CHAPTER 13

管理ネットワークの接続

この章では、ONS 15454 SDH Data Communications Network（DCN; データ通信ネットワーク）接続の概要について説明します。Cisco Optical Networking System（ONS）ネットワーク通信は、Cisco Transport Controller（CTC; シスコトランスポートコントローラ）コンピュータと ONS 15454 SDH ノード間の通信、接続された ONS 15454 SDH ノード間の通信を含む IP に基づいています。この章では、一般的な IP ネットワーク構成での Cisco ONS 15454 SDH ノードのシナリオを示します。また、プロビジョニング可能なパッチコード、IP ルーティング テーブル、外部ファイアウォール、およびオープン Gateway Network Element（GNE; ゲートウェイ ネットワーク エレメント）ネットワークについても説明します。

（注） この章では、IP ネットワーキングの概念と手順については、詳細には説明しません。また、すべてのネットワーキング シナリオを満たす IP アドレスの例は表示していません。ONS 15454 SDH ネットワーキングの設定手順については、『*Cisco ONS 15454 SDH Procedure Guide*』の「Turn Up a Node」の章を参照してください。

ONS 15454 SDH DCN 通信は IP に基づいていますが、ONS 15454 SDH ノードは、Open Systems Interconnection（OSI; 開放型システム間相互接続）プロトコル スイートに基づいている機器に接続できます。この章では、ONS 15454 SDH OSI の実装について説明します。また、IP と OSI が混在する環境内で ONS 15454 SDH を接続できる形態を示すシナリオを提供します。

この章では、次の内容について説明します。

- 13.1　IP ネットワーキングの概要（p.13-2）
- 13.2　IP アドレッシング シナリオ（p.13-3）
- 13.3　ルーティング テーブル（p.13-27）
- 13.4　外部ファイアウォール（p.13-29）
- 13.5　オープン GNE（p.13-31）
- 13.6　TCP/IP および OSI ネットワーキング（p.13-34）
- 13.7　IPv6 ネットワークの互換性（p.13-63）

（注） ONS 15454 SDN ノードを IP ネットワークに接続する場合には、LAN 管理者または IP ネットワークのトレーニングを受けた経験を持つ現場担当者と一緒に作業してください。

13.1　IP ネットワーキングの概要

ONS 15454 SDH ノードは、IP 環境で次のようなさまざまな形態で接続できます。

- 直接接続またはルータを使用して LAN に接続する。
- IP サブネット化を行うと、単一のクラス A、B、または C の IP ネットワーク内に複数の論理 ONS 15454 SDH ネットワークの作成が可能。サブネット化を行わない場合は、クラス A、B、または C のネットワークで利用できるネットワークは 1 つ。
- ネットワークでの特定の作業を遂行するために、さまざまな IP 機能とプロトコルを使用。たとえば、プロキシ Address Resolution Protocol（ARP; アドレス解決プロトコル）により、LAN に接続された 1 つの ONS 15454 SDH を、LAN に接続されていない ONS 15454 SDH ノードのゲートウェイとして使用できます。
- スタティック ルートを作成し、複数の CTC セッションを使用して、同じサブネット上の複数の ONS 15454 SDH ノードを接続する。
- ONS 15454 SDH ノードを Open Shortest Path First（OSPF）ネットワークに接続し、ONS 15454 SDH ネットワークの情報を複数の LAN や WAN 上で自動的にやり取りする。
- ONS 15454 SDH プロキシ サーバによって、CTC コンピュータと ONS 15454 SDH 要素ノードの間の可視性とアクセス可能性を制御する。

13.2　IP アドレッシング シナリオ

ONS 15454 SDH の IP アドレッシングには、一般的に 8 つのシナリオ（構成）があります。これらのシナリオは、より複雑なネットワーク構成の基礎として使用してください。表 13-1 に、IP ネットワークで ONS 15454 SDH ノードを設定する際の一般的なチェック項目の一覧を示します。

表 13-1　ONS 15454 SDH の一般的な IP トラブルシューティングのチェックリスト

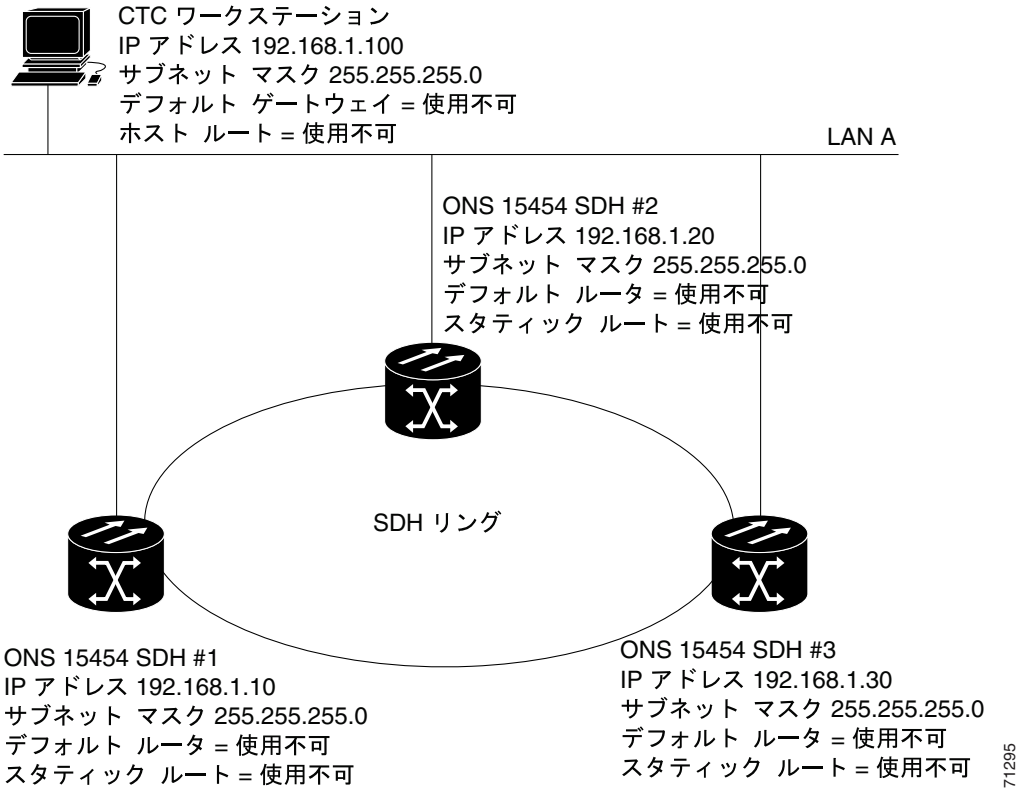
項目	チェック内容
リンク完全性	次の構成要素の間でリンク完全性があることを確認します。 • CTC コンピュータと、ネットワーク ハブまたはスイッチ • ONS 15454 SDH ノード（MIC-C/T/P ワイヤーラップ ピンまたは RJ-45 ポート）と、ネットワーク ハブまたはスイッチ • ルータ ポートと、ハブ ポートまたはスイッチ ポート
ONS 15454 SDH ハブ ポート / スイッチ ポート	接続に問題がある場合は、ONS 15454 SDH に接続しているハブまたはスイッチ ポートを 10 Mbps の半二重に設定します。
ping	ノードに対して ping を実行して、コンピュータと ONS 15454 SDH ノード間の接続をテストします。
IP アドレス / サブネット マスク	ONS 15454 SDH の IP アドレスとサブネット マスクが正しく設定されていることを確認します。
光通信の接続	ONS 15454 SDH の光トランク（スパン）ポートがイン サービスで、DCC が各トランク ポートで有効であることを確認します。

TCC2P カードのセキュア モードでは、2 つの IP アドレスのうち、1 つを MIC-C/P LAN ポートに、1 つを TCC2P LAN（TCP/IP）ポートにプロビジョニングできます。セキュア モードの IP アドレッシングの例は、「13.2.9　シナリオ 9：セキュア モードを有効にした IP アドレッシング」（p.13-22）に記載されています。他のシナリオで示される IP アドレスは、セキュア モードが有効でないことを前提としています。セキュア モードが有効である場合、例で示される IP アドレスは MIC-C/T/P LAN ポートに当てはまります。セキュア モード、リピータ（単一 IP アドレス）モード、およびコンフィギュレーション ロックの詳細については、「13.2.9　シナリオ 9：セキュア モードを有効にした IP アドレッシング」（p.13-22）を参照してください。

13.2.1　シナリオ 1：同一サブネット上での CTC と ONS 15454 SDH ノード

シナリオ 1 は、ONS 15454 SDH の基本的な LAN 構成を示します（図 13-1）。ONS 15454 SDH ノードと CTC コンピュータは同一サブネットにあります。すべての ONS 15454 SDH ノードが LAN A に接続され、すべての ONS 15454 SDH ノードに DCC が接続されています。

図 13-1　シナリオ 1：同一サブネット上での CTC と ONS 15454 SDH ノード

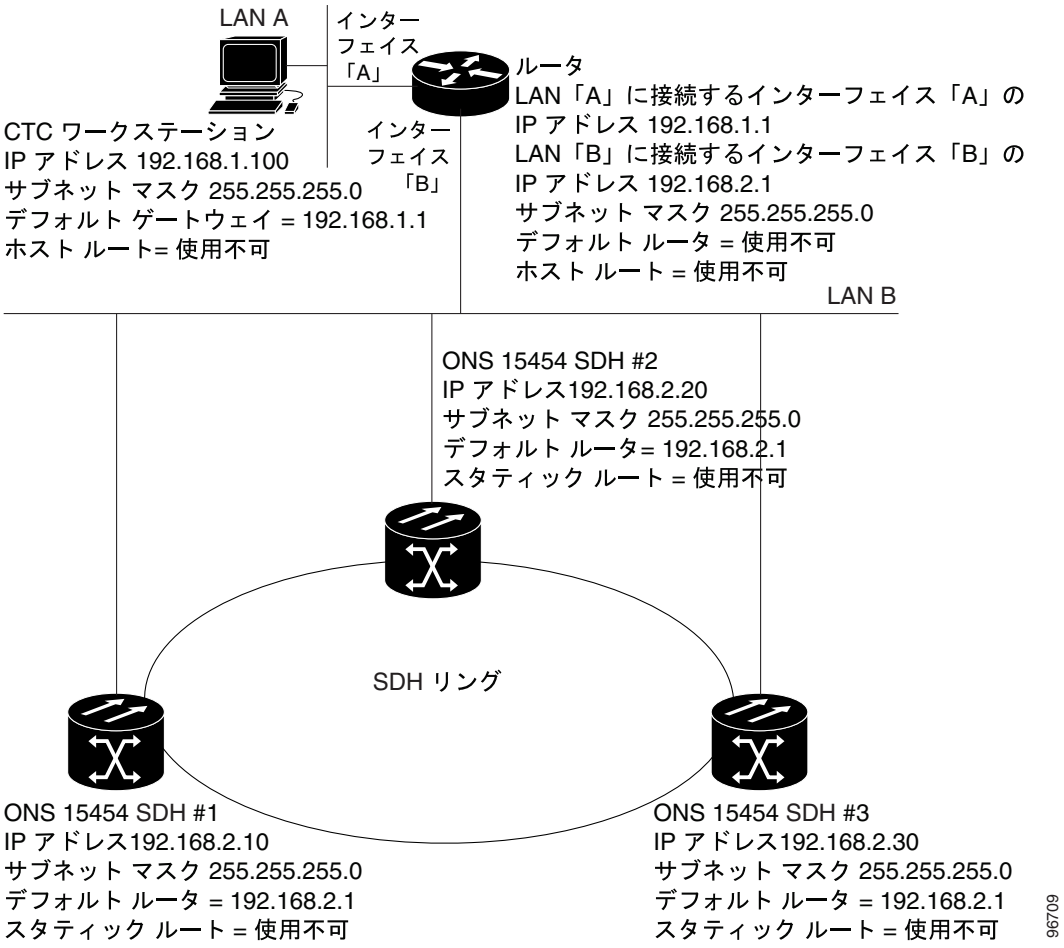


13.2.2　シナリオ 2：ルータに接続された CTC と ONS 15454 SDH ノード

シナリオ 2 では、CTC コンピュータはサブネット（192.168.1.0）上にあり、LAN A に接続されています（図 13-2）。ONS 15454 SDH ノードは異なるサブネット（192.168.2.0）上にあり、すべての ONS 15454 が LAN B に接続されています。ルータによって、LAN A と LAN B が接続されています。ルータ インターフェイス A の IP アドレスは LAN A（192.168.1.1）に、ルータ インターフェイス B の IP アドレスは LAN B（192.168.2.1）にそれぞれ設定されています。

CTC コンピュータでは、デフォルト ゲートウェイがルータ インターフェイス A に設定されています。LAN で Dynamic Host Configuration Protocol（DHCP）を使用する場合は、デフォルト ゲートウェイと IP アドレスが自動的に割り当てられます。図 13-2 に示した例では、DHCP サーバは使用できません。

図 13-2　シナリオ 2：ルータに接続された CTC と ONS 15454 SDH ノード



13.2.3　シナリオ 3：プロキシ ARP による ONS 15454 SDH ゲートウェイの有効化

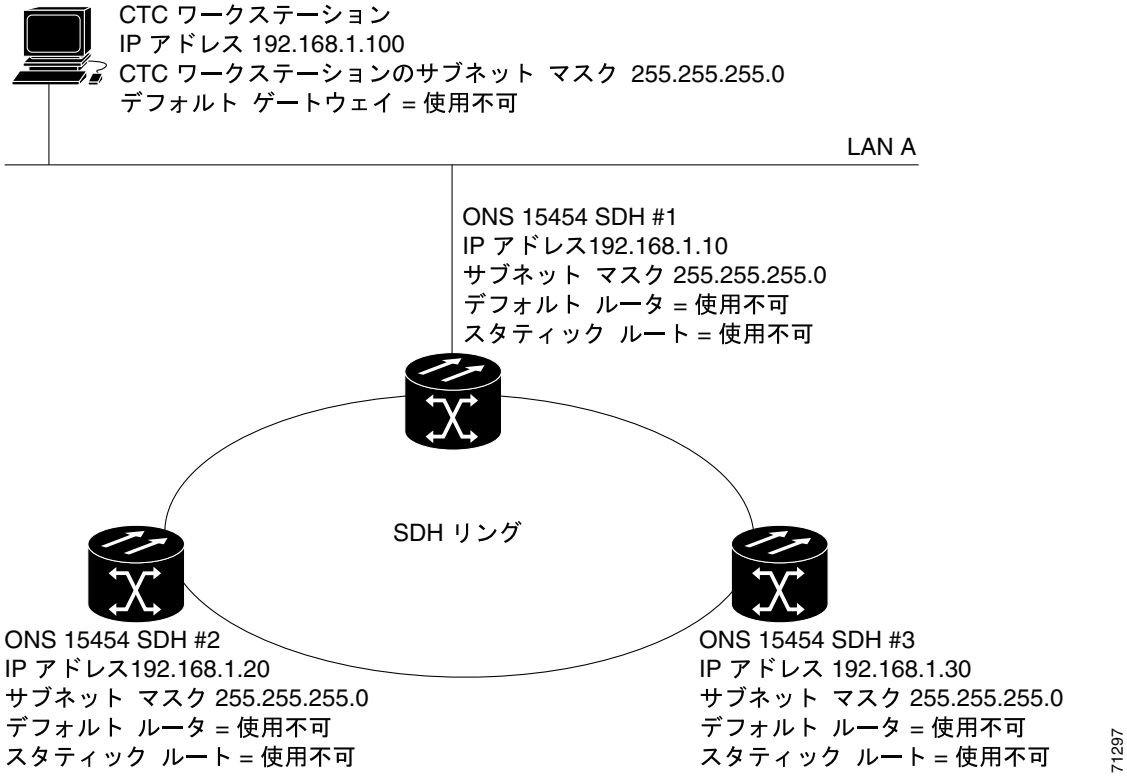
ARP は、上位レベルの IP アドレスを宛先ホストの物理アドレスに一致させます。ARP は、ルックアップ テーブル（ARP キャッシュと呼ばれる）を使用して変換を行います。ARP キャッシュ内でアドレスが見つからない場合は、ARP 要求と呼ばれる特別な形式でブロードキャストをネットワークに送ります。ネットワーク上の 1 つのマシンがそのマシンの IP アドレスを含む ARP 要求を認識すると、ARP 要求の送信側ホストへ ARP 応答を返します。ARP 応答には、受信側ホストの物理ハードウェア アドレスが含まれます。送信側ホストはその ARP キャッシュにこのアドレスを保存します。このため、この宛先 IP アドレスへの以降のすべてのデータグラム（パケット）が物理アドレスに変換できます。

プロキシ ARP により、LAN に接続された ONS 15454 SDH は、LAN に接続されていない ONS 15454 SDH ノードの ARP 要求に応答できます（ONS 15454 SDH プロキシ ARP に対する、ユーザによる設定は必要ありません）。DCC 接続された ONS 15454 SDH ノードは同一サブネット上に存在している必要があります。LAN 装置が LAN に接続されていない ONS 15454 SDH に ARP 要求を送信すると、ゲートウェイ ONS 15454 SDH はその MAC アドレスを LAN 装置に返します。次に、LAN 装置が、リモートの ONS 15454 SDH 宛てのデータグラムを、プロキシ ONS 15454 SDH の MAC アドレスに送信します。プロキシ ONS 15454 SDH は、自身のルーティング テーブルを使用して、このデータグラムを LAN に接続されていない ONS 15454 SDH に転送します。

シナリオ 3 はシナリオ 1 に似ていますが、LAN に接続されている ONS 15454 SDH（#1）は 1 つだけです（図 13-3）。2 つの ONS 15454 SDH ノード（#2 および #3）が、SDH DCC を介して ONS 15454 SDH #1 に接続されています。すべての 3 つのノードが同一サブネット上にあるため、プロキシ ARP は ONS 15454 SDH #1 を有効にして、ONS 15454 SDH #2 および #3 のゲートウェイとして使用することができます。

（注）　このシナリオでは、すべての CTC が ONS 15454 SDH #1 に接続されているものと想定しています。ラップトップ コンピュータが ONS 15454 SDH #2 または #3 のどちらかに接続されている場合は、ネットワーク分割が発生します。ラップトップ コンピュータおよび CTC コンピュータのどちらも、表示できないノードがあります。ラップトップを終端のネットワーク要素に直接接続する場合は、スタティック ルート（シナリオ 5 参照）を作成するか、または ONS 15454 SDH プロキシ サーバ（シナリオ 7 参照）を有効化する必要があります。

図 13-3　シナリオ 3：プロキシ ARP の使用

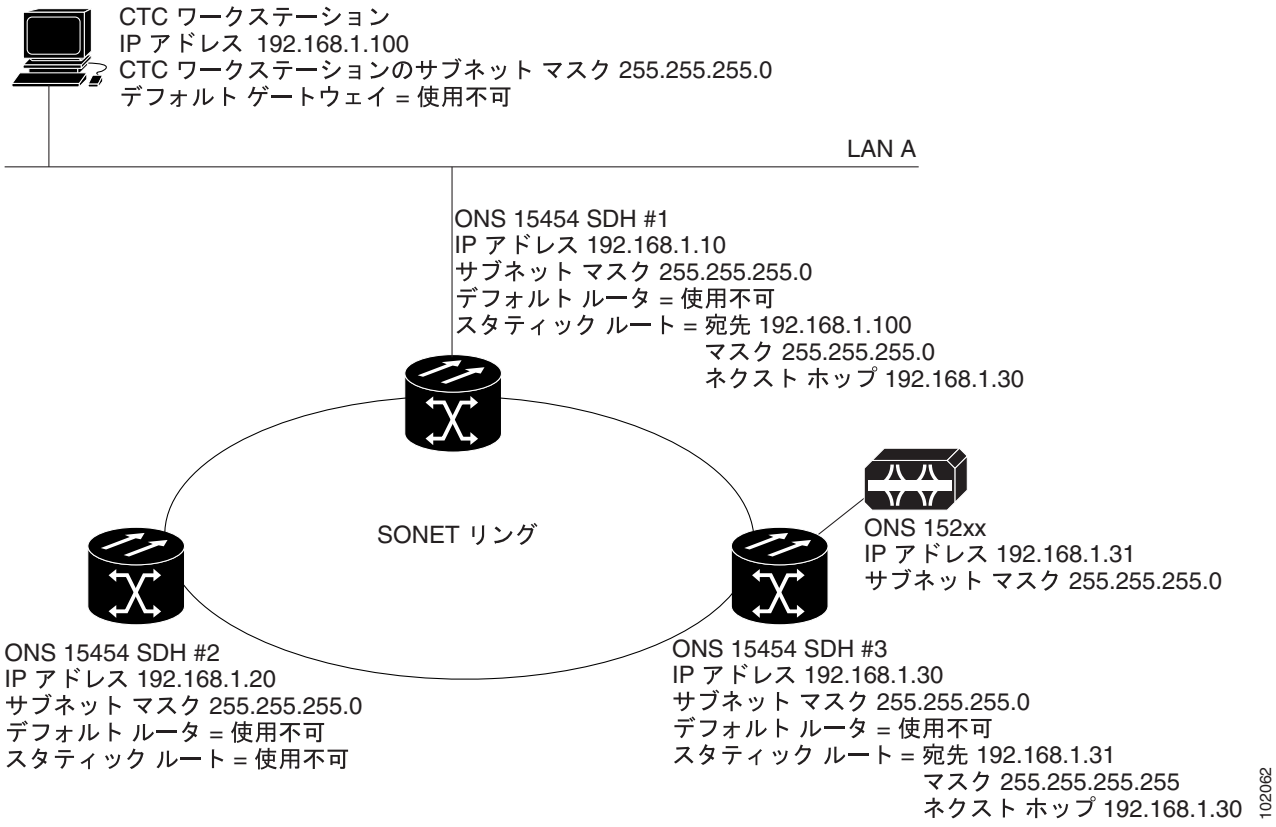


また、プロキシ ARP を使用して、DCC 接続されたノードのクラフト イーサネット ポートに接続されているホストと通信することもできます（図 13-4）。ホストが接続されているノードには、そのホストへのスタティック ルートが必要です。スタティック ルートは、OSPF によってすべての DCC ピアへ伝播されます。ホストを追加した場合、既存のプロキシ ARP ノードがゲートウェイになります。各ノードは、同じサブネット上にあって DCC ネットワークへ接続されていないホストへのルートを、それぞれのルーティング テーブルで調べます。このような追加ホストに対する ARP 要求には既存のプロキシ サーバが応答し、対象ノードの MAC アドレスを返します。ルーティング テーブルにホストへのルートが存在していれば、追加されたホストに対し、IP パケットを正常に送信できます。ノードおよび追加ホスト間のスタティック ルートを確立する以外のプロビジョニングは必要ありません。次の制約事項が適用されます。

- ホストの追加の際にプロキシ ARP サーバとして機能するノードは 1 つのみ。
- ノードをそのイーサネット ポートに接続されているホストのプロキシ ARP にすることはできない。

図 13-4 では、ONS 15454 SDH #1 は、ONS 15454 SDH #2 および #3 に対し、ONS 15454 SDH #1 が CTC ホストに接続できることをアナウンスします。同様に、ONS 15454 SDH #3 は、ONS 15454 SDH #3 が ONS 152xx に接続できることをアナウンスします。ONS 152xx は、一例です。実際には、どのネットワーク要素でも追加ホストとしてセットアップできます。

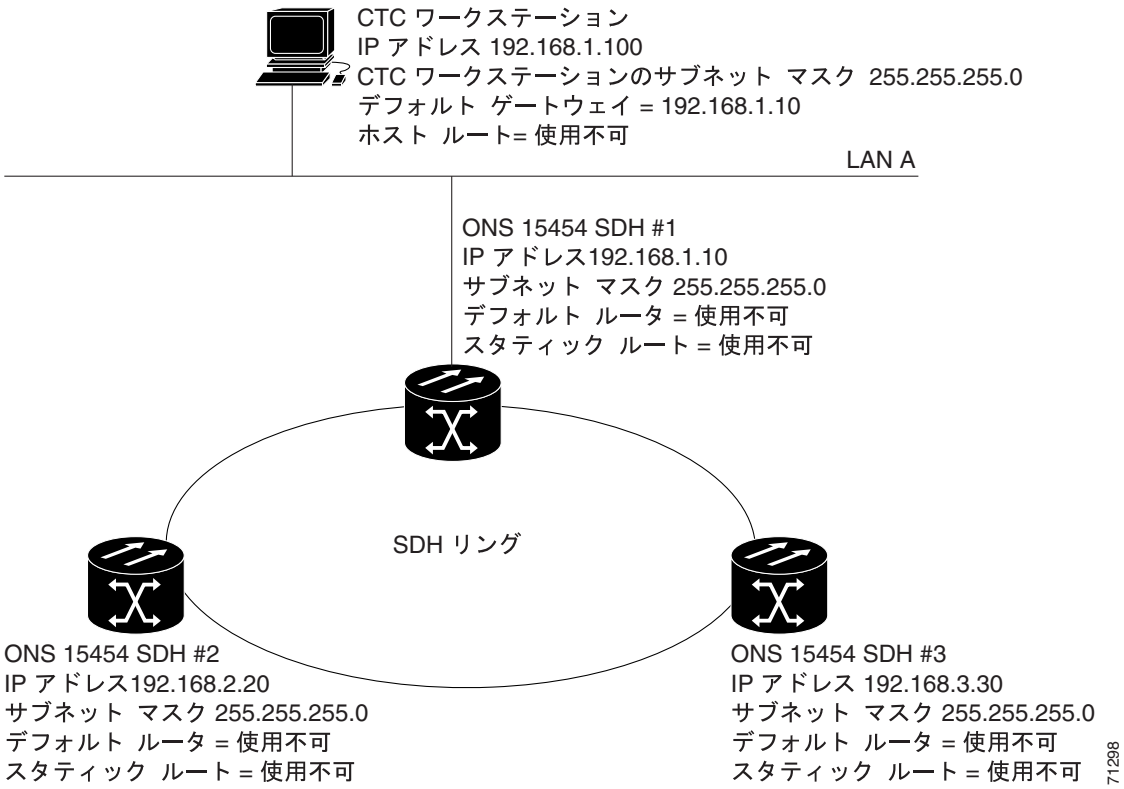
図 13-4　シナリオ 3 : スタティック ルーティングでのプロキシ ARP の使用



