」の項で説明しているように、フィルタを使用して適切なインターフェイスに適用します。フィルタの適用によって、アクセス リストがアクティブ化されます。

名前を使用したアクセス リストの作成

IPX 名前付きアクセス リストを使用すると、番号ではなく、英数字の文字列（名前）で IPX アクセス リストを識別できます。IPX 名前付きアクセス リストを使用すると、各ユーザまたはインターフェイス用の独立した簡単に識別可能なアクセス リストを使用することによって、セキュリティを維持できます。また、IPX 名前付きアクセス リストを使用すると、フィルタ タイプごとに 100 までというリスト数の制限がなくなります。次のタイプの IPX 名前付きアクセス リストを無制限に設定できます。

- 標準
- 拡張
- SAP
- NetBIOS

番号付きではなく、名前付きのアクセス リストで識別する場合は、モードとコマンド構文が少し異なります。

実装の注意事項

IPX 名前付きアクセス リストを設定する前に、次の点に注意してください。

- NetBIOS アクセス リストを除いて、名前によって識別されるアクセス リストには Cisco IOS Release 11.2(4)F 以前のリリースとの互換性がありません。
- アクセス リスト名は、すべてのプロトコルで一意にする必要があります。
- NetBIOS アクセス リストを除いて、番号付きアクセス リストも使用できます。

IPX 名前付きアクセス リストの設定タスク リスト

標準、拡張、SAP、NLSP ルート集約（要約）または NetBIOS アクセス リストに IPX 名前付きアクセス リストを設定するには、次のいずれかまたは複数のタスクを実行します。

- 名前付き標準アクセス リストの作成（P.40）（任意）
- 名前付き拡張アクセス リストの作成（P.41）（任意）
- 名前付き SAP フィルタリング アクセス リストの作成（P.42）（任意）
- NetBIOS アクセス リストの作成（P.43）（任意）
- アクセス リストへの時間範囲の適用（P.44）（任意）

名前付き標準アクセス リストの作成

名前付き標準アクセス リストを作成するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx access-list standard** *name*
4. {**deny** | **permit**} *source-network* [*.source-node* [*source-node-mask*]] [*destination-network* [*.destination-node* [*destination-node-mask*]]]
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。 • 必要に応じて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	**ipx access-list standard** *name* **例：** `Router(config)# ipx access-list standard stan1`	名前を使用して標準 IPX アクセス リストを定義します（汎用、ルーティング、およびブロードキャスト フィルタでこのタイプのアクセス リストを使用します）。

	コマンドまたはアクション	目的
ステップ 4	{**deny** | **permit**} *source-network* [.*source-node* [*source-node-mask*]] [*destination-network* [.*destination-node* [*destination-node-mask*]]] **例：** `Router (config-access-list)# permit source-network1 0x22`	アクセス リスト コンフィギュレーション モードで、1 つまたは複数の条件が許可されるか、拒否されるかを指定します。これによって、パケットが通過するか、廃棄されるかが決まります。
ステップ 5	**exit** **例：** `Router(config-access-list)# exit`	アクセス リスト コンフィギュレーション モードを終了します。

名前付き標準アクセス リストを作成する方法の例については、この章の最後にある「標準の名前付きアクセス リストの例」の項を参照してください。

名前付き拡張アクセス リストの作成

名前付き拡張アクセス リストを作成するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx access-list standard** *name*
4. {**deny** | **permit**} *protocol* [*source-network*] [[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*] [[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*] [**log**] [*time-range time-range-name*]
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。 • 必要に応じて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	**ipx access-list standard** *name* **例：** `Router(config)# ipx access-list standard stan2`	名前を使用して、拡張 IPX アクセス リストを定義します（汎用、ルーティング、およびブロードキャスト フィルタでこのタイプのアクセス リストを使用します）。

	コマンドまたはアクション	目的
ステップ 4	{**deny** | **permit**} *protocol* [*source-network*] [[[.*source-node*] *source-node-mask*] | [.*source-node source-network-mask.source-node-mask*]] [*source-socket*] [*destination-network*] [[[.*destination-node*] *destination-node-mask*] | [.*destination-node destination-network-mask.destination-nodemask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*] **例：** `Router (config-access-list)# permit protocol1 source-network1 0x22`	アクセス リスト コンフィギュレーション モードで、条件が許可されるか、拒否されるかを指定します。**log** キーワードを使用し、違反も含めて、アクセス リスト ロギング メッセージを取得します。**permit** 文または **deny** 文が有効な場合、制限する時間範囲を指定します。
ステップ 5	**exit** **例：** `Router(config-access-list)# exit`	アクセス リスト コンフィギュレーション モードを終了します。

名前付き SAP フィルタリング アクセス リストの作成

SAP 要求をフィルタリングするために名前付きアクセス リストを作成するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx access-list standard** *name*
4. {**deny** | **permit**} *network* [.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]]
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。 • 必要に応じて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	**ipx access-list standard** *name* **例：** `Router(config)# ipx access-list standard stan2`	名前を使用して SAP フィルタリング アクセス リストを定義します（SAP、GNS、および Get General Service（GGS）の応答フィルタでこのタイプのアクセス リストを使用します）。

	コマンドまたはアクション	目的
ステップ 4	{**deny** | **permit**} *network* [.*node*] [*network-mask.node-mask*] [*service-type* [*server-name*]] **例：** `Router (config-access-list)# permit network1 0x3 0x11 service-type2 server2`	アクセス リスト コンフィギュレーション モードで、条件が許可されるか、拒否されるかを指定します。
ステップ 5	**exit** **例：** `Router(config-access-list)# exit`	アクセス リスト コンフィギュレーション モードを終了します。

NetBIOS アクセス リストの作成

NetBIOS アクセス リストを作成するには、グローバル コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **netbios** *access-list host name* {**deny** | **permit**} *string*
4. **netbios** *access-list bytes name* {**deny** | **permit**} *offset byte-pattern*
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。 • 必要に応じて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	**netbios access-list host** *name* {**deny** | **permit**} *string* **例：** `Router(config)# ipx 234 standard stan2`	ノード名を基準として IPX NetBIOS パケットをフィルタリングするためのアクセス リストを作成します (NetBIOS フィルタでこのタイプのアクセス リストを使用します)。

	コマンドまたはアクション	目的
ステップ 4	**netbios access-list bytes** *name* {**deny** | **permit**} *offset byte-pattern* **例：** `Router (config)# netbios 234 testbyte permit pattern1`	任意のバイト パターンを基準として IPX NetBIOS パケットをフィルタリングするためのアクセス リストを作成します（NetBIOS フィルタでこのタイプのアクセス リストを使用します）。
ステップ 5	**exit** **例：** `Router(config-access-list)# exit`	アクセス リスト コンフィギュレーション モードを終了します。

IPX 名前付きアクセス リストの変更

最初にアクセス リストを作成した後、追加される内容はリストの末尾に配置されます。追加は、端末から入力される場合もあります。そのため、アクセス リスト コマンド ラインを選択的に特定のアクセス リストの中間に追加することはできません。ただし、**no permit** コマンドと **no deny** コマンドを使用して、名前付きアクセス リストからエントリを削除することはできます。

（注） アクセス リストを作成する場合、デフォルトでは、末尾に達するまでに一致が見つからない場合、すべてのアクセス リストの末尾に明示的な deny 文が含まれることに注意してください。

汎用フィルタを作成する方法の例については、この章の最後にある「IPX ネットワーク アクセスの例」の項を参照してください。

名前付きアクセス リストのインターフェイスへの適用

アクセス リストを作成したら、この章の「フィルタの作成」の項で説明しているように、フィルタを使用して適切なインターフェイスに適用する必要があります。フィルタの適用によって、アクセス リストがアクティブ化されます。

アクセス リストへの時間範囲の適用

time-range コマンドを使用して、時刻や日付に基づいてアクセス リストを実装できるようになりました。これを行うには、時間範囲の名前、時刻および日付を定義し、アクセス リスト内の名前によって時間範囲を参照し、時間範囲の制約事項をアクセス リストに適用します。

現在、時間範囲を使用できる機能は、IP および IPX の名前付きまたは番号付きの拡張アクセス リストのみです。時間範囲を使用すると、ネットワーク管理者はアクセス リストで **permit** 文または **deny** 文がいつ有効になるかを定義できます。この時間範囲機能を使用できるようになる前は、アクセス リストの文が作成されると、常に有効になっていました。**time-range** キーワードおよび引数は、前述の「番号を使用したアクセス リストの作成」および「名前を使用したアクセス リストの作成」の名前付きおよび番号付きの拡張アクセス リストのタスク表に記載されています。**time-range** コマンドは、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Performing Basic System Management」という章で設定されています。IPX 時間範囲の設定例については、この章の最後にある「IPX ネットワーク アクセスの例」の項を参照してください。

時間範囲の利点は、次のように多数あります。

- ネットワーク管理者は、リソースへのユーザ アクセスを許可するか拒否するかについて、詳細に制御できます。リソースとは、アプリケーション（IP アドレス/マスク ペアとポート番号の組み合わせで識別されるもの）、ポリシー ルーティング、オンデマンド リンク（ダイヤラの対象となるトラフィックとして識別されるもの）などです。

- ネットワーク管理者が設定可能な時間ベースのセキュリティ ポリシーとしては、Cisco IOS Firewall フィーチャ セットまたはアクセス リストを使用する境界セキュリティなどがあります。

フィルタの作成

フィルタを使用すると、ルータのインターフェイスで転送またはブロックされるトラフィックを制御できます。フィルタでは、特定の番号付きまたは名前付きのアクセス リストがインターフェイスに適用されます。

フィルタを作成するには、ここで説明するタスクを実行します。

- 汎用フィルタの作成（P.45）（任意）
- ルーティング テーブルの更新のためのフィルタの作成（P.46）（任意）
- SAP フィルタの作成（P.48）（任意）
- GNS 応答フィルタの作成（P.49）（任意）
- GGS 応答フィルタの作成（P.50）（任意）
- IPX NetBIOS フィルタの作成（P.51）（任意）
- ブロードキャスト メッセージ フィルタの作成（P.53）（任意）

汎用フィルタの作成

汎用フィルタでは、発信元および宛先のアドレス、IPX プロトコル タイプ、および発信元と宛先のパケットのソケット番号に基づいて、インターフェイスとの間で送受信するデータ パケットが特定されます。

汎用フィルタを作成するには、まず、この章の「アクセス リストの作成」の項で説明したように標準または拡張アクセス リストを作成し、フィルタをインターフェイスに適用します。

汎用フィルタをインターフェイスに適用するには、インターフェイス 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. **interface type** *number*
4. **ipx access-group** {*access-list-number* | *name*}[**in** | **out**]
5. **end**

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。 • 必要に応じて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)# configure terminal`	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	**ipx access-group** {*access-list-number* | *name*} [**in** | **out**] **例：** `Router(config-if)# ipx access-group 312 in`	汎用フィルタをインターフェイスに適用します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスまたはサブインターフェイスごとに、1 つの入力フィルタおよび出力フィルタだけを適用できます。オートノマス スイッチングがすでに設定されているインターフェイスで、出力フィルタを設定することはできません。同様に、出力フィルタがすでに存在しているインターフェイスで、オートノマス スイッチングを設定することもできません。*いずれかの*インターフェイスでオートノマス スイッチングがすでに設定されている場合、インターフェイスで入力フィルタを設定することはできません。同様に、*いずれかの*インターフェイスでオートノマス スイッチングがすでに有効になっている場合、入力フィルタを設定することはできません。

汎用フィルタを作成する方法の例については、この章の最後にある「IPX ネットワーク アクセスの例」の項を参照してください。

ルーティング テーブルの更新のためのフィルタの作成

ルーティング テーブルの更新フィルタでは、Cisco IOS ソフトウェアでルーティング テーブルを受け入れるエントリ、ルーティング アップデートでアドバタイズするネットワークを制御します。

ルーティング テーブルの更新を制御するためのフィルタを作成するには、この章の「アクセス リストの作成」の項で説明したように標準または拡張アクセス リストを作成し、1 つまたは複数のフィルタをインターフェイスに適用します。

ルーティング テーブルの更新フィルタをインターフェイスに適用するには、インターフェイス コンフィギュレーション モードまたはルータ コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type** *number*
4. **ipx access-group** {*access-list-number* | *name*}
5. **ipx output-network-filter** {*access-list-number* | *name*}
6. **distribute-list** {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]
7. **ipx router-filter** {*access-list-number* | *name*}
8. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx input-network-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx input-network-filter 123`	IPX ルーティング アップデートが受信されたときに、ルーティング テーブルに追加されるネットワークを制御します。
ステップ 5	**ipx output-network-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx output-network-filter {123 | stamp}`	Cisco IOS ソフトウェアによって送信される RIP ルーティング アップデートでアドバタイズされるネットワークを制御します。
ステップ 6	**distribute-list** {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*] **例：** `Router(config-if)# distribute-list 222 out ppp`	Cisco IOS ソフトウェアによって送信される Enhanced IGRP ルーティング アップデートでアドバタイズされるネットワークを制御します。

	コマンドまたはアクション	目的
ステップ 7	**ipx router-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx router-filter 222`	ルーティング アップデートが受け入れられるルータを制御します。
ステップ 8	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

（注） **ipx output-network-filter** コマンドは IPX RIP のみに適用されます。Enhanced IGRP でルーティング アップデートをフィルタリングするときに、ルートのアドバタイズを制御するには、**distribute-list out** コマンドを使用します。詳細については、この章の「ルーティング アップデートでのルートのアドバタイジングの制御」の項を参照してください。

SAP フィルタの作成

Novell ネットワークでのトラフィックの共通ソースは SAP メッセージです。これは NetWare サーバおよび Cisco IOS ソフトウェアで利用可能なサービスをブロードキャストするときに生成されます。

ネットワーク セグメントまたは特定のサーバから IPX ネットワーク間で SAP メッセージがルーティングされる方法を制御するには、まず、この章の「アクセス リストの作成」の項で説明したように SAP フィルタリング アクセス リストを作成し、1 つまたは複数のフィルタをインターフェイスに適用します。

SAP フィルタをインターフェイスに適用するには、インターフェイス コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipx input-sap-filter** [*access-list-number* | *name*]
5. **ipx output-sap-filter** [*access-list-number* | *name*]
6. **ipx router-sap-filter** [*access-list-number* | *name*]
7. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx input-sap-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx input-sap-filter 234`	着信サービス アドバタイズメントにフィルタを適用します。
ステップ 5	**ipx output-sap-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx output-sap-filter 432`	発信サービス アドバタイズメントにフィルタを適用します。
ステップ 6	**ipx router-sap-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx router-sap-filter 101`	特定のルータからフィルタ サービス アドバタイズメントを受信します。
ステップ 7	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

各 SAP フィルタのいずれかを、インターフェイスごとに適用できます。

SAP フィルタを作成および適用する例については、この章の最後にある「SAP 入力フィルタの例」および「SAP 出力フィルタの例」の項を参照してください。

GNS 応答フィルタの作成

Cisco IOS ソフトウェアによって送信される GNS 応答に含まれるサーバを制御するためのフィルタを作成するには、まず、この章の「アクセス リストの作成」の項で説明したように SAP フィルタリング アクセス リストを作成し、GNS フィルタをインターフェイスに適用します。

GNS フィルタをインターフェイスに適用するには、インターフェイス 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. **interface** *type number*
4. **ipx output-gns-filter** {*access-list-number* | *name*}
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx output-gns-filter** {*access-list-number* | *name*} **例：** `Router(config-if)# ipx output-gns-filter 444`	GNS 応答メッセージでサーバのリストにフィルタを適用します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GGS 応答フィルタの作成

Cisco IOS ソフトウェアによって送信される Get General Service（GGS）応答に含まれるサーバを制御するためのフィルタを作成するには、まず、この章の「アクセス リストの作成」の項で説明したように SAP フィルタリング アクセス リストを作成し、GGS フィルタをインターフェイスに適用します。

（注） GGS SAP 応答フィルタは出力 SAP フィルタよりも前に適用されるため、GGS SAP 応答フィルタを通過することが許可された SAP エントリも、出力 SAP フィルタによってフィルタリングできます。

GGS フィルタをインターフェイスに適用するには、インターフェイス 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. **interface** *type number*
4. **ipx output-ggs-filter**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx output-ggs-filter** **例：** `Router(config-if)# ipx output-ggs-filter`	GGS 応答メッセージでサーバのリストにフィルタを適用します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GGS SAP 応答フィルタを作成する例については、この章の最後にある「IPX ネットワーク アクセス：例」の項を参照してください。

IPX NetBIOS フィルタの作成

Novell IPX NetBIOS では、英数字の名前を使用するノードとノード アドレスの間でメッセージを交換できます。したがって、Cisco IOS ソフトウェアでは、ノード名またはパケット内の任意のバイト パターン（ノード アドレスなど）で、着信および発信 NetBIOS FindName パケットをフィルタリングできます。

