CHAPTER 18

DLP D100 ～ D199

DLP-D100 プロキシ トンネルの削除

目的	この作業では、プロキシ トンネルを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

ステップ 1 **Provisioning > Network > Proxy** タブをクリックします。

ステップ 2 削除するプロキシ トンネルをクリックします。

ステップ 3 **Delete** をクリックします。

ステップ 4 元の NTP（手順）に戻って、続けます。

DLP-D101 ファイアウォール トンネルの削除

目的	この作業では、ファイアウォール トンネルを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

ステップ 1 **Provisioning > Network > Firewall** タブをクリックします。

ステップ 2 削除するファイアウォール トンネルをクリックします。

ステップ 3 **Delete** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D102 CTC を使用した CE-100T-8 カードのハードリセット

目的	この作業では、CE-100T-8 イーサネット カードをハードリセットします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

注意　CE-100T-8 カードをハードリセットすると、トラフィック ヒットが発生します。

（注）　ハードリセット オプションがイネーブルになるのは、カードが Locked-disabled,maintenance サービス状態の場合のみです。

ステップ 1　ノード ビューで、**Inventory** タブをクリックします。インベントリ ペインで適切なカードを検索します。

ステップ 2　**Admin State** ドロップダウン リストをクリックして、**Locked,maintenance** を選択します。**Apply** をクリックします。

ステップ 3　[Action may be service affecting. Are you sure?] ダイアログボックスで **Yes** をクリックします。

ステップ 4　カードのサービス状態が Locked enabled, loopback & maintenance になります。Cisco Transport Controller（CTC; シスコ トランスポート コントローラ）ではカードの前面プレートがブルーで表示され、SRV LED はオレンジになります。

ステップ 5　カードを右クリックして、ショートカット メニューを表示します。

ステップ 6　**Hard-reset Card** をクリックします。

ステップ 7　[Are you sure you want to hard-reset this card?] ダイアログボックスで、**Yes** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-D103 CTC を使用した CE-100T-8 カードのソフトリセット

目的	この作業では、CE-100T-8 カードをソフトリセットします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

（注） CE-100T-8 カードをソフトリセットしても、通常はエラーが発生しません。ソフト リセット中にプロビジョニングを変更した場合、またはソフトウェア アップグレード プロセス中にファームウェアを交換した場合は、リセット中にエラーが発生します。

ステップ 1　ノード ビューで、CE-100T-8 カードを右クリックして、ショートカット メニューを表示します。

ステップ 2　**Soft-reset Card** をクリックします。

ステップ 3　[Are you sure you want to soft-reset this card?] ダイアログボックスで、**Yes** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D104 MRC カードへのファイバ クリップの取り付け

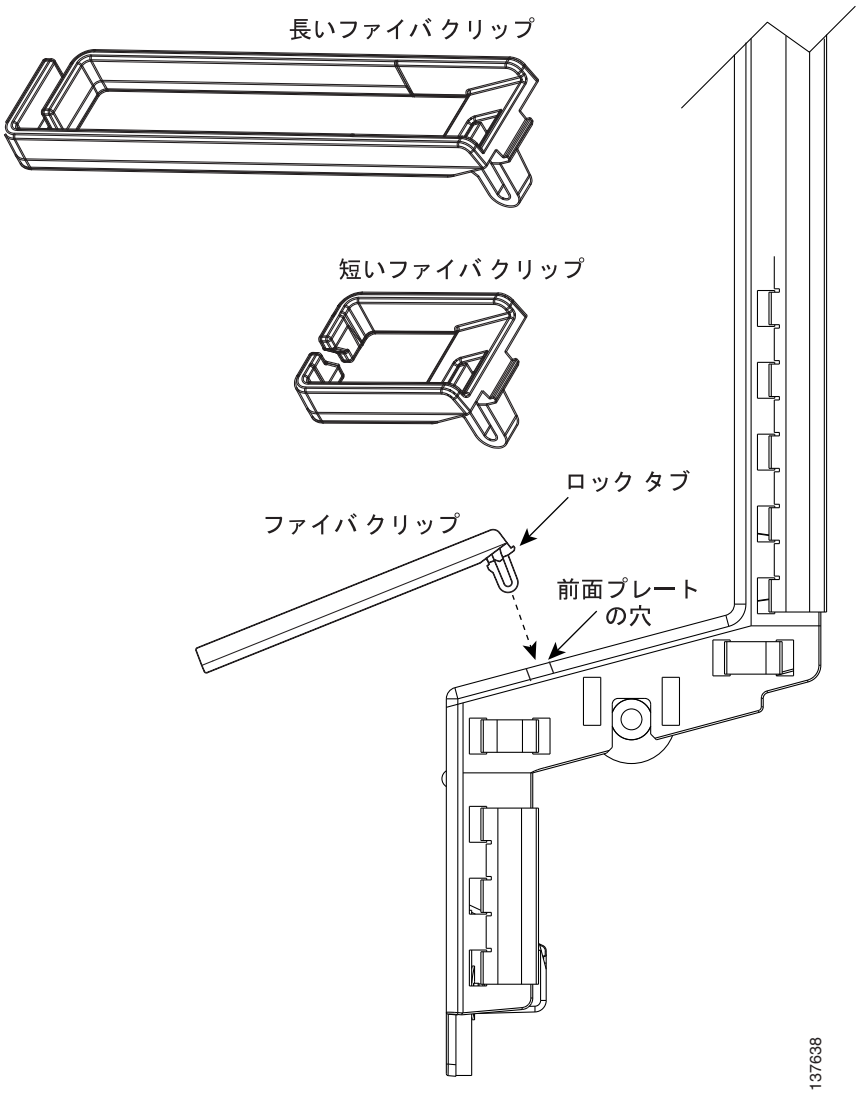
目的	この作業では、ファイバを適切に配線できるように、ファイバ クリップを取り付けます。この作業は、15454_MRC-12 および MRC-2.5G-12 カードの場合に必須です。CTC では、15454_MRC-12 カードは [MRC-12] とのみ表示されます。
工具 / 機器	必要に応じて、短い、または長いファイバ クリップ
事前準備手順	NTP-D16 STM-N カードおよびコネクタの取り付け（p.2-7）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

（注） 光ファイバを MRC カードに取り付ける前、または取り付けたあとに、ファイバ クリップを取り付けることができます。

ステップ 1　使用に適したクリップを判別します。標準キャビネット扉の場合は短いクリップを、拡張扉の場合は長いクリップを使用します。

ステップ 2　ファイバ クリップの突起を、前面プレートの傾斜面にある長方形の穴に差し込みます（図 18-1）。

図 18-1　ファイバ クリップの取り付け



ステップ 3　クリップを穴に押し込んで、ロック タブを所定場所にしっかりはめ込みます。ファイバ クリップを取り外すには、クリップを前方上側に傾けながらロック タブを押し、外します。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D105 ノードへの RADIUS 認証の設定

目的	この作業では、ノードに Remote Authentication Dial In User Service（RADIUS）認証を設定します。RADIUS は、ネットワークに接続しようとしているリモート ユーザを検証します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49） ノードに RADIUS 認証を設定する前に、まずノードをネットワーク デバイスとして RADIUS サーバに追加する必要あります。RADIUS サーバの設定手順については、『*User Guide for Cisco Secure ACS for Windows Server*』を参照してください。
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

注意　ノードに RADIUS 認証を設定するには、目的のノードを RADIUS サーバに追加し、RADIUS サーバを認証者リストに追加する必要があります。RADIUS 認証をアクティブにする前にノードを RADIUS サーバに追加しておかないと、ユーザはノードにアクセスできません。RADIUS サーバにノードを追加する手順については、『*User Guide for Cisco Secure ACS for Windows Server*』を参照してください。

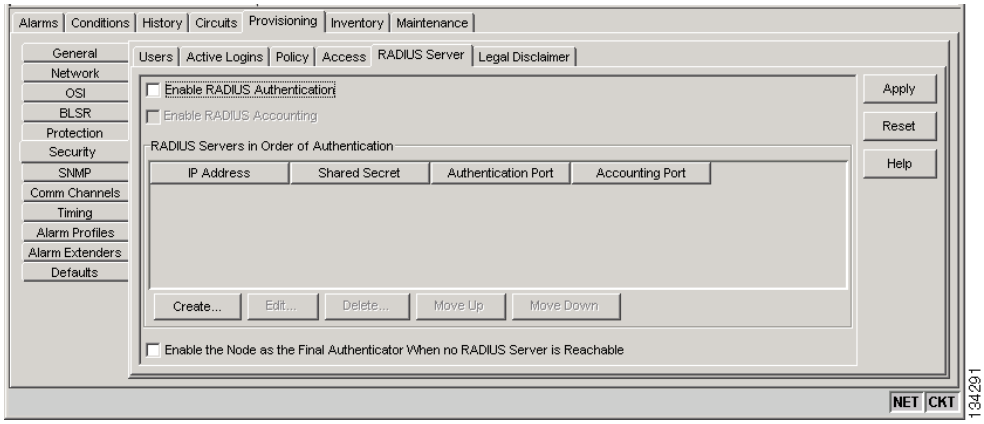
（注）　RADIUS サーバにユーザを追加する場合は、次の Cisco VSA（vendor-specific attribute; ベンダー固有属性）を指定する必要があります。

shell:priv-lvl=*N*。ここで *N* は次のいずれかです。

- 0（検索ユーザ）
- 1（メンテナンス ユーザ）
- 2（プロビジョニング ユーザ）
- 3（スーパーユーザ）

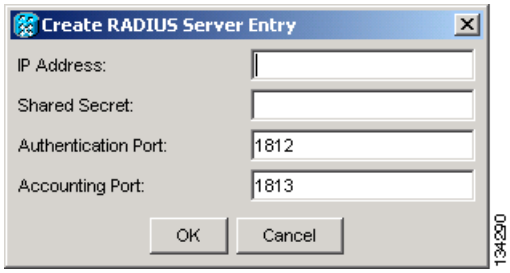
ステップ 1　ノード ビューで、**Provisioning > Security > RADIUS Server** タブをクリックします（図 18-2）。

図 18-2　RADIUS Server タブ



ステップ 2　**Create** をクリックして、認証者リストに RADIUS サーバを追加します。Create RADIUS Server Entry ウィンドウが表示されます（図 18-3）。

図 18-3　Create RADIUS Server Entry ウィンドウ



ステップ 3　IP Address フィールドに、RADIUS サーバの IP アドレスを入力します。ノードが End Network Element（ENE）の場合は、このフィールドに Gateway Network Element（GNE; ゲートウェイ ネットワーク エレメント）の IP アドレスを入力します。

GNE はネットワーク内の ENE から RADIUS サーバに認証要求を渡します。GNE が RADIUS サーバのクライアントとして指定されている場合は、認証が許可されます。

注意　ENE ノードは GNE を使用して RADIUS サーバに認証要求を渡します。したがって、認証を行うには、RADIUS サーバに ENE ノードを個別に追加する必要があります。RADIUS 認証をアクティブにする前に ENE ノードを RADIUS サーバに追加しておかないと、ユーザはノードにアクセスできません。RADIUS サーバにノードを追加する手順については、『*User Guide for Cisco Secure ACS for Windows Server*』を参照してください。

ステップ 4　Shared Secret フィールドに共有秘密を入力します。共有秘密は、RADIUS クライアントと RADIUS サーバ間のパスワードとして機能するテキスト ストリングです。

ステップ 5　Authentication Port フィールドに RADIUS 認証ポート番号を入力します。デフォルト ポートは 1812 です。ノードが ENE の場合は、認証ポートを 1860 ～ 1869 の番号に設定します。

ステップ 6　Accounting Port フィールドに RADIUS アカウンティング ポートを入力します。デフォルト ポートは 1813 です。ノードが ENE の場合は、アカウンティング ポートを 1870 ～ 1879 の番号に設定します。

ステップ 7　**OK** をクリックします。RADIUS 認証者リストに RADIUS サーバが追加されます。

（注）　ノードの認証者リストには RADIUS サーバを 10 台まで追加できます。

ステップ 8　既存の RADIUS サーバを変更するには、**Edit** をクリックします。変更できるのは、IP アドレス、共有秘密、認証ポート、およびアカウンティング ポートです。

ステップ 9　選択された RADIUS サーバを削除するには、**Delete** をクリックします。

ステップ 10　RADIUS 認証者リストを並べ替えるには、**Move Up** または **Move Down** をクリックします。ノードはリストの上から下に向かって順に、サーバからの認証を要求します。到達可能なサーバがない場合、ノードはリストに記載された次の RADIUS サーバからの認証を要求します。

ステップ 11　ノードに対するリモート サーバ認証を有効にするには、**Enable RADIUS Authentication** チェックボックスをクリックします。

ステップ 12　監査証跡で RADIUS 認証情報を表示する場合は、**Enable RADIUS Accounting** チェックボックスをクリックします。

ステップ 13　ノードを最終認証者として設定する場合は、**Enable the Node as the Final Authenticator** チェックボックスをクリックします。このようにすると、使用可能な RADIUS 認証者が存在しない場合、ノードはユーザをロックアウトしないで、ログイン認証を行います。

ステップ 14　すべての変更を保存する場合は **Apply** を、すべての変更をクリアする場合は **Reset** をクリックします。

ステップ 15　元の NTP（手順）に戻ります。

DLP-D106 アクティブ ログインの表示および終了

目的	この作業では、アクティブ CTC ログインを表示し、最終アクティビティ時刻を検索し、現在のログインをすべて終了します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	表示の場合は検索以上のレベル、セッション終了の場合はスーパーユーザ

ステップ 1　ノード ビューで、**Provisioning > Security > Active Logins** タブをクリックします。Active Logins サブタブに次の情報が表示されます。

- ユーザ ID
- ユーザ IP アドレス
- ユーザが現在ログインしているノード
- セッション タイプ（EMS、TL1、FTP、Telnet、または SSH）
- ログイン時刻
- 最終アクティビティ時刻

ステップ 2　ログインしているすべてのユーザのセッションを終了するには、**Logout** をクリックします。これでログイン中のスーパーユーザを除いて、現在のすべてのユーザがログアウトします。

ステップ 3　Last Activity Time フィールドにユーザの最新アクティビティの日時を表示するには、**Retrieve Last Activity Time** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D107 SFP または XFP デバイスの事前プロビジョニング

目的	この作業では、MRC-12、MRC-2.5G-12、および STM64-XFP カードに着脱可能小型フォーム ファクタ（SFP/XFP）を事前にプロビジョニングします。SFP/XFP は CTC では Pluggable Port Module（PPM）として表されます。シスコ承認の STM-1、STM-4、STM-16、STM-64、およびマルチレート PPM は、ONS 15454 SDH と互換性があります。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	なし

（注）　MRC-12 または MRC-2.5G-12 カードに SFP を取り付ける前に、『*Cisco ONS 15454 SDH Reference Manual*』の「Optical Cards」の章のカードに関する情報を参照し、SFP を取り付けるポートおよび使用中のクロスコネクト カードに基づいた帯域幅制限を確認してください。

（注）　マルチレート SFP を事前プロビジョニングする場合は、「DLP-D132 MRC-12 および MRC-2.5G-12 カード上でのマルチレート PPM のプロビジョニング」（p.18-28）に従って、次に回線レートを選択する必要があります。

ステップ 1　ノード ビューで、**Alarms** タブをクリックします。

a. アラーム フィルタの機能がオフであることを確認します。必要に応じて、「DLP-D227 アラーム フィルタのディセーブル化」（p.19-29）を参照してください。

b. 不明な状態がネットワーク上に表示されていないことを確認します。不明な状態が表示されている場合は、作業を進める前に解決してください。『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

c. 「DLP-D147 CTC データのエクスポート」（p.18-41）を行い、アラームおよび状態の情報をエクスポートします。

ステップ 2　ノード ビューで、PPM 設定をプロビジョニングするカードをダブルクリックします。

ステップ 3　**Provisioning > Pluggable Port Modules** タブをクリックします。

ステップ 4　Pluggable Port Modules 領域で、**Create** をクリックします。Create PPM ダイアログボックスが表示されます。

ステップ 5　Create PPM ダイアログボックスで次の情報を入力します。

- PPM — ドロップダウン リストから、SFP/XFP を事前プロビジョニングするスロットの番号を選択します。
- PPM Type — ドロップダウン リストから、SFP/XFP でサポートされているポート数を選択します。サポートされているポート数が 1 の場合、使用できるのは PPM (1 port) オプションのみです。

ステップ 6　**OK** をクリックします。Pluggable Port Modules 領域に新規に選択されたポートが表示されます。SFP/XFP が実際に取り付けられるまで、Pluggable Port Modules 領域の行はライト ブルーになり、Actual Equipment Type カラムには事前プロビジョニングされた PPM が unknown と表示されます。SFP/XFP を取り付けると、行はホワイトになり、カラムには機器の名前が表示されます。

ステップ 7　Pluggable Port Modules 領域のリストに PPM が表示されているか確認します。表示されない場合は、ステップ 4 ～ 6 を繰り返します。

ステップ 8　Provisioning タブで、**Line** サブタブをクリックします。事前プロビジョニングする PPM によっては、必要に応じて **Reach** および **Wavelength** カラムを使用してこれらのパラメータを設定します。

（注）　特定のプラットフォーム タイプの PPM で編集可能なパラメータのみプロビジョニングできます。たとえば、プラットフォームによっては、PPM で波長または到達範囲が設定できない場合があります。この場合、波長および到達範囲はプロビジョニングできません。

ステップ 9　別の PPM を作成する場合は、この作業を繰り返します。

ステップ 10　**OK** をクリックします。

ステップ 11　SFP/XFP を取り付ける準備ができたら、「DLP-D335 GBIC または SFP/XFP デバイスの取り付け」（p.20-31）を行います。

ステップ 12　元の NTP（手順）に戻ります。

DLP-D108 STM-N カードの回線設定の変更

目的	この作業では、STM-N カードの回線の伝送設定を変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） ユーザがプロビジョニングできるカード設定のデフォルト値とドメインについては、『*Cisco ONS 15454 SDH Reference Manual*』の付録「Network Element Defaults」を参照してください。

ステップ 1　ノード ビューで、回線の設定を変更する STM-N カードをダブルクリックします。

ステップ 2　**Provisioning > Line** タブをクリックします。

ステップ 3　表 18-1 のリストに示されている設定を変更します。

ステップ 4　**Apply** をクリックします。

表 18-1　STM-N カードの回線設定

パラメータ	内容	オプション
Port	（表示専用）ポート番号	• 1（STM-4、STM-16、STM-64） • 1 ～ 4（OC3 IR 4/STM1 SH 1310、OC12 IR/STM4 SH 1310-4） • 1 ～ 8（OC3IR/STM1SH 1310-8） • 1 ～ 12（MRC-12、MRC-2.5G-12）
Port Name	ポートに名前を割り当てます。	ユーザ定義。名前を 32 文字以下の英数字または特殊文字で指定します。デフォルトではブランクです。 「DLP-D314 ポートへの名前の割り当て」（p.20-8）を参照してください。
Port Rate	（表示専用）（MRC-12、MRC-2.5G-12、および STM64-XFP カードのみ）PPM に設定されたポート レートを表示します。	• STM-1 • STM-4 • STM-16 • STM-64（STM64-XFP のみ）
SF BER	Signal Fail Bit Error Rate（SFBER; 信号損失ビット エラー レート）を設定します。	• 1E-3 • 1E-4 • 1E-5
SD BER	信号劣化ビット エラー レートを設定します。	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9

表 18-1　STM-N カードの回線設定（続き）

パラメータ	内容	オプション
Provides Synch	（表示専用）オンにすると、そのカードがネットワーク要素（NE）のタイミング基準としてプロビジョニングされます。	• ○ • ×
Send Do Not Use	オンにすると、DUS（do not use）メッセージが S1 バイトで送信されます。	• ○ • ×
Synch Message In	Synchronization Status Message（SSM）（S1 バイト）をイネーブルにして、そのノードで最適なタイミング ソースを選択できるようにします。	• ○ • ×
Send <FF> DoNotUse	オンにすると、特別な DUS（0xff）メッセージが S1 バイトで送信されます。	• ○ • ×
Admin SSM In	ここで指定した値は、デフォルト設定の同期追跡不能（STU）より優先されます。STM-N カードで Sync Message In がイネーブルになっている場合は、Admin SSM In を選択できません。	• G811 • G812T • G812L • SETS • DUS
MS-SPRing Ext.Byte	このパラメータで、Multiplex Section-Shared Protection Ring（MS-SPRing; 多重化セクション共有保護リング）の拡張バイトを変更できます。	• K3 • Z2 • E2 • F1
PJVC4Mon#	ポインタの位置調整に使用される VC4 を設定します。ゼロに設定すると、VC4 を監視します。各 STM-N ポートで 1 つの VC4 だけを監視できます。	• 0 ～ 1（STM-1、ポートごと） • 0 ～ 4（STM-4、ポートごと） • 0 ～ 16（STM-16） • 0 ～ 64（STM-64）
Admin State	ポートの管理サービス状態を設定します。ネットワークの状態によっては変更できません。管理状態の詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の付録「Administrative and Service States」を参照してください。	• Unlocked — ポートをインサービス状態にします。ポートのサービス状態は、Unlocked-enabled に変化します。 • Unlocked,automaticInService — ポートを自動インサービス状態にします。ポートのサービス状態は、Unlocked-disabled,automaticInService に変化します。 • Locked,disabled — サービスからポートを外して、ディセーブルにします。ポートのサービス状態は、Locked-enabled,disabled に変化します。 • Locked,maintenance — メンテナンスのためにサービスからポートを外します。ポートのサービス状態は、Locked-enabled,maintenance に変化します。 **（注）** CTC では、ポートのサービス状態を Unlocked-enabled から Locked-enabled,disabled に変更できません。最初にポートを Locked-enabled,maintenance サービス状態に変更してから、Locked-enabled,disabled サービス状態にする必要があります。

