ISO CLNS の設定

International Organization for Standardization（ISO; 国際標準化機構）の Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）プロトコルは、Open System Interconnection（OSI; オープン システム インターコネクション）モデルのネットワーク層に関する標準です。このプロトコルを設定する前に、アドレスとルーティング プロセスについて理解しておく必要があります。このモジュールでは、アドレス、ルーティング プロセス、および ISO CLNS の設定手順について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「ISO CLNS 設定の機能情報」（P.71）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp 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。

目次

- 「ISO CLNS の設定に関する前提条件」（P.2）
- 「ISO CLNS の設定に関する制約事項」（P.2）
- 「ISO CLNS の設定に関する情報」（P.2）
- 「ISO CLNS の設定方法」（P.9）
- 「ISO CLNS の設定例」（P.52）
- 「その他の関連資料」（P.70）
- 「ISO CLNS 設定の機能情報」（P.71）

ISO CLNS の設定に関する前提条件

ISO CLNS を設定するには、エンド システムのアドレスを指定する Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）とネットワーク装置を識別するタイトルが必要です。

ISO CLNS の設定に関する制約事項

ISO CLNS では、ネットワーク経由で送信されるパケットごとにパスが個別に決定されるため、接続の設定または終了は実行されません。

ISO CLNS の設定に関する情報

ISO CLNS を設定するには、次の概念を理解しておく必要があります。

- 「概要」（P.2）
- 「アドレスの概要」（P.3）

概要

Cisco IOS ソフトウェアでは、イーサネット、トークン リング、FDDI、シリアルなどのさまざまなデータリンク層を使用してネットワーク上の ISO CLNS のパケット転送およびルーティングがサポートされます。

CLNS ルーティングは、シリアル インターフェイスで HDLC、PPP、Link Access Procedure, Balanced（LAPB; 平衡型リンク アクセス手順）、X.25、SMDS、またはフレーム リレーのカプセル化を行って使用することができます。HDLC カプセル化を使用するには、リンクの両端にルータが存在する必要があります。X.25 カプセル化を使用する場合は、Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）と X.121 のマッピングを手動で入力する必要があります。LAPB、X.25、フレーム リレー、および SMDS のカプセル化は、他のベンダーと相互運用します。

また、Cisco CLNS の実装は、Government OSI Profile (GOSIP) Version 2 に準拠しています。

CLNS のサポートの一環として、Cisco ルータでは、次の ISO 規格と American National Standards Institute（ANSI; 米国規格協会）規格が完全にサポートされています。

- ISO 9542：ES-IS ルーティング交換プロトコルについて文書化しています。
- ISO 8473：ISO Connectionless Network Protocol（CLNP; コネクションレス型ネットワーク プロトコル）について文書化しています。
- ISO 8348/Ad2：NSAP アドレスについて文書化しています。
- ISO 10589：IS-IS ドメイン内ルーティング交換プロトコルについて文書化しています。

ISO が策定した IS-IS ルーティング プロトコルと Cisco ISO Interior Gateway Routing Protocol（IGRP）の両方が ISO CLNS のダイナミック ルーティングに対してサポートされています。さらに、ISO CLNS のスタティック ルーティングがサポートされています。

（注） Cisco アクセス サーバでは、現在、ES-IS ルーティング プロトコルはサポートされていますが、IS-IS ルーティング プロトコルはサポートされていません。

アドレスの概要

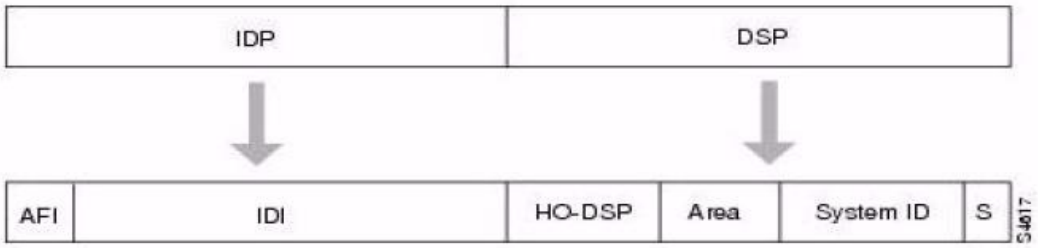
ISO ネットワーク アーキテクチャでは、アドレスは Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスおよび Network Entity Title（NET）と呼ばれます。OSI ネットワーク内の各ノードには 1 つ以上の NET が設定されます。さらに、多数の NSAP アドレスが設定されます。各 NSAP アドレスは、そのノードのいずれかの NET とは最終バイトだけが異なります。このバイトは *N セレクタ*と呼ばれます。その機能は、他のプロトコル スイートのポート番号に似ています。

シスコの実装では、ISO 8348/Ad2 で定義されているすべての NSAP アドレス形式がサポートされます。ただし、IS-IS に関する ISO 規格（ISO 10589）で定義されているアドレス制約に準拠する NSAP アドレスに対してのみ ISO Interior Gateway Routing Protocol（IGRP）または Intermediate System-to-Intermediate System（IS-IS）ダイナミック ルーティングを利用できます。

NSAP アドレスは、図 1 に示すように、次の 2 つの主要フィールドで構成されます。

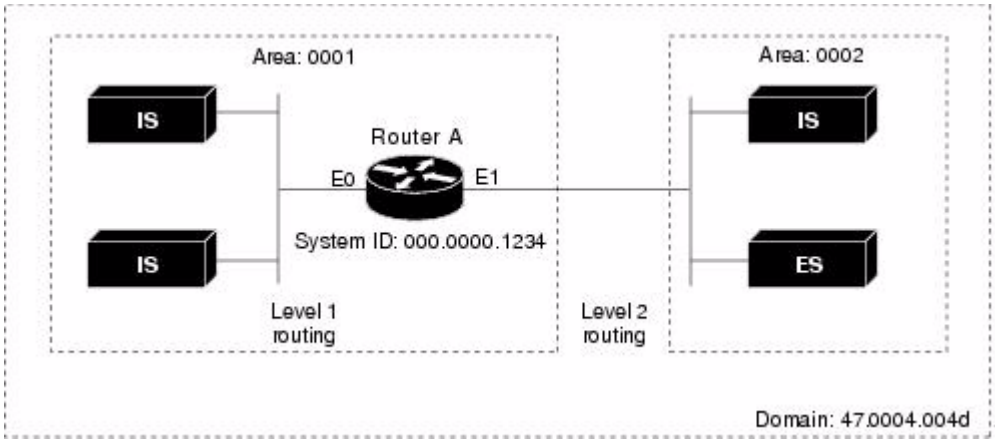
- Initial Domain Part（IDP）: 1 バイトの Authority and Format Identifier（AFI）と可変長の Initial Domain Identifier（IDI）で構成されます。IDI の長さと Domain Specific Part（DSP; ドメイン特定部分）の符号化形式は、AFI の値に基づきます。
- DSP：High Order DSP（HO-DSP）、エリア ID、システム ID、および 1 バイトの N セレクタ（S と示されています）で構成されます。

図 1　　NSAP アドレスのフィールド



ドメインおよびエリアのアドレスまたは NET を割り当てます。ドメイン アドレスは、ルーティング ドメインを一意に識別します。特定のドメイン内のすべてのルータに同じドメイン アドレスが付与されます。図 2 に示すように、各ルーティング ドメイン内で 1 つ以上のエリアを設定できます。どのルータをどのエリアに割り当てるかを決定します。エリア アドレスはルーティング エリアを一意に識別し、システム ID は各ノードを識別します。

図 2　　ドメイン アドレスとエリア アドレスの例



ISO IGRP と IS-IS NSAP のアドレッシング方式の主な違いは、エリア アドレスの定義です。どちらもレベル 1 ルーティング（エリア内ルーティング）にはシステム ID を使用しますが、エリア ルーティングにおけるアドレス指定方法はそれぞれ異なります。ISO IGRP NSAP アドレスには、*ドメイン*、*エリア*、および*システム ID* の 3 つの異なるルーティング用フィールドが含まれます。IS-IS アドレスには、単一の連続した*エリア*フィールド（ドメイン フィールドとエリア フィールドで構成）、および*システム ID* の 2 つのフィールドが含まれます。

ここでは、アドレスに関する次のトピックについても説明します。

- 「ISO IGRP NSAP アドレス」（P.4）
- 「IS-IS NSAP アドレス」（P.5）
- 「アドレッシング規則」（P.5）
- 「アドレッシングの例」（P.6）
- 「ルーティング テーブルの例」（P.6）

ISO IGRP NSAP アドレス

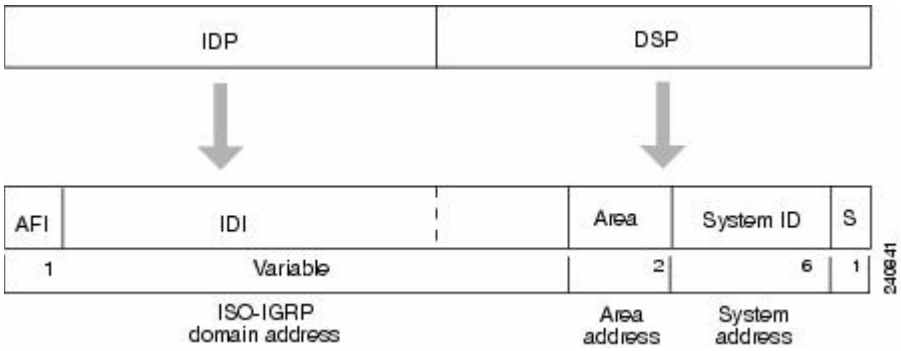
ISO IGRP NSAP アドレスは、ドメイン部分、エリア アドレス、およびシステム ID の 3 つの部分に分割されます。ドメイン ルーティングがアドレスのドメイン部分に対して実行されます。特定のドメインのエリア ルーティングでエリア アドレスが使用されます。特定のエリアのシステム ルーティングでシステム ID 部分が使用されます。NSAP アドレスの内容は次のとおりです。

- ドメイン部分は可変長で、エリア アドレスの前にあります。
- エリア アドレスは 2 バイトで、システム ID の前にあります。
- システム ID は 6 バイトで、N セレクタの前にあります。
- N セレクタ（S）は NSAP アドレスの最終バイトです。

Cisco ISO IGRP ルーティングの実装では、AFI から DSP のエリア フィールドまで（ただし、このフィールドは含まれない）のバイトが *ドメイン ID* として解釈されます。エリア フィールドではエリアが指定され、システム ID ではシステムが指定されます。

図 3 に、ISO IGRP NSAP アドレッシング構造を示します。アドレスの最大サイズは 20 バイトです。

図 3　ISO IGRP NSAP アドレッシング構造



IS-IS NSAP アドレス

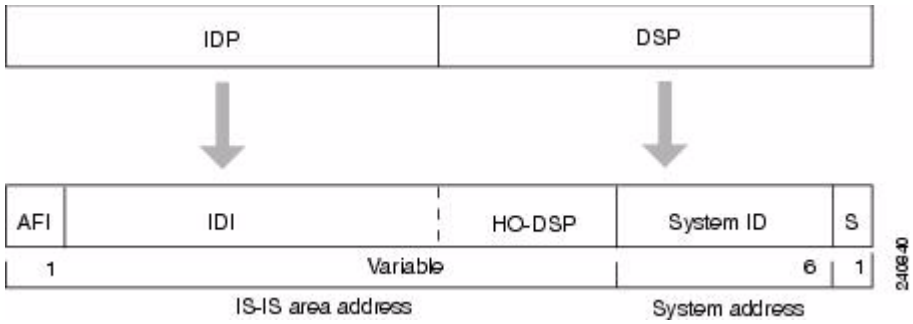
IS-IS NSAP アドレスは、エリア アドレスおよびシステム ID の 2 つの部分に分割されます。レベル 2 ルーティング（エリア間ルーティング）でエリア アドレスが使用されます。レベル 1 ルーティング（エリア内ルーティング）でシステム ID アドレスが使用されます。NSAP アドレスの定義は次のとおりです。

- エリア アドレスは、システム ID と N セレクタを含まない NSAP アドレスです。
- システム ID は、エリア アドレスと N セレクタ バイトの間にあります。
- N セレクタ（S）は NSAP アドレスの最終バイトです。

IS-IS ルーティング プロトコルでは、AFI から DSP のシステム ID フィールドまで（ただし、このフィールドは含まれない）のバイトが*エリア ID* として解釈されます。システム ID では*システム*が指定されます。

図 4 に、IS-IS NSAP アドレッシング構造を示します。アドレスの最大サイズは 20 バイトです。

図 4　IS-IS NSAP アドレッシング構造



アドレッシング規則

NSAP アドレスはすべて、次の制約に従う必要があります。

- システムの NET は、通常、N セレクタ バイトがゼロに設定された NSAP アドレスとして記述されます。

- 2 つのノードに、NET が同じアドレス（DSP の N セレクタ（S）フィールド以外がすべて一致するアドレス）を設定することはできません。
- 同じエリア内に存在する 2 つのノードに、システム ID フィールドが同じアドレスを設定することはできません。
- ISO IGRP では、10 バイト（ドメインの 1 バイト、エリアの 2 バイト、システム ID の 6 バイト、および N セレクタの 1 バイト）以上の長さが必要です。
- ISO IGRP と IS-IS を同じエリアに対して設定することはできません。ISO IGRP と IS-IS の両方のルーティングをイネーブルにする場合は、システム ID まで（ただし、このフィールドは含まれない）のすべてのバイトが同じ NSAP アドレスは指定*しないでください*。
- ルータには 1 つ以上のエリア アドレスを設定できます。複数のエリア アドレスの概念については、このマニュアルの「IS-IS エリアへの複数のエリア アドレスの割り当て」の項で説明されています。
- シスコによる IS-IS の実装では、8 バイト（エリアの 1 バイト、システム ID の 6 バイト、および N セレクタの 1 バイト）以上の長さが必要です。

アドレッシングの例

次に、ISO IGRP 実装を使用して OSI ネットワークと Government OSI Profile（GOSIP）の NSAP アドレスを設定する例を示します。

次に、OSI ネットワークの NSAP アドレス形式の例を示します。

```
|     Domain|Area|     System ID| S|
47.0004.004D.0003.0000.0C00.62E6.00
```

次に、GOSIP の NSAP アドレス構造の例を示します。この構造は、International Code Designator（ICD）0005 アドレッシング ドメインから割り当てられるアドレスの場合に必要です。詳細については、GOSIP ドキュメント『*U.S. Government Open Systems Interconnection Profile (GOSIP)*』（ドラフト バージョン 2.0、1989 年 4 月）を参照してください。

```
|                    Domain|Area|     System ID| S|
47.0005.80.ffff00.0000.ffff.0004.0000.0c00.62e6.00
 |   |    |    |    |    |
AFI IDI  DFI  AAI  Resv  RD
```

ルーティング テーブルの例

（**clns route** コマンドを使用して）NSAP プレフィクスとネクスト ホップ NET のペアを指定することでスタティック ルートを入力します。NSAP プレフィクスは、NSAP アドレスのどの部分でもかまいません。NET は、NSAP アドレスと機能が似ています。

着信パケットの宛先 NSAP アドレスがルーティング テーブルの既存の NSAP アドレスと一致しない場合、Cisco IOS ソフトウェアでは、パケットをルーティングするために NSAP アドレスと NSAP プレフィクスの照合が試行されます。ルーティング テーブルにおける最適な一致とは、宛先 NSAP アドレスの先頭と一致する最長の NSAP プレフィクス エントリを意味します。

表 1 に、スタティック ルーティング テーブルの例を示します。ここでは、全体を示すためにネクスト ホップ NET が示されていますが、ルーティング アルゴリズムを理解するために必要なわけではありません。表 2 は、一致する最長の NSAP プレフィクスを表 1 のルーティング テーブル エントリと照合する例を示しています。

表 1　ルーティング テーブル エントリの例

Entry	NSAP アドレス プレフィクス	ネクスト ホップ NET
1	47.0005.000c.0001	47.0005.000c.0001.0000.1234.00
2	47.0004	47.0005.000c.0002.0000.0231.00
3	47.0005.0003	47.0005.000c.0001.0000.1234.00
4	47.0005.000c	47.0005.000c.0004.0000.0011.00
5	47.0005	47.0005.000c.0002.0000.0231.00

表 2　階層型ルーティングの例

データグラムの宛先 NSAP アドレス	使用されるテーブル エントリの番号
47.0005.000c.0001.0000.3456.01	1
47.0005.000c.0001.6789.2345.01	1
47.0004.1234.1234.1234.1234.01	2
47.0005.0003.4321.4321.4321.01	3
47.0005.000c.0004.5678.5678.01	4
47.0005.0001.0005.3456.3456.01	5

NSAP アドレスと NET の内部境界にはオクテット境界を使用する必要があります。

ISO CLNS ルーティング プロセスの概要

ルータの基本機能はパケットの転送です。インターフェイスでパケットを受信し、別の（または同じ）インターフェイスから適切な宛先に送信します。すべてのルータがテーブルで宛先アドレスを検索してパケットを転送します。テーブルはダイナミックまたはスタティックに構築できます。テーブルのすべてのエントリを自分で設定する場合は、*スタティック ルーティング*を使用することになります。ルーティング プロセスを使用してテーブルを構築する場合は、*ダイナミック ルーティング*を使用することになります。スタティック ルーティングとダイナミック ルーティングの両方を同時に使用することもでき、場合によってはこれが必要になります。

ISO CLNS だけを設定し、ルーティング プロトコルを設定しない場合、Cisco IOS ソフトウェアでは転送判断だけが実行されます。その他のルーティング関連の機能は実行されません。このような設定では、ソフトウェアによって隣接データのテーブルがコンパイルされますが、この情報はアドバタイズされません。ルーティング テーブルに挿入される情報は、このルータの NSAP および NET アドレス、スタティック ルート、および隣接情報だけです。

あるインターフェイスで ISO CLNS のルーティングを行い、同時にその ISO CLNS を別のインターフェイスに透過的にブリッジングすることができます。このタイプのルーティングをイネーブルにするには、**bridge crb** コマンドを使用して、Concurrent Routing and Bridging をイネーブルにする必要があります。ブリッジングの詳細については、『*Cisco IOS Bridging and IBM Networking Configuration Guide*』の「Configuring Transparent Bridging」の章を参照してください。

ISO CLNS ルーティング プロセスについて理解するには、次の項目を理解しておく必要があります。

- 「ダイナミック ルーティング」（P.8）
- 「中継システムとエンド システム」（P.8）
- 「スタティック ルーティング」（P.8）

- 「ルーティング決定」（P.9）
- 「IPv4 および IPv6 パケットの GRE/CLNS トンネル サポート」（P.9）

ダイナミック ルーティング

シスコは、次の 2 つの ISO CLNS ネットワークのダイナミック ルーティング プロトコルをサポートします。

- ISO IGRP
- IS-IS

ダイナミック ルーティングを行う場合、ISO IGRP または IS-IS のいずれかを選択することも、両方のルーティング プロトコルを同時にイネーブルにすることもできます。どちらのルーティング プロトコルも、*エリア*という概念をサポートしています。エリア内では、すべてのルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータは適切なエリアに到達する方法を認識しています。

ISO IGRP は、*システム ルーティング*、*エリア ルーティング*、*ドメイン間ルーティング*の 3 つのルーティング レベルをサポートします。ドメインをまたがるルーティング（ドメイン間ルーティング）は、ISO IGRP を使用してスタティックまたはダイナミックに行うことができます。IS-IS は、*ステーション ルーティング*（エリア内）、*エリア ルーティング*（エリア間）の 2 つのルーティング レベルをサポートします。

中継システムとエンド システム

一部の Intermediate System（IS; 中継システム）は、エリア内のすべての End System（ES; エンド システム）と通信する方法を追跡しているため、レベル 1 ルータ（*ローカル ルータ*とも呼ばれる）として機能します。その他の IS は、ドメイン内の他のエリアと通信する方法を追跡しているため、レベル 2 ルータ（*エリア ルータ*とも呼ばれる）として機能します。Cisco ルータは、ISO IGRP ルーティングの場合は常にレベル 1 およびレベル 2 ルータになりますが、IS-IS ルーティングの場合は、レベル 1 のみ、レベル 2 のみ、またはレベル 1 とレベル 2 の両方のルータになるように設定することができます。

ES は、ES-IS プロトコルを使用して IS と通信します。レベル 1 とレベル 2 の IS は、ISO IS-IS または Cisco ISO IGRP プロトコルを使用して相互に通信します。