（注） このようなフィルタは IPX NetBIOS FindName パケットのみに適用されます。Logical Link Control, Type 2（LLC2; 論理リンク制御タイプ 2）、NetBIOS パケットには影響を与えません。

実装の注意事項

IPX NetBIOS アクセス コントロールを設定する場合、次の点に注意してください。

- ホスト（ノード）名では、大文字と小文字が区別されます。
- ホストとバイトのアクセス リストは互いに独立しているため、同じ名前を付けることができます。
- ノードが名前を基準としてフィルタリングされる場合、IPX NetBIOS の「find name」要求のために、アクセス リスト内の名前が宛先名フィールドと比較されます。
- バイトのオフセットを基準とするアクセス フィルタは、各パケットを調べる必要があるため、パケット伝送レートに重大な影響を与える可能性があります。このようなアクセス リストは、どうしても必要な場合にだけ使用してください。
- ノード名がアクセス リストに見つからない場合、デフォルトの処理はアクセス拒否です。

IPX NetBIOS フィルタの設定

IPX NetBIOS アクセスを制御するためのフィルタを作成するには、まず、この章の「アクセス リストの作成」の項で説明したように NetBIOS アクセス リストを作成し、アクセス リストをインターフェイスに適用します。

NetBIOS アクセス リストをインターフェイスに適用するには、インターフェイス コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipx netbios input-access-filter host** *name*
5. **ipx netbios input-access-filter bytes** *name*
6. **ipx netbios output-access-filter host** *name*
7. **ipx netbios output-access-filter bytes** *name*
8. **end**

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。 • 必要に応じて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 ethernet0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipx netbios input-access-filter host** *name* **例：** `Router(config-if)# ipx netbios input-access-filter host node1`	着信パケットをノード名ごとにフィルタを適用します。
ステップ 5	**ipx netbios input-access-filter bytes** *name* **例：** `Router(config-if)# ipx netbios input-access-filter bytes pattern1`	着信パケットをバイト パターンごとにフィルタを適用します。
ステップ 6	**ipx netbios output-access-filter host** *name* **例：** `Router(config-if)# ipx netbios output-access-filter host node2`	発信パケットをノード名ごとにフィルタを適用します。
ステップ 7	**ipx netbios output-access-filter bytes** *name* **例：** `Router(config-if)# ipx netbios output-access-filter bytes pattern2`	発信パケットをバイト パターンごとにフィルタを適用します。
ステップ 8	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

これらの 4 つのフィルタをインターフェイスごとに適用できます。

IPX NetBIOS を制御するためのフィルタを作成する方法の例については、この章の最後にある「IPX NetBIOS フィルタの例」の項を参照してください。

ブロードキャスト メッセージ フィルタの作成

ルータは通常、すべてのブロードキャスト要求をブロックし、他のネットワーク セグメントには転送しないため、ネットワーク全体でのブロードキャスト トラフィックによるパフォーマンスの低下が防止されます。ブロードキャスト メッセージ フィルタをインターフェイスに適用することによって、他のネットワークに転送されるブロードキャスト メッセージを定義できます。

ブロードキャスト メッセージを制御するためのフィルタを作成するには、まず、この章の「アクセス リストの作成」の項で説明したように標準または拡張アクセス リストを作成し、ブロードキャスト メッセージ フィルタをインターフェイスに適用します。

ブロードキャスト メッセージ フィルタをインターフェイスに適用するには、インターフェイス 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. **interface** *type number*
4. **ipx helper-address** *network.node*

5. **ipx helper-list** {*access-list-number* | *name*}
6. **end**

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。 • 必要に応じて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-if)# interface ethernet0/1`	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 4	**ipx helper-address** *network.node* 例： `Router(config-if)# ipx helper-address 1.2.3.1`	ブロードキャスト メッセージの転送のためのヘルパー アドレスを指定します。
ステップ 5	**ipx helper-list** {*access-list-number* | *name*} 例： `Router(config-if)# ipx helper-list 143`	ブロードキャスト メッセージ フィルタをインターフェイスに適用します。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

（注） インターフェイスで **ipx helper-address** コマンドまたは **ipx type-20-propagation** コマンドを発行して、ブロードキャスト メッセージの転送をイネーブルにして制御しないと、ブロードキャスト メッセージ フィルタは有効になりません。これらのコマンドについては、この章の後の方で説明します。

ブロードキャスト メッセージ フィルタを作成および適用する方法の例については、この章の最後にある「ブロードキャストを制御するヘルパー機能：例」の項を参照してください。

IPX ネットワーク パフォーマンスの調整

IPX ネットワークパフォーマンスを調整するには、ここで説明するいずれかまたは複数のタスクを実行します。

- Novell IPX 準拠の制御（P.55）（任意）
- RIP および SAP の情報の調整（P.65）（任意）

- ロード シェアリングの設定（P.84）（任意）
- ブロードキャスト メッセージの使用の指定（P.86）（任意）
- IPX ファースト スイッチングのディセーブル化（P.89）（任意）
- ルート キャッシュの調整（P.90）（任意）
- デフォルト ルートの調整（P.92）（任意）
- 奇数長のパケットのパディング（P.94）（任意）

Novell IPX 準拠の制御

1992 年 11 月 17 日に発行された『*Novell IPX Router Specification, version 1.10*』というマニュアルで定義されているように、IPX ルータの完全な機能を提供するために、シスコによる Novell IPX プロトコルの実装が認証されています。

Novell の仕様への準拠を制御するには、ここで説明する必須タスクを実行します。

- タイプ 20 パケットの転送の制御（P.55）（任意）
- パケット内遅延の制御（P.60）（任意）
- IPX ネットワークのシャットダウン（P.63）（任意）
- 完全な Novell 準拠の実現（P.63）（任意）

タイプ 20 パケットの転送の制御

NetBIOS over IPX では、すべてのネットワークにフラッディングされるタイプ 20 の伝播ブロードキャスト パケットを使用して、ネットワーク上で名前付きノードについての情報を取得します。NetBIOS では、ネットワーク レイヤを実装しないため、ブロードキャスト メカニズムを使用してこの情報を取得します。

ルータは通常、すべてのブロードキャスト要求をブロックします。タイプ 20 パケットの伝播をイネーブルにすると、ルータの IPX インターフェイスでタイプ 20 パケットを受け入れ、転送することができます。

タイプ 20 パケットの伝播方法

タイプ 20 の伝播のために設定されたインターフェイスがタイプ 20 パケットを受信すると、Cisco IOS ソフトウェアは Novell の仕様に従ってパケットを処理します。Cisco IOS ソフトウェアはパケットを次のインターフェイスに伝播します。タイプ 20 パケットは最大 8 つのホップ カウントを伝播できます。

ループ検出とその他のチェック

IPX ルータの仕様で説明されているように、パケットの転送（フラッディング）前に、ルータはループ検出を実行します。

IPX の仕様で説明されているループ検出以外のタイプ 20 伝播パケットのチェックを適用するように、Cisco IOS ソフトウェアを設定できます。これらのチェックは、ヘルパーで処理された all-nets ブロードキャスト パケットに適用されるチェックと同じです。タイプ 20 ブロードキャスト パケットの不要な重複を制限できます。その他のヘルパー チェックは次のとおりです。

- プライマリ ネットワークのみでタイプ 20 伝播パケットを受け入れます。プライマリ ネットワークは、発信元ネットワークへのプライマリ パスとなるネットワークです。
- 発信元ネットワークに戻らないネットワークのみを介してタイプ 20 の伝播パケットを転送します。

この追加チェックでは不要なパケット重複量を減らすことによってタイプ 20 伝播パケットの処理の堅牢性が向上しますが、次の 2 つの副作用があります。

- タイプ 20 パケット伝播がすべてのインターフェイスでは設定されない場合、プライマリ インターフェイスが変更されると、これらのパケットがブロックされる可能性があります。
- タイプ 20 パケット伝播のために、任意の手動スパニング ツリーを設定することはできません。

タイプ 20 の伝播とヘルパー アドレスの関係

ヘルパー アドレスを使用して、タイプ 20 以外のブロードキャスト パケットをその他のネットワーク セグメントに転送します。その他のブロードキャスト パケットの転送の詳細については、この章の「ヘルパー アドレスを使用したブロードキャスト パケットの転送」の項を参照してください。

ネットワークで、ヘルパー アドレスとタイプ 20 伝播を組み合わせて使用できます。ヘルパー アドレスを使用して、タイプ 20 以外のブロードキャスト パケットを転送し、タイプ 20 伝播を使用して、タイプ 20 ブロードキャスト パケットを転送します。

タイプ 20 パケット設定タスク リスト

個々のインターフェイスでタイプ 20 パケットの転送をイネーブルにできます。さらに、タイプ 20 パケットの受け入れと転送を制限することもできます。また、Novell の仕様に準拠しないで、タイプ 20 伝播ではなく、ヘルパー アドレスを使用してタイプ 20 パケットを転送することもできます。ここでは、このようなタスクについて説明します。

- タイプ 20 パケットの転送のイネーブル化（P.56）（任意）
- 着信タイプ 20 パケットの受け入れの制限（P.57）（任意）
- 発信タイプ 20 パケットの転送の制限（P.58）（任意）
- ヘルパー アドレスを使用したタイプ 20 パケットの転送（P.59）（任意）

タイプ 20 パケットの転送のイネーブル化

デフォルトでは、Cisco IOS ソフトウェアではタイプ 20 伝播パケットが破棄されます。タイプ 20 伝播ブロードキャスト パケットを受信し、他のネットワーク セグメントに転送（フラッディング）して、ループ検出の対象とするように、このソフトウェアを設定できます。

タイプ 20 パケットの受信と転送をイネーブルにするには、インターフェイス 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. **interface** *type number*
4. **ipx type-20-propagation**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx type-20-propagation** **例：** `Router(config-if)# ipx type-20-propagation`	IPX タイプ 20 伝播パケット ブロードキャストを、他のネットワーク セグメントに転送します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

タイプ 20 伝播をイネーブルにすると、Cisco IOS は最大 8 つのホップのブロードキャストを次のインターフェイスに伝播します。

着信タイプ 20 パケットの受け入れの制限

着信タイプ 20 伝播パケットについては、Cisco IOS ソフトウェアのデフォルトでは、タイプ 20 伝播パケットの受信がイネーブルになっているすべてのインターフェイスでパケットを受け入れるように設定されます。発信元ネットワークへのプライマリ ルートである単一のネットワークからのパケットのみを受け入れるようにソフトウェアを設定できます。これは、その他のネットワークを介して受信される同じ発信元からの同様のパケットが破棄されることを意味します。

着信タイプ 20 伝播ブロードキャスト パケットのチェックは、インターフェイスがタイプ 20 パケットを受信して転送するように設定されている場合のみに実行されます。

IPX 仕様で定義されたチェックに加えて、着信タイプ 20 伝播パケットの受信に制限を適用するには、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. **ipx type-20-input-checks**
4. **end**

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。 • 必要に応じて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	**ipx type-20-input-checks** **例：** `Router(config)# ipx type-20-input-checks`	IPX タイプ 20 伝播パケットの受け入れを制限します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

発信タイプ 20 パケットの転送の制限

発信タイプ 20 伝播パケットについては、Cisco IOS ソフトウェアのデフォルトでは、タイプ 20 伝播パケットの送信がイネーブルになっているすべてのインターフェイスでパケットを送信し、ループ検出の対象とするように設定されます。発信元ネットワークへのルートではないネットワークだけにこのようなパケットを送信するようにソフトウェアを設定できます（このソフトウェアでは、現在のルーティング テーブルを使用して、ルートを定義します）。

発信タイプ 20 伝播ブロードキャスト パケットのチェックは、インターフェイスがタイプ 20 パケットを受信して転送するように設定されている場合のみに実行されます。

タイプ 20 伝播パケットの転送に制限を適用し、このようなパケットを IPX 仕様で定義されたチェックだけを使用するすべてのネットワークに転送するには、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. **ipx type-20-output-checks**
4. **end**

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。 • 必要に応じて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	**ipx type-20-output-checks** **例：** `Router(config)# ipx type-20-output-checks`	IPX タイプ 20 伝播パケットの転送を制限します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ヘルパー アドレスを使用したタイプ 20 パケットの転送

タイプ 20 パケット伝播ではなく、ヘルパー アドレスを使用して、特定のネットワーク セグメントにタイプ 20 パケットを転送することもできます。

ネットワーク内の一部のルータで、タイプ 20 伝播をサポートしないバージョンの Cisco IOS を実行している場合、ヘルパー アドレスを使用してタイプ 20 パケットを転送する必要があります。ネットワーク内の一部のルータがタイプ 20 伝播をサポートしていて、その他のルータがサポートしていない場合、ヘルパー アドレスを使用して、パケットを特定のセグメントのみに伝送すると、ネットワークのあらゆる場所にパケットがフラッディングされることを防止できます。

Cisco IOS Release 9.1 以前のバージョンでは、タイプ 20 伝播がサポートされません。

（注） ヘルパー アドレスを使用するタイプ 20 パケットの転送は、Novell IPX のルータ仕様に準拠していません。

ヘルパー アドレスを使用してタイプ 20 パケット アドレスを転送するには、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. **ipx type-20-helpered**
4. **interface** *type number*
5. **ipx helper-address** *network.node*
6. **end**

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。 • 必要に応じて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	**ipx type-20-helpered** **例：** `Router(config)# ipx type-20-helpered`	IPX タイプ 20 パケットを特定のネットワーク セグメントに転送します。この手順により、タイプ 20 の伝播がオフになります。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface ethernet0/1`	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 5	**ipx helper-address** *network.node* **例：** `Router(config-if)# ipx helper-address 1.2.1.1`	インターフェイス コンフィギュレーション モードから、IPX タイプ 20 パケットを含めて、ブロードキャスト メッセージを転送するためのヘルパー アドレスを指定します。
ステップ 6	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco IOS ソフトウェアでは、タイプ 20 パケットが **ipx helper-address** コマンドで指定されたノードだけに転送されます。

（注） **ipx type-20-helpered** コマンドを使用すると、**ipx type-20-propagation** コマンドで指定されているように、タイプ 20 伝播パケットの受信と転送がディセーブルになります。

パケット内遅延の制御

パケット内遅延を制御するには、グローバル コンフィギュレーション コマンドとインターフェイス コンフィギュレーション コマンドの組み合わせを使用できます。

グローバル コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx default-output-rip-delay** *delay*
4. **ipx default-triggered-rip-delay** *delay*

5. **ipx default-output-sap-delay** *delay*
6. **ipx default-triggered-sap-delay** *delay*
7. **end**

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。 • 必要に応じて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	**ipx default-output-rip-delay** *delay* **例：** `Router(config)# ipx default-output-rip-delay 32`	すべてのインターフェイスで送信される、複数パケットのルーティング アップデートのパケット内遅延を設定します。
ステップ 4	**ipx default-triggered-rip-delay** *delay* **例：** `Router(config)# ipx default-triggered-rip-delay 45`	すべてのインターフェイスで送信される、複数パケットでトリガーされるルーティング アップデートのパケット内遅延を設定します。
ステップ 5	**ipx default-output-sap-delay** *delay* **例：** `Router(config)# ipx default-output-sap-delay 44`	すべてのインターフェイスで送信される、複数パケットの SAP アップデートのパケット内遅延を設定します。
ステップ 6	**ipx default-triggered-sap-delay** *delay* **例：** `Router(config)# ipx default-triggered-sap-delay 56`	すべてのインターフェイスで送信される、複数パケットでトリガーされる SAP アップデートのパケット内遅延を設定します。
ステップ 7	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイス コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipx output-rip-delay** *delay*

5. **ipx triggered-rip-delay** *delay*
6. **ipx output-sap-delay** *delay*
7. **ipx triggered-sap-delay** *delay*
8. **end**

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。 • 必要に応じて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 ehternet0/1`	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 4	**ipx output-rip-delay** *delay* **例：** `Router(config)# ipx output-rip-delay 11`	単一のインターフェイスで送信される、複数パケットのルーティング アップデートのパケット内遅延を設定します。
ステップ 5	**ipx triggered-rip-delay** *delay* **例：** `Router(config)# ipx triggered-rip-delay 25`	単一のインターフェイスで送信される、複数パケットでトリガーされるルーティング アップデートのパケット内遅延を設定します。
ステップ 6	**ipx output-sap-delay** *delay* **例：** `Router(config)# ipx output-sap-delay 56`	単一のインターフェイスで送信される、複数パケットの SAP アップデートのパケット内遅延を設定します。
ステップ 7	**ipx triggered-sap-delay** *delay* **例：** `Router(config)# ipx triggered-sap-delay 55`	単一のインターフェイスで送信される、複数パケットでトリガーされる SAP アップデートのパケット内遅延を設定します。
ステップ 8	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