表 18-1　STM-N カードの回線設定（続き）

パラメータ	内容	オプション
Service State	（表示専用）ポートの全体的な状態を示します。自動的に生成されます。サービス状態は、Primary State-Primary State Qualifier, Secondary State という形式で表されます。サービス状態の詳細は、『*Cisco ONS 15454 SDH Reference Manual*』の付録「Administrative and Service States」を参照してください。	• Unlocked-enabled — ポートは完全に動作し、プロビジョニングされたとおりに動作します。 • Unlocked-disabled,automaticInService — ポートはアウト オブ サービスですが、トラフィックは伝送されます。アラームの報告は抑制されています。ONS ノードは、ポートで信号にエラーがないかを監視します。エラーのない信号を検出したあと、ポートはソーク期間の間 Unlocked-disabled,automaticInService 状態に留まります。ソーク期間が過ぎると、ポートのサービス状態は Unlocked-enabled に変化します。 • Locked-enabled,disabled — ポートはアウト オブ サービス状態で、トラフィックは伝送できません。 • Locked-enabled,maintenance — ポートは、メンテナンスのためのアウト オブ サービス状態です。アラームの報告は抑制されていますが、トラフィックは伝送され、ループバックが許可されます。
AINS Soak	自動インサービス ソーク期間を設定します。	• カードが自動的にインサービス状態（IS）へ変わるために必要な期間、つまり、入力信号が有効であり続ける期間。hh:mm の形式で表します。 • 0 ～ 48 時間、15 分刻み
Type	ポートが SDH として表示されます。	• SDH
ALS Mode	自動レーザー シャットダウン機能を設定します。	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test
Reach	（一部のカードには適用されない）到達範囲をプロビジョニングできます。Auto Provision を選択して、ハードウェアの PPM 到達範囲から到達範囲を自動的にプロビジョニングすることもできます。	ドロップダウン リストに表示されるオプションは、カードによって異なります。 • SR（短距離、最大 2 km） • SR-1（最大 2 km） • IR-1（中距離、最大 15 km） • IR-2（最大 40 km） • LR-1（長距離、最大 40 km） • LR-2（最大 80 km） • LR-3（最大 80 km）
Wavelength	（一部のカードには適用されない）波長周波数をプロビジョニングできます。	• First Tunable Wavelength • 1310 nm • 1550 nm • 1470 nm • 1490 nm • 1510 nm • 1530 nm • 1570 nm • 1590 nm • 1610 nm

ステップ 5　元の NTP（手順）に戻ります。

DLP-D109 STM-64、MRC-12、および MRC-2.5G-12 カードの光しきい値設定の変更

目的	この作業では、STM-64、MRC-12、MRC-2.5G-12 カードの光しきい値設定を変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、光設定を変更するカードをダブルクリックします。

ステップ 2　**Provisioning > Optics Thresholds** タブをクリックします。

ステップ 3　変更するフィールドをクリックして、表 18-2 で説明されている設定を任意に変更します。フィールドには、ドロップダウン リストからオプションを選択するもの、値を入力するもの、およびチェックボックスをオンまたはオフにするものがあります。

表 18-2　光しきい値の設定

パラメータ	内容	オプション
Port	（表示専用）ポート番号	• 1（STM-64、STM64-XFP） • 1 ～ 12（MRC_12、MRC-2.5G-12）
LBC-LOW	レーザー バイアス電流（最小）	デフォルト（15 分 /1 日）：50%
LBC-HIGH	レーザー バイアス電流（最大）	デフォルト（15 分 /1 日）：150%
OPT-LOW	伝送光パワー（最小）	デフォルト（15 分 /1 日）：80%
OPT-HIGH	伝送光パワー（最大）	デフォルト（15 分 /1 日）：120%
OPR-LOW	受信光パワー（最小）	デフォルト（15 分 /1 日）：50%
OPR-HIGH	受信光パワー（最大）	デフォルト（15 分 /1 日）：200%
Set OPR	受信光パワーを設定すると、受信パワー レベルが 100% に設定されます。レシーバ パワーが減少すると、レシーバ パワーの低下を反映するように OPR 値が小さくなります。たとえば、レシーバ パワーが 3 dBm 減少すると、OPR は 50% 減少します。	**SET** をクリックします。
Types	しきい値を超えた場合に発生するアラートのタイプを設定します。しきい値のタイプを変更するには、タイプを選択して、**Refresh** をクリックします。	• Threshold Cross Alert（TCA） • Alarm
Intervals	パラメータ数を収集するためのインターバルを設定します。インターバルを変更するには、目的のインターバルを選択して、**Refresh** をクリックします。	• 15 Min • 1 Day

ステップ 4　**Apply** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

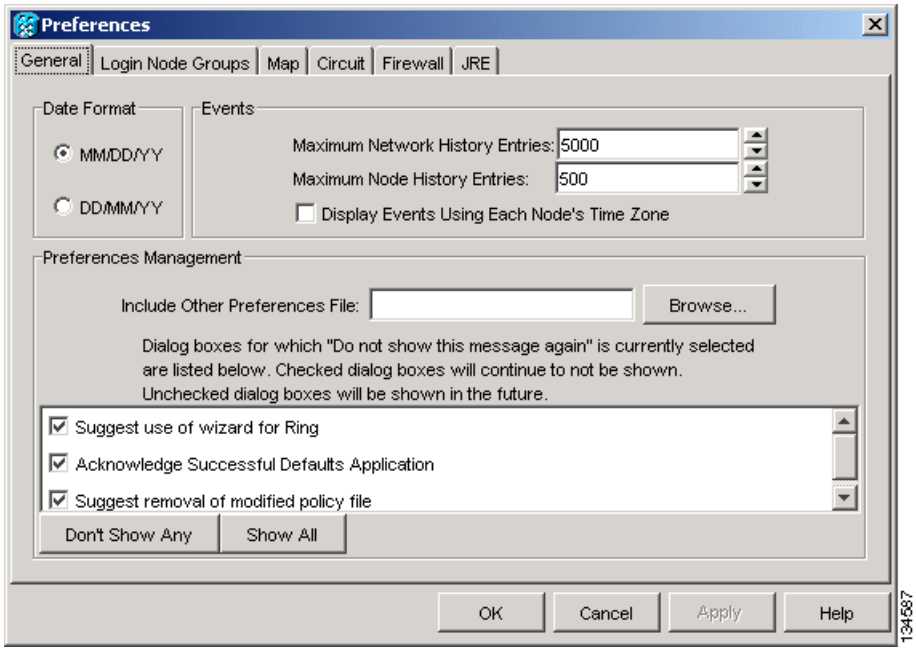
DLP-D111 アラーム履歴のセッション エントリ最大数の変更

目的	この作業では、アラーム履歴に記録できるセッション エントリの最大数を変更します。履歴リストには、将来の参照やトラブルシューティングで使用する情報が保存されます。この作業は、その履歴リストを拡張するときに使用します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　[Edit] メニューから **[Preferences]** を選択します。

CTC の Preferences ダイアログ ボックスが表示されます（図 18-4）。

図 18-4　CTC の Preferences ダイアログ ボックス



ステップ 2　Maximum History Entries フィールドの横にある上矢印または下矢印ボタンをクリックして、エントリを変更します。

ステップ 3　**Apply** をクリックし、**OK** をクリックします。

（注）　Maximum History Entries の値を選択可能な最大値に設定すると、CTC のメモリが多く使用されて、CTC のパフォーマンスが低下する可能性があります。

（注）　この作業では、CTC セッションで記録された履歴の最大エントリ数を変更します。このエントリ数を変更しても、ネットワーク、ノード、およびカードに対して表示可能な履歴の最大エントリ数には影響しません。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D112 時間帯に合わせたアラームと状態の表示

目的	この作業では、イベントのタイムスタンプを、アラームの報告元 ONS ノードが位置する時間帯に変更します。デフォルトでは、イベントのタイムスタンプが CTC ワークステーションの属する時間帯に設定されています。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　[Edit] メニューから **[Preferences]** を選択します。

CTC の Preferences ダイアログ ボックスが表示されます（図 18-4）。

ステップ 2　**Display Events Using Each Node's Timezone** チェックボックスをオンにします。Apply ボタンがイネーブルになります。

ステップ 3　**Apply** をクリックし、**OK** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D113 アラームの同期

目的	この作業は、カード、ノード、またはネットワーク レベルで発生した ONS 15454 SDH のイベントを表示するときに使用します。また、アラーム リストをリフレッシュして、アラームと状態の変化（発生またはクリア）を調べるときにも使用します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　カード ビュー、ノード ビュー、またはネットワーク ビューで、**Alarms** タブをクリックします。

ステップ 2　**Synchronize** をクリックします。

このボタンをクリックすると、カード、ノード、またはネットワークで発生している現在のアラームの概要が表示されます。CTC では、ノードから発生メッセージまたはクリア メッセージが届くと Alarms ウィンドウが自動的に更新されます。そのため、この手順は必要なときにだけ使用します。

（注）　セッションが進行しているときに発生したアラームは、Alarms ウィンドウで New カラムにチェック マークが付けられます。Synchronize をクリックすると、このチェック マークは消えます。

ステップ 3　元の NTP（手順）に戻ります。

DLP-D114 状態の表示

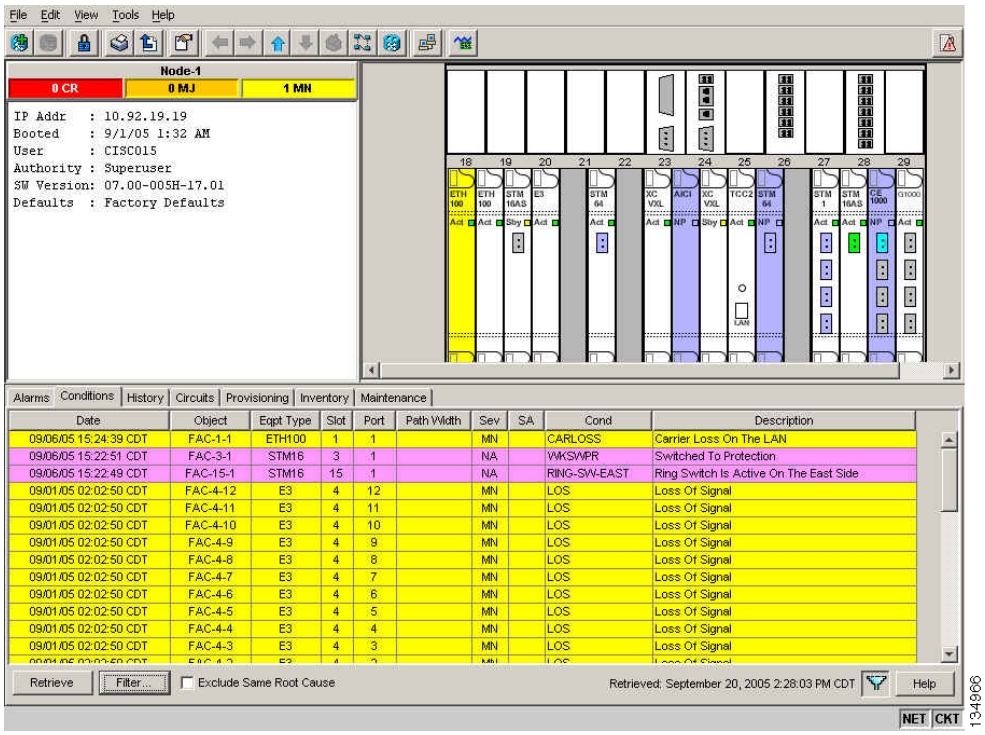
目的	この作業は、カード、ノード、またはネットワークのレベルで状態（重大度が報告なし [NR] のイベント）を表示するときに使用します。Conditions タブでは、アラームに至らなかった変化やイベントの記録が詳細に得られます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　カード ビュー、ノード ビュー、またはネットワーク ビューで、**Conditions** タブをクリックします。

ステップ 2　**Retrieve** をクリックします（図 18-5）。

Retrieve ボタンをクリックすると、ノード、カード、またはネットワークに発生している現在の障害状態がまとめて表示されます。ノード上のイベントに変化があっても、ウィンドウはアップデートされません。変化を確認するには、Retrieve ボタンをクリックする必要があります。

図 18-5　ノード ビューの Conditions ウィンドウ



Conditions ウィンドウには、ノードで発生した障害の状態が、報告されるかどうかに関係なくすべて表示されます。

（注）　フィルタによって表示対象から除外されたアラームは、報告されません。詳細については、「DLP-D227 アラーム フィルタのディセーブル化」（p.19-29）を参照してください。

重大度がメジャー（MJ）、マイナー（MN）、またはクリティカル（CR）で報告されるイベントはアラームです。アラームなし（NA）として報告されるイベントは状態です。まったく報告されない状態は、Conditions ウィンドウの重大度カラムに報告なし（NR）のマークが付きます。

重大度が CR、MJ、MN、または NA であっても、除外または抑制によって報告されない状態があります。それらの状態も、Conditions ウィンドウで NR のマークが付きます。

アラーム プロファイルを使用している場合は、そこで選択した重大度が現在の状態に表示されます。アラーム プロファイルの詳細については、「NTP-D71 アラーム重大度プロファイルの作成、ダウンロード、および割り当て」（p.9-8）を参照してください。

（注）　ポートのサービス状態が Locked-enabled,maintenance になると、Alarms Suppressed for Maintenance（AS-MT）状態が発生します。アラームと状態のトラブルシューティングについては、『*Cisco ONS 15454 SDH Troubleshooting Guide*』を参照してください。

（注）　ポートのサービス状態が Unlocked-disabled,automaticInService になっても、有効な信号線に接続されていないと Loss of Signal（LOS; 信号消失）アラームが発生します。

ステップ 3　除外規則を適用する場合は、ノード ビューまたはネットワーク ビューの **Exclude Same Root Cause** チェックボックスをオンにします。カード ビューの Exclude Same Root Cause チェックボックスはオンにしないでください。

除外規則を適用すると、原因が同じ下位レベルのアラームまたは状態はすべて排除されます。たとえば、光ファイバが切断されると LOS アラーム、Alarm Indication Signal（AIS; アラーム表示信号）状態、および Signal Failure（SF）が発生しますが、Exclude Same Root Cause チェックボックスをオンにしておくと、LOS アラームだけが表示されます。

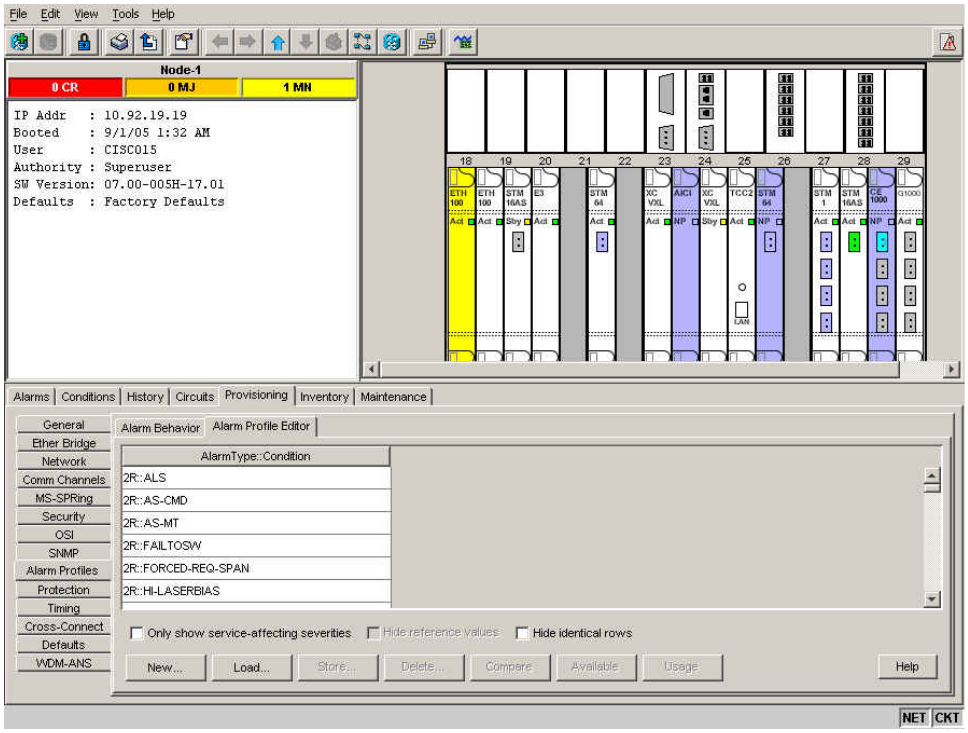
ステップ 4　元の NTP（手順）に戻ります。

DLP-D117 カードおよびノードへのアラーム プロファイルの適用

目的	この作業では、カードまたはノードにカスタムまたはデフォルトのアラーム プロファイルを適用します。
工具 / 機器	なし
事前準備手順	DLP-D425 アラーム重大度プロファイルの新規作成または複製（p.21-6） DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします（図 18-6）。

図 18-6　ノード ビューのアラーム プロファイル



ステップ 2　1 枚のカードにプロファイルを適用する場合は、次の手順を実行します。

a.　カードの Profile 行をクリックします。

b.　ドロップダウン リストから新しいプロファイルを選択します。

c.　**Apply** をクリックします。

ステップ 3　ノード全体にプロファイルを適用する場合は、次の手順を実行します。

a.　ウィンドウの下にある **Node Profile** ドロップダウン リストの矢印をクリックします（図 18-6）。

b.　ドロップダウン リストから新しいアラーム プロファイルを選択します。

c.　**Apply** をクリックします。

ステップ 4　新しいプロファイルを適用したあとで、以前のアラーム プロファイルを再適用する場合は、そのプロファイルを選択してもう一度 **Apply** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D121 ポインタ位置調整カウントの PM のイネーブル化

目的	この作業では、ポインタ位置調整カウントをイネーブルにして、VC4 ペイロードの位相変動を調整したり、ノード間のクロック同期を監視したりできるようにします。ポインタ位置調整カウントの状態が大きい値のままで推移している場合は、ノード間のクロック同期に問題があります。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　DLP-D122 IPPM のイネーブル化（p.18-22）で指定された IPPM のイネーブル化

ステップ 2　ノード ビューで、監視する STM-N カードをダブルクリックします。カード ビューが表示されます。

STM-N Line Terminating Equipment（LTE）カードのリストについては、表 18-3 を参照してください。

表 18-3　回線を終端するためのトラフィック カード（LTE）

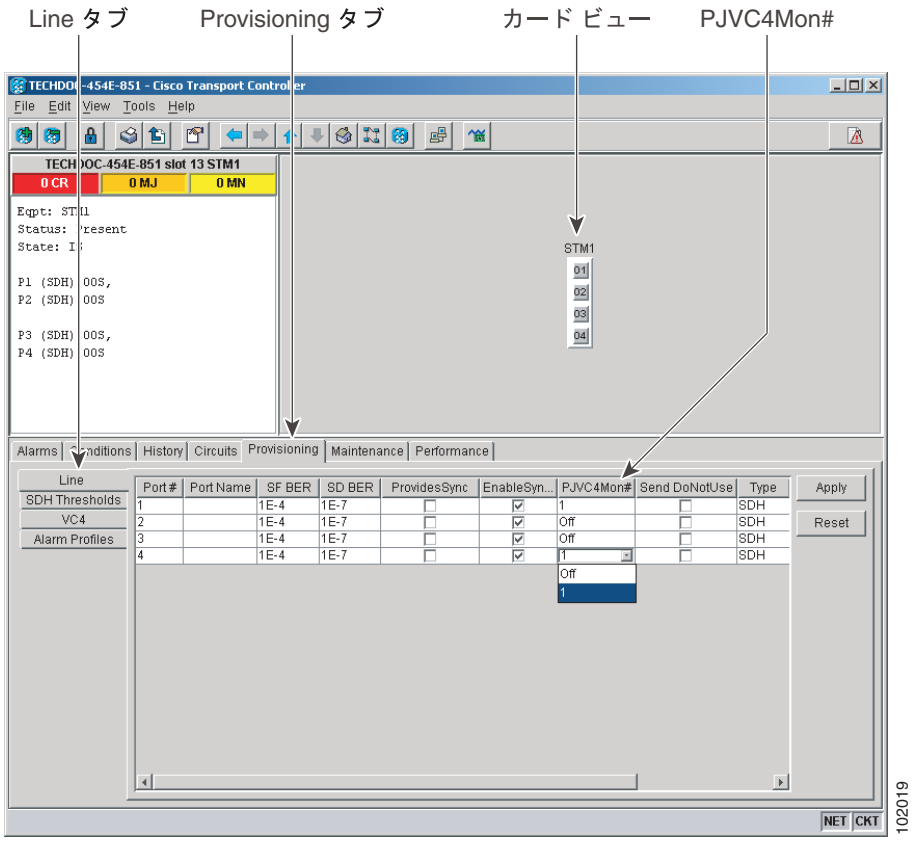
LTE
STM1E-12
OC3 IR 4/STM1 SH 1310
OC3 IR/STM1SH 1310-8
OC12 IR/STM4 SH 1310
OC12 LR/STM4 LH 1310
OC12 LR/STM4 LH 1550
OC12-4 IR/STM4 SH 1310-4
OC48 IR/STM16 SH AS 1310
OC48 LR/STM16 LH AS 1550
OC48 ELR/STM16 EH 100 GHz
OC192 SR/STM64 IO 1310
OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550
OC192 ELR/STM64 LH ITU 15xx.xx