スタティック ルーティング

スタティック ルーティングは、ダイナミック ルーティングの使用が不可能であるか望ましくない場合に使用します。たとえば、次のような場合にスタティック ルーティングを使用します。

- ネットワークに接続時間やパケット単位での課金が発生する WAN リンクが含まれる場合は、そのリンク上のルーティング プロトコルの実行や、そのすべてのルーティング アップデート パケットに対して支払うのではなく、スタティック ルーティングを使用します。
- ドメイン間ルーティング プロトコルを実行していない場合にルータで外部ネットワークへの接続がアドバタイズされるようにするには、スタティック ルーティングを使用する*必要があります*。
- シスコがサポートするダイナミック ルーティング プロトコルをサポートしていない別のベンダーの機器との相互運用が必要な場合は、スタティック ルーティングを使用する必要があります。
- X.25、フレーム リレー、または SMDS ネットワークで運用する場合は、一般的にスタティック ルーティングが望ましいと言えます。

（注） スタティック ルーティングに設定されているインターフェイスでは、障害の発生したリンクを*避けて*再ルーティングすることはできません。

ルーティング決定

定義済み NSAP アドレスまたは NET のいずれかに送信される Connectionless Network Protocol（CLNP; コネクションレス型ネットワーク プロトコル）パケットは、ルータによって受信されます。Cisco IOS ソフトウェアは、次のアルゴリズムを使用してパケットの送信時に使用する NET を選択します。

- ダイナミック ルーティング プロトコルを実行していない場合、発信インターフェイスに定義されている NET があるときはそれを使用し、ないときはルータに定義されている NET を使用します。
- ISO IGRP を実行している場合、インターフェイスで実行されている ISO IGRP ルーティング プロセスの NET を使用します。
- IS-IS を実行している場合、インターフェイスで実行されている IS-IS ルーティング プロセスの NET を使用します。

IPv4 および IPv6 パケットの GRE/CLNS トンネル サポート

CLNS ネットワークを介した IPv4 および IPv6 パケットの GRE トンネリングにより、Cisco CLNS トンネル（CTunnel）と他のベンダーのネットワーキング機器との相互運用が可能になります。この機能は RFC 3147 に準拠しています。

チェックサム、キー、シーケンスなど、ヘッダー フィールドで定義される任意の GRE サービスはサポートされていません。受信したパケットやそのようなサービスの要求は、ドロップされます。

ISO CLNS の設定方法

ISO CLNS を設定するには、ルーティング プロセスを設定し、アドレスをそのルーティング プロセスに関連付け、特定のネットワーク用にルーティング プロセスをカスタマイズする必要があります。

ISO CLNS プロトコルを設定するには、次に示す作業を組み合わせて実行する必要があります。

- 「ISO IGRP ダイナミック ルーティングの設定」（任意）
- 「IS-IS ダイナミック ルーティングの設定」（任意）
- 「CLNS スタティック ルーティングの設定」（任意）
- 「その他の機能の設定」（任意）
- 「CLNS over WANs の設定」（任意）
- 「ISO CLNS のパフォーマンスの向上」（任意）
- 「ISO CLNS ネットワークのモニタおよびメンテナンス」（任意）
- 「ISO CLNS での TARP の設定」（任意）

設定例については、この章の最後にある「ISO CLNS の設定例」の項を参照してください。

ISO IGRP ダイナミック ルーティングの設定

ISO IGRP は、さまざまな帯域幅と遅延の特性を持つ大規模で任意に複雑なネットワークが含まれる自律システムのルーティング用に設計された、シスコ独自のダイナミック ディスタンスベクトル ルーティング プロトコルです。

ISO IGRP を設定するには、次に示す作業を実行します。「ISO IGRP パラメータの設定」の項の作業は任意ですが、使用している特定のアプリケーションによっては実行が必要になる場合があります。

- 「ISO IGRP のイネーブル化」（必須）
- 「ISO IGRP パラメータの設定」（任意）

また、次に示すその他の機能を設定できます。これらの機能については、この章で後述します。

- ルーティング情報のフィルタリング：「パケット転送フィルタの作成と隣接の確立」の項を参照。
- ルーティング プロセス間でのルーティング情報の再配布：「ルーティング情報の再配布」の項を参照。
- アドミニストレーティブ ディスタンスの設定：「優先ルートの指定」の項を参照。

ISO IGRP のイネーブル化

ISO IGRP ダイナミック ルーティングを設定するには、ISO IGRP ルーティング プロセスをイネーブルにし、ルータのアドレスを識別し、ISO IGRP をルーティングするインターフェイスを指定する必要があります。必要に応じて、インターフェイスの設定時にルーティング アップデートのレベルを設定することもできます。ISO IGRP を設定するときに、ルータの CLNS ルーティングはデフォルトでイネーブルになります。最大 10 個の ISO IGRP ルーティング プロセスを指定できます。

ルータで ISO IGRP ダイナミック ルーティングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# router iso-igrp [tag]`	ISO IGRP ルーティング プロセスをイネーブルにして、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 2	`Router(config-router)# net network-entity-title`	ルーティング プロセスの NET またはアドレスを設定します。

IS-IS では複数の NET を設定できますが、ISO IGRP で設定できるのはルーティング プロセスにつき 1 つの NET だけです。

tag オプションを使用して、ルーティング プロセスにわかりやすい名前を割り当てることができます。アドレスに加えて NET の名前を指定することもできます。名前を割り当てる方法については、この章の「ショートカット NSAP アドレスの指定」の項を参照してください。

レベル 2 の情報のみをアドバタイズするようにインターフェイスを設定できます。このオプションを使用すると、特定のインターフェイスでレベル 2 のルーティング アップデートだけを送信するよう Cisco IOS ソフトウェアに指定することで、ルータ間のトラフィック量が少なくなります。レベル 2 オプションが設定されているインターフェイスに、レベル 1 の情報は渡されません。

インターフェイスで ISO IGRP ダイナミック ルーティングを設定するには、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。

コマンド	目的
`Router(config-if)# clns router iso-igrp tag [level 2]`	指定したインターフェイスで ISO IGRP をイネーブルにします。また、ルーティング アップデートのレベル タイプを設定します。

ダイナミック ルーティングの設定例については、この章の最後にある「重複するエリアでのダイナミック ルーティング の例」、「ダイナミック ドメイン間ルーティングの例」、および「ISO CLNS over X.25 の例」の項を参照してください。

ISO IGRP パラメータの設定

シスコの ISO IGRP 実装では、特定の ISO IGRP パラメータをカスタマイズすることができます。次に示す任意の作業を実行できます。

- 「ISO IGRP メトリックの調整」（任意）
- 「ISO IGRP タイマーの調整」（任意）
- 「スプリット ホライズンのイネーブル化またはディセーブル化」（任意）

ISO IGRP メトリックの調整

ISO IGRP のルーティングおよびメトリック計算のデフォルト動作を変更することもできます。たとえば、デフォルト動作を変更すると、システムの動作をチューニングして人工衛星を介した送信が可能になります。ISO IGRP メトリックのデフォルトは、大半のネットワークで優れた処理を実現できるよう慎重に選択されていますが、メトリックを調整することもできます。

（注） ISO IGRP メトリックを調整すると、ネットワーク パフォーマンスに多大な影響を与えるため、すべてのメトリックの調整は慎重に行うようにしてください。この作業は複雑であるため、経験豊富なシステム設計者からのアドバイスがある場合にのみ行うことを推奨します。

CLNS の ISO IGRP ルーティング プロトコルには、さまざまなメトリックを使用できます。信頼性と負荷の ISO IGRP 複合メトリック計算に使用するメトリック定数を設定するには、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。

コマンド	目的
`Router(config-router)# metric weights qos k1 k2 k3 k4 k5`	ISO IGRP メトリックを調整します。

2 つの追加の ISO IGRP メトリック（インターフェイスに関連付けられた帯域幅と遅延）を設定できます。これらのメトリックの設定に使用する **bandwidth**（インターフェイス）および **delay** インターフェイス コンフィギュレーション コマンドの詳細については、マニュアル『*Cisco IOS Interface Command Reference*』を参照してください。

（注） **bandwidth**（インターフェイス）および **delay** コマンドを使用して ISO IGRP メトリックの値を変更すると、IP IGRP メトリックの値も変更されます。

ISO IGRP タイマーの調整

ISO IGRP の基本的なタイミング パラメータは調整可能です。ISO IGRP ルーティング プロトコルは分散型で非同期のルーティング アルゴリズムを実行するため、ネットワーク内のすべてのルータでこれらのタイマーが同じであることが重要です。

ISO IGRP タイミング パラメータを調整するには、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。

コマンド	目的
`Router(config-router)# timers basic update-interval holddown-interval invalid-interval`	ISO IGRP タイマーを調整します（秒単位）。

スプリット ホライズンのイネーブル化またはディセーブル化

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からルート情報がアドバタイズされないようにします。通常、この機能は複数のルータ間の（特にリンクが破損した場合の）通信を最適化します。

ISO IGRP アップデートのスプリット ホライズンをイネーブルまたは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。

コマンド	目的
`Router(config-if)# clns split-horizon`	ISO IGRP アップデートのスプリット ホライズンをイネーブルにします。
`Router(config-if)# no clns split-horizon`	ISO IGRP アップデートのスプリット ホライズンをディセーブルにします。

すべての LAN インターフェイスのデフォルトでは、スプリット ホライズンがイネーブルになり、X.25、フレーム リレー、または Switched Multimegabit Data Service（SMDS; スイッチド マルチメガビット データ サービス）ネットワーク上の WAN インターフェイスのデフォルトでは、スプリット ホライズンがディセーブルになります。

IS-IS ダイナミック ルーティングの設定

IS-IS は ISO ダイナミック ルーティングの仕様です。IS-IS は、ISO 10589 で説明されています。シスコによる IS-IS の実装では、IS-IS を ISO CLNS ルーティング プロトコルとして設定できます。

IS-IS 設定作業リスト

IS-IS を設定するには、次に示す作業を実行します。IS-IS のイネーブル化は必須です。それ以外の作業は任意ですが、使用している特定のアプリケーションによっては実行が必要になる場合があります。

- 「IS-IS のイネーブル化」（必須）
- 「インターフェイスでのエリアのルーティングのイネーブル化」（任意）
- 「IS-IS エリアへの複数のエリア アドレスの割り当て」（任意）
- 「IS-IS インターフェイス パラメータの設定」（任意）
- 「その他の IS-IS パラメータの設定」（任意）

また、次に示すその他の機能を設定できます。これらの機能については、この章で後述します。

- ルーティング情報のフィルタリング：「パケット転送フィルタの作成と隣接の確立」の項を参照。
- ルーティング プロセス間でのルーティング情報の再配布：「ルーティング情報の再配布」の項を参照。
- アドミニストレーティブ ディスタンスの設定：「優先ルートの指定」の項を参照。

IS-IS のイネーブル化

他のルーティング プロトコルとは異なり、IS-IS をイネーブルにするには、IS-IS ルーティング プロセスを作成し、それをネットワークではなく、特定のインターフェイスに割り当てる必要があります。マルチエリア IS-IS 設定構文を使用して、シスコ ユニットごとに複数の IS-IS ルーティング プロセスを指定できます。その後、IS-IS ルーティング プロセスのインスタンスごとにパラメータを設定します。

小規模の IS-IS ネットワークは、ネットワークにすべてのルータが含まれる単一のエリアとして構築されます。ネットワークの規模が大きくなるにつれて、通常、ネットワークはすべてのエリアからのすべてのレベル 2 ルータの集合で構成されるバックボーンに再編成され、そこからローカル エリアに接続されます。ローカル エリア内では、ルータがすべてのシステム ID に到達する方法を認識しています。エリア間では、ルータはバックボーンに到達する方法を認識しており、バックボーン ルータが他のエリアに到達する方法を認識しています。

ルータはレベル 1 隣接を確立して、ローカル エリア内でルーティングを実行します（エリア内ルーティング）。ルータはレベル 2 隣接を確立して、レベル 1 エリア間でルーティングを実行します（エリア間ルーティング）。

ネットワークの中には、レベル 1 ルーティングだけをサポートするレガシー機器を使用するものもあります。このような装置は、通常、パフォーマンスの制限が原因で集約できない多数の小規模なエリアに分かれています。Cisco ルータを使用して、各エリアとレベル 2 バックボーンの相互接続を確立します。

単一の Cisco ルータは最大 29 個のエリアに参加でき、レベル 2 ルーティングをバックボーンで実行できます。通常、各ルーティング プロセスは 1 つのエリアに対応します。デフォルトでは、最初に設定されるルーティング プロセスのインスタンスで、レベル 1 とレベル 2 の両方のルーティングが実行されます。自動的にレベル 1 エリアとして扱われる追加のルータ インスタンスを設定できます。パラメータは IS-IS ルーティング プロセスのインスタンスごとに個別に設定する必要があります。

（注） ルーティング情報とエリア トポロジが制限されていない限り、多くの場合、29 個の IS-IS プロセスを実行するために必要な CPU メモリはローエンド プラットフォームにはありません。

IS-IS マルチエリア ルーティングの場合、レベル 2 ルーティングを実行するために設定できるプロセスは 1 つだけですが、シスコ ユニットごとに最大 29 個のレベル 1 エリアを定義できます。任意のプロセスでレベル 2 ルーティングが設定されている場合、すべての追加プロセスは自動的にレベル 1 に設定されます。同時にレベル 1 ルーティングを実行するようにこのプロセスを設定できます。レベル 2 ルーティングがルータ インスタンスで必要ない場合、**is-type** コマンドを使用してレベル 2 機能を削除します。**is-type** コマンドは、別のルータ インスタンスをレベル 2 ルータとして設定するためにも使用します。

IS-IS 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。

	コマンド	目的
ステップ 1	`Router(config)# router isis [area-tag]`	指定したルーティング プロセスで IS-IS ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 この IS-IS ルータ インスタンスが割り当てられるエリアを識別するには、*area-tag* 引数を使用します。複数の IS-IS エリアを設定する場合、*tag* の値は必須です。 最初に設定される IS-IS インスタンスは、デフォルトでレベル 1-2 になります。それ以外のインスタンスは自動的にレベル 1 になります。特定のルーティング プロセスによって実行されるルーティングのレベルを変更するには、**is-type** コマンドを使用します。
ステップ 2	`Router(config-router)# net network-entity-title`	ルーティング プロセスの NET を設定します。マルチエリア IS-IS を設定する場合は、ルーティング プロセスごとに NET を指定します。NET とアドレスの名前を指定できます。

tag オプションを使用して、ルーティング プロセスにわかりやすい名前を割り当てることができます。アドレスに加えて NET の名前を指定することもできます。名前を割り当てる方法については、この章の「ショートカット NSAP アドレスの指定」の項を参照してください。

IS-IS ルーティングの設定例については、この章の最後にある「IS-IS ルーティングの設定例」の項を参照してください。

インターフェイスでのエリアのルーティングのイネーブル化

CLNS ルーティングをイネーブルにし、IS-IS ルーティング プロセスのインスタンスごとにエリアを指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# interface type number`	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 2	`Router(config-if)# clns router isis [area-tag]`	ネットワーク プロトコルが ISO-CLNS である場合にインターフェイスが IS-IS をアクティブにルーティングするように指定し、このインターフェイスのこのルーティング プロセスに関連付けられたエリアを識別します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスの IP アドレスを定義します。 インターフェイスで統合 IS-IS ルーティング プロトコルを使用する場合は、そのインターフェイスに IP アドレスが必要です。統合 IS-IS ルーティング プロトコルは、IP ベースのネットワークと CLNS ベースのネットワークのルーティング プロトコルとして使用できます。

IS-IS ルーティングの設定例については、この章の最後にある「IS-IS ルーティングの設定例」の項を参照してください。

IS-IS エリアへの複数のエリア アドレスの割り当て

IS-IS ルーティングでは、同じルータでの複数のエリア アドレスの割り当てがサポートされています。この概念は *マルチホーミング* と呼ばれます。マルチホーミングでは、次のようにネットワーク アドレスをスムーズに移行するためのメカニズムが用意されています。

- エリアの分割：特定のエリア内のノードが管理の困難な状態にまで蓄積したり、ノードが原因で過剰なトラフィックが発生したり、エリアの使用可能なアドレス空間を超えたりするおそれがあります。複数のエリア アドレスを割り当てて、サービスを中断せずにネットワークを個別のエリアにスムーズに分割することができます。
- エリアの結合：暫定のエリア アドレスを使用して、3 つまでの個別のエリアを同一のエリア アドレスを共有する単一エリアに結合します。
- 別のアドレスへの変更：特定のノード グループのエリア アドレスを変更することが必要になる場合があります。複数のエリア アドレスを使用して、古いエリア アドレス用の着信トラフィックを引き続き関連するノードにルーティングできるようにします。

単一ルータでの複数のエリア アドレスの割り当てはスタティックに行う必要があります。シスコは現在、単一ルータでの最大 3 つのエリア アドレスの割り当てをサポートしています。すべてのアドレスでシステム ID が同じである必要があります。たとえば、1 つのアドレス（*area1* とシステム ID）を割り当てて、異なるエリアで 2 つの追加アドレス（*area2* とシステム ID、*area3* とシステム ID）を割り当てることができます（システム ID は同じ）。1 つのドメイン内で使用できるエリアの数に制限はありません。

ルータは、隣接ルータをダイナミックに認識できます。このプロセスの一環として、ルータは互いにそれぞれのエリア アドレスを通知します。2 つのルータが少なくとも 1 つのエリア アドレスを共有している場合は、2 つのルータのエリア アドレス セットが結合されます。結合されたセットに含めることができるアドレスは 3 つまでです。それより多い場合は、数値が最小の 3 つのアドレスが保持され、他のアドレスはすべてドロップされます。

IS-IS エリアで複数のエリア アドレスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# router isis [area-tag]`	指定したルーティング プロセスで IS-IS ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 この IS-IS ルータ インスタンスが割り当てられるエリアを識別するには、*area-tag* 引数を使用します。マルチエリア IS-IS を設定する場合、*area-tag* の値は必須です。従来の IS-IS を設定する場合、*area-tag* の値は任意です。 最初に設定される IS-IS インスタンスは、デフォルトでレベル 1-2 になります。それ以外のインスタンスは自動的にレベル 1 になります。特定のルーティング プロセスによって実行されるルーティングのレベルを変更するには、**is-type** コマンドを使用します。
ステップ 2	`Router(config-router)# net network-entity-title`	ルーティング プロセスの NET を設定します。マルチエリア IS-IS を設定する場合は、ルーティング プロセスごとに NET を指定します。NET とアドレスの名前を指定できます。

NET と複数のエリア アドレスの設定例については、この章の最後にある「NET の設定例」の項を参照してください。

IS-IS インターフェイス パラメータの設定

シスコの IS-IS 実装を使用すると、インターフェイス固有の IS-IS パラメータをカスタマイズできます。次に示す任意の作業を実行できます。

- 「IS-IS リンクステート メトリックの調整」（任意）
- 「アドバタイズされる hello 間隔と hello 乗数の設定」（任意）
- 「アドバタイズされる Complete Sequence Number PDU 間隔の設定」（任意）
- 「再送信間隔の設定」（任意）
- 「再送信スロットル間隔の設定」（任意）
- 「代表ルータの選定の指定」（任意）
- 「インターフェイス回線タイプの指定」（任意）
- 「IS-IS 認証パスワードの設定」（任意）
- 「LSP フラッディングの制限」（任意）

これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータについては、ネットワーク内のすべてのルータで統一性を維持する必要があります。したがって、これらのパラメータを設定する場合は、ネットワーク上のすべてのルータのコンフィギュレーションと互換性のある値にしてください。

IS-IS リンクステート メトリックの調整

指定したインターフェイスのコストを設定できます。デフォルト メトリックが IS-IS メトリックの値として使用され、Quality of Service（QoS）ルーティングが実行されない場合に割り当てられます。Cisco IOS ソフトウェアでサポートされている設定可能なメトリックは *default-metric* だけで、レベル 1 ルーティングとレベル 2 ルーティングのいずれか、または両方で設定できます。*default-metric* の範囲は 0 ～ 63 です。デフォルト値は 10 です。

リンクステート メトリックを設定するには、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。

コマンド	目的
`Router(config-if)# isis metric default-metric [level-1 | level-2]`	指定したインターフェイスのメトリック（コスト）を設定します。