（注） 低速 WAN インターフェイスでは **ipx output-rip-delay** コマンドと **ipx output-sap-delay** コマンドを使用することをお勧めします。Cisco IOS Release 11.1 以降のバージョンのデフォルトの遅延は 55 ミリ秒です。

IPX ネットワークのシャットダウン

Novell に準拠する方法を使用して IPX ネットワークをシャットダウンするには、インターフェイス 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. **interface** *type number*
4. **ipx down** *network*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx down** *network* **例：** `Router(config-if)# ipx down 234`	インターフェイスで、IPX ネットワークを管理された状態でシャットダウンします。これによって、インターフェイスからネットワークが削除されます。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ipx down コマンドを使用して IPX ネットワークをシャットダウンする場合の方が、**shutdown** コマンドを使用するよりもコンバージェンスが短縮されます。

完全な Novell 準拠の実現

IPX 用に設定される各インターフェイスで完全準拠を実現にするには、インターフェイス 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. **interface** *type number*
4. **ipx output-rip-delay** *delay*
5. **ipx output-sap-delay** *delay*
6. **ipx type-20-propagation**
7. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx output-rip-delay** *delay* 例： `Router(config-if)# ipx output-rip-delay 55`	複数パケットのルーティング アップデートのパケット内遅延を設定します。 • この例では、遅延が 55 ミリ秒に設定されます。
ステップ 5	**ipx output-sap-delay** *delay* 例： `Router(config-if)# ipx output-sap-delay 55`	複数パケットの SAP アップデートのパケット内遅延を設定します。 • この例では、遅延が 55 ミリ秒に設定されます。
ステップ 6	**ipx type-20-propagation** 例： `Router(config-if)# ipx type-20-propagation`	ルータ間でタイプ 20 のブロードキャスト トラフィックを転送する場合、必要に応じてタイプ 20 パケット伝播をイネーブルにします。
ステップ 7	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

また、複数パケットの RIP および SAP のアップデートのパケット内遅延をグローバルに設定して、完全準拠を実現すると、各インターフェイスで遅延を設定する必要がなくなります。このようなパケット内遅延を設定するには、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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx default-output-rip-delay** *delay*
4. **ipx default-output-sap-delay** *delay*
5. **end**

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。 • 必要に応じて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	**ipx default-output-rip-delay** *delay* **例：** `Router(config)# ipx output-rip-delay 55`	すべてのインターフェイスで送信される、複数パケットのルーティング アップデートのパケット内遅延を設定します。 この例では、遅延が 55 ミリ秒に設定されます。
ステップ 4	**ipx default-output-sap-delay** *delay* **例：** `Router(config)# ipx default-output-sap-delay 55`	すべてのインターフェイスで送信される、複数パケットの SAP アップデートのパケット内遅延を設定します。 この例では、遅延が 55 ミリ秒に設定されます。
ステップ 5	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

（注） Cisco IOS Release 11.1 以降のバージョンのデフォルトの遅延は 55 ミリ秒です。

RIP および SAP の情報の調整

RIP および SAP の情報を調整するには、次のいずれかまたは複数の作業を実行します。

- スタティック ルートの設定（P.66）（任意）
- RIP 遅延フィールドの調整（P.68）（任意）
- RIP 要求への応答の制御（P.69）（任意）
- RIP アップデート タイマーの調整（P.70）（任意）
- RIP アップデート パケット サイズの設定（P.73）（任意）
- スタティック SAP テーブル エントリの設定（P.74）（任意）

- SAP 要求のキューの長さの設定（P.75）（任意）
- SAP アップデート タイマーの調整（P.76）（任意）
- SAP アップデート パケット サイズの設定（P.79）（任意）
- SAP-after-RIP のイネーブル化（P.80）（任意）
- RIP または SAP の汎用クエリー送信のディセーブル化（P.81）（任意）
- GNS 要求への応答の制御（P.82）（任意）

スタティック ルートの設定

IPX では、宛先への複数のパスが存在する場合に、RIP、Enhanced IGRP、または NLSP を使用して、最適なパスを決定します。ルーティング プロトコルによって、ルーティング テーブルが動的に更新されます。ただし、スタティック ルートをルーティング テーブルに追加して、特定の宛先へのパスを明示的に指定する場合もあります。スタティック ルートは、動的に学習したパスよりも常に優先されます。

スタティック ルートを割り当てる場合は、慎重に行ってください。スタティック ルートに関連付けられたリンクが失われると、代替パスを使用できる場合でも、トラフィックの転送が停止したり、存在しない宛先にトラフィックが転送されたりする可能性があります。

スタティック ルートをルーティング テーブルに追加するには、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. **ipx route** {*network* [*network-mask*] | default} {*network.node* | *interface*}[*ticks*] [*hops*]
4. **end**

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。 • 必要に応じて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。

	コマンドまたはアクション	目的
ステップ 3	**ipx route** {*network* [*network-mask*] | **default**} {*network.node* | *interface*}[*ticks*] [*hops*] **例：** `Router(config)# ipx route 234 1.1.2.1`	スタティック ルートをルーティング テーブルに追加します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

動的に学習したルートよりも優先できるスタティック ルートを設定します。このようなルートは浮動スタティック ルートと呼ばれます。浮動スタティック ルートを使用して、ダイナミック ルーティング情報を使用できない場合のみに使用されるラスト リゾートのパスを作成できます。

（注） デフォルトでは、浮動スタティック ルートはその他のダイナミック プロトコルに再配布されません。

浮動スタティック ルートをルーティング テーブルに追加するには、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. **ipx route** {*network* [*network-mask*] | default} {*network.node* | *interface*}[*ticks*] [*hops*]
4. **end**

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。 • 必要に応じて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。

	コマンドまたはアクション	目的
ステップ 3	**ipx route** {*network* [*network-mask*] | **default**} {*network.node* | *interface*} [*ticks*] [*hops*] [**floating-static**] **例：** `Router(config)# ipx route default interface floating-static`	浮動スタティック ルートをルーティング テーブルに追加します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

RIP 遅延フィールドの調整

デフォルトでは、すべての LAN インターフェイスが RIP 遅延 1、すべての WAN インターフェイスが RIP 遅延 6 になります。ほとんどのインターフェイスで、遅延はデフォルト値のままで十分です。ただし、ティック カウントを設定することによって、RIP 遅延フィールドを調整できます。ティック カウントを設定するには、インターフェイス 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. **interface** *type number*
4. **ipx delay** *ticks*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx delay** *ticks* **例：** `Router(config-if)# ipx delay 22`	IPX RIP 遅延フィールドで使用されるティック カウントを設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP 要求への応答の制御

RIP 要求への応答を制御するには、インターフェイス 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. **interface** *type number*
4. **ipx rip-response-delay** *ms*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx rip-response-delay** *ms* **例：** `Router(config-if)# ipx rip-response-delay 22`	RIP 要求に応答する場合の遅延を設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP アップデート タイマーの調整

インターフェイス単位で IPX RIP アップデートの間隔を設定できます。また、インターフェイス単位またはグローバル ベースで複数パケットの RIP アップデートのパケット間の遅延を指定することもできます。さらに、インターフェイス単位またはグローバル ベースで、複数パケットでトリガーされる RIP アップデートのパケット間の遅延を指定できます。

すべてのルータが Cisco ルータであるか、または IPX ルータでタイマーを設定できる設定でのみ、RIP アップデート タイマーを設定できます。同じケーブル セグメントに接続されているすべてのデバイスに対して、タイマーを同じにする必要があります。選択したアップデート値は、次のように内部 IPX タイマーに影響します。

- アップデート間隔の値の 3 倍（3 * *interval*）以内でルーティング アップデートが行われず、無制限のメトリックでアドバタイズされる場合、IPX ルートが無効とマークされます。
- アップデート間隔の値の 4 倍（4 * *interval*）以内でルーティング アップデートが行われない場合、ルーティング テーブルから IPX ルートが削除されます。
- ルータ内で複数のインターフェイスにタイマーを定義する場合、タイマーの細かさは、ルータ内のインターフェイスのいずれかに定義された最も低い値によって決まります。この細かさの間隔でルータが「再起動」し、必要に応じて、アップデートを送信します。細かさの詳細については、『*Cisco IOS AppleTalk and Novell IPX Command Reference*』の「Novell IPX Commands」の章を参照してください。

ネットワーク上の一部の PC が低速であるか、低速のインターフェイスが存在する場合は、複数パケットのアップデートでパケット間の遅延を設定することがあります。

インターフェイス単位で RIP アップデート タイマーを調整するには、インターフェイス コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipx update interval** {**rip** | **sap**} {*value* | **changes-only** | passive}
5. **ipx output-rip-delay** *delay*
6. **ipx triggered-rip-delay** *delay*
7. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx update interval** {**rip** | **sap**} {*value* | **changes-only** | **passive**} **例：** `Router(config-if)# ipx update interval rip 22`	RIP アップデート タイマーを調整します。
ステップ 5	**ipx output-rip-delay** *delay* **例：** `Router(config-if)# ipx output-rip-delay 21`	単一のインターフェイスに送信される複数パケットのルーティング アップデート間の遅延を調整します。
ステップ 6	**ipx triggered-rip-delay** *delay* **例：** `Router(config-if)# ipx triggered-rip-delay 12`	単一のインターフェイスに送信される複数パケットでトリガーされるルーティング アップデート間の遅延を調整します。
ステップ 7	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グローバル ベースで RIP アップデート タイマーを調整するには、グローバル コンフィギュレーション モードで次のいずれかまたは両方のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx default-output-rip-delay** *delay*
4. **ipx default-triggered-rip-delay** *delay*
5. **end**

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。 • 必要に応じて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	**ipx default-output-rip-delay** *delay* **例：** `Router(config)# ipx default-output-rip-delay 8`	すべてのインターフェイスに送信される複数パケットのルーティング アップデート間の遅延を調整します。
ステップ 4	**ipx default-triggered-rip-delay** *delay* **例：** `Router(config)# ipx default-triggered-rip-delay 7`	すべてのインターフェイスに送信される複数パケットでトリガーされるルーティング アップデート間の遅延を調整します。
ステップ 5	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

デフォルトでは、ネットワークまたはサーバの RIP エントリが、RIP タイマーの 3 倍の間隔で期限切れになります。間隔を制御する乗数を設定するには、インターフェイス 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. **interface** *type number*
4. **ipx rip-multiplier** *multiplier*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx rip-multiplier** *multiplier* **例：** `Router(config-if)# ipx rip-multiplier 23`	ネットワーク RIP エントリが期限切れになる間隔を設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP アップデート パケット サイズの設定

デフォルトでは、インターフェイスで送信される RIP アップデートの最大サイズが 432 バイトです。このサイズでは、それぞれ 8 バイトの 50 ルートに加えて、32 バイトの IPX RIP ヘッダーが許容されます。最大パケット サイズを変更するには、インターフェイス 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. **interface** *type number*
4. **ipx rip-max-packetsize** *bytes*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx rip-max-packetsize** *bytes* **例：** `Router(config-if)# ipx rip-max-packetsize 456`	インターフェイスで送信される RIP アップデートの最大パケット サイズを設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スタティック SAP テーブル エントリの設定

サーバは SAP を使用し、ブロードキャスト パケットによってサービスをアドバタイズします。Cisco IOS ソフトウェアではこの情報を、サーバ情報テーブルとも呼ばれる SAP テーブル内に保存します。このテーブルは動的に更新されます。クライアントは常に特定のサーバのサービスを使用するため、サーバ情報テーブルにエントリを明示的に追加する必要があります。スタティック SAP 割り当ては、ホップ カウントに関係なく、動的に学習された SAP テーブル内の同一のエントリよりも常に優先されます。スタティック SAP エントリに関連付けられたダイナミック ルートが失われたか、削除された場合、ルートを学習するまで、スタティック SAP エントリが通知されません。

スタティック エントリを SAP テーブルに追加するには、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. **ipx sap** *service-type name network.node socket hop-count*
4. **end**

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。 • 必要に応じて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	**ipx sap** *service-type name network.node socket hop-count* **例：** `Router(config)# ipx sap 234 strap1 1.1.2.1 222 12`	スタティック SAP テーブル エントリを指定します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

SAP 要求のキューの長さの設定

Cisco IOS ソフトウェアでは、サーバに到達しようと試行しているクライアントからのすべての保留中の Get Nearest Server（GNS）クエリーを含めて、処理する SAP 要求のリストが維持されます。電源に障害が発生した後、またはその他の予期しないイベントが発生した後にネットワークが再起動されると、サーバに対する何百もの要求がルータに殺到する可能性があります。通常、これらの多くは同じクライアントからの繰り返し要求です。保留中の SAP 要求キューで許容される最大長を設定できます。キューがいっぱいになると受信する SAP 要求が破棄されるため、クライアントは再送信する必要があります。

SAP 要求のキューの長さを設定するには、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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx sap-queue-maximum** *number*
4. **end**

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。 • 必要に応じて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	**ipx sap-queue-maximum** *number* **例：** `Router(config)# ipx sap-queue-maximum 33`	SAP キューの最大長を設定します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

SAP アップデート タイマーの調整

SAP アップデートが送信される間隔を調整できます。また、インターフェイス単位またはグローバル ベースで複数パケットの SAP アップデートのパケット間の遅延を設定することもできます。さらに、インターフェイス単位またはグローバル ベースで、複数パケットでトリガーされる SAP アップデートのパケット間の遅延を指定できます。

SAP アップデートが送信される間隔の変更は、低速のインターフェイスなどの帯域幅が制限されたポイントツーポイント リンクで最も役立ちます。指定されたネットワーク上のすべての IPX サーバおよびルータに、同じ SAP 間隔が設定されていることを確認する必要があります。そうでない場合、サーバが実際には起動しているが、ダウンしていると判断される可能性があります。

ほとんどの PC ベースのサーバでは、SAP アップデートが送信される間隔を変更することはできません。したがって、サーバが属しているイーサネットまたはトークン リング ネットワークの間隔を変更しないでください。

変更が発生した場合だけにアップデートを送信するようにルータを設定できます。**changes-only** キーワードを使用して、リンクが確立されたとき、リンクが管理的に切断されたとき、またはデータベースが変更されたときのみに SAP アップデートが送信されるように指定します。**changes-only** キーワードを指定すると、ルータで次のことが実行されます。

- リンクが確立されたときに、単一の完全なブロードキャスト アップデートを送信する
- リンクが切断されたときに、適切にトリガーされたアップデートを送信する
- 特定のサービス情報が変更されたときに、適切にトリガーされたアップデートを送信する

インターフェイス単位で SAP アップデート タイマーを変更するには、インターフェイス コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ipx update interval** {**rip** | **sap**} {*value* | **changes-only** | **passive**}
5. **ipx output-sap-delay** *delay*
6. **ipx triggered-sap-delay** *delay*
7. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx update interval** {**rip** | **sap**} {*value* | **changes-only** | **passive**} **例：** `Router(config-if)# ipx update interval sap 23`	SAP アップデートが送信される間隔を調整します。
ステップ 5	**ipx output-sap-delay** *delay* **例：** `Router(config-if)# ipx output-sap-delay 12`	単一のインターフェイスで送信される、複数パケットの SAP アップデートのパケット内遅延を調整します。
ステップ 6	**ipx triggered-sap-delay** *delay* **例：** `Router(config-if)# ipx triggered-sap-delay 10`	単一のインターフェイスで送信される、複数パケットでトリガーされる SAP アップデートのパケット内遅延を調整します。
ステップ 7	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

グローバル ベースで SAP アップデート タイマーを調整する（インターフェイス単位で遅延を設定する必要をなくす）には、グローバル コンフィギュレーション モードで次のいずれかまたは両方のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx default-output-sap-delay** *delay*
4. **ipx default-triggered-sap-delay** *delay*
5. **end**

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。 • 必要に応じて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	**ipx default-output-sap-delay** *delay* 例： `Router(config)# ipx default-output-sap-delay 11`	すべてのインターフェイスで送信される、複数パケットの SAP アップデートのパケット内遅延を調整します。
ステップ 4	**ipx default-triggered-sap-delay** *delay* 例： `Router(config)# ipx default-triggered-sap-delay 15`	すべてのインターフェイスで送信される、複数パケットでトリガーされる SAP アップデートのパケット内遅延を調整します。
ステップ 5	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

デフォルトでは、ネットワークまたはサーバの SAP エントリが、SAP アップデート間隔の 3 倍の間隔で期限切れになります。間隔を制御する乗数を設定するには、インターフェイス 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. **interface** *type number*
4. **ipx sap-multiplier** *multiplier*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx sap-multiplier** *multiplier* **例：** `Router(config-if)# ipx sap-multiplier 13`	ネットワークまたはサーバの SAP エントリが期限切れになる間隔を設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP アップデート パケット サイズの設定

