CHAPTER 8

管理ネットワークの接続

この章では、ONS 15454 Data Communication 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）ネットワークの通信は、Cisco Transpot Controller（CTC）コンピュータと ONS 15454 ノード間の通信、ネットワーク接続された ONS 15454 ノード間の通信を含め、IP に基づいて行われます。この章では、一般的な IP ネットワーク構成における Cisco ONS 15454 ノードのシナリオを紹介するとともに、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、開放型 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説明します。

ONS 15454 DCN の通信は IP ベースですが、ONS 15454 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 スイートに基づいた機器にネットワーク接続できます。この章では、ONS 15454 OSI の実装についても説明し、IP と OSI が混在する環境で ONS 15454 をネットワーク接続するシナリオを紹介します。

この章では、IP ネットワーキング全般の概念や手順については説明しません。また、あらゆるネットワーク状況に対応する IP アドレッシングの例も紹介しません。ONS 15454 ネットワーキング設定手順については、『*Cisco ONS 15454 DWDM Procedure Guide*』の「Turn Up a Node」の章を参照してください。

（注） この章では、特に指定のないかぎり、[ONS 15454] は ANSI と ETSI の両方のシェルフ アセンブリを意味します。

この章では、次の内容について説明します。

（注）　ONS 15454 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。

8.1　IP ネットワーキングの概要

IP 環境で ONS 15454 を接続する方法は、いろいろあります。

- 直接接続またはルータを使用して LAN に接続する。
- IP サブネット化で ONS 15454 ノード グループを作成する。このノード グループにより、ネットワーク内のノードに接続された非 Data Communication Channel（DCC; データ通信チャネル）をプロビジョニングできます。
- さまざまな IP 機能とプロトコルを使用してネットワーク上で特定の作業を行う。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 を、LAN に接続されていない ONS 15454 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 Cisco Transport Controller（CTC）セッションを使用して、複数の CTC セッションがある同じサブネット上の ONS 15454 を接続する。
- ONS 15454 を Open Shortest Path First（OSPF）ネットワークに接続し、ONS 15454 ネットワークの情報を複数の LAN や WAN で自動的に通信する。
- ONS 15454 プロキシ サーバは、CTC コンピュータと ONS 15454 要素ノードの間の可視性とアクセス可能性を制御します。

8.2　IP アドレッシング シナリオ

ONS 15454 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 8-1 に、IP ネットワークで ONS 15454 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。

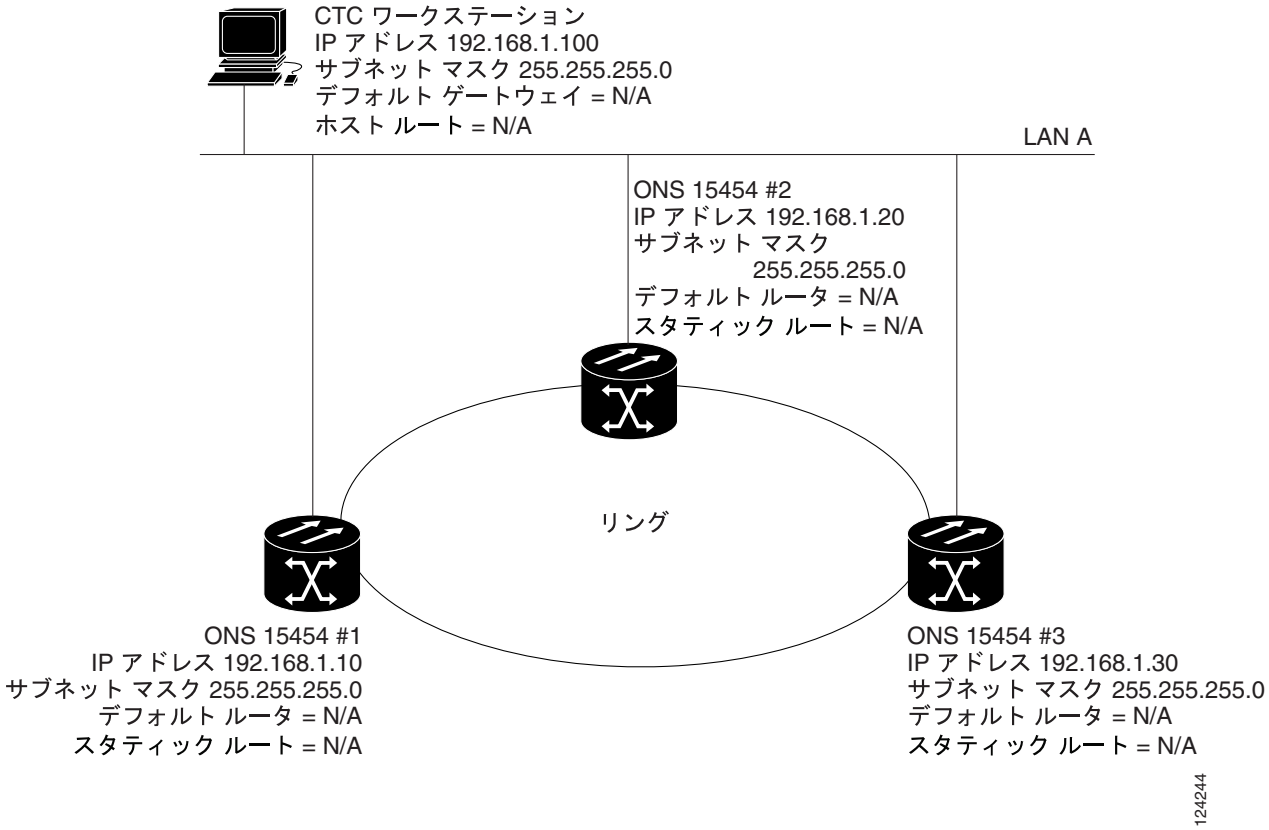
表 8-1　ONS 15454 の一般的な IP トラブルシューティングのチェックリスト

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（バックプレーン [ANSI] または MIC-C/T/P [ETSI] ワイヤラップ 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 ハブ ポート / スイッチ ポート	接続で問題が発生した場合は、ONS 15454 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 の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 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。
光接続	ONS 15454 の光トランク ポートが稼働中で、DCC が各トランク ポートでイネーブルであることを確認します。

8.2.1　シナリオ 1：同一サブネット上の CTC および ONS 15454

シナリオ 1 は、ONS 15454 の基本的な LAN 構成を示します（図 8-1）。ONS 15454 と CTC コンピュータは同一サブネット上に存在します。すべての ONS 15454 が LAN A に接続され、すべての ONS 15454 が DCC 接続されています。

図 8-1　シナリオ 1：同一サブネット上の CTC と ONS 15454（ANSI および ETSI）

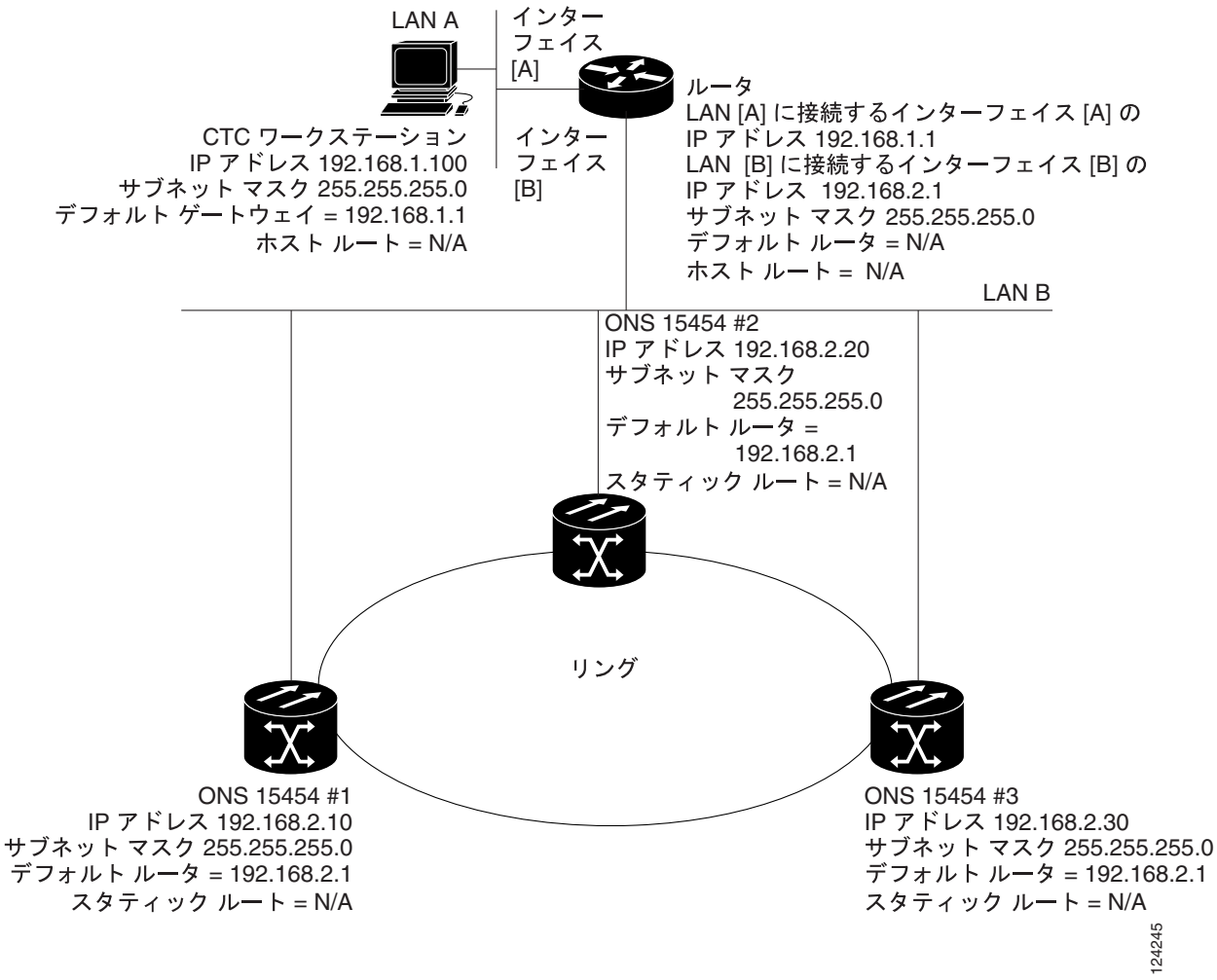


8.2.2　シナリオ 2：ルータに接続された CTC および ONS 15454

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（図 8-2）に接続されています。ONS 15454 は異なるサブネット（192.168.2.0）上にあり、すべて 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。各ルータのサブネットマスクは 255.255.255.0 です。

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; ダイナミック ホスト コンフィギュレーション プロトコル）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 8-2 では、DHCP サーバを使用していません。

図 8-2　シナリオ 2：ルータに接続された CTC と ONS 15454（ANSI および ETSI）



8.2.3　シナリオ 3：プロキシ ARP による ONS 15454 ゲートウェイのイネーブル化

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信します。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）を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 は、LAN に接続されていない ONS 15454 の ARP 要求に応答できます（ONS 15454 プロキシ ARP に対する設定は必要ありません）。ただし、DCC 接続の ONS 15454 が LAN 接続（ゲートウェイ）の ONS 15454 と同じサブネット上に存在する必要があります。LAN 装置が LAN に接続されていない ONS 15454 に ARP 要求を送信すると、（LAN に接続されている）ゲートウェイ ONS 15454 が LAN 装置に MAC（メディア アクセス制御）アドレスを返します。LAN 装置は、次にリモートの ONS 15454 宛てのデータグラムを、このプロキシ ONS 15454 の MAC アドレスに送信します。プロキシ ONS 15454 は自身の ARP 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 に送信します。

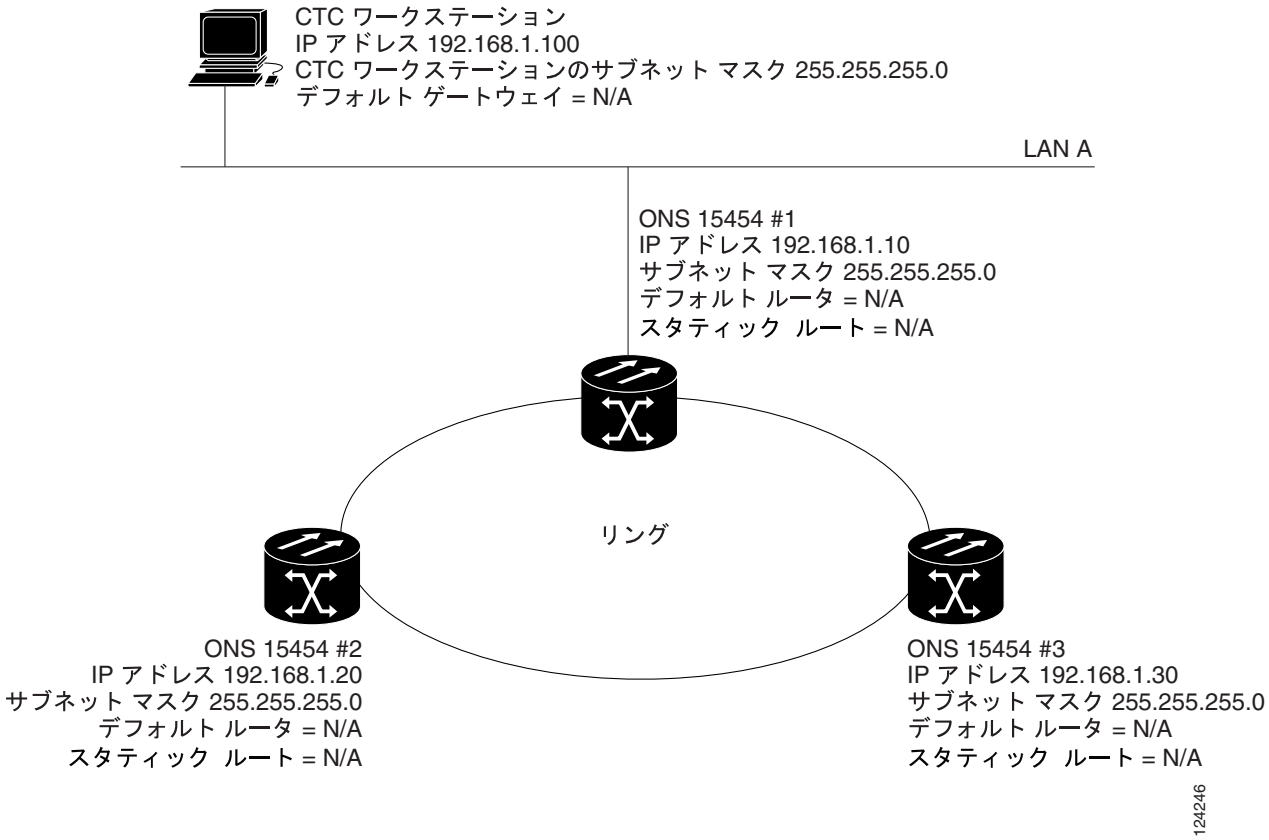
シナリオ 3 はシナリオ 1 に似ていますが、LAN に接続されている ONS 15454（ノード 1）は 1 つだけです（図 8-3）。2 つの ONS 15454（ノード 2 およびノード 3）がセクション DCC を介して ONS 15454 ノード 1 に接続されています。3 つの ONS 15454 がすべて同じサブネット上にあるため、プロキシ ARP は ONS 15454 ノード 1 をイネーブルにして、ONS 15345 ノード 2 およびノード 3 のゲートウェイとして使用することができます。