ステップ 3　**Provisioning > Line** タブをクリックします。

ステップ 4　PJVC4Mon# ドロップダウン リストをクリックし、次の規則に基づいて選択します（図 18-7）。

- Off — ポインタ位置調整のモニタリングがディセーブルであることを示します（デフォルト）。
- 1 ～ *n* — ポート上の VC4 の番号です。PJVC4Mon# カード ドロップダウン リストを使用して、ポートごとに VC4 を 1 つイネーブルにできます。

図 18-7　ポインタ位置調整カウントのパラメータのイネーブル化またはディセーブル化



ステップ 5　Service State フィールドで、ポートのサービス状態が Unlocked-enabled になっていることを確認します。

ステップ 6　ポートの状態が Unlocked-enabled になっている場合は、**Apply** をクリックします。ポートのサービス状態がアウト オブ サービス（Locked-enabled,disabled、Locked-enabled,maintenance、Unlocked-disabled,automaticInService）になっている場合は、Admin State ドロップダウン リストで **Unlocked** を選択してから、**Apply** をクリックします。

ステップ 7　**Performance** タブをクリックして、Performance Monitoring（PM）のパラメータを表示します。PM の情報、詳細および定義については、『*Cisco ONS 15454 SDH Reference Manual* 』の「Performance Monitoring」の章を参照してください。

（注）　ポインタ位置調整カウントの PM がイネーブルになっていないと、Positive Pointer Justification Count（PPJC）パラメータと Negative Pointer Justification Count（NPJC）パラメータは、白黒で表示されます。

ステップ 8　元の NTP（手順）に戻ります。

DLP-D122 IPPM のイネーブル化

目的	この作業では、Intermediate Path Performance Monitoring（IPPM）をイネーブルにします。IPPM をイネーブルにすることによって、中間ノードに流れる大量の VC4 トラフィックを監視できるようになります。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

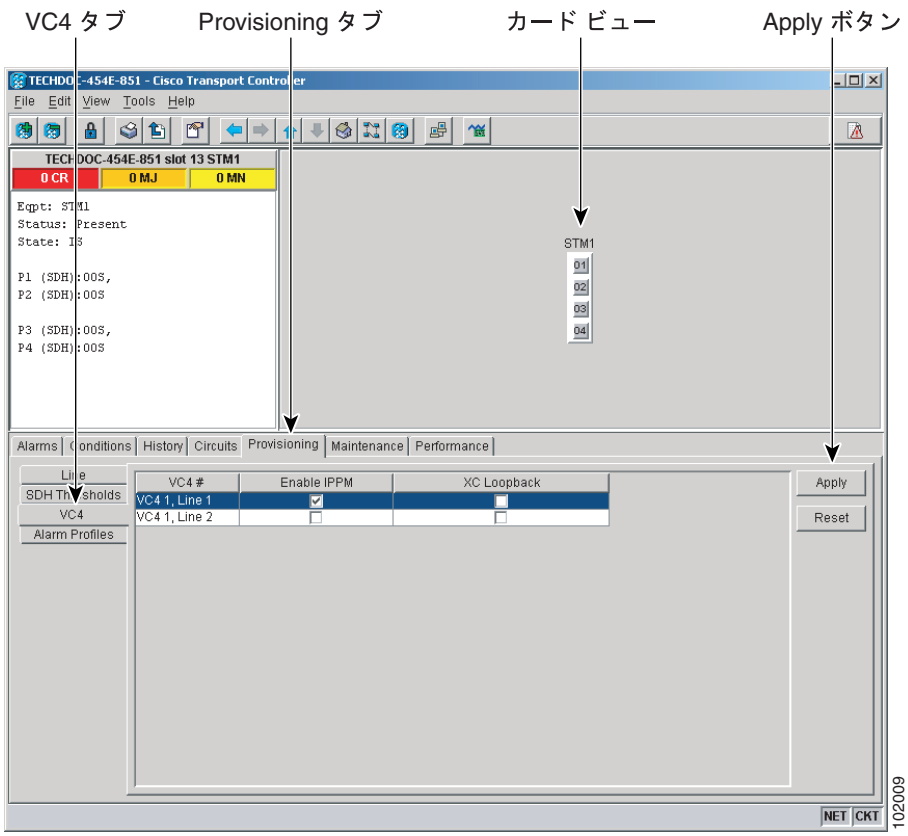
（注） IPPM で監視できるパラメータは、P-EB、P-BBE、P-ES、P-SES、および P-UAS です。IPPM パラメータの詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

ステップ 1　ノード ビューで、監視する STM-N カードをダブルクリックします。カード ビューが表示されます。

STM-N LTE カードのリストについては、表 18-3 を参照してください。

ステップ 2　**Provisioning > VC4** タブをクリックします（図 18-8）。

図 18-8　IPPM をイネーブルまたはディセーブルにするための VC4 タブ



ステップ 3　Enable IPPM カラムにあるチェックボックスをクリックし、次の規則に基づいて選択します。

- チェックボックスがオフ — その VC4 の IPPM はディセーブルです（デフォルト）。
- チェックボックスがオン — その VC4 の IPPM はイネーブルです。

ステップ 4　**Apply** をクリックします。

ステップ 5　**Performance** タブをクリックして、PM パラメータを表示します。IPPM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D124 15 分間隔で行う PM カウントのリフレッシュ

目的	この作業では、ウィンドウの表示を変更して、PM カウントを 15 分間隔で表示するようにします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　ノード ビューで、PM カウントを表示するカードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** タブをクリックします。

ステップ 3　**15 min** オプション ボタンをクリックします。

ステップ 4　**Refresh** をクリックします。PM パラメータが、時刻に合わせて 15 分間隔で表示されます。

ステップ 5　Curr カラムを表示し、15 分間隔で表示されている現在の PM カウントを確認します。

監視対象のパフォーマンス パラメータには、現在の間隔に対するしきい値がそれぞれあります。カウンタの値が 15 分の間隔に対して定義されているしきい値を超えると、TCA が発生します。表示される数字は、各 PM パラメータのカウンタ値を表しています。

ステップ 6　Prev-*n* カラムを表示し、15 分間隔で表示された以前の PM カウントを確認します。

（注）　15 分間隔で完全にカウントすることができないと、値の背景がイエローになります。不完全なカウントや不正確なカウントの原因としては、カウンタが開始されてからまだ 15 分が経過していない、ノードのタイミング設定が変更された、時間帯の設定が変更された、カードが交換された、カードがリセットされた、ポートの状態が変更された、といったような原因が考えられます。問題が解決されると、次の間隔（15 分間）の値はホワイトの背景で表示されます。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D125 1 日間隔で行う PM カウントのリフレッシュ

目的	この作業では、ウィンドウの表示を変更して、PM パラメータを 1 日間隔で表示するようにします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　ノード ビューで、PM カウントを表示するカードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** タブをクリックします。

ステップ 3　**1 day** オプション ボタンをクリックします。

ステップ 4　**Refresh** をクリックします。PM パラメータが、時刻に合わせて 1 日間隔で表示されます。

ステップ 5　Curr カラムを表示し、1 日間隔で表示されている現在の PM カウントを確認します。

監視対象のパフォーマンス パラメータには、現在の間隔に対するしきい値がそれぞれあります。カウンタの値が 1 日間隔に対して定義されているしきい値を超えると、TCA が発生します。表示される数字は、各 PM パラメータのカウンタ値を表しています。

ステップ 6　Prev-*n* カラムを表示し、1 日間隔で表示された以前の PM カウントを確認します。

（注）　1 日間隔で完全にカウントすることができないと、値の背景がイエローになります。不完全なカウントや不正確なカウントの原因としては、カウンタが開始されてからまだ 24 時間が経過していない、ノードのタイミング設定が変更された、時間帯の設定が変更された、カードが交換された、カードがリセットされた、ポートの状態が変更された、といったような原因が考えられます。問題を解決すると、次の間隔（1 日）の値はホワイトの背景で表示されます。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D126 近端側の PM カウント表示

目的	この作業では、選択したカードおよびポートについて、近端側の PM カウントを表示します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　ノード ビューで、PM カウントを表示するカードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** タブをクリックします。

ステップ 3　**Near End** オプション ボタンをクリックします。

ステップ 4　**Refresh** をクリックします。選択したカードで着信時にカウントされたすべての PM パラメータが表示されます。PM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

ステップ 5　Curr カラムを表示して、現在の間隔の PM カウントを確認します。

ステップ 6　Prev-*n* カラムを表示して、以前の間隔の PM カウントを確認します。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D127 遠端側の PM カウント表示

目的	この作業では、選択したカードおよびポートについて、遠端側の PM カウントを表示します。遠端側を監視できるカードは、オプションの Far End オプション ボタンが実装されているカードだけです。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　ノード ビューで、PM カウントを表示するカードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** タブをクリックします。

ステップ 3　**Far End** オプション ボタンをクリックします。

ステップ 4　**Refresh** をクリックします。選択したカードの遠端ノードで発信時に記録された PM パラメータが、すべて表示されます。PM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

ステップ 5　Curr カラムを表示して、現在の間隔の PM カウントを確認します。

ステップ 6　Prev-*n* カラムを表示して、以前の間隔の PM カウントを確認します。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D129 現在の PM カウントのリセット

目的	この作業では、現在の PM カウントをクリアします。累積 PM カウントはクリアしません。この作業を行うことで、PM カウントの上昇傾向を把握することができます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　ノード ビューで、PM カウントを表示するカードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** タブをクリックします。

ステップ 3　**Baseline** をクリックします。

Baseline ボタンをクリックすると、現在の間隔に表示されている PM カウントがクリアされます。カードの PM カウントはクリアされません。現在の間隔が終了した場合や表示ウィンドウを変更した場合は、カードとそのウィンドウの PM カウントの合計が、対応するカラムに表示されます。別のウィンドウを表示してから Performance Monitoring ウィンドウに戻ると、ベースラインの値は廃棄されます。

ステップ 4　現在の統計情報カラムを表示して、現在の間隔の PM カウントが変化する様子を観察します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D131 回線の検索

目的	この作業では、ネットワーク ビュー、ノード ビュー、またはカード ビューのレベルで ONS 15454 SDH 回線を検索します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　適切な CTC ビューに移動します。

- ネットワーク全体を検索する場合 — View メニューで **Go to Network View** を選択します。
- 特定のノードを始点または終点とする回線、または特定のノードをパススルーする回線を検索する場合 — View メニューで **Go to Other Node** を選択して検索するノードを選択し、**OK** をクリックします。
- 特定のカードを始点または終点とする回線、または特定のカードをパススルーする回線を検索する場合 — シェルフの図でカードをダブルクリックし、カード ビューでカードを開きます。

ステップ 2　**Circuits** タブをクリックします。

ステップ 3　ノード ビューまたはカード ビューが表示されている場合は、Scope ドロップダウン リストで、検索の範囲を選択します（**Network** または **Node**）。

ステップ 4　**Search** をクリックします。

ステップ 5　Circuit Name Search ダイアログボックスで、次の情報を入力します。

- Find What — 検索する回線名を入力します。
- Match Whole Word Only — このチェックボックスをオンにすると、CTC では Find What フィールドに入力したテキストと単語全体が一致する回線だけが選択されます。
- Match Case — このチェックボックスをオンにすると、CTC では、大文字と小文字の区別も含めて Find What フィールドに入力したテキストと一致した回線だけが選択されます。
- Direction — 検索の方向を選択します。検索は、選択している現在の回線から上方向または下方向に行われます。

ステップ 6　**Find Next** をクリックします。一致する回線が見つからない場合は、**Find Next** をもう一度クリックして次の回線を検索します。

ステップ 7　ステップ 5 と 6 を繰り返して、見つかったら **Cancel** をクリックします。

ステップ 8　元の NTP（手順）に戻ります。

DLP-D132 MRC-12 および MRC-2.5G-12 カード上でのマルチレート PPM のプロビジョニング

目的	この作業では、MRC-12 および MRC-2.5G-12 カードの PPM をプロビジョニングします。シングルレート SFP ではプロビジョニングは不要です。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、PPM 設定をプロビジョニングする MRC-12 または MRC-2.5G-12 カードをダブルクリックします。

ステップ 2　**Provisioning > Pluggable Port Modules** タブをクリックします。

ステップ 3　Pluggable Port Modules 領域で、**Create** をクリックします。Create PPM ダイアログボックスが表示されます。

ステップ 4　Create PPM ダイアログボックスで次の情報を入力します。

- PPM — ドロップダウン リストから、SFP が搭載されたスロットの番号を選択します。
- PPM Type — ドロップダウン リストから、SFP でサポートされているポート数を選択します。サポートされているポート数が 1 の場合、使用できるのは PPM (1 port) オプションのみです。

ステップ 5　**OK** をクリックします。Pluggable Port Modules 領域に新規に作成されたポートが表示されます。Pluggable Port Modules 領域の行はライト ブルーになり、Actual Equipment Type カラムには機器の名前が表示されます。

ステップ 6　Pluggable Port Modules 領域のリストに PPM が表示されているか確認します。表示されない場合は、ステップ 4 ～ 5 を繰り返します。

ステップ 7　別の PPM をプロビジョニングする場合は、この作業を繰り返します。

ステップ 8　**OK** をクリックします。

ステップ 9　回線レートをプロビジョニングするには、「DLP-D133 MRC-12 および MRC-2.5G-12 カード上での光回線レートのプロビジョニング」（p.18-29）に進みます。

ステップ 10　元の NTP（手順）に戻ります。

DLP-D133 MRC-12 および MRC-2.5G-12 カード上での光回線レートのプロビジョニング

目的	この作業では、マルチレート PPM の光回線レートをプロビジョニングします。シングルレート SFP では回線レートのプロビジョニングは不要です。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、PPM 設定をプロビジョニングする MRC-12 または MRC-2.5G-12 カードをダブルクリックします。

ステップ 2　**Provisioning > Pluggable Port Modules** タブをクリックします。

ステップ 3　Pluggable Ports 領域で、**Create** をクリックします。Create Port ダイアログボックスが表示されます。

ステップ 4　Create Port ダイアログボックスで次の情報を入力します。

- Port — ドロップダウン リストで、PPM 番号およびポート番号をクリックします。最初の番号は PPM を、2 番めの番号は PPM のポート番号を示します。たとえば、最初の PPM は 1-1、2 番めの PPM は 2-1 と表示されます。
- Port Type — ドロップダウン リストからポートのタイプを選択します。ポート タイプ リストには、PPM でサポートされているポート レートが表示されます。MRC-12 および MRC-2.5G-12 カードでサポートされているレートの定義については、表 18-4 を参照してください。

表 18-4　PPM ポート タイプ

カード	ポート タイプ
MRC-12 MRC-2.5G-12	• STM-1 — 155 Mbps • STM-4 — 622 Mbps • STM-16 — 2.48 Gbps

ステップ 5　**OK** をクリックします。

ステップ 6　必要に応じてステップ 3 ～ 5 を繰り返して、ポート レートを設定します。

ステップ 7　**OK** をクリックします。SFP が実際に搭載されるまで Pluggable Port 領域の行はライト ブルーになります。搭載されると、ホワイトになります。

ステップ 8　元の NTP（手順）に戻ります。

DLP-D134 MRC-12 および MRC-2.5G-12 カード上での光回線レートの変更

目的	この作業では、マルチレート PPM の光回線レートを変更します。この作業は、プロビジョニングされたマルチレート SFP のポート レートを変更する場合に実行します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、PPM 設定をプロビジョニングする MRC-12 または MRC-2.5G-12 カードをダブルクリックします。

ステップ 2　**Provisioning > Pluggable Port Modules** タブをクリックします。

ステップ 3　Pluggable Ports 領域で、ポート レートを変更するポートをクリックします。強調表示がダーク ブルーに変わります。

ステップ 4　**Edit** をクリックします。Edit Port Rate ダイアログボックスが表示されます。

ステップ 5　Change To フィールドのドロップダウン リストで新しいポート レートを選択し、**OK** をクリックします。

ステップ 6　Confirm Port Rate Change ダイアログボックスで **Yes** をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D135 MRC-12、MRC-2.5G-12 または STM64-XFP カードからの PPM の削除

目的	この作業では、MRC-12、MRC-2.5G-12 または STM64-XFP カードの SFP に対する PPM のプロビジョニングを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　PPM を削除できるかどうかを判別します。

PPM のポートがインサービス状態の場合、保護グループに含まれる場合、使用中の通信チャネル終端がある場合、タイミング ソースとして使用される場合、回線が設定されている場合、またはオーバーヘッド回線が設定されている場合は、ポートを削除できません。必要に応じて、次の手順および作業を行います。

- DLP-D150 1:1 保護グループの変更（p.18-45）
- NTP-D85 ノードのタイミング変更（p.11-8）

- NTP-D277 通信チャネルの終端の変更および削除（p.11-7）
- NTP-D287 回線の変更と削除（p.7-5）
- NTP-D288 オーバーヘッド回線およびサーバ追跡の変更と削除（p.7-6）
- DLP-D214 ポートのサービス状態の変更（p.19-12）

ステップ 2　ノード ビューで、PPM 設定を削除する MRC-12、MRC-2.5G-12 または STM64-XFP カードをダブルクリックします。

ステップ 3　**Provisioning > Pluggable Port Modules** タブをクリックします。

ステップ 4　PPM および関連ポートを削除するには、次の作業を実行します。

a. Pluggable Port Modules 領域に表示された PPM 回線をクリックします。強調表示がダーク ブルーに変わります。

b. **Delete** をクリックします。Delete PPM ダイアログボックスが表示されます。

c. **Yes** をクリックします。Pluggable Port Modules 領域および Pluggable Ports 領域から PPM のプロビジョニングが削除されます。

ステップ 5　PPM のプロビジョニングが削除されたことを確認します。

- 事前プロビジョニングされていた PPM を削除すると、CTC には空のスロットが表示されます。
- PPM のプロビジョニングを削除したあとも SFP（PPM）が物理的に存在する場合、CTC は削除状態に遷移し、ポート（存在する場合）は削除され、PPM の図は CTC 内でグレー表示されます。CTC で SFP を再度プロビジョニングしたり、機器を取り外すことができます。機器を取り外した場合は、図が表示されなくなります。

ステップ 6　SFP を取り外す場合は、「DLP-D336 GBIC または SFP/XFP デバイスの取り外し」（p.20-34）を参照してください。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D136 CE-100T-8 および CE-MR-10 イーサネット ポートのプロビジョニング

目的	この作業では、トラフィックを伝送する CE-100T-8、CE-MR-10 イーサネット ポートをプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　CE-100T-8 および CE-MR-10 カードへの SONET Contiguous concatenated（CCAT）または VCAT 回線のプロビジョニングは、カードのイーサネット ポートまたは Packet-over-SDH（POS）ポートをプロビジョニングする前またはあとに実行できます。必要に応じて、「NTP-D323 自動ルーティングによる高次回線の作成」（p.6-63）または「NTP-D283 自動ルーティングによる VCAT 回線の作成」（p.6-114）を参照してください。