デフォルトでは、インターフェイスで送信される SAP アップデートの最大サイズが 480 バイトです。このサイズでは、7 台のサーバ（それぞれ 64 バイト）に加えて、32 バイトの IPX RIP ヘッダーが許容されます。最大パケット サイズを変更するには、インターフェイス 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. **interface** *type number*
4. **ipx sap-max-packetsize** *bytes*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx sap-max-packetsize** *bytes* **例：** `Router(config-if)# ipx sap-max-packetsize 22`	インターフェイスで送信される SAP アップデートの最大パケット サイズを設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SAP-after-RIP のイネーブル化

IPX SAP-after-RIP 機能では、対応する RIP アップデートの完了直後に SAP ブロードキャストとユニキャスト アップデートが自動的に発生するように、SAP アップデートを RIP アップデートにリンクします。この機能を使用すると、サービスへの有効なルートがないため、リモート ルータがサービス情報を拒否しなくなります。この機能の結果として、定期的な SAP アップデートが RIP アップデートと同じ間隔で送信されます。

ルータのデフォルト動作では、設定に応じてそれぞれ独自のアップデート間隔で RIP と SAP の定期的なアップデートが送信されます。また、RIP と SAP の定期的なアップデートにはわずかな時間のずれがあるため、時間の経過とともに差が広がる傾向にあります。この機能では、SAP と RIP のアップデートが同期化されます。

単一のアップデートですべての SAP と RIP の情報を送信すると、帯域幅の需要が減少し、SAP ブロードキャストを誤って拒否することがなくなります。

SAP と RIP のアップデートをリンクすると、サービスへのルートが存在しないためにサービスが拒否されないことから、リモート ルータのサービス テーブルへの入力が迅速化されます。サービス テーブルへの入力の迅速化は、アップデート間隔が大幅に広がり、リンク上の定期的なアップデートのトラフィックの全体的なレベルが下がった WAN 回路で特に役立ちます。

RIP ブロードキャストの後に SAP アップデートを送信するようにルータを設定するには、インターフェイス 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. **interface** *type number*
4. **ipx update sap-after-rip**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx update sap-after-rip** **例：** `Router(config-if)# ipx update sap-after-rip`	RIP ブロードキャストの直後に SAP ブロードキャストを送信するようにルータを設定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP または SAP の汎用クエリー送信のディセーブル化

最初にリンクを確立するときに、RIP または SAP の汎用クエリーの送信をディセーブルにして、トラフィックを減少させ、帯域幅を節約することができます。

RIP と SAP の汎用クエリーは通常、回路が最初に起動したときにリモート ルータによって送信されます。WAN 回路では、それぞれの種類の 2 つの完全なアップデートがリンクを越えて送信されることがあります。最初のアップデートは、link-up イベントによってローカルでトリガーされた完全なブロードキャスト アップデートです。2 番目のアップデートは、リモート ルータから受信した汎用クエリーによってトリガーされる特定の（ユニキャスト）応答です。リンクが最初に確立されるときに汎用クエリーの送信をディセーブルにすると、トラフィックを単一のアップデートまで減少させ、帯域幅を節約できます。

インターフェイスが確立されるときに RIP または SAP の汎用クエリーの送信をディセーブルにするには、インターフェイス 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. **interface** *type number*
4. **no ipx linkup-request** {**rip** | **sap**}
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx linkup-request** {**rip** | **sap**} 例： `Router(config-if)# no ipx linkup-request rip`	インターフェイスが確立されるときに、RIP または SAP の汎用クエリーの送信をディセーブルにします。 • この例は、汎用 RIP クエリーの送信をディセーブルにする方法を示しています。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RIP または SAP の汎用クエリーの送信を再びイネーブルにするには、no ではない形式のコマンドを使用します。

GNS 要求への応答の制御

ルータが SAP GNS 要求に応答する方法を設定したり、これらの要求への応答における遅延時間を設定したり、これらの要求への応答の送信を完全にディセーブルにしたりできます。

デフォルトでは、必要に応じて、ルータが GNS 要求に応答します。たとえば、良好なメトリックを持つローカル サーバが存在している場合、ルータはそのセグメインで GNS 要求に応答しません。

GNS 要求を送信するためのデフォルトの方法は、アベイラビリティが最後に学習されたサーバで応答することです。

GNS 要求への応答を制御するには、グローバル コンフィギュレーション モードで次のいずれかまたは両方のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx gns-round-robin**
4. **ipx gns-response-delay** [*milliseconds*]
5. **end**

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。 • 必要に応じて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	**ipx gns-round-robin** **例：** `Router(config)# ipx gns-round-robin`	ラウンドロビン選択方法を使用して GNS 要求に応答します。
ステップ 4	**ipx gns-response-delay** [*milliseconds*] **例：** `Router(config)# ipx gns-response-delay 22`	GNS 要求に応答するときの遅延を設定します。
ステップ 5	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

（注） **ipx gns-response-delay** コマンドは、インターフェイス コンフィギュレーション コマンドとしてもサポートされます。特定のインターフェイスのグローバル遅延値を上書きするには、インターフェイス コンフィギュレーション モードで **ipx gns-response-delay** コマンドを使用します。

インターフェイス単位で GNS クエリーをディセーブルにするには、インターフェイス 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. **interface** *type number*
4. **ipx gns-reply-disable**

5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx gns-reply-disable** **例：** `Router(config-if)# ipx gns-reply-disable`	Get Nearest Server（GNS）クエリーへの応答の送信をディセーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ロード シェアリングの設定

ラウンドロビンまたはホスト単位のロード シェアリングを実行するように IPX を設定するには、ここで説明するタスクを実行します。

- ラウンドロビン ロード シェアリングのイネーブル化（P.84）（任意）
- ホスト単位のロード シェアリングのイネーブル化（P.85）（任意）

ラウンドロビン ロード シェアリングのイネーブル化

宛先への等価コストのパラレル パスの最大数を設定できます（パスのコストが異なる場合、Cisco IOS ソフトウェアで高コストのルートよりも低コストのルートが優先されて選択されることに注意してください）。その後、ラウンドロビン方式のパケット単位で出力が分割されます。つまり、最初のパケットが最初のパスで送信され、2 番目のパケットが 2 番目のパスで送信されます。最後のパスに到達したとき、次のパケットが最初のパスに送信され、その次のパケットが 2 番目のパスに送信されます。このラウンドロビン方式は、ファースト スイッチングがイネーブルかどうかに関係なく使用されます。

等価コスト パスの数を制限すると、メモリに制限がある場合、または非常に大規模な設定でルータ上のメモリを節約できます。さらに、out-of-sequence パケットのキャッシュ能力が制限されている多数の複数パスおよびシステムが存在しているネットワークでは、多数のパス間でトラフィックが分割される場合にパフォーマンスが低下する可能性があります。

パスの最大数を設定するには、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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx maximum-paths** *paths*
4. **end**

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。 • 必要に応じて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	**ipx maximum-paths** *paths* **例：** `Router(config)# ipx maximum-paths 26`	宛先への等価コスト パスの最大数を設定します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ホスト単位のロード シェアリングのイネーブル化

ipx maximum-paths を 1 よりも大きな値に設定した場合のデフォルト動作は、ラウンドロビン ロード シェアリングになります。ラウンドロビン ロード シェアリングは、個々のエンド ホストまたはユーザ セッションに関係なく、連続する等価コスト パスでデータ パケットを送信することによって動作します。パスの使用率によって転送速度が向上しますが、特定のエンド ホストに送信されるパケットが異なるパスを通過し、正しくない順序で到着する可能性があります。

ホスト単位のロード シェアリングをイネーブルにすると、正しくない順序でパケットが到着する可能性を解決できます。ホスト単位のロード シェアリングでも、ロード シェアリングを実現するためにルータは複数の等価コスト パスを使用します。ただし、複数の等価コスト パスが使用可能な場合でも、特定のエンド ホストへのパケットが同じパスを通過することが保証されます。異なるエンド ホストのトラフィックは異なるパスを通過する傾向がありますが、真のロード バランシングは保証されません。ロード バランシングの実際の達成度は、ワークロードの実際の性質に応じて異なります。

ホスト単位のロード シェアリングをイネーブルにするには、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. **ipx maximum-paths** *paths*
4. **ipx per-host-load-share**
5. **end**

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。 • 必要に応じて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	**ipx maximum-paths** *paths* **例：** `Router(config)# ipx maximum-paths 22`	宛先への等価コスト パスの最大数を 1 よりも大きな値に設定します。
ステップ 4	**ipx per-host-load-share** **例：** `Router(config)# ipx per-host-load-share`	ホスト単位のロード シェアリングをイネーブルにします。
ステップ 5	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ブロードキャスト メッセージの使用の指定

ブロードキャスト メッセージの使用を指定するには、ここで説明するタスクを実行します。

- ヘルパー アドレスを使用したブロードキャスト パケットの転送（P.86）（任意）
- IPX ダイレクト ブロードキャスト パケットのファースト スイッチングのイネーブル化（P.88）（任意）

ヘルパー アドレスを使用したブロードキャスト パケットの転送

ルータは通常、すべてのブロードキャスト要求をブロックし、他のネットワーク セグメントには転送しないため、ネットワーク全体でのパフォーマンスの低下が防止されます。ただし、他のネットワーク セグメント上のヘルパー アドレスへのブロードキャスト パケットの転送を、ルータでイネーブルにすることは可能です。

ヘルパー アドレスの動作

ヘルパー アドレスは、認識不能なブロードキャスト パケットを受信できる別のセグメント上のネットワークおよびノードを指定します。認識不能なブロードキャスト パケットとは、ローカル ネットワークを宛先としない RIP 以外および SAP 以外のパケットです。

ヘルパー アドレスが設定されたインターフェイスが、認識不能なブロードキャスト パケットを受信すると、Cisco IOS ソフトウェアでブロードキャスト パケットがユニキャストに変更され、他のネットワーク セグメント上の指定されたネットワークおよびノードにパケットが送信されます。認識不能なブロードキャスト パケットが、ネットワーク全体にフラッディングされるわけではありません。

ヘルパー アドレスでは、ブロードキャスト パケットがホップ可能な回数に制限がありません。

ファースト スイッチングのサポート

Cisco IOS では、ヘルパーで処理されたブロードキャスト パケットのファースト スイッチングがサポートされます。

ヘルパー アドレスの使用条件

ブロードキャスト パケット（タイプ 20 パケットを除く）を他のネットワーク セグメントに転送する場合、ヘルパー アドレスを使用します。

ブロードキャスト パケットのヘルパー アドレスへの転送は、ネットワーク セグメントに特定のタイプのブロードキャスト要求に対応できるエンドホストがない場合に役立つことがあります。ブロードキャスト パケットを処理できるサーバまたはネットワークを指定できます。

ヘルパー アドレスとタイプ 20 伝播の関係

タイプ 20 パケット伝播は、タイプ 20 パケットを他のネットワーク セグメントに転送するために使用します。タイプ 20 パケットの転送の詳細については、この章の「タイプ 20 パケットの転送の制御」の項を参照してください。

ネットワークで、ヘルパー アドレスとタイプ 20 伝播を組み合わせて使用できます。ヘルパー アドレスを使用して、タイプ 20 以外のブロードキャスト パケットを転送し、タイプ 20 伝播を使用して、タイプ 20 ブロードキャスト パケットを転送します。

実装の注意事項

ヘルパー アドレスの使用は Novell に準拠していません。ただし、ヘルパー アドレスを使用すると、ネットワークをフラッディングすることなく、ルータがブロードキャスト パケットを、それを処理可能なネットワーク セグメントに転送することができます。また、タイプ 20 伝播がサポートされていないバージョンの Cisco IOS を実行しているルータで、タイプ 20 パケットを転送することもできます。

Cisco IOS ソフトウェアでは、all-networks flooded ブロードキャスト（*all-nets flooding* とも呼ばれる）がサポートされます。これは、すべてのネットワークに転送されるブロードキャスト メッセージです。all-nets flooding では、受信側ネットワークが過負荷になり、他のトラフィックが通過できなくなる可能性があるため、使用する際には注意が必要です。必要な場合のみに使用してください。

転送されるブロードキャスト パケットを制御するアクセス リストを定義するには、この章で説明した **ipx helper-list** コマンドを使用します。

ヘルパー アドレスの使用

ブロードキャスト パケットを転送するためのヘルパー アドレスを指定するには、インターフェイス 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. **interface** *type number*
4. **ipx helper-address** *network.node*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx helper-address** *network.node* **例：** `Router(config-if)# ipx helper-address 1.1.2.1`	ブロードキャスト メッセージの転送のためのヘルパー アドレスを指定します。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

1 つのインターフェイス上で複数のヘルパー アドレスを指定できます。

ヘルパー アドレスを使用してブロードキャスト メッセージを転送する例については、この章の最後にある「ブロードキャストを制御するヘルパー機能：例」の項を参照してください。

IPX ダイレクト ブロードキャスト パケットのファースト スイッチングのイネーブル化

デフォルトでは、Cisco IOS ソフトウェアが、ヘルパーで処理されたパケットをブロードキャスト アドレスにスイッチングします。このような IPX ダイレクト ブロードキャスト パケットのファースト スイッチングをイネーブルにするには、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. **ipx broadcast-fastswitching**
4. **end**

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。 • 必要に応じて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	**ipx broadcast-fastswitching** **例：** `Router(config)# ipx broadcast-fastswitching`	IPX ダイレクト ブロードキャスト パケットのファースト スイッチングをイネーブルにします。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IPX ファースト スイッチングのディセーブル化

デフォルトでは、ファースト スイッチングがサポートされるすべてのインターフェイス上で、ファースト スイッチングがイネーブルになっています。

ファースト スイッチングを使用すると、以前のパケットで作成されたキャッシュを使用してパケットをスイッチングすることによって、スループットが向上します。ファースト スイッチングは、デフォルトでファースト スイッチングがサポートされるすべてのインターフェイス上でイネーブルになっています。

通常、ファースト スイッチングがイネーブルになっている場合、パケット転送のパフォーマンスが高まります。ただし、インターフェイス カードのメモリ容量を節約したり、広帯域幅インターフェイスで大量の情報が低帯域幅のインターフェイスに書き込まれる場合の輻輳を回避したりするために、ファースト スイッチングをディセーブルにする場合もあります。

注意 ファースト スイッチングをオフにすると、システムのオーバーヘッドが増加します。

IPX ファースト スイッチングをディセーブルにするには、インターフェイス 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. **interface** *type number*
4. **no ipx route-cache**
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx route-cache** **例：** `Router(config-if)# no ipx route-cache`	IPX ファースト スイッチングをディセーブルにします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ルート キャッシュの調整

ルート キャッシュを調整すると、ルート キャッシュのサイズを制御し、メモリ消費を減少させ、ルータのパフォーマンスを向上させることができます。ルート キャッシュのサイズと無効化を制御することによって、これらのタスクを実行します。ここでは、このような任意タスクについて説明します。

- ルート キャッシュのサイズ制御（P.90）（任意）
- ルート キャッシュの無効化の制御（P.91）（任意）

ルート キャッシュのサイズ制御

IPX ルート キャッシュに保存されるエントリの数を制限すると、ルータのメモリの空き容量が増え、ルータの処理が容易になります。

ルート キャッシュに保存するエントリが多すぎると、大量のルータ メモリが消費され、ルータの処理速度が低下する可能性があります。この状況は、NetWare 用のネットワーク管理アプリケーションを実行する大規模なネットワークでは一般的です。

たとえば、ネットワーク管理ステーションで非常に大規模な（ノード数が 50,000 を超える）Novell ネットワーク内のすべてのクライアントおよびサーバを管理している場合、ローカル セグメント上のルータにルート キャッシュ エントリが殺到する可能性があります。このようなルータでルート キャッシュ エントリの最大数を設定すると、ルータのメモリの空き容量が増え、ルータの処理が容易になります。

IPX ルート キャッシュのエントリの最大制限を設定するには、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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx route-cache max-size** *size*
4. **end**

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。 • 必要に応じて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	**ipx route-cache max-size** *size* **例：** `Router(config)# ipx route-cache max-size 226`	IPX ルート キャッシュのエントリの最大制限を設定します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ルート キャッシュに指定された制限を超えるエントリが存在しても、過剰なエントリは削除されません。ただし、ルート キャッシュの無効化が使用されている場合は、過剰なエントリが削除されます。ルート キャッシュ エントリの無効化の詳細については、この章の「ルート キャッシュの無効化の制御」の項を参照してください。

ルート キャッシュの無効化の制御

非アクティブな fast-switch キャッシュ エントリを無効化するようにルータを設定することができます。このようなエントリが 1 分間無効のままになっている場合、ルータはルート キャッシュからエントリを消去します。