アドバタイズされる hello 間隔と hello 乗数の設定

Cisco IOS ソフトウェアがインターフェイス上で送信する hello パケットの間隔（秒単位）を指定できます。また、IS-IS hello パケットで送信されるホールド タイムを決定するためにインターフェイス上で使用されるデフォルトの hello パケット乗数を変更することもできます（デフォルトは 3 です）。

ホールド タイムは、ネイバーが次の hello パケットを待機する時間を決定します。この時間が経過すると、ネイバーはダウンしていると宣言されます。ホールド タイムは、不具合のあるリンクまたはネイバーが検出され、ルートが再計算されるまでの時間を表します。

アドバタイズされる hello 間隔と hello 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。

	コマンド	目的
ステップ 1	`Router(config-if)# isis hello-interval seconds [level-1 | level-2]`	Cisco IOS ソフトウェアにより送信される hello パケットの時間間隔を指定します。
ステップ 2	`Router(config-if)# isis hello-multiplier multiplier [level-1 | level-2]`	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ルータは隣接がダウンしていると宣言します。

hello 間隔は、シリアル ポイントツーポイント インターフェイスを除き、レベル 1 およびレベル 2 について個別に設定できます（シリアル リンクで送信される hello パケットのタイプは 1 種類だけであるため、hello パケットはレベル 1 またはレベル 2 とは関係ありません）。X.25、SMDS、およびフレーム リレー マルチアクセス ネットワークの任意のレベルを指定してください。

isis hello-multiplier コマンドは、hello パケットが頻繁に失われ、必要以上に IS-IS 隣接で障害が発生する状況で使用します。リンク障害を検出するために必要な時間を長くせずに、hello プロトコルの信頼性をあげるには、hello 乗数を大きくし、hello 間隔を小さくします（**isis hello-interval** コマンド）。

アドバタイズされる Complete Sequence Number PDU 間隔の設定

Complete Sequence Number PDU（CSNP）は、データベースの同期を維持するために代表ルータによって送信されます。

インターフェイスの IS-IS CSNP 間隔を設定するには、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。

コマンド	目的
`Router(config-if)# isis csnp-interval seconds [level-1 | level-2]`	指定したインターフェイスの IS-IS CSNP 間隔を設定します。

isis csnp-interval コマンドは、シリアル ポイントツーポイント インターフェイスには適用されません。WAN がマルチアクセス メッシュ ネットワークとして認識されている場合、これは WAN 接続にも適用されます。

再送信間隔の設定

ポイントツーポイント リンクの Link-State PDU（LSP; リンクステート PDU）の再送信間隔を秒数で設定できます。

再送信レベルを設定するには、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。

コマンド	目的
`Router(config-if)# isis retransmit-interval seconds`	ポイントツーポイント リンクの IS-IS LSP の再送信間隔を秒数で設定します。

指定する値は、ネットワーク上の任意の 2 つのルータ間で予測されるラウンド トリップ遅延よりも大きい整数にする必要があります。このパラメータの設定は慎重に行う必要があります。設定を誤ると、不要な再送信が発生します。この設定値は、シリアル回線と仮想リンクでは大きくする必要があります。

再送信スロットル間隔の設定

ポイントツーポイント リンクで IS-IS LSP を再送信する最大レート（パケット間のミリ秒数）を設定できます。この間隔は、再送信間隔（*同じ* LSP の連続する再送信の間隔）とは異なります。

再送信スロットル間隔を設定するには、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。

コマンド	目的
`Router(config-if)# isis retransmit-throttle-interval` *milliseconds*	IS-IS LSP 再送信スロットル間隔を設定します。

このコマンドは通常では不要ですが、非常に大規模なネットワークにおいてポイントツーポイントのネイバー数が多い場合に必要になります。

代表ルータの選定の指定

代表ルータの選定に使用するプライオリティを設定できます。プライオリティは、レベル 1 およびレベル 2 で個別に設定できます。代表ルータを使用すると、マルチアクセス ネットワークに必要な隣接関係の数を削減でき、これによってルーティング プロトコル トラフィックの量とトポロジ データベースのサイズも削減されます。

代表ルータの選定に使用するプライオリティを設定するには、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。

コマンド	目的
`Router(config-if)# isis priority` *value* [**level-1** | **level-2**]	代表ルータの選定に使用するプライオリティを設定します。

インターフェイス回線タイプの指定

IS-IS プロトコルでは自動的にエリア境界が決定され、レベル 1 とレベル 2 のルーティングが別々に維持されるため、通常、この機能を設定する必要はありません。ただし、指定したインターフェイスの隣接レベルを指定できます。

指定したインターフェイスのネイバーの隣接を設定するには、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。

コマンド	目的
`Router(config-if)# isis circuit-type` [**level-1** | **level-1-2** | **level-2-only**]	指定したインターフェイスのネイバーに必要な隣接のタイプを設定します（インターフェイス回線タイプを指定します）。

レベル 1 を指定した場合、このノードとそのネイバーに共通するエリア アドレスが少なくとも 1 つ存在するときには、レベル 1 隣接が確立されます。

レベル 1 とレベル 2 の両方を指定した場合（デフォルト値）、ネイバーもレベル 1 とレベル 2 の両方として設定されており、共通するエリアが少なくとも 1 つ存在するときには、レベル 1 隣接とレベル 2 隣接が確立されます。共通するエリアが存在しない場合、レベル 2 隣接が確立されます。

レベル 2 だけを指定した場合、レベル 2 隣接が確立されます。ネイバー ルータがレベル 1 ルータである場合、隣接は確立されません。

IS-IS 認証パスワードの設定

ルーティング レベルごとに異なる認証パスワードを割り当てることができます。デフォルトでは、認証はディセーブルです。レベル 1 またはレベル 2 を指定すると、レベル 1 ルーティングまたはレベル 2 ルーティングだけのパスワードがそれぞれイネーブルになります。レベルを指定しない場合、デフォルトはレベル 1 です。

インターフェイスの認証パスワードを設定するには、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。

コマンド	目的
`Router(config-if)# isis password password [level-1 | level-2]`	インターフェイスの認証パスワードを設定します。

認証パスワードはエリアとドメインに割り当てることができます。エリア パスワードは、レベル 1（ステーション ルータ）の LSP、CSNP、および Partial Sequence Number PDU（PSNP）に挿入されます。ルーティング ドメイン認証パスワードは、レベル 2（エリア ルータ）の LSP、CSNP、および PSNP に挿入されます。

エリア パスワードまたはドメイン パスワードを設定するには、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。

コマンド	目的
`Router(config-router)# area-password password`	エリア認証パスワードを設定します。
`Router(config-router)# domain-password password`	ルーティング ドメイン認証パスワードを設定します。

LSP フラッディングの制限

LSP フラッディングの制限は IS-IS ネットワークにおいて一般的に重要であり、マルチエリア IS-IS ネットワークの設定に限られません。NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）トランスポート上の完全メッシュ化されたポイントツーポイント リンク セットなど、冗長性の高いネットワークでは、LSP のフラッディングによってネットワークのスケーラビリティが制限されることがあります。LSP フラッディングは、次の 2 つの方法で低減できます。

- 「特定のインターフェイス上でのフラッディングのブロック」

  メッシュ グループよりもフル ブロッキングが優れている点は、設定と理解が簡単で、フラッディングされる LSP がより少なくなることです。すべてのリンクでフラッディングをブロックすると最高のスケーリング パフォーマンスが得られますが、ネットワーク構造の堅牢性が低下します。すべてのリンクでフラッディングを許可すると、スケーリング パフォーマンスが低下します。

- 「メッシュ グループの設定」

  フル ブロッキングよりもメッシュ グループが優れている点は、フル ブロッキングでは、複数ホップ上で一部のルータが LSP を受信できるのに対して、メッシュ グループでは、1 ホップ上でメッシュのすべてのルータに LSP をフラッディングできることです。フラッディングにおけるこの比較的短い遅延は、コンバージェンス時間に影響することもありますが、コンバージェンス時間全体に比べればごくわずかです。

特定のインターフェイス上でのフラッディングのブロック

特定のインターフェイス上でフラッディングを完全にブロック（フル ブロッキング）することができます。この場合、それらのインターフェイスで新しい LSP がフラッディングされることはありません。ただし、多数のリンクでフラッディングをブロックした場合に、残りのリンクがすべてダウンすると、ネットワークの他の部分に接続可能であっても、ルータがリンクステート データベースを同期できなくなります。リンクステート データベースが更新されなくなると、多くの場合、ルーティング ループが発生します。

選択したポイントツーポイント リンクで CSNP を使用してリンクステート データベースを同期するには、選択したポイントツーポイント リンク（通常のフラッディングはブロックされるリンク）に対して、**isis csnp-interval** コマンドを使用して CSNP 間隔を設定します。この目的に CSNP を使用するのは、他の方法がない場合だけにする必要があります。

メッシュ グループの設定

メッシュ グループ（1 つのルータのインターフェイス セット）を設定すると、冗長フラッディングを制限できます。特定のメッシュ グループの複数のインターフェイス経由で到達可能なすべてのルータは、密に接続されている（各ルータが他のルータへのリンクを多数持っている）と見なされます。この場合、多数のリンクに障害が発生しても、ネットワークから孤立するルータは 1 つもありません。

通常、新しい LSP が 1 つのインターフェイスで受信されると、新しい LSP は、そのルータの他のすべてのインターフェイスでフラッディングされます。メッシュ グループに属する 1 つのインターフェイスで新しい LSP が受信されると、新しい LSP は、同じメッシュ グループに属するその他のインターフェイスではフラッディングされません。

メッシュ グループは、ルータ グループ間のリンクから成るフル メッシュに依存します。1 つ以上のフル メッシュのリンクがダウンした場合、ネットワークの他の部分に接続可能であっても、フル メッシュは破損し、一部のルータで新しい LSP を受信できなくなることがあります。LSP フラッディングを最適化または制限するためにメッシュ グループを設定する場合は、メッシュ グループのインターフェイスがダウンしたときにフラッディングを行う代替パスを選択する必要があります。

不完全なフラッディングが行われる可能性を最小限に抑えるには、メッシュ内の最低限のリンク セットで制限なくフラッディングできるようにする必要があります。すべての物理パスをカバーできる必要最低限の論理リンクを選択した場合、フラッディングは非常に小さくなりますが、堅牢性も低下します。理想的には、LSP フラッディングがスケーリング パフォーマンスの不利益にならない程度のリンクだけを選択すべきですが、考えられる障害状況の大半で、残りのネットワークから論理的に切断されるルータがないことを保証するのに十分なリンクを選択する必要があります。

その他の IS-IS パラメータの設定

シスコの IS-IS 実装を使用すると、特定の IS-IS パラメータをカスタマイズできます。次に示す任意の作業を実行できます。

- 「ルータ レベル サポートの指定」（任意）
- 「IS-IS LSP エラーの無視」（任意）
- 「隣接状態の変化のロギング」（任意）
- 「IS-IS LSP 最大伝送ユニット サイズの変更」（任意）
- 「パーティショニングの回避のイネーブル化」（任意）
- 「エリアのルーティング レベルの変更」（任意）
- 「show コマンドの出力の変更」（任意）

ルータ レベル サポートの指定

IS-IS プロトコルでは自動的に IS タイプが決定されるため、IS タイプを設定する必要はほとんどありません。ただし、ルータを、レベル 1（エリア内）ルータ、レベル 1 ルータとレベル 2（エリア間）ルータの両方、またはエリア間ルータのみとして機能するように設定できます。

IS-IS レベルを設定するには、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。

コマンド	目的
`Router(config-router)# is-type [level-1 | level-1-2 | level-2-only]`	ルータが動作する IS-IS レベルを設定します。

IS-IS LSP エラーの無視

内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するようにルータを設定できます。受信側ルータは、LSP を使用してルーティング テーブルのメンテナンスを行います。

IS-IS プロトコルの定義では、正しくないデータリンク チェックサムを持つ LSP を受信した場合は受信側でパージして、LSP の発信側によって再生成されるようにする必要があります。ただし、正しいデータリンク チェックサムを持つ LSP をまだ送信している間にデータ破損を引き起こすリンクがネットワークにあった場合、大量の LSP をパージして再生成する連続サイクルが発生し、ネットワークの機能が停止してしまう可能性があります。

内部チェックサム エラーのある LSP をルータが無視できるようにするには、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。

コマンド	目的
`Router(config)# router isis`	IS-IS ルーティング プロトコルを指定し、IS-IS プロセスを指定します。
`Router(config-router)# ignore-lsp-errors`	LSP に内部チェックサム エラーがある場合に LSP をパージするのではなく無視します。

（注） デフォルトでは、**ignore-lsp-errors** コマンドはイネーブルです。したがって、ネットワークの安定性のため、破損した LSP はパージされずにドロップされます。破損した LSP を明示的にパージするには、**no ignore-lsp-errors** コマンドを発行してください。

隣接状態の変化のロギング

IS-IS の隣接状態が変化（アップまたはダウン）したときにログ メッセージを生成するように IS-IS を設定できます。ログ メッセージを生成すると、大規模なネットワークをモニタする場合に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

IS-IS の隣接状態が変化したときにログ メッセージを生成するには、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。

コマンド	目的
Router(config-router)# **log-adjacency-changes**	IS-IS の隣接状態の変化をロギングします。

IS-IS LSP 最大伝送ユニット サイズの変更

通常の状況では、デフォルトの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズで十分です。ただし、リンクの MTU が 1500 バイトよりも小さい場合、それに応じて、ネットワークの各ルータで LSP MTU を小さくする必要があります。LSP MTU を小さくしないと、ルーティングで予期しない動作が発生します。

MTU サイズは、ネットワークのすべてのリンクのうちの最小 MTU 以下にする必要があります。デフォルトのサイズは 1497 バイトです。

注意 リンクの CLNS MTU（IP のルーティングに使用される場合でも、IS-IS で適用される値）は、IP MTU と異なることがあります。IS-IS に関連するリンク MTU を確認するには、**show clns interface** コマンドを使用して値を表示してください。

IS-IS LSP の MTU サイズを変更するには、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。

コマンド	目的
Router(config-router)# **lsp-mtu** *size*	最大 LSP パケット サイズ（バイト単位）を指定します。

（注） ネットワークのいずれかのリンクで MTU を小さくした場合は、そのリンクに直接接続されたルータだけでなく、すべてのルータを変更する必要があります。このルールはネットワークのすべてのルータに適用されます。

パーティショニングの回避のイネーブル化

冗長性トポロジを使用している ISO CLNS ネットワークでは、レベル 1-2 ボーダ ルータ、すべての隣接レベル 1 ルータ、およびエンド ホストとの間でフル接続が失われた場合、エリアを「パーティショニング済み」とする可能性があります。そのような場合、どのルータもレベル 1 エリアにあるエンド ホストのサブセットだけにしか到達できない場合であっても、複数のレベル 1-2 ボーダ ルータがレベル 1 エリア プレフィクスをバックボーン エリアにアドバタイズします。

イネーブルの場合、ボーダ ルータがレベル 1 エリア プレフィクスをレベル 2 バックボーンにアドバタイズするのを停止することによって、**partition avoidance** コマンドでこのパーティショニングを回避できます。

レベル 1 エリア自体内における他のケースの接続消失は、ボーダ ルータによって検出または修正されず、このコマンドは無効です。

パーティショニングの回避をイネーブルにするには、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。

コマンド	目的
`Router(config-router)# partition avoidance`	ボーダ ルータ、すべての隣接レベル 1 ルータ、およびエンド ホストとの間でフル接続が失われた場合に、IS-IS レベル 1-2 ボーダ ルータで、レベル 1 エリア プレフィクスをレベル 2 バックボーンにアドバタイズするのを停止させます。

エリアのルーティング レベルの変更

エリアに対して設定されたルーティング レベルは、**is-type** コマンドを使用して変更できます。ルータ インスタンスがレベル 1-2 エリア（シスコ ユニットにおける IS-IS ルーティング プロセスの最初のインスタンスのデフォルト）に設定されている場合は、**is-type** コマンドを使用してそのエリアのレベル 2（エリア間）ルーティングを削除し、ルーティング レベルをレベル 1（エリア内）に変更できます。**is-type** コマンドを使用してエリアにレベル 2 ルーティングを設定することもできますが、シスコ ユニットでレベル 2 に設定されている IS-IS ルータのインスタンスは、レベル 2 に設定されている唯一のインスタンスである必要があります。

特定のエリアの IS-IS ルーティング プロセスのルーティング レベルを変更するには、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。

コマンド	目的
`Router(config-router)# is-type [level-1 | level-1-2 | level-2-only]`	IS-IS ルーティング プロセスのインスタンスのルーティング レベルを設定します。

show コマンドの出力の変更

マルチエリア機能を使用しているときに出力をカスタマイズして、出力を読みやすくするには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# isis display delimiter [return cnt |char cnt]`	個々の IS-IS エリアに関する情報の表示を分割するために使用する区切り文字を指定します。

たとえば、次のコマンドを実行すると、個々のエリアに関する情報が 14 個のハイフン（-）で区切られて表示されます。

```
isis display delimiter - 14
```

2 つのレベル 1 エリアと 1 つのレベル 2 エリアが設定されている場合の出力は次のようになります。

```
dtp-5# show clns neighbors
--------------
Area L2BB:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0009 Tu529       172.21.39.9     Up     25        L1L2 IS-IS
--------------
Area A3253-01:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0053 Et1         0060.3e58.ccdb  Up     22        L1   IS-IS
0000.0000.0003 Et1         0000.0c03.6944  Up     20        L1   IS-IS
--------------
Area A3253-02:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 Et2         0000.0c03.6bc5  Up     27        L1   IS-IS
0000.0000.0053 Et2         0060.3e58.ccde  Up     24        L1   IS-IS
```

CLNS スタティック ルーティングの設定

スタティック ルーティング機能を使用するために、ルーティング プロセスを明示的に指定する必要はありません。ルータで ISO IGRP または IS-IS ダイナミック ルーティングを設定している場合でも、特定のスタティック ルートを入力し、それをグローバルに適用することができます。

スタティック ルートを設定するには、次に示す作業を実行します。CLNS のイネーブル化だけが必須です。それ以外の作業は任意ですが、使用している特定のアプリケーションによっては実行が必要になる場合があります。

- 「スタティック ルートのイネーブル化」（必須）
- 「スタティック ルートのバリエーションの設定」（任意）
- 「メディア アドレスへの NSAP アドレスのマッピング」（任意）

スタティック ルートのイネーブル化

スタティック ルーティングを設定するには、ルータおよびインターフェイスで CLNS をイネーブルにする必要があります。ISO IGRP または IS-IS ルーティング プロトコルを設定するときに、ルータの CLNS ルーティングはデフォルトでイネーブルになります。指定した NSAP プレフィクスで始まる NSAP アドレスは、ネクスト ホップ ノードに転送されます。

ルータで CLNS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# clns routing`	CLNS を設定します。
ステップ 2	`Router(config-if)# clns net {net-address | name}`	ルータが ISO IGRP または IS-IS を使用して CLNS パケットをダイナミックにルーティングするように設定されていない場合に、NSAP アドレスをルータに割り当てます。
ステップ 3	`Router(config)# clns route nsap-prefix {next-hop-net | name}`	特定のスタティック ルートを入力します。

（注） ISO IGRP または IS-IS を使用して CLNS パケットをダイナミックにルーティングするようにルータを設定していない場合は、アドレスをルータに割り当てる必要があります。

インターフェイスでダイナミック ルーティングを実行しないでエンド システムへの ISO CLNS パケット トラフィックを通過させる場合は、インターフェイスごとに ISO CLNS をイネーブルにする必要もあります。インターフェイスで IS-IS または ISO IGRP ルーティングを設定すると、ISO CLNS は自動的にイネーブルになりますが、インターフェイスでダイナミック ルーティングを実行しない場合は、手動で CLNS をイネーブルにする必要があります。NSAP アドレスは特定のインターフェイスに割り当てることができます。NSAP アドレスを割り当てると、Cisco IOS ソフトウェアで各インターフェイスの異なるアドレスをアドバタイズできるようになります。異なるアドレスのアドバタイズは、スタティック ルーティングを実行していて、各インターフェイスのルータに使用される送信元 NET を制御する必要がある場合に役立ちます。

インターフェイスで CLNS 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。

	コマンド	目的
ステップ 1	`Router(config-if)# clns enable`	各インターフェイスの ISO CLNS をイネーブルにします。
ステップ 2	`Router(config-if)# clns net {nsap-address | name}`	NSAP アドレスを特定のインターフェイスに割り当てます。