（注）　このシナリオでは、すべての CTC がノード 1 に接続されているものと仮定しています。ラップトップ コンピュータが ONS 15454 ノード 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にも、表示できないノードがあります。ラップトップを終端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 プロキシ サーバ（シナリオ 7 参照）をイネーブルにする必要があります。

次のことに注意してください。

- GNE および ENE 15454 プロキシ ARP はディセーブルにされています。
- 指定されたイーサネット セグメント上に存在するプロキシ ARP サーバは 1 つです。ただし、ANSI または ETSI トポロジーには複数のサーバが存在する場合もあります。
- このプロキシ ARP サーバは同じイーサネット セグメント上にある任意のノードまたはホストに対してプロキシ ARP 機能を実行しません。
- 図 8-3 では、CTC ワークステーションがプロキシ ARP サーバと同じサブネットおよびイーサネット セグメントに配置されていることが重要です。

図 8-3　シナリオ 3：プロキシ ARP の使用（ANSI および ETSI）

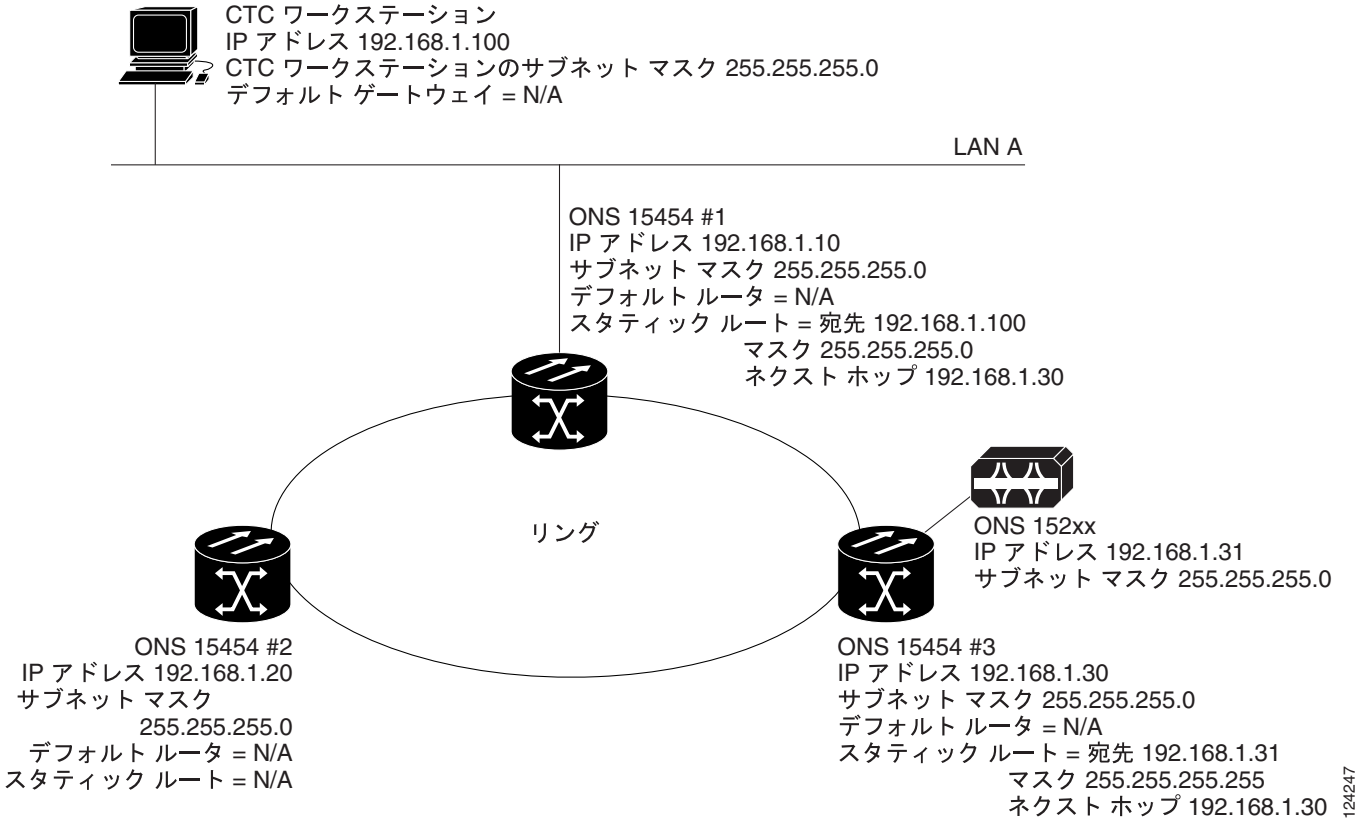


また、プロキシ ARP を使用して、DCC 接続されたノードのクラフト イーサネット ポートに接続されているホストと通信することもできます（図 8-4）。ホストが接続されているノードは、そのホストへのスタティック ルートがなければなりません。スタティック ルートは、OSPF によってすべての DCC ピアへ伝播されます。ホストを追加した場合、既存のプロキシ ARP ノードがゲートウェイになります。各ノードは、同じサブネット上にあって DCC ネットワークに接続されていないホストへのルートを、それぞれのルーティング テーブルで調べます。このような追加ホストに対する ARP 要求には、対象ノードの MAC アドレスを使用して既存のプロキシ サーバが応答します。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、追加ホストにアドレス指定されている IP パケットを正常にルーティングできます。ノードと追加ホスト間のスタティック ルートを確立する以外に、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。

- 指定した任意の追加ホストのプロキシ ARP サーバとして機能できるノードは 1 つのみ。
- ノードは、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 にすることはできません。

図 8-4 では、ノード 1 は、ノード 2 および 3 に対し、ノード 1 が CTC ホストに到達できることを通知します。同様に、ノード 3 は、ノード 3 が ONS 152xx に到達できることを通知します。図では例として、ONS 152xx が示されていますが、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。

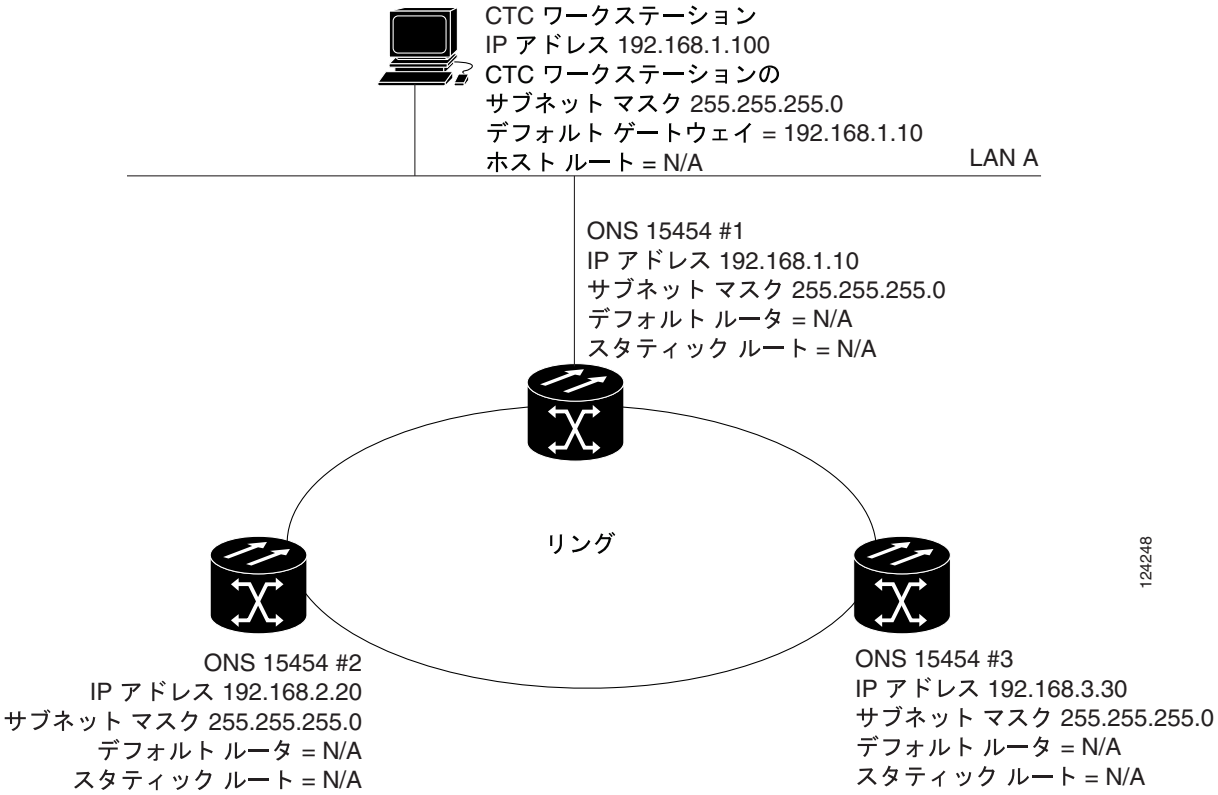
図 8-4　シナリオ 3：スタティック ルーティングでのプロキシ ARP の使用（ANSI および ETSI）



8.2.4　シナリオ 4：CTC コンピュータ上のデフォルト 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にあります（図 8-5）。ノード 1 と CTC コンピュータはサブネット 192.168.1.0 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 は使用しません。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 8-5　シナリオ 4：CTC コンピュータのデフォルト ゲートウェイ（ANSI および ETSI）



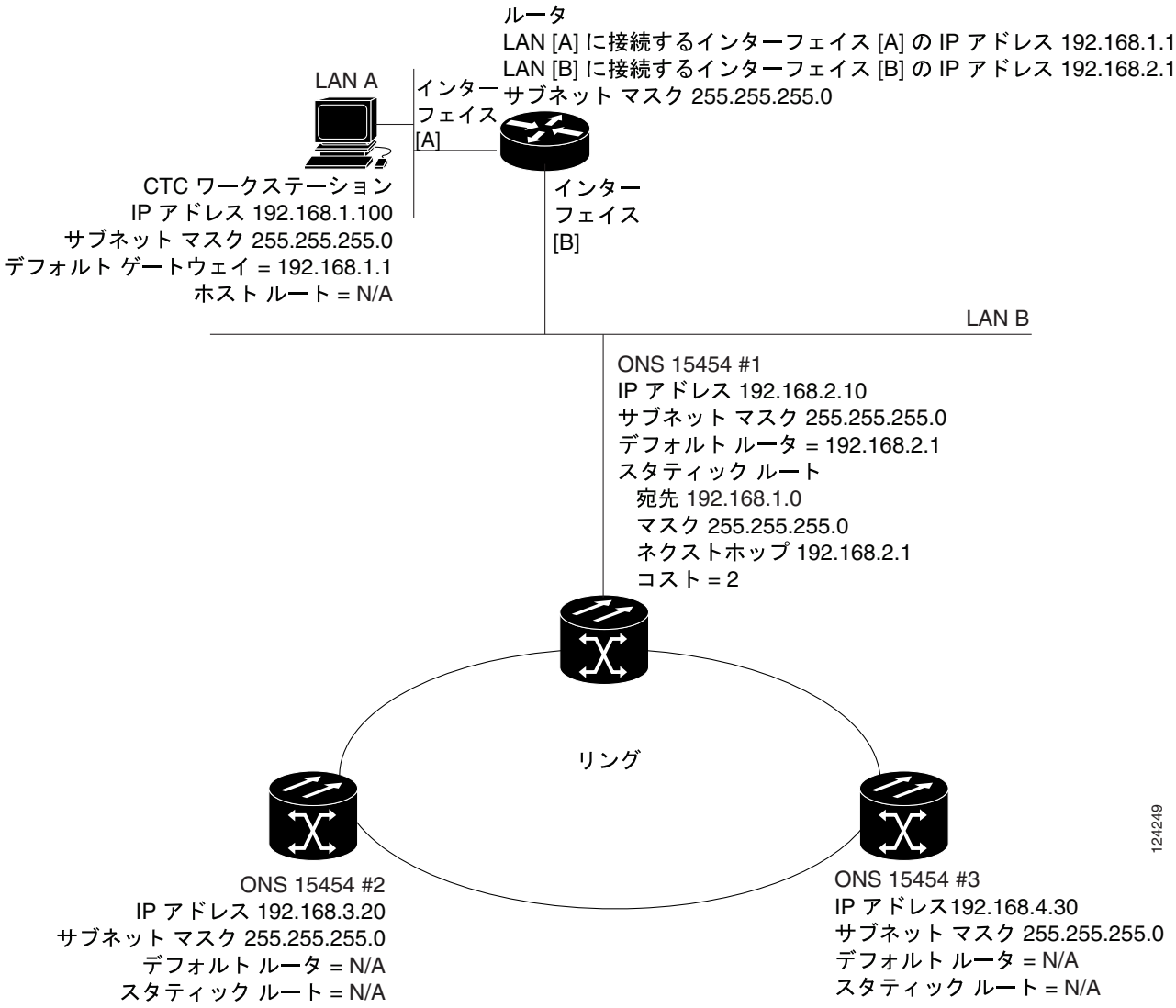
8.2.5　シナリオ 5：スタティック ルートを使用した LAN 接続

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 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 に接続します（OSPF がイネーブルの場合には、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 の間で複数の CTC セッションをイネーブルにします。

図 8-6 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 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イネーブルにしません。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 8-6　シナリオ 5：宛先として使用される CTC コンピュータのスタティック ルート（ANSI および ETSI）