無効のエントリを消去すると、ルート キャッシュのサイズが小さくなり、メモリ消費が減少し、ルータのパフォーマンスが向上します。また、エントリを消去すると、ルート キャッシュ情報が正確になります。

有効な fast-switch キャッシュ エントリがどれほどの期間だけ非アクティブになっていると、ルータで無効化されかを指定します。また、ルータで 1 分間に無効化できるキャッシュ エントリ数も指定できます。

非アクティブな fast-switch キャッシュ エントリを無効化するようにル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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx route-cache inactivity-timeout** *period* [*rate*]
4. **end**

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。 • 必要に応じて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	**ipx route-cache inactivity-timeout** *period* [*rate*] **例：** `Router(config)# ipx route-cache inactivity-timeout 12 10`	非アクティブな fast-switch キャッシュ エントリを無効化します。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ipx route-cache inactivity-timeout コマンドを **ipx route-cache max-size** コマンドと組み合わせて使用すると、ルート キャッシュのサイズが小さくなり、エントリが最新状態に保たれます。

デフォルト ルートの調整

IPX ネットワークでデフォルト ルートの使用を調整できます。デフォルト ルートとしての、ネットワーク番号 -2 の使用をオフにできます。また、ルータでデフォルト RIP ルートだけをインターフェイスにアドバタイズするように指定することもできます。ここでは、このような任意タスクについて説明します。

- デフォルト ルートとしてのネットワーク番号 -2 のディセーブル化（P.92）（任意）
- デフォルト RIP ルートのみのアドバタイズ（P.93）（任意）

デフォルト ルートとしてのネットワーク番号 -2 のディセーブル化

デフォルト ルートは、宛先ネットワークへのルートが不明な場合に使用されます。宛先アドレスへのルートが不明なすべてのパケットがデフォルト ルートに転送されます。デフォルトでは、IPX でネットワーク番号 -2（0xFFFFFFFE）がデフォルト ルートとして扱われます。

デフォルト ルートの概要については、この章の「IPX デフォルト ルート」の項を参照してください。IPX のデフォルトのルートを処理する方法に関する詳細な背景情報については、Novell の『*NetWare Link Services Protocol（NLSP）Specification, Revision 1.1*』を参照してください。

デフォルトでは、Cisco IOS ソフトウェアでネットワーク -2 がデフォルト ルートとして扱われます。このデフォルトの動作をディセーブルにして、ネットワーク -2 をネットワークの通常のネットワーク番号として使用することができます。

ネットワーク番号 -2 のデフォルト ルートとしての使用をディセーブルにするには、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. **no ipx default-route**
4. **end**

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。 • 必要に応じて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 ipx default-route** **例：** `Router(config)# no ipx default-route`	デフォルト ルートとしての扱いをディセーブルにします。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

デフォルト RIP ルートのみのアドバタイズ

特に設定される場合を除いて、既知のすべての RIP ルートが各インターフェイスからアドバタイズされます。ただし、既知の場合はデフォルト RIP ルートのみをアドバタイズできるため、ルーティングテーブルのサイズが大きい場合に、CPU のオーバーヘッドが大幅に減少します。

インターフェイスからデフォルト ルートのみをアドバタイズするには、インターフェイス 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. **interface** *type number*
4. **ipx advertise-default-route-only** *network*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx advertise-default-route-only** *network* **例：** `Router(config-if)# ipx advertise-default-route-only 563`	デフォルト RIP ルートのみをアドバタイズします。
ステップ 5	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

奇数長のパケットのパディング

一部の IPX エンド ホストは、偶数長のイーサネット パケットのみを受け入れます。パケットの長さが奇数の場合、エンド ホストで受信できるように、パケットに余分なバイトをパディングする必要があります。Cisco IOS のデフォルトでは、奇数長のイーサネット パケットがパディングされます。

ただし、特定のトポロジで、パディングされないイーサネット パケットがリモート イーサネット ネットワークに転送される場合があります。特定の条件下で、この問題の一時的な回避策として、中間メディアでパディングをイネーブルにできます。このタスクは、カスタマー エンジニアまたはその他のサービス担当者に指示された場合にのみ実行してください。

奇数長パケットのパディングをイネーブルにするには、インターフェイス 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. **interface** *type number*
4. **no ipx route-cache**
5. **ipx pad-process-switched-packets**
6. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx route-cache** **例：** `Router(config-if)# no ipx route-cache`	ファースト スイッチングをディセーブルにします。
ステップ 5	**ipx pad-process-switched-packets** **例：** `Router(config-if)# ipx pad-process-switched-packets`	奇数長パケットのパディングをイネーブルにします。
ステップ 6	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPX ネットワークのシャットダウン

IPX ネットワークは、2 つの方法で管理的にシャットダウンできます。その方法の 1 つでは、コンフィギュレーション内にネットワークが存在したままになりますが、アクティブではなくなります。シャットダウンすると、ネットワークからネイバーにシャットダウンを通知するアップデート パケットが送信されるため、このネットワークを介して学習したルートおよびサービスのタイム アウトを待つことなく、ネイバー システムでルーティング テーブル、SAP テーブル、およびその他のテーブルを更新できます。

コンフィギュレーション内にネットワークが存在したままの IPX ネットワークをシャットダウンするには、インターフェイス 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. **interface** *type number*
4. **ipx down** *network*
5. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**ipx down** *network* 例： `Router(config-if)# ipx down 345`	IPX ネットワークをシャットダウンしますが、コンフィギュレーション内にネットワークが存在したままになります。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPX ネットワークをシャットダウンし、そのネットワークをコンフィギュレーションから削除するには、インターフェイス コンフィギュレーション モードで次のいずれかのコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipx network**
5. **no ipx network** *network*（ここで、network は 1 のプライマリ インターフェイス）
6. **no ipx network** *network*（ここで、network はセカンダリ インターフェイスの番号 [1 以外]）

7. **end**

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。 • 必要に応じて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 ethernet0/1`	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 4	**no ipx network** **例：** `Router(config-if)# ipx down network3`	IPX ネットワークをシャットダウンし、コンフィギュレーションから削除します。
ステップ 5	**no ipx network** *network* （ここで、*network* は 1 のプライマリ インターフェイス） **例：** `Router(config-if)# no ipx network 1`	インターフェイスで複数のネットワークが設定されている場合、すべてのネットワークをシャットダウンし、インターフェイスから削除します。
ステップ 6	**no ipx network** *network*（ここで、*network* はセカンダリ インターフェイスの番号 [1 以外]） **例：** `Router(config-if)# no ipx network 323`	インターフェイスで複数のネットワークが設定されている場合、セカンダリ ネットワークのいずれかをシャットダウンし、インターフェイスから削除します。
ステップ 7	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスで複数のネットワークが設定されていて、セカンダリ ネットワークのいずれかをシャットダウンしてインターフェイスから削除する場合、セカンダリ ネットワークのいずれかのネットワーク番号を指定する以前のテーブルで、2 番目のコマンドを使用します。

IPX ネットワークをシャットダウンする例については、この章の最後にある「IPX ルーティング：例」の項を参照してください。

IPX アカウンティングの設定

IPX アカウンティングを使用すると、IPX パケットおよび Cisco IOS ソフトウェアでスイッチングされるバイト数についての情報を収集できます。情報は、発信元と宛先の IPX アドレスに基づいて収集されます。IPX アカウンティングでは、IPX アカウンティングが設定されているインターフェイスにルーティングされる IPX トラフィックのみを追跡します。ルータ自体で生成されたか、終了したトラフィックは追跡しません。

Cisco IOS ソフトウェアでは、アクティブなデータベースとチェックポイント データベースの 2 つのアカウンティング データベースが維持されます。アクティブなデータベースには、データベースがクリアされるまで追跡されるアカウンティング データが保存されます。アクティブなデータベースがクリアされると、保存されていたデータはチェックポイント データベースにコピーされます。これらの 2 つのデータベースを組み合わせて使用すると、現在のトラフィックと以前にルータを通過したトラフィックの両方を監視できます。

スイッチングのサポート

プロセスとファースト スイッチングでは、IPX アカウンティングの統計情報がサポートされます。自律およびシリコン スイッチング エンジン（SSE）のスイッチングでは、IPX アカウンティングの統計情報がサポートされます。

（注） MIP インターフェイスでは、CiscoBus（Cbus）と SSE はサポートされません。

アクセス リストのサポート

IPX アクセス リストでは、IPX アカウンティングの統計情報がサポートされます。

IPX アカウンティング タスク リスト

IPX アカウンティングを設定するには、ここで説明するタスクを実行します。最初のタスクは必須で、残りのタスクは任意です。

- IPX アカウンティングのイネーブル化（P.98）（必須）
- IPX アカウンティングのカスタマイズ（P.99）（任意）

IPX アカウンティングのイネーブル化

IPX アカウンティングをイネーブルにするには、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. **ipx accounting-list** *network-host network-mask*
4. **end**

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。 • 必要に応じて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	**ipx accounting-list** *newtork-host network-mask* **例：** `Router(config)# ipx accounting-list 1.2.1.0 255.0.1.255`	IPX アカウンティングをイネーブルにします。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IPX アカウンティングのカスタマイズ

IPX アカウンティングをカスタマイズするには、グローバル コンフィギュレーション モードで次のいずれかまたは複数のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipx accounting-threshold** *threshold*
4. **ipx accounting-transits** *count*
5. **ipx accounting-list** *network-host network-mask*
6. **end**

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。 • 必要に応じて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	**ipx accounting-threshold** *threshold* **例：** `Router(config)# ipx accounting-threshold 23`	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	**ipx accounting-transits** *count* **例：** `Router(config)# ipx accounting-transits 333`	中継エントリの最大数を設定します。
ステップ 5	**ipx accounting-list** *network-host network-mask* **例：** `Router(config)# ipx accounting-list 1.2.1.0 255.255.0.1`	IPX アカウンティング情報が保存されるフィルタ ネットワークを定義します。ネットワークごとに 1 つのコマンドを使用します。
ステップ 6	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

中継エントリとは、**ipx accounting-list** コマンドで指定されたどのネットワークとも一致しないデータベース内のエントリです。

インターフェイス上で IPX アカウンティングをイネーブルにするものの、アカウンティング リストを指定しない場合、IPX アカウンティングでは、アカウンティングのしきい値の制限に達するまで、インターフェイスを通過するすべてのトラフィック（すべての中継エントリ）を追跡します。

IPX アカウンティングを設定する方法の例については、この章の最後にある「IPX アカウンティング：例」の項を参照してください。

LAN 間の IPX の設定

Cisco IOS ソフトウェアでは、イーサネット エミュレート LAN とトークン リング エミュレーション LAN の間での、IPX のルーティングがサポートされます。エミュレート LAN およびこれらの間での IPX のルーティングの詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Configuring LAN Emulation」の章を参照してください。

VLAN 間の IPX の設定

Cisco IOS ソフトウェアでは、VLAN 間の IPX のルーティングがサポートされます。Novell NetWare 環境を使用しているユーザは、VLAN の境界を越えて Inter-Switch Link（ISL）のカプセル化をルーティングする 4 つの IPX イーサネットのカプセル化のいずれかを使用できます。VLAN および ISL でのこれらの間での IPX のルーティングの詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Configuring Routing Between VLANs with ISL Encapsulation」の章を参照してください。

IPX マルチレイヤ スイッチングの設定

Cisco IOS ソフトウェアでは、IPX Multilayer Switching（MLS; マルチレイヤ スイッチング）がサポートされます。IPX MLS の詳細については、『*Cisco IOS Switching Services Configuration Guide*』の「Multilayer Switching」の章を参照してください。

IPX ネットワークのモニタリングおよびメンテナンス

IPX ネットワークのモニタおよびメンテナンスを行うには、ここで説明するオプションのタスクを実行します。

- モニタリングとメンテナンスの一般タスク（P.101）（任意）
- IPX Enhanced IGRP のモニタリングおよびメンテナンス（P.103）（任意）
- IPX アカウンティングのモニタリングおよびメンテナンス（P.105）（任意）

モニタリングとメンテナンスの一般タスク

ここで説明するように、1 つまたは複数のモニタリングおよびメンテナンスの一般タスクを実行できます。

- キャッシュ、テーブル、インターフェイスおよび統計情報のモニタリングとメンテナンス（P.101）（任意）
- ping パケットのタイプと使用の指定（P.102）（任意）
- ネットワーク接続のトラブルシューティング（P.103）（任意）

キャッシュ、テーブル、インターフェイスおよび統計情報のモニタリングとメンテナンス

Novell IPX ネットワーク内のキャッシュ、テーブル、インターフェイスおよび統計情報のモニタおよびメンテナンスを実行するには、EXEC モードで次のいずれかまたは複数のコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 1	`Router> clear ipx cache`	IPX ファースト スイッチング キャッシュ内のすべてのエントリを削除します。
ステップ 2	`Router> clear ipx route [network | *]`	IPX ルーティング テーブル内のエントリを削除します。
ステップ 3	`Router> clear ipx traffic`	IPX トラフィック カウンタをクリアします。
ステップ 4	`Router> show ipx cache`	IPX ファースト スイッチング キャッシュ内のエントリをリストします。

	コマンドまたはアクション	目的
ステップ 5	Router> **show ipx interface** [*type number*]	ルータで設定された IPX インターフェイスのステータスと、各インターフェイスで設定されたパラメータを表示します。
ステップ 6	Router> **show ipx route** [*network*] [**default**] [**detailed**]	IPX ルーティング テーブル内のエントリをリストします。
ステップ 7	Router> **show ipx servers** [**unsorted** | **sorted** [**name** | **net** | **type**]] [**regexp** *name*]	SAP アドバタイズメントによって検出されたサーバをリストします。
ステップ 8	Router> **show ipx traffic** [**since** {**bootup** | **show**}]	送受信される IPX パケットの数とタイプについての情報を表示します。
ステップ 9	Router> **show sse summary**	SSE の統計情報の要約を表示します。

ping パケットのタイプと使用の指定

Cisco IOS ソフトウェアでは、シスコの ping と、NLSP 仕様または診断要求パケットで定義されている Novell の標準 ping を送信できます。デフォルトでは、シスコの ping が生成されます。ping のタイプを選択するには、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. **ipx ping-default** {**cisco** | **novell** | **diagnostic**}
4. **end**

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。 • 必要に応じて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	**ipx ping-default** {**cisco** | **novell** | **diagnostic**} **例：** Router(config)# ipx ping-default novell	ping のタイプを選択します。
ステップ 4	**end** **例：** Router(config)# end	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IPX 診断 ping 機能では、ユニキャストまたはブロードキャスト診断パケットを受け入れて処理することによって、診断に関する問題を解決します。現在の IPX **ping** コマンドは、診断パケットを使用して他のステーションに ping を送信し、応答パケットに設定情報を表示するよう拡張されたものです。

（注） あるステーションから別のステーションに ping が送信されると、すぐに応答が返信されるはずです。**ipx ping-default** コマンドが診断に設定された場合は、応答が複数のパケットで構成され、各ノードは要求を受信してから 0.5 秒以内に返信することが期待されます。end-of-message フラグが存在しないため、遅延が生じ、要求元はすべての応答が到着するまで待機する必要があります。したがって、詳細モードでは、応答データが表示されるまでに 0.5 秒の短い遅延が発生する可能性があります。
ipx ping コマンドで **diagnostic** キーワードを使用すると、到着可能性テストの実行に使用できます。正確なラウンドトリップ遅延の測定には使用しないでください。

ping を開始するには、EXEC モードで次のいずれかのコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 1	Router# **ping ipx** *network.node*	基本 IPX ネットワーク接続を診断します（ユーザ レベルコマンド）。
ステップ 2	Router# **ping** [**ipx**] [*network.node*]	基本 IPX ネットワーク接続を診断します（特権コマンド）。

ネットワーク接続のトラブルシューティング

IPX の宛先を追跡し、ラウンドトリップ遅延を測定するには、ユーザ EXEC モードまたは特権 EXEC モードで次のコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 1	Router> **trace** [*protocol*] [*destination*]	ネットワーク上のパケット ルートを追跡します（ユーザまたは特権）。

（注） ユーザ EXEC モードでは、ルート追跡のタイムアウト間隔、プローブ カウント、最小と最大の存続可能時間、および詳細モードを変更することはできません。これらを実行するには、特権 EXEC モードで **trace** コマンドを使用します。