スタティック ルートの設定例については、この章の最後にある「基本的なスタティック ルーティングの例」、「スタティック ドメイン内ルーティングの例」、および「スタティック ドメイン間ルーティングの例」の項を参照してください。

スタティック ルートのバリエーションの設定

clns route グローバル コンフィギュレーション コマンドのバリエーションを使用する次の作業を実行できます。

- ネイバーの NSAP アドレスがわからない場合に、指定したインターフェイスおよびメディア アドレスにネクスト ホップをバインドする。このバージョンの **clns route** コマンドが特定のインターフェイスに文字通り*適用*されるわけではないことに注意してください。
- ルータのドメイン（ISO IGRP）外またはエリア（IS-IS）外にある特定の NSAP プレフィクスを持つパケットを廃棄する。
- デフォルトのプレフィクスを指定する。

特定のスタティック ルートの入力、パケットの廃棄、またはデフォルトのプレフィクスの設定を行うには、グローバル コンフィギュレーション モードで次のコマンドの 1 つまたはすべてを使用します。

（注） ルータのドメイン（ISO IGRP）またはエリア（IS-IS）内にある NSAP プレフィクスを持つパケットを廃棄またはフィルタするには、この章の「パケット転送フィルタの作成と隣接の確立」の項を参照してください。

コマンド	目的
`Router(config)# clns route nsap-prefix type number [snpa-address]`	特定のインターフェイスの特定のスタティック ルートを入力します。
`Router(config)# clns route nsap-prefix discard`	指定した NSAP プレフィクスを持つパケットを廃棄するようソフトウェアに明示的に指定します。
`Router(config)# clns route default type number`	NSAP プレフィクスを指定するのではなく、デフォルトのプレフィクスを設定します。

メディア アドレスへの NSAP アドレスのマッピング

概念上は、各 ES は 1 つのエリアに存在します。ES は、ES-IS パケットを待ち受けることによって最も近い IS を検出します。各 ES は、そのエリア内の IS と直接通信できる必要があります。

ある ES が別の ES と通信する場合、その ES は同じメディア上の任意の IS にパケットを送信します。

1. IS は宛先 NSAP アドレスを検索し、最適ルートに沿ってパケットを転送します。宛先 NSAP アドレスが別のエリアの ES のものである場合、レベル 1 IS が最も近いレベル 2 IS にパケットを送信します。
2. レベル 2 IS は、宛先エリア内にあるレベル 2 IS に到達するまで、宛先エリアへの最適パスに沿ってパケットを転送します。

3. 次に、この宛先エリア内の IS は、宛先 ES にパケットが配信されるまで、そのエリア内の最適パスに沿ってパケットを転送します。

ES はそのエリアのレベル 1 IS に到達する方法を認識する必要があり、レベル 1 IS はそのインターフェイスを介して直接到達可能なすべての ES を認識する必要があります。この情報を提供するために、ルータでは ES-IS プロトコルをサポートしています。ルータは、ES-IS プロトコルを実行しているすべての ES をダイナミックに検出します。ES-IS プロトコルを実行していない ES は、スタティックに設定する必要があります。

ルータが、ES-IS、ISO IGRP、または IS-IS を通じて学習されたネイバーではなく、スタティックに設定されたネイバーを持つことが望ましい場合もあります。

（注） ES-IS をサポートしていない ES に対してのみ、スタティック マッピングを使用する必要があります。Cisco IOS ソフトウェアは、ES-IS をサポートしている ES のダイナミックな検出を続けます。

（注） インターフェイスで ISO CLNS、ISO IGRP、または IS-IS を設定している場合、ES-IS ルーティング ソフトウェアはそれらのインターフェイスに対して自動的に ES-IS をオンにします。

ES または IS の NSAP プロトコル アドレスと Subnetwork Point of Attachment（SNPA; サブネットワーク接続点）アドレス（メディア）間のスタティック マッピング情報を入力するには、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。

コマンド	目的
`Router(config-if)# clns es-neighbor nsap snpa`	手動で NSAP/SNPA マッピングを指定するときに使用されるすべてのエンド システムを設定します。
`Router(config-if)# clns is-neighbor nsap snpa`	手動で NSAP/SNPA マッピングを指定するときに使用されるすべての中継システムを設定します。

詳細については、この章の「CLNS over WANs の設定」の項を参照してください。

（注） SNPA は、インターフェイスの CLNS ルートの設定に使用されるデータリンク層アドレス（イーサネット アドレス、X.25 アドレス、フレーム リレー DLCI アドレスなど）です。

その他の機能の設定

ISO CLNS ネットワークのその他の機能を設定するには、次に示す任意の作業を実行します。

- 「ショートカット NSAP アドレスの指定」（任意）
- 「IP ドメイン ネーム システムを使用した ISO CLNS アドレスの検出」（任意）
- 「パケット転送フィルタの作成と隣接の確立」（任意）
- 「ルーティング情報の再配布」（任意）
- 「優先ルートの指定」（任意）
- 「ES-IS hello パケットのパラメータの設定」（任意）
- 「DECnet OSI（フェーズ V）のクラスタ エイリアスの設定」（任意）

- 「Digital-Compatible モードの設定」（任意）
- 「セキュリティ オプションが設定されたパケットの通過許可」（任意）

ショートカット NSAP アドレスの指定

名前に対する NSAP アドレスのマッピングを定義できます。NSAP アドレスに関連付けられた長い一連の数字を入力する代わりに、この名前を使用できるようになります。

名前に対する NSAP アドレスのマッピングを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# clns host name nsap`	名前に対する NSAP アドレスのマッピングを定義します。

使用可能な場合は、**show** および **debug** EXEC コマンドで、割り当てられた NSAP 名が表示されます。ただし、NET および NSAP アドレスを表す名前の使用に関しては、いくつかの影響と要件があります。

コンフィギュレーション ファイルが解析されるとき、**clns host** グローバル コンフィギュレーション コマンドは他のすべての CLNS コマンドの後に生成されます。そのため、NVRAM バージョンの設定を編集して、元の **clns host** コマンドで定義されているアドレスを明示的に変更することはできません。元のアドレスを参照するすべてのコマンドを明示的に変更する必要があります。これらの変更は、名前を受け入れるすべてのコマンドに影響します。

これらの要件の影響を受けるコマンドは次のとおりです。

- **net**（ルータ コンフィギュレーション コマンド）
- **clns is-neighbor**（インターフェイス コンフィギュレーション コマンド）
- **clns es-neighbor**（インターフェイス コンフィギュレーション コマンド）
- **clns route**（グローバル コンフィギュレーション コマンド）

IP ドメイン ネーム システムを使用した ISO CLNS アドレスの検出

ルータで ISO CLNS と IP の両方がイネーブルになっている場合、RFC 1348 に記載されているように、NSAP アドレス タイプを使用して ISO CLNS アドレスを照会するために Domain Naming System（DNS; ドメイン ネーム システム）を使用することができます。この機能は、ISO CLNS の **ping** EXEC コマンドで利用され、Telnet 接続を確立する場合にも役立ちます。この機能は、デフォルトでイネーブルにされています。

ISO CLNS アドレスの DNS クエリーをイネーブルまたは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。

コマンド	目的
`Router(config)# ip domain-lookup nsap`	CLNS アドレスの DNS クエリーをイネーブルにします。
`Router(config)# no ip domain-lookup nsap`	CLNS アドレスの DNS クエリーをディセーブルにします。

パケット転送フィルタの作成と隣接の確立

強力な CLNS フィルタ式（アクセス リスト）を作成することができます。これらのフィルタ式を使用して、ルータ インターフェイスを介したフレームの転送を制御したり、あるいは ES/IS ネイバー、ISO IGRP ネイバー、または IS-IS ネイバーの任意の組み合わせに対して隣接の確立またはフィルタの適用を制御したりすることができます。

CLNS フィルタ式は、CLNS フィルタ セットの複合的かつ論理的な組み合わせです。CLNS フィルタ セットは、CLNS アドレスと照合されるアドレス テンプレートのリストです。アドレス テンプレートは CLNS アドレスのパターンです。パターンは、1 つのアドレスだけと一致する単純な CLNS アドレスか、またはワイルドカード文字、プレフィクス、サフィクスを使用することで複数の CLNS アドレスと一致するパターンです。簡単に参照できるように、頻繁に使用されるアドレス テンプレートにはエイリアスを指定することができます。

CLNS フィルタを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# clns template-alias name template`	頻繁に使用されるアドレス テンプレートにエイリアスを作成します。
`Router(config)# clns filter-set sname [permit | deny] template`	複数のアドレス テンプレートの permit および deny 条件のフィルタ セットを作成します。
`Router(config)# clns filter-expr ename term`	1 つ以上のフィルタ セットを使用して、フィルタ式を作成します。

フィルタ式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。

コマンド	目的
`Router(config-if)# clns access-group name [in | out]`	インターフェイスに転送される、またはインターフェイスから転送されるフレームに、フィルタ式を適用します。
`Router(config-if)# isis adjacency-filter name [match-all]`	IS-IS 隣接にフィルタ式を適用します。
`Router(config-if)# iso-igrp adjacency-filter name`	ISO IGRP 隣接にフィルタ式を適用します。
`Router(config-if)# clns adjacency-filter {es | is} name`	ES-IS によって形成された ES または IS 隣接にフィルタ式を適用します。

CLNS フィルタの設定例については、この章の最後にある「CLNS フィルタの例」の項を参照してください。

ルーティング情報の再配布

Cisco IOS ソフトウェアでは、複数のルーティング プロトコルを同時に実行できるだけでなく、ルーティング プロセス間で情報の再配布を行うこともできます。CLNS ルーティングでは、レベル 1 ホスト ルートのレベル 2 への再配布は行われません。レベル 1 アドレスだけがレベル 2 にアドバタイズされます。

IS-IS ルーティングでは、すべてのレベル 1 エリアのすべてのエリア アドレスからレベル 2 への再配布が暗黙的に行われ、この再配布のために追加の設定を行う必要はありません。IS-IS エリア間の明示的な再配布は設定できません。その他のルーティング プロトコルから特定のエリアへの再配布は可能であり、再配布は、**redistribute** および **route map** コマンドを使用して、ルータ インスタンスごとに設定します。デフォルトでは、再配布はレベル 2 が対象となります。

2 つのルーティング プロセスと 2 つの NET を設定し（これにより、ルータが 2 つのドメインに配置される）、ドメイン間でルーティング情報を再配布することで、ドメイン間ダイナミック ルーティングを実行するように Cisco IOS ソフトウェアを設定することもできます。このように設定されたルータは、*ボーダルータ*と呼ばれます。2 つのルーティング ドメインに存在するルータがある場合に、2 つのドメイン間でルーティング情報を再配布することがあります。

（注） エリア間の再配布を使用する必要はありません。再配布が行われるのは、レベル 2 ルーティングの場合だけです。

ルーティング情報を ISO IGRP ドメインに再配布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。

コマンド	目的
`Router(config)# router iso-igrp [tag]`	ルーティング情報の配布先のルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute iso-igrp [tag] [route-map map-tag]`	再配布する 1 つ以上の ISO IGRP ルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute isis [tag] [route-map map-tag]`	再配布する IS-IS ルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute static [clns | ip]`	再配布するスタティック ルートを指定します。

ルーティング情報を IS-IS ドメインに再配布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。

コマンド	目的
`Router(config)# router isis [tag]`	ルーティング情報の配布先のルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute isis [tag] [route-map map-tag]`	再配布する IS-IS ルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute iso-igrp [tag] [route-map map-tag]`	再配布する 1 つ以上の ISO IGRP ルーティング プロトコルおよびタグ（該当する場合）を指定します。
`Router(config-router)# redistribute static [clns | ip]`	再配布するスタティック ルートを指定します。

（注） デフォルトでは、スタティック ルートが IS-IS に再配布されます。

ルーティング ドメイン間でのルートの再配布を条件付きで制御するには、2 つのドメイン間の*ルート マップ*を定義します。ルート マップを定義すると、ルートのタグを使用して、ルート再配布に影響を与えることができます。

ドメイン間でのルートの再配布を条件付きで制御するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **route-map** *map-tag* {**permit** | **deny**} *sequence-number*	再配布を制御するのに必要なルート マップをすべて定義します。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する場合の条件を定義するには、通常、**route-map** コマンドに続けて、**match** コマンドと **set** コマンドをそれぞれ 1 つ以上使用します。**match** コマンドを使用しない場合は、すべてのルートが再配布されます。**set** コマンドを使用しない場合は、設定アクションが実行されません（照合のみが実行される）。

各 **route-map** コマンドには、関連する **match** および **set** コマンドのリストがあります。**match** コマンドでは*一致基準*を指定します。これは、現在の **route-map** コマンドで許可された再配布の条件です。**set** コマンドでは、再配布の*設定アクション*を指定します。これは、**match** コマンドによって設定された基準に合致する場合に実行する特定の再配布アクションです。すべての **match** 基準に合致したときに、すべての **set** アクションが実行されます。

match route-map コンフィギュレーション コマンドには複数の形式があります。**match** コマンドは任意の順序で入力される可能性がありますが、定義されたすべての一致基準を満たし、**set** コマンドで指定された*設定アクション*に従ってルートが再配布される必要があります。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する場合の一致基準を定義するには、ルート マップ コンフィギュレーション モードで、次のコマンドを 1 つ以上使用します。

コマンド	目的
Router(config-route-map)# **match clns address** *name* [*name...name*]	指定した名前（標準アクセス リスト、フィルタ セット、または式）の 1 つ以上と一致するネットワーク アドレスを持つルートを照合します。
Router(config-route-map)# **match clns next-hop** *name* [*name...name*]	指定した名前（標準アクセス リスト、フィルタ セット、または式）の 1 つ以上と一致するネクスト ホップ アドレスを持つルートを照合します。
Router(config-route-map)# **match clns route-source** *name* [*name...name*]	指定した名前（標準アクセス リスト、フィルタ セット、または式）の 1 つ以上と一致するルータによってアドバタイズされているルートを照合します。
Router(config-route-map)# **match interface** *type number* [*type number...type number*]	指定したインターフェイスの 1 つ以上と一致するネクスト ホップ出力を持つルートを照合します。
Router(config-route-map)# **match metric** *metric-value*	指定したメトリックを持つルートを照合します。
Router(config-route-map)# **match route-type** [**level-1** | **level-2**]	指定したルート タイプのルートを照合します。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する場合の設定アクションを定義するには、ルート マップ コンフィギュレーション モードで、次のコマンドを 1 つ以上使用します。

コマンド	目的
`Router(config-route-map)# set level [level-1 | level-2 | level-1-2]`	ルーティング ドメインの指定されたエリアにアドバタイズされるルートのルーティング レベルを設定します。
`Router(config-route-map)# set metric metric-value`	再配布ルートのメトリック値を設定します。
`Router(config-route-map)# set metric-type {internal | external}`	再配布ルートのメトリック タイプを設定します。
`Router(config-route-map)# set tag tag-value`	再配布ルートに関連付けるタグ値を設定します。

ルート マップの設定例については、この章の最後にある「ダイナミック ドメイン間ルーティングの例」および「TARP の設定例」の項を参照してください。

優先ルートの指定

複数のルーティング プロセスが同じ CLNS ルータで実行されている場合、複数のルーティング プロセスで同じルートをアドバタイズすることができます。

ルータがパケットを転送している場合は、ルータが自身のドメインおよびエリアの外部の宛先にルーティングしない限り、常にダイナミック ルートがスタティック ルートよりも優先されます。ルータは、一致するルートが見つかるまで、自身のエリア内の ISO IGRP ルート、自身のドメイン内の ISO IGRP ルート、自身のエリア内の IS-IS ルートの順に検索します。一致するルートが見つからなかった場合、ルータは自身のプレフィクス テーブル（スタティック ルートと、このルータのエリア（ISO IGRP）、ドメイン（ISO IGRP）、およびエリア（IS-IS）の各ルートの外部の宛先へのルートが格納されている）をチェックします。ルータが自身のプレフィクス テーブルを使用している場合、アドミニストレーティブ ディスタンスが最小のルートが選択されます。

デフォルトでは、次のアドミニストレーティブ ディスタンスが割り当てられます。

- スタティック ルート：10
- ISO IGRP ルート：100
- IS-IS ルート：110

ルーティング プロセスのアドミニストレーティブ ディスタンスを変更する場合は、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。

コマンド	目的
`Router(config-router)# distance value [clns]`	最小のアドミニストレーティブ ディスタンスを設定して、優先ルートを指定します。

（注） **distance** コマンドを入力して設定した CLNS ルートのアドミニストレーティブ ディスタンスは、ルートがルーティング プレフィクス テーブルに格納されている場合にのみ有効になります。

ISO IGRP プレフィクス ルートをスタティック ルートより優先させる場合は、ルーティング プロセスのアドミニストレーティブ ディスタンスを 10（スタティック ルート用に割り当てられた管理ディスタンス）より小さく設定する必要があります。スタティック ルート用に割り当てられたアドミニストレーティブ ディスタンスは変更することができません。

ES-IS hello パケットのパラメータの設定

エンド システムとルータの間の通信用に、ES-IS パラメータを設定することができます。ES-IS パラメータは、通常はデフォルト値のままにします。

ES-IS ルータを設定する場合は、次の点に留意してください。

- ES-IS は、ブロードキャスト機能がイネーブルになっていない限り、X.25 リンク上では実行されません。
- ES hello パケットおよび IS hello パケットは、オプションなしで送信されます。受信パケットにオプションが指定されていても無視されます。

IS および ES は、定期的に hello パケットを送信して、可用性をアドバタイズします。hello パケットの送信頻度は設定可能です。

hello パケットの受信者は、送信元のシステムの隣接エントリを作成します。指定した間隔内に次の hello パケットが受信されなかった場合は、隣接がタイムアウトし、隣接ノードは到達不能と見なされます。

hello パケットおよびパケットの有効性に関するデフォルト レートが設定されています。このデフォルトを変更するには、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。

コマンド	目的
`Router(config)# clns configuration-time` *seconds*	ES hello パケットおよび IS hello パケットの送信レートを指定します。
`Router(config)# clns holding-time` *seconds*	ES hello パケットまたは IS hello パケット内の情報を有効と見なす時間を、これらのパケットの送信者が指定できるようにします。

ES Configuration Timer（ESCT; ES 設定タイマー）のオプションに関するデフォルト レートが設定されています。このデフォルトを変更するには、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。

コマンド	目的
`Router(config-if)# clns esct-time` *seconds*	エンド システムが ES hello パケット PDU を送信する頻度を指定します。

DECnet OSI（フェーズ V）のクラスタ エイリアスの設定

DECnet フェーズ V の *クラスタ エイリアス*を設定すると、複数のシステムで、同じシステム ID をエンド システムの hello パケットでアドバタイズすることができます。Cisco IOS ソフトウェアのクラスタ エイリアスの設定では、NSAP アドレスが同じで SNPA アドレスが異なる複数の ES 隣接をキャッシュ

します。パケットの宛先が共通の NSAP アドレスの場合、Cisco IOS ソフトウェアは、各 SNPA アドレスにパケット負荷を分散します。この機能をサポートしているルータは、各システムにトラフィックを転送します。この機能は、インターフェイス単位でイネーブルにすることができます。

クラスタ エイリアスを設定するには、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。

コマンド	目的
`Router(config-if)# clns cluster-alias`	複数のシステムで、同じシステム ID をエンド システムの hello パケットでアドバタイズできるようにします。

DECnet フェーズ V のクラスタ エイリアスがインターフェイス上でディセーブルになっている場合は、ES hello パケットの情報を使用して、NSAP アドレスの既存の隣接情報がすべて置き換えられます。それ以外の場合は、同じ NSAP アドレスの隣接（SNPA アドレスは異なる）が追加で作成されます。

DECnet OSI のクラスタ エイリアスの設定例については、この章の最後にある「DECnet クラスタ エイリアスの例」の項を参照してください。

Digital-Compatible モードの設定

ES-IS の DECnet の実装が古く、IS hello パケットでアドバタイズされた NSAP アドレスに N セレクタ バイトが存在しない場合は、送受信された IS hello パケットが N セレクタ バイトを無視できるように Cisco IOS ソフトウェアを設定することができます。N セレクタ バイトは、NSAP アドレスの最終バイトです。

Digital-Compatible モード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。

コマンド	目的
`Router(config-if)# clns dec-compatible`	送受信された IS hello パケットが N セレクタ バイトを無視できるようにします。

