CHAPTER 22

DLP A500 ～ A599

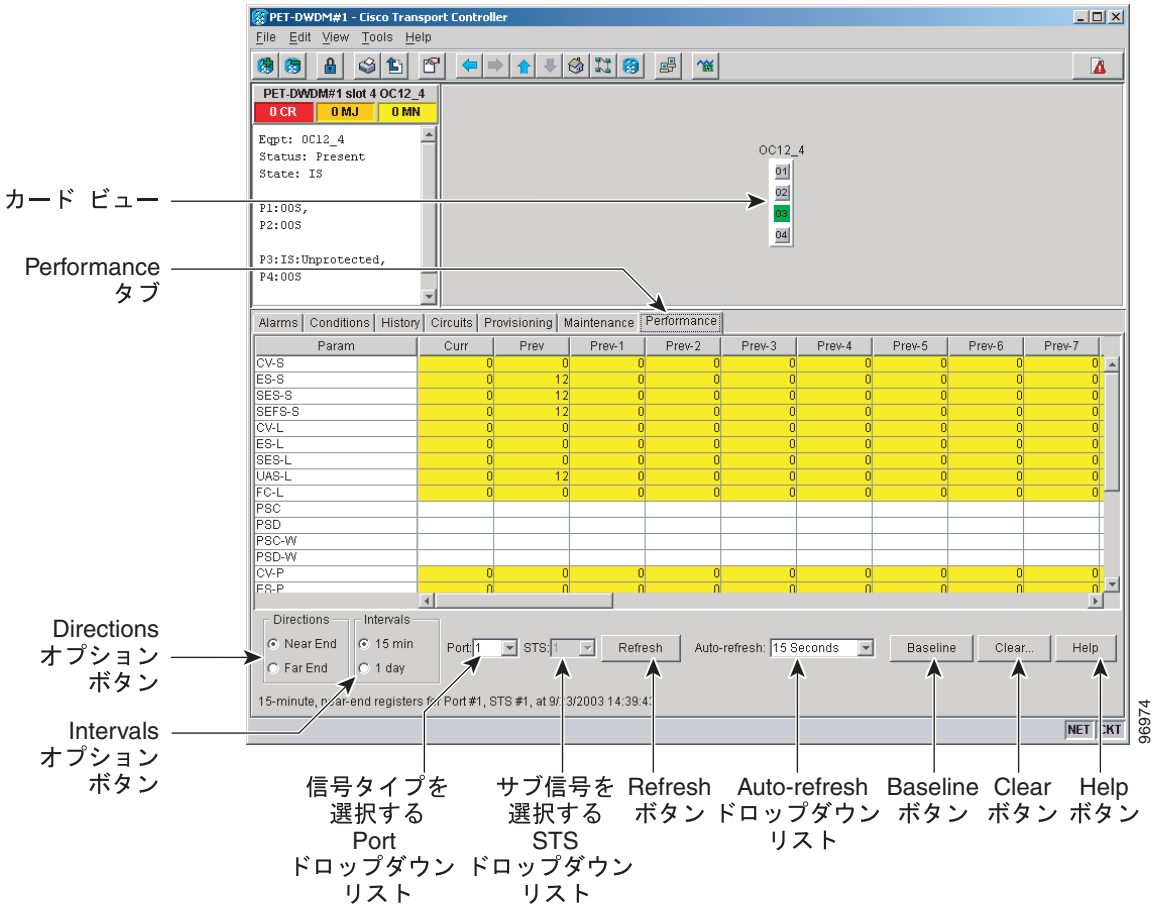
DLP-A507 OC-N PM パラメータの表示

目的	この作業では、OC-N カードおよびポートの Performance Monitoring（PM; パフォーマンス モニタリング）カウントを表示して、パフォーマンスの問題を事前に検出します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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 OC-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。

ステップ 2 **Performance** タブをクリックします（図 22-1）。

図 22-1　OC-N カードの PM 情報の表示



ステップ 3　Port ドロップダウン リストで、モニタするポートをクリックします。

ステップ 4　**Refresh** をクリックします。

ステップ 5　Param カラムに、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。PM パラメータの値は、Curr（現在）および Prev-*n*（過去）の各カラムに表示されます。PM パラメータの定義については、『*Cisco ONS 15454 Reference Manual*』の「Performance Monitoring」の章を参照してください。