IPX Enhanced IGRP のモニタリングおよびメンテナンス

IPX ネットワークで Enhanced IGRP のモニタおよびメンテナンスを行うには、EXEC モードで次のいずれかまたは複数のコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 1	Router> **show ipx eigrp neighbors** [**servers**] [*autonomous-system-number* | *type number* [**regexp** *name*]]	IPX Enhanced IGRP によって検出されたネイバーをリストします。
ステップ 2	Router> **show ipx eigrp interfaces** [*type number*] [*as-number*]	Enhanced IGRP に対して設定されたインターフェイスに関する情報を表示します。
ステップ 3	Router> **show ipx eigrp topology** [*network*]	IPX Enhanced IGRP トポロジ テーブルの内容を表示します。

	コマンドまたはアクション	目的
ステップ 4	Router> **show ipx route** [*network*]	Enhanced IGRP エントリを含めて、IPX ルーティング テーブルの内容を表示します。
ステップ 5	Router> **show ipx traffic**	Enhanced IGRP トラフィックを含めて、IPX トラフィックについての情報を表示します。

Enhanced IGRP ネイバーの隣接関係の変更ロギング

ルーティング システムの安定性を監視し、問題を検出しやすくするために、ネイバー ルータとの隣接関係の変更のロギングをイネーブルにできます。デフォルトでは、隣接関係の変更はロギングされません。

Enhanced IGRP ネイバーの隣接関係の変更ロギングをイネーブルにするには、IPX ルータ 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. **ipx router** {**eigrp** | **rip**} *autonomous-system-number*
4. **log-neighbor-changes**
5. **end**

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。 • 必要に応じて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	**ipx router** {**eigrp** | **rip**} **autonomous-system-number** **例：** Router(config)# ipx router eigrp 123	自律システム番号付きの IPX ルーティング プロトコルを指定し、IPX ルータ 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	**log-neighbor-changes** **例：** Router(config-ipx-router)# log-neighbor-changes	Enhanced IGRP ネイバーの隣接関係の変更ロギングをイネーブルにします。
ステップ 5	**end** **例：** Router(config-ipx-router)# end	IPX ルータ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPX アカウンティングのモニタリングおよびメンテナンス

IPX ネットワークで IPX アカウンティングのモニタリングおよびメンテナンスを行うには、EXEC モードで次のコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 1	`Router> clear ipx accounting [checkpoint]`	IPX アカウンティング データベースまたはアカウンティング チェックポイント データベースの、すべてのエントリを削除します。
ステップ 2	`Router> show ipx accounting [checkpoint]`	IPX アカウンティング データベースまたはアカウンティング チェックポイント データベースのエントリをリストします。

Novell IPX の設定例

ここでは、次の IPX の設定例について詳しく説明します。

- IPX ルーティング：例（P.105）
- Enhanced IGRP：例（P.109）
- WAN 上の IPX：例（P.111）
- IPX ネットワーク アクセス：例（P.114）
- ブロードキャストを制御するヘルパー機能：例（P.121）
- IPX アカウンティング：例（P.124）

IPX ルーティング：例

ここでは、単一のネットワークと複数のネットワークのインターフェイス上で IPX ルーティングをイネーブルにする例を示します。また、ルーティング プロトコルのさまざまな組み合わせをイネーブルおよびディセーブルにする例も示します。

ここでは、次の例を示します。

- 単一ネットワークでの IPX ルーティング：例（P.105）
- 複数ネットワークでの IPX ルーティング：例（P.106）
- IPX ルーティング プロトコル：例（P.108）

単一ネットワークでの IPX ルーティング：例

次に、IPX ルーティングをイネーブルにして、最初の IEEE 対応のインターフェイス（この例では、イーサネット 0）の IPX ホスト アドレスをデフォルトにする例を示します。IPX ネットワーク 2abc および 1def に対して、イーサネット 0 およびイーサネット 1 でルーティングがイネーブルになります。

```
ipx routing
interface ethernet 0
 ipx network 2abc
interface ethernet 1
 ipx network 1def
```

複数ネットワークでの IPX ルーティング：例

複数のネットワークがサポートされるインターフェイスで IPX をイネーブルにする方法は 2 つあります。サブインターフェイスまたは、プライマリ ネットワークおよびセカンダリ ネットワークを使用できます。ここでは、それぞれの例を示します。

サブインターフェイスの例

次に、サブインターフェイスを使用して、イーサネット インターフェイス 0 上に 4 つの論理ネットワークを作成する例を示します。各サブインターフェイスのカプセル化は、それぞれ異なります。個々のサブインターフェイスで指定するインターフェイス コンフィギュレーション パラメータは、そのサブインターフェイスのみに適用されます。

```
ipx routing
interface ethernet 0.1
 ipx network 1 encapsulation novell-ether
interface ethernet 0.2
 ipx network 2 encapsulation snap
interface ethernet 0.3
 ipx network 3 encapsulation arpa
interface ethernet 0.4
 ipx network 4 encapsulation sap
```

（注） NLSP をイネーブルにして複数のカプセル化を同じ物理 LAN インターフェイスで設定するには、サブインターフェイスを使用する必要があります。セカンダリ ネットワークは使用できません。

各サブインターフェイスに対して **shutdown** 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、4 つのサブインターフェイスを個別に管理的にシャットダウンできます。次に、サブインターフェイスを管理的にシャットダウンする例を示します。

```
interface ethernet 0.3
 shutdown
```

ネットワーク 1 をダウンするには、次のコマンドを使用します。

```
interface ethernet 0.1
 ipx down 1
```

ネットワーク 1 を稼動状態に戻すには、次のコマンドを使用します。

```
interface ethernet 0.1
 no ipx down 1
```

インターフェイス上のすべてのネットワークを削除するには、次のインターフェイス コンフィギュレーション コマンドを使用します。

```
interface ethernet 0.1
 no ipx network
interface ethernet 0.2
 no ipx network
interface ethernet 0.3
 no ipx network
interface ethernet 0.4
 no ipx network
```

プライマリ ネットワークおよびセカンダリ ネットワークの例

（注） 次の例では、プライマリ ネットワークとセカンダリ ネットワークについて説明します。将来の Cisco IOS ソフトウェア リリースでは、プライマリ ネットワークとセカンダリ ネットワークがサポートされなくなります。サブインターフェイスを使用してください。

次に、プライマリ ネットワークとセカンダリ ネットワークを使用して、すでに説明した 4 つの同じ論理ネットワークを作成する例を示します。このインターフェイスで指定するインターフェイス設定パラメータは、すべての論理ネットワークに適用されます。たとえば、ルーティング アップデート タイマーを 120 秒に設定する場合、この値は 4 つのネットワークすべてに使用されます。

```
ipx routing
interface ethernet 0
 ipx network 1 encapsulation novell-ether
 ipx network 2 encapsulation snap secondary
 ipx network 3 encapsulation arpa secondary
 ipx network 4 encapsulation sap secondary
```

shutdown 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イーサネット インターフェイス 0 を管理的にシャットダウンする場合、この方法を使用して論理ネットワークを設定すると、4 つの論理ネットワークがすべてシャットダウンされます。**shutdown** コマンドを使用して、各論理ネットワークを個別にダウンすることはできません。ただし、**ipx down** コマンドを使用するとダウンできます。

次に、ネットワーク 1 をシャットダウンする例を示します。

```
interface ethernet 0
 ipx down 1
```

次に、ネットワークを稼動状態に戻す例を示します。

```
interface ethernet 0
 no ipx down 1
```

次に、インターフェイス上の 4 つのネットワークすべてをシャットダウンし、インターフェイス上のすべてのネットワークを削除する 2 つの例を示します。

```
 no ipx network

 no ipx network 1
```

次に、インターフェイス上のいずれかのセカンダリ ネットワーク（この場合、ネットワーク 2）を削除する例を示します。

```
 no ipx network 2
```

次に、FDDI インターフェイス 0.2 および 0.3 で IPX ルーティングをイネーブルにする例を示します。FDDI インターフェイス 0.2 では、カプセル化のタイプが SNAP です。FDDI インターフェイス 0.3 では、カプセル化のタイプが Novell FDDI_RAW です。

```
ipx routing
interface fddi 0.2
 ipx network f02 encapsulation snap
interface fddi 0.3
 ipx network f03 encapsulation novell-fddi
```

IPX ルーティング プロトコル：例

IPX に設定されるインターフェイスで、RIP、Enhanced IGRP、および NLSP の 3 つのルーティング プロトコルを実行できます。ここでは、ルーティング プロトコルのさまざまな組み合わせをイネーブルおよびディセーブルにする例を示します。

ipx routing グローバル コンフィギュレーション コマンドで IPX ルーティングをイネーブルにすると、RIP ルーティング プロトコルが自動的にイネーブルになります。次に、ネットワーク 1 および 2 で RIP をイネーブルにする例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 1
!
interface ethernet 1
 ipx network 2
```

次に、ネットワーク 1 および 2 で RIP をイネーブルにし、ネットワーク 1 で Enhanced IGRP をイネーブルにする例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 1
!
interface ethernet 1
 ipx network 2
!
ipx router eigrp 100
 network 1
```

次に、ネットワーク 2 で RIP をイネーブルにし、ネットワーク 1 で Enhanced IGRP をイネーブルにする例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 1
!
interface ethernet 1
 ipx network 2
!
ipx router eigrp 100
 ipx network 1
!
ipx router rip
 no ipx network 1
```

次に、ルータのイーサネット インターフェイス上で NLSP を設定する方法の例を示します。これらの両方のインターフェイスで RIP が自動的にイネーブルになることに注意してください。この例では、カプセル化のタイプがイーサネット 802.2 であると仮定しています。

```
ipx routing
 ipx internal-network 3
!
ipx router nlsp area1
area-address 0 0
!
interface ethernet 0
 ipx network e0 encapsulation sap
ipx nlsp area1 enable
!
```

```
interface ethernet 1
 ipx network e1 encapsulation sap
 ipx nlsp area1 enable
```

Enhanced IGRP：例

ここでは、IPX Enhanced IGRP ルーティングを設定するいくつかの例を示します。

- IPX Enhanced IGRP の例（P.109）
- VRF IPX SAP-Incremental IGRP の例（P.109）
- Enhanced IGRP SAP アップデートの例（P.109）
- SAP アップデートのアドバタイズメントと処理の例（P.110）
- IPX Enhanced IGRP の帯域幅の設定例（P.110）

IPX Enhanced IGRP の例

次に、自律システム 1 で Enhanced IGRP ルーティングのための 2 つのインターフェイスを設定する例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 10
!
interface serial 0
 ipx network 20
!
ipx router eigrp 1
 network 10
 network 20
```

VRF IPX SAP-Incremental IGRP の例

次に、IPX SAP Enhanced IGRP をイネーブルにするための設定例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 1
 ipx sap-incremental eigrp 1
 ipx sap-incremental split-horizon
!
ipx router eigrp 100
 network 1
```

Enhanced IGRP SAP アップデートの例

イーサネット インターフェイスに Enhanced IGRP 用に設定されたすべてのネイバーが含まれる場合、段階的に SAP アップデートを送信することによって、SAP パケットで使用される帯域幅を減らすことがあります。次に、SAP アップデートを段階的に送信する例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 10
```

```
 ipx sap-incremental eigrp 1
!
interface serial 0
 ipx network 20
!
ipx router eigrp 1
 network 10
 network 20
```

次に、Enhanced IGRP のためにシリアル回線でインクリメンタル SAP アップデートのみを送信する例を示します。

```
ipx routing
!
interface ethernet 0
 ipx network 10
!
interface serial 0
 ipx network 20
 ipx sap-incremental eigrp 1 rsup-only
!
ipx router eigrp 1
 network 10
 network 20
```

SAP アップデートのアドバタイズメントと処理の例

次に、Enhanced IGRP ルーティング プロセスによって、ネットワーク 3 からのサービスのみがアドバタイズされる例を示します。

```
access-list 1010 permit 3
access-list 1010 deny -1
!
ipx router eigrp 100
 network 3
 distribute-sap-list 1010 out
```

IPX Enhanced IGRP の帯域幅の設定例

次に、IPX Enhanced IGRP で使用される帯域幅を設定する例を示します。この例では、Enhanced IGRP プロセス 109 が 128-kbps の回路の最大 25 パーセント（32-kbps）を使用するように設定されます。

```
interface serial 0
 bandwidth 128
 ipx bandwidth-percent eigrp 109 25
```

次に、ルーティング ポリシーの理由で、56-kbps の回路の帯域幅を 20 kbps に設定する例を示します。Enhanced IGRP プロセス 109 は、回路の最大 200 パーセント（40 kbps）を使用するように設定されます。

```
interface serial 1
 bandwidth 20
 ipx bandwidth-percent eigrp 109 200
```

WAN 上の IPX：例

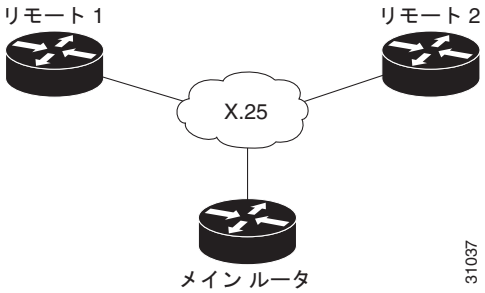
ここでは、WAN インターフェイスおよびダイヤル インターフェイスで IPX を設定する例を示します。

- WAN インターフェイスでの IPX の例（P.111）
- IPX over DDR の例（P.112）

WAN インターフェイスでの IPX の例

Cisco IOS ソフトウェアで、X.25 や PPP などの WAN プロトコルを実行しているシリアル インターフェイス上で IPX パケットを転送するように設定する場合、パケットが転送のためにカプセル化される方法を指定します。このカプセル化は、IPX LAN インターフェイスで使用されるカプセル化とは同じではありません。図 1 に、WAN インターフェイス上の IPX を示します。

図 1　WAN インターフェイス上の IPX



次に、X.25 カプセル化および非メッシュ構造のトポロジで使用されるいくつかの IPX サブインターフェイスのために、シリアル インターフェイスを設定する例を示します。

メイン ルータ用の設定

```
hostname Main
!
no ip routing
ipx routing 0000.0c17.d726
!
interface ethernet 0
 no ip address
 Novell network 100
 media-type 10BaseT
!
interface serial 0
 no ip address
 shutdown
!
interface serial 1
 no ip address
 encapsulation x25
 x25 address 33333
 x25 htc 28
!
interface serial 1.1 point-to-point
 no ip address
 novell network 2
 x25 map novell 2.0000.0c03.a4ad 11111 BROADCAST
!
interface serial 1.2 point-to-point
```

```
 no ip address
 novell network 3
 x25 map novell 3.0000.0c07.5e26 55555 BROADCAST
```

ルータ 1 用の設定

```
hostname Remote1
!
no ip routing
ipx routing 0000.0c03.a4ad
!
interface ethernet 0
 no ip address
 novell network 1
!
interface serial 0
 no ip address
 encapsulation x25
 novell network 2
 x25 address 11111
 x25 htc 28
 x25 map novell 2.0000.0c17.d726 33333 BROADCAST
```

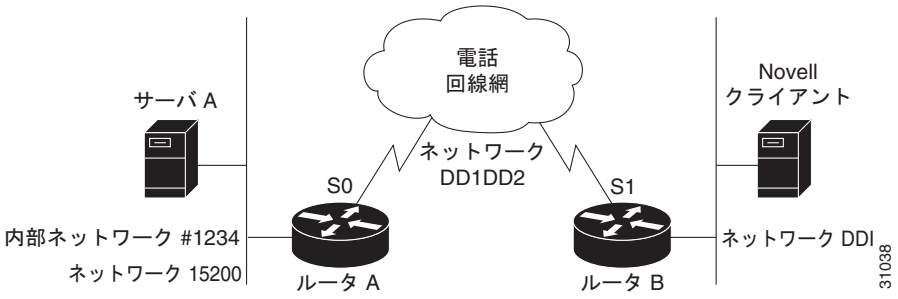
ルータ 2 用の設定

```
hostname Remote2
!
no ip routing
ipx routing 0000.0c07.5e26
!
interface ethernet 0
 no ip address
 novell network 4
 media-type 10BaseT
!
interface serial 0
 no ip address
 shutdown
!
interface serial 1
 no ip address
 encapsulation x25
 novell network 3
 x25 address 55555
 x25 htc 28
 x25 map novell 3.0000.0c17.d726 33333 BROADCAST
```

IPX over DDR の例

図 2 に示すコンフィギュレーションでは、IPX クライアントが DDR 電話回線によってサーバから切り離されています。

図 2　IPX over DDR の設定



ルーティングとサービスの情報は、60 秒ごとに送信されます。この例で定義される出力 RIP および SAP フィルタによってアップデートがフィルタリングされ、ルータ A とルータ B の間でのアップデートの送信が防止されます。このようなパケットを転送する場合は、2 台のルータのそれぞれが 60 秒ごとにもう一方に電話をかける必要があります。送信されたパケット数に基づいて料金が請求されるシリアル リンクでは、この動作は一般的に望ましくありません（この問題は専用シリアル回線では発生しません）。