セキュリティ オプションが設定されたパケットの通過許可

デフォルトでは、Cisco IOS ソフトウェアは、セキュリティ オプションが設定されたパケットをすべて破棄します。この動作はディセーブルにすることができます。このようなパケットが通過できるようにするには、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。

コマンド	目的
`Router(config)# clns security pass-through`	ソフトウェアでセキュリティ オプションが設定されていると見なされたパケットの受信を許可します。

（注） ISO CLNS ルーティング ソフトウェアは、輻輳が発生した場合を除き、レコード ルート オプション、ソース ルート オプション、および QoS オプションを無視します。セキュリティ オプションが設定されていると、オプションが不正であることが示され、パケットが拒否されます。

CLNS over WANs の設定

この項では、ISO CLNS over WANs の実行に関する一般情報を示します。

High-Level Data Link Control（HDLC; ハイレベル データ リンク制御）、PPP、Link Access Procedure, Balanced（LAPB; 平衡型リンク アクセス手順）、X.25、フレーム リレー、Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）、または SMDS のカプセル化を行うと、シリアル インターフェイスで CLNS ルーティングを使用することができます。CLNS の着信パケットおよび発信パケットは、PPP を介した高速スイッチングが可能です。

HDLC カプセル化を使用するには、リンクの両端にルータが存在する必要があります。X.25 カプセル化を使用する場合、および IS-IS または ISO IGRP がインターフェイスで使用されていない場合は、NSAP-to-X.121 アドレス マッピングを手動で入力する必要があります。LAPB、SMDS、フレーム リレー、および X.25 のカプセル化では、他のベンダーと相互運用します。

ISO IGRP および IS-IS は、WAN を介して設定することができます。

X.25 はブロードキャスト メディアではないため、NSAP/NET（プロトコル アドレス）と SNPA（メディア アドレス）の間のマッピングを自動的にアドバタイズしたり、記録したりするプロトコル（ES-IS など）をブロードキャストしません（X.25 では、SNPA が X.25 ネットワークのアドレス（X.121 アドレス）になります。これらのアドレスは、通常、X.25 ネットワークのプロバイダーによって割り当てられます）。スタティック ルーティングを使用している場合は、**x25 map** コマンドで、NSAP-to-X.121 アドレス マッピングを設定する必要があります。

CLNS over X.25 を使用するようシリアル回線を設定するには、一般的な X.25 情報と CLNS に固有の情報を設定する必要があります。まず最初に、一般的な X.25 情報を設定します。次に、CLNS のスタティック マッピング情報を入力します。

X.25 の非デフォルト パケットやウィンドウ サイズ、着信払い情報などを指定できます。X.25 機能の指定可能な情報は、『*Cisco IOS Wide-Area Networking Configuration Guide*』の「Configuring X.25 and LAPB」の章に記載されている **x25 map** インターフェイス コンフィギュレーション コマンドの情報とまったく同じです。

CLNS over X.25 の設定例については、この章の最後にある「ISO CLNS over X.25 の例」の項を参照してください。

ISO CLNS のパフォーマンスの向上

通常、CLNS パケット スイッチングに関するルータのデフォルト設定を変更する必要はありません。ただし、ネットワークのパフォーマンスに関する変更を行う場合には、変更できる点がいくつかあります。ここでは、ISO CLNS の変更可能なパラメータについて説明します。

- 「MTU サイズの指定」（任意）
- 「チェックサムのディセーブル化」（任意）
- 「キャッシュによる高速スイッチングのディセーブル化」（任意）
- 「輻輳のしきい値の設定」（任意）
- 「Error Protocol Data Unit の送信」（任意）
- 「Redirect Protocol Data Unit の制御」（任意）
- 「ローカル ソース パケットのパラメータの設定」（任意）

各種のパフォーマンス パラメータの設定例については、この章の最後にある「パフォーマンス パラメータの例」の項を参照してください。

MTU サイズの指定

すべてのインターフェイスには、デフォルトの最大パケット サイズがあります。ただし、フラグメンテーションを減らすために、インターフェイスで送信されるパケットの MTU サイズを設定することができます。最小値は 512 です。パケットのデフォルト サイズおよび最大サイズは、インターフェイス タイプによって異なります。

mtu インターフェイス コンフィギュレーション コマンドで MTU 値を変更すると、CLNS MTU 値に影響する場合があります。CLNS MTU がインターフェイス MTU の最大値に達した場合、CLNS MTU はインターフェイス MTU と共に変化します。ただし、この逆は真ではありません。つまり、CLNS MTU 値を変更しても、**mtu** インターフェイス コンフィギュレーション コマンドの値には影響しません。

指定したインターフェイスの CLNS MTU パケット サイズを設定するには、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。

コマンド	目的
*bytes*Router(config-if)# **clns mtu**	インターフェイスで送信されるパケットの MTU サイズを設定します。

（注） CTR カードは、4472 バイトを超えるフレームのスイッチングをサポートしていません。CTR カードと他のトークン リング カードが同じネットワークで同時に使用されている場合、相互運用性に関する問題が発生することがあります。こうした問題が発生する可能性を最小限に抑えるには、CLNS MTU サイズを小さくして、ネットワーク上のすべてのルータで同じになるようにします。

チェックサムのディセーブル化

ISO CLNS ルーティング ソフトウェアから CLNS パケットを送信する場合、デフォルトでチェックサムが生成されます。この機能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。

コマンド	目的
Router(config-if)# **no clns checksum**	チェックサムの生成をディセーブルにします。

（注） チェックサムの生成をイネーブルにしても、ルータから送信されるルーティング パケット（ES-IS、ISO IGRP、および IS-IS）には影響しませんが、ping や traceroute パケットには適用されます。

キャッシュによる高速スイッチングのディセーブル化

キャッシュによる高速スイッチングは、サポート対象のすべてのインターフェイスで、デフォルトでイネーブルになっています。高速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。

コマンド	目的
Router(config-if)# **no clns route-cache**	高速スイッチングをディセーブルにします。

（注） **no clns route-cache** インターフェイス コンフィギュレーション コマンドの使用後も、キャッシュは存在し、使用されます。ただし、キャッシュによる高速スイッチングは、ソフトウェアでサポートされなくなります。

輻輳のしきい値の設定

CLNS 用に設定されたルータで輻輳が発生すると、輻輳検出ビットが設定されます。輻輳のしきい値は、インターフェイス単位で設定することができます。このしきい値を設定すると、指定した数を超えるパケットが出力キューに入った場合に、システムによって輻輳検出ビットが設定されます。

輻輳のしきい値を設定するには、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。

コマンド	目的
`Router(config-if)# clns congestion-threshold number`	輻輳のしきい値を設定します。

Error Protocol Data Unit の送信

CLNS パケットを受信したとき、ルーティング ソフトウェアは、ネクスト ホップのルーティング テーブルを調べます。ルーティング テーブルが見つからなかった場合、パケットは破棄され、Error Protocol Data Unit（ERPDU）が送信されます。

ERPDU の送信間隔は設定可能です。ERDPU の最小送信間隔を設定すると、ERDPU で使用される帯域幅の量を減らすことができます。ERPDU の最小送信間隔を設定するには、指定されたインターフェイスで **clns erpdu-interval** コマンドを設定します。ERPDU の最小送信間隔は、*milliseconds* 引数を使用して設定します。Cisco IOS ソフトウェアは、指定されたインターフェイスで、「x」ミリ秒に 1 回を超える頻度で ERPDU を送信することはありません（「x」は、*milliseconds* 引数に入力した値）。

ERPDU を送信し、ERPDU の最小送信間隔を設定するには、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。

	コマンド	目的
ステップ 1	`Router(config-if)# clns send-erpdu`	ルーティング ソフトウェアがデータ PDU 内のエラーを検出したときに、ERPDU を送信します。この機能は、デフォルトでイネーブルになっています。
ステップ 2	`Router(config-if)# clns erpdu-interval milliseconds`	ERPDU の最小送信間隔（ミリ秒単位）を設定します。

Redirect Protocol Data Unit の制御

パケットが着信したのと同じインターフェイスから送信される場合、Redirect Protocol Data Unit（RDPDU）をパケットの送信者に送信することもできます。RDPDU は、次の方法で制御することができます。

- デフォルトでは、特定のホストのより適切なルートがわかった場合に、CLNS によって RDPDU が送信されます。この機能はディセーブルにすることができます。この機能をディセーブルにすると、パケットが不必要にルータを経由し続ける可能性があるため、帯域幅が小さくなります。
- RDPDU の送信間隔は設定可能です。

（注） SNPA マスクが送信されることはありません。ルータが IS として機能している場合、Cisco IOS ソフトウェアは RDPDU を無視します。

RDPDU 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のいずれかを使用します。

コマンド	目的
`Router(config-if)# clns send-rdpdu`	特定のホストのより適切なルートがわかった場合に、RPDU を送信します。
`Router(config-if)# clns rdpdu-interval` *milliseconds*	RDPDU の最小送信間隔（ミリ秒単位）を設定します。

ローカル ソース パケットのパラメータの設定

指定したルータから送信されるパケットのパラメータを設定するには、グローバル コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的
`Router(config)# clns packet-lifetime` *seconds*	ローカルで生成されたパケットの初期ライフタイムを秒単位で指定します。
`Router(config)# clns want-erpdu`	ルータから送信されたパケットに対して ERPDU を要求するかどうかを指定します。

ループが頻繁に発生するインターネットワークでは、パケットのライフタイムを短く設定する必要があります。

（注） **clns want-erpdu** グローバル コンフィギュレーション コマンドは、ルータから送信されるルーティング パケット（ES-IS、ISO IGRP、および IS-IS）には影響しませんが、ping や traceroute パケットには適用されます。

ISO CLNS ネットワークのモニタおよびメンテナンス

ISO CLNS のキャッシュ、テーブル、およびデータベースのモニタおよびメンテナンスを行うには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> clear clns cache`	CLNS ルーティング キャッシュをクリアおよび再初期化します。
`Router> clear clns es-neighbors`	隣接データベースから ES ネイバー情報を削除します。
`Router> clear clns is-neighbors`	隣接データベースから IS ネイバー情報を削除します。
`Router> clear clns neighbors`	隣接データベースから CLNS ネイバー情報を削除します。
`Router> clear clns route`	動的に派生した CLNS ルーティング情報を削除します。
`Router> ping clns` {*host* | *address*}	接続をテストするための診断ツールを呼び出します。
`Router> show clns`	CLNS ネットワークに関する情報を表示します。

コマンド	目的
Router> **show clns cache**	CLNS ルーティング キャッシュ内のエントリを表示します。
Router> **show clns** [*area-tag*] **es-neighbors** [*type number*] [**detail**]	ES ネイバー エントリ（関連のあるエリアなど）を表示します。
Router> **show clns filter-expr** [*name*] [**detail**]	フィルタ式を表示します。
Router> **show clns filter-set** [*name*]	フィルタ セットを表示します。
Router> **show clns interface** [*type number*]	各インターフェイスの CLNS 固有の情報または ES-IS 情報を表示します。
Router> **show clns** [*area-tag*] **is-neighbors** [*type number*] [**detail**]	IS ネイバー エントリを、配置されているエリアに応じて表示します。
Router> **show clns** [*area-tag*] **neighbors** [*type number*] [**detail**]	ES ネイバーと IS ネイバーの両方を表示します。
Router> **show clns** [*area-tag*] **neighbor areas**	IS-IS ネイバーおよび IS-IS ネイバーが属しているエリアに関する情報を表示します。
Router> **show clns** [*area-tag*] **protocol** [*domain* | *area-tag*]	このルータ内の各 IS-IS または ISO IGRP ルーティング プロセスに対するプロトコル固有の情報を表示します。
Router> **show clns route** [*nsap*]	このルータが CLNS パケットをルーティングする方法を把握している宛先をすべて表示します。
Router> **show clns** [*area-tag*] **traffic**	このルータで確認された CLNS パケットに関する情報を表示します。
Router> **show isis** [*area-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [*lspid*]	IS-IS リンクステート データベースを表示します。
Router> **show isis** [*area-tag*] **route**	IS-IS レベル 1 ルーティング テーブルを表示します。
Router> **show isis** [*area-tag*] **spf-log**	IS-IS の Shortest Path First（SPF）計算の履歴を表示します。
Router> **show isis** [*area-tag*] **topology**	すべてのエリアで接続済みルータのリストを表示します。
Router> **show route-map** [*map-name*]	設定されているすべてのルート マップ、または指定された 1 つのルート マップを表示します。
Router> **trace clns** *destination*	パケットがたどった、指定された宛先までのパスをネットワーク内で検出します。
Router> **which-route** {*nsap-address* | *clns-name*}	指定された CLNS の宛先が見つかったルーティング テーブルを表示します。

ISO CLNS での TARP の設定

SONET デバイスで実行される一部のアプリケーション（通常、電話会社で使用される）は、ターゲット ID（TID）でこれらのデバイスを識別します。そのため、ルータで、TID-to-network アドレス マッピングをキャッシュする必要があります。通常、これらのアプリケーションは OSI を介して実行されるため、マッピング関連のネットワーク アドレスは OSI NSAP になります。

あるデバイスが別の不明なデバイス（つまり、リモート デバイスの TID に対応する NSAP アドレスの情報がないデバイス）にパケットを送信しなければならない場合は、その情報をデバイスから直接（またはネットワーク内の中間デバイスから）要求するための方法が必要になります。この機能は、TID Address Resolution Protocol（TARP）と呼ばれるアドレス解決プロトコルで提供されます。

情報の要求および関連する応答は TARP PDU として送信され、TARP PDU は Connectionless Network Protocol（CLNP; コネクションレス型ネットワーク プロトコル）のデータ パケットして送信されます。TARP PDU は、NSAP アドレスの一意の N セレクタによって区別されます。TARP PDU の 5 つのタイプを次に示します。

- タイプ 1：デバイスの TID に一致する NSAP が含まれていない場合に送信されます。タイプ 1 PDU は、すべてのレベル 1（IS-IS および ES-IS）のネイバーに送信されます。指定した制限時間内に応答が受信されなかった場合、タイプ 2 PDU が送信されます。パケットのループを防止するためには、ルータでループ検出バッファを維持します。タイプ 1 PDU は、**tarp resolve** コマンドを使用している場合に送信されます。
- タイプ 2：デバイスの TID に一致する NSAP が含まれておらず、タイプ 1 PDU からの応答が受信されなかった場合に送信されます。タイプ 2 PDU は、すべてのレベル 1 およびレベル 2 のネイバーに送信されます。タイプ 2 PDU に対する制限時間を指定することもできます。タイプ 2 PDU は、**tarp resolve** コマンドを使用し、オプション 2 を指定している場合に送信されます。
- タイプ 3：タイプ 1、タイプ 2、またはタイプ 5 の PDU に対する応答として送信されます。タイプ 3 PDU は、要求の送信元に対して直接送信されます。
- タイプ 4：ローカルで変更（TID または NSAP に関する変更など）が行われた場合に、通知として送信されます。タイプ 4 PDU の多くは、デバイスの電源が投入されたときや、デバイスがオンラインにされたときに送信されます。
- タイプ 5：特定の NSAP に対応する TID がデバイスで必要な場合に送信されます。すべてのレベル 1 およびレベル 2 のネイバーに送信されるタイプ 1 およびタイプ 2 の PDU とは異なり、タイプ 5 PDU は、特定のルータにのみ送信されます。TARP PDU には、タイプの他に、送信側の NSAP、送信側の TID、およびターゲット TID が含まれます（PDU がタイプ 1 またはタイプ 2 の場合）。タイプ 5 PDU は、**tarp query** コマンドを使用している場合に送信されます。

TARP は、レベル 1 エリアを 1 つ、およびレベル 2 エリアを 1 つ含む従来の IS-IS 設定（または、レベル 1 エリアを 1 つ、*または*レベル 2 エリアを 1 つ含む設定）に対して使用できます。

複数のレベル 1 エリアが定義されている場合、ルータは TARP を使用してアドレスを解決します。その方法を次に示します。

1. ルータは、ローカルに割り当てられたターゲット ID を使用して、レベル 2 エリアの NSAP を取得します（存在する場合）。
2. レベル 1 エリアだけが設定されている場合、ルータは、TARP 設定（「tarp run」）時に設定に表示されているように、最初のアクティブ レベル 1 エリアの NSAP を使用します（レベル 1 エリアはタグ名のアルファベット順でソートされ、大文字が小文字よりも前になります。たとえば、AREA-1 は AREA-2 よりも前で、area-1 は AREA-2 の後ろになります）。TARP 動作後に新規レベル 1 エリアが設定に追加される場合、TID NSAP はリロード後に変更できることに注意してください。
3. ルータは、このルータのすべてのタイプ 1 およびタイプ 2 PDU の処理を継続します。ターゲット ID がローカル TID キャッシュにある場合、タイプ 1 PDU はローカルに処理されます。処理されない場合、*同じ*レベル 1 エリア内の全インターフェイスに「伝播」（ルーティング）されます（同一エリアは、入力インターフェイス上に設定されたエリアとして定義されます）。
4. 指定したターゲット ID がローカル TID キャッシュにある場合、タイプ 2 PDU はローカルに処理されます。そうでない場合、TARP がイネーブルであるすべてのインターフェイス（すべてのレベル 1 またはレベル 2 エリア）を経由して伝播されます。PDU の送信元が別のエリアの場合、情報もローカル TID キャッシュに追加されます。タイプ 2 PDU は、すべてのスタティック隣接を経由して伝播されます。
5. （ローカルで実行された変更の）タイプ 4 PDU がすべてのレベル 1 およびレベル 2 エリアに伝播します（内部的に「レベル 1-2」として扱われるため）。
6. タイプ 3 および 5 PDU が引き続きルーティングされます。
7. スタティック NSAP がこのルータにあるレベル 1 エリアの 1 つである場合、タイプ 1 PDU はレベル 1 スタティック隣接を介してだけ「伝播」（ルーティング）されます。

TARP 設定作業リスト

ルータで TARP を設定するには、次の作業を実行します。最初の作業のみが必須で、他の作業はすべて任意です。

- 「TARP のイネーブル化および TARP TID の設定」（必須）
- 「TARP キャッシングのディセーブル化」（任意）
- 「TARP PDU の発信および伝播のディセーブル化」（任意）
- 「複数の NSAP アドレスの設定」（任意）
- 「スタティック TARP 隣接および隣接ブラックリストの設定」（任意）
- 「TID および NSAP の決定」（任意）
- 「TARP タイマーの設定」（任意）
- 「TARP PDU に関するその他の情報の設定」（任意）
- 「TARP プロトコルのモニタおよびメンテナンス」（任意）
- 「トンネル タイプの決定」（P.46）（任意）
- 「IPv4 および IPv6 パケットを伝送するための GRE/CLNS CTunnel の設定」（P.47）（任意）
- 「トンネルの設定と動作の確認」（P.50）（任意）

TARP の設定例については、この章の最後にある「TARP の設定例」の項を参照してください。

TARP のイネーブル化および TARP TID の設定

TARP 機能を使用できるようにするには、TARP を明示的にイネーブルにして、ルータに TID を割り当てる必要があります。また、TARP パケットをインターフェイスに送出するには、各インターフェイスで TARP をイネーブルにして、そのインターフェイスで TARP PDU を伝播できるようにする必要があります。

ルータは、CLNS 機能を使用して、TARP PDU を送受信するようになります。IS として設定されているルータは、IS-IS を実行する必要があります。ES として設定されているルータは、ES-IS を実行する必要があります。

TARP 機能を有効にするには、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。

コマンド	目的
`Router(config)# tarp run`	TARP 機能を有効にします。
`Router(config)# tarp tid tid`	TID をルータに割り当てます。

1 つ以上のインターフェイスで TARP 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。

コマンド	目的
`Router(config-if)# tarp enable`	インターフェイスで TARP をイネーブルにします。

TARP キャッシングのディセーブル化

デフォルトでは、TID-to-NSAP アドレス マッピングは、TID キャッシュに格納されます。この機能をディセーブルにすると、TID キャッシュがクリアされます。この機能を再度イネーブルにすると、以前にクリアしたすべてのローカル エントリと、すべてのスタティック エントリが復元されます。

TID キャッシュ内の TID-to-NSAP アドレス マッピング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。

コマンド	目的
`Router(config)# no tarp allow-caching`	TARP TID-to-NSAP アドレス マッピングをディセーブルにします。

TARP PDU の発信および伝播のディセーブル化

デフォルトでは、TARP PDU の発信はルータが行い、TARP PDU のネイバーへの伝播はルータおよびインターフェイスが行います。これらの機能をディセーブルにすると、ルータは TARP PDU を発信しなくなります。また、ルータおよび特定のインターフェイスは、他のルータから受信した TARP PDU を伝播しなくなります。