13.2.4　シナリオ 4：CTC コンピュータのデフォルト ゲートウェイ

シナリオ 4 はシナリオ 3 に似ていますが、ノード #2 とノード #3 がそれぞれ 192.168.2.0 と 192.168.3.0 の異なるサブネット上にあります（図 13-5）。ノード #1 と CTC コンピュータはサブネット 192.168.1.0 上にあります。このネットワークに異なるサブネットが含まれるため、プロキシ ARP は使用されません。CTC コンピュータが ノード #2 および #3 と通信するために、ノード #1 が CTC コンピュータのデフォルト ゲートウェイとなります。

図 13-5　シナリオ 4：CTC コンピュータのデフォルト ゲートウェイ



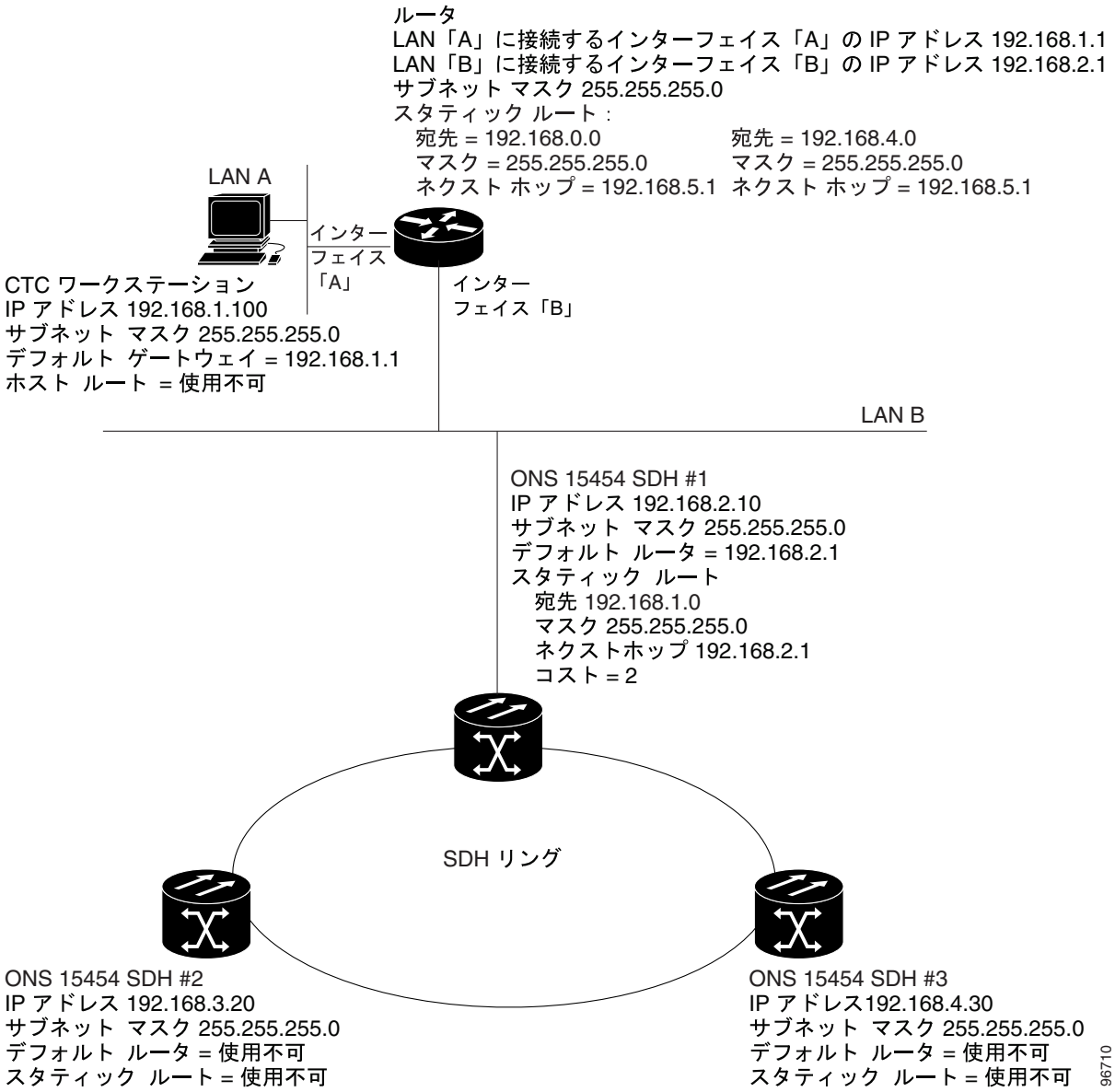
13.2.5　シナリオ 5：スタティック ルートを使用した LAN への接続

スタティック ルートは次の 2 つの目的で使用します。

- ONS 15454 SDH ノードをサブネット上の CTC セッションに接続し、ルータによって別のサブネット上にある ONS 15454 SDH ノードに接続する（OSPF が使用可能な場合には、これらのスタティック ルートは必要ありません）。シナリオ 6 に、OSPF の例を示します。
- 同一サブネット上にある ONS 15454 SDH ノードの間で複数の CTC セッションを使用可能にする。

図 13-6 では、サブネット 192.168.1.0 上の CTC がインターフェイス A でルータに接続されています（このルータは OSPF で設定されていません）。別のサブネット上の ONS 15454 SDH ノードは ノード #1 に接続され、インターフェイス B でルータに接続されています。ノード #2 と #3 がそれぞれ異なるサブネットにあるため、プロキシ ARP はノード #1 をゲートウェイとして使用可能にしません。LAN A 上の CTC コンピュータに接続するために、ノード #1 でスタティック ルートが作成されます。

図 13-6　シナリオ 5：宛先として使用される 1 つの CTC コンピュータのスタティック ルート

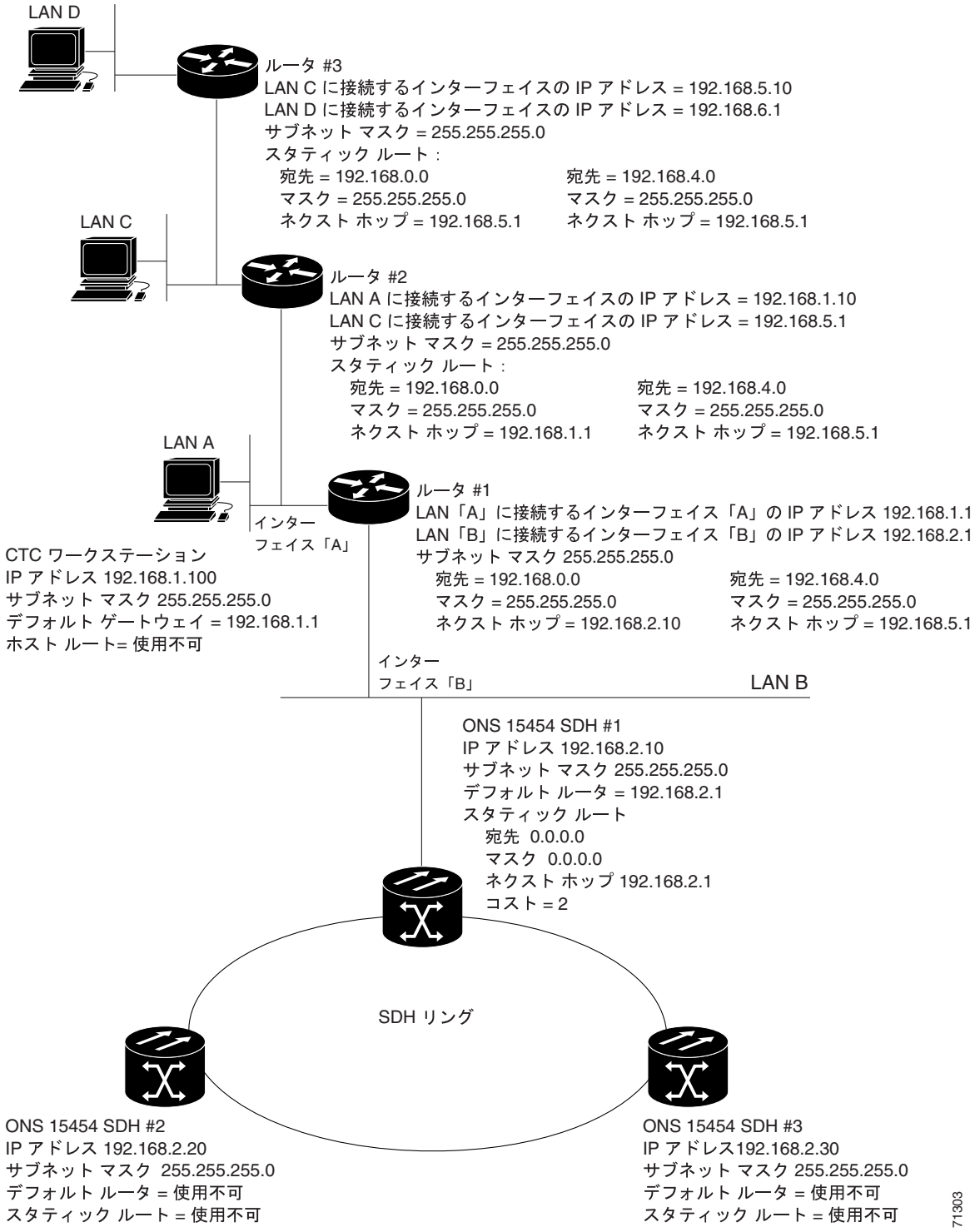


宛先エントリとサブネット マスク エントリは、ONS 15454 SDH ノードへのアクセスを制御します。

- 単一の CTC コンピュータがルータに接続されている場合は、サブネット マスク 255.255.255.255 で、宛先として完全な CTC「ホスト ルート」IP アドレスを入力します。
- サブネット上の複数の CTC コンピュータが 1 つのルータに接続されている場合は、宛先サブネット（この例では 192.168.1.0）とサブネット マスク 255.255.255.0 を入力します。
- すべての CTC コンピュータが 1 つのルータに接続されている場合は、宛先 0.0.0.0 とサブネット マスク 0.0.0.0 を入力します。図 13-7 に例を示します。

ルータ インターフェイス B の IP アドレスがネクストホップとして入力されています。コスト（発信元から宛先へのホップの数）は 2 です。

図 13-7　シナリオ 5：複数 LAN 宛先でのスタティック ルート



13.2.6　シナリオ 6：OSPF の使用

OSPF は、リンクステート ルーティング プロトコルです。リンクステート プロトコルは、「Hello プロトコル」を使用して隣接ルータでリンクを監視したり、ネイバへのリンクのステータスをテストします。リンクステート プロトコルは、直接接続されているネットワークとそのアクティブなリンクにアドバタイズします。それぞれのリンクステート ルータは、リンクステート「アドバタイズメント」を取り込み、これらをまとめてネットワーク全体のまたは領域のトポロジを作成します。ルータは、このデータベースから最短パス ツリーを構築してルーティング テーブルを計算します。ルートは、現行のトポロジの変更を反映するため、継続的に再計算されます。

ONS 15454 SDH ノードは内部 ONS 15454 SDH ネットワーク内で、ノードの検出、回線のルーティング、ノードの管理のために OSPF プロトコルを使用します。ONS 15454 SDH ノードで OSPF を使用可能にすることで、ONS 15454 SDH トポロジが LAN 上の OSPF ルータに送られます。ONS 15454 SDH ネットワーク トポロジを LAN ルータにアドバタイズすることで、ONS 15454 SDH サブネットワークのスタティック ルートを手動で入力する必要がなくなります。

OSPF は、ネットワークを、領域と呼ばれる小さな地域に分割します。領域は、トラフィック パターン別に構成されるネットワークの終端システム、ルータ、および伝送ファシリティの集合です。各 OSPF 領域には、領域 ID と呼ばれる一意の ID 番号があります。各 OSPF ネットワークには、「領域 0」と呼ばれるバックボーン領域が 1 つあります。他のすべての OSPF 領域は領域 0 に接続する必要があります。

OSPF ネットワークへのアドバタイズのために ONS 15454 SDH の OSPF トポロジを使用可能にする場合は、ONS 15454 SDH ネットワークに OSPF 領域 ID を割り当てる必要があります。LAN 管理者に相談して、割り当てる領域 ID 番号を決定してください。DCC 接続されたすべての ONS 15454 SDH ノードには、同じ OSPF 領域 ID を割り当ててください。

図 13-8 に OSPF を有効にしたネットワークを示します。

図 13-8　シナリオ 6：OSPF が有効なネットワーク

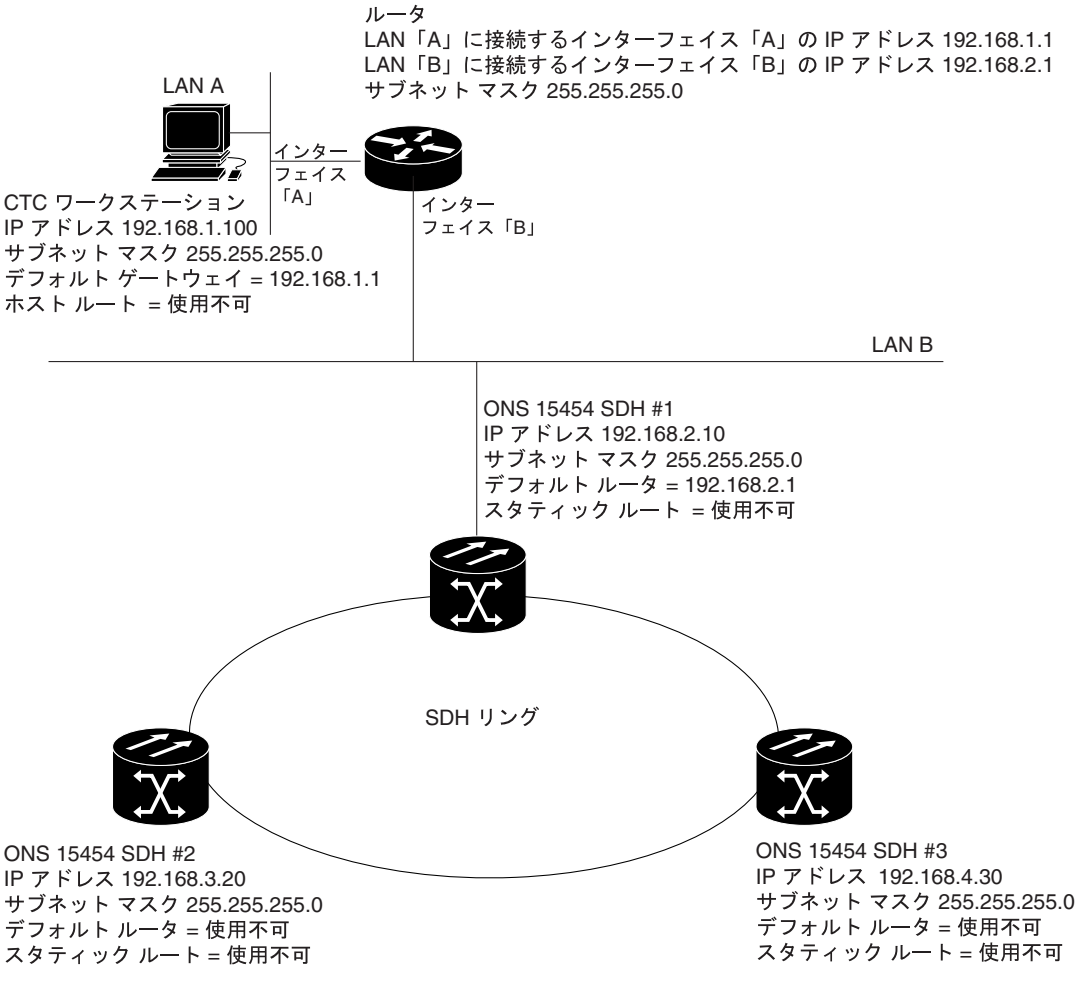
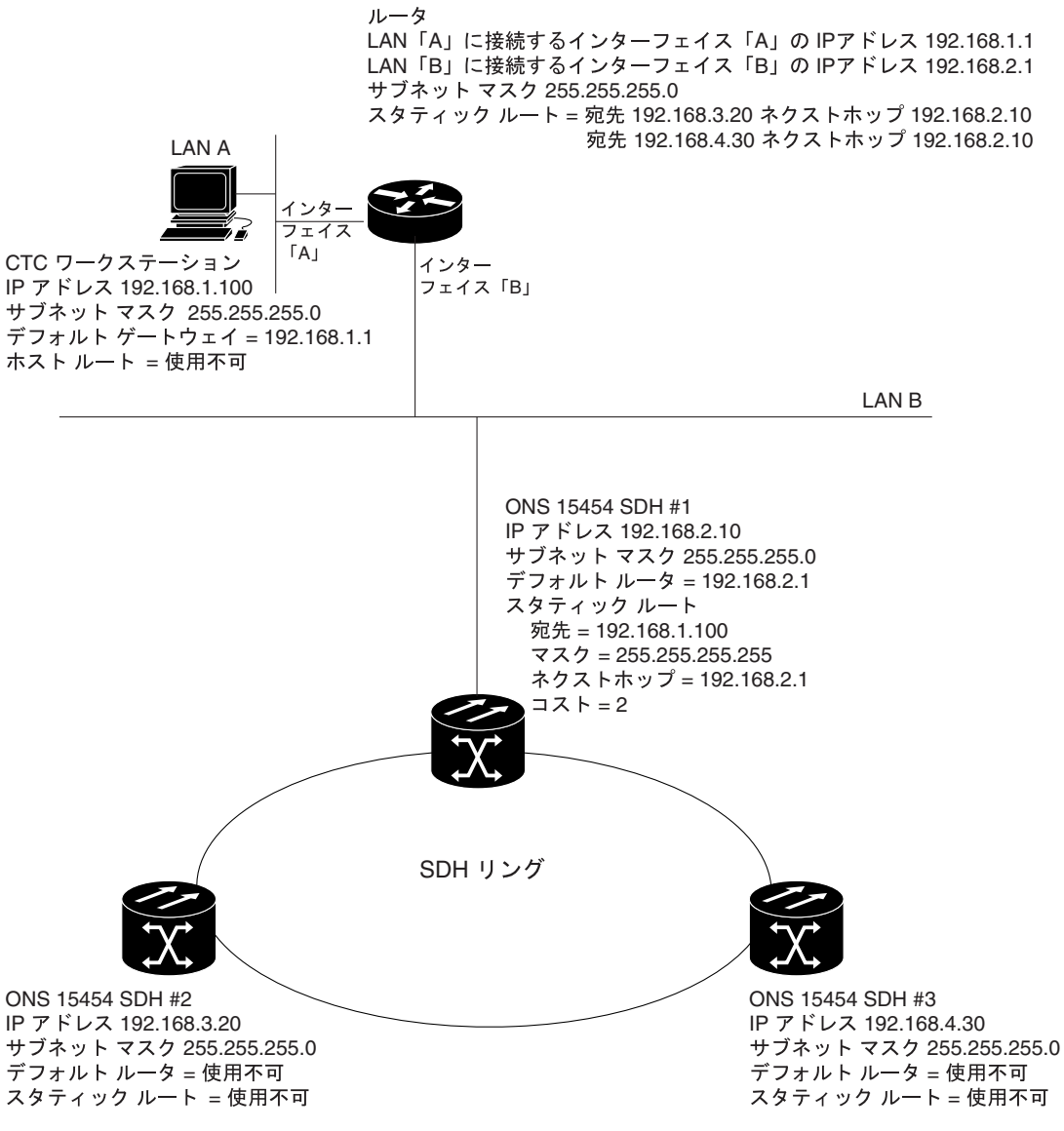


図 13-9 に OSPF のない、図 13-8 と同じネットワークを示します。スタティック ルートは、LAN A 上の CTC コンピュータが ノード #2 および #3 と通信するために手動でルータに追加する必要があります。これは、これらのノードがそれぞれ異なるサブネット上にあるためです。

図 13-9　シナリオ 6：OSPF が無効なネットワーク



13.2.7　シナリオ 7：ONS 15454 SDH プロキシ サーバのプロビジョニング

ONS 15454 SDH プロキシ サーバは機能の集まりで、ONS 15454 SDH ノードと CTC コンピュータの間の可視性とアクセス可能性を制限する必要のある環境で ONS 15454 SDH ノードのネットワーク通信を制御します。たとえば、ネットワークを設定して、現場技術者が Network Operating Center（NOC; ネットワーク オペレーティング センター）の LAN にアクセスするのを制限しながら、現場技術者と NOC の担当者が同じ ONS 15454 SDH ノードにアクセスできるようにできます。この設定を行うには、1 つの ONS 15454 SDH を GNE としてプロビジョニングし、他の ONS 15454 SDH ノードを End Network Element（ENE; 終端ネットワーク要素）としてプロビジョニングします。GNE は CTC コンピュータと ENE ONS 15454 SDH ノードの間の接続をトンネルし、ONS 15454 SDH の管理目的以外のアクセスを防止しながら管理機能を提供します。

ONS 15454 SDH プロキシ サーバは次の作業を実行します。

- DCC IP トラフィックをイーサネット（クラフト ポート）トラフィックから分離し、フィルタリング規則に基づいてパケットを受け付ける。フィルタリング規則（表 13-3 [p.13-19] と表 13-4 [p.13-20] を参照）は、パケットが ONS 15454 SDH DCC または TCC2/TCC2P イーサネット インターフェイスのどちらに着信するかによって異なります。
- Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）および Network Time Protocol（NTP; ネットワーク タイム プロトコル）の要求を処理する。ENE は、SNTP/NTP LAN サーバから GNE ONS 15454 SDH を介して Time-of-Day（ToD）を導出できます。
- SNMPv1 トラップを処理します。GNE ONS 15454 SDH は、SNMPv1 トラップを ENE ONS 15454 SDH ノードから受信し、プロビジョニングされているすべての SNMPv1 トラップ宛先に転送します。

ONS 15454 SDH プロキシ サーバは、Provisioning > Network > General タブにある、Enable proxy server on port チェックボックスを使用してプロビジョニングします（図 13-10）。プロキシを有効にすると、この ONS 15454 SDH は、このサーバへ DCC 接続されている CTC クライアントと ONS 15454 SDH 間のプロキシとして機能します。CTC クライアントはプロキシ ノードを介して DCC 接続されているノードへの接続を確立します。CTC クライアントは、CTC クライアントを動作しているホストから直接接続できないノードに、間接的に接続できます。プロキシを有効にしない場合には、確立したプロキシ接続は CTC クライアントが終了するまで継続しますが、このノードは CTC クライアントのプロキシとしては動作しません。また、プロキシ サーバを ENE または GNE として設定することができます。

- External Network Element（ENE）— ENE として設定すると、ONS 15454 SDH はデフォルト ルートやスタティック ルートに対し、確立もアドバタイズも行いません。CTC コンピュータは、TCC2/TCC2P クラフト ポートを使用して ONS 15454 SDH と通信できますが、DCC 接続された他の ONS 15454 SDH とは直接通信できません。

  また、ファイアウォールを有効にすると、このノードにより DCC と LAN ポートの間で IP トラフィックがルーティングされません。ONS 15454 SDH は、LAN ポートに接続されたマシン、または DCC によって接続されたマシンと通信できます。ただし、DCC 接続されたマシンは、LAN 接続されたマシンと通信できません。同様に、LAN 接続されたマシンは DCC 接続されたマシンと通信できません。ファイアウォール対応ノードとの接続に LAN を使用している CTC クライアントは、プロキシ機能を使用して DCC 接続されたノードを管理できます。別の方法では、この DCC 接続されたノードに到達することはできません。DCC 接続されたノードに接続されている CTC クライアントは、他の DCC 接続されたノードとファイアウォールそのものだけを管理できます。
- Gateway Network Element（GNE）— GNE として設定すると、CTC コンピュータは、他の DCC 接続されたノードと通信できるようになり、ファイアウォールが有効になります。
- Proxy-only — このチェック ボックスを選択すると、CTC は他の DCC 接続された ONS 15454 SDH と通信できなくなり、ファイアウォールも無効になります。

（注）　Network Address Translation（NAT; ネットワーク アドレス変換）または Port Address Translation（PAT; ポート アドレス変換）ルータを介してノードに対して CTC を起動し、そのノードでプロキシが使用可能になっていない場合は、CTC セッションが開始され、最初は問題なく動作しているように見えます。ただし、CTC はアラームの更新を受け取ることなく、2 分ごとに切断と再接続を繰り返します。プロキシが誤って使用不可になった場合は、再接続時にプロキシを使用可能にして、NAT/PAT ファイアウォールを介した場合を含め、ノードの管理機能を回復することができます。