ステップ 1　ノード ビューで、CE-100T-8 カードまたは CE-MR-10 カードの図をダブルクリックして、カードを開きます。

ステップ 2　**Provisioning** > **Ether Ports** タブをクリックします。

ステップ 3　各 CE-100T-8 ポートまたは CE-MR-10 ポートについて、次のパラメータをプロビジョニングします。

- Port Name — ポートに名前を付ける場合は、ポート名を入力します。
- Admin State — ポートをインサービス状態にするには、**Unlocked** を選択します。
- Expected Speed — イーサネット ポートに接続されている、または今後接続するデバイスの予測速度を選択します。速度が判明している場合は、接続されたデバイスに合わせて **100 Mbps** または **10 Mbps**（CE-100T-8 用）、または **1000 Mbps**、**100 Mbps**、または **10 Mbps**（CE-MR-10 用）を選択します。速度が不明な場合に **Auto** を選択すると、ポート速度の自動ネゴシエーションがイネーブルになり、CE-100T-8 または CE-MR-10 ポートは接続先デバイスと、相互に使用可能な速度をネゴシエートしようとします。予測速度が **Auto** に設定されている場合は、選択自動ネゴシエーションをイネーブルにすることはできません。
- Expected Duplex — イーサネット ポートに接続されている、または今後接続するデバイスの予測デュプレックスを選択します。デュプレックスが判明している場合は、接続されたデバイスに合わせて **Full** または **Half** を選択します。デュプレックスが不明な場合に **Auto** を選択すると、ポート速度の自動ネゴシエーションがイネーブルになり、CE-100T-8 または CE-MR-10 ポートは接続先デバイスと、相互に使用可能なデュプレックスをネゴシエートしようとします。予測デュプレックスが **Auto** に設定されている場合は、選択自動ネゴシエーションをイネーブルにすることはできません。
- Enable Selective Auto Negotiation — イーサネット ポート上で選択自動ネゴシエーションをイネーブルにするには、このチェックボックスをオンにします。選択自動ネゴシエーションをイネーブルにしない場合は、このチェックボックスをオフにします。オンにすると、CE-100T-8 または CE-MR-10 ポートは選択済みの予測速度または予測デュプレックスにのみ自動ネゴシエートしようと試みます。自動ネゴシエーションしている接続先デバイスの予測速度と予測デュプレックスの両方がポートの速度およびデュプレックスに一致すると、リンクが確立されます。予測速度または予測デュプレックスのいずれかが **Auto** に設定されている場合は、選択自動ネゴシエーションをイネーブルにできません。
- Enable Flow Control — ポート上でフロー制御をイネーブルにするには、このチェックボックスをオンにします（デフォルト）。フロー制御をイネーブルにしない場合は、ボックスをオフにします。CE-100T-8 または CE-MR-10 カードは接続先デバイスと、対称的なフロー制御をネゴシエートしようとします。
- 802.1Q VLAN CoS — Class of Service（CoS; サービス クラス）タグ付きフレームの場合、CE-100T-8 または CE-MR-10 カードは CoS で指定された 8 つのプライオリティを優先処理またはベストエフォート処理にマッピングできます。CTC で指定されたクラスよりも上位の CoS クラスには、低遅延を実現する優先処理がマッピングされます。デフォルトでは、CoS に 7（CoS の最大値）が設定されているため、すべてのトラフィックがベストエフォート方式で処理されます。
- IP ToS — CE-100T-8 または CE-MR-10 カードは IP Type-Of-Service（ToS; タイプ オブ サービス）で指定された 256 のプライオリティを優先処理またはベストエフォート処理にマッピングすることもできます。CTC で指定されたクラスよりも上位の ToS クラスには、低遅延を実現する優先処理がマッピングされます。デフォルトでは、ToS には 255（ToS の最大値）が設定されているため、デフォルトではすべてのトラフィックがベストエフォート キューに送信されます。

（注）　タグなしトラフィックは、ベストエフォート方式で処理されます。

（注）　トラフィックに CoS と IP ToS が両方タグ付けされているときは、CoS 値が 7 の場合を除き、CoS 値が使用されます。

ステップ 4　**Apply** をクリックします。

ステップ 5　イーサネットの統計情報をリフレッシュします。

a. **Performance > Ether Ports > Statistics** タブをクリックします。

b. **Refresh** をクリックします。

（注）　CE-100T-8 または CE-MR-10 カードにイーサネット ポートを再プロビジョニングしても、そのポートでのイーサネット統計情報はリセットされません。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D137 STM-N ポートで行う J1 パス トレースのプロビジョニング

目的	この作業では、回線パス内で高次 VC4 ポートにおけるパス トレースを監視します。
工具 / 機器	監視対象の STM-N ポートが存在するカードは、パス トレースを受信できる STM-N カードである必要があります。該当するカードのリストについては、表 19-5 を参照してください。
事前準備手順	DLP-D264 回線の送信元ポートと宛先ポートにおける J1 パス トレースのプロビジョニング（p.19-77） DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　STM-N ポートで J1 パスを監視する場合は、回線のエンドポイントが VC3 J1 ではなく、VC4 J1 を送信している必要があります。

ステップ 1　View メニューから **Go to Other Node** を選択します。Select Node ダイアログボックスで、回線の送信元ポートと宛先ポートにパス トレースがプロビジョニングされているノードを選択します。

ステップ 2　**Circuits** をクリックします。

ステップ 3　送信元ポートと宛先ポートにパス トレースがプロビジョニングされている VC4 回線を選択して、**Edit** をクリックします。

ステップ 4　Edit Circuit ウィンドウで、ウィンドウの下部にある Show Detailed Map チェックボックスをオンにします。送信元ポートと宛先ポートが詳細に示されている回線の図が表示されます。

ステップ 5　詳細な回線マップで回線の STM-N ポート（送信元ノード アイコンの右または左にある四角）を右クリックし、ショートカット メニューから **Edit Path Trace** を選択します。

（注）　STM-N ポートは、表 19-5 のリストにある受信専用のカードに存在している必要があります。受信専用のカードに存在しないと、Edit Path Trace メニュー項目は表示されません。

ステップ 6　Circuit Path Trace ウィンドウで、Path Trace Mode ドロップダウン リストから、**Auto** または **Manual** を選択して、パス トレースの予測文字列をイネーブルにします。

- Auto ― 現在の予測文字列として、反対側のパス トレースのポートから受信した最初の文字列を使用します。ベースラインとは異なる文字列を受信すると、アラームが表示されます。STM-N ポートの場合は、Auto を推奨します。Manual モードにすると、Edit Circuit ウィンドウに表示されている回線を追跡して、そのポートが送信元パスまたは宛先パスのいずれであるかを判断しなければなりません。
- Manual ― ベースライン文字列として、Current Expected String フィールドの値を使用します。Current Expected String と異なる文字列を受信すると、アラームが表示されます。

（注）　予測文字列の形式（16 バイトまたは 64 バイト）は、設定しなくてもかまいません。その形式は、パス トレースのプロセスが自動的に判別してくれます。

ステップ 7　Path Trace Mode フィールドを Manual に設定した場合は、STM-N ポートが受信しなければならない文字列を New Expected String フィールドに入力します。この作業を行うには、詳細な回線ウィンドウで回線パスを追跡してポートが回線の送信元パスまたは宛先パスのいずれであるかを確認したあと、New Expected String に、回線の始点または終点から送信される文字列を設定する必要があります。Path Trace Mode フィールドを Auto に設定した場合は、このステップを省略してください。

ステップ 8　**Apply** をクリックしてから **Close** をクリックします。

ステップ 9　元の NTP（手順）に戻ります。

DLP-D140 ノード名、日付、時刻、および連絡先の変更

目的	この作業では、ノード名、日付、時刻、連絡先などの基本情報を変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　日付、時刻、または時間帯を変更すると、ノードの PM カウンタが無効になることがあります。

ステップ 1　ノード ビューで、**Provisioning > General** タブをクリックします。

ステップ 2　次のいずれかを変更します。

- General:Node Name
- General:Contact
- Location:Latitude
- Location:Longitude
- Location:Description

（注）　ネットワーク マップの経度または緯度の変更を確認する場合は、ネットワーク ビューへ進んで特定のノードを右クリックし、**Reset Node Position** をクリックします。

- Time:Use NTP/SNTP Server
- Time:Date（M/D/Y）
- Time:Time（H:M:S）
- Time:Time Zone
- Time:Use Daylight Saving Time

フィールドの詳細については、「NTP-D316 名前、日付、時刻、連絡先情報の設定」（p.4-5）を参照してください。

ステップ 3　**Apply** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D141 CE-100T-8、CE-1000-4、CE-MR-10 POS ポートのプロビジョニング

目的	この作業では、トラフィックを伝送する CE-100T-8、CE-1000-4、または CE-MR-10 の POS ポートをプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　CE-100T-8、CE-1000-4、または CE-MR-10 カードの SONET CCAT 回線または VCAT 回線は、カードの Ethernet ポートおよび POS ポートのプロビジョニングの前またはあとにプロビジョニングできます。必要に応じて、「NTP-D323 自動ルーティングによる高次回線の作成」（p.6-63）または「NTP-D283 自動ルーティングによる VCAT 回線の作成」（p.6-114）を参照してください。

ステップ 1　ノード ビューで、CE-100T-8、CE-1000-4、または CE-MR-10 カードの図をダブルクリックして、カードを開きます。

ステップ 2　**Provisioning** > **POS Ports** タブをクリックします。

ステップ 3　各 CE-100T-8、CE-1000-4、または CE-MR-10 ポートについて、次のパラメータをプロビジョニングします。

- Port Name — ポートに名前を付ける場合は、ポート名を入力します。
- Admin State — ポートをインサービス状態にするには、**Unlocked** を選択します。
- Framing Type — **GPF-F** POS フレーミング（デフォルト）または **HDLC** POS フレーミングを選択します。フレーミング タイプは SONET 回線の一端にある POS デバイスのフレーミング タイプと一致する必要があります。
- Encap CRC — GFP-F フレーミングを使用する場合、ユーザは **32-bit** Cyclic Redundancy Check（CRC; 巡回冗長検査）（デフォルト）または **none**（CRC なし）を設定できます。HDLC フレーミングの場合は、32 ビット CRC が設定されます。CRC は SONET 回線の一端にある POS デバイスの CRC と一致する必要があります。

（注） カプセル化、フレーミング、および CRC を含む ONS イーサネット カードの相互運用性の詳細については、『*Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*』の「POS on ONS Ethernet Cards」の章を参照してください。

（注） CE シリーズ カードでは、LEX カプセル化を使用します。これは、ONS イーサネット カードで主に使用される POS カプセル化です。

ステップ 4　**Apply** をクリックします。

ステップ 5　POS の統計情報をリフレッシュします。

a. **Performance > POS Ports > Statistics** タブをクリックします。
b. **Refresh** をクリックします。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D142 スタティック ルートの変更

目的	この作業では、ONS 15454 SDH のスタティック ルートを変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49） DLP-D65 スタティック ルートの作成（p.17-56）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Network** タブをクリックします。

ステップ 2　**Static Routing** タブをクリックします。

ステップ 3　変更するスタティック ルートをクリックします。

ステップ 4　**Edit** をクリックします。

ステップ 5　Edit Selected Static Route ダイアログボックスで、次の情報を入力します。

- Mask
- Next Hop
- Cost

フィールドの詳細については、「DLP-D65 スタティック ルートの作成」（p.17-56）を参照してください。

ステップ 6　**OK** をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D143 スタティック ルートの削除

目的	この作業では、ONS 15454 SDH に設定されている既存のスタティック ルートを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49） DLP-D65 スタティック ルートの作成（p.17-56）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Network** > **Static Routing** タブをクリックします。

ステップ 2　削除するスタティック ルートをクリックします。

ステップ 3　**Delete** をクリックします。確認用のダイアログボックスが表示されます。

ステップ 4　**Yes** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D144 OSPF のディセーブル化

目的	この作業では、ONS 15454 SDH LAN の Open Shortest Path First（OSPF）ルーティング プロトコル処理をディセーブルにします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注） OSPF をディセーブルにすると、TCC2/TCC2P カードが再起動されます。TCC2/TCC2P カードが再起動されている間は、一時的にノードへ接続できなくなります。しかし、トラフィックには影響しません。

ステップ 1　ノード ビューで、**Provisioning** > **Network** > **OSPF** タブをクリックします。OSPF サブタブにはいくつかのオプションがあります。

ステップ 2　OSPF on LAN 領域で、**OSPF active on LAN?** チェックボックスをオフにします。

ステップ 3　**Apply** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D145 ネットワーク ビューの背景色変更

目的	この作業では、ネットワーク ビューの背景色や、ドメイン ビューの背景色（ドメインを開いたときに表示される領域）を変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

（注） 変更した背景の色は、コンピュータの CTC ユーザ プロファイルに保存されます。変更は、他の CTC ユーザには影響しません。

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　ドメインの背景色を変更する場合は、そのドメインをダブルクリックします。それ以外の場合は、ステップ 3 へ進みます。

ステップ 3　ネットワーク ビューまたはドメイン マップ領域を右クリックして、ショートカット メニューから **Set Background Color** を選択します。

ステップ 4　Choose Color ダイアログボックスで、背景の色を選択します。

ステップ 5　**OK** をクリックします。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D146 CTC データの印刷

目的	この作業では、Windows にプロビジョニングされているプリンタを使用して、CTC カード、ノード、またはネットワーク データを図形式または表形式で印刷します。
工具 / 機器	直接接続またはネットワーク接続によって CTC コンピュータに接続されているプリンタ
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　印刷対象の情報を含むタブ（および存在する場合はサブタブ）をクリックします。たとえば、Alarms ウィンドウのデータを印刷する場合は **Alarms** タブをクリックします。

印刷はすべてのネットワーク、ノード、およびカード ビュー ウィンドウで行えます。

ステップ 2　File メニューから **Print** を選択します。

ステップ 3　Print ダイアログボックスで、印刷オプションをクリックします（図 18-9）。

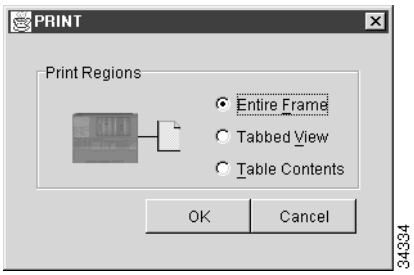
- Entire Frame — カード、ノード、またはネットワークの図も含めて、CTC ウィンドウ全体を印刷します。このオプションはすべてのウィンドウで使用可能です。
- Tabbed View — タブとデータを含む、CTC ウィンドウの下半分を印刷します。印刷結果には、選択したタブ（一番上）とタブ ウィンドウ内の表示データが出力されます。たとえば、History ウィンドウを Tabbed View で印刷すると、ウィンドウに表示されている履歴項目だけが印刷されます。このオプションはすべてのウィンドウで使用可能です。
- Table Contents — シェルフ、カード、またはタブの図を含めないで、CTC データを表形式で印刷します。このオプションは、以下のウィンドウには適用されません。
  - Provisioning > General > General Multishelf Config ウィンドウおよび Power Monitor ウィンドウ
  - Provisioning > Network > General ウィンドウ
  - Provisioning > Security > Policy ウィンドウ、Access ウィンドウ、および Legal Disclaimer ウィンドウ
  - Provisioning > SNMP ウィンドウ
  - Provisioning > Timing > General ウィンドウおよび BITS Facilities ウィンドウ
  - Provisioning > OSI > Main Setup ウィンドウ
  - Provisioning > OSI > TARP > Config ウィンドウ

- Provisioning > Cross-Connect ウィンドウ
- Provisioning > Comm Channels > LMP > General ウィンドウ
- Provisioning > WDM-ANS > Node Setup ウィンドウ
- Maintenance > Cross-Connect > Cards ウィンドウ
- Maintenance > Database ウィンドウ
- Maintenance > Diagnostic ウィンドウ
- Maintenance > Protection ウィンドウ
- Maintenance > Timing > Source ウィンドウ
- Maintenance > DWDM > ROADM Power Monitoring ウィンドウ

Table Contents オプションを選択すると、テーブルに含まれているすべてのデータとカラムの見出しが印刷されます。たとえば、History ウィンドウを Table Contents ビューで印刷すると、ウィンドウに表示されているかどうかに関わらず、テーブル内のすべてのデータが印刷されます。

ヒント　Tabbed View オプションを使用して印刷すると、出力結果がネットワーク、ノード、またはカードのどのビューのものであるのかを区別できない場合があります。どのビューであるかを判別するには、出力のタブを比較します。ネットワーク ビューに Inventory タブまたは Performance タブが含まれていないことを除けば、ネットワーク、ノード、およびカードの各ビューはまったく同じです。

図 18-9　印刷対象にする CTC データの選択



ステップ 4　**OK** をクリックします。

ステップ 5　Windows Print ダイアログボックスで、プリンタをクリックし、**OK** をクリックします。

ステップ 6　印刷するウィンドウごとに、この作業を繰り返します。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D147 CTC データのエクスポート

目的	この作業では、テキスト エディタ、ワープロ、スプレッドシート、データベース管理、または Web ブラウザの各アプリケーションでデータを表示または編集するために、CTC のテーブル データを詳細なテキストとしてエクスポートします。また、Edit Circuits ウィンドウからデータをエクスポートすることもできます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

ステップ 1　エクスポートする情報を含むタブをクリックします（Alarms タブまたは Circuits タブなど）。

ステップ 2　詳しい回線情報をエクスポートする場合は、以下を実行します。

a. Circuits ウィンドウで、回線を選択し、**Edit** をクリックします。回線の情報を示す Edit Circuits ウィンドウが表示されます。

b. Edit Circuit ウィンドウで、対象となるタブ（**Drops**、**SNCP Selectors**、**SNCP Switch Counts**、**State**、または **Merge**）を選択します。

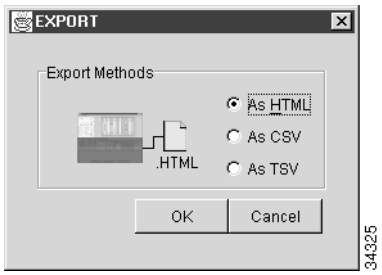
（注）　設定によっては、Edit をクリックしたときに、これらのタブの一部が表示されない場合があります。

ステップ 3　File メニューから **Export** を選択します。

ステップ 4　Export ダイアログボックスで、次のいずれかのデータ フォーマットをクリックします（図 18-10）。

- **As HTML —** 図なしの単純な HTML テーブル ファイルとしてデータを保存します。このファイルは、Netscape Navigator、Microsoft Internet Explorer、または HTML ファイルを開くことのできるその他のアプリケーションで表示および編集できます。
- **As CSV —** CTC のテーブルを CSV（コンマ区切り値）として保存します。Maintenance > Timing > Report ウィンドウには、このオプションを適用できません。
- **As TSV —** CTC のテーブルを TSV（タブ区切り値）として保存します。

図 18-10　エクスポートの対象にする CTC データの選択



ステップ 5　アプリケーションでファイルを開く場合は、使用するテキスト エディタまたはワード プロセッサごとに手順が違います。通常は、File > Open コマンドを使用して CTC データを表示するか、ファイル名をダブルクリックして「メモ帳」などのアプリケーションを選択します。

テキスト エディタとワープロ アプリケーションでは、コンマやタブ セパレータも含めて、エクスポートされた形式のままでデータを表示および編集することができます。またデータ ファイルを開くことができるアプリケーションであれば、どのアプリケーションでもデータを編集することができます。

ステップ 6　スプレッドシートまたはデータベース管理アプリケーションでファイルを開く場合は、使用するアプリケーションごとに手順が違います。通常は、アプリケーションを開いたあと、File > Import を選択してコンマ / タブ区切りのファイルを選択し、セル内のデータを編集することができます。

スプレッドシートやデータベース管理プログラムでは、エクスポートしたデータを管理することもできます。

（注）　CTC では、エクスポートしたファイルを開けません。

エクスポート操作は以下のウィンドウには適用されません。

- Provisioning > General > General Multishelf Config ウィンドウおよび Power Monitor ウィンドウ
- Provisioning > Network > General ウィンドウ
- Provisioning > Security > Policy ウィンドウ、Access ウィンドウ、および Legal Disclaimer ウィンドウ
- Provisioning > SNMP ウィンドウ
- Provisioning > Timing > General ウィンドウおよび BITS Facilities ウィンドウ
- Provisioning > OSI > Main Setup ウィンドウ
- Provisioning > OSI > TARP > Config ウィンドウ
- Provisioning > Cross-Connect ウィンドウ
- Provisioning > Comm Channels > LMP > General ウィンドウ
- Provisioning > WDM-ANS > Node Setup ウィンドウ
- Maintenance > Cross-Connect > Cards ウィンドウ
- Maintenance > Database ウィンドウ
- Maintenance > Diagnostic ウィンドウ
- Maintenance > Protection ウィンドウ
- Maintenance > Timing > Source ウィンドウ
- Maintenance > DWDM > ROADM Power Monitoring ウィンドウ

ステップ 7　**OK** をクリックします。

ステップ 8　Save ダイアログボックスの File name フィールドに、次のいずれかのフォーマットで名前を入力します。

- *Filename*.html — HTML ファイルの場合
- *Filename*.csv — CSV ファイルの場合
- *Filename*.tsv — TSV ファイルの場合

ステップ 9　ファイルの格納先ディレクトリに移動します。

ステップ 10　**OK** をクリックします。

ステップ 11　エクスポートするウィンドウごとに、この作業を繰り返します。

ステップ 12　元の NTP（手順）に戻ります。

DLP-D148 ドメイン アイコンの作成

目的	この作業では、ドメインを作成します。ドメインとは、CTC のネットワーク ビューで ONS 15454 SDH のアイコンをグループ化するためのアイコンです。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

（注）　あるユーザが作成したドメインは、ネットワークにログインするすべてのユーザから見ることができます。

（注）　スーパーユーザが CTC.network.LocalDomainCreationAndViewing NE のデフォルト値を TRUE に設定すると、すべてのセキュリティ レベルのユーザに対し、ローカル ドメイン（ホーム CTC セッションでのみ表示されるドメイン）の作成が許可されます。TRUE という値は、すべてのユーザが各自の Preference ファイルにドメイン情報を保持できるということを意味します。つまり、ドメインの変更が他の CTC セッションに影響することはありません（デフォルト値が FALSE の場合、ドメイン情報がすべての CTC セッションに影響し、スーパーユーザのみがドメインの作成またはドメインへのノードの配置を実行できることを意味します）。NE デフォルト値を変更するには、「NTP-D345 NE のデフォルト値の編集」（p.15-30）を参照してください。

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　ネットワーク マップを右クリックして、ショートカット メニューから **Create New Domain** を選択します。

ステップ 3　ドメイン アイコンがマップに表示されたら、マップ名をクリックして、ドメイン名を入力します。

ステップ 4　**Enter** キーを押します。

ステップ 5　ノードをドメインに追加する場合は、「DLP-D149 ドメイン アイコンの管理」（p.18-44）へ進みます。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D149 ドメイン アイコンの管理