TARP PDU の発信および伝播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。

コマンド	目的
`Router(config)# no tarp originate`	TARP PDU の発信をディセーブルにします。
`Router(config)# no tarp global-propagate`	TARP PDU のグローバルな伝播をディセーブルにします。

特定のインターフェイスでの TARP PDU の伝播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。

コマンド	目的
`Router(config-if)# no tarp propagate [all | message-type {unknowns | type-number} [type-number] [type-number]]`	インターフェイスでの TARP PDU の伝播をディセーブルにします。

複数の NSAP アドレスの設定

ルータには、複数の NSAP アドレスを設定できます。NSAP の要求が送信されると（タイプ 1 またはタイプ 2 の PDU）、最初の NSAP アドレスが返されます。ルータに関連付けられているすべての NSAP アドレスを受信するには、各 NSAP アドレスの TID キャッシュに TID-to-NSAP スタティック ルートを入力します。

TID-to-NSAP スタティック ルートを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tarp map tid nsap`	TID-to-NSAP スタティック ルートを入力します。

スタティック TARP 隣接および隣接ブラックリストの設定

TARP ルータは、そのすべての IS-IS/ES-IS 隣接の他に、そのすべてのスタティック TARP 隣接に PDU を伝播します。TARP を実行していないルータは、そのすべての隣接に PDU を伝播する代わりに、TARP PDU を破棄します。TARP は、TARP が実行されていない可能性があるルート上のルータをバイパスできるようにするためのスタティック TARP 隣接機能を備えています。スタティック隣接は、特別なキューに格納されます。

スタティック TARP 隣接を作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **tarp route-static** *nsap* [**all** | **message-type** {**unknowns** | *type-number*} [*type-number*] [*type-number*]]	スタティック TARP 隣接を入力します。

TARP は、TARP が実行されていない可能性がある IS-IS/ES-IS 隣接への PDU の伝播を停止するための隣接ブラックリスト機能を備えています。ルータは、ブラックリストに登録されているルータに TARP PDU を伝播しないようになります。

ルータをブラックリストに登録するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# **tarp blacklist-adjacency** *nsap*	TARP を実行していないルータをバイパスします。

TID および NSAP の決定

TID の NSAP アドレスまたは NSAP アドレスの TID を決定するには、次のコマンドを EXEC モードで使用します。

コマンド	目的
Router> **tarp query** *nsap*	特定の NSAP に関連付けられている TID を取得します。
Router> **tarp resolve** *tid* [**1** | **2**]	特定の TID に関連付けられている NSAP を取得します。

TID を決定する際に、ルータはまずローカル TID キャッシュをチェックします。ローカル TID キャッシュ内に TID エントリが存在する場合、要求された情報が表示されます。ローカル TID キャッシュ内に TID エントリが存在しない場合、指定された NSAP アドレスに TARP タイプ 5 PDU が送信されます。

NSAP アドレスを決定する際に、ルータはまずローカル TID キャッシュをチェックします。ローカル TID キャッシュ内に NSAP エントリが存在する場合、要求された情報が表示されます。ローカル TID キャッシュ内に NSAP エントリが存在しない場合、TARP タイプ 1 またはタイプ 2 の PDU が送信されます。デフォルトでは、タイプ 1 PDU が、すべてのレベル 1（IS-IS および ES-IS）のネイバーに送信されます。応答が受信された場合、要求された情報が表示されます。応答時間内に応答が受信されなかった場合、タイプ 2 PDU が、すべてのレベル 1 およびレベル 2 のネイバーに送信されます。**tarp resolve** *tid* **2** EXEC コマンドを指定すると、タイプ 2 PDU のみが送信されます。

ルータが応答を待機する時間は（タイプ 3 PDU の形式で）設定することができます。

TARP タイマーの設定

TARP タイマーにはデフォルト値が指定されており、通常は変更する必要がありません。

タイプ 1 PDU、タイプ 2 PDU、およびタイプ 5 PDU からの応答の受信をルータが待機する時間は設定することができます。また、ホップ数に基づいて、PDU のライフタイムを設定することもできます。

さらに、動的に作成された TARP エントリが TID キャッシュ内に留まる期間、およびシステム ID とシーケンス番号のマッピング エントリがループ検出バッファ テーブル内に留まる期間を制御するタイマーを設定することもできます。ループ検出バッファ テーブルを使用すると、TARP PDU のループを防止することができます。

TARP PDU タイマーの設定、PDU のライフタイムの制御、およびエントリがキャッシュ内に留まる期間の設定を行うには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tarp t1-response-timer seconds`	ルータが TARP タイプ 1 PDU からの応答を待機する秒数を設定します。
`Router(config)# tarp t2-response-timer seconds`	ルータが TARP タイプ 2 PDU からの応答を待機する秒数を設定します。
`Router(config)# tarp post-t2-response-timer seconds`	デフォルト タイマーの期限が切れた後、ルータが TARP タイプ 2 PDU からの応答を待機する秒数を設定します。
`Router(config)# tarp arp-request-timer seconds`	ルータが TARP タイプ 5 PDU からの応答を待機する秒数を設定します。
`Router(config)# tarp lifetime hops`	TARP PDU が破棄されるまでに経由できるルータの数を設定します。
`Router(config)# tarp cache-timer seconds`	動的に作成された TARP エントリが TID キャッシュ内に留まる秒数を設定します。
`Router(config)# tarp ldb-timer seconds`	システム ID とシーケンス番号のマッピング エントリがループ検出バッファ テーブル内に留まる秒数を設定します。

TARP PDU に関するその他の情報の設定

通常、TARP PDU に関するデフォルト値を変更する必要はありません。

ただし、TARP PDU のシーケンス番号の設定、リモート ルータでキャッシュを更新するかどうかを制御するために使用されるリモート キャッシュの更新ビットの設定、TARP PDU を識別するために PDU で使用される N セレクタの指定、発信 PDU で使用されるネットワーク プロトコル タイプの指定を行うことができます。

PDU に関するその他の情報を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tarp sequence-number number`	次の発信 TARP PDU のシーケンス番号を変更します。
`Router(config)# tarp urc [0 | 1]`	すべての後続の発信 TARP PDU で、リモート キャッシュの更新ビットを設定します。このビットによって、リモート ルータでキャッシュの更新が行われるかどうかが決まります。

コマンド	目的
Router(config)# **tarp nselector-type** *hex-digit*	TARP PDU の識別に使用される N セレクタを指定します。
Router(config)# **tarp protocol-type** *hex-digit*	発信 TARP PDU で使用されるプロトコル タイプを指定します。16 進値 0xFE（CLNP を表す）しか指定できません。[1]

1. CLNP = Connectionless Network Protocol（コネクションレス型ネットワーク プロトコル）

TARP プロトコルのモニタおよびメンテナンス

TARP のキャッシュ、テーブル、およびデータベースのモニタおよびメンテナンスを行うには、次のコマンドを EXEC モードで使用します。

コマンド	目的
Router> **clear tarp counters**	**show tarp traffic** コマンドで表示される TARP カウンタをリセットします。
Router> **clear tarp ldb-table**	TARP ループ検出バッファ テーブル内にあるシステム ID とシーケンス番号のマッピング エントリをすべて削除します。
Router> **clear tarp tid-table**	TID キャッシュ内にある動的に作成された TARP TID-to-NSAP アドレス マッピングのエントリをすべて削除します。
Router> **show tarp**	グローバル TARP パラメータをすべて表示します。
Router> **show tarp blacklisted-adjacencies**	ブラックリストに登録されている隣接（伝播された TARP PDU を受信しない隣接）をすべてリストします。
Router> **show tarp host tid**	ローカル TID キャッシュに格納されている特定の TARP ルータに関する情報を表示します。
Router> **show tarp interface** [**type number**]	TARP がイネーブルになっているルータのインターフェイスをすべてリストします。
Router> **show tarp ldb**	ループ検出バッファ テーブルの内容を表示します。
Router> **show tarp map**	TID キャッシュ内のスタティック エントリをすべてリストします。
Router> **show tarp static-adjacencies**	スタティック TARP 隣接をすべてリストします。
Router> **show tarp tid-cache**	TID キャッシュ内のエントリに関する情報を表示します。
Router> **show tarp traffic**	TARP PDU に関する統計情報を表示します。

IP over ISO CLNS ネットワークのルーティング

IP over CLNS トンネル機能を使用すると、SONET リングの Data Communications Channel（DCC; データ通信チャネル）などで、Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）を介して IP トラフィックを転送することができます。

IP over CLNS トンネルは、CLNS ネットワークとの相互作用を強化する仮想インターフェイスです。IP over CLNS トンネルでは、Connectionless Network Protocol（CLNP; コネクションレス型ネットワーク プロトコル）を使用して IP パケットをトンネリングすることにより、TCP/IP サービスを維持することができます。

IP over CLNS トンネル（CTunnel）を設定すると、CLNS 接続しかないリモート ルータと Telnet 接続することができます。また、CTunnel を設定しないと CLNS ネットワークで使用できない、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、TFTP などのその他の管理機能を使用することもできます。

機能に関連付けられているハードウェア プラットフォームやソフトウェア イメージに関する情報を識別するには、Cisco.com の Feature Navigator を使用して、その機能に関する情報を検索するか、特定のリリースのソフトウェア リリース ノートを参照します。

IP over CLNS トンネルの設定

IP over CLNS トンネル（CTunnel）を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# interface ctunnel` *interface-number*	CLNS トンネルを介して IP を転送する仮想インターフェイスを作成し、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。インターフェイス番号は、各 CTunnel インターフェイスで一意である必要があります。
ステップ 2	`Router(config-if)# ctunnel destination` *remote-nsap-address*	CTunnel の宛先パラメータを設定します。IP パケットが抽出される、CTunnel の宛先 Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスを指定します。
ステップ 3	`Router(config-if)# ip address` *ip-address mask*	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

（注） 1 組のルータ間に CTunnel を設定するには、各ルータで上記のコマンドを入力する必要があります。ルータ A の宛先 NSAP アドレスは、ルータ B の NSAP アドレスとなり、ルータ B の宛先 NSAP アドレスは、ルータ A の NSAP アドレスとなります。トンネルのいずれかの端にある仮想インターフェイスで使用される IP アドレスは、同じ IP サブネットにあることが理想的です。

設定の確認

IP over CLNS トンネル機能が正しく設定されていることを確認するには、次の手順を実行します。

ステップ 1 ルータ A で、ルータ B の CTunnel インターフェイスの IP アドレスに対して ping を実行します。

ステップ 2 ルータ B で、ルータ A の CTunnel インターフェイスの IP アドレスに対して ping を実行します。

トラブルシューティングのヒント

CTunnel が機能しない場合、「設定の確認」の項の説明に従って、両方のルータが正しく設定されていることを確認します。

IP over CLNS トンネルのモニタおよびメンテナンス

IP over CLNS トンネルのステータスを表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# show interfaces ctunnel interface-number`	IP over CLNS トンネルに関する情報を表示します。

トンネル タイプの決定

トンネルを設定する前に、作成する必要があるトンネルのタイプを決定する必要があります。

手順の概要

1. パッセンジャ プロトコルを決定します。
2. トンネルの CLI タイプを決定します。
3. 必要に応じて **tunnel mode** コマンドのキーワードを決定します。

手順の詳細

ステップ 1 パッセンジャ プロトコルを決定します。

パッセンジャ プロトコルはカプセル化の対象となるプロトコルです。

ステップ 2 トンネルの CLI タイプを決定します。

表 3 に、トンネルで使用するトランスポート プロトコルに必要なトンネルの Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドを決定する方法を示します。

表 3　トランスポート プロトコルごとのトンネル CLI の決定

トランスポート プロトコル	トンネルの CLI コマンド
CLNS	**ctunnel**（任意の **mode gre** キーワードを使用）
その他	**tunnel mode**（適切なキーワードを使用）

ステップ 3 必要に応じて **tunnel mode** コマンドのキーワードを決定します。

表 4 に、**tunnel mode** コマンドで使用する適切なキーワードを決定する方法を示します。このモジュールの以降に示す作業では、**tunnel mode** コマンドに関連するキーワードのみを示します。

表 4　tunnel mode コマンド キーワードの決定

キーワード	目的
dvmrp	ディスタンス ベクトル マルチキャスト ルーティング プロトコルによるカプセル化の使用を指定するには、**dvmrp** キーワードを使用します。
gre ip	IP での GRE カプセル化の使用を指定するには、**gre ip** キーワードを使用します。

表 4　tunnel mode コマンド キーワードの決定 （続き）

キーワード	目的
gre ipv6	IPv6 での GRE カプセル化の使用を指定するには、**gre ipv6** キーワードを使用します。
gre multipoint	Multipoint GRE（mGRE; マルチポイント GRE）カプセル化の使用を指定するには、**gre multipoint** キーワードを使用します。
ipip [**decapsulate-any**]	IP-in-IP カプセル化の使用を指定するには、**ipip** キーワードを使用します。任意の **decapsulate-any** キーワードは、1 つのトンネル インターフェイスで任意の数の IP-in-IP トンネルを終了させます。このトンネルは発信トラフィックを伝送しませんが、任意の数のリモート トンネル エンドポイントでは、このように設定されたトンネルを宛先として使用することができます。
ipv6	IPv6 での汎用パケット トンネリングの使用を指定するには、**ipv6** キーワードを使用します。
ipv6ip	IPv6 をパッセンジャ プロトコルとして使用し、IPv4 をキャリア（カプセル化）プロトコルおよびトランスポート プロトコルとして使用することを指定するには、**ipv6ip** キーワードを使用します。追加のキーワードを使用しない場合は、手動の IPv6 トンネルが設定されます。追加のキーワードを使用すると、IPv4-compatible、6to4、または ISATAP トンネルを指定することができます。
mpls	Traffic Engineering（TE; トラフィック エンジニアリング）トンネルの設定に MPLS を使用するように指定するには、**mpls** キーワードを使用します。
rbscp	RBSCP トンネルの使用を指定するには、**rbscp** キーワードを使用します。

IPv4 および IPv6 パケットを伝送するための GRE/CLNS CTunnel の設定

GRE モードで CTunnel を設定して IPv4 および IPv6 パケットを CLNS ネットワークで転送するには、この作業を実行します。

単一のルータ ペア間で CTunnel を設定するには、IP アドレスを使用してトンネル インターフェイスを設定し、トンネルの宛先を定義する必要があります。ルータ A の宛先 Network Services Access Point（NSAP; ネットワーク サービス アクセス ポイント）のアドレスは、ルータ B の NSAP アドレスとなり、ルータ B の宛先 NSAP アドレスは、ルータ A の NSAP アドレスとなります。トンネルのいずれかの端にある仮想インターフェイスで使用される IP アドレスは、同じ IP サブネットにあることが理想的です。必ずトンネルの両側にルータを設定するようにしてください。

CLNS ネットワークを経由する IPv4 および IPv6 パケット用トンネル

CTunnel インターフェイスで **ctunnel mode gre** コマンドを設定すると、IPv4 および IPv6 パケットを、RFC 3147 に従って CLNS 経由でトンネリングすることが可能になります。この RFC に準拠することで、同じ標準が採用されているシスコ機器と他のベンダー機器間の相互運用が可能になります。

RFC 3147 では、パケットのトンネリングに GRE の使用を指定しています。この機能の実装には、ヘッダー フィールドで定義されている GRE サービス（チェックサム、キー、またはシーケンスの指定に使用されるサービスなど）のサポートは含まれていません。これらの機能の使用を指定している受信パケットは、すべてドロップされます。

デフォルトの CTunnel モードは、IPv4 パケットだけをトンネリングする標準のシスコ カプセル化をそのまま使用します。IPv6 パケットのトンネリングを行う場合は、GRE カプセル化モードを使用する必要があります。いずれの方法でも正常に動作するためには、トンネルの両端を同じモードで設定する必要があります。

前提条件

- IPv4 または IPv6 アドレスを CTunnel インターフェイスで設定することが必要であり、CTunnel の宛先には、手動設定された CLNS アドレスを割り当てることが必要です。
- 設定された CTunnel の両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートする必要があります。
- CTunnel の送信元と宛先は、同じモードで実行されるように設定する必要があります。

制約事項

GRE サービス（チェックサム、キー、またはシーケンスの指定に使用されるサービスなど）はサポートされていません。これら機能の使用を要求するパケットはすべてドロップされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface ctunnel** *interface-number*
4. **ip address** *ip-address mask*

   または

   ipv6 address *ipv6-prefix*/*prefix-length* [**eui-64**]
5. **ctunnel destination** *remote-nsap-address*
6. **ctunnel mode gre**
7. **end**
8. **show interfaces ctunnel** *interface-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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 ctunnel** *interface-number* **例：** `Router(config)# interface ctunnel 102`	CLNS トンネルを介して IP を転送する仮想インターフェイスを作成し、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。 **（注）** インターフェイス番号は、各 CTunnel インターフェイスで一意である必要があります。
ステップ 4	**ip address** *ip-address mask* または **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 2001:0DB8:1234:5678::3/126`	インターフェイスに割り当てられている IPv4 または IPv6 ネットワークを指定して、インターフェイス上で IPv4 または IPv6 パケット処理をイネーブルにします。 **（注）** IPv6 アドレスの設定の詳細については、「Implementing Basic Connectivity for IPv6」モジュールを参照してください。
ステップ 5	**ctunnel destination** *remote-nsap-address* **例：** `Router(config-if)# ctunnel destination 192.168.30.1`	パケットが抽出される CTunnel の宛先 NSAP アドレスを指定します。 • CTunnel のエンドポイントの NSAP アドレスを指定するには、*remote-nsap-address* 引数を使用します。
ステップ 6	**ctunnel mode gre** **例：** `Router(config-if)# ctunnel mode gre`	IPv4 トラフィックと IPv6 トラフィックの両方において、CTunnel が GRE モードで実行されるように指定します。 **（注）** **ctunnel mode gre** コマンドは、GRE をトンネルのカプセル化プロトコルとして指定します。
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。
ステップ 8	**show interfaces ctunnel** *interface-number* **例：** `Router# show interfaces ctunnel 102`	（任意）IP over CLNS トンネルに関する情報を表示します。 • *interface-number* 引数を使用して、CTunnel インターフェイスを指定します。 • このコマンドを使用して、CTunnel の設定を確認します。

トンネルの設定と動作の確認

この任意の作業では、トンネルの設定と動作の確認方法を説明します。この作業手順に含まれるコマンドは、任意の順序で使用することができ、繰り返し実行する必要がある場合があります。次のコマンドは、GRE トンネル、IPv6 手動設定トンネル、および IPv6 over IPv4 GRE トンネルに使用できます。プロセスは、次に示す一般的な手順で構成されています（詳しい手順はその後に説明します）。

ステップ 1 ルータ A で、ルータ B の CTunnel インターフェイスの IP アドレスに対して ping を実行します。

ステップ 2 ルータ B で、ルータ A の CTunnel インターフェイスの IP アドレスに対して ping を実行します。

手順の概要

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]
3. **ping** [*protocol*] *destination*
4. **show ip route** [*address* [*mask*]]
5. **ping** [*protocol*] *destination*

手順の詳細

ステップ 1 **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。

```
Router> enable
```

ステップ 2 **show interfaces tunnel** *number* [**accounting**]

IPv6 手動設定トンネルと IPv6 over IPv4 GRE トンネルの両方に適した汎用例として、2 つのルータがトンネルのエンドポイントとして設定されていることを想定します。ルータ A では、IPv4 アドレスが 10.0.0.1、IPv6 プレフィクスが 2001:0DB8:1111:2222::1/64 のトンネル インターフェイス 0 に対する送信元として、イーサネット インターフェイス 0/0 が設定されています。ルータ B では、IPv4 アドレスが 10.0.0.2、IPv6 プレフィクスが 2001:0DB8:1111:2222::2/64 のトンネル インターフェイス 1 に対する送信元として、イーサネット インターフェイス 0/0 が設定されています。

トンネルの送信元と宛先アドレスが設定されていることを確認するには、ルータ A で **show interfaces tunnel** コマンドを使用します。

```
RouterA# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (Ethernet0/0), destination 10.0.0.2, fastswitch TTL 255
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input 00:00:14, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 352 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 704 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ステップ 3 **ping** [*protocol*] *destination*

ローカル エンドポイントが設定され、動作していることを確認するには、ルータ A で **ping** コマンドを使用します。