（注）　別のプライベート サブネットワークに属する ENE は、一意の IP アドレスを持つ必要はありません。異なる GNE に接続された 2 つの ENE は、同じ IP アドレスを持つことができます。ただし、同じ GNE に接続する ENE は、常に一意の IP アドレスを持つ必要があります。

図 13-10　プロキシ サーバ ゲートウェイの設定

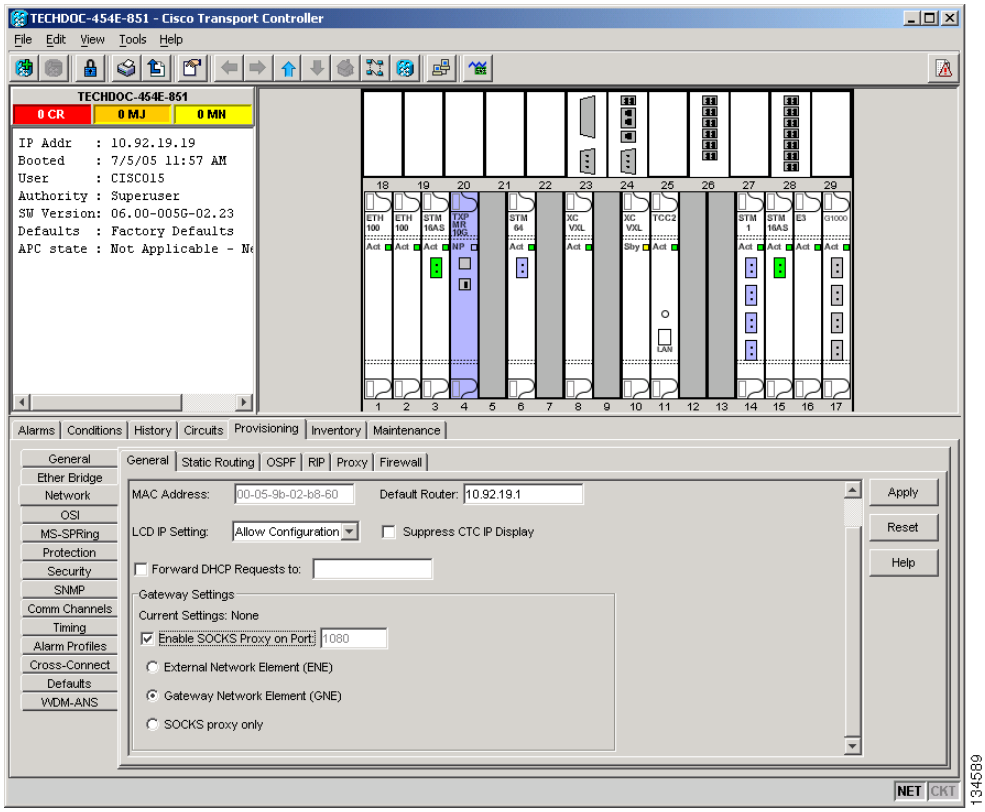


図 13-11 に、ONS 15454 SDH プロキシ サーバの実装を示します。GNE ONS 15454 SDH は、セントラル オフィス LAN と ENE ONS 15454 SDH ノードに接続されています。セントラル オフィス LAN は、CTC コンピュータを備えた NOC LAN に接続されています。NOC CTC コンピュータと技術者が、ONS 15454 SDH ENE にアクセスできる必要があります。ただし、技術者が NOC やセントラル オフィス LAN にアクセスしたりするのを制限する必要があります。

この例では、ONS 15454 SDH GNE はセントラル オフィス LAN の範囲内の IP アドレスが割り当てられ、その LAN ポートによって LAN に物理的に接続されています。ONS 15454 SDH ENE には、セントラル オフィス LAN の範囲外の IP アドレスが割り当てられ、プライベート ネットワークの IP

アドレスが割り当てられています。複数の ONS 15454 SDH ENE が 1 つの場所に設置されている場合は、クラフト LAN ポートをハブに接続できます。ただし、ハブが他のネットワークに接続されていないようにします。

図 13-11　シナリオ 7：同一サブネット上にある GNE と ENE を使用した SDH プロキシ サーバ

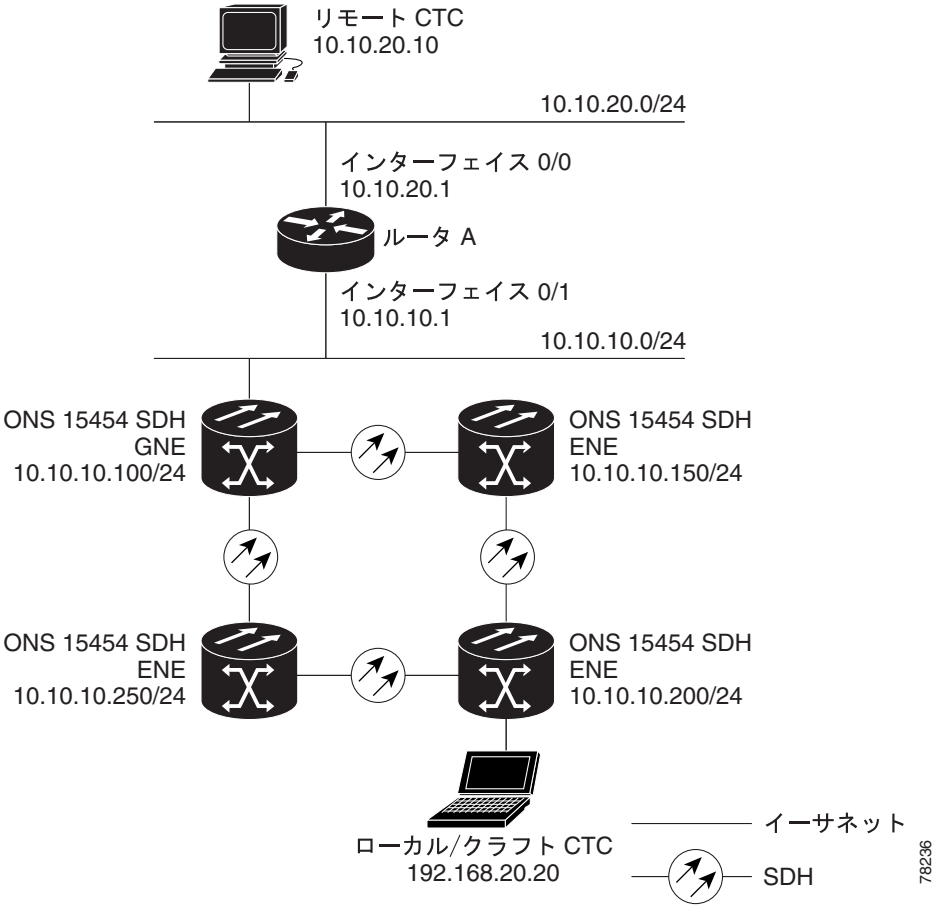


表 13-2 に、図 13-11 の構成での ONS 15454 SDH GNE および ENE の推奨する設定を示します。

表 13-2　ONS 15454 SDH GNE および ENE の設定

設定	ONS 15454 SDH GNE	ONS 15454 SDH ENE
Craft Access Only	オフ	オン
Enable Proxy	オン	オン
Enable Firewall	オン	オン
OSPF	オフ	オフ
SNTP Server（使用している場合）	SNTP サーバ の IP アドレス	ONS 15454 SDH GNE の IP アドレスに設定
SNMP（使用している場合）	SNMPv1 トラップ宛先	SNMPv1 トラップ宛先を ONS 15454 SDH GNE、ポート 391 に設定

図 13-12 に、異なるサブネット上にある ONS 15454 SDH ENE を使用した、同じプロキシ サーバの実装を示します。この例では、ONS 15454 SDH GNE と ENE は表 13-2 に示す設定でプロビジョニングされます。

図 13-12　シナリオ 7：異なるサブネット上にある GNE と ENE を使用した ONS 15454 SDH プロキシ サーバ

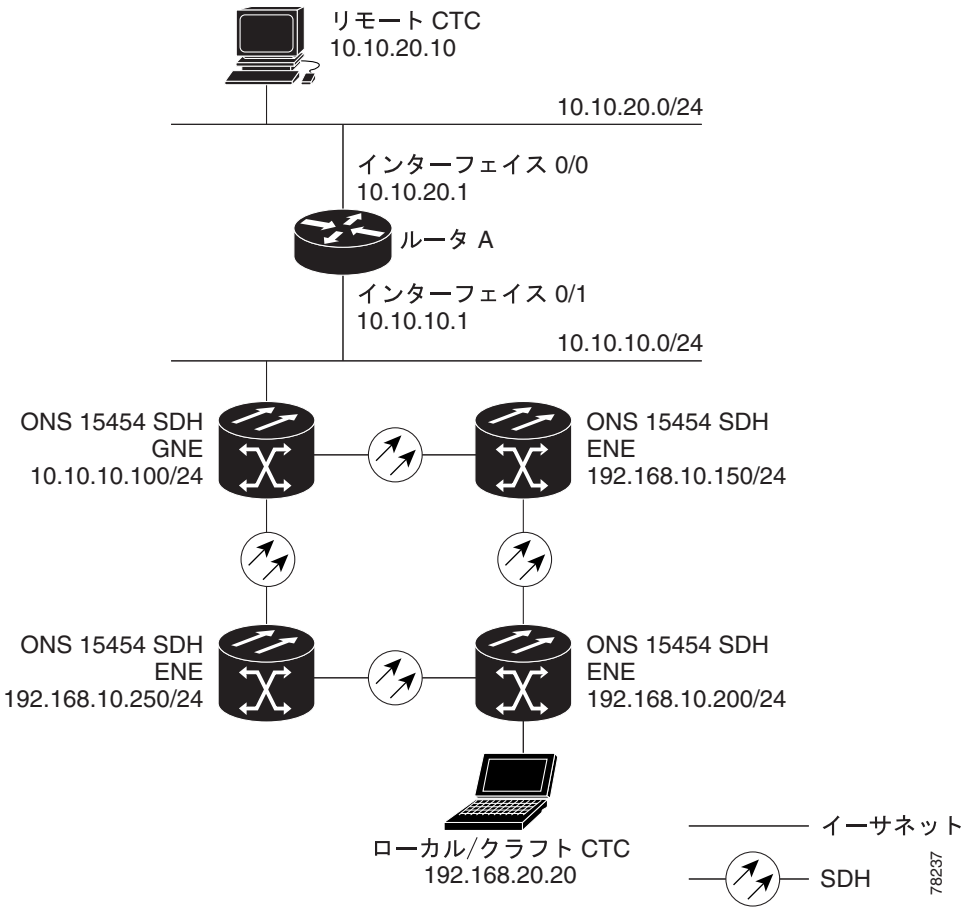


図 13-13 に、ONS 15454 SDH ENE が複数のリングにある場合の実装例を示します。この例では、ONS 15454 SDH GNE と ENE は表 13-2 に示す設定でプロビジョニングされます。

図 13-13　シナリオ 7：ENE が複数のリングにある ONS 15454 SDH プロキシ サーバ

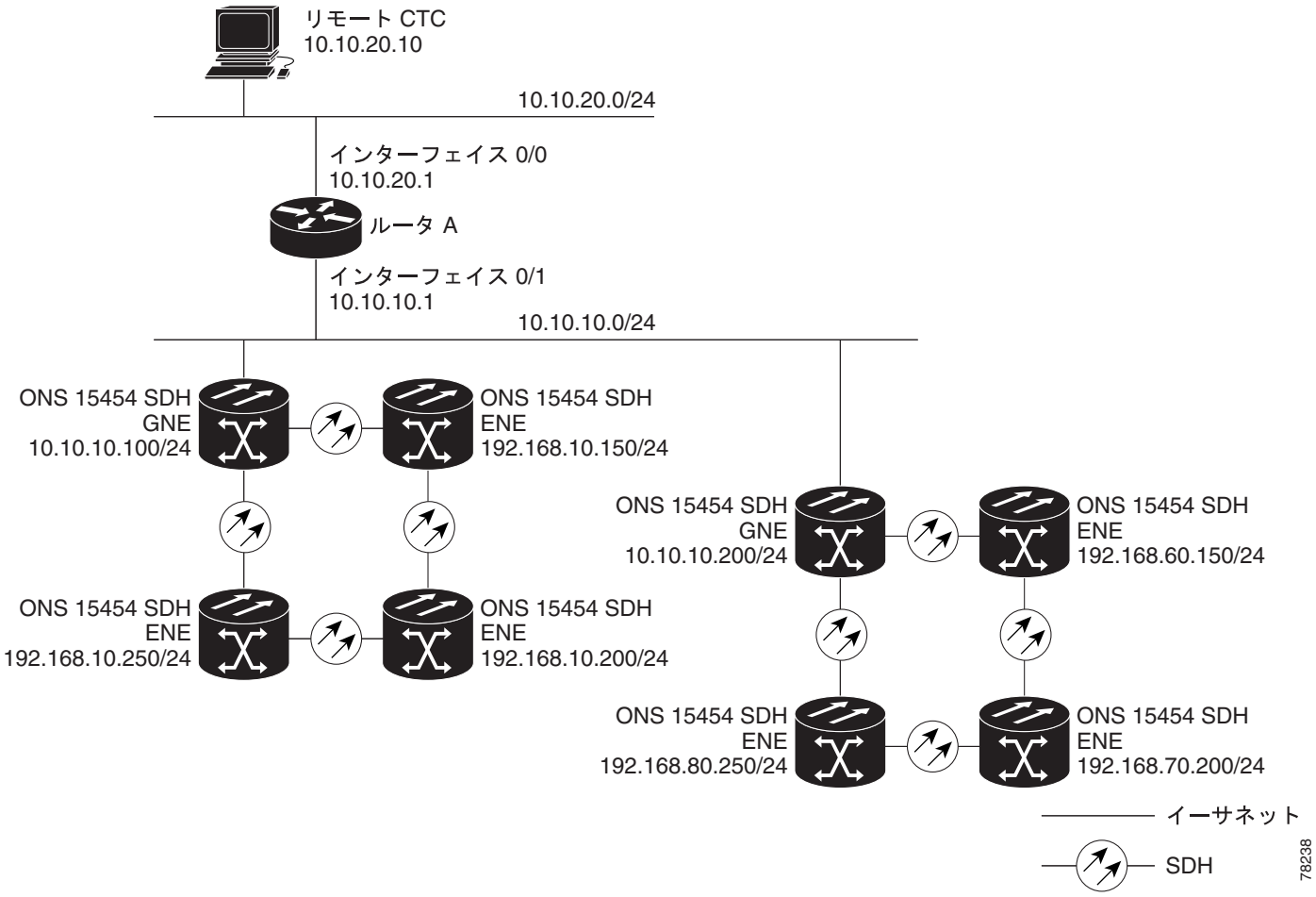


表 13-3 に、Enable Firewall チェックボックスを選択した場合に ONS 15454 SDH が従うパケットのフィルタリング規則を示します。

表 13-3　プロキシ サーバのファイアウォール フィルタリング規則

パケットの着信先	パケットを受け付けるための IP 宛先アドレスの条件
TCC2/TCC2P イーサネット インターフェイス	• ONS 15454 SDH 自身の IP アドレス • ONS 15454 SDH ノードのサブネット ブロードキャスト アドレス • 224.0.0.0/8 ネットワーク内のアドレス（標準マルチキャスト メッセージで使用するために予約されているネットワーク） • サブネット マスク = 255.255.255.255
DCC インターフェイス	• ONS 15454 SDH 自身の IP アドレス • 別の DCC インターフェイスで接続されている宛先 • 224.0.0.0/8 ネットワーク内のアドレス

パケットの宛先が ONS 15454 SDH の場合は、追加の規則が適用されます（表 13-4）。拒否されたパケットは報告せずに、そのまま廃棄されます。

表 13-4　パケットの宛先が ONS 15454 SDH の場合のプロキシ サーバのファイアウォール フィルタリング規則

パケットの着信先	許可	拒否
TCC2/TCC2P イーサネット インターフェイス	• Rejected 欄以外のすべての UDP パケット	• SNMP トラップ リレー ポート（391）宛ての UDP パケット
DCC インターフェイス	• すべての UDP パケット • 宛先が Telnet および SOCKS プロキシ サーバ ポート以外のすべての TCP パケット • OSPF パケット • ICMP パケット	• Telnet ポート宛ての TCP パケット • プロキシ サーバ ポート宛ての TCP パケット • UDP、TCP、OSPF、および ICMP 以外の全パケット

プロキシ サーバを実装する際には、次の規則に留意してください。

- 同一イーサネット セグメント上の DCC 接続されたすべての ONS 15454 SDH ノードでは、Craft Access Only 設定を同じにする必要があります。これらの設定が異なると予測できない結果となり、共用イーサネット セグメントでいくつかのノードが到達不可能になる場合があります。
- 同一イーサネット セグメント上の DCC 接続されたすべての ONS 15454 SDH ノードでは、Enable Firewall 設定を同じにする必要があります。これらの設定が異なる場合は、予測できない結果となります。いくつかのノードが到達不可能になる場合があります。
- Enable Firewall を有効にする場合は、必ず Enable Proxy も選択します。Enable Proxy を選択しない場合には、CTC は ONS 15454 SDH の DCC 側のノードにアクセスできなくなります。
- Craft Access Only を選択する場合は、必ず Enable Proxy も選択します。Enable Proxy を選択しない場合には、CTC は ONS 15454 SDH の DCC 側のノードにアクセスできなくなります。

上記の 1、2、3 の場合でノードが到達不可能になったときは、次のどちらかの動作を実行して設定を修正できます。

- 到達不可能となった ONS 15454 SDH からクラフト コンピュータを接続解除します。到達不可能となった ONS 15454 SDH に DCC 接続されているネットワークの別の ONS 15454 SDH を介して、到達不可能な ONS 15454 SDH に接続します。
- 到達不可能となった ONS 15454 SDH からイーサネット ケーブルを外します。CTC コンピュータを ONS 15454 SDH へ直接接続します。

13.2.8　シナリオ 8：サブネット上のデュアル GNE

ONS 15454 SDH は、GNE のロードバランシングに対応しており、ENE を OSPF によってアドバタイズすることなく、複数の GNE を介して CTC は ENE へ接続できます。この機能により、GNE が異なるサブネット上にある場合でも、GNE の障害から迅速に回復できます。1 つの GNE が停止すると、その GNE を介した接続はすべて失敗します。CTC は、障害の発生した GNE とその GNE がプロキシとなっているすべての ENE から切り離され、残りの GNE を通じて再接続されます。GNE ロードバランシング によって、起動側 GNE と DCC の帯域幅への依存度は少なくなります。これによって CTC のパフォーマンスが向上します。図 13-14 に、同じサブネットにデュアル GNE のあるネットワークを示します。

図 13-14　シナリオ 8：同一サブネット上のデュアル GNE

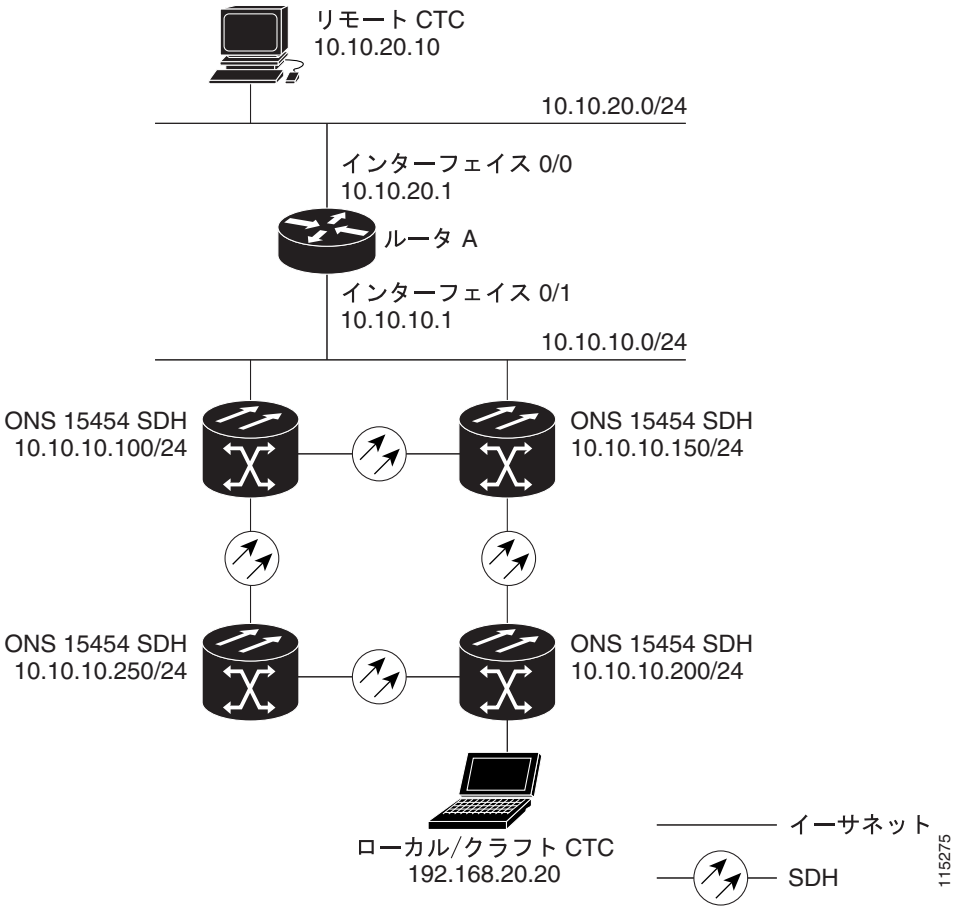
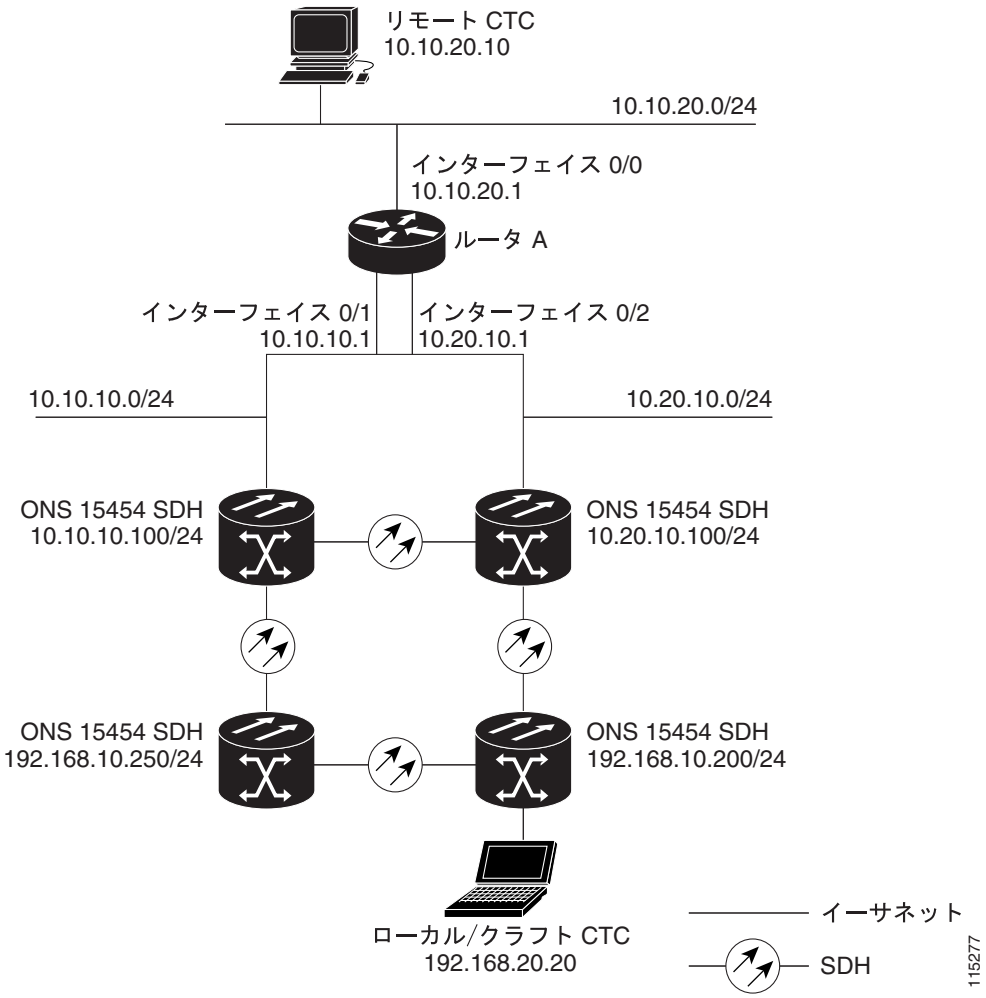


図 13-15 に異なるサブネット上にデュアル GNE のあるネットワークを示します。

図 13-15　シナリオ 8：異なるサブネットのデュアル GNE



13.2.9　シナリオ 9：セキュア モードを有効にした IP アドレッシング

TCC2 カードと TCC2P カードは、いずれもノンセキュア モードがデフォルトです。このモードでは、前面の TCP/IP および MIC-C/T/P イーサネット（LAN）ポートは、単一の MAC アドレスと IP アドレスを共有します。TCC2P カードを使用すると、ノードをセキュア モードにすることができます。このモードでは、クラフト ポート ユーザが MIC-C/T/P ポートから LAN にアクセスすることはできません。セキュア モードはロックすることにより、モードの変更を禁止できます。ノードをセキュア モードにする、またはセキュア ノードをロックする場合は、『*Cisco ONS 15454 SDH Procedure Guide*』の「Change Node Settings」の章を参照してください。