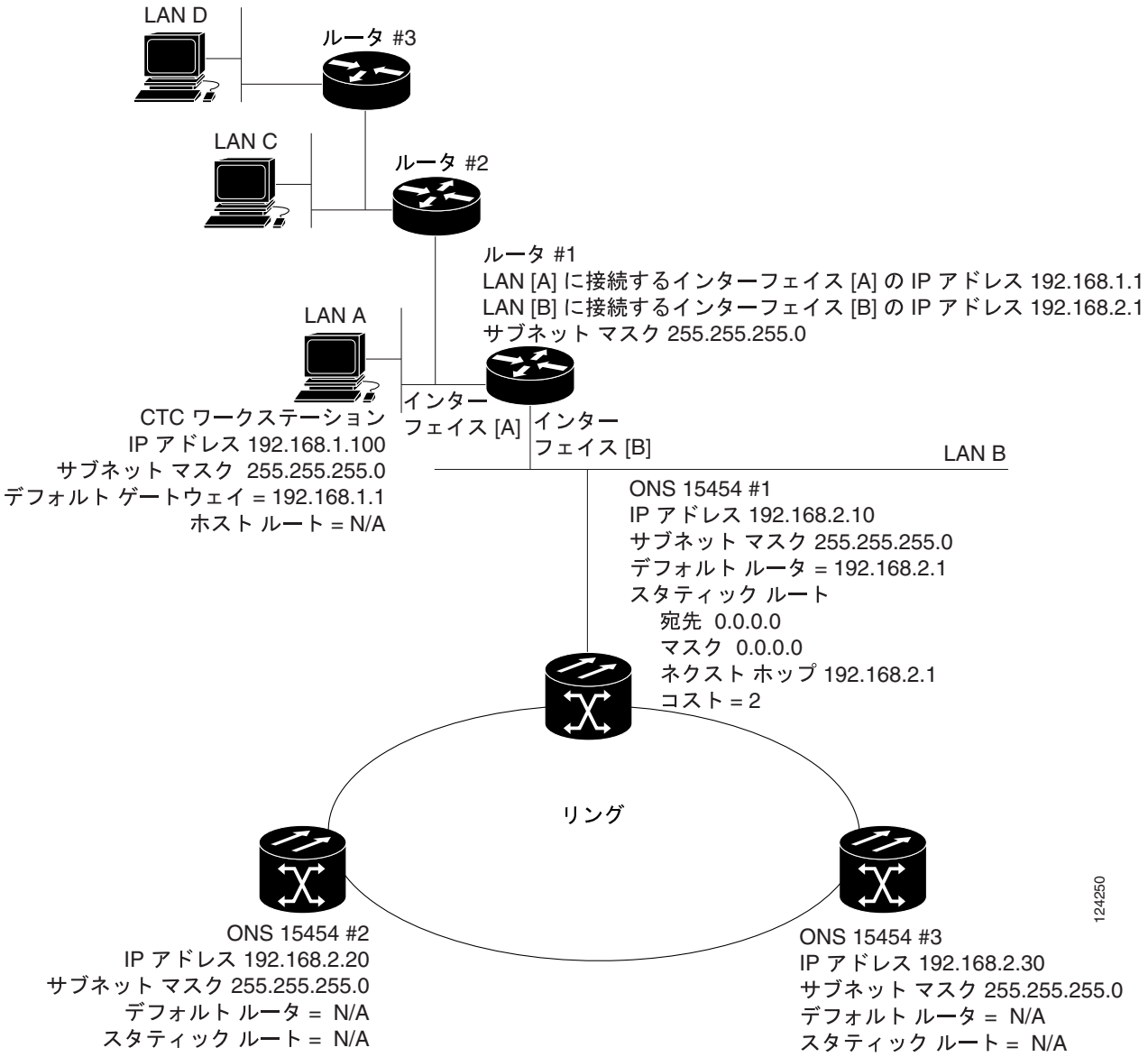


宛先エントリとサブネット マスク エントリは、ONS 15454 へのアクセスを制御します。

- 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 8-7 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（送信元から宛先へのホップの数）は 2 です。

図 8-7　シナリオ 5：複数の LAN 宛先のスタティック ルート（ANSI および ETSI）



8.2.6　シナリオ 6：OSPF の使用

OSPF は、リンクステート インターネット 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とのリンクをモニタリングしたり、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を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」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ーを作成します。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、トポロジーが変更されたときに再計算されます。

ONS 15454 は内部 ONS 15454 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 で OSPF をイネーブルにすることで、ONS 15454 トポロジーが LAN 上の OSPF ルータに送信されます。ONS 15454 ネットワーク トポロジーを LAN ルータにアドバタイズすることで、ONS 15454 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。図 8-8 に、OSPF がイネーブルにされたネットワークを示します。図 8-9 に、OSPF が使用されていない同一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。

OSPF は、ネットワークを、領域と呼ばれる小さなリージョンに分割します。領域は、トラフィック パターン別に構成す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まりです。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 OSPF トポロジーをイネーブルにする場合は、ONS 15454 ネットワークに 10 進形式の OSPF 領域 ID を割り当てる必要があります。領域 ID は IP アドレスに類似した「ドットで区切られた 4 つの」値です。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 には、同じ OSPF 領域 ID を割り当ててください。

（注） OSPF 領域の 15454 の数を制限することを推奨します。それにより CTC へのロード時間が短縮され、エラーが発生する可能性も減少します。

図 8-8　シナリオ 6：OSPF がイネーブルになっているネットワーク（ANSI および ETSI）

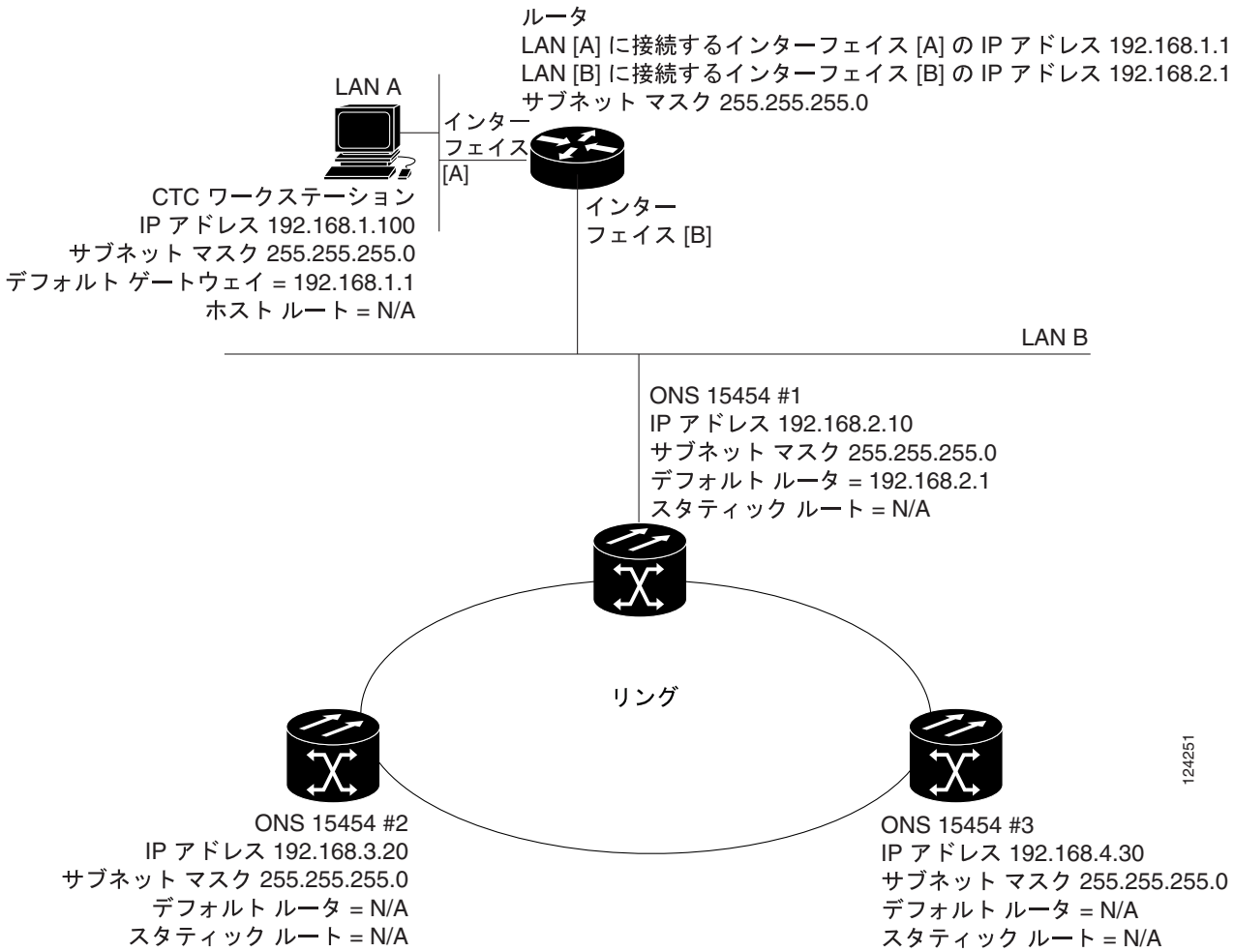
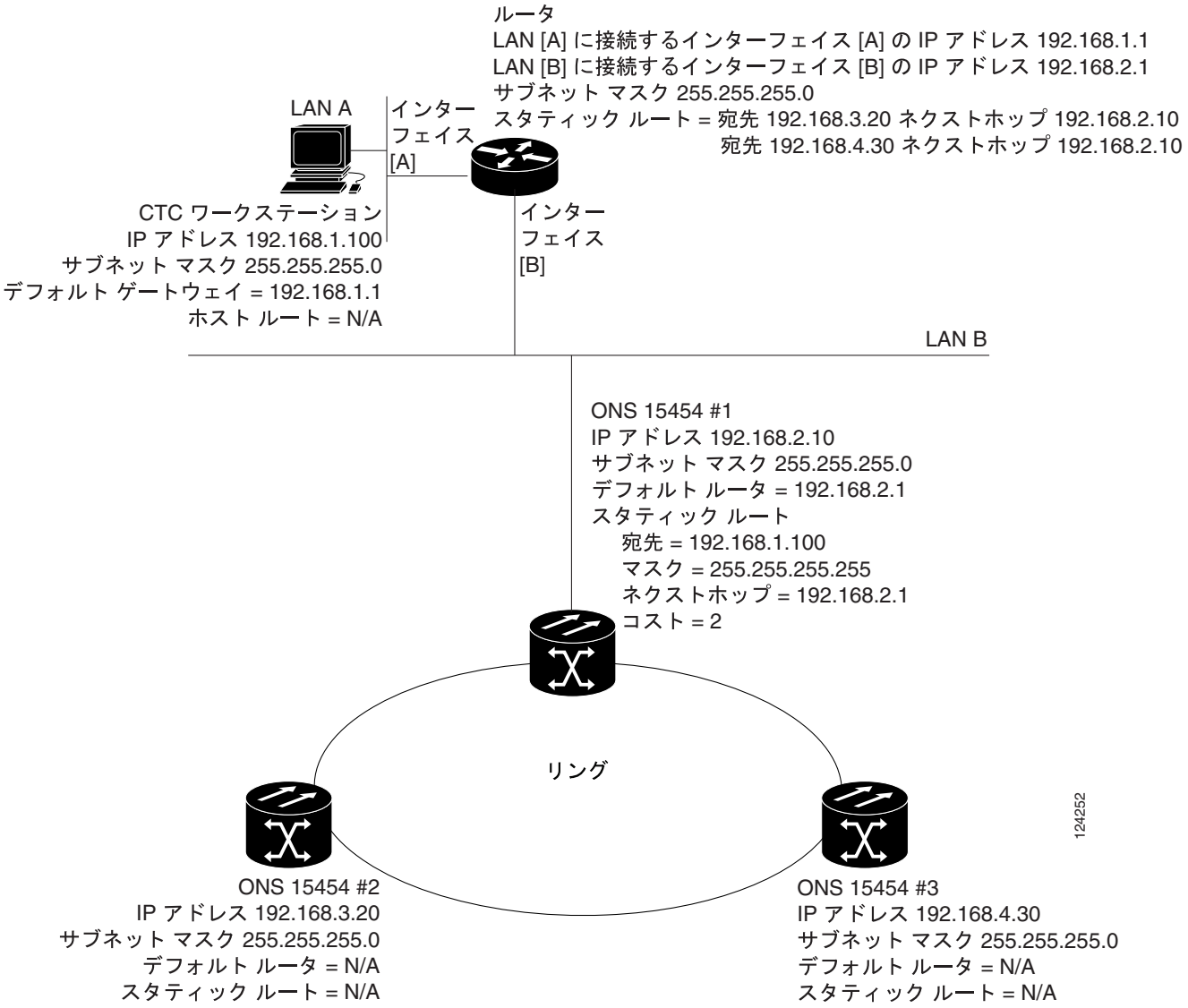


図 8-9　シナリオ 6：OSPF がイネーブルではないネットワーク（ANSI および ETSI）



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

ONS 15454 プロキシ サーバは、ONS 15454 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 をネットワーク接続できるようにする機能セットです。たとえば、ネットワークを設定して、現場技術者が Network Operations Center（NOC）LAN にアクセスするのを制限しながら、現場技術者と NOC の担当者の両者が同じ ONS 15454 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 を Gateway Network Element（GNE; ゲートウェイ ネットワーク要素）として設定し、他の ONS 15454 を End Network Element（ENE; 終端ネットワーク要素）として設定します。GNE ONS 15454 は CTC コンピュータと ENE ONS 15454 の間の接続をトンネルし、ONS 15454 管理目的以外のアクセスを制限しながら管理できます。

ONS 15454 ゲートウェイの設定により、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 8-3 および 表 8-4 を参照）は、パケットが ONS 15454 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）の要求を処理する。ONS 15454 ENE は、SNTP/NTP LAN サーバから GNE ONS 15454 を介して Time-of-Day（ToD）を得ることができます。
- SNMP version 1（SNMPv1; 簡易ネットワーク管理プロトコル バージョン 1）トラップを処理する。GNE ONS 15454 は、SNMPv1 トラップを ENE ONS 15454 から受信し、そのトラップを SNMPv1 トラップ宛先または ONS 15454 SNMP リレー ノードに転送またはリレーします。

ONS 15454 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。このチェックボックスを選択すると、ONS 15454 は CTC クライアントとプロキシ ONS 15454 に DCC 接続されている ONS 15454 の間の接続用にプロキシとして動作します。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 クライアントが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。チェックボックスを選択しない場合には、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。

- ENE — ENE として設定すると、ONS 15454 はイーサネット ポートを通るデフォルト ルートやスタティック ルートの設定もアドバタイズも行いません。ただし、ENE は DCC を通るルートに対して設定およびアドバタイズを行います。CTC コンピュータは、TCC2/TCC2P クラフト ポートを使用して ONS 15454 と通信できますが、DCC 接続された他の ONS 15454 には直接通信できません。

  また、ファイアウォールがイネーブルになり、ノードで DCC と LAN ポート間の IP トラフィックがルーティングされなくなります。ONS 15454 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。
- 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イネーブルになります。
- プロキシのみ — プロキシのみを選択すると、ファイアウォールはイネーブルになりません。CTC は他の DCC 接続された ONS 15454 と通信できます。

（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イネーブル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。プロキシが誤ってディセーブルになった場合は、再接続時にプロキシをイネーブルにして、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。

図 8-10 に、ONS 15454 プロキシ サーバの実装を示します。GNE ONS 15454 は、セントラル オフィス LAN と ENE ONS 15454 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 コンピュータとクラフト技術者の両方が、ONS 15454 ENE にアクセスできる必要があります。ただし、クラフト技術者が NOC やセントラル オフィス LAN にアクセスしたり、参照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 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 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、私設ネットワーク IP アドレスが割り当てられています。複数の ONS 15454 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 8-10　シナリオ 7：同一サブネット上に GNE と ENE を備えた ONS 15454 プロキシ サーバ（ANSI および ETSI）