目的	この作業では、CTC のネットワーク ビューにあるドメイン アイコン管理します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49） DLP-D148 ドメイン アイコンの作成（p.18-43）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　ノード　アイコンの追加や削除といったドメインの変更は、ネットワークへログインするすべてのユーザに反映されます。

（注）　スーパーユーザが CTC.network.LocalDomainCreationAndViewing NE のデフォルト値を TRUE に設定すると、すべてのセキュリティ レベルのユーザに対し、ローカル ドメイン（ホーム CTC セッションでのみ表示されるドメイン）の作成が許可されます。TRUE という値は、すべてのユーザが各自の Preference ファイルにドメイン情報を保持できるということを意味します。つまり、ドメインの変更が他の CTC セッションに影響することはありません（デフォルト値が FALSE の場合、ドメイン情報がすべての CTC セッションに影響し、スーパーユーザのみがドメインの作成またはドメインへのノードの配置を実行できることを意味します）。NE デフォルト値を変更するには、「NTP-D345 NE のデフォルト値の編集」（p.15-30）を参照してください。

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　表 18-5 の中から必要なドメインの操作を選んで、その手順を実行します。

表 18-5　ドメインの管理操作

ドメインの操作	手順
ドメインを移動する	ドメイン アイコンを別の場所にドラッグ アンド ドロップします。
ドメイン名を変更する	ドメイン アイコンを右クリックして、ショートカット メニューから **Rename Domain** を選択します。ドメイン名のフィールドに別の名前を入力します。
ドメインにノードを追加する	ノード アイコンをドメイン アイコンにドラッグ アンド ドロップします。
ノードをドメインからネットワーク マップに移動する	ドメインを開き、ノードを右クリックします。**Move Node Back to Parent View** を選択します。

表 18-5　ドメインの管理操作（続き）

ドメインの操作	手順
ドメインを開く	次のいずれかを行います。 • ドメイン アイコンをダブルクリックします。 • ドメインを右クリックし、**Open Domain** を選択します。
ネットワーク ビューに戻る	ドメイン ビューの領域を右クリックして、ショートカット メニューから **Go to Parent View** を選択します。
ドメインのコンテンツをプレビューする	ドメイン アイコンを右クリックし、**Show Domain Overview** を選択します。ドメインの中に、各ノードが小さなプレビューとなって表示されます。ドメインの概要を消す場合は、その表示を右クリックして、**Show Domain Overview** を選択します。
ドメインを削除する	ドメイン アイコンを右クリックして、**Remove Domain** を選択します。ドメインにあったノードは、ネットワーク マップに戻されます。

ステップ 3　元の NTP（手順）に戻ります。

DLP-D150 1:1 保護グループの変更

目的　この作業では、電気回路カード（E3-12、および DS3i-N-12）の 1:1 保護グループを変更します。

工具 / 機器　なし

事前準備手順　DLP-D71 1:1 保護グループの作成（p.17-63）

DLP-D60 CTC へのログイン（p.17-49）

必須 / 適宜　適宜

オンサイト / リモート　オンサイトまたはリモート

セキュリティ レベル　プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 2　Protection Groups 領域で、変更する 1:1 保護グループをクリックします。

ステップ 3　Selected Group 領域で、次の情報を必要に応じて変更します。

- Name — 保護グループの名前を変更するときは、ここにその新しい名前を入力します。保護グループの名前は、32 字までの英数字で指定できます。
- Revertive — 障害から復旧したあと、正常な状態が Reversion Time ドロップダウン リストで指定されている時間だけ続いたという条件で、トラフィックを現用カードに戻すようにする場合は、このボックスにオンにします。トラフィックを現用に戻さないようにする場合は、オフにします。
- Reversion Time — Revertive チェックボックスをオンにした場合は、この Reversion Time ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。この時間は、トラフィックが現用カードに復帰するまでの時間です。切り替えの原因になった状態が解消されると、トラフィックが復帰します。

ステップ 4　**Apply** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

（注）　1:1 保護グループを変換する場合は、「NTP-D91 DS3 i-N-12 保護カードの 1:1 保護から 1:N 保護へのアップグレード」（p.10-5）を参照してください。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D151 GNE 対応 SNMP の設定

目的	この作業では、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ネットワーク管理ソフトウェアを ONS 15454 SDH と併用できるように、SNMP パラメータをプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > SNMP** タブをクリックします。

ステップ 2　Trap Destinations 領域で、**Create** をクリックします。

ステップ 3　Create SNMP Trap Destination ダイアログボックスで、次のフィールドを設定します。

- Destination IP Address — NMS（network management system; ネットワーク管理システム）の IP アドレスを入力します。
- Community — SNMP のコミュニティ名を入力します。（SNMP の詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「SNMP」の章を参照）。

（注）　コミュニティ名は、認証とアクセス　コントロールを組み合わせた形式で指定します。ONS 15454 SDH に割り当てられたコミュニティ名は、大文字と小文字の違いも含めて、NMS のコミュニティ名と一致する必要があります。

- UDP Port — SNMP トラップのデフォルト UDP ポートは 162 です。
- Trap Version — SNMPv1 と SNMPv2 のいずれかを選択します。SNMPv1 または SNMPv2 のどちらを使用するかについては NMS のマニュアルを参照してください。

ステップ 4　**OK** をクリックします。新しいトラップ宛先をプロビジョニングしたノードのノード IP アドレスが、Trap Destinations 領域に表示されます。

ステップ 5　Trap Destinations 領域に表示されたノード IP アドレスをクリックします。Selected Destination リストに表示される SNMP 情報を確認します。

ステップ 6　SNMP エージェントで特定の MIB に関する SNMP SET 要求を処理できるようにする場合は、**Allow SNMP Sets** チェックボックスをオンにします。このチェックボックスをオフにした場合、SET 要求は拒否されます。

ステップ 7　SNMP　のプロキシ機能を設定することで、ONS　のファイアウォールを介してネットワーク管理、メッセージ レポーティング、およびパフォーマンス統計の各情報を取得できるようにする場合は、SNMP タブにある **Enable SNMP Proxy** チェックボックスをオンにします。

ステップ 8　汎用 SNMP MIB の使用を許可する場合は、**Use Generic MIB** チェックボックスをオンにします。

（注）　ONS のファイアウォール プロキシ機能は、リリース 4.6 以上が稼働するノードでのみ動作します。この情報を使用すると、ONS のファイアウォールをすり抜けて管理情報を交換できます。

SNMP プロキシ機能の詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「SNMP」の章を参照してください。

ステップ 9　**Apply** をクリックします。

ステップ 10　元の NTP（手順）に戻ります。

DLP-D152 1:N 保護グループの変更

目的	この作業では、DS3i-N-12 カードの 1:N 保護グループを変更します。
工具 / 機器	なし
事前準備手順	DLP-D72 1:N 保護グループの作成（p.17-64） DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　DS3i-N-12 カードが、「DLP-D72 1:N 保護グループの作成」（p.17-64）に記載されている 1:N の仕様に従って取り付けられていることを確認します。

ステップ 2　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 3　Protection Groups 領域で、修正する 1:N 保護グループをクリックします。

ステップ 4　Selected Group 領域で、次の情報を必要に応じて変更します。

- Name — 保護グループの名前を変更するときは、ここにその新しい名前を入力します。保護グループの名前は、32 字までの英数字で指定できます。
- Available Entities — カードが取り付けられている場合は、ここに表示されます。矢印ボタンを使用して、Working Cards カラムにカードを移動します。
- Working Entities — 矢印ボタンを使用して、Working Cards カラムからカードを移動します。

- Reversion Time — ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。この時間は、トラフィックが現用カードに復帰するまでの時間です。切り替えの原因になった状態が解消されると、トラフィックが復帰します。

フィールドの説明については、「DLP-D72 1:N 保護グループの作成」（p.17-64）を参照してください。

ステップ 5　**Apply** をクリックします。変更が適用されます。変更内容を確認し、完了していなければ作業を繰り返します。

（注）　1:1 保護グループを変換する場合は、「NTP-D91 DS3 i-N-12 保護カードの 1:1 保護から 1:N 保護へのアップグレード」（p.10-5）を参照してください。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D153 ENE 対応 SNMP の設定

目的	この作業では、GNE で SNMP プロキシを使用する場合に、ENE になるように設定された ONS 15454 SDH の SNMP パラメータをプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > SNMP** タブをクリックします。

ステップ 2　Trap Destinations 領域で、**Create** をクリックします。

ステップ 3　Create SNMP Trap Destination ダイアログボックスで、次のフィールドを設定します。

- Destination IP Address — NMS の IP アドレスを入力します。
- Community — SNMP のコミュニティ名を入力します。（SNMP の詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「SNMP」の章を参照）。

（注）　コミュニティ名は、認証とアクセス　コントロールを組み合わせた形式で指定します。ONS 15454 SDH に割り当てられたコミュニティ名は、大文字と小文字の違いも含めて、NMS のコミュニティ名と一致する必要があります。

- UDP Port — SNMP トラップのデフォルト UDP ポートは 162 です。
- Trap Version — SNMPv1 と SNMPv2 のいずれかを選択します。SNMPv1 または SNMPv2 のどちらを使用するかについては NMS のマニュアルを参照してください。

ステップ 4　**OK** をクリックします。新しいトラップ宛先をプロビジョニングしたノードのノード IP アドレスが、Trap Destinations 領域に表示されます。

ステップ 5　Trap Destinations 領域に表示されたノード IP アドレスをクリックします。Selected Destination リストに表示される SNMP 情報を確認します。

ステップ 6　SNMP エージェントで特定の MIB に関する SNMP SET 要求を処理できるようにする場合は、**Allow SNMP Sets** チェックボックスをオンにします。このチェックボックスをオフにした場合、SET 要求は拒否されます。

ステップ 7　SNMP　のプロキシ機能を設定することで、ONS　のファイアウォールを介してネットワーク管理、メッセージ レポーティング、およびパフォーマンス統計の各情報を取得できるようにする場合は、SNMP タブにある **Enable SNMP Proxy** チェックボックスをオンにします。

（注）　ONS のファイアウォール プロキシ機能は、リリース 4.6 以上が稼働するノードでのみ動作します。この情報を使用すると、ONS のファイアウォールをすり抜けて管理情報を交換できます。

SNMP プロキシ機能の詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「SNMP」の章を参照してください。

ステップ 8　**Apply** をクリックします。

ステップ 9　SNMP プロキシを設定する場合は、トラップの宛先アドレスごとに 3 つのリレーを設定して、SNMP トラップを NE から NMS に伝送することができます。次のサブステップを実行します。

a.　トラップの最初の宛先 IP アドレスをクリックします。Destination フィールドにアドレスとコミュニティ名が表示されます。

b.　ログインしているノードが ENE の場合は、Relay A のアドレスを GNE に設定し、Community フィールドにコミュニティ名を入力します。GNE と ENE の間に NE が存在する場合は、Relay B および Relay C のフィールドに、最大 2 つの SNMP プロキシ リレー アドレスおよびコミュニティ名を入力できます。その場合、次の注意事項に従ってください。

- NE が GNE に直接接続されている場合は、Relay A に GNE のアドレスおよびコミュニティ名を入力します。
- この NE がその他の NE を介して GNE に接続されている場合は、Relay A の GNE にアドレスとコミュニティ名、および Relay B に NE 1 と Relay C に NE 2 のアドレスおよびコミュニティ名を入力します。

SNMP プロキシは、SNMP トラップを一般的な順序
（ENE > RELAY A > RELAY B > RELAY C > NMS）に従って転送します。
たとえば、次のようになります。

- 中間リレーが存在しない場合、順序は ENE > RELAY A（GNE）> NMS です。
- 中間リレーが 1 つ存在する場合、順序は ENE > RELAY A（NE 1）> RELAY B（GNE）> NMS
- 中間リレーが 2 つ存在する場合、順序は ENE > RELAY A（NE 1）> RELAY B（NE 2）> RELAY C（GNE）> NMS です。

ステップ 10　**Apply** をクリックします。

ステップ 11　GNE と ENE 間のすべての NE に ステップ 2 ～ 10 を繰り返します。

ステップ 12　元の NTP（手順）に戻ります。

DLP-D154 1+1 保護グループの変更

目的	この作業では、光ポート（STM-1、STM-4、STM-16、STM-64）の 1+1 保護グループを変更します。
工具 / 機器	なし
事前準備手順	DLP-D73 1+1 保護グループの作成（p.17-65） DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 2　Protection Groups 領域で、変更する 1+1 保護グループをクリックします。

ステップ 3　Selected Group 領域で、次の情報を必要に応じて変更します。

- Name — 保護グループの名前を変更するときは、ここにその新しい名前を入力します。保護グループの名前は、32 字までの英数字で指定できます。
- Bidirectional switching — オンまたはオフにします。
- Revertive — 障害から復旧したあと、正常な状態が Reversion Time ドロップダウン リストで指定されている時間だけ続いたという条件で、トラフィックを現用カードに戻すようにする場合は、このボックスにオンにします。トラフィックを現用に戻さないようにする場合は、オフにします。
- Reversion Time — Revertive チェックボックスをオンにした場合は、この Reversion Time ドロップダウン リストから復元時間を選択します。選択できる範囲は 0.5 ～ 12.0 分です。デフォルトは 5.0 分です。この時間は、トラフィックが現用カードに復帰するまでの時間です。切り替えの原因になった状態が解消されると、トラフィックが復帰します。

フィールドの説明については、「DLP-D73 1+1 保護グループの作成」（p.17-65）を参照してください。

ステップ 4　**Apply** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D155 保護グループの削除

目的	この作業では、1:1、1:N、1+1、または Y ケーブル保護グループを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **Protection** タブをクリックします。

ステップ 2　Protection Groups 領域で、削除する保護グループをクリックします。

ステップ 3　**Delete** をクリックします。

ステップ 4　Delete Protection Group ダイアログボックスで、**Yes** をクリックして削除を行います。変更内容を確認し、完了していなければ、ステップ 1 ～ 3 を繰り返します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D157 ノードのタイミング ソース変更

目的	この作業では、ONS 15454 SDH の SDH タイミング ソースを変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　次の手順はサービスに影響するので、計画された保守時間中に作業を行ってください。

（注）　この作業で扱うフィールドの説明については、「DLP-D69 外部タイミングまたはライン タイミングの設定」（p.17-59）を参照してください。

ステップ 1　ノード ビューで、**Provisioning > Timing > General** タブをクリックします。

ステップ 2　General Timing セクションで、次の情報を変更します。

- Timing Mode

（注）　種類の違うタイミング ソースを使用すると、タイミングのループが発生することがあります。そのため、Mixed Timing オプションの使用は推奨しません。このモードを使用するときは注意してください。

- Revertive
- Reversion Time

ステップ 3　Reference Lists 領域で、次の情報を必要に応じて変更します。

（注）　基準リストでは、ノードのタイミング基準を最大 3 つまでと、BITS Out 基準を最大 6 つまで定義できます。BITS Out 基準では、ノードに MIC-C/T/P カードが実装されていて、その BITS ピンに接続されている装置がある場合に、その装置で使用するタイミング基準を定義します。装置を BITS Out ピンに接続する場合は、特別なことがないかぎり、Line モードでノードへ接続します。装置が外部タイミング基準に近ければ、そのタイミング基準に線で直接つなぐことができるからです。

- NE Reference
- BITS-1 Out
- BITS-2 Out

ステップ 4　**BITS Facilities** タブをクリックします。

ステップ 5　BITS In 領域と BITS Out 領域で、次の情報を必要に応じて変更します。

（注）　BITS Facilities セクションには、BITS-1 タイミング基準と BITS-2 タイミング基準のパラメータを設定します。これらの設定は、そのほとんどがタイミング ソースのメーカーによって決まっています。装置のタイミングを BITS Out から引き込んでいれば、その装置の要件を満たすようにタイミング パラメータを設定できます。

- Facility Type:E1、2 MHz
- BITS In State
- BITS Out State
- Coding
- Framing
- Sync Messaging
- Admin SSM
- AIS Threshold
- Sa Bit

ステップ 6　**Apply** をクリックします。

（注）　タイミングについては、『*Cisco ONS 15454 SDH Reference Manual*』にある「Timing」の章を参照してください。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D158 ユーザのパスワードとセキュリティ レベルの変更：単一ノードの場合

目的	この作業では、既存ユーザの設定を 1 つのノードだけで変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

ステップ 1　ノード ビューで、**Provisioning** > **Security** > **Users** タブをクリックします。

ステップ 2　設定を変更するユーザをクリックします。

ステップ 3　**Change** をクリックします。

ステップ 4　Change User ダイアログボックスで、次の作業を行います。

- 既存ユーザのパスワード変更
- 既存ユーザのセキュリティ レベル変更
- ユーザのロックアウト

フィールドの説明については、「NTP-D30 ユーザの作成とセキュリティの割り当て」（p.4-4）を参照してください。

ステップ 5　**OK** をクリックします。

（注）　この作業で変更したユーザ設定の内容は、ユーザがログオフして再びログインするまで有効になりません。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D159 ユーザの削除：単一ノードの場合

目的	この作業では、既存ユーザを 1 つのノードから削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

（注） ログインしているユーザを削除することはできません。ユーザをログアウトさせるには、「DLP-D315 ユーザのログアウト：単一ノード」（p.20-8）を行うか、Delete User ダイアログボックスで Logout before delete オプションを選択します。

（注） CTC では、最後のスーパーユーザを 1 人残して、他のスーパーユーザをすべて削除することができます。たとえば、スーパーユーザ CISCO15 は、それ以外のスーパーユーザを作成すれば削除することができます。このオプションを使用するときは注意してください。

ステップ 1　ノード ビューで、**Provisioning** > **Security** > **Users** タブをクリックします。

ステップ 2　削除するユーザを選択します。

ステップ 3　**Delete** をクリックします。

ステップ 4　Delete User ダイアログボックスに削除するユーザ名が表示されていることを確認します。

ステップ 5　**OK** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D160 ユーザのパスワードとセキュリティ レベルの変更：複数ノードの場合

目的	この作業では、既存ユーザの設定を複数ノードで変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

（注） ユーザのアクセスするノードが複数ある場合は、それらすべてのノードで同じユーザ名とパスワードを追加する必要があります。

ステップ 1　View メニューから **Go to Network View** を選択します。ユーザを追加するすべてのノードについて、アクセスできることを確認します。

ステップ 2　**Provisioning** > **Security** > **Users** タブをクリックします。設定を変更するユーザの名前を選択します。

ステップ 3　**Change** をクリックします。Change User ダイアログボックスが表示されます。

ステップ 4　Change User ダイアログボックスで、次の情報を入力します。

- New Password
- Confirm New Password
- セキュリティ レベル

フィールドの説明については、「DLP-D75 複数ノードでの新規ユーザの作成」（p.17-67）を参照してください。

ステップ 5　Select applicable nodes で、ユーザの設定を変更しないノードをすべてオフにします（デフォルトではすべてのノードが選択されています）。

ステップ 6　**OK** をクリックします。Change Results 確認ダイアログボックスが表示されます。

ステップ 7　**OK** をクリックして、変更を許可します。

ステップ 8　元の NTP（手順）に戻ります。

DLP-D161 ユーザの削除：複数ノードの場合

目的	この作業では、既存ユーザを複数のノードから削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

（注）　ログインしているユーザを削除することはできません。ユーザをログアウトさせるには、「DLP-D316 ユーザのログアウト：複数ノード」（p.20-9）を行うか、Delete User ダイアログボックスで Logout before delete オプションを選択します。

（注）　CTC では、最後のスーパーユーザを 1 人残して、他のスーパーユーザをすべて削除することができます。たとえば、スーパーユーザ CISCO15 は、それ以外のスーパーユーザを作成すれば削除することができます。このオプションを使用するときは注意してください。

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Provisioning** > **Security** > **Users** タブをクリックします。削除するユーザの名前を選択します。

ステップ 3　**Delete** をクリックします。Delete User ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックします。Change Results 確認ダイアログボックスが表示されます。

ステップ 5　**OK** をクリックして、変更を許可します。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D162 SNMP コマンドまたは処理用の NMS コミュニティ ストリングのフォーマット化および入力

目的	この作業では、GNE および ENE に対する SNMP コマンド（Get、GetBulk、GetNext、および Set）を実行するために NMS コミュニティ ストリングをフォーマットする方法について説明します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　GNE として設定された ONS 15454 SDH で、SNMP **Get** コマンド（またはその他の処理）がイネーブル化されている場合は、MIB ブラウザの コミュニティ名フィールドに、GNE に割り当てられたコミュニティ名を入力します。

（注）　コミュニティ名は、認証とアクセス コントロールを組み合わせた形式で指定します。NMS のコミュニティ名は、ONS 15454 SDH に割り当てられたコミュニティ名と一致する必要があります。

ステップ 2　SOCKS プロキシ対応 GNE を介して、ENE に対して SNMP **Get** コマンド（またはその他の処理）がイネーブル化されている場合は、MIB ブラウザのコミュニティ名フィールドに入力するフォーマット化文字列を作成します。ブラウザに対してこのストリングを作成する場合は、次の例を参照してください。

- フォーマット化されたコミュニティ ストリングの入力例 1：

  ```
  allviews{192.168.7.4,,,net7node4}
  ```

  プロキシ対応 SNMP エージェント（GNE）で「allviews」が有効なコミュニティ名である場合、GNE は Protocol Data Unit（PDU; プロトコル データ ユニット）を 192.168.7.4 のポート 161 に転送します。発信 PDU のコミュニティ名は「net7node4」です。ENE のアドレスが 192.168.7.4 である場合、このコミュニティ名は有効です。