13.2.9.1　セキュア モードの動作

TCC2P ノードをノンセキュア モードからセキュア モードに変更すると、ONS 15454 SDH に 2 つの IP アドレスをプロビジョニングでき、ノードでは各ポートに対して異なる MAC アドレスが割り当てられます。セキュア モードでは、ONS 15454 SDH の MIC-C/T/P イーサネット（LAN）ポートに

対して 1 つの IP アドレスがプロビジョニングされ、TCC2P イーサネット ポートに対してもう 1 つの IP アドレスがプロビジョニングされます。両アドレスは異なるサブネットに属するため、クラフト アクセス ポートと ONS 15454 SDH LAN 間を分離するレイヤが追加されます。セキュア モードが有効である場合、両方の TCP/IP ポートにプロビジョニングされる IP アドレスは、IP アドレッシングの一般的ガイドラインに準拠している必要があり、いずれも他方の IP アドレスおよびデフォルト ルータの IP アドレスとは異なるサブネットに属する必要があります。

セキュア モードでは、MIC-C/T/P イーサネット（LAN）ポートに割り当てられる IP アドレスがプライベート アドレスになる一方、バックプレーンはセントラル オフィスの LAN または企業の専用ネットワークを通じてノードを Operations Support System（OSS）に接続します。スーパーユーザはノードを設定することにより、CTC、ルーティング テーブル、または自律メッセージ レポートにおける MIC-C/T/P のイーサネット（LAN）IP アドレスの表示 / 非表示を切り替えることができます。

ノンセキュア モードでは、ノードは GNE または ENE になります。ノードをセキュア モードにすると、SOCKS プロキシが自動的にオンになり、そのノードのデフォルトは GNE ステータスになります。ただし、ノードを ENE に変更することは可能です。ノンセキュア モードでは、ENE の SOCKS プロキシを無効にすることができます（ノードは事実上、LAN ファイアウォールにより隔離されます）。ただし、セキュア モードでは無効にすることはできません。ノードの GNE または ENE ステータスを変更し、SOCKS プロキシを無効にする場合は、『*Cisco ONS 15454 SDH Procedure Guide*』の「Turn Up a Node」の章を参照してください。

注意　セキュア モードを有効にすると、TCC2P カードが再起動します。TCC2P カードの再起動はトラフィックに影響を与えます。

（注）　TCC2 カードが取り付けられていない場合、セキュア モード オプションは CTC に表示されません。1 つの TCC2 カードと 1 つの TCC2P カードがノードに取り付けられている場合は、セキュア モードが CTC に表示されますが、変更することはできません。

（注）　（ユーザのプロビジョニングやネットワークの障害のために）TCC2P TCP/IP ポートと MIC-C/T/P ポートが ENE で無効になり、そのノードが DCC 通信から隔離されている場合、両方のポートは自動的に再有効化されます。

図 13-16 に、TCC2P TCP/IP ポート アドレスが同一サブネットに属する、セキュア モードの ONS 15454 SDH ノードの例を示します。

図 13-16　シナリオ 9 : セキュア モードを有効にした同一サブネット上の ONS 15454 SDH GNE および ENE

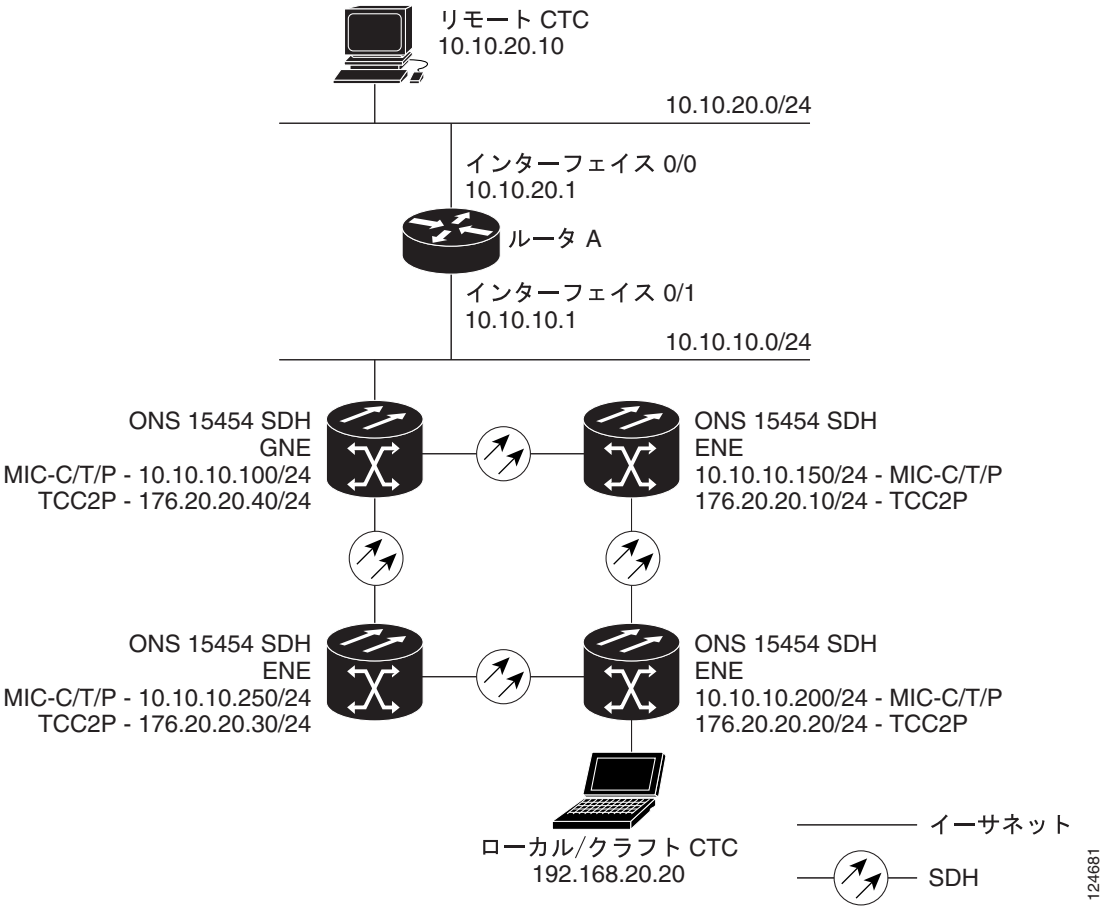
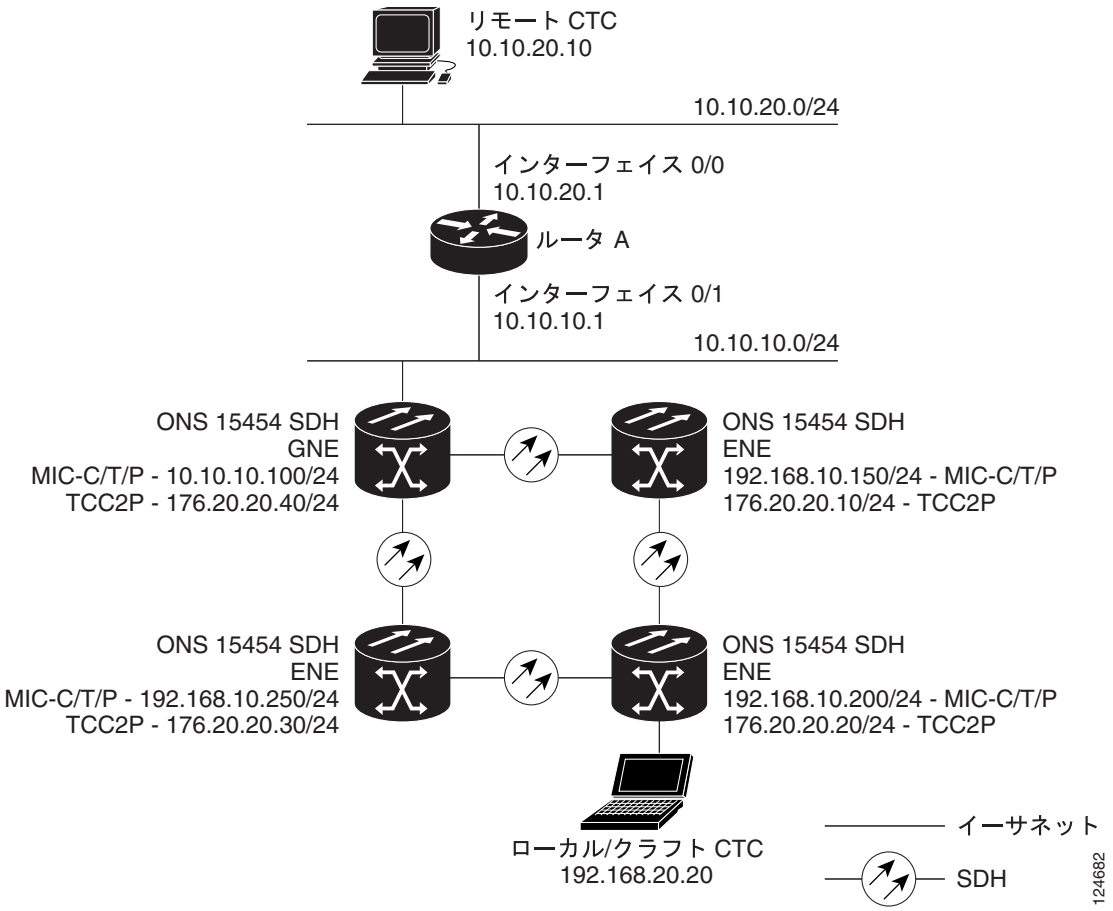


図 13-17 に、セキュア モードを有効にした、ルータに接続された ONS 15454 SDH ノードの例を示します。各例では、ノードの TCC2P ポート アドレス（ノード アドレス）は、ノードの MIC-C/T/P IP アドレスとは異なるサブネットに属しています。

図 13-17　シナリオ 9 : セキュア モードを有効にした異なるサブネット上の ONS 15454 SDH GNE および ENE



13.2.9.2　セキュア ノードのロック時およびロック解除時の動作

ノードのセキュア モードは、ロック モードまたはロック解除モードのいずれかで動作できます。デフォルトでは、セキュア モードのステータスはロック解除です。それをロック モードに変更できるのは、スーパーユーザだけです。ロック モードに変更すると、アクティブおよびスタンバイ TCC2P カードとシャーシのハードウェア コンフィギュレーションは永久的に変更されます。

カードとシェルフは互いに分離してもロック ステータスを維持するため、ロック モードは慎重に使用する必要があります。たとえば、ノードがセキュアなロック モードにあるときにスタンバイ TCC2P カードを取り外し、それを別のノードにアクティブ カードとして取り付けると、セキュアなロック モードがその新しいノードのシャーシとスタンバイ TCC2P に書き込まれます。セキュアなロック ノードのアクティブおよびスタンバイ TCC2P カードを取り外し、以前はロック解除モードにあったシャーシに両方のカードを取り付けると、そのノードはロック状態になります。

セキュアなロック モードにあるときは、ノードのコンフィギュレーション、イーサネット ポートのステータス、セキュア モード、およびロック ステータスは、スーパーユーザを含むどのネットワーク ユーザによっても変更できません。セキュア ノードのロックを解除するには、シスコのテクニカル サポートに連絡し、シャーシと TCC2P の Return Material Authorization（RMA; 返品許可）を手配します。必要に応じて、「マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン」（p.xxiv）を参照してください。

注意　TCC2P とシャーシは、同時にロック解除する必要があります。1 つのコンポーネント（シェルフなど）だけをロック解除しても、システムはロック モードに戻ります。

13.3　ルーティング テーブル

ONS 15454 SDH のルーティング情報は Maintenance > Routing Table タブで表示されます。ルーティング テーブルには、次の情報が表示されます。

- Destination — 宛先のネットワークまたはホストの IP アドレスを表示します。
- Mask — 宛先のホストまたはネットワークに到達するために使用するサブネット マスクを表示します。
- Gateway — 宛先のネットワークまたはホストに到達するために使用するゲートウェイの IP アドレスを表示します。
- Usage — リストされたルートの使用回数を表示します。
- Interface — 宛先にアクセスするために使用する ONS 15454 SDH インターフェイスを表示します。値は次のとおりです。
  - motfcc0 — ONS 15454 SDH イーサネット インターフェイス、つまり TCC2/TCC2P カード上の RJ-45 ジャックと MIC-C/T/P FMEC 上の LAN 接続
  - pdcc0 — DCC/OSC/GCC インターフェイス
  - lo0 — ループバック インターフェイス

表 13-5 に、ONS 15454 SDH のルーティング テーブルのエントリの例を示します。

表 13-5　ルーティング テーブルのエントリの例

エントリ	宛先	マスク	ゲートウェイ	インターフェイス
1	0.0.0.0	0.0.0.0	172.20.214.1	motfcc0
2	172.20.214.0	255.255.255.0	172.20.214.92	motfcc0
3	172.20.214.92	255.255.255.255	127.0.0.1	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	pdcc0

エントリ 1 の内容は次のとおりです。

- 宛先（0.0.0.0）：デフォルトのルート エントリです。ルーティング テーブル内のすべての未定義宛先ネットワークまたは宛先ホスト エントリはデフォルトのルート エントリにマップされます。
- マスク（0.0.0.0）：常にデフォルト ルートを示す 0 です。
- ゲートウェイ（172.20.214.1）：デフォルトのゲートウェイ　アドレスです。このルーティング テーブルにないすべての送信トラフィック、またはノードのローカル サブネットにない送信トラフィックは、このゲートウェイに送信されます。
- インターフェイス（motfcc0）：ゲートウェイに到達するために ONS 15454 SDH イーサネット インターフェイスを使用することを示します。

エントリ 2 の内容は次のとおりです。

- 宛先（172.20.214.0）：宛先ネットワーク IP アドレスです。
- マスク（255.255.255.0）：24 ビット マスクで、172.20.214.0 サブネット内のすべてのアドレスが宛先となります。
- ゲートウェイ（172.20.214.92）：ゲートウェイ　アドレスです。このネットワークに属するすべての送信トラフィックは、このゲートウェイに送信されます。
- インターフェイス（motfcc0）：ゲートウェイに到達するために ONS 15454 SDH イーサネット インターフェイスを使用することを示します。

エントリ 3 の内容は次のとおりです。

- 宛先（172.20.214.92）：宛先ホスト IP アドレスです。

- マスク（255.255.255.255）：32 ビット マスクで、アドレス 172.20.214.92 だけが宛先であることを示します。
- ゲートウェイ（127.0.0.1）：ループバック　アドレスです。このホストは、このアドレスを使用してネットワーク トラフィックを自身に送信します。
- インターフェイス（lo0）：ゲートウェイに到達するためにローカル ループバック インターフェイスを使用することを示します。

エントリ 4 の内容は次のとおりです。

- 宛先（172.20.214.93）：宛先ホスト IP アドレスです。
- マスク（255.255.255.255）：32 ビット マスクで、アドレス 172.20.214.93 だけが宛先であることを示します。
- ゲートウェイ（0.0.0.0）：宛先ホストがノードに直接接続されていることを意味します。
- インターフェイス（pdcc0）：宛先ホストに到達するために SDH RS-DCC インターフェイスを使用することを示します。

エントリ 5 は、直接接続されていないノードを介してアクセス可能な DCC 接続されたノードを示します。

- 宛先（172.20.214.94）：宛先ホスト IP アドレスです。
- マスク（255.255.255.255）：32 ビット マスクで、アドレス 172.20.214.94 だけが宛先であることを示します。
- ゲートウェイ（172.20.214.93）：IP アドレスが 172.20.214.93 であるノードによって宛先ホストがアクセスされることを示します。
- インターフェイス（pdcc0）：ゲートウェイに到達するために SDH RS-DCC インターフェイスを使用することを示します。

13.4　外部ファイアウォール

ここでは、外部ファイアウォールの Access Control List（ACL; アクセス制御リスト）の例を示します。表 13-6 は、TCC2/TCC2P カードで使用するポートの一覧です。

表 13-6　TCC2/TCC2P で使用するポート

ポート	機能	アクション[1]
0	未使用	D
20	FTP	D
21	FTP の制御	D
22	SSH（セキュア シェル）	D
23	Telnet	D
80	HTTP	D
111	SUNRPC（Sun Remote Procedure Call）	NA
161	SNMP トラップ宛先	D
162	SNMP トラップ宛先	D
513	rlogin	D
683	CORBA IIOP	OK
1080	プロキシ サーバ（socks）	D
2001 ～ 2017	I/O カード Telnet	D
2018	アクティブな TCC2/TCC2P での DCC プロセッサ	D
2361	TL1	D
3082	Raw TL1	D
3083	TL1	D
5001	BLSR サーバ ポート	D
5002	BLSR クライアント ポート	D
7200	SNMP アラーム入力ポート	D
9100	EQM ポート	D
9401	TCC ブート ポート	D
9999	フラッシュ マネージャ	D
10240 ～ 12287	プロキシ クライアント	D
57790	デフォルトの TCC リスナー ポート	OK

1.　D = deny（拒否）、NA = not applicable（適用なし）、OK = 拒否しない

次に示す ACL の例では、プロキシ サーバのゲートウェイ設定が有効でない場合のファイアウォールの設定を示しています。この例では、CTC ワークステーションのアドレスは 192.168.10.10 で、ONS 15454 SDH のアドレスは 10.10.10.100 です。ファイアウォールは GNE CTC に接続されているため、受信は CTC から GNE へ、送信は GNE から CTC へと送られます。CTC の Common Object Request Broker Architecture（CORBA）標準定数が 683、TCC CORBA デフォルトが TCC 固定（57790）です。

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 any host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with ONS 15454 SDH using http (port
80) access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with ONS 15454 SDH GNE (port
57790)
***
access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 any host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from ONS 15454 SDH (random port) to the
CTC workstation (port 683) ***
access-list 100 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from ONS 15454 SDH GNE to CTC ***
```

次に示す ACL の例では、プロキシ サーバのゲートウェイ設定が有効な場合のファイアウォール設定を示しています。最初の例と同様に、CTC ワークステーションのアドレスは 192.168.10.10、ONS 15454 SDH のアドレスは 10.10.10.100 です。ファイアウォールは GNE CTC に接続されているため、受信が CTC から GNE、送信が GNE から CTC へと送られます。CTC CORBA 標準定数が 683、TCC CORBA デフォルトが TCC 固定（57790）です。

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 any host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15454 SDH using http (port
80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with the 15454 SDH GNE (port
57790) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15454 SDH GNE proxy
server (port 1080) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 683 host 10.10.10.100 range 10240 10495
access-list 100 remark *** allows CTC communication with the 15454 SDH ENEs (ports
10240 - 10495) via the GNE proxy server
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 established
access-list 100 remark *** allows ACKs from CTC to the 15454 SDH GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 any host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms and other communications from the 15454 SDH
(random port) to the CTC workstation
(port 683) ***
access-list 100 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15454 SDH GNE to CTC ***
```

13.5　オープン GNE

ONS 15454 SDH は、自動ノードおよびリンク検出にとって必要な、PPP（ポイントツーポイント プロトコル）ベンダー拡張や OSPF タイプ 10 の不明瞭な Link-State Advertisement（LSA; リンクステート アドバタイズ）をサポートしない、ONS 以外のノードとも通信できます。オープン GNE 構成では、DCC ベースのネットワークが ONS 以外のノードの IP ネットワークとして機能できます。

オープン GNE ネットワークを構成するためには、RS-DCC、MS-DCC、および GCC 終端を、デフォルト IP アドレスの 0.0.0.0 か、指定した IP アドレスのいずれかを使用して、遠端の ONS 以外のノードを含めるようにプロビジョニングします。遠端の ONS 以外のノードは RS-DCC、MS-DCC、および GCC の作成の際に「Far End is Foreign」チェックボックスをチェックすることでプロビジョニングできます。デフォルトの 0.0.0.0 の IP アドレスを設定することによって、遠端の ONS 以外のノードに IP アドレスを割り当てることができます。0.0.0.0 以外の IP アドレスを設定すると、遠端ノードがその IP アドレスで自身を識別できる場合だけリンクが確立され、それによって、セキュリティのレベルが向上します。

デフォルトでは、プロキシ サーバは検出した ONS ピアとの接続だけを許可します。ファイアウォールは、DCC ネットワークと LAN の間のすべての IP トラフィックをブロックします。ただし、プロキシ トンネルを、ONS 以外のノードへの SOCKS バージョン 5 接続のための最大 12 の追加の宛先を許可するようにプロビジョニングできます。また、ファイアウォール トンネルを、DCC ネットワークと LAN 間の直接 IP 接続のための最大 12 の追加の宛先を許可するようにプロビジョニングすることもできます。プロキシ トンネルとファイアウォール トンネルには 送信元と宛先の両方のサブネットを含めることができます。コネクションは、送信元サブネット内から開始し宛先サブネット内で終わる必要があります。そうでない場合、SOCKS 接続や IP パケット フローはいずれも許可されません。

CTC でプロキシ サブネットとファイアウォール サブネットを設定するには、Provisioning > Network > Proxy and Firewalls サブタブを使用します。プロキシ トンネルやファイアウォール トンネルの利用の可否は、次のように、ノードのネットワーク アクセス設定によって異なります。

- ノードが GNE または ENE モードでプロキシ サーバを有効にして設定されている場合、プロキシ トンネルかファイアウォール トンネル、またはその両方を設定する必要があります。
- ノードがプロキシ専用モードでプロキシ サーバを有効にして設定されている場合、プロキシ トンネルを設定できます。ファイアウォール トンネルは設定できません。
- ノードがプロキシ　サーバを無効にして設定されている場合、プロキシ　トンネルもファイアウォール トンネルも設定できません。

図 13-18 に、DCC ネットワークに接続された外部ノードの例を示します。この例では、プロキシ トンネルとファイアウォール トンネルが有効に機能します。これらを使用しないと、GNE によって PC と外部ノードの間の IP アクセスはブロックされます。

図 13-18　異種終端でのプロキシ トンネルとファイアウォール トンネル

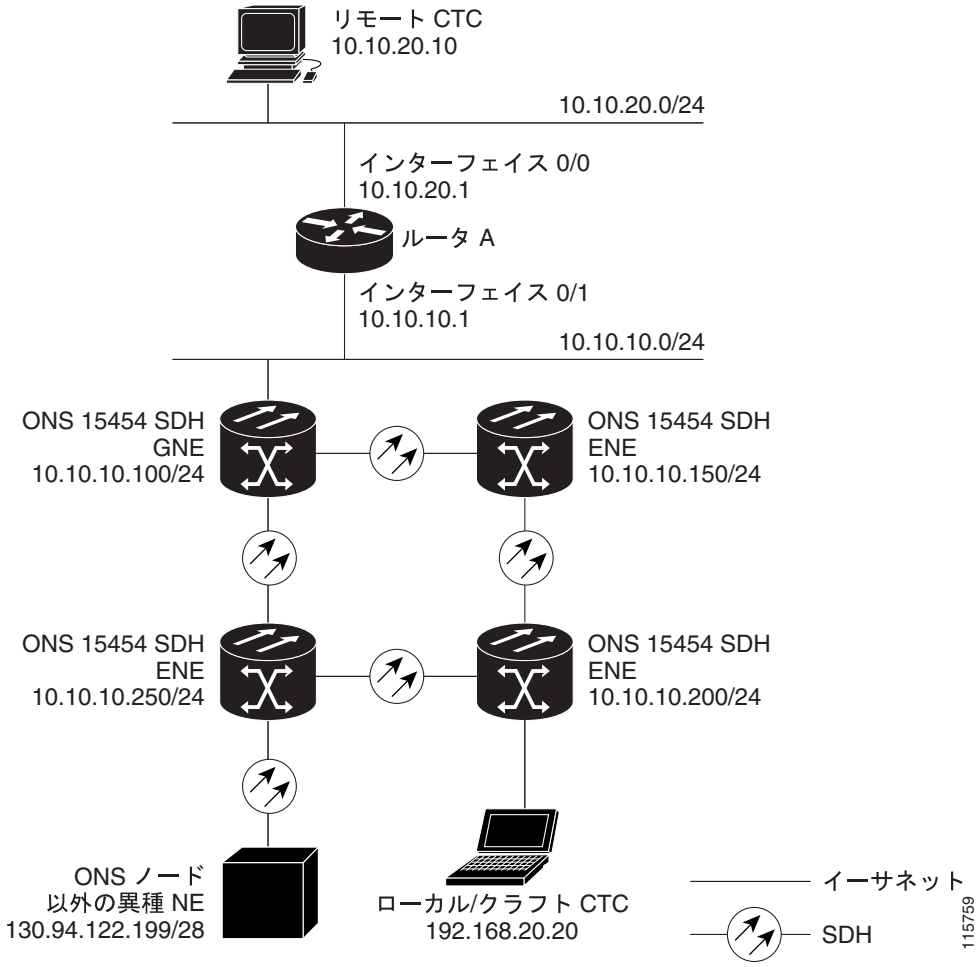
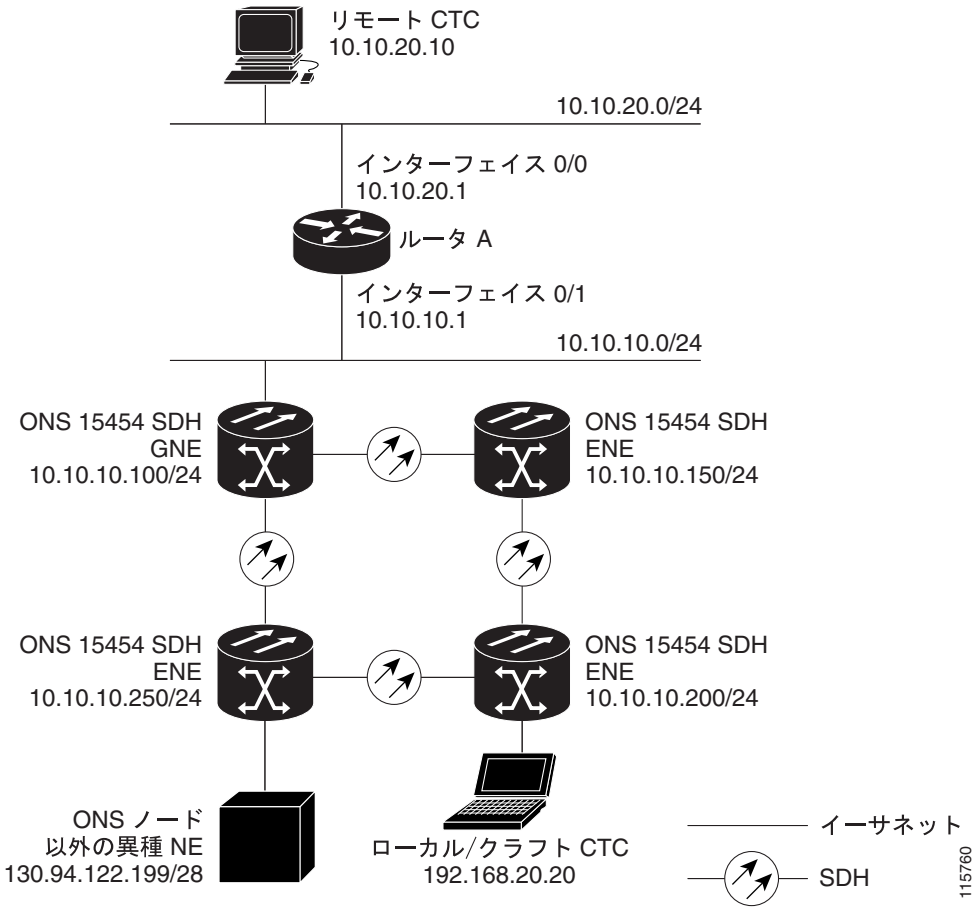