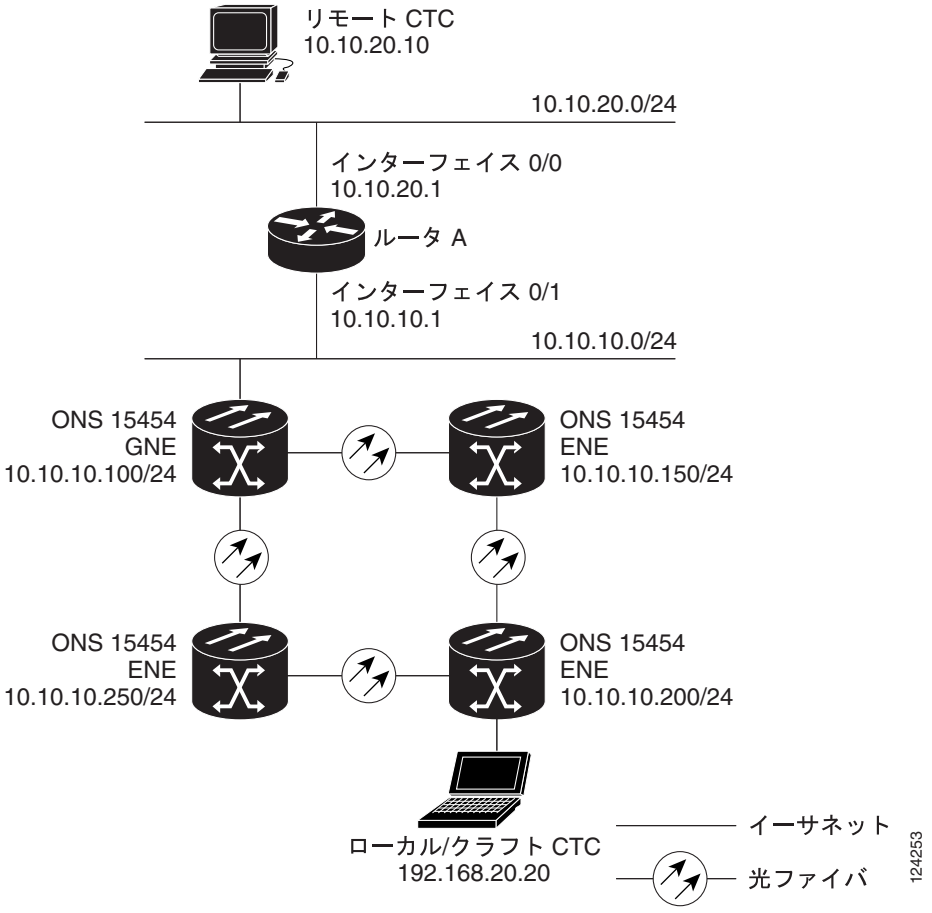


表 8-2 に、図 8-10 の構成における ONS 15454 GNE および ENE の推奨設定値を示します。

表 8-2　ONS 15454 GNE および ENE の設定

設定	ONS 15454 GNE	ONS 15454 ENE
OSPF	オフ	オフ
SNTP サーバ（使用している場合）	SNTP サーバの IP アドレス	ONS 15454 GNE 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 GNE、ポート 391 に設定

図 8-11 に、異なるサブネット上にある ONS 15454 ENE を使用したプロキシ サーバの実装を示します。ONS 15454 GNE および ENE は表 8-2 に示す設定でプロビジョニングされます。

図 8-11　シナリオ 7:異なるサブネット上に GNE と ENE を備えた ONS 15454 プロキシ サーバ(ANSI および ETSI)

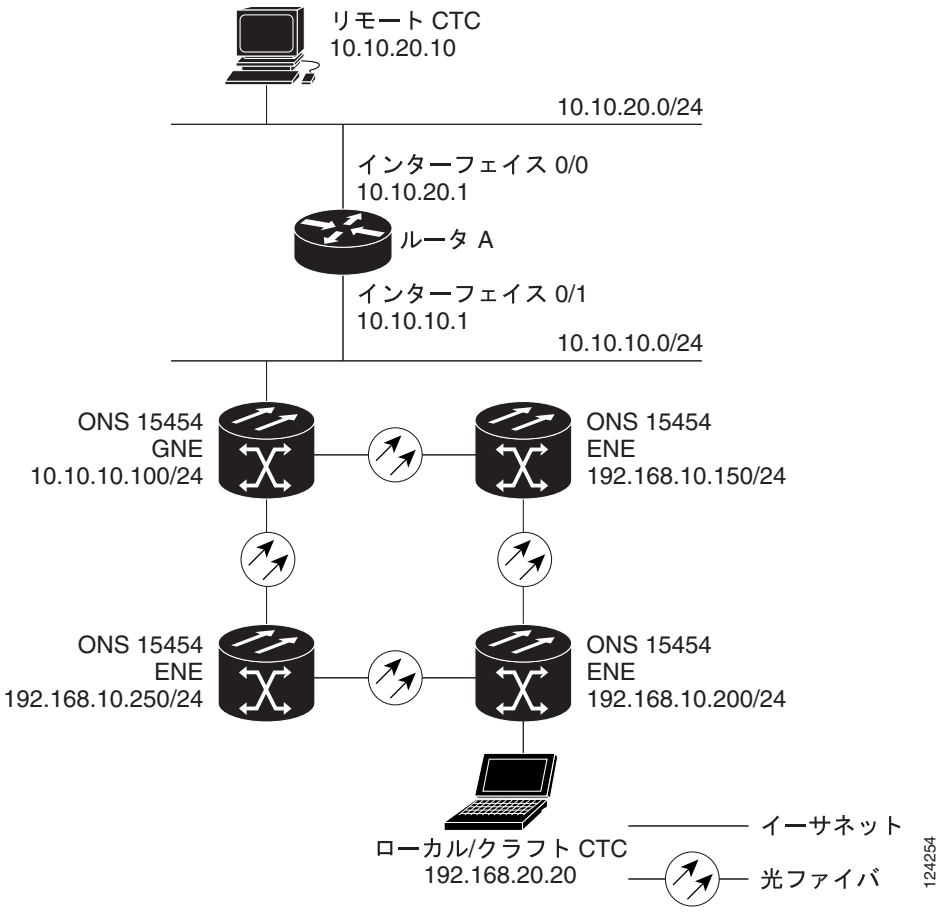


図 8-12 に、ONS 15454 ENE が複数のリングにある場合の同一プロキシ サーバの実装を示します。

図 8-12　シナリオ 7：ENE が複数のリングにある ONS 15454 プロキシ サーバ（ANSI および ETSI）

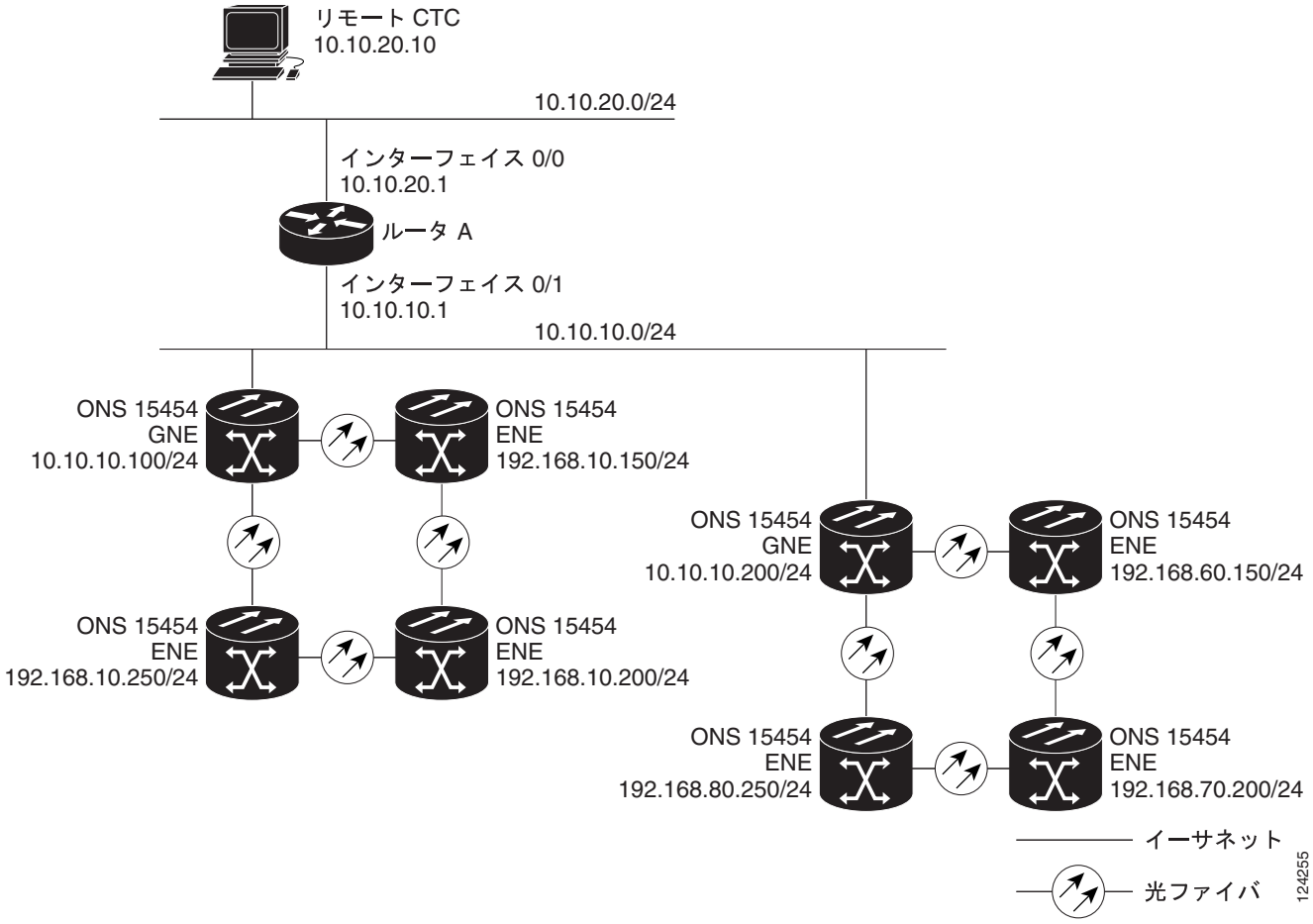


表 8-3 に、ノードが ENE および GNE として設定される場合にファイアウォールのパケットをフィルタリングするために ONS 15454 が従う規則を示します。パケットの宛先が ONS 15454 の場合は、表 8-4 に示す追加の規則が適用されます。拒否されたパケットは報告せずに、そのまま廃棄されます。

表 8-3　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宛先 IP 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 自身の IP アドレス • ONS 15454 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 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

表 8-4　パケットの宛先が ONS 15454 の場合のプロキシ サーバのファイアウォール フィルタリング処理規則

パケットの着信先	拒否する条件
TCC2/TCC2P イーサネット インターフェイス	• 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	• プロキシ サーバ ポート（1080）宛ての TCP パケット

プロキシ サーバを実装する場合、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 で、ゲートウェイ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。

ノードが到達不可能になった場合は、次のいずれかを実行して設定を正しく修正します。

- 到達不可能となった ONS 15454 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 に DCC 接続されている別のネットワーク ONS 15454 を介して問題の ONS 15454 に接続します。
- 近接ノードの DCC をすべてディセーブルにすることで、ノードへの接続を解除します。CTC コンピュータを ONS 15454 に直接接続して、その設定を変更します。

8.2.8　シナリオ 8：サブネット上のデュアル GNE

ONS 15454 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 から ENE へ接続することができます。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、ネトワークが GNE 損失から迅速に回復することができます。1 つの GNE が停止すると、その GNE を介した接続はすべて停止します。CTC は障害のある GNE およびその GNE がプロキシ機能を担っていたすべての ENE からの接続を解除し、そのあとで、残っている GNE を介して再接続します。GNE ロード バランシングは、ともに CTC のパフォーマンスを強化する、起動 GNE と DCC 帯域幅への依存を低減します。

（注）　デュアル GNE は特別なプロビジョニングを必要としません。

図 8-13 に、同一サブネットにデュアル GNE を設定したネットワークを示します。

図 8-13　シナリオ 8：同一サブネットにおけるデュアル GNE（ANSI および ETSI）

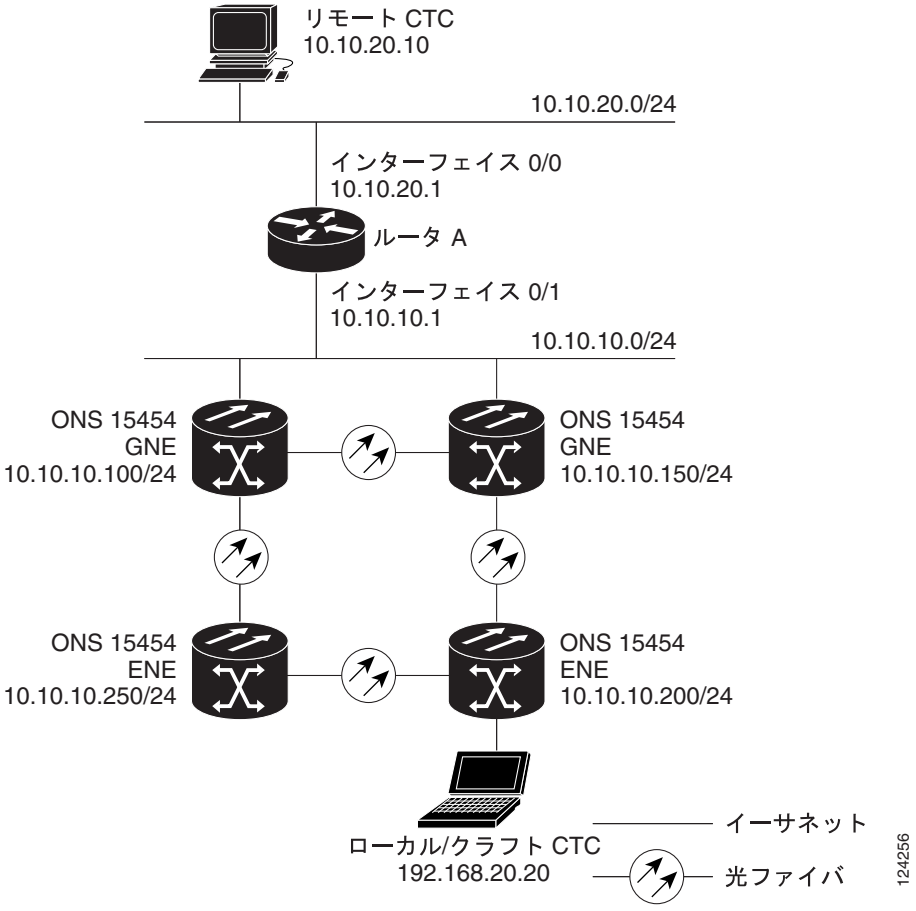
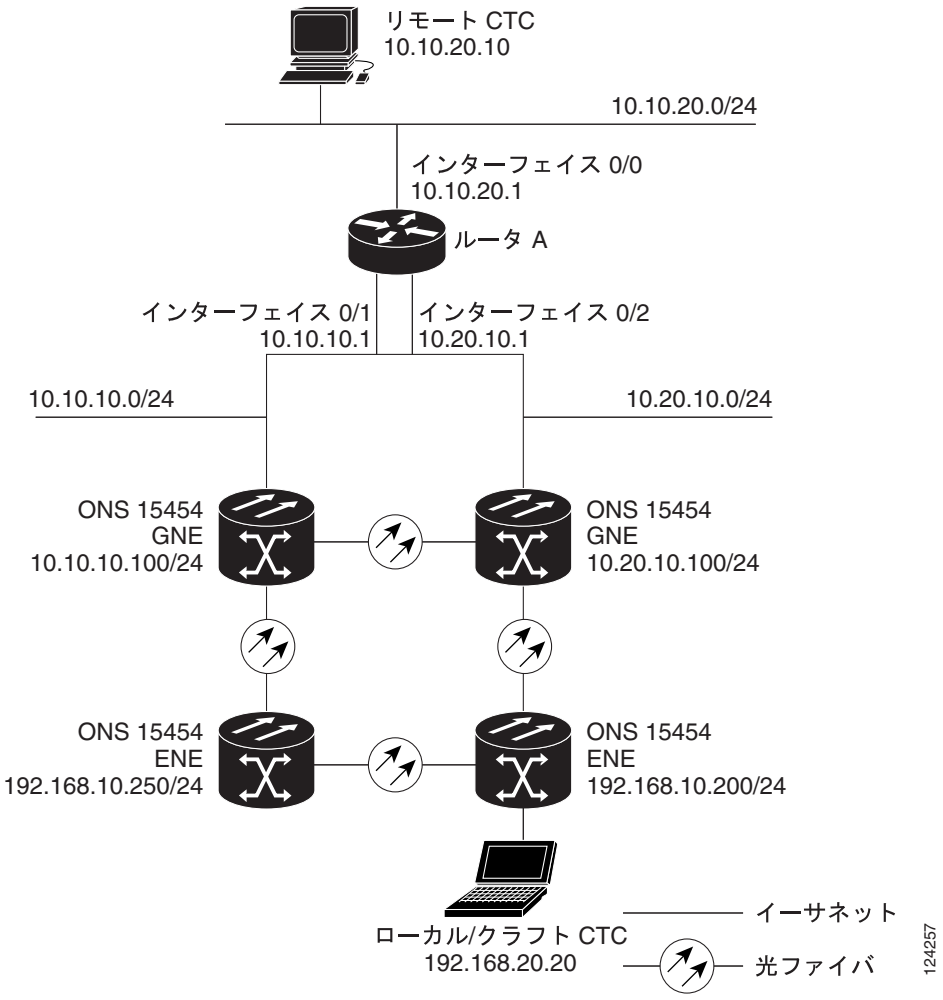