ステップ 6　マルチポート カードで別のポートをモニタする場合は、Port ドロップダウン リストで別のポートを選択して、**Refresh** をクリックします。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A509 CE-1000-4 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-1000-4 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-A60 CTC へのログイン（p.17-71）
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-1000-4 カードへの SONET Contiguous Concatenated（CCAT）または Virtual Concatenated（VCAT; 仮想連結）回線のプロビジョニングは、カードのイーサネット ポートと Packet-over-SONET（POS）ポート（またはどちらか一方）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-A343 自動ルーティングによる光回線の作成」（p.6-47）または「NTP-A264 自動ルーティングによる VCAT 回線の作成」（p.6-99）を参照してください。

ステップ 1　ノード ビューで、CE-1000-4 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-1000-4 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 — ポートにラベルを付ける場合は、ポート名を入力します。
- Admin State — ポートのサービス状態を選択します。詳細については、「DLP-A214 ポートのサービス状態の変更」（p.19-10）を参照してください。
- Flow Control — ポートのフロー制御を選択します。値は、**None**、**Symmetrical**、および **Pass Through** のいずれかです。
- Auto Negotiation — ポート上で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（デフォルト）。自動ネゴシエーション制御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。
- MTU — ジャンボ サイズのイーサネット フレームの受け入れを許可する場合、10004（デフォルト）を選択します。ジャンボ サイズのイーサネット フレームの受け入れを許可しない場合は、1548 を選択します。
- Watermark — ポートのフロー制御水準点を選択します。フロー制御水準点の低遅延をプロビジョニングする場合は、ドロップダウン リストから **Low Latency** を選択します。Flow Ctrl Lo の値と Flow Ctrl Hi の値が変更されます。カスタム フロー制御水準点をプロビジョニングする場合は、ドロップダウン リストから **Custom** を選択します。Flow Ctrl Hi カラムおよび Flow Ctrl Lo カラムに値を入力します。Flow Ctrl Lo の値の有効範囲は 1 ～ 510 で、Flow Ctrl Hi の値の有効範囲は 2 ～ 511 です。Flow Ctrl Lo の値は、Flow Ctrl Hi の値より低く設定する必要があります。

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-1000-4 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-A510 DS-3 回線の送信元と宛先のプロビジョニング

目的	この作業では、DS-3 回線の電気回線の送信元と宛先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-A60 CTC へのログイン（p.17-71）
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、回線の送信元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、送信元とな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、回線の送信元になる DS-3 カードが取り付けられているスロットを選択します。DS-3 回線を Transmux カードで設定する場合、DS3XM-6 または DS3XM-12 カードを選択します。

ステップ 3　Port ドロップダウン リストから、適切な送信元 DS-3、DS3/EC1-48、DS3XM-6、または DS3XM-12 カードを選択します。

ステップ 4　セカンダリ送信元を作成する場合は（マルチベンダー Unidirectional Path Switched Ring［UPSR; 単方向パス スイッチ型リング］における UPSR ブリッジまたはセレクタ回線の入口ポイントなど）、**Use Secondary Source** をクリックし、ステップ 1 ～ 3 を繰り返してセカンダリ送信元を定義します。セカンダリ送信元を作成する必要がない場合は、ステップ 5 へ進みます。

ステップ 5　**Next** をクリックします。

ステップ 6　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 7　Slot ドロップダウン リストから、宛先カードのあるスロットを選択します。宛先は、通常、DS3XM-6 または DS-3 カードになります。OC-N カードを選択して、DS-3 回線を同期転送信号（STS）にマップすることもできます。

ステップ 8　ステップ 2 で選択したカードに対応して表示されるドロップダウン リストから、宛先カードに合った宛先ポートまたは STS を選択します。有効なオプションのリストは、表 6-2（p.6-3）を参照してください。Cisco Transport Controller（CTC）は、他の回線によってすでに使用されているポート、STS、Virtual Tributary（VT）、または DS3 を表示しません。同じネットワークで作業している 2 人のユーザが、同じポート、STS、VT、ポート、または DS3 を同時に選択した場合は、一方のユーザに [Path in Use] のエラーが表示され、回線を完成させることができません。回線が PARTIAL になった方のユーザは、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 9　セカンダリ宛先を作成する場合は（マルチベンダー UPSR における UPSR 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 6 ～ 8 を繰り返してセカンダリ宛先を定義します。