```
RouterA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

ステップ 4 **show ip route** [*address* [*mask*]]

リモート エンドポイント アドレスに対するルートが存在することを確認するには、**show ip route** コマンドを使用します。

```
RouterA# show ip route 10.0.0.2

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Ethernet0/0
      Route metric is 0, traffic share count is 1
```

ステップ 5 **ping** [*protocol*] *destination*

リモート エンドポイント アドレスが到達可能であることを確認するには、ルータ A で **ping** コマンドを使用します。

（注） フィルタリングが原因で、**ping** コマンドを使用するとリモート エンドポイント アドレスが到達可能ではないのに、トンネル トラフィックは宛先に到達できる場合があります。

```
RouterA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms
```

リモート IPv6 トンネル エンドポイントが到達可能であることを確認するには、ルータ A で **ping** コマンドを使用します。この例にも、フィルタリングに関する同じ注釈が当てはまります。

```
RouterA# ping 1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

トンネルのもう一方のエンドポイントでもこの手順を繰り返すことができます。

インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』を参照してください。

ISO CLNS の設定例

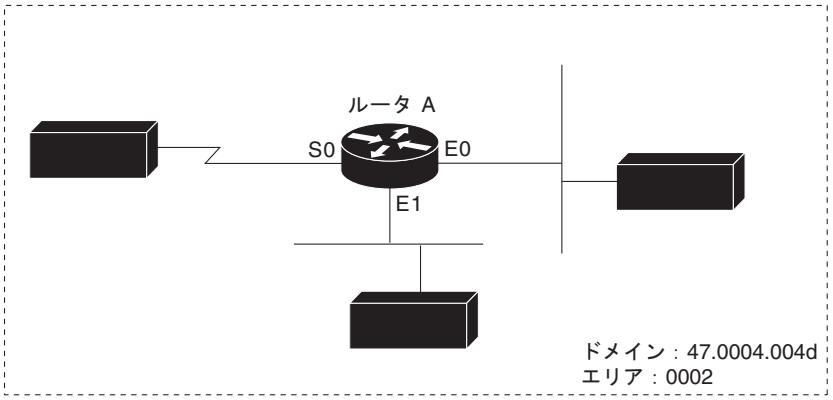
ここでは、スタティック、ISO IGRP、および IS-IS ルーティング技術を使用する、ドメイン内、およびドメイン間のスタティック ルーティングとダイナミック ルーティングの設定例を示します。

- 「同一エリア内でのダイナミック ルーティングの例」
- 「複数エリアでのダイナミック ルーティングの例」
- 「重複するエリアでのダイナミック ルーティング の例」
- 「ダイナミック ドメイン間ルーティングの例」
- 「IS-IS ルーティングの設定例」
- 「NET の設定例」
- 「2 つのエリアにあるルータの例」
- 「基本的なスタティック ルーティングの例」
- 「スタティック ドメイン内ルーティングの例」
- 「スタティック ドメイン間ルーティングの例」
- 「CLNS フィルタの例」
- 「ルート マップの例」
- 「DECnet クラスタ エイリアスの例」
- 「ISO CLNS over X.25 の例」
- 「パフォーマンス パラメータの例」
- 「TARP の設定例」
- 「IP over CLNS トンネルの例」
- 「IPv4 および IPv6 パケットを伝送するための GRE/CLNS CTunnel の設定例」

同一エリア内でのダイナミック ルーティングの例

図 5 および後続の例は、ルーティング ドメイン内にダイナミック ルーティングを設定する方法を示しています。ルータは、ドメイン内の 1 つ以上のエリアに存在することができます。ルータ A という名前のルータは、単一エリアに存在します。

図 5　　単一エリア内での CLNS ダイナミック ルーティング

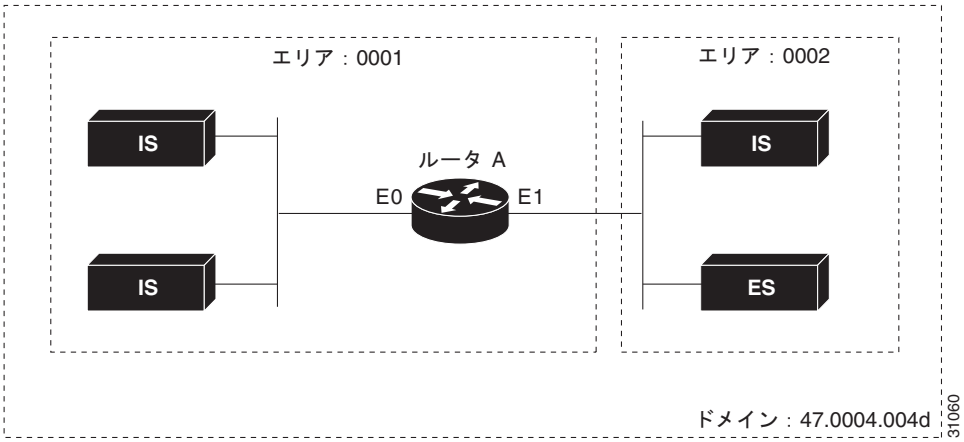



```
! Define a tag castor for the routing process
router iso-igrp castor
! configure the net for the process in area 2, domain 47.0004.004d
 Net 47.0004.004d.0002.0000.0C00.0506.00
! Specify iso-igrp routing using the previously specified tag castor
interface ethernet 0
 clns router iso-igrp castor
 ! Specify iso-igrp routing using the previously specified tag castor
interface ethernet 1
 clns router iso-igrp castor
! Specify iso-igrp routing using the previously specified tag castor
interface serial 0
 clns router iso-igrp castor
```

複数エリアでのダイナミック ルーティングの例

図 6 および後続の例は、2 つのエリアに存在するルータ A という名前のルータを設定する方法を示しています。

図 6　　2 つのエリア内での CLNS ダイナミック ルーティング




```
! Define a tag orion for the routing process
router iso-igrp orion
! Configure the net for the process in area 1, domain 47.0004.004d
 net 47.0004.004d.0001.212223242526.00
! Specify iso-igrp routing using the previously specified tag orion
interface ethernet 0
 clns router iso-igrp orion
! Specify iso-igrp routing using the previously specified tag orion
interface ethernet 1
 clns router iso-igrp orion
```

重複するエリアでのダイナミック ルーティング の例

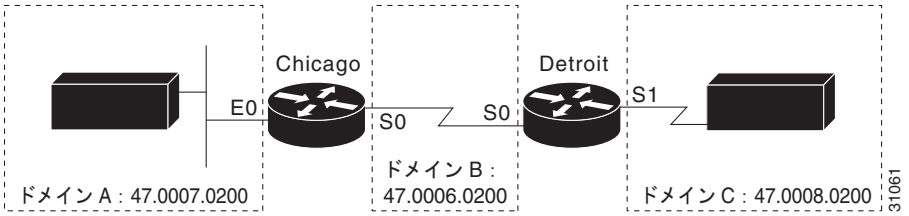
次に、重複するエリアでルータを設定する例を示します。

```
! Define a tag capricorn for the routing process
router iso-igrp capricorn
! Configure the NET for the process in area 3, domain 47.0004.004d
 net 47.0004.004d.0003.0000.0C00.0508.00
! Define a tag cancer for the routing process
router iso-igrp cancer
! Configure the NET for the process in area 4, domain 47.0004.004d
 net 47.0004.004d.0004.0000.0C00.0506.00
! Specify iso-igrp routing on interface ethernet 0 using the tag capricorn
interface ethernet 0
 clns router iso-igrp capricorn
! Specify iso-igrp routing on interface ethernet 1 using the tags capricorn and cancer
interface ethernet 1
 clns router iso-igrp capricorn
 clns router iso-igrp cancer
! Specify iso-igrp routing on interface ethernet 2 using the tag cancer
interface ethernet 2
 clns router iso-igrp cancer
```

ダイナミック ドメイン間ルーティングの例

図 7 および後続の例は、透過的に接続される 3 つのドメインを設定する方法を示しています。

図 7　　CLNS ダイナミック ドメイン間ルーティング



Chicago ルータ

次に、Chicago ルータでダイナミック ドメイン間ルーティングを設定する例を示します。

```
! Define a tag A for the routing process
router iso-igrp A
! Configure the NET for the process in area 2, domain 47.0007.0200
 net 47.0007.0200.0002.0102.0104.0506.00
! Redistribute iso-igrp routing information throughout domain A
redistribute iso-igrp B
! Define a tag B for the routing process
router iso-igrp B
! Configure the NET for the process in area 3, domain 47.0006.0200
 net 47.0006.0200.0003.0102.0104.0506.00
! Redistribute iso-igrp routing information throughout domain B
redistribute iso-igrp A
! Specify iso-igrp routing with the tag A
interface ethernet 0
clns router iso-igrp A
! Specify iso-igrp routing with the tag B
interface serial 0
clns router iso-igrp B
```

Detroit ルータ

次に、Detroit ルータでダイナミック ドメイン間ルーティングを設定する例を示します。この例では、簡略化するためにコメント行を削除しています。

```
router iso-igrp B
 net 47.0006.0200.0004.0102.0104.0506.00
 redistribute iso-igrp C
router iso-igrp C
 net 47.0008.0200.0005.0102.01040.506.00
 redistribute iso-igrp B
interface serial 0
 clns router iso-igrp B
interface serial 1
 clns router iso-igrp C
```

Chicago はドメイン A のプレフィクス ルートをドメイン B に挿入しています。ドメイン B はこのプレフィクス ルートとドメイン B のプレフィクス ルートをドメイン C に挿入しています。

ドメイン A とドメイン C の間にボーダ ルータを設定することもできます。

IS-IS ルーティングの設定例

次に、IS-IS ルーティングの基本構文とコンフィギュレーション コマンド シーケンスを表す例を示します。

レベル 1 とレベル 2 のルーティング

次に、IS-IS プロトコルを使用して、レベル 1 とレベル 2 のルーティングで単一のエリア アドレスを設定する例を示します。

```
! Route dynamically using the is-is protocol
router isis
! Configure the NET for the process in area 47.0004.004d.0001
 net 47.0004.004d.0001.0000.0c00.1111.00
! Enable is-is routing on ethernet 0
interface ethernet 0
 clns router isis
! Enable is-is routing on ethernet 1
interface ethernet 1
 clns router isis
! Enable is-is routing on serial 0
interface serial 0
 clns router isis
```

レベル 2 のルーティングのみ

次の設定例は、レベル 1 とレベル 2 のルーティングを指定した場合に使用される単一のエリア アドレスの設定に似ています。ただし、この場合は、インターフェイスのシリアル インターフェイス 0 はレベル 2 ルーティングのみに設定されています。この例では、簡略化するためにほとんどのコメント行を削除しています。

```
router isis
 net 47.0004.004d.0001.0000.0c00.1111.00
interface ethernet 0
 clns router isis
interface ethernet 1
 clns router isis
interface serial 0
 clns router isis
! Configure a level 2 adjacency only for interface serial 0
 isis circuit-type level-2-only
```

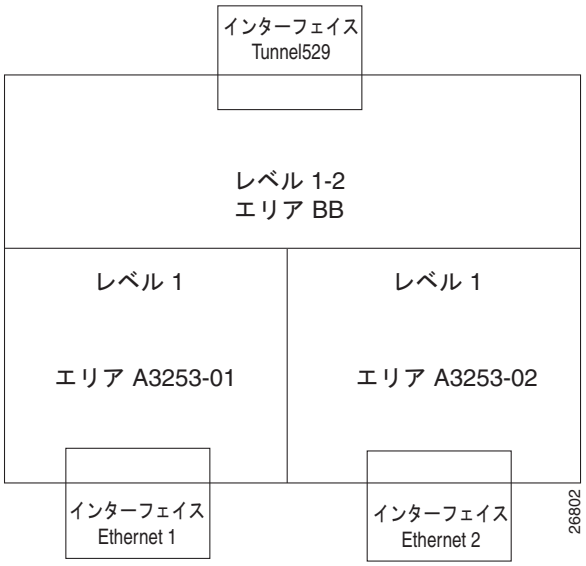
マルチエリア IS-IS 設定

次に、レベル 1 エリアを 2 つ、レベル 1-2 エリアを 1 つ持つマルチエリア IS-IS 設定の例を示します。図 8 に、この設定を示します。

```
clns routing

...

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
```

```
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

...

router isis BB                          ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

図 8　　レベル 1 エリアを 3 つ、レベル 2 エリアを 1 つ持つマルチエリア IS-IS 設定



OSI の設定

次に、OSI の設定例を示します。この例では、IS-IS は 2 つのエリア アドレス、調整されたメトリック、および各インターフェイスに指定された別々の回線タイプで実行されます。この例では、簡略化するためにほとんどのコメント行を削除しています。

```
! Enable is-is routing in area 1
router isis area1
! Router is in areas 47.0004.004d.0001 and 47.0004.004d.0011
net 47.0004.004d.0001.0000.0c11.1111.00
net 47.0004.004d.0011.0000.0c11.1111.00
! Enable the router to operate as a station router and an interarea router
is-type level-1-2
!
interface ethernet 0
 clns router isis area1
! Specify a cost of 5 for the level-1 routes
 isis metric 5 level-1
! Establish a level-1 adjacency
 isis circuit-type level-1
```

```
!
interface ethernet 1
 clns router isis area1
 isis metric 2 level-2
 isis circuit-type level-2-only
!
interface serial 0
 clns router isis area1
 isis circuit-type level-1-2
! Set the priority for serial 0 to 3 for a level-1 adjacency
 isis priority 3 level-1
 isis priority 1 level-2
```

ISO CLNS ダイナミック ルート再配布

次に、IS-IS ドメインと ISO IGRP ドメイン間のルート再配布の例を示します。この場合、IS-IS ドメインはイーサネット インターフェイス 0 上にあり、ISO IGRP ドメインはシリアル インターフェイス 0 上にあります。IS-IS ルーティング プロセスにはヌル タグが割り当てられ、ISO IGRP ルーティング プロセスには remote-domain のタグが割り当てられます。この例では、簡略化するためにほとんどのコメント行を削除しています。

```
router isis
 net 39.0001.0001.0000.0c00.1111.00
! Redistribute iso-igrp routing information throughout remote-domain
redistribute iso-igrp remote-domain
!
router iso-igrp remote-domain
 net 39.0002.0001.0000.0c00.1111.00
! Redistribute is-is routing information
redistribute isis
!
interface ethernet 0
 clns router isis
!
interface serial 0
 clns router iso-igrp remote
```

NET の設定例

次に、ISO IGRP と IS-IS の両方に NET を設定する例を示します。

ISO IGRP

次に、NET を指定する例を示します。

```
router iso-igrp Finance
 net 47.0004.004d.0001.0000.0c11.1111.00
```

次に、NET に対して名前を使用する例を示します。

```
clns host NAME 39.0001.0000.0c00.1111.00
router iso-igrp Marketing
 net NAME
```

この **net** ルータ コンフィギュレーション コマンドを使用すると、システム ID、エリア アドレス、およびドメイン アドレスを設定できます。ルーティング プロセスごとに 1 つの NET のみが許可されます。

```
router iso-igrp local
 net 49.0001.0000.0c00.1111.00
```

IS-IS

次に、単一の NET を指定する例を示します。

```
router isis Pieinthesky
 net 47.0004.004d.0001.0000.0c11.1111.00
```

次に、NET に対して名前を使用する例を示します。

```
clns host NAME 39.0001.0000.0c00.1111.00
router isis
 net NAME
```

IS-IS マルチホーミングの例

次に、**net** コマンドを使用して、単一のルータに対して 3 つの個別のエリア アドレスを割り当てる例を示します。エリア アドレス 47.0004.004d.0001、47.0004.004d.0002、または 47.0004.004d.0003 が含まれ、同じシステム ID を持つ受信トラフィックは、このルータに転送されます。

```
router isis eng-area1
!   |      IS-IS Area|     System ID| S|
 net 47.0004.004d.0001.0000.0C00.1111.00
 net 47.0004.004d.0002.0000.0C00.1111.00
 net 47.0004.004d.0003.0000.0C00.1111.00
```

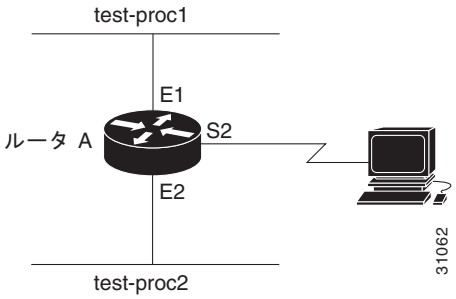
2 つのエリアにあるルータの例

次の 2 つの例は、2 つのエリアでルータを設定する方法を示しています。最初の例では ISO IGRP を設定し、2 つ目の例では IS-IS を設定します。

ISO IGRP

次の例は、49.0001 ドメイン内にあり、aaaa.aaaa.aaaa のシステム ID を持つルータを示しています。このルータは、31 と 40（10 進数）の 2 つのエリアにあります。図 9 に、この設定を示します。

図 9　　ISO IGRP の設定




```
router iso-igrp test-proc1
! 001F in the following net is the hex value for area 31
 net 49.0001.001F.aaaa.aaaa.aaaa.00
router iso-igrp test-proc2
! 0028 in the following net is the hex value for area 40
 net 49.0001.0028.aaaa.aaaa.aaaa.00
!
interface ethernet 1
 clns router iso-igrp test-proc1
!
```

```
interface serial 2
 clns router iso-igrp test-proc1
!
interface ethernet 2
 clns router iso-igrp test-proc2
```

IS-IS

次に、IS-IS を ISO IGRP の代わりに実行する例を示します。ここでも、図 9 を適用できます。イーサネット インターフェイス 2 は IS-IS ルーティング用に設定され、このインターフェイスには、test-proc2 のタグが割り当てられています。

```
router iso-igrp test-proc1
 net 49.0002.0002.bbbb.bbbb.bbbb.00
router isis test-proc2
 net 49.0001.0002.aaaa.aaaa.aaaa.00
!
interface ethernet 1
 clns router iso-igrp test-proc1
!
interface serial 2
clns router iso-igrp test-proc1
!
interface ethernet 2
 clns router is-is test-proc2
```

CLNS パケットのみがルーティング アップデートを行わずに盲目的にインターフェイスを通過できるようにするには、次の設定を使用します。

```
clns routing
interface serial 2
! Permits serial 2 to pass CLNS packets without having CLNS routing turned on
 clns enable
```

基本的なスタティック ルーティングの例

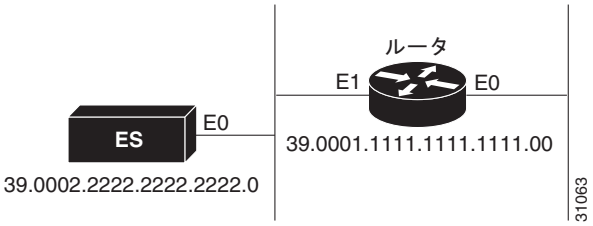
CLNS で FDDI、イーサネット、トークン リング、およびシリアル回線を設定することは、インターフェイスで CLNS をイネーブルにすることと同じくらい簡単です。インターフェイスで CLNS をイネーブルにするために必要なことは、HDLC カプセル化を使用するシリアル回線でこれまで必要とされたことのみです。イーサネットまたはトークン リング上のすべてのシステムが ISO 9542 ES-IS をサポートしている場合は、何も設定する必要はありません。

次に、イーサネットとシリアル回線を設定する例を示します。

```
! Enable clns packets to be routed
 clns routing
! Configure the following network entity title for the routing process
 clns net 47.0004.004d.0055.0000.0C00.BF3B.00
! Pass ISO CLNS traffic on ethernet 0 to end systems without routing
interface ethernet 0
 clns enable
! Pass ISO CLNS traffic on serial 0 to end systems without routing
interface serial 0
 clns enable
! Create a static route for the interface
 clns route 47.0004.004d.0099 serial 0
 clns route 47.0005 serial 0
```

次に、CLNS スタティック ルーティングを 2 つのイーサネット インターフェイスを持つシステムで行った場合のより詳細な例を示します。ルーティングを設定した後は、NET を定義して、イーサネット 0 インターフェイスとイーサネット 1 インターフェイスで CLNS をイネーブルにします。次に ES ネイバーを定義し、以下に示されているように、**clns route** グローバル コンフィギュレーション コマンドを使用してスタティック ルートを定義します。この状況では、ES は ES-IS をサポートしていないイーサネット 1 上にあります。図 10 に、このネットワークを示します。