図 13-19 に、ENE イーサネット ポートに接続されたリモート ノードを示します。この例では、プロキシ トンネルとファイアウォール トンネルが有効に機能します。これらを使用しないと、GNE によって PC と異種ノードの間の IP アクセスはブロックされます。この構成では ENE 上にファイアウォール トンネルも必要です。

図 13-19　ENE イーサネット ポートへの異種ノード接続



13.6　TCP/IP および OSI ネットワーキング

ONS 15454 DCN 通信は、TCP/IP プロトコル スイートに基づいています。ただし、ONS 15454 SDH ノードは、OSI プロトコル スイートを使用する機器で接続することもできます。TCP/IP プロトコルと OSI プロトコルは直接の互換性がありませんが、それらは同じ目的を持ち、OSI 参照モデルの同様のレイヤを占有します。表 13-7 に、TCP/IP ベースの NE が OSI ベースの NE とネットワーク接続されている場合の各プロトコルとメディエーション プロセスを示します。

表 13-7　TCP/IP および OSI プロトコル

<table>
<tr><th>OSI モデル</th><th>IP プロトコル</th><th colspan="2">OSI プロトコル</th><th>IP と OSI 間の
メディエーション</th></tr>
<tr><td>レイヤ 7 アプリケーション</td><td>• TL1
• FTP
• HTTP</td><td rowspan="4">• TARP[1]</td><td>• TL1-over-OSI
• FTAM[2]
• ACSE[3]</td><td>• T–TD[4]
• FT–TD[5]</td></tr>
<tr><td>レイヤ 6 プレゼンテーション</td><td rowspan="2">• Telnet
• IIOP</td><td>• PST[6]</td><td></td></tr>
<tr><td>レイヤ 5 セッション</td><td>• Session</td><td></td></tr>
<tr><td>レイヤ 4 トランスポート</td><td>• TCP
• UDP</td><td>• TP（トランスポート）クラス 4</td><td rowspan="3">• IP-over-CLNS[7] トンネル</td></tr>
<tr><td>レイヤ 3 ネットワーク</td><td>• IP
• OSPF</td><td colspan="2">• CLNP[8]
• ES-IS[9]
• IS-IS[10]</td></tr>
<tr><td>レイヤ 2 データ リンク</td><td>• PPP</td><td colspan="2">• PPP
• LAP-D[11]</td></tr>
<tr><td>レイヤ 1 物理</td><td>DCC、LAN、ファイバ、電気回路</td><td colspan="2">DCC、LAN、ファイバ、電気回路</td><td></td></tr>
</table>

1. TARP = TID Address Resolution Protocol
2. FTAM = File Transfer and Access Management
3. ACSE = Association Control Service Element（アソシエーション制御サービス要素）
4. T–TD = TL1–Translation Device
5. FT–TD = File Transfer–Translation Device
6. PST = Presentation layer
7. CLNS = Connectionless Network Layer Service
8. CLNP = Connectionless Network Layer Protocol
9. ES-IS = End System-to-Intermediate System
10. IS-IS = Intermediate System-to-Intermediate System
11. LAP-D = Link Access Protocol on the D Channel

13.6.1　PPP

PPP（ポイントツーポイント プロトコル）は、ポイントツーポイント リンクを介してデータグラムを転送するデータ リンク（レイヤ 2）カプセル化プロトコルです。PPP は IP トラフィックを転送するように開発されましたが、OSI CLNP を含む他のプロトコルを伝送できます。OSI の転送で使用される PPP コンポーネントは、次のとおりです。

- High-Level Data Link Control（HDLC; ハイレベル データリンク制御）— ポイントツーポイント リンクを介して転送するデータグラムのカプセル化を実行します。
- Link Control Protocol（LCP; リンク制御プロトコル）— ポイントツーポイント接続を確立し、構成し、テストします。

CTC は、RS-DCC または MS-DCC を作成するたびに、IP over PPP を自動的に有効にします。OSI over PPP をサポートするように、RS-DCC または MS-DCC をプロビジョニングできます。

13.6.2　LAP-D

Link Access Protocol on the D Channel（LAP-D）は、OSI プロトコル スタックで使用されるデータ リンク プロトコルです。LAP-D は、ONS 15454 SDH RS-DCC を OSI 専用でプロビジョニングする場合に割り当てられます。プロビジョニング可能な LAP-D パラメータは、次のとおりです。

- Transfer Service — 次の転送サービスのいずれかを割り当てる必要があります。
  - Acknowledged Information Transfer Service（AITS）— （デフォルト）2 つの LAP-D ユーザ間の論理接続が確立される前にデータを交換しません。このサービスは、信頼性の高いデータ転送、フロー制御、およびエラー制御メカニズムを提供します。
  - Unacknowledged Information Transfer Service（UITS）— 確認応答がないユーザ データを含むフレームを転送します。このサービスでは、1 人のユーザが発信したデータが確実に別のユーザに配信されることを保証しません。また、配信が失敗した場合にユーザに通知しません。フロー制御またはエラー制御メカニズムも提供しません。
- Mode — LAP-D は、Network または User モードのどちらかに設定されています。このパラメータは、LAP-D フレームの Command/Response（C/R）値を設定します。これは、フレームがコマンドまたは応答かを示します。
- Maximum Transmission Unit（MTU; 最大伝送ユニット）— LAP-D N201 パラメータは、LAP-D 情報フレームの最大オクテット数を設定します。範囲は、512 ～ 1500 オクテットです。

（注）　MTU は、ネットワーク上のすべての NE で同じサイズである必要があります。

- Transmission Timers — 次の LAP-D タイマーをプロビジョニングできます。
  - T200　タイマーは、再試行の開始または障害の通知に関するタイムアウト期間を設定します。
  - T203 タイマーは、フレームの交換（LAP-D「キープアライブ」Receive Ready [RR] フレームの送信に対するトリガー）が行われない最大の時間をプロビジョニングします。

固定値は、次の LAP-D パラメータに割り当てられます。

- Terminal Endpoint Identifier（TEI; 端末終端点識別子）— 0 の固定値が割り当てられています。
- Service Access Point Identifier（SAPI）— 62 の固定値が割り当てられています。
- N200 supervisory frame retransmissions — 3 の固定値が割り当てられています。

13.6.3　OSI CLNS

OSI Connectionless Network Service（CLNS）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）および CLNS を使用して実装されます。CLNP と CLNS は、ISO 8473 標準に記述されています。CLNS は、CLNP を通じて、トランスポート レイヤにネットワーク レイヤ サービスを提供します。パスはネットワークを通じて送信される各パケットによって独自に決まるので、CLNS は接続設定または終了を実行しません。CLNS は、エラーの検出および修正を行う場合に、トランスポート レイヤ プロトコルに依存します。

CLNP は、コネクションレス リンク上で上位レイヤのデータおよびエラー表示を伝送する OSI ネットワーク レイヤ プロトコルです。CLNP は、CLNS および上位レイヤ間のインターフェイスを提供します。CLNP は、IP と同じ多くのサービスをトランスポート レイヤに対して実行します。CLNP データグラムは、IP データグラムに非常によく似ています。CLNP データグラムは、フラグメン

テーションのメカニズム（データ ユニットの識別、フラグメント / 全長、およびオフセット）を提供します。IP と同様に、CLNP ヘッダーで計算されたチェックサムは CLNP データグラムを処理するのに使用された情報が正しく送信されたかどうかを検証し、ライフタイム制御メカニズム（Time to Live [TTL]）はシステムでデータグラムが存続できる時間を制限します。

CLNP は、Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）を使用して、ネットワーク デバイスを識別します。CLNP の送信元および宛先アドレスは、NSAP です。さらに、CLNP は Network Element Title（NET）を使用して End System（ES）または Intermediate System（IS）のネットワーク エンティティを識別します。NET は、NSAP アドレスと同じネーム スペースから割り当てられます。アドレスが NSAP アドレスか NET であるかどうかは、NSAP のネットワーク セレクタ値によって異なります。

ONS 15454 SDH は、ISO 8348 で規定されている ISO Data Country Code（ISO-DCC）NSAP アドレス フォーマットをサポートしています。NSAP アドレスは、Initial Domain Part（IDP）と Domain-Specific Part（DSP）に分かれます。表 13-8 に NSAP フィールドを示します。NSAP フィールドは、16 進数の形式です。NSAP はすべて編集可能です。より短い NSAP を使用することもできます。ただし、同一 OSI ネットワーク領域内に存在するすべての NE に対する NSAP は、通常、同一の NSAP 形式を持ちます。

表 13-8　NSAP フィールド

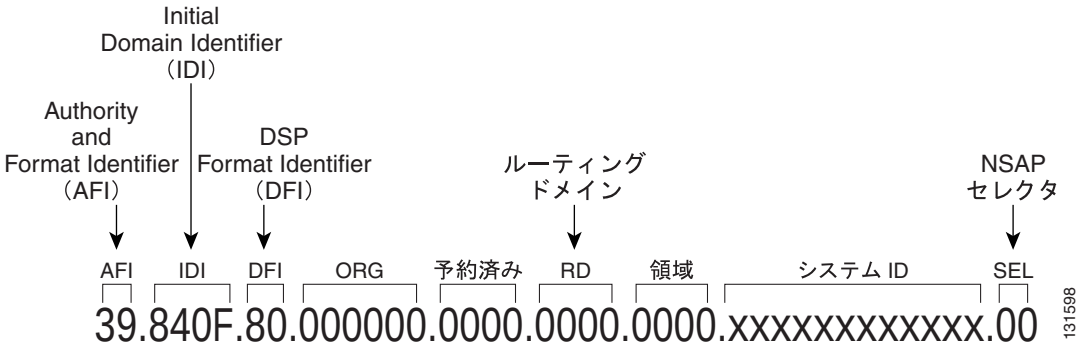
フィールド	定義	説明
IDP		
AFI	Authority and Format Identifier（AFI）	NSAP アドレス形式を指定します。ISO-DCC アドレス形式の場合、初期値は 39 です。
IDI	Initial Domain Identifier（IDI）	国コードを指定します。初期値が 840F の場合、F が付いたアメリカ合衆国の国コードを表します。
DSP		
DFI	DSP Format Identifier（DFI）	DSP 形式を指定します。初期値は 80 で、DSP 形式が American National Standards Institute（ANSI）標準に従っていることを示します。
ORG	組織	組織識別子。初期値は 000000 です。
Reserved	予約済み	予約済み NSAP フィールド。予約済みフィールドは、通常、すべてゼロ（0000）です。
RD	ルーティング ドメイン	ルーティング ドメインを定義します。初期値は 0000 です。
AREA	領域	ノードが属する OSI ルーティング領域を識別します。初期値は 0000 です。
System	システム ID	ONS 15454 SDH システム識別子は、IEEE 802.3 の MAC アドレスに設定されます。各 ONS 15454 SDH は、3 つの OSI 仮想ルータをサポートしています。各ルータの NSAP システム ID は、ONS 15454 SDH IEEE 802.3 の MAC アドレス + *n* で、*n* = 0 ～ 2 です。プライマリ仮想ルータの場合は、*n* = 0 です。

表 13-8　NSAP フィールド（続き）

フィールド	定義	説明
SEL	セレクタ	セレクタ フィールドは、CLNP ネットワーク レイヤ サービスを使用して、Protocol Data Unit（PDU; プロトコル データ ユニット）を正しい宛先に送信します。ONS 15454 SDH がサポートしているセレクタ値は、次のとおりです。 • 00 — Network Entity Title（NET）。ES-IS と IS-IS ルーティング交換プロトコルで PDU を交換するのに使用されます（「13.6.4.1　ES-IS プロトコル」[p.13-39] および「13.6.4.2　IS-IS」[p.13-40] を参照）。 • 1D — トランスポート クラス 4（および FTAM および TL1 アプリケーション [Telcordia GR-253-CORE 標準]）のセレクタ • AF — TARP プロトコル（Telcordia GR-253-CORE 標準）のセレクタ • 2F — GRE IP-over-CLNS トンネル（ITU/RFC 標準）のセレクタ • CC — Cisco IP-over-CLNS トンネル（シスコ固有）のセレクタ • E0 — OSI PING アプリケーション（シスコ固有）のセレクタ NSEL は、ノードが ES として設定されている場合にのみアドバタイズされます。NSEL は、ノードが IS として設定されている場合にはアドバタイズされません。トンネル NSEL は、トンネルが作成されるまでアドバタイズされません。

図 13-20 に、ONS 15454 SDH に含まれているデフォルト値による ISO-DCC NSAP アドレスを示します。システム ID には、自動的にノードの MAC アドレスが入力されます。

図 13-20　ISO-DCC NSAP アドレス



ONS 15454 SDH のメイン NSAP アドレスは、ノード ビューの Provisioning > OSI > Main Setup サブタブに表示されます。このアドレスは、ルータ 1 のプライマリ手動領域のアドレスでもあり、Provisioning > OSI > Routers サブタブで表示して編集できます。CTC の OSI ルータおよび手動領域のアドレスについては、「13.6.7　OSI 仮想ルータ」（p.13-45）を参照してください。

13.6.4　OSI ルーティング

OSI アーキテクチャには、ES と IS が含まれます。OSI ルーティング方式は、次のとおりです。

- ES と IS がルートを判別するのに必要な情報を収集し、配信できるようにするルーティング プロトコル セット。プロトコルには、ES-IS および IS-IS プロトコルがあります。ES-IS ルーティングは、同一（単一）のサブネットワークに接続された ES および IS 間の接続を確立します。
- ES 間のルートが計算される情報を含む Routing Information Base（RIB）。RIB は、宛先（たとえば、NSAP）、その宛先に到達するためにパケットが転送される必要があるサブネットワーク、およびルーティング メトリックを識別するエントリのテーブルで構成されています。ルーティング メトリックは、ルートの特性（遅延プロパティまたは予想されるエラー レート）をやり取りします。ルートの特性は、特定のパケットまたはパケット クラスを転送する場合、異なるプロパティを持つ別のルートと比較されるルートの適格性の評価に使用されます。
- ルーティング アルゴリズム（Shortest Path First [SPF]）。RIB に含まれる情報を使用して、ES 間のルートを導出します。

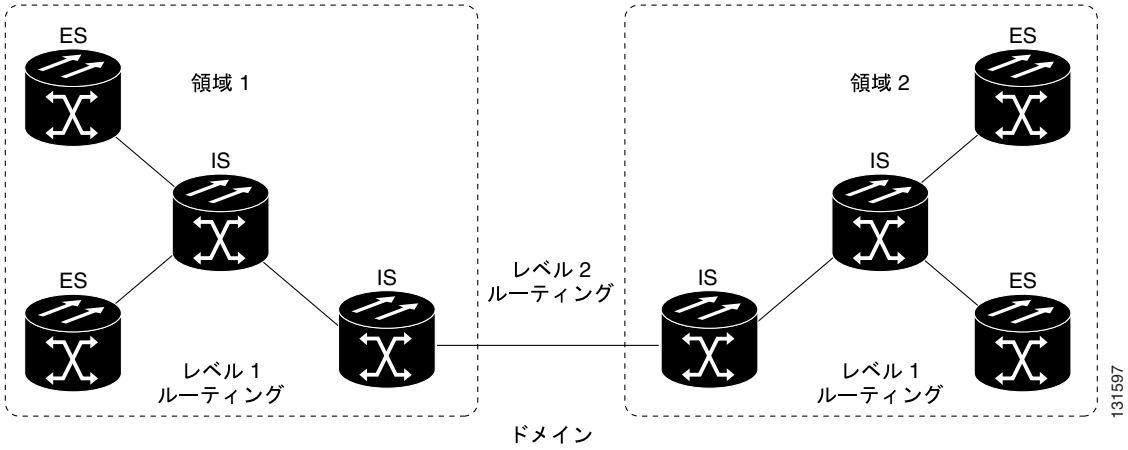
OSI ネットワーキングでは、検出はアナウンスに基づいています。ES は ES-IS プロトコルの End System Hello（ESH）メッセージを使用して、同一ネットワークに接続されている IS と ES に自身の存在をアナウンスします。ESH を待ち受けている ES または IS がコピーを受け取ります。IS は NSAP アドレスおよび対応するサブネット アドレスのペアをルーティング テーブルに格納します。ES はアドレスを格納するか、そのような情報が必要になったときに IS に通知されるまで待機する可能性があります。

IS は Intermediate System Hello（ISH）メッセージを構成して、同一ブロードキャスト サブネットワークに接続されている IS と ES にその構成情報をアナウンスします。ESH と同様に、ISH には IS（NET と Subnetwork Point-of-Attachment Address [SNPA; サブネットワーク ポイント アタッチメント]）および待機時間のアドレス情報が含まれます。ISH が、ES に設定タイマーを推奨する提案された ES 設定時間をやり取りする場合もあります。

ISH の交換は、ネイバ グリーティングまたは初期化と呼ばれます。各ルータは、直接接続を共有する他のルータについて学習します。初期化の完了後、各ルータは Link-State Packet（LSP; リンクステート パケット）を構築します。LSP には、IS のネイバの名前および各ネイバに到達するまでのコストのリストが含まれています。その後、ルータは LSP を他のすべてのルータに配信します。すべての LSP がすべてのルータに伝播される場合、各ルータにはネットワーク トポロジの完全なマップ（LSP の形式）が含まれます。ルータは LSP と SPF アルゴリズムを使用して、ネットワーク内のすべての宛先へのルートを計算します。

OSI ネットワークは、領域とドメインに分けられます。領域は連続するネットワークと接続されたホストのグループで、ネットワーク管理者によって領域として指定されています。ドメインは、接続された領域の集合体です。ルーティング ドメインは、ルーティング ドメイン内のすべての ES に対するフル接続を提供します。同一領域内のルーティングは、レベル 1 ルーティングと呼ばれます。2 つの領域間のルーティングは、レベル 2 ルーティングと呼ばれます。レベル 1 領域内で交換される LSP は、L1 LSP と呼ばれます。レベル 2 領域で交換される LSP は L2 LSP と呼ばれます。図 13-21 に、レベル 1 とレベル 2 のルーティングの例を示します。

図 13-21　レベル 1 とレベル 2 の OSI ルーティング



TCP/IP と OSI プロトコル スタックの両方を使用する NE によるネットワーク用に ONS 15454 SDH をプロビジョニングする場合、次のいずれかにプロビジョニングします。

- End System — ONS 15454 SDH は、OSI ES 機能を実行し、OSI 領域内に存在するノードとやり取りする場合は IS に依存します。
- Intermediate System Level 1 — ONS 15454 SDH は、OSI IS 機能を実行します。OSI 領域内に存在する IS および ES ノードとやり取りします。OSI 領域外に存在する IS と ES ノードとやり取りする場合は、IS L1/L2 ノードに依存します。
- Intermediate System Level 1/Level 2 — ONS 15454 SDH は、IS 機能を実行します。OSI 領域内に存在する IS および ES ノードとやり取りします。他の OSI 領域に存在する IS L1/L2 ノードともやり取りします。ノードが異なる OSI 領域に存在する別の IS L1/L2 ノードに接続されている場合を除いて、このオプションをプロビジョニングしないでください。また、ノードは IS L1/L2 としてプロビジョニングされている領域内のすべてのノードに接続されている必要があります。

13.6.4.1　ES-IS プロトコル

End System-to-Intermediate System（ES-IS）は、ES（ホスト）と IS（ルータ）が相互に学習する方法を定義する OSI プロトコルです。ES-IS 設定情報は、ES および IS の Hello メッセージを通じて通常間隔で送信されます。Hello メッセージには、このメッセージを生成するシステムのサブネットワークとネットワーク レイヤのアドレスが含まれます。

ES-IS 構成プロトコルは、OSI ネットワーク レイヤおよび OSI サブネットワークのアドレスの両方でやり取りします。OSI ネットワーク レイヤ アドレスは、NSAP（OSI レイヤ 3 および レイヤ 4 間のインターフェイス）または NET（OSI IS のネットワーク レイヤ エンティティ）を識別します。OSI SNPA は、ES または IS がサブネットワークに物理的に接続されているポイントです。SNPA アドレスは、サブネットワークに接続されている各システムを一意に識別します。たとえば、イーサネット ネットワークでは、SNPA は 48 ビットの MAC アドレスです。ES-IS によって送信された設定情報の一部は、NSAP と SNPA 間または NET と SNPA 間のマッピングになります。

13.6.4.2　IS-IS

Intermediate System-to-Intermediate System（IS-IS）は、ネットワークにリンクステート情報をフラッディングして、一貫した完全な状態のネットワーク トポロジを構築する OSI リンクステートの階層ルーティング プロトコルです。IS-IS は、レベル 1 とレベル 2 の IS 間を区別します。レベル 1 の IS は、同一領域内の他のレベル 1 の IS とやり取りします。レベル 2 の IS はレベル 1 領域間をルーティングして、ドメイン内ルーティングのバックボーンを形成します。レベル 1 の IS は、最短のレベル 2 の IS に到達するための方法だけを知る必要があります。バックボーンのルーティング プロトコルは、領域内のルーティング プロトコルに影響することなく、変更できます。

OSI ルーティングは、ES が ISH パケットを待ち受けて、最短の IS を検出したときに開始します。ES が別の ES にパケットを送信する場合、ネットワークに直接接続された IS の 1 つにパケットを送信します。その後、ルータが宛先アドレスを調べ、パケットを最適なルートで転送します。宛先 ES が同一サブネットワーク上にある場合、ローカル IS は ESH を待ち受けて同一サブネットワーク上にあることを認識してから、パケットを適切に転送します。また、IS は Redirect（RD）メッセージを送信元に戻し、他の直行ルートがあることを通知する可能性があります。宛先アドレスが同一領域内の別のサブネットワークの ES である場合、IS は正しいルートを認識し、適切にパケットを転送します。宛先アドレスが別の領域の ES である場合、レベル 1 の IS はパケットを最短のレベル 2 の IS に送信します。パケットが宛先領域のレベル 2 の IS に到着するまで、レベル 2 の IS を経由した転送が続行します。宛先領域内では、宛先 ES に到達するまで、IS がパケットを最適なパスで転送します。

リンクステートのアップデート メッセージは、IS がネットワーク トポロジについて学習するのに役立ちます。各 IS は、接続されている ES と IS、または関連付けられたメトリックを指定するアップデートを生成します。その後、アップデートは近接するすべての IS に送信され、さらに近接する IS がアップデートをネイバに転送（フラッディング）します（シーケンス番号は、フラッディングを終了し、古いアップデートと新規のアップデートを区別します）。アップデートを使用すると、各 IS がネットワークの完全なトポロジを構築できます。トポロジが変更されると、新規のアップデートが送信されます。