図 8-14 に、異なるサブネット上にデュアル GNE を設定したネットワークを示します。

図 8-14　シナリオ 8：異なるサブネットにおけるデュアル GNE（ANSI および ETSI）



8.2.9　シナリオ 9：セキュア モードをイネーブルにした IP アドレッシング

TCC2 カードおよび TCC2P カードは、いずれもデフォルトでノンセキュア モードになっています。このモードでは、前面と背面のイーサネット（LAN）ポートは、単一の MAC アドレスと IP アドレスを共有しています。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。これにより、前面からアクセスするクラフト ポートのユーザがバックプレーン ポートを介して LAN にアクセスするのを防ぐことができます。セキュア モードはロックすることができ、モードを変更しないようにできます。ノードをセキュア モードに設定することや、セキュア ノードをロックすることについては、『*Cisco ONS 15454 DWDM Procedure Guide*』の「Manage the Node」の章を参照してください。

8.2.9.1　セキュア モード動作

TCC2P ノードをノンセキュア モードからセキュア モードに変更することで、ONS 15454 の 2 つのイーサネット アドレスをプロビジョニングすることができ、ノードでポートに個別の MAC アドレスを割り当てることができます。セキュア モードでは、1 つの IP アドレスが ONS 15454 バックプレーン LAN（イーサネット）ポートにプロビジョニングされ、他の IP アドレスは、TCC2P イーサネット ポートにプロビジョニングされます。両方のアドレスは別のサブネットにあり、クラフト アクセス ポートと ONS 15454 LAN 間の分離レイヤが 1 つ増えます。セキュア モードがイネーブルの場合、両方の TCC2P イーサネット ポートにプロビジョニングされている IP アドレスは、一般的な IP アドレッシング ガイドラインに従う必要があり、互いに異なるサブネットとデフォルト ルータ IP アドレスに存在する必要があります。

セキュア モードでは、前面の LAN（イーサネット）ポートに割り当てられた IP アドレスがプライベート アドレスになり、バックプレーンがノードをセントラル オフィス LAN または企業のプライベート ネットワーク経由で Operation Support System（OSS）に接続します。スーパーユーザは、CTC、ルーティング テーブル、または自律メッセージ レポートのバックプレーン LAN IP アドレスを表示したり隠したりするようにノードを設定できます。

ノンセキュア モードでは、ノードは GNE または ENE です。ノードをセキュア モードにすると、自動的に SOCKS プロキシがオンになり、ノードはデフォルトで GNE 状態になります。ただし、ノードを ENE に戻すこともできます。ノンセキュア モードでは、LAN ファイアウォールの先にあるノードを効率的に分離するために、ENE の SOCKS プロキシをディセーブルにすることができますが、セキュア モードではディセーブルにできません。ノードの GNE または ENE 状態を変更して SOCKS プロキシをディセーブルにするには、『*Cisco ONS 15454 DWDM Procedure Guide*』の「Turn Up a Node」の章を参照してください。

注意　セキュア モードをイネーブルにすると、TCC2P カードが再起動します。TCC2P カードを再起動するとトラフィックに影響します。

（注）　TCC2 カードがインストールされている場合、セキュア モード オプションは CTC には表示されません。1 つの TCC2 と 1 つの TCC2P カードがノードに装着されている場合、セキュア モードが CTC に表示されますが、変更できません。

（注）　前面およびバックプレーン アクセス ポートが ENE でディセーブルになっていて、（ユーザのプロビジョニングまたはネットワーク障害により）ノードが DCC 通信から隔離されている場合、前面およびバックプレーン ポートは自動的に再度イネーブルになります。

図 8-15 に、同じサブネットにある前面アクセス イーサネット ポート アドレスのセキュア モード ONS 15454 ノードの例を示します。

図 8-15　シナリオ 9：同一サブネット上の ONS 15454 GNE および ENE（セキュア モードがイネーブルの場合）

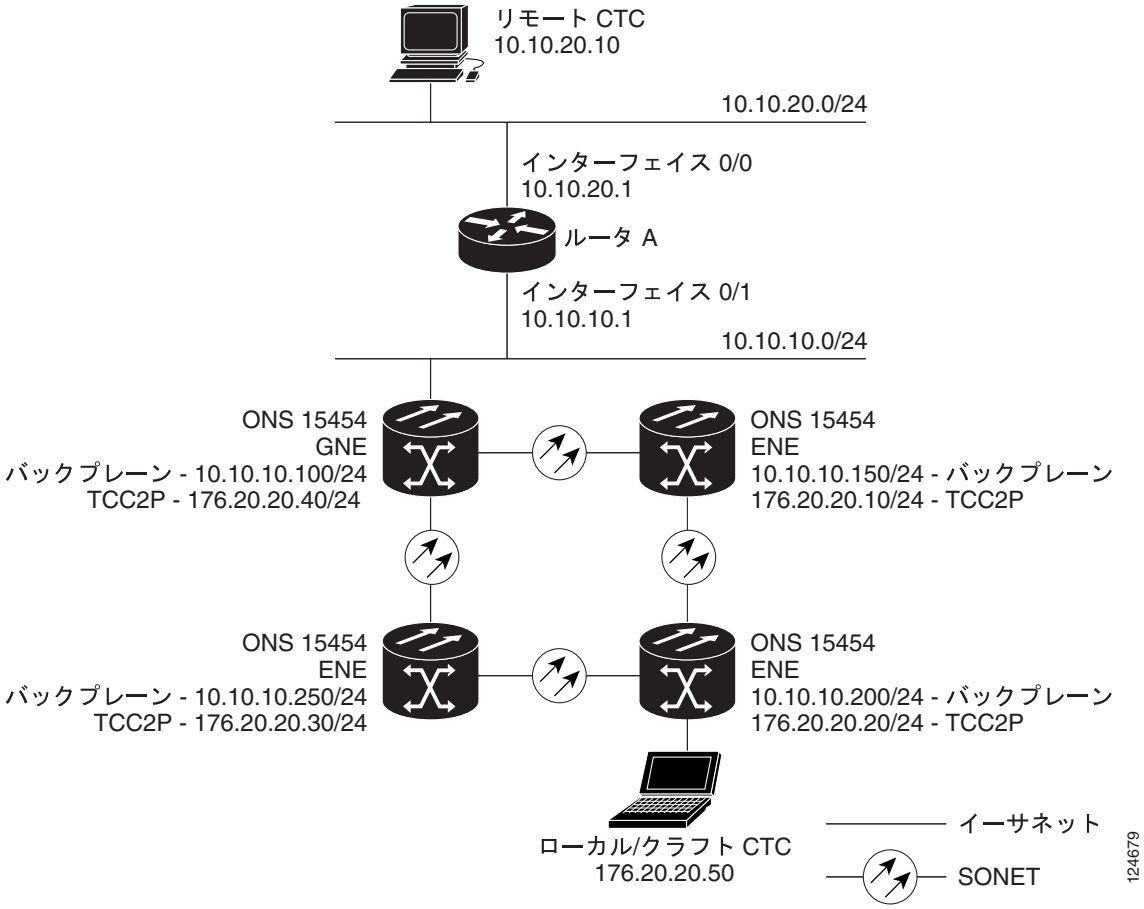
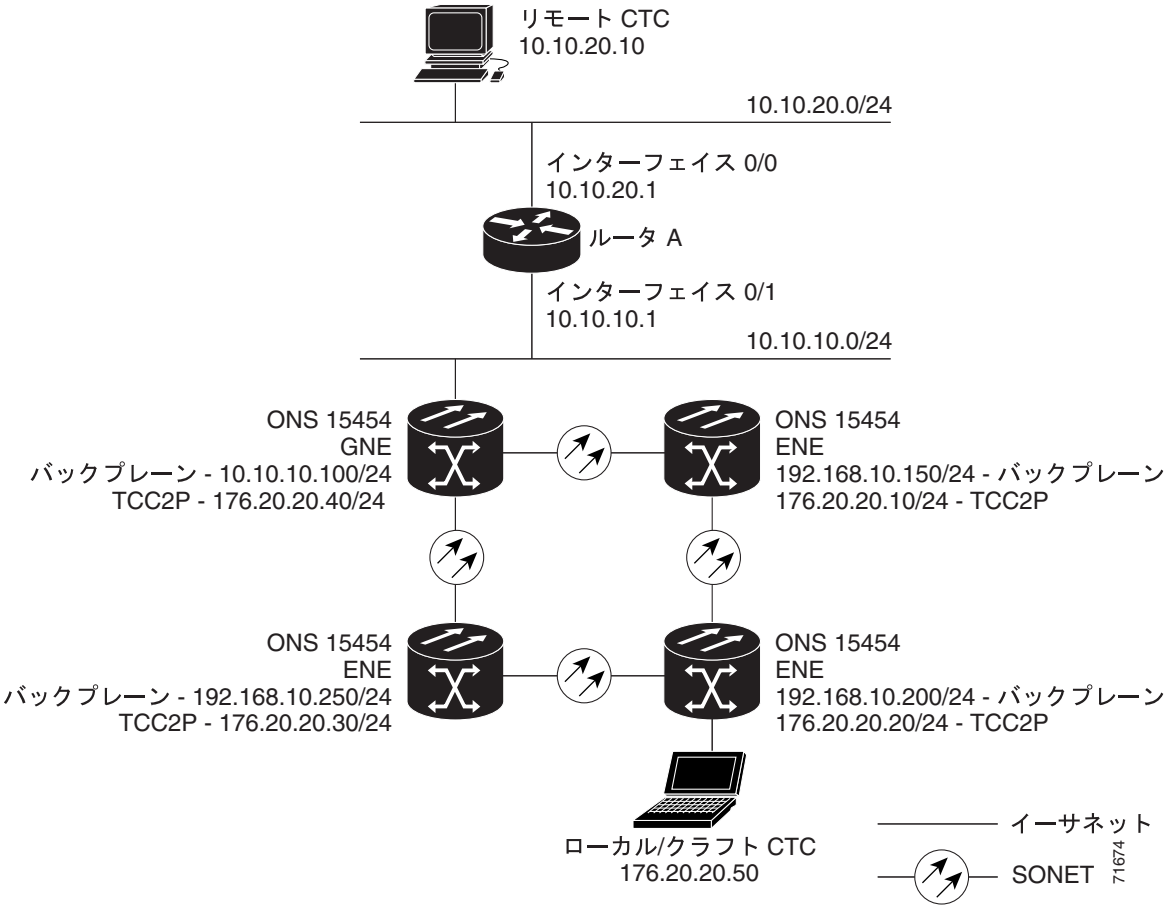


図 8-16 に、セキュア モードをイネーブルにしてルータに接続された ONS 15454 の例を示します。各例では、ノードの TCC2P ポート アドレス（ノード アドレス）がノード バックプレーン アドレスとは別のサブネットにあります。

図 8-16　シナリオ 9 : 異なるサブネット上の ONS 15454 GNE および ENE（セキュア モードがイネーブルの場合）



8.2.9.2　セキュア ノードのロックおよびロック解除動作

セキュア モードは、ロックされたノードまたはロック解除されたノードで動作します。デフォルトのステータスはロック解除で、スーパーユーザのみがロックに設定できます。セキュア モードを永久にロックに設定すると、シャーシと同様に、アクティブおよびスタンバイ TCC2P カードのハードウェア構成が変更されます。

カードとシェルフが分離されている場合でも、ロックステータスは保持されるので、ロック モードは注意して使用する必要があります。たとえば、ノードがセキュア ロック モードのとき、カードをスタンバイ TCC2P から取り外し、このカードをアクティブなカードとして別のノードに挿入すると、セキュア ロック モードが新しいノードのシャーシおよびスタンバイ TCC2P に書き込まれます。セキュアでロックされたノードのアクティブおよびスタンバイ TCC2P からカードを取り外し、以前はロック解除モードだったシャーシに両方のカードを挿入すると、このノードはロックされます。

ノードがセキュアでロックされている場合、ノードの設定、イーサネット ポート ステータス、そのセキュア 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 ユーザからも変更できません。セキュア ノードのロックを解除するには、Cisco Technical Support に連絡してシャーシおよび TCC2P 用の Return Material Authorization（RMA; 返品許可）を手配してください。必要に応じて、「テクニカル サポート」（p.xxvi）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だけ（シェルフなど）がロック解除されると、システムはロック モードに戻ります。

8.3　プロビジョニング可能なパッチコード

プロビジョニング可能なパッチコードは、ネットワークを介して OSPF によりアドバタイズされるユーザがプロビジョニングしたリンクです。プロビジョニング可能なパッチコード（仮想リンク）は次のような状況で必要になります。

- 光ポートが透過モードで設定されたトランスポンダまたはマックスポンダ クライアント ポートに接続されている。
- 光 ITU ポートが DWDM 光チャネル カードに接続されている。
- 2 つのトランスポンダまたはマックスポンダ トランク ポートが DWDM 光チャネル カードに接続されている。また、Generic Control Channel（GCC）がリングを介して透過的に伝送されている。
- トランスポンダまたはマックスポンダ クライアントおよびトランク ポートが再生器グループにある。カードが透過モードにある。および DCC/GCC 終端が利用できない。

プロビジョニング可能なパッチコードは物理リンクの両端で必要になります。各端でのプロビジョニングには、ローカル パッチコード ID、スロット / ポート情報、リモート IP アドレス、およびリモート パッチコード ID が含まれます。パッチコードは CTC ネットワーク ビューに点線として表示されます。

光パッチコードは、OCH フィルタと OCH トランク ポートとの間でプロビジョニングされる必要があります。手動でプロビジョニングされたパッチコードは、トランスポンダ（TXP）または マックスポンダ（MXP）が最初に調整可能な波長で自動プロビジョンに設定される場合、OCH フィルタとして自動的に TXP または MXP トランクを調整します。自動的に内部および外部（仮想リンク）パッチコードを CTC 内で自動的に調整できます。TL1 では、内部パッチコードのみをプロビジョニングできます。