サーバとクライアントの接続が確立されると、サーバは定期的にウォッチドッグ キープアライブ パケットを送信します。SPX が使用される場合、サーバとクライアントの両方がキープアライブ パケットを送信します。この目的は、サーバとクライアントの間の接続が維持されていることを確認することです。このようなパケットには、その他の情報は含まれません。サーバは約 5 分ごとにウォッチドッグ パケットを送信します。

ルータ A でサーバのキープアライブ パケットをルータ B に送信できる場合、ルータ A はこのようなパケットを送信するためだけに 5 分ごとにルータ B に電話をかける必要があります。この場合も、送信されたパケット数に基づいて料金が請求されるシリアル リンクでは、この動作は一般的に望ましくありません。ルータ A でキープアライブ パケットを送信するだけのためにルータ B に電話をかける代わりに、ルータ A でウォッチドッグ スプーフィングをイネーブルにすることができます。その結果、このルータに接続されたサーバがキープアライブ パケットを送信し、ルータ A がリモート クライアント（ルータ B に接続されたクライアント）の代わりに応答します。SPX が使用される場合、サーバとクライアントの両方がキープアライブ パケットを送信するため、ルータ A と B の両方で SPX キープアライブ パケットのスプーフィングをイネーブルにして、送信を禁止します。

ipx watchdog-spoof 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、ウォッチドッグ スプーフィングの期間をイネーブルにして設定します。スプーフィングが何時間連続してイネーブルになるかと、スプーフィングが何分間ディセーブルになるかを指定できます。このコマンドは、ファースト スイッチングとオートノマス スイッチングがディセーブルになっているシリアル インターフェイスだけで使用します。

次に、ルータ A を設定する例を示します。ウォッチドッグ スプーフィングは 1 時間イネーブルになった後、20 分ディセーブルになり、再びイネーブルになる前に、サーバで非アクティブな接続をクリーンアップできます。

```
ipx routing 0000.0c04.4878
!
interface Ethernet0
     ipx network 15200
!
interface Serial0
! PPP encap for DDR(recommended)
 encapsulation ppp
 ipx network DD1DD2
! Kill all rip updates
ipx output-network-filter 801
! Kill all sap updates
ipx output-sap-filter 1001
```

```
! fast-switching off for watchdog spoofing
no ipx route-cache
! Don't listen to rip
ipx router-filter 866
! IPX watchdog spoofing
ipx watchdog-spoof 1 20
!SPX watchdog spoofing
ipx spx-spoof
! Turn on DDR
dialer in-band
 dialer idle-timeout 200
 dialer map IP 198.92.96.132 name R13 7917
 dialer map IPX DD1DD2.0000.0c03.e3c3 7917
  dialer-group 1
ppp authentication chap
! Chap authentication required
pulse-time 1
!
access-list 801 deny  FFFFFFFF
access-list 866 deny  FFFFFFFF
!  Serialization packets
access-list 900 deny  0 FFFFFFFF 0 FFFFFFFF 457
! RIP packets
access-list 900 deny  1 FFFFFFFF 453 FFFFFFFF 453
! SAP packets
access-list 900 deny  4 FFFFFFFF 452 FFFFFFFF 452
! Permit everything else
access-list 900 permit -1 FFFFFFFF 0 FFFFFFFF 0
!
access-list 1001 deny  FFFFFFFF
!
! Static ipx route for remote network
ipx route DD1 DD1DD2.0000.0c03.e3c3
!
!
! IPX will trigger the line up (9.21 and later)
dialer-list 1 list 900
```

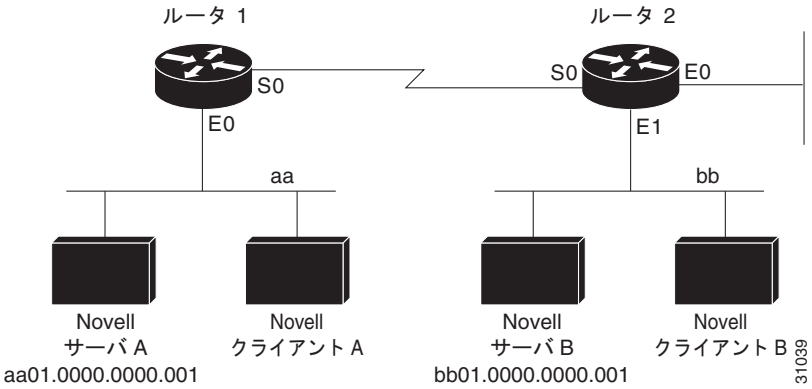
IPX ネットワーク アクセス：例

ここでは、IPX ネットワークへのアクセスを制御する例を示します。各項では、さまざまなアクセス リストとフィルタの設定を示します。

IPX ネットワーク アクセスの例

アクセス リストを使用したトラフィック ルーティングの管理は、ネットワーク制御全体における強力なツールです。ただし、ある程度の計画と、関連するいくつかのコマンドの適切な適用が必要です。図 3 に、2 つのネットワーク セグメントに 2 台のルータが存在しているネットワークを示します。

図 3　　アクセス制御の必要な Novell IPX サーバ



ネットワーク aa 上のクライアントとサーバがネットワーク bb 上のサービスを使用することは禁止しますが、ネットワーク bb 上のクライアントとサーバがネットワーク aa 上のサービスを使用することは許可するとします。この設定を実現するには、ルータ 2 上のイーサネット インターフェイス 1 で、ネットワーク aa からネットワーク bb に送信されるすべてのパケットをブロックするアクセス リストが必要です。ルータ 1 上のイーサネット インターフェイス 0 には、アクセス リストは必要ありません。

次に、ルータ 2 上でイーサネット インターフェイス 1 を設定する例を示します。

```
ipx routing
access-list 800 deny aa bb01
access-list 800 permit -1 -1
interface ethernet 1
 ipx network bb
 ipx access-group 800
```

次に、ルータ 1 のインターフェイス イーサネット 0 に入力フィルタを配置することによって、前の例と同じ結果をより効率的に実現する例を示します。また、同じ出力フィルタをルータ 1、インターフェイス シリアル 0 に配置することもできます。

```
ipx routing
access-list 800 deny aa bb01
access-list 800 permit -1 -1
interface ethernet 0
 ipx network aa
 ipx access-group 800 in
```

（注） ファースト スイッチングがオンになっているインターフェイスでアクセス コントロール リストのロギングを使用すると、アクセス リストと一致する（ロギングする必要がある）パケットは、ファースト スイッチングではなくスロー スイッチングされます。

アクセス コントロール リスト違反のロギング

次に、**access-list** コマンドの末尾にキーワード **log** を使用して、アクセス コントロール リスト違反のすべてのログを保存する例を示します。

```
access-list 907 deny -1 -1 0 100 0 log
```

前の例では、すべてのソケットからのすべてのプロトコルによるすべての送信元からルータに到着した、ネットワーク 100 のすべての宛先へのすべてのパケットが拒否され、ロギングされます。

次に、**access-list** コマンドのログ エントリの例を示します。

```
%IPX-6-ACL: 907 deny SPX B5A8 50.0000.0000.0001 B5A8 100.0000.0000.0001 10 pkts
```

この例では、10 個の SPX パケットがアクセス リスト番号 907 と一致したため、拒否されました。パケットは、ネットワーク 50.0000.0000.0001 上のソケット B5A8 からネットワーク 100.0000.0000.0001 のソケット B5A8 宛てに送信されました。

標準の名前付きアクセス リストの例

次に、fred という名前の標準アクセス リストを作成する例を示します。IPX ネットワーク番号 5678 との通信のみが拒否されます。

```
ipx access-list standard fred
 deny 5678 any
 permit any
```

拡張名前付きアクセス リストの時間範囲の例

次に、test という名前の拡張アクセス リストを作成する例を示します。月曜日から金曜日までの午前 8:00 から午後 6:00 までの SPX トラフィックが 許可されます。

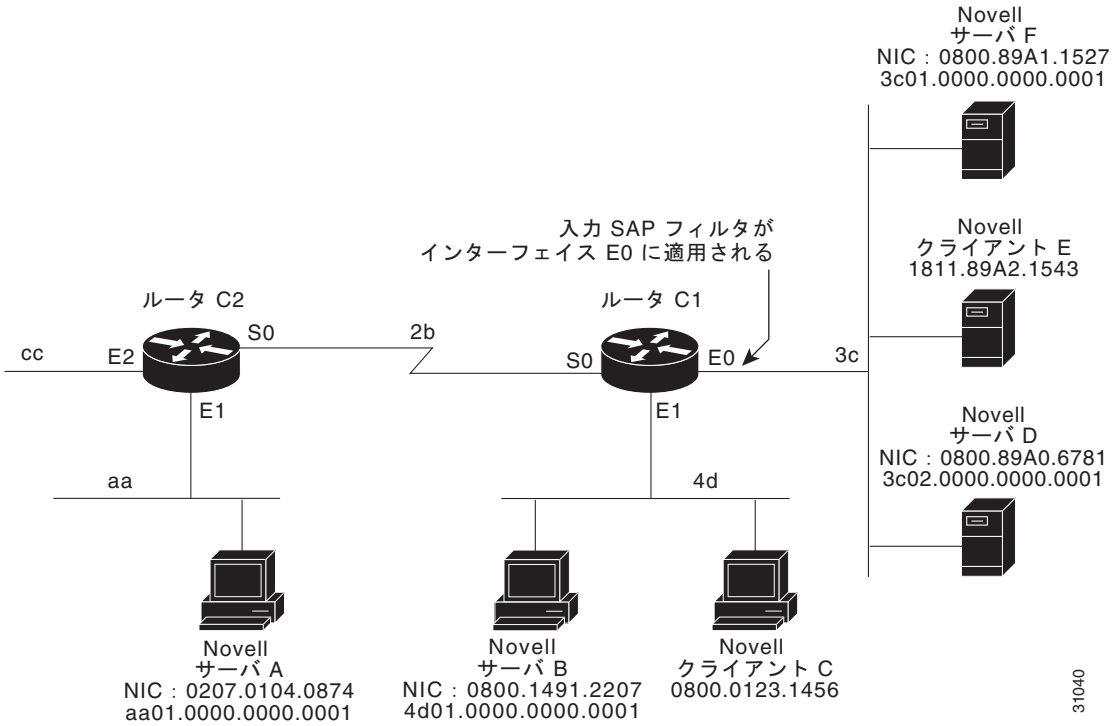
```
time-range no-spx
 periodic weekdays 8:00 to 18:00
!
ipx access-list extended test
 permit spx any all any all time-range no spx
```

SAP 入力フィルタの例

SAP 入力フィルタを使用すると、ルータでサービスについての情報を受け入れるかどうかを判断できます。

図 4 に示すルータ C1 は Novell サーバ F についての情報を受け入れず、そのためアドバタイズすることもありません。ただし、ルータ C1 はネットワーク 3c 上のその他のすべてのサーバについての情報を受け入れます。ルータ C2 はサーバ D および B についての情報を受信します。

図 4　　SAP 入力フィルタ



次に、ルータ C1 を設定する例を示します。最初の行ではサーバ F を拒否し、2 番目の行ではその他のすべてのサーバを受け入れます。

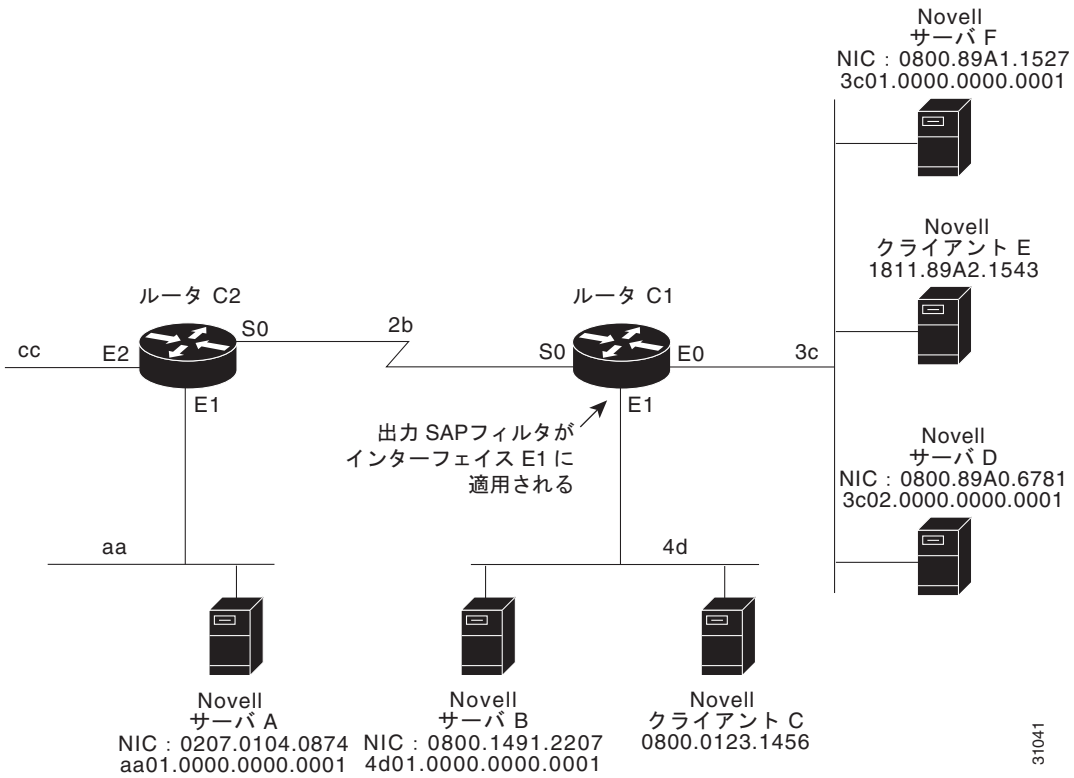
```
access-list 1000 deny 3c01.0000.0000.0001
access-list 1000 permit -1
interface ethernet 0
 ipx network 3c
 ipx input-sap-filter 1000
interface ethernet 1
 ipx network 4d
interface serial 0
 ipx network 2b
```

（注）　NetWare バージョン 3.11 以降では、内部ネットワークとノード番号をアクセス リスト コマンド（この例の最初のコンフィギュレーション コマンド）のためのアドレスとして使用します。

SAP 出力フィルタの例

SAP 出力フィルタは、Cisco IOS ソフトウェアで特定のインターフェイスに情報を送信する前に適用されます。次の例では、(図 5 に示す) ルータ C1 が Novell サーバ A についての情報をインターフェイス イーサネット 1 にアドバタイズすることを禁止しますが、ネットワーク 3c のサーバ A はアドバタイズできます。

図 5　　SAP 出力フィルタ



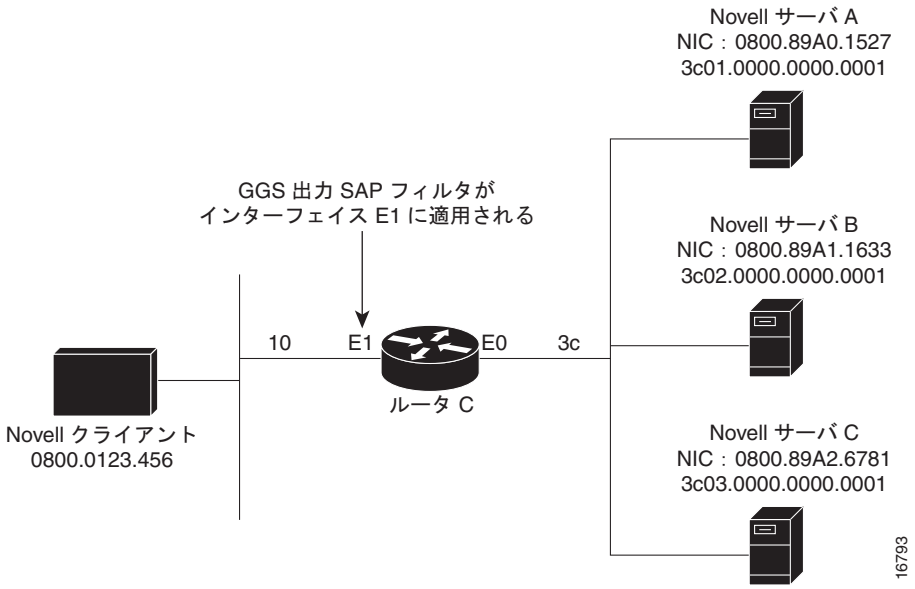
次に、ルータ C1 を設定する例を示します。最初の行ではサーバ A を拒否します。その他のすべてのサーバは許可されます。

```
access-list 1000 deny aa01.0000.0000.0001
access-list 1000 permit -1
interface ethernet 0
 novell net 3c
interface ethernet 1
 ipx network 4d
 ipx output-sap-filter 1000
interface serial 0
 ipx network 2b
```