IS-IS は、必要なデフォルト メトリック（最大パス値が 1024）を 1 つ使用します。メトリックは任意で、通常、ネットワーク管理者によって割り当てられます。1 つのリンクは最大 64 の値を持つことが可能で、パス リンクは加算リンク値によって計算されます。最大メトリック値はこのようなレベルで設定されており、さまざまなリンク タイプをサポートするための粒度を提供すると同時に、ルートの計算に使用されている最短パスのアルゴリズムが適度に効率的であるようにします。ONS 15454 SDH では、3 つのオプション（delay、expense、および error）の IS-IS メトリック（コスト）がサポートされていません。IS-IS は、Quality of Service（QoS; サービス品質）オプションに対するメトリックのマッピングを CLNP パケット ヘッダーで維持します。IS-IS はマッピングを使用して、インターネットワークを経由するルートを計算します。

13.6.5　TARP

TARP は、TL1 Target Identifier（TID; ターゲット ID）を NSAP アドレスに変換する必要がある場合に使用されます。TID から NSAP への変換は、TID を NET にマッピングしてから、NSAP セレクタ値を使用して NET から NSAP を導出することによって行われます（表 13-8）。

TARP は、選択可能な PDU 伝播方法論を、TID と NET 間のマッピングの分散データベース（NE 内に存在）と併せて使用します。TARP を使用すると、NE が他の NE とマッピング情報を自動的に交換して、TID と NET 間で変換できるようになります。TARP PDU は、標準の CLNP データ PDU によって伝送されます。表 13-9 に TARP PDU フィールドを示します。

表 13-9　TARP PDU フィールド

フィールド	省略形	サイズ（バイト）	説明
TARP Lifetime	tar-lif	2	TARP time-to-live（TTL）（ホップ数）
TARP Sequence Number	tar-seq	2	ループの検出に使用される TARP のシーケンス番号
Protocol Address Type	tar-pro	1	TID がマッピングされる必要があるプロトコル アドレスのタイプを識別するのに使用されます。FE の値は、CLNP アドレス タイプを識別するのに使用されます。
TARP Type Code	tar-tcd	1	PDU の TARP タイプを識別するのに使用されます。表 13-10 に表示されている 5 つの TARP タイプを定義できます。
TID Target Length	tar-tln	1	tar-ttg フィールドのオクテット数
TID Originator Length	tar-oln	1	tar-tor フィールドのオクテット数
Protocol Address Length	tar-pln	1	tar-por フィールドのオクテット数
TID of Target	tar-ttg	*n* = 0、1、2...	ターゲット NE の TID 値
TID of Originator	tar-tor	*n* = 0、1、2...	TARP PDU 発信元の TID 値
Protocol Address of Originator	tar-por	*n* = 0、1、2...	TARP PDU 発信元の tar-pro フィールドで特定されているプロトコル タイプに対するプロトコル アドレス。tar-pro フィールドが FE（16 進）に設定されている場合、tar-por には CLNP アドレス（NET）が含まれます。

表 13-10 に、TARP の相互関係とルーティングを制御する TARP PDU タイプを示します。

表 13-10　TARP PDU タイプ

タイプ	説明	プロシージャ
1	装置が持つ TID に対応する NSAP が一致しないときに送信します。	NE が TARP Type 1 の PDU を発信したあと、PDU が NE のルーティング領域内のすべての隣接装置に送信されます。
2	装置が持つ TID に対応する NSAP が一致せず、かつ Type 1 の PDU から応答がない場合に送信します。	NE が TARP Type 2 の PDU を発信したあと、PDU が すべてのレベル 1 およびレベル 2 のネイバに送信されます。
3	Type 1、Type 2、または Type 5 の PDU に対する応答として送信されます。	TARP Request（Type 1 または 2）の PDU が受信されたあと、TARP Type 3 の PDU が要求の発信元に送信されます。Type 3 の PDU は、TARP 伝播プロシージャを使用しません。
4	TID の変更や NSAP の変更など、ローカルな変更が発生した場合の通知を送信します。NE の初期化のときにも送信される場合があります。	Type 4 の PDU は、通知を発信する NE での TID または Protocol Address の変更に対する通知です。PDU は、NE ルーティング領域内外のすべての隣接装置に送信されます。
5	特定の NSAP に対応する TID が装置で必要なときに送信されます。	Type 5 の PDU が送信される場合、CLNP の宛先アドレスは既知であるので、そのアドレスだけに PDU が送信されます。Type 5 の PDU は、TARP 伝播プロシージャを使用しません。

13.6.5.1　TARP プロセス

TARP Data Cache（TDC）は、TARP プロセスを円滑にするために各 NE で作成されます。CTC では、TDC がノード ビューの Maintenance > OSI > TDC サブタブで表示され、管理されます。TDC サブタブには、次の TARP PDU フィールドがあります。

- TID — 発信元 NE（tar-tor）の TID
- NSAP — 発信元 NE の NSAP
- Type — TARP PDU が TARP 伝播プロセス（ダイナミック）を通じて作成されたか、手動（スタティック）で作成されたかを示します。

プロビジョニング可能なタイマー（表 13-11 を参照）は、TARP プロセスを制御します。

表 13-11　TARP タイマー

タイマー	説明	デフォルト（秒）	範囲（秒）
T1	TARP Type 1 Request の PDU への応答を待機しています。	15	0 ～ 3600
T2	TARP Type 2 Request の PDU への応答を待機しています。	25	0 ～ 3600
T3	アドレス解決要求の応答を待機しています。	40	0 ～ 3600
T4	T2 の期限が切れたときにタイマーが開始します（エラーの回復時に使用されます）。	20	0 ～ 3600

表 13-12 に、TARP のメイン プロセスと各プロセスで発生するイベントの一般的なシーケンスを示します。

表 13-12　TARP プロセスのフロー

プロセス	TARP の一般的なフロー
TID に一致する NET を検索	**1.** TARP は、一致する TDC がないか確認します。一致する TID がある場合は、TARP はその結果を要求アプリケーションに返します。 **2.** 一致する TID がない場合、TARP Type 1 の PDU が生成され、Timer T1 が開始します。 **3.** 一致する TID が検出される前に Timer T1 の期限が切れると、Type 2 の PDU が生成され、Timer T2 が開始します。 **4.** 一致する TID が検出される前に Timer T2 の期限が切れると、Timer T4 が開始します。 **5.** 一致する TID が検出される前に Timer T4 の期限が切れると、Type 2 の PDU が生成され、Timer T2 が開始します。
NET に一致する TID を検索	Type 5 の PDU が生成されます。Timer T3 が使用されます。ただし、タイマーの期限が切れると、エラー回復プロシージャは発生せず、TID を検索できなかったことを示すステータス メッセージが送られます。
TID またはプロトコル アドレス変更の通知を送信	TARP は、Type 4 の PDU を生成します。Type 4 の PDU の tar-ttg フィールドには、TID またはプロトコル アドレスが変更される前の NE の TID 値が含まれます。他の NE がアドレス変更を正常に受信したことを示す確認は、送信されません。

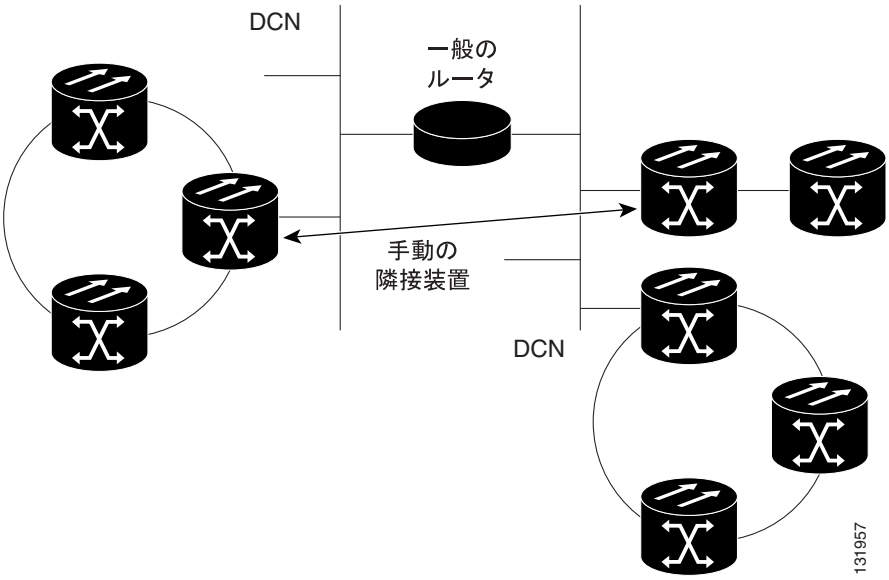
13.6.5.2　TARP LDB

TARP Loop Detection Buffer（LDB）を有効にして、重複した TARP PDU が TDC に入るのを防ぐことができます。TARP Type 1、2、または 4 の PDU が到着すると、TARP は PDU 発信元の NET アドレス（tar-por）が一致するか LDB を確認します。一致する NET アドレスがない場合、TARP は PDU を処理し、PDU の tar-por、tar-seq（シーケンス）エントリを LBD に割り当てます。tar-seq がゼロである場合、LDB エントリに関連付けられたタイマーが、ノード ビューの OSI > TARP > Config タブのプロビジョニング可能な LDB エントリ タイマーを使用して開始します。一致する NET アドレスが存在する場合、tar-seq が LDB エントリと比較されます。tar-seq がゼロ以外で、LDB エントリ以下である場合、PDU が廃棄されます。tar-seq が LDB エントリを超える場合、PDU が処理され、LDB エントリの tar-seq フィールドが新規の値で更新されます。Cisco ONS 15454 SDH LDB は、約 500 のエントリを保持します。LDB はノード ビューの OSI > TARP > Config タブの LDB Flush タイマーに設定された時間に基づいて、定期的に消去されます。

13.6.5.3　手動の TARP 隣接装置

TARP 隣接装置は、ONS 15454 SDH ノードがルータ間または TARP 対応でない非 SONET NE とやり取りする必要があるネットワークに手動でプロビジョニングできます。CTC では、ノード ビューの Provisioning > OSI > TARP > MAT（Manual Area Table）サブタブで手動の TARP 隣接装置をプロビジョニングします。手動の隣接装置によって、TARP 要求が一般のルータまたは非 SONET NE にホップします（図 13-22 を参照）。

図 13-22　手動の TARP 隣接装置



13.6.5.4　TID から NSAP の手動プロビジョニング

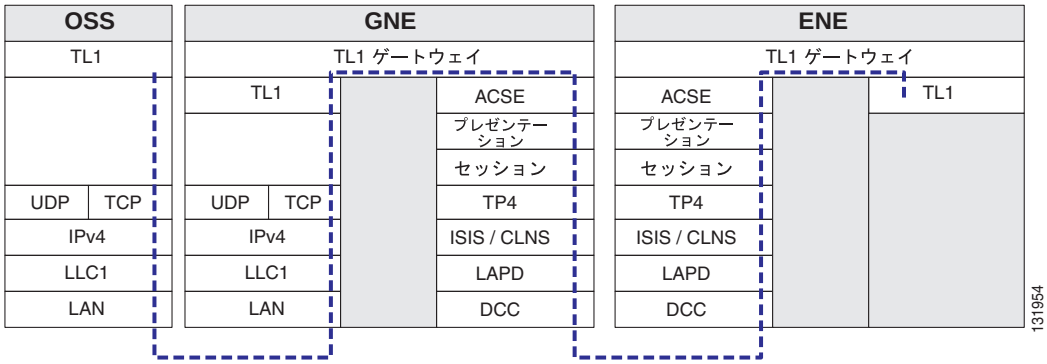
TID は、NSAP に手動でリンクさせ、TDC に追加できます。スタティック TDC エントリは、スタティック ルートに類似しています。特定の TID には、特定の NSAP を強制します。その TID に対する解決要求は、必ずその NSAP に返されます。TARP ネットワーク伝播または瞬時の応答は、ありません。スタティック エントリによって、ユーザは TARP をサポートしない NE に TL1 コマンドを転送できます。ただし、スタティック TDC エントリが動的に更新されないので、ターゲット ノードの TID または NSAP が変更されても古いエントリが削除されません。

13.6.6　TCP/IP と OSI 間のメディエーション

2 つのメディエーション プロセスは、TCP/IP と OSI プロトコル スイートを実行する NE と ONS クライアント コンピュータ間の TL1 ネットワーキングとファイル転送を円滑にします。

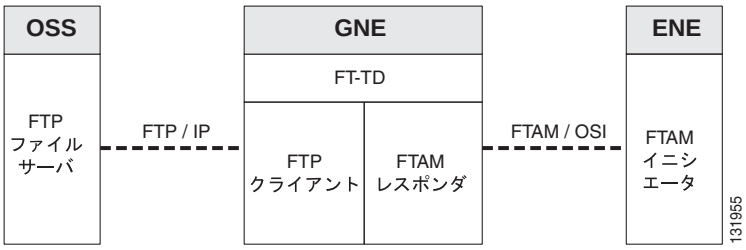
- T-TD — TL1-over-IP と TL1-over-OSI 間のゲートウェイ メディエーションを実行して、IP ベースの OSS が GNE に従属する OSI 専用の NE を管理できるようにします。図 13-23 に、T–TD プロトコルのフローを示します。

図 13-23　T-TD プロトコルのフロー



- FT-TD — FTAM と FTP 間の FTP 変換を実行します。FT-TD ゲートウェイ エンティティには FTAM レスポンダ（サーバ）と FTP クライアントが含まれ、FTAM イニシエータ（クライアント）が FTP サーバのファイルを格納、検索、または削除できるようにします。FT-TD ゲートウェイは単方向で、FTAM イニシエータによって稼働します。FT–TD FTAM レスポンダは、フル OSI スタックを介して FTAM イニシエータとメッセージを交換します。図 13-24 に、FT–TD プロトコルのフローを示します。

図 13-24　FT-TD プロトコルのフロー



ONS 15454 SDH は、次のファイル転送プロセスで FT–TD を使用します。

- ソフトウェアのダウンロード
- データベースのバックアップと復元
- Cisco IOS コンフィギュレーションのバックアップ、および ML と ML2 シリーズ カードの復元

13.6.7　OSI 仮想ルータ

ONS 15454 SDH は、3 つの OSI 仮想ルータをサポートしています。Provisioning > OSI > Routers タブで、ルータをプロビジョニングできます。各ルータは、編集可能な手動領域のアドレス、およびノードの MAC アドレス +*n* に設定されている一意の NSAP システム ID を保持しています。ルータ 1 では *n* = 0 です。ルータ 1 では *n* = 1 です。ルータ 2 では *n* = 2 です。各ルータは異なる OSI ルーティング領域に対して有効化し、接続することができます。ただし、ルータ 1 はプライマリ ルータで、ルータ 2 とルータ 3 が有効になる前に有効にする必要があります。ルータ 1 の手動領域のアドレスとシステム ID によって、ノードの TID に割り当てられる NSAP アドレスが作成されます。さらに、ルータ 1 は、ルータ 2 とルータ 3 ではサポートされていない OSI TARP、メディエーション、およびトンネリング機能をサポートします。次の内容が含まれます。

- TID から NSAP への変換
- TARP データ キャッシュ
- IP-over-CLNS トンネル
- FTAM
- FT–TD
- T–TD
- LAN サブネット

OSI 仮想ルータの制約は、ノードにプロビジョニングされたルーティング モデルに応じて変わります。表 13-13 に、各ルータでサポートされている IS L1、IS L1/L2、および DCC の数を示します。IS L1 と IS L1/L2 は 1 つの DCC につき 1 個の ES をサポートし、1 つの LAN サブネットにつき最大 100 個の ES をサポートします。

表 13-13　OSI 仮想ルータの制約

ルーティング モード	ルータ 1	ルータ 2	ルータ 3	（領域単位） IS L1	（領域単位） IS L1/L2	（IS 単位）DCC
ES	○	×	×	—	—	—
IS L1	○	○	○	250	—	40
IS L1/L2	○	○	○	250	50	40

各 OSI 仮想ルータは、プライマリの手動領域のアドレスを保持しています。さらに 2 つの手動領域のアドレスを作成できます。このような手動領域のアドレスは、次のような場合に使用できます。

- 領域を分ける場合 — 所定の領域内のノードは、管理するのが困難なポイントにまで蓄積したり、トラフィック量が必要以上に増える原因になったり、領域の利用可能なアドレス スペースにまで及んだりする恐れがあります。追加の手動領域のアドレスを割り当てることができるので、サービスを中断することなく、ネットワークを別個の領域に円滑に分割できます。
- 領域をマージする場合 — 移行領域のアドレスを使用して、最大 3 つの別個の領域を共通領域のアドレスを共有する 1 つの領域にマージします。
- 異なるアドレスに変更する場合 — 特定のノード グループに対する領域アドレスの変更が必要な場合があります。複数の手動領域のアドレスを使用して、古い領域のアドレスに向けられた着信トラフィックが関連付けられたノードにそのままルーティングされるようにします。

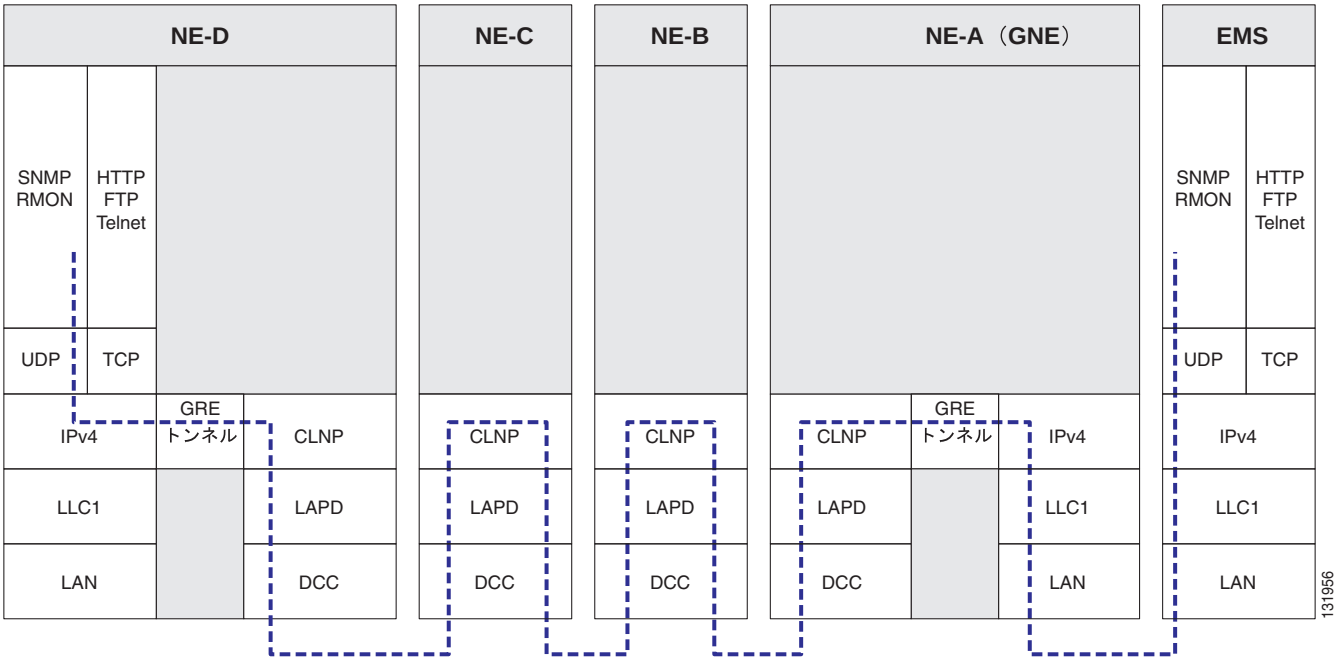
13.6.8　IP-over-CLNS トンネル

IP-over-CLNS トンネルは、OSI NE 間で転送するために IP をカプセル化する場合に使用されます。ONS 15454 SDH は、2 つのトンネル タイプをサポートしています。

- GRE（Generic Routing Encapsulation; 総称ルーティング カプセル化）— 別のネットワーク レイヤに転送するために 1 つのネットワーク レイヤをカプセル化するトンネリング プロトコル。GRE トンネルは、CLNS ヘッダーと GRE ヘッダーの両方をトンネル フレームに追加します。GRE トンネルは、シスコ製ルータと他のベンダーによる一部の NE でサポートされています。
- Cisco IP — Cisco IP トンネルは、中間ヘッダーなしで、IP パケットを直接カプセル化します。Cisco IP は、ほとんどのシスコ製ルータでサポートされています。

図 13-23 に、IP-over-CLNS トンネルが 4 つの NE（A、B、C、および D）で作成される場合のプロトコルのフローを示します。トンネルの終端は、IP と OSI の両方をサポートする NE A と D に設定されます。NE B と C は OSI だけをサポートするので、OSI パケットだけをルーティングします。

図 13-25　IP-over-CLNS トンネルのフロー



13.6.8.1　IP-over-CLNS トンネルのプロビジョニング

IP-over-CLNS トンネルは、ノードの可視性と接続性が失われないように慎重に計画する必要があります。トンネルを開始する前に、トンネル タイプ（Cisco IP または GRE のいずれか）が他の終端の機器によってサポートされているかを確認します。IP と NSAP アドレスを必ず確認してください。CTC の IP-over-CLNS トンネルのプロビジョニングは、ノード ビューの Provisioning > OSI > IP over CLNS Tunnels タブで実行されます。手順については、『*Cisco ONS 15454 SDH Procedure Guide*』の「Turn Up a Node」の章を参照してください。

シスコ製ルータに IP-over-CLNS トンネルをプロビジョニングする場合、他の OSI プロビジョニングのほか、次の作業があらかじめ必要です。

- （必須）IS-IS を有効にします。
- （任意）インターフェイスの領域に対するルーティングを有効にします。
- （任意）複数領域のアドレスを割り当てます。

- （任意）IS-IS インターフェイスのパラメータを設定します。
- （任意）さまざまな IS-IS のパラメータを設定します。

表 13-14 に、IP-over-CLNS トンネル（CTunnel）を作成する場合に使用される Cisco IOS コマンドを示します。

表 13-14　IP-over-CLNS トンネル の IOS コマンド

ステップ	コマンド	目的
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。
2	Router (config-if # **ctunnel destination** *remote-nsap-address*	CTunnel の宛先パラメータを設定します。CTunnel の 宛先 NSAP1 アドレスを指定します。ここで、IP パケットが抽出されます。
3	Router (config-if) # **ip address** *ip-address mask*	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。

シスコ製ルータに IP-over-CLNS トンネルをプロビジョニングする場合、プロビジョニングしているルータの Cisco IOS マニュアルに表示されている手順に必ず従ってください。IP-over-CLNS トンネルを含む ISO CLNS プロビジョニングについては、『*Cisco IOS Apollo Domain, Banyon VINES, DECnet, ISO CLNS, and XNS Configuration Guide*』の「Configuring ISO CLNS」の章を参照してください。

13.6.8.2　IP-over-CLNS トンネルのシナリオ 1：ONS ノードから他のベンダーの GNE

図 13-26 に、ONS ノードから他のベンダーの GNE に作成された IP-over-CLNS トンネルを示します。他のベンダーの NE には、CTC コンピュータが接続される IP DCN への IP 接続があります。OSI 専用の（LAP-D）RS-DCC と GRE トンネルは、ONS NE 1 と他のベンダーの GNE 間に作成されます。

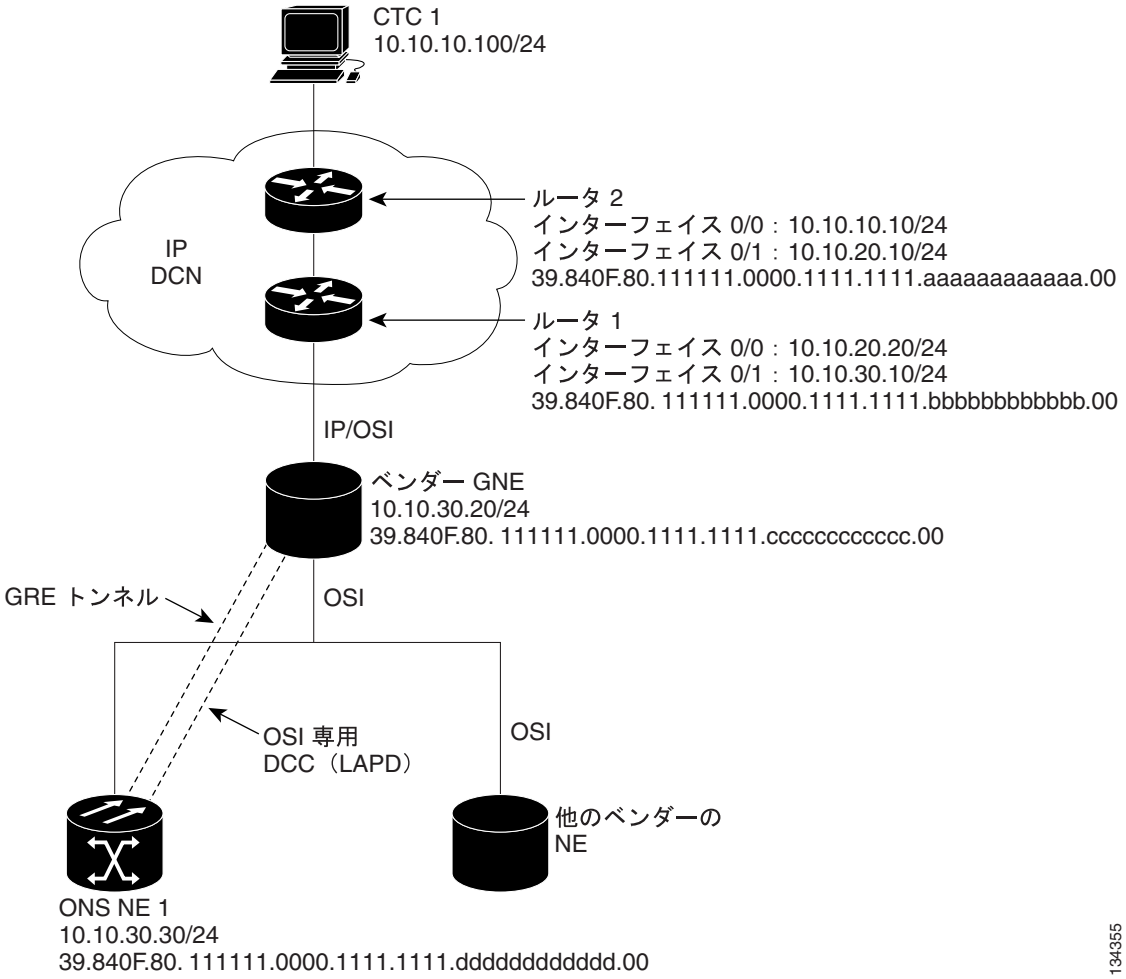
ONS NE 1 にプロビジョニングされる IP-over-CLNS トンネル

- 宛先：10.10.10.100（CTC 1）
- マスク：255.255.255.255（ホスト ルート、CTC 1 専用）、または 255.255.255.0（サブネット ルート、10.10.10.0 サブネットに存在するすべての CTC コンピュータ）
- NSAP：39.840F.80.1111.0000.1111.1111.cccccccccccc.00（他のベンダーの GNE）
- メトリック：110
- トンネル タイプ：GRE