表 8-5 に、プロビジョニング可能なパッチコードでサポートされる、クライアントおよびトランク ポートのカードの組み合わせを示します。

表 8-5　プロビジョニング可能なパッチコード用の Cisco ONS 15454 クライアント / トランク カードの組み合わせ

	クライアント カード						
トランク カード	MXP_2.5G_10G/ TXP_MR_10G	TXP_MR_2.5G/ TXPP_MR_2.5G	MXP_2.5G_10E/ TXP_MR_10E	32MUX-O 32DMX-O	32WSS/ 32DMX	AD-xC-xx.x	4MD-xx.x
MXP_2.5G_10G/ TXP_MR_10G	—	—	—	可	可	可	可
TXP_MR_2.5G/ TXPP_MR_2.5G	—	—	—	可	可	可	可
MXP_2.5G_10E/ TXP_MR_10E	—	—	—	可	可	可	可
MXP_MR_2.5G/ MXPP_MR_2.5G	—	—	—	可	可	可	可
OC-192	可	—	可	—	—	—	—
OC-48	可	可	可	—	—	—	—
OC-192 ITU	—	—	—	可	可	可	可
OC-48 ITU	—	—	—	可	可	可	可

表 8-6 に、パッチコードのクライアント ツー クライアント ポートでサポートされる、カードの組み合わせを示します。

表 8-6　プロビジョニング可能なパッチコード用の Cisco ONS 15454 クライアント / クライアント カードの組み合わせ

クライアント カード	MXP_2.5G_10G/ TXP_MR_10G	TXP_MR_2.5G/ TXPP_MR_2.5G	MXP_2.5G_10E/ TXP_MR_10E
MXP_2.5G_10G/TXP_MR_10G	可	—	可
TXP_MR_2.5G/TXPP_MR_2.5G	—	可	—
MXP_2.5G_10E/TXP_MR_10E	可	—	可

表 8-7 は、パッチコードのトランク ツー トランク ポートでサポートされる、カードの組み合わせを示します。

表 8-7　プロビジョニング可能なパッチコード用の Cisco ONS 15454 トランク / トランク カードの組み合わせ

トランク カード	MXP_2.5G_10G/ TXP_MR_10G	TXP_MR_2.5G/ TXPP_MR_2.5G	MXP_2.5G_10E/ TXP_MR_10E
MXP_2.5G_10G/TXP_MR_10G	可	—	可
TXP_MR_2.5G/TXPP_MR_2.5G	—	可	—
MXP_2.5G_10E/TXP_MR_10E	可	—	可

光ポートをプロビジョニング可能なパッチコードで使用する場合は次のような要件があります。

- トランスポンダ / マックスポンダ ポート、アド / ドロップ マルチプレクサ ポート、またはマルチプレクサ / デマルチプレクサ ポートに接続された光ポートには、セクション DCC/ ライン DCC（SDCC/LDCC または RS-DCC/MS-DCC）終端が必要です。
- 光ポートが 1+1 グループの保護ポートである場合、現用ポートには SDCC/LDCC または RS-DCC/MS-DCC 終端がプロビジョニングされている必要があります。
- パッチコードのリモート終端が Y 字ケーブル保護、アド / ドロップ マルチプレクサ ポート、マルチプレクサ / デマルチプレクサ ポートのいずれかである場合は、光ポートには 2 つのパッチコードが必要です。

トランスポンダおよびマックスポンダをプロビジョニング可能なパッチコードで使用する場合は次のような要件があります。

- トランスポンダ / マックスポンダ ポートをアド / ドロップ マルチプレクサまたはマルチプレクサ / デマルチプレクサ ポートに接続する場合は、2 つのパッチコードが必要となります。自動的に CTC は 2 つめのパッチコードを設定するようにユーザに求めます。
- パッチコードが再生器グループのクライアント ポート上にある場合、パッチコードの他端が同一ノード上および同一再生器グループ内のポート上にあります。
- パッチコードは、カードが透過モードにある場合にのみ、クライアント ポート上に許可されます。

DWDM カードは、光チャネル ポート上でのみ、プロビジョニング可能なパッチコードをサポートします。各 DWDM 光チャネル ポートには、プロビジョニング可能なパッチコードを 1 つのみ設定できます。

8.4　ルーティング テーブル

ONS 15454 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 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 イーサネット インターフェイス、すなわち、TCC2/TCC2P の RJ-45 ジャック、バックプレーン上の LAN 1 ピン（ANSI シェルフの場合）、MIC-C/T/P 上の LAN 接続（ETSI シェルフの場合）
  - pdcc0 — SDCC または RS-DCC インターフェイス、つまり SDCC または RS-DCC 終端として認識された OC-N トランク カード
  - lo0 — ループバック インターフェイス

表 8-8 に、ONS 15454 のルーティング エントリ例を示します。

表 8-8　ルーティング テーブルのエントリ例

エントリ	宛先	マスク	ゲートウェイ	使用回数	インターフェイス
1	0.0.0.0	0.0.0.0	172.20.214.1	265103	motfcc0
2	172.20.214.0	255.255.255.0	172.20.214.92	0	motfcc0
3	172.20.214.92	255.255.255.255	127.0.0.1	54	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	16853	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	16853	pdcc0

エントリ 1 の内容は次のとおりです。

- 宛先（0.0.0.0）は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 エントリにマッピングされます。
- マスク（0.0.0.0）は常にデフォルト ルートを示す 0 です。
- ゲートウェイ（172.20.214.1）はデフォルトのゲートウェイ アドレスです。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）は、ゲートウェイに到達するために ONS 15454 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）は、宛先ネットワーク IP アドレスです。
- マスク（255.255.255.0）は 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）はゲートウェイ 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）は、ゲートウェイに到達するために ONS 15454 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）は、宛先ホスト IP アドレスです。
- マスク（255.255.255.255）は 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）はループバック 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）は、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）は、宛先ホスト IP アドレスです。
- マスク（255.255.255.255）は 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）は、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）は、宛先ホストに到達するために 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）は、宛先ホスト IP アドレスです。
- マスク（255.255.255.255）は 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）は、IP アドレスが 172.20.214.93 であるホスト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）は、ゲートウェイに到達するために DCC インターフェイスを使用することを示します。

8.5　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 8-9 は、TCC2/TCC2P で使用するポートの一覧です。

表 8-9　TCC2/TCC2P で使用するポート

ポート	説明	アクション[1]
0	未使用	D
20	FTP（ファイル転送プロトコル）	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	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 = 拒否、NA = 適用されない、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イネーブル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、CTC ワークステーションのアドレスは 192.168.10.10、ONS 15454 アドレスは 10.10.10.100 です。ファイアウォールは GNE 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 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 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with ONS 15454 using http (port 80)
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with ONS 15454 GNE (port 57790)
***
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 back from CTC to ONS 15454 GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from the 15454 (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 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イネーブル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 アドレスは 10.10.10.100 です。ファイアウォールは GNE 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 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15454 using http (port 80)
***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15454 GNE (port 1080) ***
access-list 100 remark