- フォーマット化されたコミュニティ ストリングの入力例 2：

  ```
  allviews{192.168.7.99,,,enter7{192.168.9.6,161,,net9node6}}
  ```

  プロキシ対応 GNE で「allviews」が有効なコミュニティ名である場合、GNE は PDU を 192.168.7.99 のデフォルト ポート（ポート 161）に転送します。発信 PDU のコミュニティ名は「enter7{192.168.9.6,161,,net9node6}」です。アドレスが 192.168.7.99 のシステム（GNE と ENE 間の NE）は、この PDU を 192.168.9.6 のポート 161（ENE 上）に転送します。発信 PDU のコミュニティ名は「net9node6」です。コミュニティ名「enter7」は、GNE と ENE 間の NE で有効です。コミュニティ名「net9node6」は、ENE で有効です。

ステップ 3　ブラウザがインストールされた NMS にログインして、ONS 15454 SDH からネットワーク情報を取得します。

ステップ 4　このコンピュータで、[スタート] をクリックし、SNMP MIB ブラウザ アプリケーションをクリックします。

ステップ 5　Host 領域および Community 領域に、情報を取得する ONS 15454 SDH に到達する場合に経由する GNE の IP アドレスを入力します。

ステップ 6　Community 領域に、コミュニティ ストリングを入力します（ステップ 2 を参照）。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D163 SNMP トラップ宛先の削除

目的	この作業では、ONS 15454 SDH の SNMP トラップ宛先を削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning** > **SNMP** タブをクリックします。

ステップ 2　Trap Destinations 領域で、削除するトラップをクリックします。

ステップ 3　**Delete** をクリックします。確認用のダイアログボックスが表示されます。

ステップ 4　**Yes** をクリックします。変更内容を確認し、完了していなければ作業を繰り返します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D165 OSI ルーティング モードのプロビジョニング

目的	この作業では、OSI（Open Systems Interconnection; オープン システム インターコネクション）ルーティング モードをプロビジョニングします。この作業は、ONS 15454 SDH が接続されたネットワークに、OSI プロトコル スタックを使用して Data Communications Network（DCN; データ通信ネットワーク）通信を実行するサードパーティ製 NE が配置されている場合に実行します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

注意　ネットワーク内のノードの役割を確認するまで、この作業を実行しないでください。ノードの役割は ES、IS Level 1、または IS Level 1/Level 2 です。この役割は慎重に決定する必要があります。OSI プロビジョニングの詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「Management Network Connectivity」の章を参照してください。

注意　ネットワーク内のすべての NE で Link State Protocol（LSP）バッファを同じに設定する必要があります。そうしないと、正常に表示されなくなることがあります。LSP バッファを変更するには、OSI 内のすべての NE に同じバッファ サイズが設定されていることを確認する必要があります。

注意　LSP バッファ サイズを、OSI 領域内の LAP-D 最大伝送ユニット（maximum transmission unit; MTU）サイズよりも大きな値に設定することはできません。

（注）　ONS 15454 SDH ノードの場合、3 台の仮想ルータをプロビジョニングできます。ノードのプライマリ Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスは、ルータ 1 のプライマリ マニュアル エリア アドレスでもあります。プライマリ NSAP を編集するには、ルータ 1 のプライマリ マニュアル エリア アドレスを編集する必要があります。Routers サブタブで ルータ 1 をイネーブルにすると、アドレスを編集するための Change Primary Area Address ボタンが使用可能になります。

ステップ 1　ノード ビューで、**Provisioning** > **OSI> Main Setup** タブをクリックします。

ステップ 2　ルーティング モードを選択します。

- **End System —** ONS 15454 SDH は end system（ES; エンド システム）機能を実行し、中継システム（intermediate system; IS）を利用して OSI 領域内のノードと通信します。

（注）　イネーブル化された仮想ルータが複数存在する場合は、ES ルーティング モードを使用できません。

- **Intermediate System Level 1 —** ONS 15454 SDH は OSI IS 機能を実行して、OSI 領域内の IS ノードおよび ES ノードと通信します。OSI 領域外の IS ノードおよび ES ノードとの通信には、IS L1/L2 ノードを利用します。
- **Intermediate System Level 1/Level 2 —** ONS 15454 SDH は IS 機能を実行して、OSI 領域内の IS ノードおよび ES ノードと通信します。また、その他の OSI 領域内の IS L1/L2 ノードと通信します。このオプションを選択する前に、次の点を確認してください。
  - 別の OSI 領域内の別の IS Level 1/Level 2 ノードに、ノードを接続します。
  - 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、ノードを接続します。

ステップ 3　必要に応じて、LSP データ バッファを変更します。

- L1 LSP Buffer Size — Level 1 リンク状態の PDU バッファ サイズを調整します。デフォルト サイズは 512 です。この値は変更しないでください。
- L2 LSP Buffer Size — Level 2 リンク状態の PDU バッファ サイズを調整します。デフォルト サイズは 512 です。この値は変更しないでください。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D166 TARP 動作パラメータのプロビジョニングまたは変更

目的	この作業では、Target Identifier Address Resolution Protocol（TARP）PDU 伝播、タイマー、Loop Detection Buffer（LDB）など、TARP 動作パラメータのプロビジョニングまたは変更を行います。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

ステップ 1　ノード ビューで、**Provisioning > OSI > TARP > Config** タブをクリックします。

ステップ 2　必要に応じて、次のパラメータをプロビジョニングします。

- TARP PDUs L1 Propagation — オン（デフォルト）の場合、ノードで受信された TARP Type 1 PDU のうち、LDB で除外されないものは、Level 1 OSI 領域内のその他の NE に伝播します（Type 1 PDU は Level 1 ルーティング領域内の Target Identifier [TID; ターゲット ID] と一致するプロトコル アドレスを要求します）。NE が Type 1 PDU のターゲットである場合、伝播は発生せず、PDU は送信元の NE に伝播されません。

（注）　ES に Node Routing Area（Provisioning > OSI > Main Setup タブ）が設定されている場合、TARP PDUs L1 Propagation は使用されません。

- TARP PDUs L2 Propagation — オン（デフォルト）の場合、ノードで受信された TARP Type 2 PDU のうち、LDB で除外されないものは、Level 2 OSI 領域内のその他の NE に伝播します（Type 2 PDU は Level 2 ルーティング領域内の TID と一致するプロトコル アドレスを要求します）。NE が Type2 PDU のターゲットでない場合、伝播は発生しますが、PDU は送信元の NE に伝播しません。

（注）　TARP PDUs L2 Propagation が使用されるのは、Node Routing Area が Intermediate System Level 1/Level 2 にプロビジョニングされている場合のみです。

- TARP PDUs Origination — オン（デフォルト）の場合、ノードは以下を含む TARP 送信元機能をすべて実行します。
  - TID/NSAP 解決要求（Type 1 および Type 2 PDU を送信）
  - NSAP/TID 要求（Type 5 PDU を送信）
  - TARP アドレス変更（Type 4 PDU を送信）

（注）　TARP Echo および NSAP/TID はサポートされていません。

- TARP Data Cache — オン（デフォルト）の場合、ノードは TARP Data Cache（TDC）を維持します。TDC は、ノードに着信した TARP Type 3 PDU から作成された TID/NSAP ペアのデータベースです。TDC を変更するには、TARP Type 4 PDU を使用します（TID から NSAP へのアップデートまたは訂正）。Type 1 および Type 2 PDU には、TARP 3 PDU が応答します。TDC には、TARP > Static TDC タブで入力されたスタティック エントリを入力することもできます。

（注）　TARP Data Cache は、TARP PDUs Origination パラメータがイネーブルの場合に限り使用されます。

- L2 TARP Data Cache — オン（デフォルト）の場合、Type 2 を送信している NE の TID および NSAP が TDC に追加されてから、ノードはその他の NE に要求を伝播します。

（注）　L2 TARP Data Cache は、その他の Intermediate System Level 1/Level 2 ノードに接続された Intermediate System Level 1/Level 2 ノードに対応するように設計されています。IS Level 1 ノードに対してこのパラメータをイネーブルにすることは推奨しません。

- LDB — オン（デフォルト）の場合、TARP LDB バッファをイネーブルにします。LDB は、TARP PDU が同じサブネットに何度も送信されないようにします。

（注）　Node Routing Mode が ES にプロビジョニングされている場合、または TARP PDUs L1 Propagation パラメータがディセーブルである場合は、LDP パラメータが使用されません。

- LAN TARP Storm Suppression — オン（デフォルト）の場合、TARP ストーム抑制をイネーブルにします。この機能は、不要な冗長 TARP PDU が LAN ネットワーク内で伝播しないようにします。

- Send Type 4 PDU on Startup — オンの場合は、ONS 15454 の初期起動中に TARP Type 4 PDU が送信されます。Type 4 PDU は、NE で TID または NSAP が変更されたことを示します（デフォルト設定はディセーブルです）。
- Type 4 PDU Delay — Send Type 4 PDU on Startup がイネーブルである場合に、Type 4 PDU が生成されるまでの経過時間を設定します。デフォルトは、60 秒です。選択できる範囲は 0 ～ 255 秒です。

（注）　TARP PDUs Origination がディセーブルである場合、Send Type 4 PDU on Startup および Type 4 PDU Delay パラメータは使用されません。

- LDB Entry — TARP LDB タイマーを設定します。LDB バッファ タイマーは、TARP シーケンス番号（tar-seq）がゼロである LDB エントリにそれぞれ割り当てられます。デフォルトは 5 分です。選択できる範囲は 1 ～ 10 分です。
- LDB Flush — LDB をフラッシュする頻度を設定します。デフォルトは 5 分です。選択できる範囲は 0 ～ 1440 分です。
- T1 — Type 1 PDU への応答待機時間を設定します。Type 1 PDU は OSI Level 1 領域内で特定の NE TID を検索します。デフォルトは 15 秒です。選択できる範囲は 0 ～ 3600 秒です。
- T2 — Type 2 PDU への応答待機時間を設定します。TARP Type 2 PDU は、OSI Level 1 領域および Level 2 領域内で特定の NE TID 値を検索します。デフォルトは 25 秒です。選択できる範囲は 0 ～ 3600 秒です。
- T3 — アドレス解決要求の待機時間を設定します。デフォルトは 40 秒です。選択できる範囲は 0 ～ 3600 秒です。
- T4 — エラー回復の待機時間を設定します。要求された NE TID を検索する前に T2 タイマーが期限切れになると、このタイマーが開始します。デフォルトは 20 秒です。選択できる範囲は 0 ～ 3600 秒です。

（注）　TARP PDUs Origination のチェックボックスがオフの場合、T1、T2、および T4 タイマーは使用されません。

ステップ 3　**Apply** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D167 TARP データ キャッシュへのスタティック TID/NSAP エントリの追加

目的	この作業では、TDC にスタティック TID/NSAP エントリを追加します。スタティック エントリは、TARP をサポートしない NE に必要な、スタティック ルートと似たエントリです。TID ごとに特定の NSAP を設定する必要があります。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > OSI > TARP > Static TDC** タブをクリックします。

ステップ 2　**Add Static Entry** をクリックします。

ステップ 3　Add Static Entry ダイアログボックスで次の情報を入力します。

- TID ― NE の TID を入力します（ONS ノードの TID は、ノード ビューの Provisioning > General タブの Node Name パラメータです）。
- NSAP ― NSAP フィールドに OSI NSAP アドレスを入力します。必要に応じて、**Use Mask** をクリックして、Masked NSAP Entry ダイアログボックスにアドレスを入力することもできます。

ステップ 4　Masked NSAP Entry ダイアログボックスが使用されている場合は、**OK** をクリックして閉じてから、**OK** をクリックして、Add Static Entry ダイアログボックスを閉じます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D168 TARP データ キャッシュからのスタティック TID/NSAP エントリの削除

目的	この作業では、TDC からスタティック TID/NSAP エントリを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > OSI > TARP > Static TDC** タブをクリックします。

ステップ 2　削除するスタティック エントリをクリックします。

ステップ 3　**Delete Static Entry** をクリックします。

ステップ 4　Delete TDC Entry ダイアログボックスで、**Yes** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D169 TARP MAT エントリの追加

目的	この作業では、TARP Manual Adjacency Table（MAT）にエントリを追加します。エントリを MAT に追加するのは、ONS 15454 SDH が TARP 機能を持たないルータ間または非 SDH NE 間で通信する必要がある場合です。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > OSI > TARP > MAT** タブをクリックします。

ステップ 2　**Add** をクリックします。

ステップ 3　Add TARP Manual Adjacency Table Entry ダイアログボックスで次の情報を入力します。

- Level — 送信される TARP Type Code を設定します。
  - **Level 1** — 隣接ノードが現在のノードと同じ領域内にあることを示します。このエントリの場合、Type 1 PDU が生成されます。
  - **Level 2** — 隣接ノードが現在のノードと異なる領域内にあることを示します。このエントリの場合、Type 2 PDU が生成されます。
- NSAP — NSAP フィールドに OSI NSAP アドレスを入力します。必要に応じて、**Use Mask** をクリックして、Masked NSAP Entry ダイアログボックスにアドレスを入力することもできます。

ステップ 4　Masked NSAP Entry ダイアログボックスが使用されている場合は、**OK** をクリックして閉じてから、**OK** をクリックして、Add Static Entry ダイアログボックスを閉じます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D171 OSI ルータのプロビジョニング

目的	この作業では OSI ルータをイネーブルにして、プライマリ マニュアル エリア アドレスを編集します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　ルータ 2 および 3 のプライマリ マニュアル エリア アドレスをイネーブルにして編集する前に、ルータ 1 をイネーブルにする必要があります。

（注）　ルータ 1 のマニュアル エリア アドレス、システム ID、およびセレクタ「00」に基づいて、ノードの NSAP アドレスが作成されます。ルータ 1 のマニュアル エリア アドレスを変更すると、ノードの NSAP アドレスが変更されます。

（注）　ルータ 1 のシステム ID はノードの MAC アドレスです。ルータ 2 および 3 のシステム ID は、ルータ 1 のシステム ID にそれぞれ 1 および 2 を追加して作成されます。システム ID は編集できません。

ステップ 1　ノード ビューで、**Provisioning > OSI > Routers > Setup** タブをクリックします。

ステップ 2　プロビジョニングするルータを選択して、**Edit** をクリックします。OSI Router Editor ダイアログボックスが表示されます。

ステップ 3　OSI Router Editor ダイアログボックスで、次の手順を実行します。

a. **Enable Router** をオンにしてルータをイネーブルにし、プライマリ エリア アドレスを編集できるようにします。
b. マニュアル エリア アドレスをクリックしてから、**Edit** をクリックします。
c. Edit Manual Area Address ダイアログボックスの Area Address フィールドで、プライマリ エリア アドレスを編集します。必要に応じて **Use Mask** をクリックし、Masked NSAP Entry ダイアログボックス内でアドレスを入力します。アドレス（16 進フォーマット）には 8 ～ 24 文字の英数字（0 ～ 9、a ～ f）を使用できます。
d. 続いて **OK** をクリックして、Masked NSAP Entry（使用する場合）、Edit Manual Area Address、および OSI Router Editor ダイアログボックスを閉じます。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D172 追加のマニュアル エリア アドレスのプロビジョニング

目的	この作業では、OSI マニュアル エリア アドレスをプロビジョニングします。これらの追加マニュアル エリア は、仮想ルータごとに作成できます。
工具 / 機器	なし
事前準備手順	NTP-D24 カードの取り付けの確認（p.4-2） DLP-D171 OSI ルータのプロビジョニング（p.18-63）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　**Provisioning > OSI > Routers > Setup** タブをクリックします。

ステップ 2　追加マニュアル エリア アドレスをプロビジョニングするルータを選択して、**Edit** をクリックします。OSI Router Editor ダイアログボックスが表示されます。

ステップ 3　OSI Router Editor ダイアログボックスで、次の手順を実行します。

a. **Enable Router** をオンにしてルータをイネーブルにし、プライマリ エリア アドレスを編集できるようにします。

b. マニュアル エリア アドレスをクリックしてから、**Add** をクリックします。

c. Add Manual Area Address ダイアログボックスの Area Address フィールドに、プライマリ エリア アドレスを追加します。必要に応じて **Use Mask** をクリックし、Masked NSAP Entry ダイアログボックス内でアドレスを入力します。アドレス（16 進フォーマット）には 2 ～ 24 文字の英数字（0 ～ 9、a ～ f）を使用できます。

d. 続いて **OK** をクリックして、Masked NSAP Entry（使用する場合）、Add Manual Area Address、および OSI Router Editor ダイアログボックスを閉じます。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D173 LAN インターフェイスでの OSI サブネットのイネーブル化

目的	この作業では、LAN インターフェイスの OSI サブネットワーク ポイント オブ アタッチメントをイネーブルにします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　Data Communication Channel（DCC; データ通信チャネル）を作成すると、DCC 上で OSI サブネットワーク ポイント オブ アタッチメントがイネーブルになります。「DLP-D363 RS-DCC 終端のプロビジョニング」（p.20-67）と「DLP-D364 MS-DCC 終端のプロビジョニング」（p.20-70）を参照してください。

（注）　OSI ルーティング モードが ES に設定されている場合は、LAN インターフェイスの OSI サブネットワーク ポイント オブ アタッチメントをイネーブルにできません。

（注）　Secure Mode がオンの場合、OSI Subnet は前面 TCC2P ポートでなく、バックプレーン LAN ポートでイネーブルです。

ステップ 1　ノード ビューで、**Provisioning > OSI > Routers > Subnet** タブをクリックします。

ステップ 2　**Enable LAN Subnet** をクリックします。

ステップ 3　Enable LAN Subnet ダイアログボックスで、次のフィールドを設定します。

- ESH — End System Hello（ESH）の伝播頻度を設定します。ES の NE は ESH を伝送して、自身が処理する NSAP の情報をその他の ES および IS に通知します。デフォルトは 10 秒です。選択できる範囲は 10 ～ 1000 秒です。
- ISH — Intermediate System Hello（ISH）PDU の伝播頻度を設定します。IS NE はその他の ES および IS に ISH を送信して、自身が処理する IS NET について通知します。デフォルトは 10 秒です。選択できる範囲は 10 ～ 1000 秒です。
- IIH — Intermediate System-to-Intermediate System（IS-IS）Hello PDU の伝播頻度を設定します。IS-IS Hello PDU は、IS 間の隣接関係の確立および維持を行います。デフォルトは 3 秒です。選択できる範囲は 1 ～ 600 秒です。
- IS-IS Cost — LAN サブネットのパケット送信コストを設定します。IS-IS プロトコルはこのコストを使用して、最短のルーティング パスを計算します。LAN サブネットのデフォルト IS-IS コストは 20 です。通常、この値は変更しないでください。
- DIS Priority — Designated Intermediate System（DIS）プライオリティを設定します。IS-IS ネットワークでは、1 台のルータが DIS として機能するように選定されます（LAN サブネットのみ）。シスコ製ルータの DIS プライオリティは 64 です。ONS 15454 LAN サブネットの場合、デフォルト DIS プライオリティは 63 です。通常はこの値を変更しないでください。

ステップ 4　**OK** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D174 IP-over-CLNS トンネルの作成

目的	この作業では、IP-over-ConnectionLess Network Service（CLNS; コネクションレス型ネットワーク サービス）トンネルを作成して、OSI プロトコル スタックを使用する機器およびネットワークの間での ONS 15454 SDH ノードの通信を可能にします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　IP-over-CLNS トンネルには 2 つのエンドポイントが必要です。1 つは ONS 15454 SDH 上に作成します。もう 1 つは、通常、ルータやサードパーティ製 NE を含む非 ONS 機器上にプロビジョニングします。作業を開始する前に、その他の機器に OSI over IP トンネルを作成できることを確認してください。

ステップ 1　ノード ビューで、**Provisioning > OSI > Tunnels** タブをクリックします。

ステップ 2　**Create** をクリックします。

ステップ 3　Create IP Over OSI Tunnel ダイアログボックスで、次のフィールドを設定します。

- Tunnel Type — トンネル タイプを選択します。
  - **Cisco** — シスコ独自の IP トンネルを作成します。Cisco IP トンネルを経由する IP パケットには、CLNS ヘッダーが追加されます。
  - **GRE** — GRE トンネルを作成します。GRE トンネルを経由する IP パケットには、CLNS ヘッダーおよび GRE ヘッダーが追加されます。

  シスコ独自のトンネルでは、各 IP パケットに GRE ヘッダーが追加されないため、GRE トンネルよりも若干効率的です。2 つのトンネル タイプには互換性がありません。ほとんどのシスコ製ルータは、Cisco IP トンネルをサポートしますが、GRE トンネルと Cisco IP トンネルを両方サポートするのはそのうちの一部のみです。2 台のシスコ製ルータ間や、シスコ製ルータと ONS ノードの間でトンネリングしている場合は、通常、Cisco IP トンネルを作成する必要があります。