他のベンダーの GNE にプロビジョニングされる IP-over-CLNS トンネル

- 宛先：10.20.30.30（ONS NE 1）
- マスク：255.255.255.255（ホスト ルート、ONS NE 1 専用）、または 255.255.255.0（サブネット ルート、10.30.30.0 サブネットに存在するすべての ONS ノード）
- NSAP：39.840F.80.1111.0000.1111.1111.dddddddddddd.00（ONS NE 1）
- メトリック：110
- トンネル タイプ：GRE

図 13-26　IP-over-CLNS トンネルのシナリオ 1：ONS NE から他のベンダーの GNE



13.6.8.3　IP-over-CLNS トンネルのシナリオ 2：ONS ノードからルータ

図 13-27 に、ONS ノードからルータへの IP-over-CLNS トンネルを示します。他のベンダーの NE には、CTC コンピュータが接続される IP DCN のルータへの OSI 接続があります。OSI 専用の（LAP-D）RS-DCC は、ONS NE 1 と他のベンダーの GNE 間に作成されます。OSI-over-IP トンネルは、ルータでサポートされているトンネル タイプに応じて、Cisco IP トンネルまたは GRE トンネルのどちらかにすることができます。

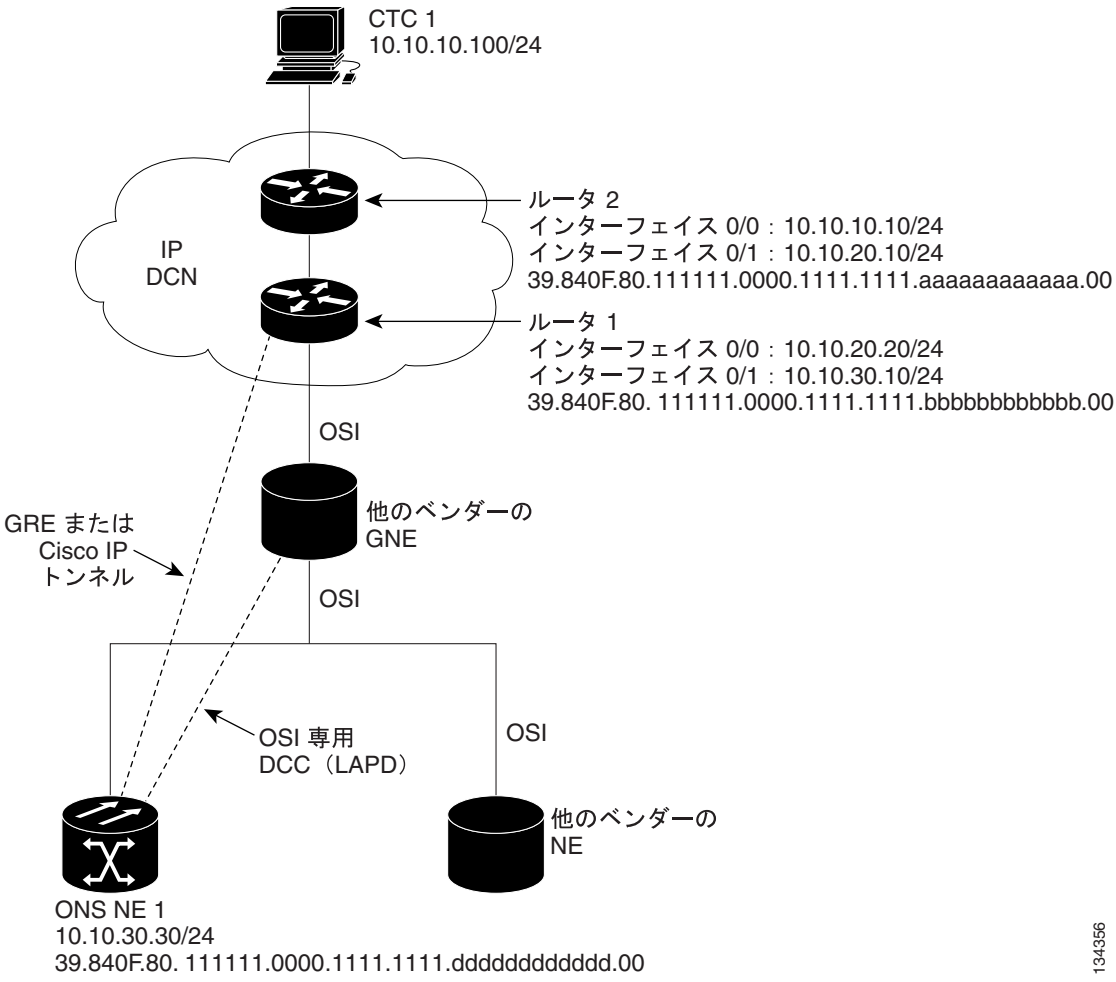
ONS NE 1 にプロビジョニングされる IP-over-CLNS トンネル

- 宛先：10.10.30.10（ルータ 1、インターフェイス 0/1）
- マスク：255.255.255.255（ホスト ルート、ルータ 1 専用）、または 255.255.255.0（サブネット ルート、同一サブネット上のすべてのルータ）
- NSAP：39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00（ルータ 1）
- メトリック：110
- トンネル タイプ：Cisco IP

ルータ 1 にプロビジョニングされる CTunnel（IP-over-CLNS）

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.ddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.bbbbbbbbbbbb.00
```

図 13-27　IP-over-CLNS トンネルのシナリオ 2：ONS ノードからルータ



13.6.8.4　IP-over-CLNS トンネルのシナリオ 3：ONS ノードからルータ（OSI DCN を介した場合）

図 13-28 に、OSI DCN を介した場合の ONS ノードからルータへの IP-over-CLNS トンネルを示します。他のベンダーの NE には、CTC コンピュータが接続される IP DCN への OSI 接続があります。OSI 専用の（LAP-D）RS-DCC は、ONS NE 1 と他のベンダーの GNE 間に作成されます。OSI-over-IP トンネルは、ルータでサポートされているトンネル タイプに応じて、Cisco IP トンネルまたは GRE トンネルのどちらかにすることができます。

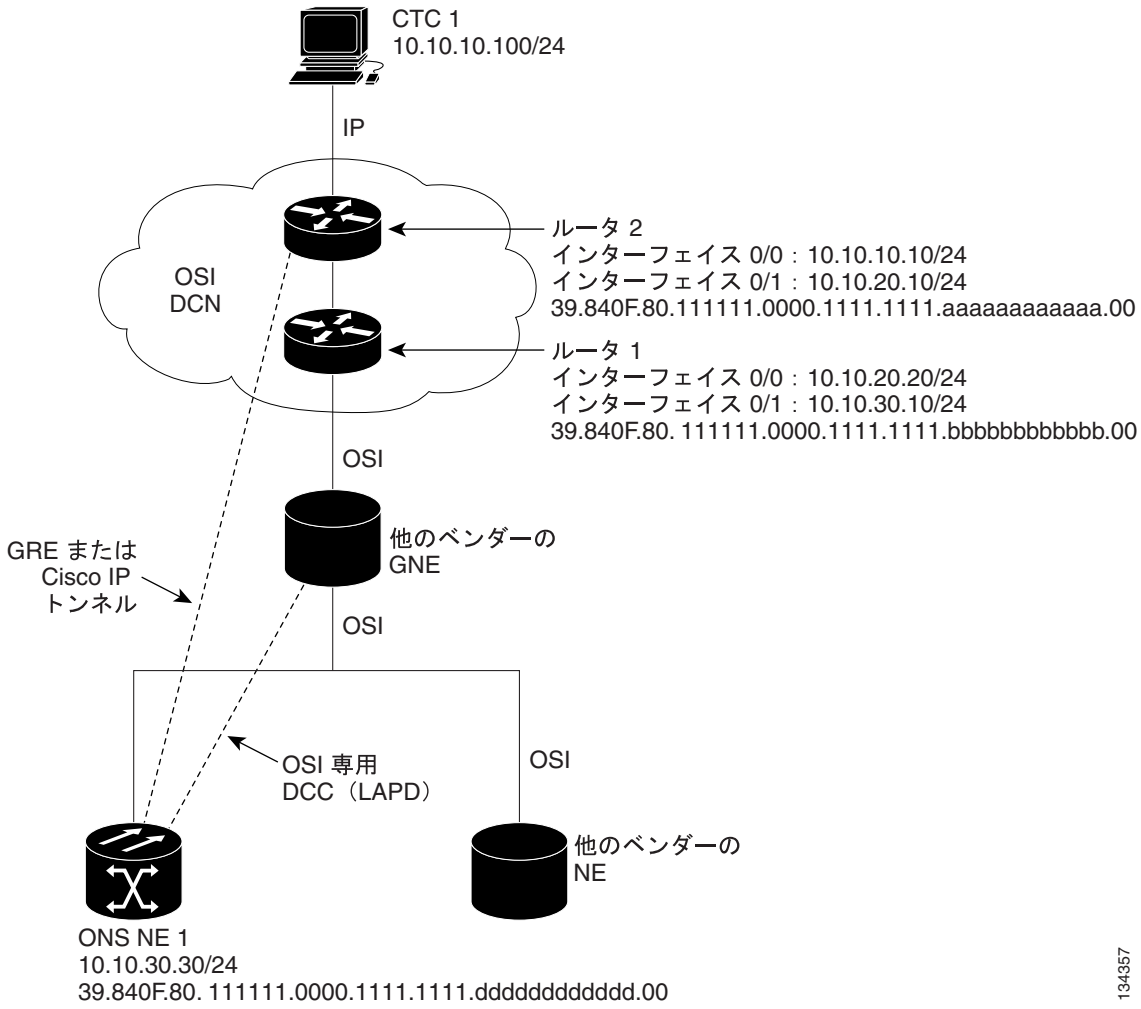
ONS NE 1 にプロビジョニングされる IP-over-CLNS トンネル

- 宛先：ルータ 2 の IP アドレス
- マスク：255.255.255.255（ホスト ルート、CTC 1 専用）、または 255.255.255.0（サブネット ルート、同一サブネット上に存在するすべての CTC コンピュータ）
- NSAP：他のベンダーによる GNE の NSAP アドレス
- メトリック：110
- トンネル タイプ：Cisco IP

ルータ 2 にプロビジョニングされる IP-over-OSI トンネル（Cisco IOS プロビジョニング例）