access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 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 GNE to CTC ***
```

8.6　オープン GNE

ONS 15454 は、ノードおよびリンクの自動検出に必要な、PPP（ポイント ツー ポイント プロトコル）ベンダー拡張または OSPF タイプ 10 オパーク Link State Advertisement（LSA; リンクステート アドバタイズ）をサポートしない非 ONS ノードと通信できます。オープン GNE を設定することにより、GCC ベースのネットワークを非 ONS ノードの IP ネットワークとして機能させることができます。

オープン GNE ネットワークを設定するには、GCC 終端をプロビジョニングして、遠端の非 ONS ノードを含めることができます。この場合、0.0.0.0 のデフォルト IP アドレスまたは指定 IP アドレスのどちらかを使用します。GCC 作成時に [Far End is Foreign] チェックボックスをオンにして遠端の非 ONS ノードを設定します。0.0.0.0 のデフォルト IP アドレスを使用する場合、遠端の非 ONS ノードは任意の IP アドレスで自身を識別します。0.0.0.0 以外の IP アドレスを指定する場合は、セキュリティ レベルを追加することで、遠端ノードが指定 IP アドレスで自身を識別する場合にだけリンクが確立します。

デフォルトでは、プロキシ サーバは検出された ONS ピアにだけ接続を許可し、ファイアウォールが GCC 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 トンネルをプロビジョニングして、非 ONS ノードに対して 12 までの SOCKS バージョン 5 接続の宛先を追加できます。また、ファイアウォール トンネルをプロビジョニングして、GCC ネットワークと LAN の間を直接 IP 接続するための宛先を 12 まで追加できます。プロキシ トンネルおよびファイアウォール トンネルには、送信元と宛先の両方のサブネットが含まれます。この接続は送信元のサブネットから発生し、宛先のサブネットで終了します。そのあとで SOCKS 接続または IP パケット フローが許可されます。CTC クライアントが送信元サブネットにあり、要求した宛先が宛先サブネットにある場合、プロキシ接続が許可されます。ファイアウォール トンネルにより、ノード イーサネットと pdcc インターフェイスの間で IP トラフィックをルーティングできます。着信イーサネット パケットは、送信元アドレスがトンネル送信元に一致し、宛先がトンネル宛先に一致する場合に、ファイアウォールを介して許可されます。着信 pdcc パケットは、送信元アドレスがトンネル宛先に一致し、宛先アドレスがトンネル送信元に一致する場合に、ファイアウォールを介して許可されます。トンネルは TCP および UDP パケットだけに影響します。

プロキシ トンネルまたはファイアウォール トンネル（またはその両方）のアベイラビリティは、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。

- ノードに GNE または ENE モードでイネーブルになったプロキシ サーバが組み込まれている場合は、プロキシ トンネルまたはファイアウォール トンネル（またはその両方）を設定する必要があります。
- ノードに proxy-only モードでイネーブルになったプロキシ サーバが組み込まれている場合は、プロキシ トンネルを設定できます。ファイアウォール トンネルは許可されません。
- ノードに組み込まれているプロキシ サーバがディセーブルの場合は、プロキシ トンネルもファイアウォール トンネルも許可されません。

図 8-17 に、GCC 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 トンネルおよびファイアウォール トンネルが有効に機能しています。これらのトンネルがないと、GNE により PC と外部ノードの間の IP アクセスがブロックされます。

図 8-17　外部終端のプロキシ トンネルおよびファイアウォール トンネル

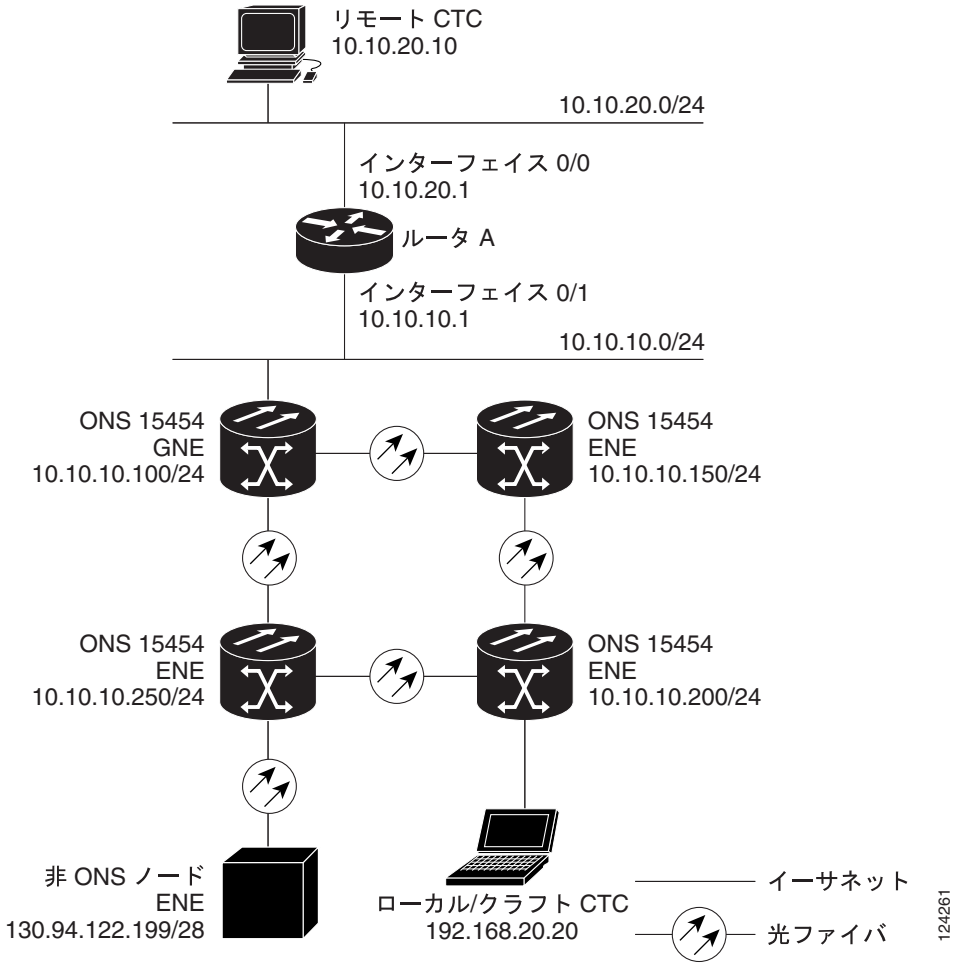
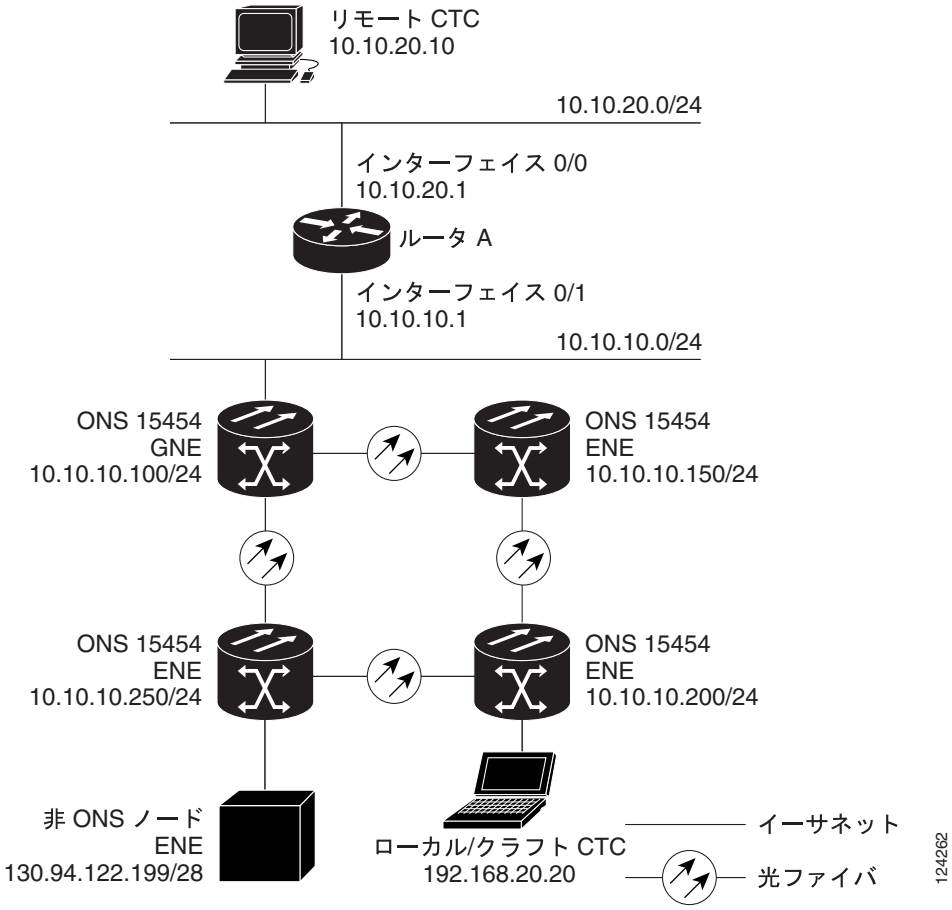


図 8-18 に、ENE イーサネット ポートに接続されたリモート ノードを示します。この例では、プロキシ トンネルおよびファイアウォール トンネルが有効に機能しています。これらのトンネルがないと、GNE により PC と外部ノードの間の IP アクセスがブロックされます。この構成には ENE のファイアウォール トンネルも必要です。

図 8-18　ENE イーサネット ポートへの外部ノード接続



8.7　TCP/IP および OSI ネットワーキング

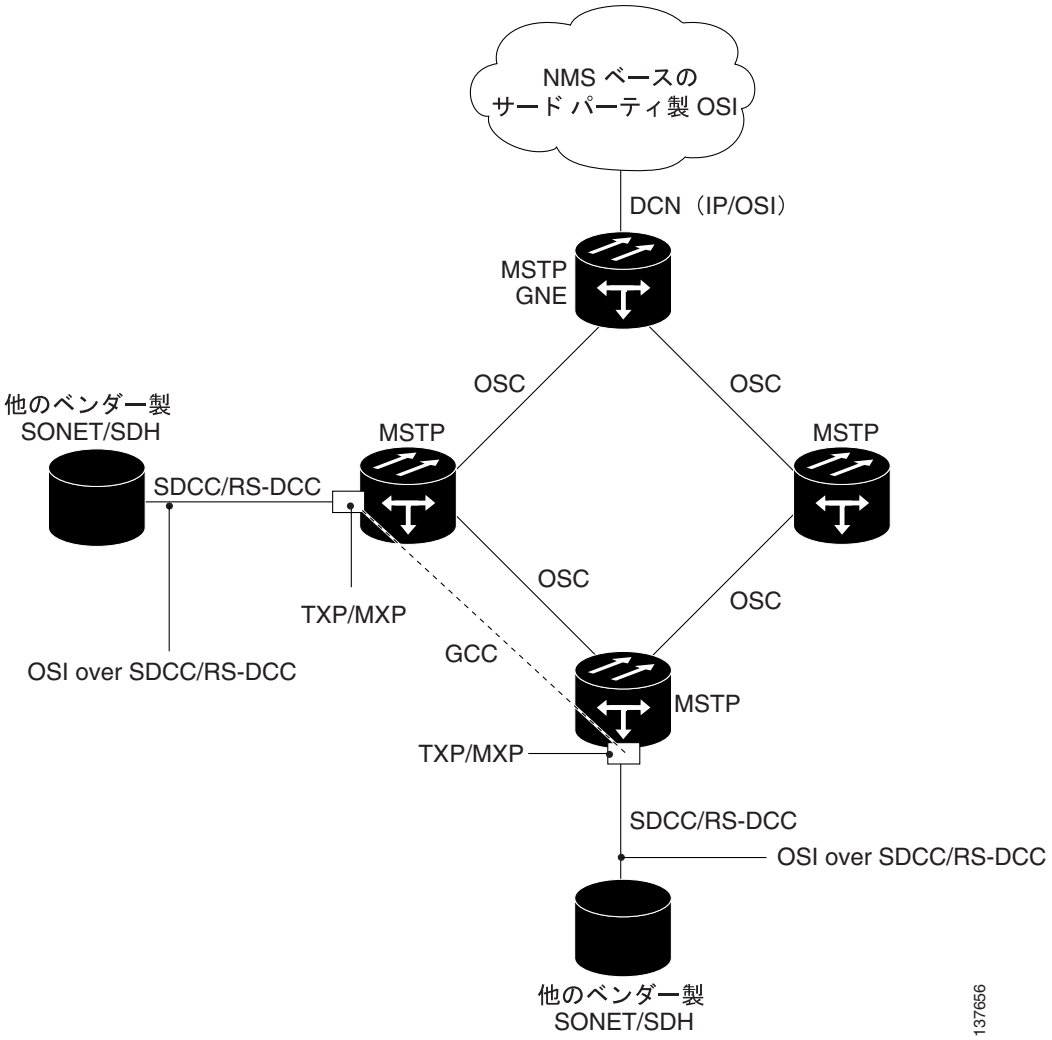
ONS 15454 DCN 通信は TCP/IP プロトコルに基づいています。ただし、ONS 15454 は OSI プロトコルを使用する機器にネットワーク接続することもできます。TCP/IP プロトコルと OSI プロトコルは直接互換性はありませんが、OSI 参照モデルの同じオブジェクトを持ち、類似するレイヤを使用しています。OSI プロトコル、処理、およびシナリオに関する詳細は、『*ONS 15454 Reference Manual*』の「Management Network Connectivity」の章を参照してください。OSI/MSTP シナリオは次のセクションで説明します。

OSI/MSTP シナリオ 1（図 8-19）では、SDCC または RS-DCC が、OSI ベースのサード パーティ製 NE から ONS NE 上の TXP/MXP カードへの OC-N 信号を伝送します。信号は GCC によって他の MSTP NE の TXP/MXP カードに伝送され、そのあと SDCC または RS-DCC によって次のサードパーティ製 NE に運ばれます。このシナリオでは、クライアント インターフェイスをセクション終端モードまたは回線終端モードでプロビジョングできる TXP/MXP が必要です。TXP/MXP には次のものがあります。

- TXP_MR_2.5 および TXPP_MR_2.5（OCn-N SFP が取り付けられている場合）
- TXP_MR_10G および TXP_MR_10E（クライアントが OC192 として設定されている場合）
- MXP_2.5_10G および MXP_2.5_10E

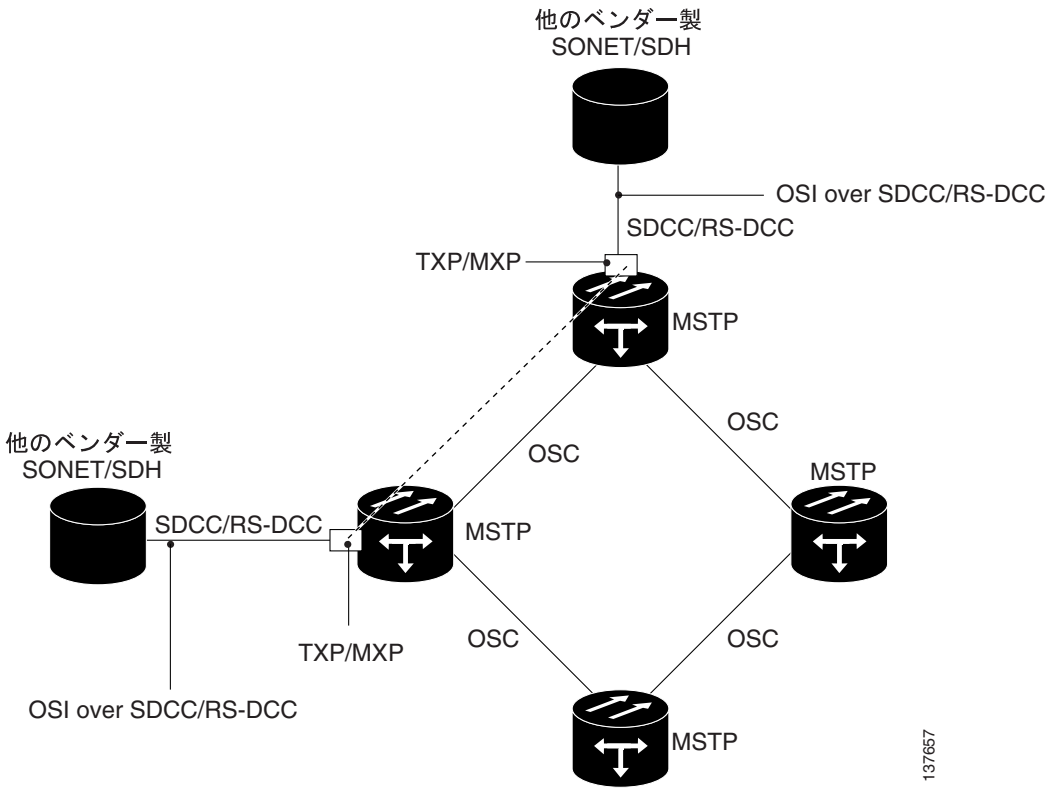
OSI は、OSC 終端、GCC 終端、またはその両方を使用して他の TXP/MXP に伝送される（またはトンネルされる）必要があります。サード パーティ製の NMS は、サード パーティ ベンダー OSI ベースの SONET 機器の GNE として機能する MSTP ONS NE を使用して、自身の NE に OSI 接続します。

図 8-19　OSI/MSTP シナリオ 1



OSI/MSTP シナリオ 2（図 8-20）は、シナリオ 1 に類似していますが、MSTP NE が OSI NMS へ接続していない点が異なります。

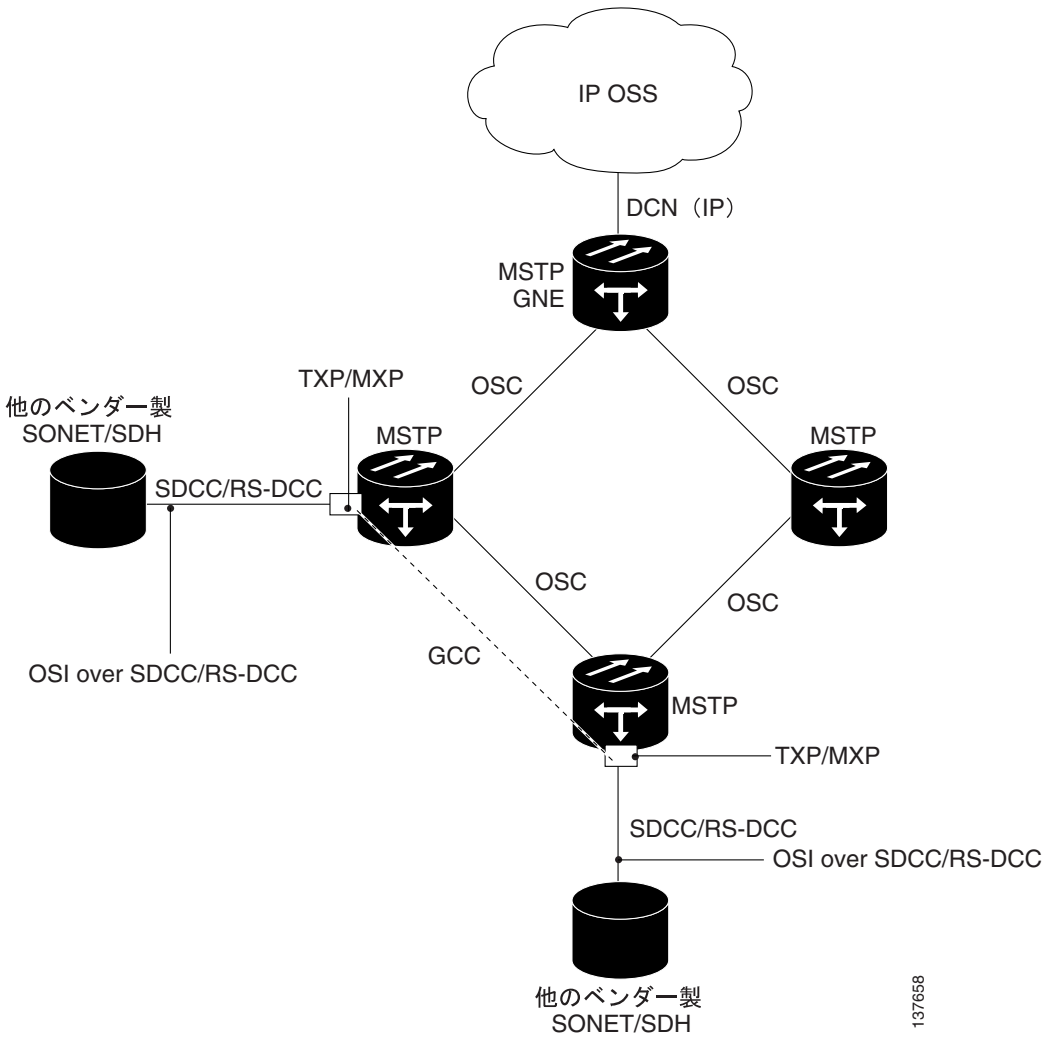
図 8-20　OSI/MSTP シナリオ 2



OSI/MSTP シナリオ 3（図 8-21）では、次の内容が示されています。

- OSI は SDCC または RS-DCC 終端上で伝送される。
- OSI は、OSC 終端、GCC 終端、またはその両方を使用して他のピア TXP/MXP に伝送される（またはトンネルされる）必要がある。
- OSS はすべての NE と IP 接続できる。
- MSTP NE は、サードパーティ製の OSI ベースの SONET NE の GNE である。MSTP NE はすべてのメディエーション機能を実行する。

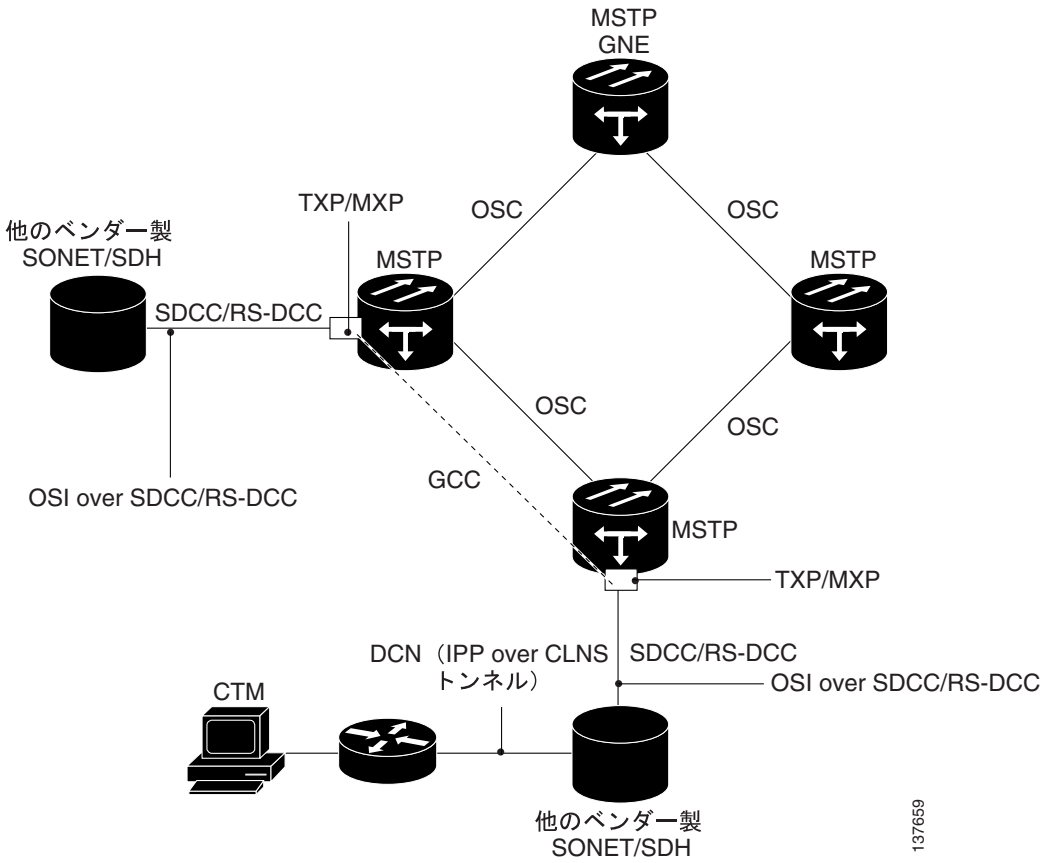
図 8-21　OSI/MSTP シナリオ 3



OSI/MSTP シナリオ 4（図 8-22）では、次の内容が示されています。

- OSI は SDCC または RS-DCC 終端上で伝送される。
- OSI は、OSC 終端、GCC 終端、またはその両方を使用して他のピア TXP/MXP に伝送される（またはトンネルされる）必要がある。
- OSS は、サード パーティ製 NE ネットワークを使用してすべての NE と IP 接続できる。
- MSTP NE は、サード パーティ製の OSI ベースの SONET NE の GNE である。MSTP NE はすべてのメディエーション機能を実行する。
- サード パーティ ベンダー製の NE は、Cisco MSTP ネットワークの GNE になる。

図 8-22　OSI/IP シナリオ 4



8.8 LMP

ここでは、Link Management Protocol（LMP; リンク管理プロトコル）の管理と設定について説明します。特定アラームのトラブルシューティングについては、『*Cisco ONS 15454 DWDM Troubleshooting Guide*』を参照してください。LMP の設定については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。

（注）　LMP では、Cisco Transport Manager（CTM）のサポートは必要ありません。

LMP は、Cisco ONS 15454 のノード間、または Cisco ONS 15454 のノードとベンダー固有のハードウェアを使用する他社製の選択されたノードの間で、Traffic Engineering（TE; トラフィック処理）リンクを確立するために使用します。

8.8.1 概要

LMP は、制御チャネルを使用してノード間の TE リンクを管理します。TE リンクは、ネットワークおよびインターネット上のトラフィック フローで可能な最も効率的なパスを定義するように設計されています。トラフィック処理には、トラフィック管理、容量管理、トラフィック測定とモデル化、ネットワークのモデル化、およびパフォーマンス分析が含まれます。トラフィック処理の方法には、呼ルーティング、接続ルーティング、Quality of Service（QoS; サービス品質）リソース管理、ルーティング テーブル管理、および容量管理などがあります。

LMP は、2 つの Optical Cross-connect（OXC; 光クロスコネクト）ノードのようなピア ノード間の TE リンクを管理します。ピア ノードには、同等のシグナリングおよびルーティングがあります。LMP は、OXP などのノードと隣接する Optical Line System（OLS; 光回線システム）ノードの間の TE リンクも管理します。OLS ノードの例として、ONS 15454 DWDM ノードがあります。

ルータ、スイッチ、OXC ノード、DWDM OLS ノード、および Add/Drop Multiplexer（ADM; アド/ドロップ マルチプレクサ）のあるネットワークでは、Generalized Multiprotocol Label Switching（GMPLS）などの共通のコントロール プレーンを使用して、リソースをプロビジョニングし、保護および復元技術を使用するネットワークの存続可能性を提供します。LMP は、GMPLS プロトコル スイートの一部です。

1 つの TE リンクは、いくつかの個々のリンクから形成できます。TE リンクの管理は、帯域外方式のほかに、帯域内メッセージングによって遂行できます。次の資料で、TE リンクを管理する 1 組のノード間の LMP について説明します。LMP は次のタスクを実行します。

- 制御チャネル接続を維持する
- データ リンクの物理的接続を検証する
- リンクのプロパティ情報を相関させる
- ダウンストリームのアラームを抑制する
- 複数のタイプのネットワークで、保護および復旧の目的でリンク障害をローカライズする

DWDM ネットワークでは、頻繁に MPLS と GMPLS を共通のコントロール プレーンとして使用して、パケットをネットワークでどのようにルーティングするかを制御します。