図 10　　スタティック ルーティング

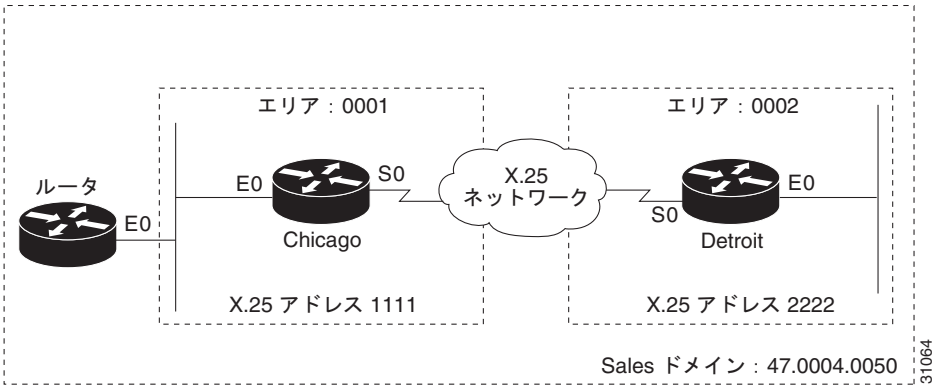



```
 clns host sid 39.0001.1111.1111.1111.00
 clns host bar 39.0002.2222.2222.2222.00
! Assign a static address for the router
 clns net sid
! Enable CLNS packets to be routed
 clns routing
! Pass ISO CLNS packet traffic to end systems without routing them
interface ethernet 0
 clns enable
! Pass ISO CLNS packet traffic to end systems without routing them
interface ethernet 1
 clns enable
! Specify end system for static routing
 clns es-neighbor bar 0000.0C00.62e7
! Create an interface-static route to bar for packets with the following NSAP address
 clns route 47.0004.000c bar
```

スタティック ドメイン内ルーティングの例

図 11 および後続の例は、ドメインの内部でスタティック ルーティングを使用する方法を示しています。Detroit と Chicago の支社が X.25 リンクで接続されている企業があるとします。これらの支社はともに Sales という名前のドメイン内にあります。

図 11　　CLNS X.25 ドメイン内ルーティング



次に、Chicago ルータを設定する 1 つの方法を示します。

```
! Define the name chicago to be used in place of the following NSAP
clns host chicago 47.0004.0050.0001.0000.0c00.243b.00
! Define the name detroit to be used in place of the following NSAP
clns host detroit 47.0004.0050.0002.0000.0c00.1e12.00
! Enable ISO IGRP routing of CLNS packets
router iso-igrp sales
! Configure net chicago, as defined above
 net chicago
! Specify iso-igrp routing using the previously specified tag sales
interface ethernet 0
 clns router iso-igrp sales
! Set the interface up as a DTE with X.25 encapsulation
interface serial 0
 encapsulation x25
 x25 address 1111
 x25 nvc 4
! Specify iso-igrp routing using the previously specified tag sales
 clns router iso-igrp sales
! Define a static mapping between Detroit's nsap and its X.121 address
 x25 map clns 2222 broadcast
```

この設定により、Chicago ルータと Detroit ルータ間の X.25 仮想回線がアップします。ルーティングアップデートはこのリンクを通して送信されます。これは、仮想回線がアップ状態を継続できることを意味します。

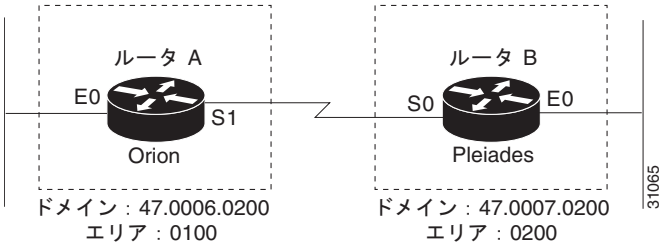
Chicago オフィスが拡大して複数のルータを導入することになった場合は、各ルータが Detroit ルータへの到着方法を把握していることが理想的です。Chicago ルータ間で情報を再配布するには、次のコマンドを追加します。

```
router iso-igrp sales
 redistribute static
```

スタティック ドメイン間ルーティングの例

図 12 および後続の例は、ドメイン間で情報を配布する 2 つのルータを設定する方法を示しています。この例では、（Orion ドメイン内にある）ルータ A と（Pleiades ドメイン内にある）ルータ B が、シリアル リンクを通して通信しています。

図 12　CLNS ドメイン間スタティック ルーティング



次に、ルータ A でスタティック ドメイン間ルーティングを設定する例を示します。

```
! Define tag orion for net 47.0006.0200.0100.0102.0304.0506.00
router iso-igrp orion
! Configure the following network entity title for the routing process
 net 47.0006.0200.0100.0102.0304.0506.00
! Define the tag bar to be used in place of Router B's NSAP
clns host bar 47.0007.0200.0200.1112.1314.1516.00
! Specify iso-igrp routing using the previously specified tag orion
interface ethernet 0
 clns router iso-igrp orion
! Pass ISO CLNS traffic to end systems without routing
interface serial 1
 clns enable
! Configure a static route to Router B
 clns route 47.0007 bar
```

次に、ルータ B でスタティック ドメイン間ルーティングを設定する例を示します。

```
router iso-igrp pleiades
! Configure the network entity title for the routing process
 net 47.0007.0200.0200.1112.1314.1516.00
! Define the name sid to be used in place of Router A's NSAP
clns host sid 47.0006.0200.0100.0102.0304.0506.00
! Specify iso-igrp routing using the previously specified tag pleiades
interface ethernet 0
 clns router iso-igrp pleiades
! Pass ISO CLNS traffic to end systems without routing
interface serial 0
 clns enable
! Pass packets bound for sid in domain 47.0006.0200 through serial 0
 clns route 47.0006.0200 sid
```

CLNS ルーティング アップデートはシリアル リンクでは送信されませんが、CLNS パケットはシリアル リンクを通して送受信されます。

CLNS フィルタの例

次に、アドレスが 47.0005 または 47.0023 のいずれかで始まるパケットを許可する例を示します。この場合、他のすべてのアドレスは暗黙的に拒否されます。

```
clns filter-set US-OR-NORDUNET permit 47.0005...
clns filter-set US-OR-NORDUNET permit 47.0023...
```

次に、アドレスが 39.840F で始まるパケットを拒否し、それ以外のすべてのアドレスを許可する例を示します。

```
clns filter-set NO-ANSI deny 38.840F...
clns filter-set NO-ANSI permit default
```

次に、2 つのシステムに限定されたエンド システムの隣接関係を、それらのシステムの ID のみに基づいて受け入れるフィルタを構築する例を示します。

```
clns filter-set ourfriends ...0000.0c00.1234.**
clns filter-set ourfriends ...0000.0c00.125a.**

interface ethernet 0
 clns adjacency-filter es ourfriends
```

ルート マップの例

次に、2 つのタイプのルートを（IP と CLNS の両方をサポートする）統合 IS-IS ルーティング テーブルに再配布する例を示します。1 番目のルートは、タグ 5 が割り当てられた OSPF 外部 IP ルートです。これらのルートは、メトリック 5 のレベル 2 IS-IS LSP に挿入されます。2 番目のルートは、CLNS フィルタ式「osifilter」に一致する ISO IGRP から派生した CLNS プレフィクス ルートです。これらのルートは、メトリック 30 のレベル 2 LSP として IS-IS に再配布されます。

```
router isis
 redistribute ospf 109 route-map ipmap
 redistribute iso-igrp nsfnet route-map osimap
!
 route-map ipmap permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
 route-map osimap permit
 match clns address osifilter
 set metric 30
 clns filter-set osifilter permit 47.0005.80FF.FF00
```

次に、ネットワーク 160.89.0.0 に対して RIP で学習されたルートと、プレフィクス 49.0001.0002 の ISP-IGRP で学習されたルートを、メトリック 5 の IS-IS レベル 2 LSP に再配布する例を示します。

```
router isis
 redistribute rip route-map ourmap
 redistribute iso-igrp remote route-map ourmap
!
 route-map ourmap permit
 match ip address 1
 match clns address ourprefix
 set metric 5
 set level level-2
!
 access-list 1 permit 160.89.0.0 0.0.255.255
 clns filter-set ourprefix permit 49.0001.0002...
```

DECnet クラスタ エイリアスの例

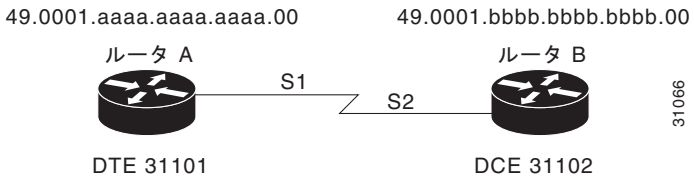
次に、CLNS でクラスタ エイリアスをイネーブルにする例を示します。

```
clns routing
clns nsap 47.0004.004d.0001.0000.0C00.1111.00
router iso-igrp pleiades
! enable cluster aliasing on interface ethernet 0
interface ethernet 0
 clns cluster-alias
! enable cluster aliasing on interface ethernet 1
interface ethernet 1
 clns cluster-alias
```

ISO CLNS over X.25 の例

次に、ルータ A 上のシリアル インターフェイス 1 が、X.25 の Data Terminal Equipment（DTE; データ端末装置）としてどのように動作するかを示します。これにより、ブロードキャストの通過が許可されます。ルータ B は、CLNS アドレス 49.0001.bbbb.bbbb.bbbb.00、および X.121 アドレス 31102 を持つ IS です。ルータ A には、CLNS アドレス 49.0001.aaaa.aaaa.aaaa.00、および X.21 アドレス 31101 があります。図 13 に、この設定を示します。

図 13　　DTE およびデータ回線終端装置（DCE）として動作するルータ



ルータ A

```
router iso-igrp test-proc
net 49.0001.aaaa.aaaa.aaaa.00
!
interface serial 1
 clns router iso-igrp test-proc
! assume the host is a DTE and encapsulates x.25
 encapsulation x25
! Define the X.121 address of 31101 for serial 1
 X25 address 31101
! Set up an entry for the other side of the X.25 link (Router B)
 x25 map clns 31102 broadcast
```

ルータ B

```
router iso-igrp test-proc
 net 49.0001.bbbb.bbbb.bbbb.00
!
interface serial 2
 clns router iso-igrp test-proc
! Configure this side as a DCE
 encapsulation x25-dce
! Define the X.121 address of 31102 for serial 2
 X25 address 31102
! Configure the NSAP of Router A and accept reverse charges
 x25 map clns 31101 broadcast accept-reverse
```

パフォーマンス パラメータの例

次に、簡単な ISO IGRP 設定で、ES hello パケット パラメータと IS hello パケット パラメータを、シリアル インターフェイスの MTU と共に設定する例を示します。

```
router iso-igrp xavier
 net 49.0001.004d.0002.0000.0C00.0506.00
! Send IS/ES hellos every 45 seconds
clns configuration-time 45
! Recipients of the hello packets keep information in the hellos for 2 minutes
clns holding-time 120
! Specify an MTU of 978 bytes; generally, do not alter the default MTU value
interface serial 2
 clns mtu 978
```

TARP の設定例

次の 2 つの項では、基本的な TARP 設定と複雑な TARP 設定の例を示しています。

基本的な TARP 設定の例

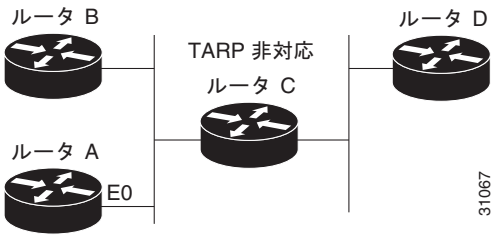
次に、ルータとイーサネット インターフェイス 0 で TARP をイネーブルにする例を示します。ルータには TID myname が割り当てられます。

```
clns routing
tarp run
tarp tid myname

interface ethernet 0
 tarp enable
```

複雑な TARP 設定の例

図 14 および後続の例は、ルータ A とインターフェイス イーサネット 0 で TARP をイネーブルにしてから TID myname を割り当てる方法を示しています。ルータ C は TARP に対応していないため、ルータ D が TARP PDU を受信できるように、スタティック ルートはルータ A（49.0001.1111.1111.1111.00）からルータ D（49.0004.1234.1234.1234.00）に作成されます。また、ルータ A が TARP PDU をルータ B に送信しないように、ルータ A で隣接ブラックリストが作成され、ルータ B（49.001.7777.7777.7777.00）がリストに指定されます。

図 14　　TARP の設定例



ルータ A

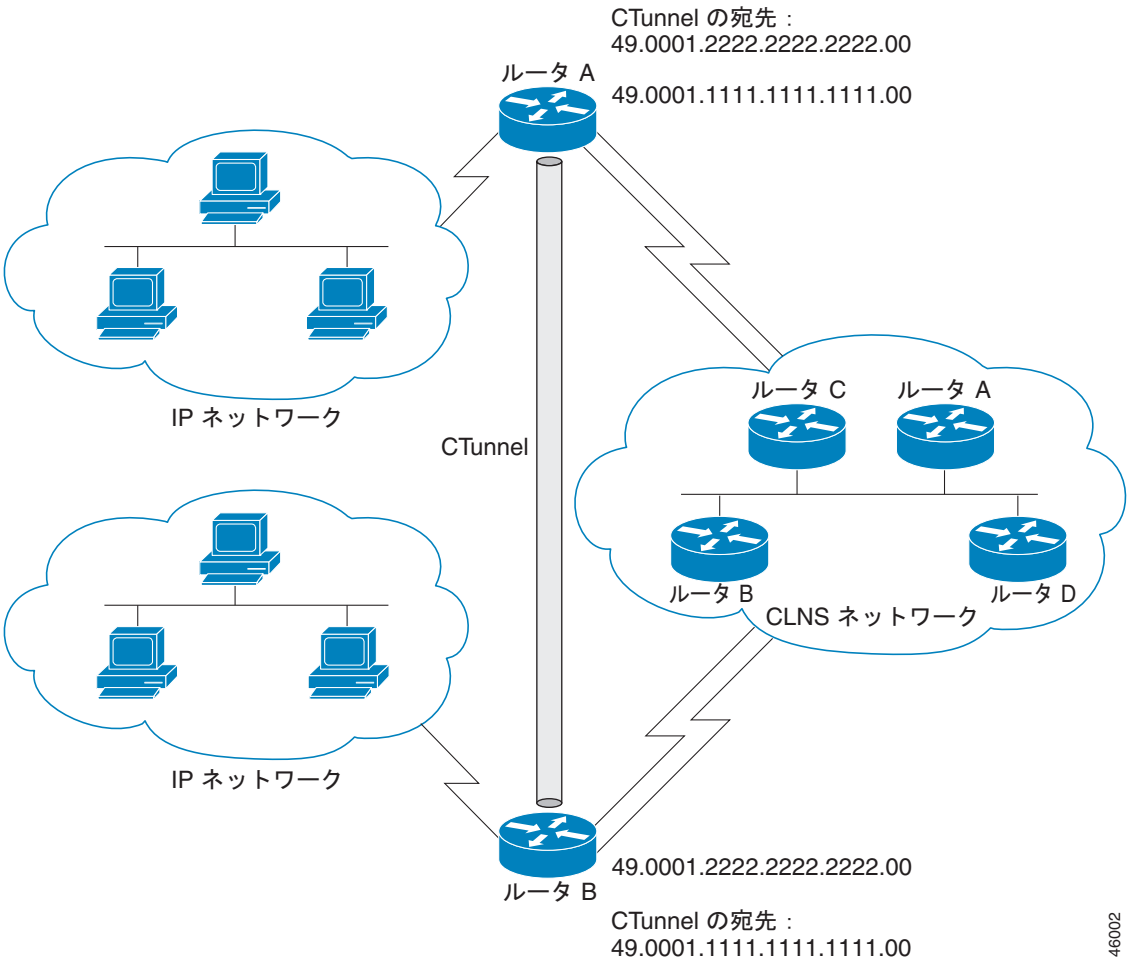
```
clns routing
tarp run
tarp cache-timer 300
```

```
tarp route-static 49.0004.1234.1234.1234.00
tarp blacklist-adjacency 49.0001.7777.7777.7777.00
tarp tid myname
interface ethernet 0
 tarp enable
```

IP over CLNS トンネルの例

図 15 に、ルータ A とルータ B 間に CTunnel を作成する例を示します。この内容は、後に続くルータ A とルータ B の設定例に示されています。

図 15　　CTunnel の作成



ルータ A

```
ip routing
clns routing

interface ctunnel 102
 ip address 10.0.0.1 255.255.255.0
 ctunnel destination 49.0001.2222.2222.2222.00
```

```
interface Ethernet0/1
 clns router isis

router isis
 net 49.0001.1111.1111.1111.00

router rip
 network 10.0.0.0
```

ルータ B

```
ip routing
clns routing

interface ctunnel 201
 ip address 10.0.0.2 255.255.255.0
 ctunnel destination 49.0001.1111.1111.1111.00

interface Ethernet0/1
 clns router isis

router isis
 net 49.0001.2222.2222.2222.00

router rip
 network 10.0.0.0
```

IPv4 および IPv6 パケットを伝送するための GRE/CLNS CTunnel の設定例

次に、CLNS ネットワーク内のルータ A とルータ B 間で、IS-IS および IPv6 トラフィックの両方を伝送する GRE CTunnel を設定する例を示します。**ctunnel mode gre** コマンドにより、RFC 3147 に準拠したトンネリング方法が提供され、シスコ機器とサードパーティ製ネットワーキング デバイス間のトンネリングが許可されます。

ルータ A

```
ipv6 unicast-routing

clns routing

interface ctunnel 102
 ipv6 address 2001:0DB8:1111:2222::1/64
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode gre

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.1111.1111.1111.00
```

ルータ B

```
ipv6 unicast-routing

clns routing
```

```
interface ctunnel 201
 ipv6 address 2001:0DB8:1111:2222::2/64
 ctunnel destination 49.0001.1111.1111.1111.00
 ctunnel mode gre

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.2222.2222.2222.00
```

シスコ機器のエンドポイント間で GRE モードをオフにして、CTunnel をデフォルトのシスコ カプセル化ルーティングのみに戻すには、**no ctunnel mode** コマンドまたは **ctunnel mode cisco** コマンドのいずれかを使用します。次に、同じ設定を IPv4 トラフィックだけを転送するよう修正した例を次に示します。

ルータ A

```
ip routing

clns routing

interface ctunnel 102
 ip address 10.2.2.5 255.255.255.0
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode cisco

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.1111.1111.1111.00
```

ルータ B

```
ip routing

clns routing

interface ctunnel 201
 ip address 10.0.0.5 255.255.255.0
 ctunnel destination 49.0001.1111.1111.1111.00
 ctunnel mode cisco

interface Ethernet0/1
 clns router isis

router isis
 network 49.0001.2222.2222.2222.00
```

その他の関連資料

ここでは、ISO CLNS 機能に関する関連資料について説明します。

関連マニュアル

内容	参照先
ISO CLNS コマンド	『Cisco IOS ISO CLNS Command Reference』
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』

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

ISO CLNS 設定の機能情報

表 5 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。この表には、Cisco IOS Release 12.3(7)T 以降のリリースで導入または変更された機能だけを示します。

すべてのコマンドがご使用の Cisco IOS ソフトウェア リリースで使用できるとは限りません。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 により、どの Cisco IOS および Catalyst OS ソフトウェア イメージが特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 5 は、Cisco IOS ソフトウェア リリース トレインで各機能のサポートが導入されたときの Cisco IOS ソフトウェア リリースだけを示しています。特に明記していないかぎり、その Cisco IOS ソフトウェア リリース トレインの以降のリリースでもその機能はサポートされます。

表 5　ISO CLNS 設定の機能情報

機能名	リリース	機能情報
ISO CLNS の設定	12.3(7)T	この機能が導入されました。
IPv4 および IPv6 の GRE トンネリングに対する CLNS サポート	12.2(25)S 12.2(33)SRA 15.0(1)M Cisco IOS XE Release 2.6	この機能は、Cisco Release 12.2(25)S に統合されました。Cisco CTunnel は、シスコのネットワーキング機器と他のベンダーの機器間の相互運用を許可する形で、IPv4 および IPv6 パケットを CLNS-only ネットワーク経由で転送します。GRE トンネル モードに対する CLNS サポートにより、この転送が可能になりました。CLNS 機能は RFC 3147 に準拠しています。