```
ip routing
clns routing
interface ctunnel 102
    ip address 10.10.30.30 255.255.255.0
    ctunnel destination 39.840F.80.1111.0000.1111.1111.ddddddddddd.00
interface Ethernet0/1
    clns router isis
router isis
    net 39.840F.80.1111.0000.1111.1111.aaaaaaaaaaaa.00
```

図 13-28　IP-over-CLNS トンネルのシナリオ 3：ONS ノードからルータ（OSI DCN を介した場合）



13.6.9　OSI/IP ネットワーキングのシナリオ

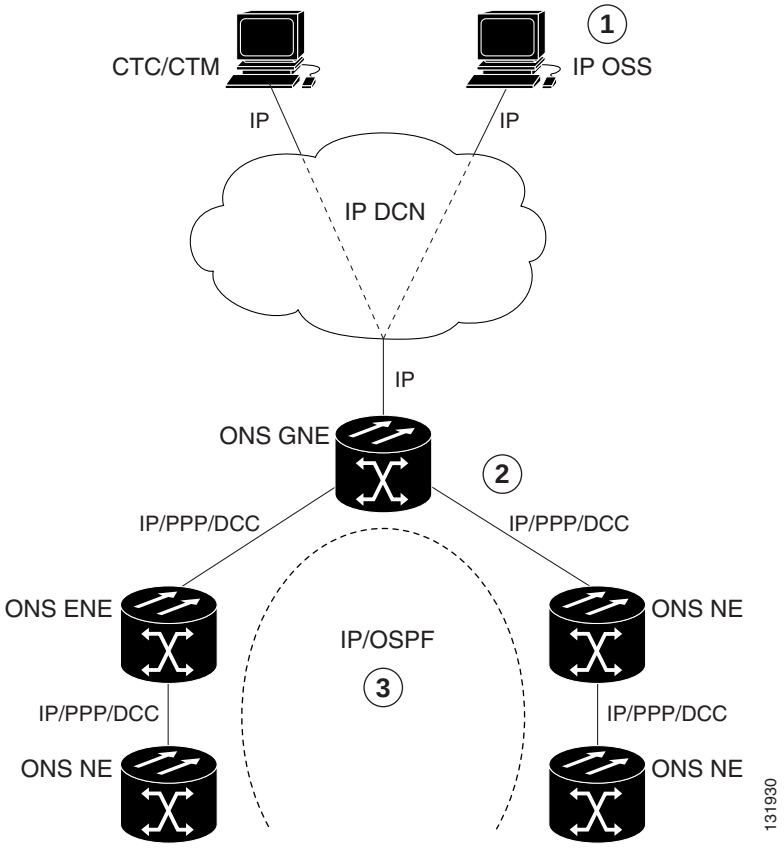
次の 8 つのシナリオは、OSI ベースの NE によるネットワークの ONS 15454 SDH ノードの例を示します。このシナリオは、各種の役割による ONS 15454 SDH ノードを示します。このシナリオでは、次の内容を前提としています。

- ONS 15454 SDH NE は、IP と NSAP アドレスの両方を使用して、デュアル OSI と IP ノードとして設定されます。ルートの再配布なしで、OSPF と OSI（IS-IS または ES-IS）の両方のルーティング プロトコルを「Ships-In-The-Night」として実行します。
- ONS 15454 SDH NE は、TARP を実行します。ここでは、TL1 TID から NSAP アドレスに変化させることができます。宛先 TID が、IP と NSAP アドレスの両方を持つ ONS 15454 SDH NE の場合、TID から IP と NSAP アドレスの両方に変化する場合があります。
- ONS 15454 SDH NE と OSI 専用の NE 間の DCC リンクは、LAP-D を介した フル OSI スタック（IS-IS、ES-IS、および TARP を含む）を実行します。
- ONS 15454 SDH NE 間の DCC リンクは、フル OSI スタックと IP（OSPF）over PPP を実行します。
- OSI ネットワークに関与するすべての ONS 15454 SDH NE が、相互に OSI over PPP を実行します。これは必須なので、他のベンダーの GNE は TL1 コマンドを、OSI ネットワークに関与するすべての ONS 15454 SDH NE にルーティングできます。

13.6.9.1　OSI/IP シナリオ 1：IP OSS、IP DCN、ONS GNE、IP DCC、および ONS ENE

図 13-29 に OSI/IP のシナリオ 1（IP DCN、IP-over-PPP DCC、および OSPF ルーティングを使用した、現在の ONS 15454 SDH IP ベースの実装）を示します。

図 13-29　OSI/IP シナリオ 1：IP OSS、IP DCN、ONS GNE、IP DCC、および ONS ENE

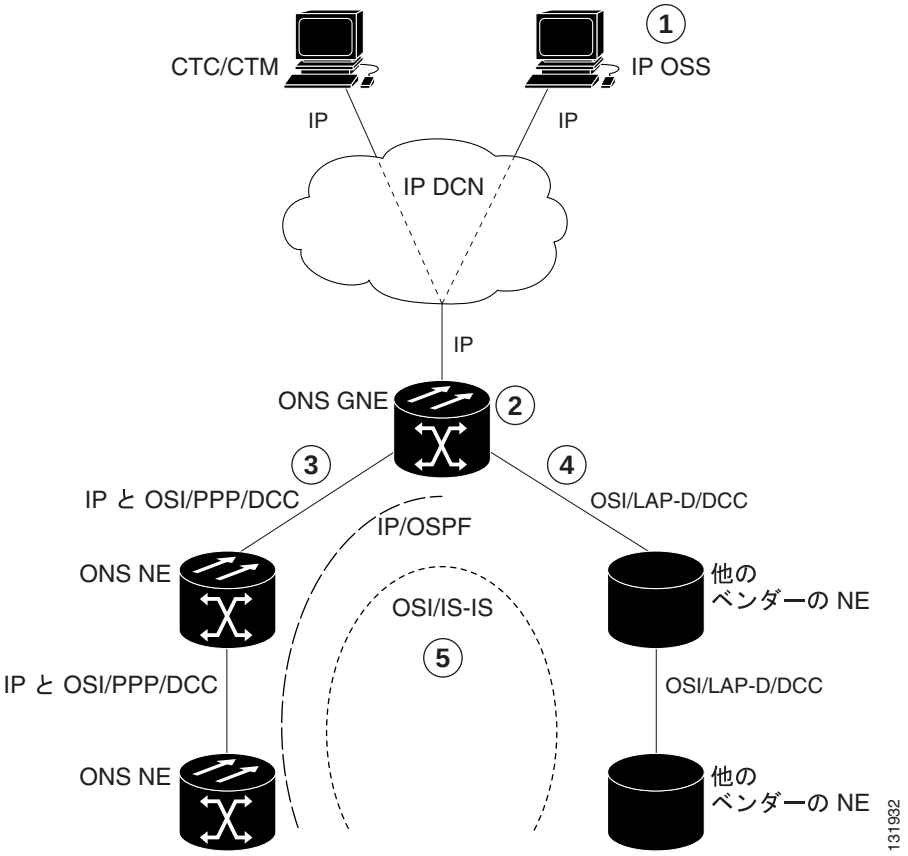


1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH を管理します。
2	DCC は、PPP プロトコルを介して IP を伝送します。
3	ONS 15454 SDH ネットワークは、IP over OSPF によって管理されています。

13.6.9.2　OSI/IP シナリオ 2：IP OSS、IP DCN、ONS GNE、OSI DCC、および他のベンダーの ENE

OSI/IP のシナリオ 2（図 13-30）は、マルチベンダー OSI ネットワークの ONS 15454 SDH GNE を示します。ONS 15454 SDH GNE と他のベンダーの NE の両方が、TL1 と FTP を使用して、IP OSS によって管理されています。また、ONS 15454 SDH は、CTC と Cisco Transport Manager（CTM）によって管理されています。他のベンダーの NE はフル OSI スタックを介して TL1 と FTAM だけをサポートするので、TL1/IP を TL1/OSI に、FTAM/OSI を FTP/IP に変換するために、ONS 15454 SDH GNE は T–TD と FT–TD 間のメディエーションを提供します。

図 13-30　OSI/IP シナリオ 2：IP OSS、IP DCN、ONS GNE、OSI DCC、および他のベンダーの ENE



1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH と他のベンダーの NE を管理します。
2	ONS 15454 SDH GNE は、他のベンダーの NE のメディエーションを実行します。
3	ONS 15454 SDH GNE と ONS 15454 SDH NE 間の DCC は、PPP を介した IP と OSI に対してプロビジョニングされます。
4	ONS 15454 SDH GNE と他のベンダーの NE 間の DCC は、LAP-D を介した OSI に対してプロビジョニングされます。
5	ONS 15454 SDH と他のベンダーの NE ネットワークには、OSPF を介した IP と IS-IS プロトコルを介した OSI が含まれます。

ONS 15454 SDH GNE は、TL1 TID を IP または NSAP アドレスに変化させて、TL1 トラフィックを正しい NE にルーティングします。他のベンダーの NE（OSI 専用ノード）に対する TL1 トラフィックの場合、TID が NSAP アドレスに変化します。ONS 15454 SDH GNE はメディエーション機能に TL1 を渡します。メディエーション機能は、フル OSI スタックを介してカプセル化し、IS-IS プロトコルを使用して宛先にルーティングします。

ONS 15454 SDH NE への TL1 トラフィックの場合、TID は IP および NSAP アドレスの両方に変化します。ONS 15454 SDH GNE は現在の TL1 プロセス モデルに従い、TCP/IP スタックと OSPF ルーティングを使用して宛先 NE に要求を転送します。

OSS で開始されたソフトウェア ダウンロードは、OSS から宛先 NE TL1 のダウンロード要求とファイル転送の 2 つの部分で構成されます。TL1 要求は、前の記述と同じように処理されます。ONS 15454 SDH NE は、ファイル転送に FTP を使用します。OSI 専用の NE は、FTAM を使用して、ファイル転送を実行します。FTAM プロトコルは、OSI NE と ONS 15454 SDH GNE 間を OSI を介して伝送されます。GNE メディエーションは、FTAM と FTP を相互に変換します。

13.6.9.3　OSI/IP シナリオ 3：IP OSS、IP DCN、他のベンダーの GNE、OSI DCC、および ONS ENE

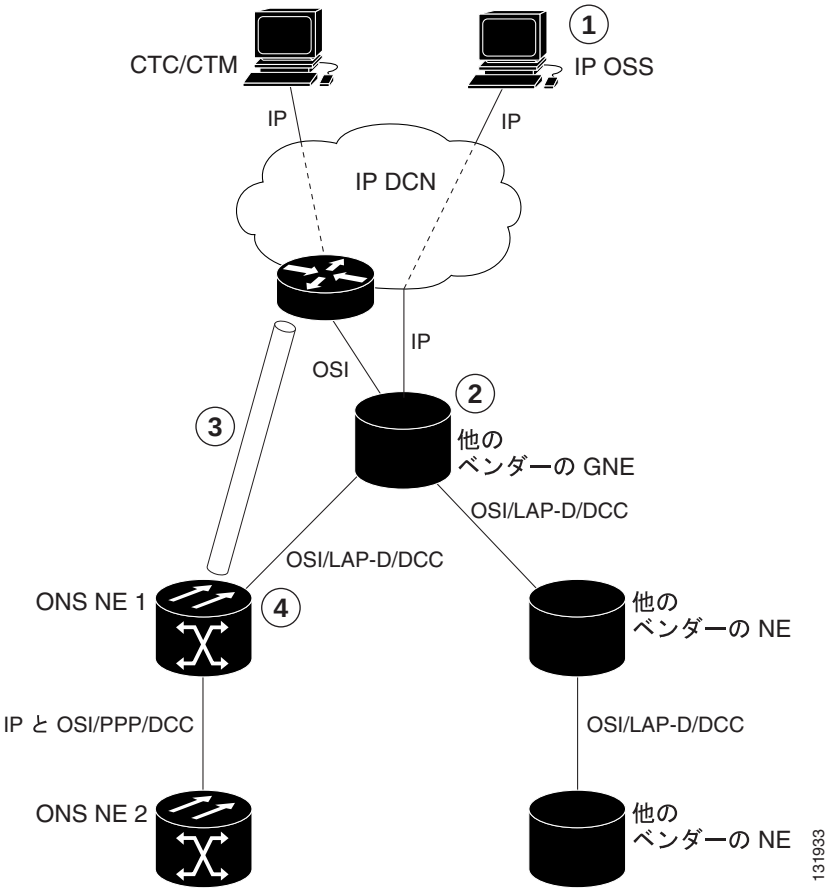
OSI/IP シナリオ 3（図 13-31）では、OSS と GNE 間のすべての TL1 トラフィックが IP DCN を介して交換されます。GNE をターゲットとした TL1 トラフィックは、ローカルで処理されます。他のすべての TL1 トラフィックは OSI スタックに転送され、IP から OSI TL1 の変換を実行します。TL1 はフル OSI スタックでカプセル化され、DCC を介してターゲットの NE に送信されます。すべての NE（ONS 15454 SDH と非 ONS 15454 SDH）が NSAP アドレスを持ち、IS-IS ルーティングをサポートするので、GNE は IS-IS ドメイン内で任意のノードにルーティングできます。

ONS 15454 SDH NE によって受信され、NSAP アドレスにアドレッシングされていない TL1 トラフィックは、IS-IS ルーティングで正しい宛先に転送されます。ONS 15454 SDH NE によって受信され、NSAP アドレスにアドレッシングされた TL1 トラフィックは、OSI スタックからメディエーション機能に送られます。メディエーション機能は、TL1 を抽出して、ONS 15454 SDH TL1 プロセッサに渡します。

OSS によって開始されたソフトウェアのダウンロードには、OSS から宛先ノード TL1 のダウンロード要求とファイル転送が含まれます。TL1 要求は、前の記述と同じように処理されます。GNE は DCC の IP をサポートせず、FTP を転送できないので、ターゲットのノードが FTAM をファイル転送に使用します。したがって、ONS 15454 SDH NE は、OSI GNE に従属する場合に、FTAM クライアントをサポートし、FTAM を使用してファイル転送を開始する必要があります。

このシナリオでは、GNE が IP と OSI DCN 接続の両方を持ちます。GNE は、TL1 と FTP-over-IP のみをサポートします。両方は変換されてから、OSI を介して宛先 ENE（ONS 15454 SDH または OSI 専用の NE）に伝送されます。他のすべての IP トラフィックは、GNE によって廃棄されます。CTC/CTM IP トラフィックは、IP-over-OSI トンネルを介して ONS 15454 SDH NE に伝送されます。トンネルは、外部ルータと ONS 15454 SDH NE の間に作成されます。トラフィックは、トンネルを終端する ONS 15454 SDH に送信されます。その ONS 15454 SDH は、トラフィックをトンネルを介して外部ルータで CTC/CTM に転送します。

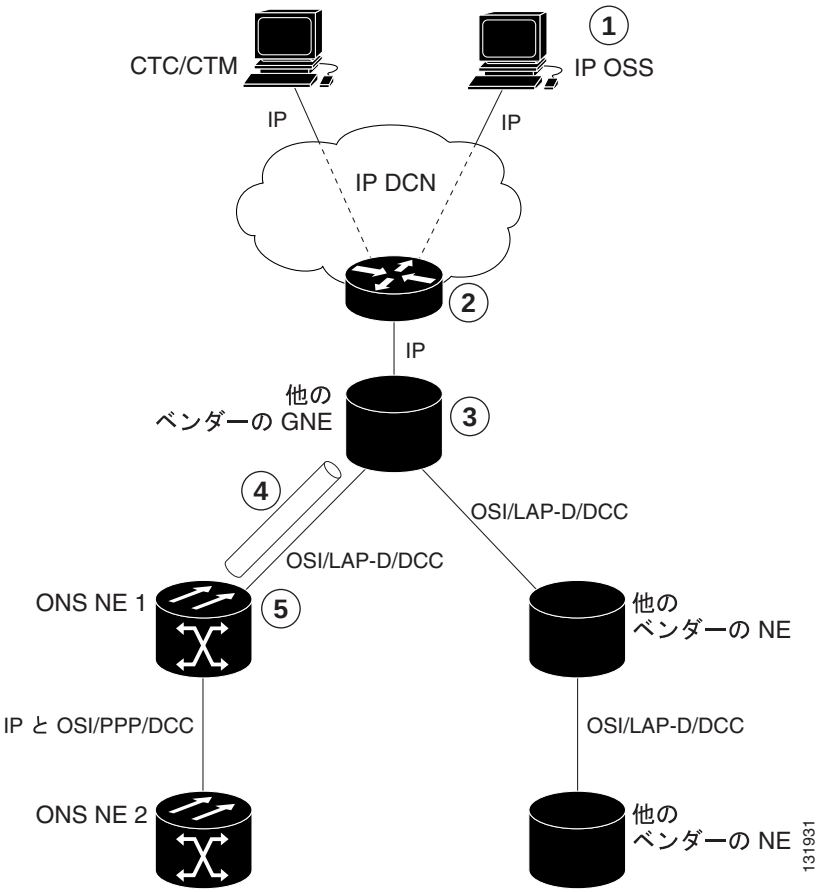
図 13-31　OSI/IP シナリオ 3 : IP OSS、IP DCN、他のベンダーの GNE、OSI DCC、および ONS ENE



1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH と他のベンダーの NE を管理します。
2	他のベンダーの GNE は、TL1 と FTP のメディエーションを実行するので、ONS 15454 SDH と他のベンダーの NE への DCC は OSI 専用になります。
3	CTC/CTM は、IP-over-CLNS トンネルを介して ONS 15454 SDH NE とやり取りします。トンネルは、ONS 15454 SDH ノードから外部ルータに作成されます。
4	ONS 15454 SDH NE は、ファイル転送用に FTAM を使用してフル OSI スタックを介して TL1 を交換します。

図 13-32 に、IP-over-CLNS トンネル エンドポイントが DCN ルータではなく GNE である点だけ異なる同一のシナリオを示します。

図 13-32　OSI/IP シナリオ 3：OSI/IP-over-CLNS トンネル エンドポイントが GNE の場合

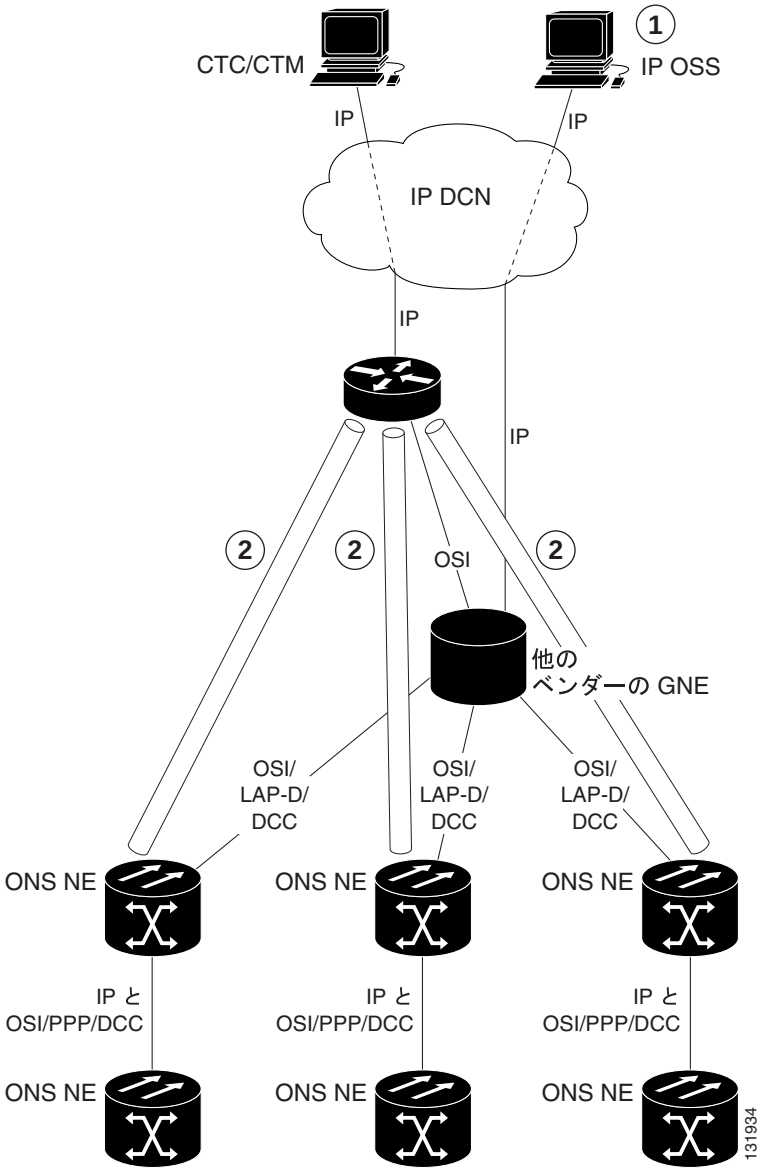


1	IP OSS は、TL1 と FTP を使用して、ONS と他のベンダーの NE を管理します。
2	他のベンダーの GNE は、TL1 と FTP のメディエーションを実行するので、ONS 15454 SDH と他のベンダーの NE への DCC は OSI 専用になります。
3	CTC/CTM は、ONS 15454 SDH と GNE 間を IP-over-CLNS トンネルを介して ONS 15454 SDH NE とやり取りします。
4	ONS 15454 SDH NE は、フル OSI スタックを介して TL1 を交換します。ファイル転送に、FTAM が使用されます。

13.6.9.4　OSI/IP シナリオ 4：複数の ONS DCC 領域

OSI/IP シナリオ 4（図 13-33）は、OSI GNE が複数の分離された ONS 15454 SDH 領域に従属する点を除いて、OSI/IP シナリオ 3 に類似しています。分離された各 ONS 15454 SDH OSPF 領域には、別個の IP-over-CLNS トンネルが必要です。別の方法として、CTC/CTM から ONS 15454 SDH NE に単一 IP-over-CLNS トンネルを作成し、その NE から分離された各 OSPF 領域の NE にトンネルを設定します。この方法には、スタティック ルートの追加が必要になります。

図 13-33　OSI/IP シナリオ 4：複数の ONS DCC 領域

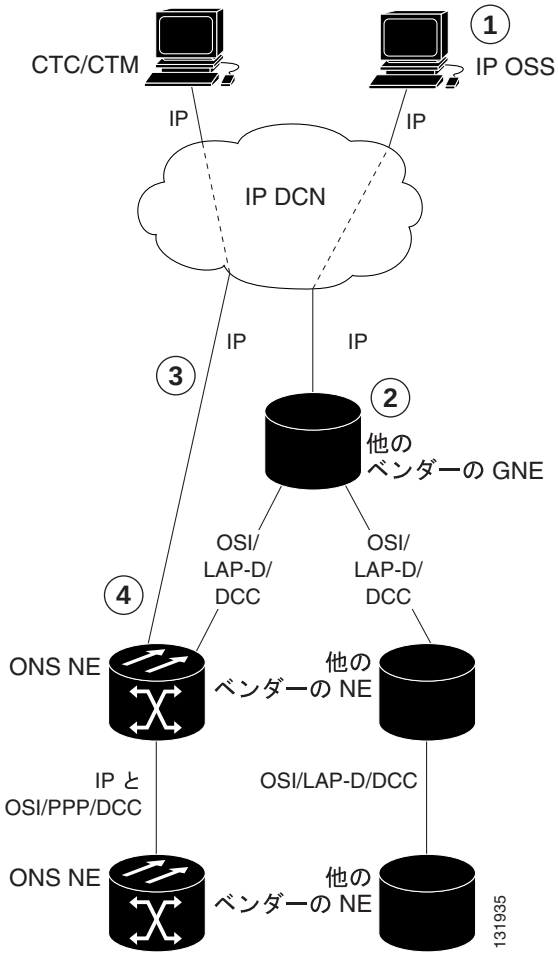


1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH と他のベンダーの NE を管理します。
2	分離された各 ONS 15454 SDH DCC 領域で別個のトンネルが作成されます。

13.6.9.5　OSI/IP シナリオ 5：OSI DCC 接続のない GNE

OSI/IP シナリオ 5（図 13-34）は、OSI GNE に DCN への IP 接続だけがある点を除いて、OSI/IP のシナリオ 3 と類似しています。IP-over-OSI トンネルを介して CTC/CTM IP トラフィックを伝送する OSI DCN 接続はありません。CTC/CTM アクセスを提供するために、ONS 15454 SDH NE 接続への別個の DCN が作成されます。

図 13-34　OSI/IP シナリオ 5：OSI DCC 接続のない GNE

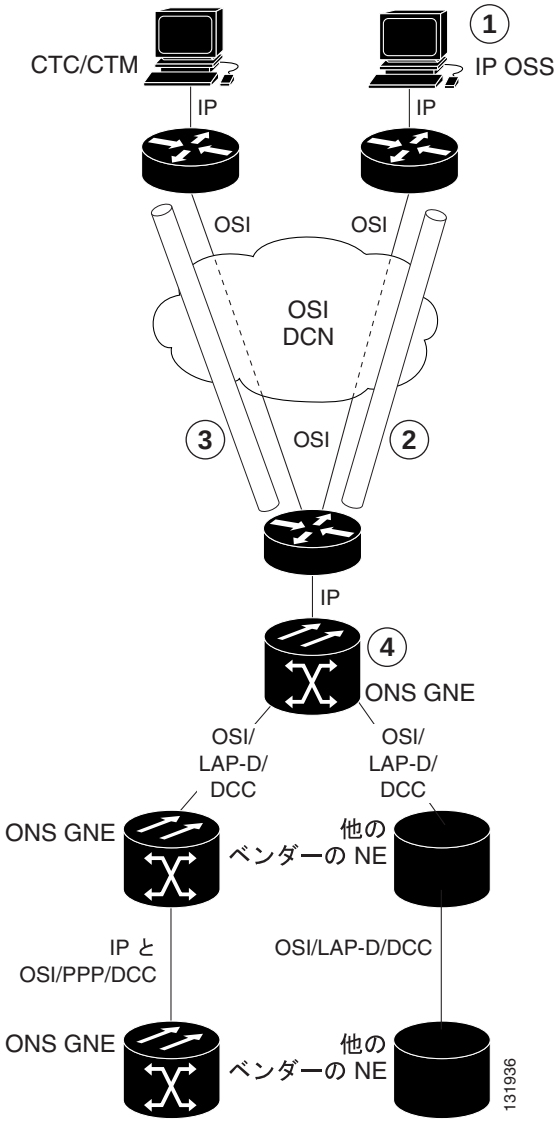


1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH と他のベンダーの NE を管理します。
2	他のベンダーの GNE は、TL1 と FTP のメディエーションを実行するので、DCC は OSI 専用です。
3	CTC/CTM は、別個の IP DCN 接続を介して ONS 15454 SDH NE とやり取りします。
4	ONS 15454 SDH NE は、フル OSI スタックを介して TL1 を交換します。ファイル転送に、FTAM が使用されます。

13.6.9.6　OSI/IP シナリオ 6：IP OSS、OSI DCN、ONS GNE、OSI DCC、および他のベンダーの ENE

OSI/IP シナリオ 6（図 13-35）は、ONS 15454 SDH が OSI DCN をサポートする方法を示します。すべての IP トラフィック（CTC/CTM、FTP、および TL1）は OSI DCN を介してトンネリングされるので、OSI DCN は ONS 15454 SDH に影響しません。

図 13-35　OSI/IP シナリオ 6：IP OSS、OSI DCN、ONS GNE、OSI DCC、および他のベンダーの ENE

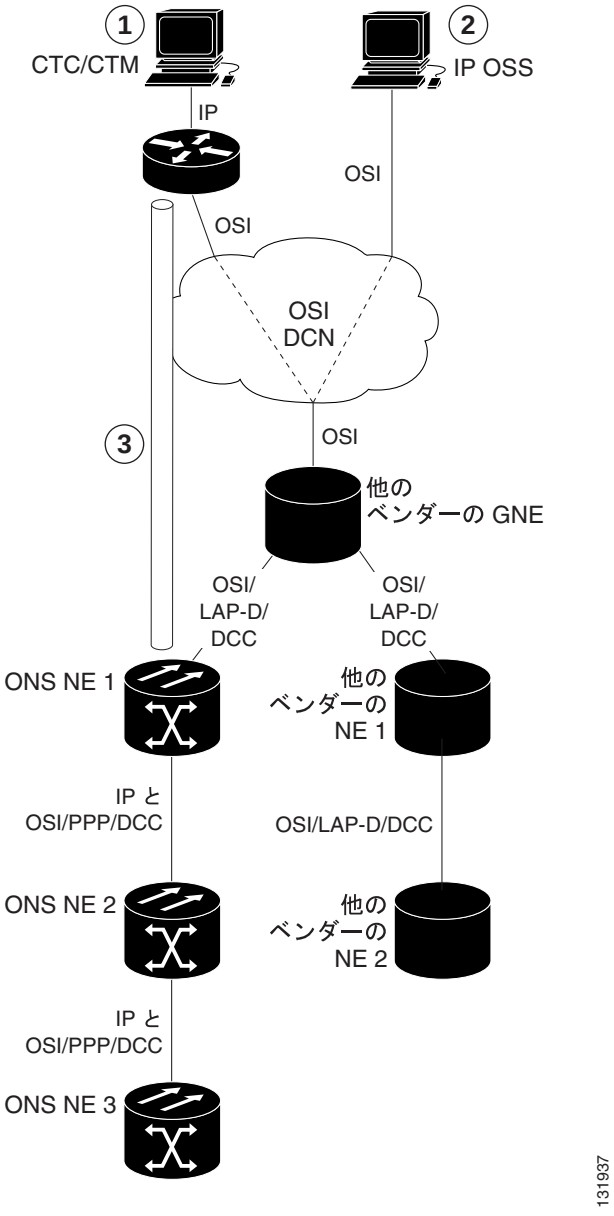


1	IP OSS は、TL1 と FTP を使用して、ONS 15454 SDH と他のベンダーの NE を管理します。
2	OSS IP トラフィックは、DCN を介して ONS 15454 SDH GNE にトンネリングされます。
3	CTC/CTM IP トラフィックは、DCN を介して ONS 15454 SDH GNE にトンネリングされます。
4	GNE は、他のベンダーの NE のメディエーションを実行します。

13.6.9.7　OSI/IP シナリオ 7 : OSI OSS、OSI DCN、他のベンダーの GNE、OSI DCC、および ONS NE

OSI/IP シナリオ 7（図 13-36）は、欧州のネットワークの例を示します。

図 13-36　OSI/IP シナリオ 7 : OSI OSS、OSI DCN、他のベンダーの GNE、OSI DCC、および ONS NE



1	ONS 15454 SDH NE は、CTC/CTM のみによって管理されています（TL1/FTP は使用されていません）。
2	OSI OSS は、他のベンダーの NE のみを管理します。
3	CTC/CTM は、ONS 15454 SDH NE と 外部ルータ間を IP-over-CLNS トンネルを介して ONS 15454 SDH とやり取りします。

欧州のネットワークの場合、次のようになります。

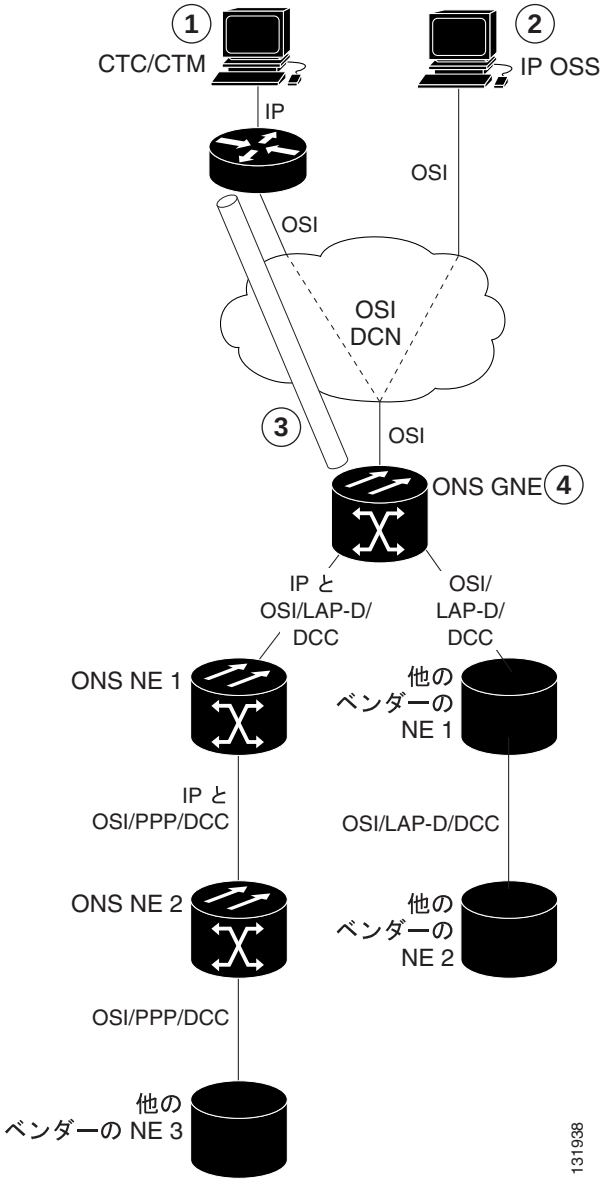
- CTC と CTM は、管理用にのみ使用されます。
- IP-over-CLNS トンネルは、幅広く受け入れられ、使用されています。
- TL1 管理は、必要ありません。
- FTP ファイル転送は、必要ありません。
- TL1/FTAM と FTP のメディエーションは、必要ありません。

CTC/CTM と ONS 15454 SDH NE 間の管理トラフィックは、IP-over-CLNS トンネルを介して伝送されます。スタティック ルートは、トンネル（ONS 15454 SDH NE 1）を終端する ONS 15454 SDH に設定されるので、ダウンストリームの ONS 15454 SDH NE（ONS 15454 SDH NE 2 と 3）は CTC/CTM に到達するための方法を認識します。

13.6.9.8　OSI/IP シナリオ 8：OSI OSS、OSI DCN、ONS GNE、OSI DCC、および他のベンダーの NE

OSI/IP シナリオ 8（図 13-37）は、欧州ネットワークの別の例を示します。OSI/IP のシナリオ 7 と同様に、ONS 15454 SDH NE は CTC/CTM によってのみ管理されます。CTC/CTM IP トラフィックは、IP-over-OSI トンネルを介して、外部ルータと ONS 15454 SDH GNE 間で伝送されます。GNE はトンネルから IP を抽出し、宛先 ONS 15454 SDH に転送します。OSS と他のベンダーの NE 間の管理トラフィックは、ONS 15454 SDH GNE と NE によってルーティングされます。すべての ONS 15454 SDH NE がデュアル スタック（OSI と IP）を実行するので、ルーティングが可能になります。

図 13-37　OSI/IP シナリオ 8 : OSI OSS、OSI DCN、ONS GNE、OSI DCC、および他のベンダーの NE



1	ONS NE は、CTC/CTM のみによって管理されています（TL1/FTP は使用されていません）。
2	OSI OSS は、他のベンダーの NE のみを管理します。
3	CTC/CTM は、ONS 15454 SDH NE と 外部ルータ間を IP-over-CLNS トンネルを介して ONS 15454 SDH とやり取りします。GNE には、スタティック ルートが必要になります。
4	ONS 15454 SDH GNE は、他のベンダーの NE に OSI トラフィックをルーティングします。IP-over-CLNS トンネルは、必要ありません。

13.6.10　CTC における OSI のプロビジョニング

表 13-15 に、ノード ビューの Provisioning タブで実行される OSI アクションを示します。OSI の手順およびタスクについては、『*Cisco ONS 15454 SDH Procedure Guide*』を参照してください。

表 13-15　CTC Provisioning タブの OSI アクション

タブ	アクション
OSI > Main Setup	• Primary Area Address を表示し、編集します。 • OSI ルーティング モードを変更します。 • LSP バッファを変更します。
OSI > TARP > Config	次の TARP パラメータを設定します。 • PDU L1/L2 伝播および発信元 • TARP データ キャッシュおよび LDB • LAN ストーム抑制 • 起動時の Type 4 の PDU • TARP タイマー：LDB、T1、T2、T3、T4
OSI > TARP > Static TDC	スタティック TARP データ キャッシュのエントリを追加および削除します。
OSI > TARP > MAT	スタティック手動領域のテーブル エントリを追加および削除します。
OSI > Routers > Setup	• ルータを有効および無効にします。 • 手動領域のアドレスを追加、削除、および編集します。
OSI > Routers > Subnets	OSI に対してプロビジョニングされている RS-DCC、MS-DCC、および LAN のサブネットを編集します。
OSI > Tunnels	Cisco トンネルおよび IP-over-CLNS トンネルを追加、削除、および編集します。
Comm Channels > RS-DCC	• RS-DCC に OSI 構成を追加します。 • データ リンク レイヤ プロトコル（PPP または LAP-D）を選択します。
Comm Channels > MS-DCC	• RS-DCC に OSI 構成を追加します。

表 13-16 に、ノード ビューの Maintenance タブで実行される OSI アクションを示します。

表 13-16　CTC Maintenance タブの OSI アクション

タブ	アクション
OSI > ISIS RIB	IS-IS ルーティング テーブルを表示します。
OSI > ESIS RIB	IS に接続されている ES を表示します。
OSI > TDC	• TARP　データ　キャッシュを表示し、スタティックおよびダイナミックなエントリを識別します。 • TID から NSAP への変換を実行します。 • TDC を消去します。

13.7　IPv6 ネットワークの互換性

Cisco ONS 15xxx 製品は、Network Address Translation - Protocol Translation（NAT-PT）をサポートするインターネット ルータが、ONS 15454 SDH などの GNE とクライアント ワークステーション間に配置されている場合に、IPv6 ネットワークで機能することができます。NAT-PT は、RFC-2766 で定義されます。IPv4 ノードと IPv6 ノードは、IPv6 DCN と IPv4 DCC ネットワーク間での IPv6 と IPv4 両方のスタックのインターフェイス接続を許可することで NAT-PT を使用して互いに通信します。

NAT-PT は、IPv6 ネットワークのアドレスを IPv4 ネットワークのアドレスに（またはその逆に）バインドし、アドレス タイプ間で搬送されるパケットに透過ルーティングを提供します。この場合、エンド ノードへの変更は必要なく、IP パケット ルーティングはエンド ノードに対して完全に透過的です。ただし、NAT-PT はサポートするセッションを追跡する必要があり、また、セッションに関連する着信および発信データグラムが同じ NAT-PT ルータを通るようにする必要があります。プロトコル変換は、プロトコル構文 / セマンティクス変換を使用してアドレス変換を拡張するときに使用されます。

（注）　IPv6 ネットワークとインターフェイス接続されているクライアントでは、Mozilla 1.7 のみがサポートされます。