LMP は、ルーティング、シグナリング、およびリンク管理のためにノード間に存在しなければならない制御チャネルを管理します。制御チャネルが存在するためには、各ノードに、もう一方のノードから到達できる IP インターフェイスが付いている必要があります。これらの IP インターフェイスがまとまって制御チャネルを形成します。コントロール メッセージ用のインターフェイスは、データ用と同じインターフェースである必要はありません。

LMP プロトコルは、インターネット ドラフト『*draft-ietf-ccamp-lmp-10.txt*』で、Internet Engineering Task Force（IETF）により規定されています。このドラフトは、2005 年 10 月 28 日に Proposed Standard、RFC 4204（http://www.ietf.org/rfc/rfc4204.txt）として発行されました。

8.8.1.1 MPLS

MPLS は、ルーティング テーブルおよびルーティング プロトコルから独立しているエンジニアリング ネットワークのトラフィック パターンのメカニズムを提供します。MPLS は、パケットをネットワークにどのように転送するかを示すショート ラベルをネットワーク パケットに割り当てます。従来のレイヤ 3 転送メカニズムでは、各ホップでパケット ヘッダーを分析し、ルーティング テーブルのルックアップに基づいて次のホップを決定する必要があります。MLPS では、パケット ヘッダーの分析は、パケットが MPLS クラウドに入ったときに 1 回だけ行われます。その後、パケットは、ラベルに指定されている Label Switch Path（LSP; ラベル スイッチ パス）として知られるストリームに割り当てられます。この短い固定の長さのラベルは、転送テーブルにおけるインデックスです。転送テーブルは、従来の各ホップでのルーティング テーブルのルックアップより効率的です。MPLS を使用して、制御プロトコル（LSP の管理に使用される）とユーザ データの両方を同じ伝送インターフェイスで伝送できます。

8.8.1.2 GMPLS

GMPLS は、MPLS がベースになっていて、Time Division Multiplexing（TDM; 時分割多重）スロット（SONET および SDH など）、レイヤ 1 の Wavelength Division Multiplexing（WDM; 波長分割多重）波長、およびファイバを含む、追加のテクノロジーをサポートするための拡張されたプロトコルを備えています。MPLS の場合、制御トラフィック（シグナリングおよびルーティング）は、伝送インターフェイスで実行できます。GMPLS では、MPLS の場合とは異なり、別の制御チャネルが使用されます。GMPLS 制御チャネルは、LMP によって管理されます。GMPLS では、2 つの隣接ノード間の制御チャネルは、これらのノード間のデータ リンクと同じ物理メディアを使用する必要はありません。

8.8.2 LMP の設定

LMP の設定は、次の 4 つの内容で構成されています。

- 制御チャネル管理
- TE リンク管理
- リンク接続の検証
- 障害管理

8.8.2.1 制御チャネル管理

制御チャネル管理では、隣接ノード間の制御チャネルを確立して維持します。制御チャネルでは、ノード間で Config メッセージ交換とファスト キープアライブ メカニズムを使用します。後者は、より低いレベルのメカニズムが制御チャネルの障害の検出に使用できない場合に必要となります。最大で 4 つの LMP 制御チャネルをサポートできます。

ノードは最初にコンフィギュレーション メッセージ（Config、ConfigAck、および ConfigNack）を交換し、これらのメッセージは、識別子を交換してキープアライブ プロトコルのためのパラメータを取り決めるために使用されます。次に、ノードは Hello メッセージの連続高速交換を行い、これらのメッセージは、チャネルのヘルスをモニタリングするために使用されます。

（注）　識別子は Local Node Id、Remote Node Id、Local Control Channel Id、および Remote Control Channel Id で、パラメータは HelloInterval および HelloDeadInterval です。

LMP アウトオブファイバおよび LMP アウトオブバンド制御チャネルは、シェルフでサポートされ、終端されます。イーサネットはデータ プレーンに使用されるファイバとは別であるため、アウトオブファイバ制御チャネルには、制御チャネルのためのコントロール プレーン ネットワーク（イーサネット）の使用が含まれています。オーバーヘッド バイトはペイロードとは別であるため、アウトオブバンド制御チャネルには、制御チャネルのためのオーバーヘッド バイト（SDCC および LDCC バイトなど）の使用が含まれています。「インバンド」は、コントロール メッセージがデータ メッセージと同じチャネル内にあることを意味しています。したがって、「アウトオブバンド」は、同じファイバ内のオーバーヘッド バイト、同じファイバ内のコントロール メッセージ専用の別の回路（SONET/SDH 回路）、または同じファイバ内の別の波長（DWDM）のことを指します。

（注）　オーバーヘッド バイトは、SONET ネットワークの SDCC または LDCC、SDH ネットワークの RS-DCC または MS-DCC、および DWDM ネットワークの GCC または OSC です。

「アウトオブバンド」は「インファイバ」を意味しており、「インバンド」を意味するのではありません。「インファイバ」はコントロール メッセージがデータ メッセージと同じファイバ内にあることを意味しており、「インバンド」と「アウトオブバンド」の両方が含まれます。「アウトオブファイバ」は、コントロール メッセージがデータ プレーンとは別のパスを通ることを意味しています。これには、別のファイバおよびイーサネットが含まれます。

OLS リンクに対するピア ノードの制御チャネル管理は、2 つのピア ノード間のリンクの場合と同じです。

（注）　ソフトウェアは、制御チャネルを管理目的でグレースフルにテイク ダウンすることをサポートしています（IETF LMP 文書のセクション 3.2.3 を参照）。ただし、グレースフル リスタートのプロビジョニングはありません（RFC 4204 のセクション 8 を参照）。

- グレースフルとは、制御チャネルに参加するノードがリンクの停止に合意することを意味します。制御チャネルをグレースフルにテイク ダウンするために、ノードは、HelloDeadInterval が期限切れになるか、またはもう一方のノードが ControlChannelDown フラグが設定された状態でメッセージを送り返すまで、メッセージ内の ControlChannelDown フラグをもう一方のノードに設定します。どちらの場合でも、その後、ノードはこの制御チャネルへのメッセージ送信を停止します。制御チャネルがテイク ダウンする前に、データ リンクを管理するために使用できるバックアップ制御チャネルが配置されている必要があります。
- ノングレースフルとは、ノードのうちの 1 つがメッセージ送信を停止することを意味します。もう一方の側は HelloDeadInterval のあとに障害を宣言しますが、Hello メッセージを送信し続けて制御チャネルがバックアップされるかどうかを確認します。

8.8.2.2　TE リンク管理

LMP は、リンクが TE リンクに分類され、これらのリンクのプロパティが両方のエンドポイントで同じになることを保証します。これが「TE リンク管理」または「リンク プロパティ相関」と呼ばれるものです。

リンク プロパティ相関は、TE リンク プロパティを同期させ、TE リンク設定を検証するために使用します。LMP のリンク プロパティ相関関数は、1 つまたは複数のデータ リンクを 1 つの TE リンクに集約し、TE リンクのプロパティを近接ノードに同期させます。この手順は、LinkSummary メッセージを近接ノードに送信することにより開始されます。LinkSummary メッセージには、ローカルおよびリモートの Link Identifier、TE リンクを構成するすべてのデータ リンクのリスト、およびさまざまなリンク プロパティが含まれます。リンク プロパティとの一致または不一致を示す LinkSummary の受信に応答して、LinkSummaryAck または LinkSummaryNack メッセージを送信することは必須です。

（注）　最大 256 個の LMP TE リンクがサポートされます。

8.8.2.3 リンク接続の検証

リンク接続の検証は、今後の CTC ソフトウェアのリリースでサポートされる可能性があります。

8.8.2.4 障害管理

障害管理は、制御チャネルがデータ リンクと物理的に異なっている場合に特に役立ちます。障害管理は、1 つまたは複数の TE リンク データ チャネルのステータスに関する高速通知に使用されます。障害管理の使用は、TE リンクの LinkSummary 交換の一部として取り決めます。データ リンクおよび TE リンク障害は高速で分離できるので、障害管理は、単方向および双方向の LSP をサポートします。割り当てられたデータ リンクのヘルスをモニタリングする従来の方法がもはや適切ではないため、透過的な装置が役立ちます。その代わりに、障害検出は、レイヤ 2 またはレイヤ 3 ではなく、物理レイヤ（たとえば、データの光または光モニタリングの損失）に委任されます。障害管理では、ChannelStatus、ChannelStatusAck、ChannelStatusRequest、および ChannelStatusResponse メッセージを使用します。

（注）　LMP Channel Activation/Deactivation Indication（LMP チャネル有効化 / 無効化表示）の手順は、サポートされません。これらの手順については、IETF LMP 文書のセクション 6.4 および 6.5 で説明しています。

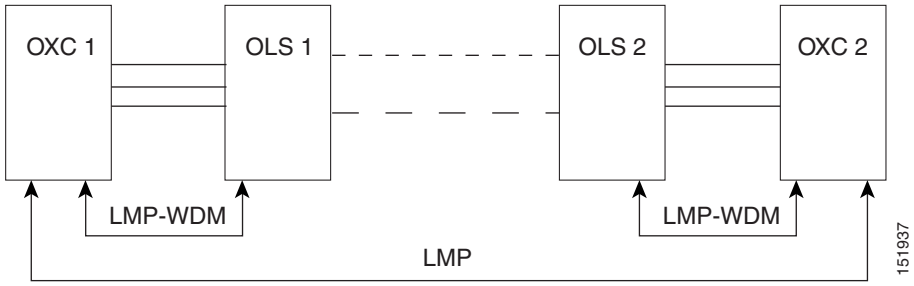
8.8.3 LMP WDM

LMP は、ピア ノード（シグナリングやルーティングで同位であるノード）間のトラフィック処理リンクを管理します。

（注）　ピア ノードと隣接 OLS ノードの間のリンクを管理できる LMP-WDM 拡張については、次の IETF 文書で説明しています。インターネット ドラフト『*draft-ietf-ccamp-lmp-wdm-03.txt*』、Proposed Standard、RFC 4209（http://www.ietf.org/rfc/rfc4209.txt）として発行（2005 年 11 月 1 日）

LMP WDM 拡張の目的は、LMP を OXC ノードと隣接 DWDM OLS ノードの間で使用できるようにすることです。図 8-23 に、LMP と LMP-WDM の関係を示します。OXC 1 と OXC 2 は、制御チャネルが LMP で管理されるピア ノードです。LMP-WDM は、OXC ノードと OLS ノードの間の制御チャネルを管理します。

図 8-23　LMP と LMP-WDM の関係



2 つの OLS ノードが LMP-WDM を介して設定および光リンクの現在の状態を 2 つのピア ノード（OXC 1 および OXC 2）に通信できる場合、ネットワーク ユーザビリティは、手動による設定の短縮および障害の検出と復旧の機能拡張により向上します。

8.8.4　LMP ネットワークの実装

図 8-24 に、ネットワーク レベルの LMP の実装を示します。これは、MPLS および GMPLS に基づくエンドツーエンド ルーティングを使用する IP プラス光ネットワークです。主なネットワーク コンポーネントは、次のとおりです。

- ルータ
  - Cisco Carrier Router System（CRS）
  - Cisco Gigabit Switch Router（GSR）
- OXC ノード
- Ultra Long-Haul（ULH; 超長距離）DWDM 機器

LMP とほかの機能により、Cisco ONS 15454 DWDM ノードは、ULH DWDM の役割を果たすことができます。図 8-24 に、ネットワーク コンポーネント間の関係を示します。

図 8-24　LMP システムの実装