GGS SAP 応答フィルタの例

図 6 に示す GGS SAP 応答フィルタを使用すると、ルータでサービスについて受信した情報を転送するかどうかを指定できます。

図 6　GGS SAP 応答フィルタ



次に、ルータ C 用の GGS SAP 応答フィルタを設定する例を示します。クライアントが GGS 要求を発行すると、出力 GGS フィルタは Novell サーバ A からの要求を拒否し、Novell サーバ B および C からの応答を許可します。

```
access-list 1000 deny 3c01.0000.0000.0001
access-list 1000 permit -1
interface ethernet 0
 ipx network 3c
interface ethernet 1
 ipx output-ggs-filter 1000
 ipx network 10
```

IPX NetBIOS フィルタの例

次に、NetBIOS ホスト名を使用して IPX NetBIOS フレームをフィルタリングする例を示します。この例では、イーサネット インターフェイス 0 上の NetBIOS ホスト名が Boston のすべての発信 IPX NetBIOS フレームを拒否します。

```
netbios access-list host token deny Boston
netbios access-list host token permit *
!
ipx routing 0000.0c17.d45d
!
interface ethernet 0
 ipx network 155 encapsulation ARPA
 ipx output-rip-delay 60
 ipx triggered-rip-delay 30
 ipx output-sap-delay 60
 ipx triggered-sap-delay 30
 ipx type-20-propagation
 ipx netbios output-access-filter host token
 no mop enabled
!
interface ethernet 1
 no ip address
 ipx network 105
!
```

```
interface fddi 0
 no ip address
 no keepalive
ipx network 305 encapsulation SAP
!
interface serial 0
 no ip address
 shutdown
!
interface serial 1
 no ip address
 no keepalive
 ipx network 600
 ipx output-rip-delay 100
 ipx triggered-rip-delay 60
 ipx output-sap-delay 100
 ipx triggered-sap-delay 60
 ipx type-20-propagation
```

次に、バイト パターンを使用して、IPX NetBIOS フレームをフィルタリングする例を示します。この例では、末尾が 05 の IPX ネットワーク番号からの IPX NetBIOS フレームを許可します。イーサネット インターフェイス 1（ネットワーク 105）および FDDI インターフェイス 0（ネットワーク 305）からのすべての IPX NetBIOS フレームが、シリアル インターフェイス 0 によって転送されます。ただし、このインターフェイスはイーサネット インターフェイス 0（ネットワーク 155）からのすべてのフレームを除外し、転送しません。

```
netbios access-list bytes finigan permit 2 **05
!
ipx routing 0000.0c17.d45d
!
ipx default-output-rip-delay 1000
ipx default-triggered-rip-delay 100
ipx default-output-sap-delay 1000
ipx default-triggered-sap-delay 100
!
interface ethernet 0
 ipx network 155 encapsulation ARPA
 ipx output-rip-delay 55
 ipx triggered-rip-delay 55
 ipx output-sap-delay 55
 ipx triggered-sap-delay 55
 ipx type-20-propagation
 media-type 10BaseT
!
interface ethernet 1
 no ip address
 ipx network 105
 ipx output-rip-delay 55
 ipx triggered-rip-delay 55
 ipx output-sap-delay 55
 ipx triggered-sap-delay 55
 media-type 10BaseT
!
interface fddi 0
 no ip address
 no keepalive
 ipx network 305 encapsulation SAP
 ipx output-sap-delay 55
 ipx triggered-sap-delay 55
!
interface serial 0
 no ip address
 shutdown
```

```
!
interface serial 1
 no ip address
 no keepalive
 ipx network 600
 ipx type-20-propagation
 ipx netbios input-access-filter bytes finigan
```

ブロードキャストを制御するヘルパー機能：例

ここでは、IPX ネットワークでブロードキャスト メッセージを制御する例を示します。

- アドレスへの転送の例（P.121）
- すべてのネットワークへの転送の例（P.123）
- all-nets flooded ブロードキャストの例（P.124）

次の例では、パケット タイプ 2 が使用されることに注意してください。このタイプは任意に選択され、使用する実際のタイプはアプリケーションによって異なります。

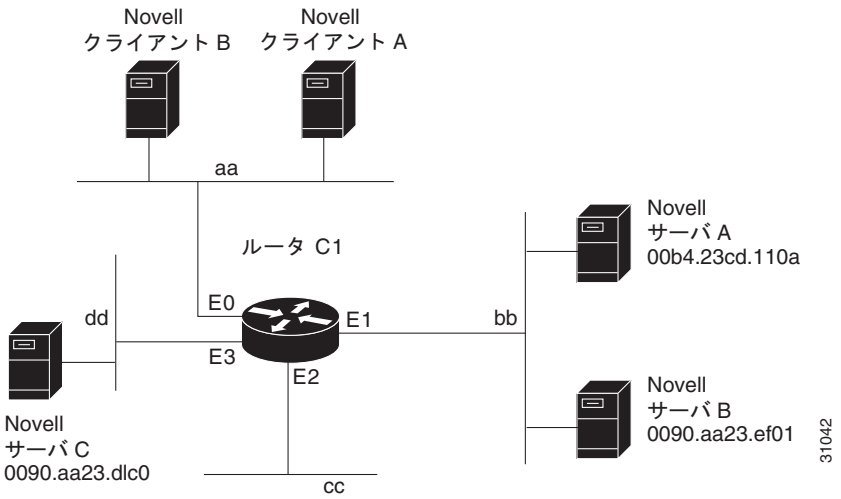
アドレスへの転送の例

通常、すべてのブロードキャスト パケットが Cisco IOS ソフトウェアによってブロックされます。ただし、タイプ 20 伝播パケットは転送でき、一部のループ防止チェックの対象となります。その他のブロードキャストは、セグメント上の一連のネットワークまたは特定のホスト（ノード）に渡される可能性があります。次の例に、これらのオプションを示します。

図 7 に、いくつかのイーサネット インターフェイスに接続されたルータ（C1）を示します。この環境では、すべての IPX クライアントがセグメント aa に接続され、すべてのサーバがセグメント bb および dd に接続されます。ブロードキャストの制御では、次の条件が適用されます。

- タイプ 2 およびタイプ 20 のブロードキャストのみが転送されます。
- ネットワーク aa 上の IPX クライアントは、タイプ 2 を介してネットワーク bb および dd の任意のサーバにブロードキャストできます。
- IPX クライアントは、タイプ 20 を介して、ネットワーク dd の任意のサーバにブロードキャストできます。

図 7　ルータを通過するサーバ アクセスが必要な IPX クライアント



次に、図 7 に示すルータを設定する例を示します。最初の行では、ネットワーク aa からタイプ 2 のブロードキャスト トラフィックを許可します。インターフェイス コマンドとネットワーク コマンドで、特定の各インターフェイスを設定します。**ipx helper-address** インターフェイス コンフィギュレーション コマンドでは、ネットワーク aa から bb へ、ネットワーク aa から dd へのブロードキャスト転送を許可します。ヘルパー リストでは、タイプ 2 のブロードキャストを転送できます（タイプ 2 のブロードキャストは例として選択されているだけであることに注意してください。使用する実際のタイプは、アプリケーションによって異なります）。**ipx type-20-伝播** インターフェイス コンフィギュレーション コマンドは、タイプ 20 のブロードキャストを可能にするためにも必要です。IPX helper-list フィルタは、helper-address メカニズムによって転送されるタイプ 2 のパケットと、タイプ 20 の伝播によって転送されるタイプ 20 パケットの両方に適用されます。

```
access-list 900 permit 2 aa
interface ethernet 0
 ipx network aa
 ipx type-20-propagation
 ipx helper-address bb.ffff.ffff.ffff
 ipx helper-address dd.ffff.ffff.ffff
 ipx helper-list 900
interface ethernet 1
 ipx network bb
interface ethernet 3
 ipx network dd
 ipx type-20-propagation
```

このコンフィギュレーションは図 7 に示す例と同様に、ネットワーク aa および aa1 に属しているルータが、一連の設定エントリでこれらのブロードキャストを転送するように設定されていない場合、ネットワーク aa からのダウンストリームである任意のネットワーク（たとえば、任意のネットワーク aa1）でルータ C1 を介してネットワーク bb にブロードキャスト（タイプ 2）できません。これらのエントリは入力インターフェイスに適用し、接続されたネットワーク間で直接ブロードキャストを転送するように設定する必要があります。この方法では、このようなトラフィックをネットワークからネットワークへ直接渡すことができます。タイプ 20 パケットも同様です。

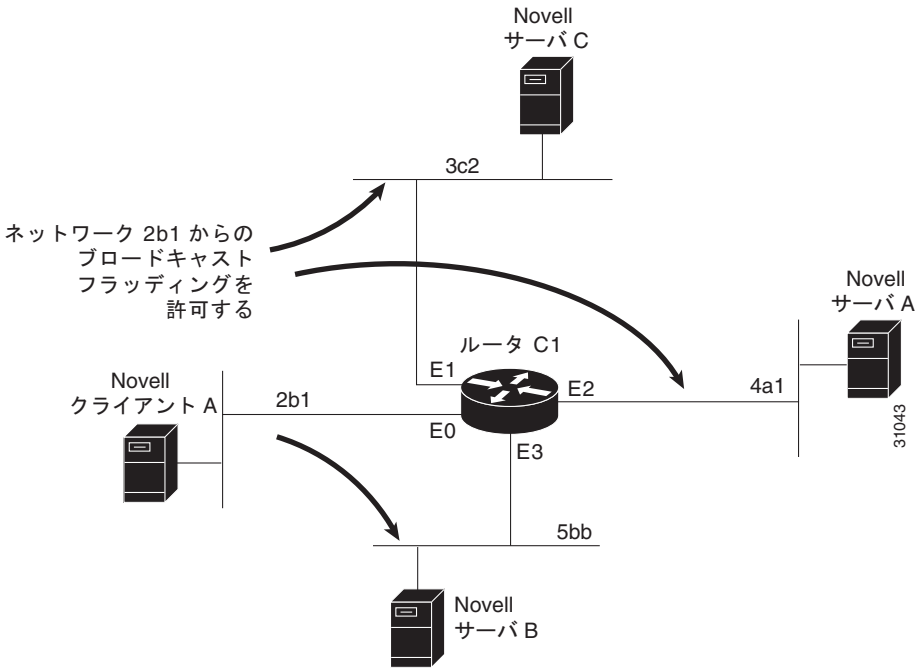
次に、サーバ A へのブロードキャストを指定するように、**ipx helper-address** インターフェイス コンフィギュレーション コマンド ラインを書き直す例を示します。

```
ipx helper-address bb.00b4.23cd.110a
! Permits node-specific broadcast forwarding to
! Server A at address 00b4.23cd.110a on network bb.
```

すべてのネットワークへの転送の例

一部のネットワークでは、クライアント ノードを複数のネットワーク上のサーバにブロードキャストできるようにする必要があります。接続されたすべてのネットワークにブロードキャストを転送するようにルータを設定する場合、インターフェイスがフラッディングされます。図 8 に示す環境では、ネットワーク 2b1 上のクライアント ノードがルータ C1 を通じて、ネットワーク 3c2、4a1、および 5bb 上の IPX サーバからサービスを取得する必要があります。この要件をサポートするには、**ipx helper-address** インターフェイス コンフィギュレーション コマンド仕様でフラッディング アドレス（-1.ffff.ffff.ffff）を使用します。

図 8　　タイプ 2 のブロードキャスト フラッディング



次の例の最初の行に、ネットワーク 2b1 からタイプ 2 のトラフィックを許可する例を示します。次に、最初のインターフェイスをネットワーク番号で設定します。all-nets ヘルパー アドレスが定義され、ヘルパー リストでタイプ 2 トラフィックへの転送が制限されます。ネットワーク 2b1 からのタイプ 2 のブロードキャストは、直接接続されたすべてのネットワークに転送されます。タイプ 20 を含めて、その他のすべてのブロードキャストがブロックされます。ブロードキャストを許可するには、**ipx helper-list** エントリを削除します。タイプ 20 ブロードキャストを許可するには、すべてのインターフェイスで **ipx type-20-propagation** インターフェイス コンフィギュレーション コマンドをイネーブルにします。

```
access-list 901 permit 2 2b1
interface ethernet 0
 ipx network 2b1
 ipx helper-address -1.ffff.ffff.ffff
 ipx helper-list 901
interface ethernet 1
 ipx network 3c2
interface ethernet 2
 ipx network 4a1
interface ethernet 3
 ipx network 5bb
```

all-nets flooded ブロードキャストの例

次に、インターフェイスで all-nets flooding を設定する例を示します。この設定の結果として、イーサネット インターフェイス 0 ですべてのブロードキャスト メッセージ（タイプ 20 を除く）が、到達方法がわかっているすべてのネットワークに転送されます。このブロードキャスト メッセージのフラッディングによって、これらのネットワークが多数のブロードキャスト トラフィックによって過負荷になり、他のトラフィックが通過できなくなる可能性があります。

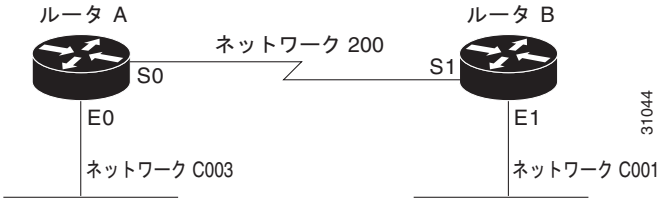
```
interface ethernet 0
 ipx network 23
 ipx helper-address -1.FFFF.FFFF.FFFF
```

IPX アカウンティング：例

次に、シリアル リンクによって接続される 2 つのイーサネット ネットワーク セグメントの例を示します（図 9 を参照）。ルータ A では、IPX アカウンティングが入力インターフェイスと出力インターフェイス（イーサネット インターフェイス 0 とシリアル インターフェイス 0）の両方でイネーブルになっています。そのため、両方向（イーサネット ネットワークへと、シリアル リンクへ）のトラフィックの統計情報が収集されます。

ルータ B では、IPX アカウンティングがシリアル インターフェイスのみでイネーブルになり、イーサネット インターフェイスではイネーブルになっていません。そのため、シリアル リンク上のルータに向かうトラフィックの統計情報だけが収集されます。また、アカウンティングのしきい値は 1000 に設定されるため、IPX アカウンティングがルータを通過するすべての IPX トラフィック（最大 1000 の発信元と宛先の組み合わせ）を追跡します。

図 9　　IPX アカウンティングの例



ルータ A の設定

```
ipx routing
interface ethernet 0
 no ip address
 ipx network C003
 ipx accounting
interface serial 0
 no ip address
 ipx network 200
 ipx accounting
```

ルータ B の設定

```
ipx routing
interface ethernet 1
 no ip address
 no keepalive
 ipx network C001
 no mop enabled
interface serial 1
 no ip address
```

```
ipx network 200
ipx accounting
ipx accounting-threshold 1000
```

その他の関連資料

ここでは、Novell IPX 機能に関する参考資料について説明します。

関連マニュアル

内容	参照先
AppleTalk コマンド リファレンス	『*Cisco IOS AppleTalk Command Reference*』
コンフィギュレーションの基礎の設定ガイド	『*Cisco IOS Configuration Fundamentals Configuration Guide*』
トランスペアレント ブリッジングの設定	『*Cisco IOS Bridging and IBM Networking Configuration Guide*』
DDR 設定の決定と準備	『*Cisco IOS Dial Technologies Configuration Guide*』
Novell IPX コマンド	『*Cisco IOS Novell IPX Command Reference*』
マルチレイヤ スイッチング	『*Cisco IOS Switching Services Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Novell IPX を設定するための機能情報

表 3 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア 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 を使用すると、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 Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 3 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 3　Novell IPX を設定するための機能情報

機能名	リリース	機能情報
Novell IPX の設定	Cisco IOS XE Release 2.1	Novell Internetwork Packet Exchange（IPX）は、Xerox Network Services（XNS）Internet Datagram Protocol（IDP; インターネット データグラム プロトコル）から派生したものです。シスコによる Novell IPX プロトコルの実装では、完全な IPX ルーティング機能を提供することが保証されます。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに実装されました。 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。 • IPX ルーティングの設定（P.5） • IPX Enhanced IGRP の設定（P.12） • WAN での IPX および SPX の設定（P.31） • IPX ネットワークへのアクセスの制御（P.35） • IPX ネットワーク パフォーマンスの調整（P.54） • IPX ネットワークのシャットダウン（P.95） • IPX アカウンティングの設定（P.98） • LAN 間の IPX の設定（P.100） • VLAN 間の IPX の設定（P.101） • IPX マルチレイヤ スイッチングの設定（P.101） • IPX ネットワークのモニタリングおよびメンテナンス（P.101）