注意　選択した IP-over-CLNS トンネル タイプが、トンネルの反対側の機器でサポートされているか、必ず確認してください。

- IP Address — IP-over-CLNS トンネルの宛先 IP アドレスを入力します。
- IP Mask — IP-over-CLNS の宛先 IP アドレスのサブネット マスクを入力します。
- OSPF Metric — IP-over-CLNS トンネル上でパケットを送信するための OSPF メトリックを入力します。OSPF ルータは OSPF メトリック（コスト）を使用して、最短パスを計算します。デフォルトは 110 です。通常、複数のトンネル ルートを作成している場合や、複数のメトリックを割り当ててルーティングにプライオリティを設定する場合を除き、OSPF メトリックは変更しません。
- NSAP Address — 宛先 NE または OSI ルータの NSAP アドレスを入力します。

ステップ 4　**OK** をクリックします。

ステップ 5　マニュアルを参照して、その他のトンネル エンド ポイントをプロビジョニングします。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D175 TARP MAT エントリの削除

目的	この作業では、TARP MAT からエントリを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　TARP MAT がノード グループとの唯一の通信手段である場合、MAT エントリが削除されると、正常に表示されなくなります。

ステップ 1　ノード ビューで、**Provisioning > OSI > TARP > MAT** タブをクリックします。

ステップ 2　削除する MAT エントリをクリックします。

ステップ 3　**Remove** をクリックします。

ステップ 4　Delete TDC Entry ダイアログボックスで、**OK** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D178 OSI ルーティング モードの変更

目的	この作業では、OSI ルーティング モードを変更します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　ネットワーク内のノードの役割を確認するまで、この作業を実行しないでください。ノードの役割は ES、IS Level 1、または IS Level 1/Level 2 です。この役割は慎重に決定する必要があります。OSI プロビジョニングの詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「Management Network Connectivity」の章を参照してください。

注意　ネットワーク内のすべての NE で LSP バッファを同じに設定する必要があります。そうしないと、正常に表示されなくなることがあります。LSP バッファを変更するには、OSI 内のすべての NE に同じバッファ サイズが設定されていることを確認する必要があります。

注意　LSP バッファ サイズを、OSI 領域内の LAP-D MTU サイズよりも大きな値に設定することはできません。

ステップ 1　次の点を確認します。

- NE 上のすべての L1/L2 仮想ルータは、同じ領域内になければなりません。つまり、すべての近接仮想ルータには、少なくとも 1 つの共通エリア アドレスがなければなりません。
- OSI L1/L2 から ES にルーティング モードを変更する場合、設定できる L1/L2 仮想ルータおよびサブネットはそれぞれ 1 つのみです。
- OSI L1 から ES にルーティング モードを変更する場合、設定できる L1 仮想ルータおよびサブネットはそれぞれ 1 つのみです。

ステップ 2　ノード ビューで、**Provisioning** > **OSI** タブをクリックします。

ステップ 3　次のいずれかのルーティング モードを選択します。

- **End System —** ONS 15454 SDH は OSI IS 機能を実行して、OSI 領域内の IS ノードおよび ES ノードと通信します。OSI 領域外の IS ノードおよび ES ノードとの通信には、IS L1/L2 ノードを利用します。
- **Intermediate System Level 1/Level 2 —** ONS 15454 SDH は IS 機能を実行して、OSI 領域内の IS ノードおよび ES ノードと通信します。また、その他の OSI 領域内の IS L1/L2 ノードと通信します。このオプションを選択する前に、次の点を確認してください。
  - 別の OSI 領域内の別の IS Level 1/Level 2 ノードに、ノードを接続します。
  - 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、ノードを接続します。

（注）　ルーティング モードの変更は、慎重に行う必要があります。OSI ES と IS および End System to Intermediate System（ES-IS）と IS-IS プロトコルの詳細については、『*Cisco ONS 15454 SDH Reference Manual*』の「Management Network Connectivity」の章を参照してください。

ステップ 4　LSP（Link State Protocol Data Unit）バッファ サイズの変更は推奨しませんが、次のフィールドでこのバッファ を調整することができませす。

- L1 LSP Buffer Size — Level 1 リンク状態の PDU バッファ サイズを調整します。
- L2 LSP Buffer Size — Level 2 リンク状態の PDU バッファ サイズを調整します。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D179 OSI ルータ設定の編集

目的	この作業では、OSI ルータのイネーブル化とディセーブル化、プライマリ エリア アドレスの編集、追加エリア アドレスの作成や編集など、OSI ルータ設定を編集します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > OSI > Routers > Setup** タブをクリックします。

ステップ 2　プロビジョニングするルータを選択して、**Edit** をクリックします。

ステップ 3　OSI Router Editor ダイアログボックスで、次の手順を実行します。

a.　Enabled ボックスをオンまたはオフにして、ルータをイネーブルまたはディセーブルにします。

（注）　ルータ 1 をイネーブルにしてから、ルータ 2 および 3 をイネーブルにする必要があります。

b. イネーブル化されたルータで、必要に応じてプライマリ エリア アドレスを編集します。アドレスに使用できる英数字は、8 ～ 24 文字です。

c. エリア アドレスをプライマリ エリアに追加したり、編集したりするには、Multiple Area Addresses 領域の下部にアドレスを入力します。エリア アドレスに使用できる数字（0 ～ 9）は 2 ～ 26 文字です。**Add** をクリックします。

d. **OK** をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D180 OSI サブネットワーク ポイント オブ アタッチメントの編集

目的	この作業では、OSI サブネット ポイント オブ アタッチメントのパラメータを表示して、編集します。セクション DCC（SDCC）、ライン DCC（LDCC）、Generic Communications Channel（GCC）、または Optical Service Channel（OSC）を作成したり、LAN サブネットをイネーブルにした場合、パラメータの初期プロビジョニングは行われます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > OSI > Routers > Subnet** タブをクリックします。

ステップ 2　編集するサブネットを選択して、**Edit** をクリックします。

ステップ 3　Edit <*subnet type*> Subnet <*slot/port*> ダイアログボックスで、次のフィールドを編集します。

- ESH — ESH PDU の伝播頻度です。ES の NE は ESH を伝送して、自身が処理する NSAP について、その他の ES および IS に通知します。デフォルトは 10 秒です。選択できる範囲は 10 ～ 1000 秒です。
- ISH — ISH PDU の伝播頻度です。IS NE はその他の ES および IS に ISH を送信して、自身が処理する NET について通知します。デフォルトは 10 秒です。選択できる範囲は 10 ～ 1000 秒です。
- IIH — IS-IS Hello PDU の伝播頻度です。IS-IS Hello PDU は、IS 間の隣接関係の確立および維持を行います。デフォルトは 3 秒です。選択できる範囲は 1 ～ 600 秒です。

（注）　IS-IS Cost および DIS Priority パラメータは、サブネットを作成した場合、またはイネーブル化した場合に、プロビジョニングされます。サブネットの作成後は、パラメータを変更できません。DIS Priority および IS-IS Cost パラメータを変更するには、サブネットを削除して、新しいサブネットを作成します。

OK をクリックします。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D181 IP-over-CLNS トンネルの編集

目的	この作業では、IP-over-CLNS トンネルのパラメータを編集します。
工具 / 機器	なし
事前準備手順	DLP-D174 IP-over-CLNS トンネルの作成（p.18-66） DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　IP または NSAP アドレスまたは IP-over-CLNS トンネルを変更すると、NE が表示されなくなったり、NE が隔離されることがあります。ネットワーク管理者に変更内容を確認するまで、ネットワーク アドレスは変更しないでください。

ステップ 1　ノード ビューで、**Provisioning > OSI > Tunnels** タブをクリックします。

ステップ 2　**Edit** をクリックします。

ステップ 3　Edit IP Over OSI Tunnel ダイアログボックスで、次のフィールドを設定します。

- Tunnel Type — トンネル タイプを編集します。
  - **Cisco —** シスコ独自の IP トンネルを作成します。Cisco IP トンネルを経由する IP パケットには、CLNS ヘッダーが追加されます。
  - **GRE —** GRE トンネルを作成します。GRE トンネルを経由する IP パケットには、CLNS ヘッダーおよび GRE ヘッダーが追加されます。

  シスコ独自のトンネルでは、各 IP パケットに GRE ヘッダーが追加されないため、GRE トンネルよりも若干効率的です。2 つのトンネル タイプには互換性がありません。ほとんどのシスコ製ルータは、Cisco IP トンネルをサポートしますが、GRE トンネルと Cisco IP トンネルを両方サポートするのはそのうちの一部のみです。2 台のシスコ製ルータ間や、シスコ製ルータと ONS ノードの間でトンネリングしている場合は、通常、Cisco IP トンネルを作成する必要があります。

注意　選択した IP-over-CLNS トンネル タイプが、トンネルの反対側の機器でサポートされているか、必ず確認してください。

- IP Address — IP-over-CLNS トンネルの宛先 IP アドレスを入力します。
- IP Mask — IP-over-CLNS の宛先 IP アドレスのサブネット マスクを入力します。

- OSPF Metric — IP-over-CLNS トンネル上でパケットを送信するための OSPF メトリックを入力します。OSPF ルータは OSPF メトリック（コスト）を使用して、最短パスを計算します。デフォルトは 110 です。通常、複数のトンネル ルートを作成している場合や、複数のメトリックを割り当ててルーティングにプライオリティを設定する場合を除き、OSPF メトリックは変更しません。
- NSAP Address — 宛先 NE または OSI ルータの NSAP アドレスを入力します。

ステップ 4　**OK** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D182 IP-over-CLNS トンネルの削除

目的	この作業では、IP-Over-CLNS トンネルを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　IP-over-CLNS トンネルを削除すると、ノードが表示されなくなったり、ノードが隔離されることがあります。ノードが隔離された場合は、オンサイト プロビジョニングを実行して、接続を回復する必要があります。トンネルを削除する場合は、必ずネットワーク管理者に確認してください。

ステップ 1　ノード ビューで、**Provisioning > OSI > Tunnels** タブをクリックします。

ステップ 2　削除する IP-over-CLNS トンネルを選択します。

ステップ 3　**Delete** をクリックします。

ステップ 4　**OK** をクリックします。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D183 IS-IS RIB の表示

目的	この作業では、IS-IS プロトコル Routing Information Base（RIB）を表示します。IS-IS は、ネットワークの NE に関する情報をネットワークにフラッディングする OSI ルーティング プロトコルです。各 NE はこの情報を使用して、ネットワーク トポロジの完全かつ一貫性のある全体像を作成します。IS-IS RIB は、IS ノードの観点からのネットワーク ビューを示します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Maintenance > OSI > IS-IS RIB** タブをクリックします。

ステップ 2　ルータ 1 に関する次の RIB 情報を表示します。

- Subnet Type — 宛先アドレスへのアクセスに使用する OSI サブネットワーク ポイント オブ アタッチメントのタイプを示します。サブネット タイプは SDCC、LDCC、GCC、OSC、LAN などです。
- Location — OSI サブネットワーク ポイント オブ アタッチメントを示します。DCC サブネットの場合は、スロットおよびポートが表示されます。LAN サブネットは LAN として示されます。
- Destination Address — IS の宛先 NSAP です。
- MAC Address — LAN サブネットからアクセスされる宛先 NE に対応する、NE の MAC アドレスです。

ステップ 3　別のルータがイネーブルである場合は、Router フィールドでルータ番号を選択し、**Refresh** をクリックして、これらの RIB を表示できます。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D184 ES-IS RIB の表示

目的	この作業では、ES-IS プロトコル RIB を表示します。ES-IS は、ES（ホスト）と IS（ルータ）の相互学習方法を定義する OSI プロトコルです。ES の場合、ES-IS RIB は、ES ノードの観点からのネットワーク ビューを示します。IS の場合は、IS ノードの観点からのネットワーク ビューを示します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Maintenance > OSI > ES-IS RIB** タブをクリックします。

ステップ 2　ルータ 1 に関する次の RIB 情報を表示します。

- Subnet Type — 宛先アドレスへのアクセスに使用する OSI サブネットワーク ポイント オブ アタッチメントのタイプを示します。サブネット タイプは SDCC、LDCC、GCC、OSC、LAN などです。
- Location — サブネット インターフェイスを示します。DCC サブネットの場合は、スロットおよびポートが表示されます。LAN サブネットは LAN として示されます。
- Destination Address — 宛先 IS NSAP です。
- MAC Address — LAN サブネットからアクセスされる宛先 NE に対応する、NE の MAC アドレスです。

ステップ 3　別のルータがイネーブルである場合は、Router フィールドでルータ番号を選択し、**Refresh** をクリックして、これらの RIB を表示できます。

ステップ 4　元の NTP（手順）に戻ります。

DLP-D185 TDC の管理

目的	この作業では、TDC を表示して、管理します。TDC は TID/NSAP マッピング リストを格納して、TARP を処理します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Maintenance > OSI > TDC** タブをクリックします。

ステップ 2　次の TDC 情報を表示します。

- TID — 送信元 NE の TID です。ONS 15454 SDH ノードの場合、TID は Provisioning > General タブの Node Name/TID フィールドに入力された名前です。
- NSAP/NET — 送信元 NE の Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）または Network Element Title です。
- Type — TDC エントリの作成方法を示します。
  - Dynamic — TARP 伝播プロセスを介してエントリが作成されました。
  - Static — エントリが手動で作成され、スタティック エントリになっています。

ステップ 3　TID と一致する NSAP をネットワーク内で照会する場合は、次のステップを実行します。それ以外の場合は、ステップ 4 へ進みます。

（注）　Provisioning > OSI > TARP タブで TDC がイネーブルでない場合は、TID to NSAP 機能を使用できません。

a. **TID to NSAP** ボタンをクリックします。

b. TID to NSAP ダイアログボックスで、NSAP にマッピングする TID を入力します。

c. **OK** をクリックしてから、情報メッセージ ボックスで **OK** をクリックします。

d. TDC タブで **Refresh** をクリックします。

TDC 内で TID が検索された場合は、一致する NSAP が戻されます。検索されない場合、TARP はネットワークを介して PDU を送信します。あとで TDC に返信が返され、「check TDC later」メッセージが表示されます。

ステップ 4　動的に生成された TDC エントリをすべて削除する場合は、**Flush Dynamic Entries** ボタンをクリックします。それ以外の場合は、ステップ 5 へ進みます。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D186 低次 VC11 回線の始点および終点のプロビジョニング

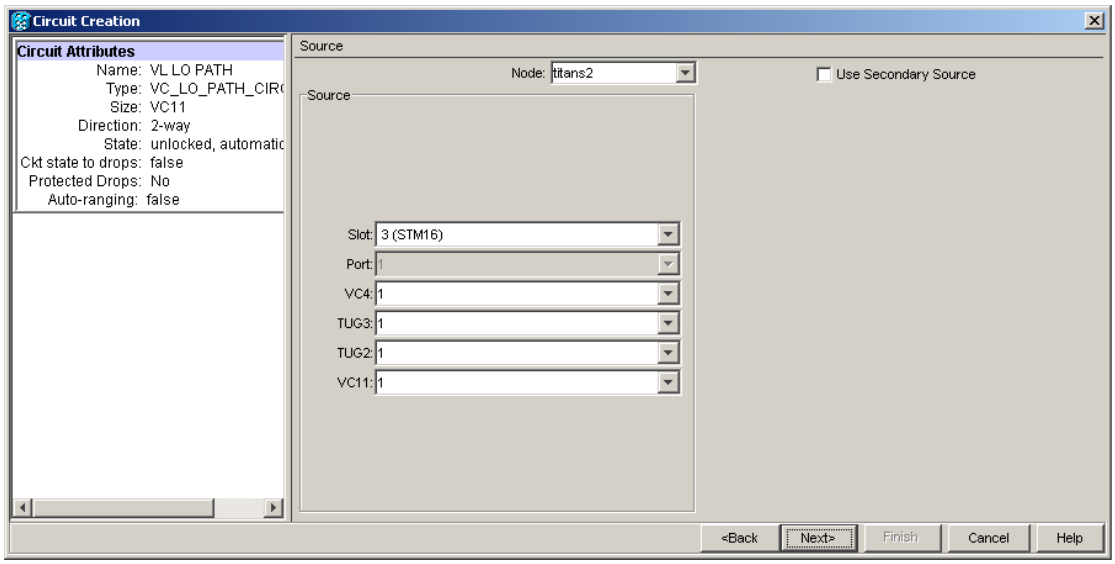
目的	この作業では、低次 VC11 回線の光回線の始点と終点をプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
	NTP-D334 自動ルーティングによる低次 VC11 回線の作成（p.6-8）、または
	NTP-D335 手動ルーティングによる低次 VC11 回線の作成（p.6-14）、または
	NTP-D336 ドロップが複数個ある単方向低次 VC11 回線の作成（p.6-18）
	Circuit Creation ウィザードの Source ページを開いておく必要があります。
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

（注）　[Circuit Source] ダイアログボックスで特定の回線作成手順に従って回線プロパティを選択すると、回線の始点をプロビジョニングする準備ができます。

ステップ 1　Node ドロップダウン リストから、始点にするノードを選択します。

ステップ 2　Slot ドロップダウン リストから、回線の始点となる STM-N、MRC-12 または MRC-2.5G-12 カードが入っているスロットを選択します（図 18-11）。STM-N カードを選択した場合は、光転送のために VC11 を VC4 にマップすることができます。

図 18-11　STM-16 カードでの回線の始点の定義



ステップ 3　Port ドロップダウン リストからポートを選択します。

ステップ 4　VC4 ドロップダウン リストから、始点 VC4 を選択します。

ステップ 5　TUG3 ドロップダウン リストから、始点 TUG3 を選択します。

ステップ 6　TUG2 ドロップダウン リストから、始点 TUG2 を選択します。

ステップ 7　VC11 ドロップダウン リストから、始点 VC11 を選択します。

ステップ 8　セカンダリ始点を作成する場合は（マルチベンダー Subnetwork Connection Protection [SNCP; サブネットワーク接続保護] リングにおける SNCP リング ブリッジまたはセレクタ回線の入り口ポイントなど）、**Use Secondary Source** をクリックし、ステップ 1 ～ 7 を繰り返してセカンダリ始点を定義します。セカンダリ始点を作成する必要がない場合は、ステップ 9 へ進みます。

ステップ 9　**Next** をクリックします。

ステップ 10　Node ドロップダウン リストから、宛先（終端）ノードを選択します。

ステップ 11　Slot ドロップダウン リストから、終点カードのあるスロットを選択します。光転送の場合は、MRC-12、MRC-2.5G-12、または STM-N カードを選択して、VC11 を VC4 にマップすることができます。

ステップ 12　ステップ 11 で選択したカードに対応して表示される宛先ポート選択用のドロップダウン リストから、終点カードに合った宛先ポートを選択します。有効なオプションのリストは、表 6-2 を参照してください。CTC では、他の回線ですでに使用されているポート（VC4、TUG3、TUG2、または VC11）は表示されません。

（注）　同じネットワークで作業しているユーザが他にもいて、同じ VC4、TUG3、TUG2、または VC11 を同時に選択していると、パス使用中（Path in Use）のエラーが表示されて、回線の設定を完了できません。回線が完全ではないユーザは、新しい宛先パラメータを選択する必要があります。

ステップ 13　セカンダリ終点を作成する場合は（マルチベンダー SNCP リングにおける SNCP リング ブリッジまたはセレクタ回線の出口ポイントなど）、**Use Secondary Destination** をクリックし、ステップ 10 ～ 12 を繰り返してセカンダリ終点を定義します。

ステップ 14　**Next** をクリックします。

ステップ 15　元の NTP（手順）に戻ります。

DLP-D187 低次 VC11 回線ルートのプロビジョニング

目的	この作業では、手動でルーティングされた低次 VC11 回線ルートをプロビジョニングします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49） NTP-D335 手動ルーティングによる低次 VC11 回線の作成（p.6-14） Circuit Creation ウィザードの Route Review and Edit ページを開いておく必要があります。
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　Circuit Creation ウィザードの Route Review and Edit 領域で、送信元ノードのアイコンをクリックします（未選択の場合）。

ステップ 2　最初に、送信元ノードにあるスパンの中から回線を通過させるスパンを選択して、その矢印をクリックします。矢印がホワイトになります。Selected Span 領域の From フィールドと To フィールドに、スパンの情報が表示されます。始点の VC11 が表示されます。

ステップ 3　始点の VC11 を変更する場合は、Source VC11 フィールドを変更します。変更しない場合は、ステップ 4 へ進みます。

ステップ 4　始点の TUG2、TUG3、VC3、または VC4 を変更する場合は、それらに対応して TUG2、TUG3、VC3、または VC4 フィールドを変更します。変更しない場合は、ステップ 5 へ進みます。

ステップ 5　**Add Span** をクリックします。Included Spans リストにスパンが追加され、スパンの矢印がブルーになります。

ステップ 6　中間ノードも含めて回線が送信元から宛先ノードまですべてプロビジョニングされるまで、ステップ 2 ～ 5 を繰り返します。Circuit Routing Preferences 領域の Fully Protect Path がオンになっている場合は、次の手順を実行します。

- すべての SNCP リング、または始点から終点までの回線ルートの保護されていない部分に対して、2 つのスパンを追加します。
- すべての MS-SPRing、または始点から終点までのルートの 1+1 部分に対して、1 つのスパンを追加します。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D188 CE シリーズ イーサネット ポートおよび POS ポートの統計情報の PM パラメータの表示

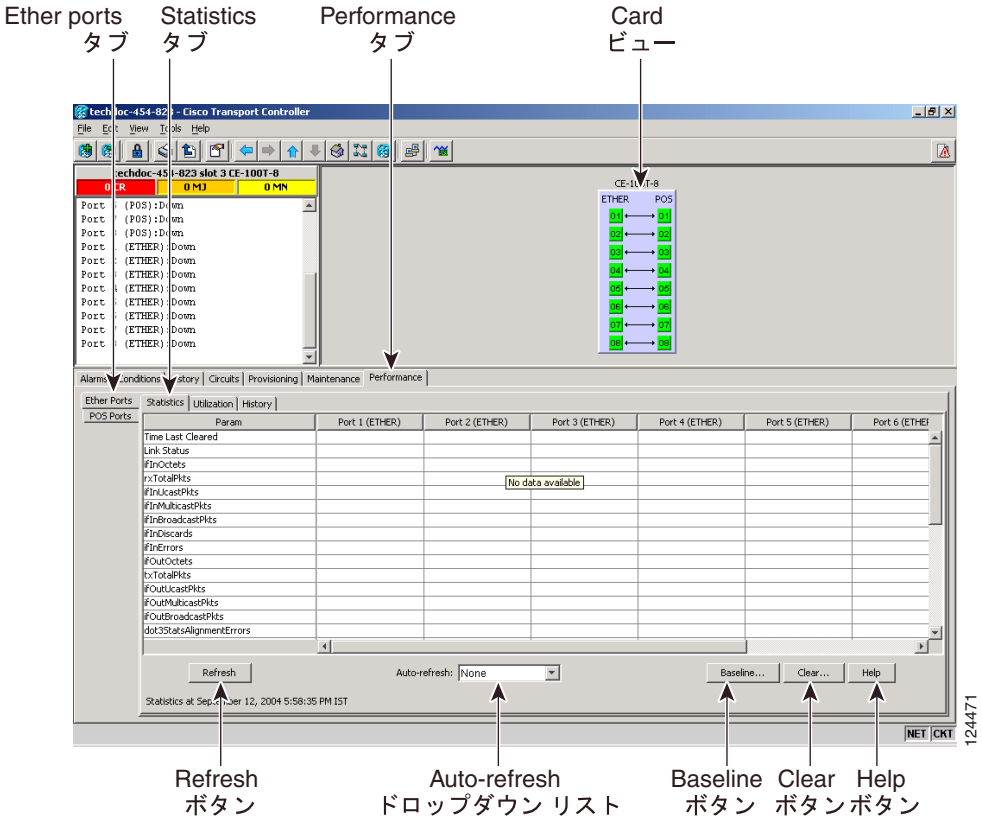
目的	この作業では、CE シリーズ カードのイーサネット ポートおよび POS ポート の統計情報の PM カウントを選択した間隔で表示します。これにより、パフォーマンスの問題を事前に検出できます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

（注）　CE シリーズ カードのプロビジョニングについては、『*Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*』を参照してください。

ステップ 1　ノード ビューで、PM カウントを表示する CE シリーズ イーサネット カードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** > **Ether Ports** > **Statistics** （図 18-12）または **Performance**> **POS Ports** > **Statistics** タブをクリックします。

図 18-12　カード ビューの Performance ウィンドウ上のイーサ ポート統計情報



ステップ 3　**Refresh** をクリックします。カード アダプタ上の各ポートについて PM の統計情報が表示されます。

ステップ 4　Param カラムを表示して、PM パラメータの名前が表示されていることを確認します。Port # カラムに PM パラメータの値が表示されます。PM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

（注）　PM カウントのリフレッシュ、リセット、またはクリアについては、「NTP-D257 PM カウントの表示変更」（p.8-2）を参照してください。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D189 1+1 現用スロットがアクティブであることの確認

目的	この作業では、1+1 保護方式の現用スロットがアクティブであること（および保護スロットがスタンバイ モードであること）を確認します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	メンテナンス以上のレベル

ステップ 1　ノード ビューで、**Maintenance > Protection** タブをクリックします。

ステップ 2　Selected Group ペインで、現用のスロットとポートが Working/Active と表示されていることを確認します。そのように表示されていれば、この作業は完了です。

ステップ 3　現用スロットのステータスが Working/Standby と表示されている場合は、次の手順に従って、現用スロットを手動で切り替えます。

a. Selected Group ペインで、ステータスが Protect/Active になっているスロットを選択します。

b. Switch Commands フィールドで、**Manual** を選択します。

c. 確認用のダイアログボックスで **Yes** をクリックします。

ステップ 4　現用スロットにトラフィックが流れていることを確認します（Working/Active）。

（注）　スロットがアクティブになっていない場合は、カードに現用トラフィックが流れない原因と考えられる状態またはアラームを探します。『*Cisco ONS 15454 SDH Troubleshooting Guide*』を参照してください。

ステップ 5　現用スロットにトラフィックが流れていたら、次の手順で手動切り替えをクリアします。

a. Switch Commands フィールドで、**Clear** を選択します。

b. 確認用のダイアログボックスで **Yes** をクリックします。

ステップ 6　現用スロットのステータスが　Standby　にスイッチバックしていないことを確認します。スイッチバックしている場合は、現用スパンで問題が発生している可能性があります。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D190 CE シリーズ イーサネット ポートおよび POS ポートの使用率の PM パラメータの表示

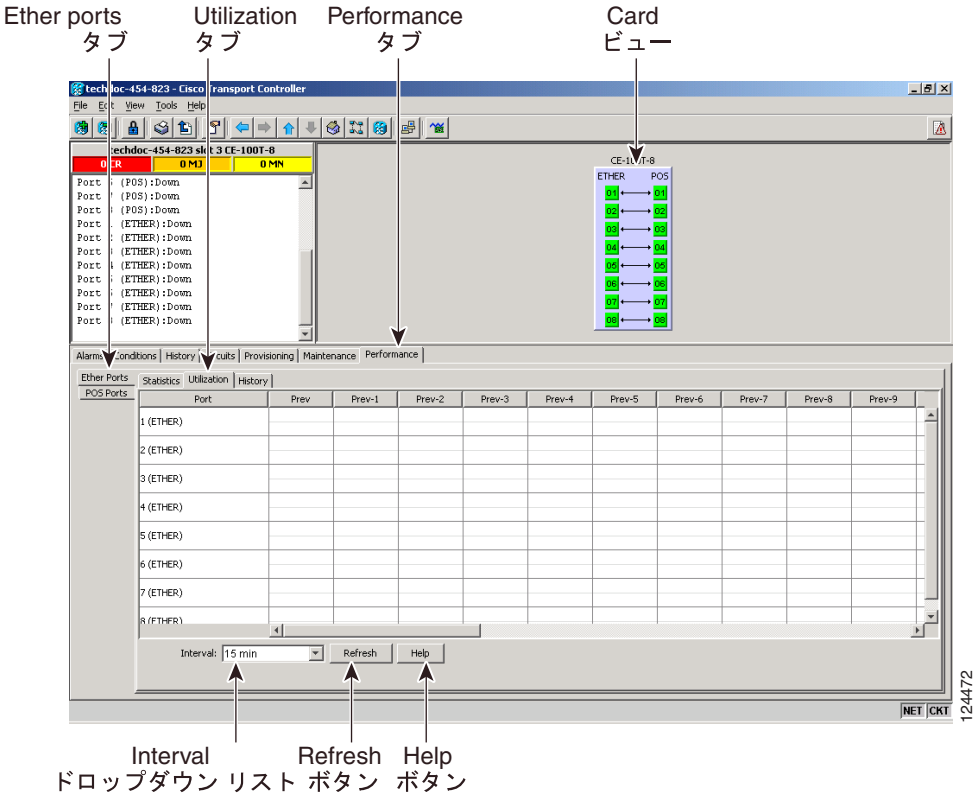
目的	この作業では、CE シリーズ カードのイーサネット ポートおよび POS ポート の使用率の PM カウントを選択した間隔で表示します。これにより、パフォーマンスの問題を事前に検出できます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

（注） CE シリーズ カードのプロビジョニングについては、『*Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*』を参照してください。

ステップ 1　ノード ビューで、PM カウントを表示する CE シリーズ イーサネット カードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance > Ether Ports > Utilization**（図 18-13）または **Performance > POS Ports > Utilization** タブをクリックします。

図 18-13　CE シリーズ カード ビューの Performance ウィンドウ上のイーサ ポート使用率



ステップ 3　**Refresh** をクリックします。カード上の各ポートについて PM の統計情報が表示されます。

ステップ 4　Param カラムを表示して、PM パラメータの名前が表示されていることを確認します。Port # カラムに PM パラメータの値が表示されます。PM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

（注）　PM カウントのリフレッシュ、リセット、またはクリアについては、「NTP-D257 PM カウントの表示変更」（p.8-2）を参照してください。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D191 カードの削除

目的	この作業では、CTC からカードを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	両方
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　シェルフの図で取り外すカードを右クリックし、**Delete Card** を選択します。

ステップ 2　次のどの状態にも該当しないこと確認します。

- カードが TCC2/TCC2P カードである。TCC2/TCC2P カードの交換については、『*Cisco ONS 15454 SDH Troubleshooting Guide*』を参照してください。
- カードが保護グループの一部になっている。「DLP-D155 保護グループの削除」（p.18-51）を参照してください。
- カードに回線がある。「DLP-D27 回線の削除」（p.17-23）を参照してください。
- カードが MS-SPRing の一部になっている。「NTP-D213 MS-SPRing ノードの削除」（p.14-8）を参照してください。
- カードがタイミングに使用されている。「DLP-D157 ノードのタイミング ソース変更」（p.18-51）を参照してください。
- カードに DCC 終端がある。「DLP-D360 RS-DCC 終端の削除」（p.20-64）または「DLP-D362 MS-DCC 終端の削除」（p.20-67）を参照してください。

（注）　CTC でカードを削除しても、そのカードをシェルフから取り外していないと、カードがリブートして再び CTC に表示されます。

ステップ 3　元の NTP（手順）に戻ります。

DLP-D192 CE シリーズ イーサネット ポートおよび POS ポートの履歴の PM パラメータの表示

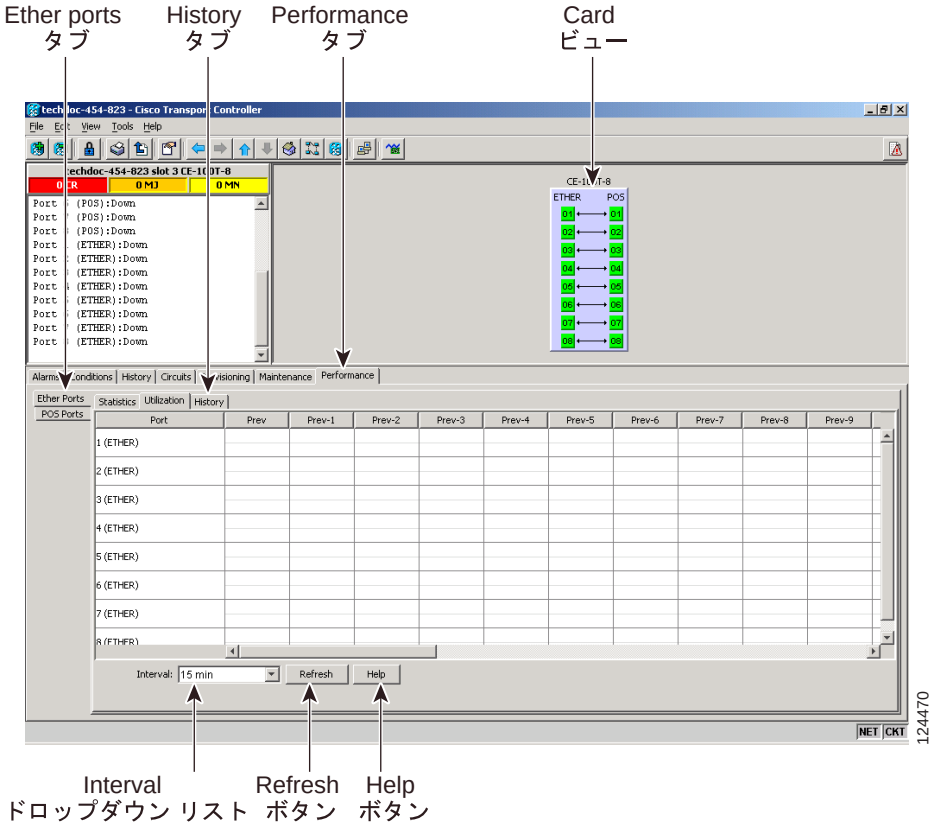
目的	この作業では、CE シリーズ カードのイーサネット ポートおよび POS ポート の履歴の PM カウントを選択した間隔で表示します。これにより、パフォーマンスの問題を事前に検出できます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

（注） CE シリーズ カードのプロビジョニングについては、『*Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*』を参照してください。

ステップ 1　ノード ビューで、PM カウントを表示する CE シリーズ イーサネット カードをダブルクリックします。カード ビューが表示されます。

ステップ 2　**Performance** > **Ether Ports** > History （図 18-14）または **Performance** > **POS Ports** > **History** タブをクリックします。

図 18-14　CE シリーズ カード ビューの Performance ウィンドウ上のイーサ ポートの履歴



ステップ 3　**Refresh** をクリックします。カード上の各ポートについて PM の統計情報が表示されます。

ステップ 4　Param カラムを表示して、PM パラメータの名前が表示されていることを確認します。Port # カラムに PM パラメータの値が表示されます。PM パラメータの定義については、『*Cisco ONS 15454 SDH Reference Manual*』の「Performance Monitoring」の章を参照してください。

（注）　PM カウントのリフレッシュ、リセット、またはクリアについては、「NTP-D257 PM カウントの表示変更」（p.8-2）を参照してください。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D193 プロビジョニング ユーザへのスーパーユーザ権限の付与

目的	この作業では、プロビジョニング ユーザが監査ログの取得、データベースの復元、およびソフトウェアのロードのアクティブ化と復帰などを実行できるようにします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	スーパーユーザのみ

ステップ 1　ノード ビューで、**Provisioning** > **Defaults** タブをクリックします。

ステップ 2　Defaults Selector 領域で **NODE > Security > grantPermission** を選択します。

ステップ 3　変更するデフォルト プロパティの Default Value カラムをクリックし、ドロップダウン リストで **Provisioning** を選択します。

（注）　**Apply** をクリックする前に **Reset** をクリックすると、すべての値が元の設定に戻ります。

ステップ 4　**Apply** をクリックします。

デフォルト値のファイルを編集したことにより、変更されるデフォルト名の隣には鉛筆型のアイコンが表示されます。

（注）　変更を有効にするには、現在の CTC セッションを閉じて、新しい CTC セッションを開始する必要があります。

ステップ 5　元の NTP（手順）に戻ります。

DLP-D194 MS-SPRing 強制リング切り替えのクリア

目的	この作業では、MS-SPRing ポートから強制切り替えを削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　View メニューから **Go to Network View** を選択します。

ステップ 2　**Provisioning > MS-SPRing** タブをクリックします。

ステップ 3　**Edit** をクリックします。

ステップ 4　ウエスト ラインの強制切り替えをクリアする場合は、次の手順を実行します。

a. 保護切り替えをクリアする MS-SPRing のウエスト ポートを右クリックして、**Set West Protection Operation** を選択します。強制切り替えが適用されているポートには、F のマークが付けられています。

b. Set West Protection Operation ダイアログ ボックスで、ドロップダウン リストから **CLEAR** を選択します。**OK** をクリックします。

c. [Confirm MS-SPRing Operation] ダイアログボックスで、**Yes** をクリックします。

ステップ 5　イースト ラインの強制切り替えをクリアする場合は、次の手順を実行します。

a. 保護切り替えをクリアする MS-SPRing のイースト ポートを右クリックして、**Set East Protection Operation** を選択します。強制切り替えが適用されているポートには、F のマークが付けられています。

b. Set East Protection Operation ダイアログ ボックスで、ドロップダウン リストから **CLEAR** を選択します。**OK** をクリックします。

c. [Confirm MS-SPRing Operation] ダイアログボックスで、**Yes** をクリックします。

MS-SPRing のネットワーク図では、各ノードがグリーンとパープルのスパン ラインで接続されているはずです。保護操作が起動されていないときの MS-SPRing の表示は、異常でないかぎり、そのようになります。

ステップ 6　File メニューから、**Close** を選択します。

ステップ 7　元の NTP（手順）に戻ります。

DLP-D195 縮小されたリングで使用されているタイミングの確認

目的	この作業では、ノードを削除したリングについて、そのタイミングを確認します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、**Provisioning > Timing > General** タブをクリックします。

ステップ 2　Timing Mode フィールドで、そのノードに設定されているタイミングの種類（Line、External、Mixed）を確認します。

ステップ 3　Reference List を NE Reference フィールドが見えるまでスクロール ダウンして、そのノードにプロビジョニングされているタイミング基準を確認します。

ステップ 4　削除したノードがただひとつの Building Integrated Timing Supply（BITS; ビル内統合タイミング供給源）タイミング ソースであった場合は、以下の手順を実行します。

a. この手順を進める前に、同期調整者または適切な担当者に連絡します。

b. リング内で BITS ソースとして使用できる別のノードを探して、そのノードの Timing Mode の値を **External** に設定します。そのノードを、リング内に存在するその他のノードのプライマリ タイミング ソースとして選択します。「DLP-D157 ノードのタイミング ソース変更」（p.18-51）を参照してください。

c. 縮小されたリング内に BITS ソースとして使用できるノードがない場合は、1 つのノードを内部タイミング ソースとして選択します。そのノードの Timing Mode を **External** に設定したあと、BITS-1 と BITS-2 の BITS In State を **OOS** に設定するとともに、NE Reference を **Internal** に設定します。続いて、リング内に存在するその他のノードの回線タイミングをすべて選択します。そうすることで、最初のノードを他のノードのプライマリ タイミング ソースにできます（「DLP-D157 ノードのタイミング ソース変更」[p.18-51] を参照）。

（注）　この種類のタイミングは SETS の要件に準拠していますが、最適とは考えられません。

ステップ 5　削除したノードがただひとつの BITS タイミング ソースではない場合は、隣接ノードのタイミング ソースとして、SDH リンク（イーストとウエスト）を使用したライン タイミングをプロビジョニングします。隣接ノードのタイミングは、このプロビジョニングによって、外部 BITS タイミングまでたどりつくことができます。「NTP-D28 タイミングの設定」（p.4-11）を参照してください。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D196 単一ノードからの MS-SPRing の削除

目的	この作業では、MS-SPRing からノードを切り離したあと、そのノードから MS-SPRing を削除します。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューで、MS-SPRing から削除したノードを表示します。

- 削除したノードが使用コンピュータと同じ LAN に接続されている場合は、File メニューで **Add Node** を選択してから、そのノードの名前または IP アドレスを入力します。
- 削除したノードが使用コンピュータと同じ LAN に接続されていない場合は、そのノードに直接接続する必要があります。手順については、第 3 章「PC の接続と GUI へのログイン」を参照してください。

ステップ 2　ノード ビューで、**Provisioning > MS-SPRing** タブをクリックします。

ステップ 3　リングを選択して **Delete** をクリックします。

ステップ 4　Suggestion ダイアログボックスで **OK** をクリックします。

ステップ 5　確認メッセージを読んで、これが削除対象のリングであることを確認します。そうであれば、**Yes** をクリックします。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D197 SNCP の強制切り替え開始

目的	この作業では、SNCP スパン上のすべての回線を切り替えます。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

注意　Force Switch Away コマンドは、通常の保護切り替えメカニズムより優先します。このコマンドを誤って適用すると、トラフィックが停止する可能性があります。

ステップ 1　ノード ビューの View メニューから、**Go to Network View** を選択します。

ステップ 2　SNCP トラフィックを切り替えるスパンを右クリックします。ショートカット メニューで **Circuits** を選択します。

ステップ 3　Circuits on Span ダイアログボックスで、**FORCE SWITCH AWAY** を選択します。**Apply** をクリックします。

ステップ 4　[Confirm SNCP Switch] ダイアログ ボックスで、**Yes** をクリックします。

ステップ 5　[Protection Switch Result] ダイアログ ボックスで **OK** をクリックします。

Circuits on Span ウィンドウにあるすべての回線の Switch State 値が FORCE になります。

（注）　スパンまたはカードに対して強制切り替え要求を出すと、CTC で FORCED-REQ 状態が発生します。強制切り替えをクリアすると、この状態もクリアされます。この状態は、単なる参考情報です。

ステップ 6　元の NTP（手順）に戻ります。

DLP-D198 SNCP の強制切り替えのクリア

目的	この作業では、SNCP の強制切り替えをクリアします。
工具 / 機器	なし
事前準備手順	DLP-D60 CTC へのログイン（p.17-49）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

ステップ 1　ノード ビューの View メニューから、**Go to Network View** を選択します。

ステップ 2　切り替えをクリアするスパンを右クリックします。ショートカット メニューで **Circuits** を選択します。

ステップ 3　Circuits on Span ダイアログボックスで **CLEAR** を選択して、強制切り替えを削除します。**Apply** をクリックします。

ステップ 4　[Confirm SNCP Switch] ダイアログ ボックスで、**Yes** をクリックします。

ステップ 5　[Protection Switch Result] ダイアログ ボックスで **OK** をクリックします。

Circuits on Span ウィンドウで、すべての SNCP 回線の Switch State が CLEAR になります。

ステップ 6　元の NTP（手順）に戻ります。