ステップ 10　**Next** をクリックします。

ステップ 11　元の NTP（手順）に戻ります。

DLP-A512 ノード アクセスと PM クリア権限の変更

目的	この作業では、ONS 15454 を接続するための物理的なアクセス ポイントとシェル プログラムをプロビジョニングして、ノード の PM データをクリアできるユーザのセキュリティ レベルを設定します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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

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

ステップ 2　Access 領域で、次の項目をプロビジョニングします。

- LAN access — 次のいずれかのオプションを選択して、ノードへのアクセス パスを設定します。
  - **No LAN Access** — Data Communication Channel（DCC; データ通信チャネル）接続を介したアクセスだけを許可します。TCC2/TCC2P RJ-45 ポートおよびバックプレーンを介したアクセスは許可されません。
  - **Front only** — TCC2/TCC2P RJ-45 ポートを介したアクセスを許可します。DCC およびバックプレーンを介したアクセスは許可されません。
  - **Backplane only** — DCC 接続およびバックプレーンを介したアクセスを許可します。TCC2/TCC2P RJ-45 ポートを介したアクセスは許可されません。
  - **Front and Backplane** — DCC、TCC2/TCC2P RJ-45、およびバックプレーン接続を介したアクセスを許可します。
- Restore Timeout — LAN Access フィールドで [DCC only] が選択されている場合に、DCC 接続が中断してから、フロントおよびバックプレーン アクセスをイネーブルにするまでの遅延時間を設定します。フロントおよびバックプレーン アクセスは、復元タイムアウト時間が経過したあとでイネーブルになります。フロントおよびバックプレーン アクセスは、DCC 接続が復元するとただちにディセーブルになります。

ステップ 3　Shell Access 領域で、ノードのアクセスに使用するシェル プログラムを設定します。

- Access State — シェル プログラム アクセス モードを Disable（シェル アクセスをディセーブル化）、Non-Secure、Secure に設定できます。Secure モードの場合は、Secure Shell（SSH; セキュア シェル）プログラムを使用してノードへアクセスできます。SSH は端末とリモート ホストとの間のインターネット プロトコルで、暗号化リンクを使用します。
- Telnet Port — Telnet ポートを使用してノードへアクセスできます。Telnet は端末とリモート ホストとの間のインターネット プロトコルで、Advanced Agency Research Project Network（ARPANET）のために開発されました。ポート 23 がデフォルトです。
- Enable Shell Password — オンになっている場合、SSH パスワードをイネーブルにします。パスワードをディセーブルにするには、このチェックボックスをオフにして、Apply をクリックする必要があります。確認ダイアログボックスにパスワードを入力し、OK をクリックして、ディセーブルにしてください。

ステップ 4　TL1 Access 領域で、目的の TL1 アクセス レベルを選択します。ディセーブルにすると、すべての TL1 アクセスが完全にディセーブルになります。Non-Secure または Secure を選択した場合は、SSH によるアクセスが可能です。

ステップ 5　PM Clearing Privilege フィールドで、ノードの PM データをクリアできる最小のセキュリティ レベルを選択します（プロビジョニングまたはスーパーユーザ）。

ステップ 6　Enable Craft Port チェックボックスを選択して、シェルフ コントローラのシリアル ポートをオンにします。

ステップ 7　リストから EMS アクセス状態を選択します。Non-Secure および Secure（SSH によるアクセスを許可）から選択できます。

TCC CORBA (IIOP/SSLIOP) Listener Port 領域で、次のリスナー ポート オプションを選択します。

- **TCC Fixed**（デフォルト）— Port 57790 を使用します。ファイアウォールの同じ側にある ONS 15454 に接続する場合、またはファイアウォールを使用しない場合（デフォルト）に適したオプションです。Port 57790 が開いている場合は、ファイアウォールを介したアクセスにこのオプションを使用することもできます。
- **Standard Constant** — Port 683（Internet Inter-ORB Protocol [IIOP]）または Port 684（SSLIOP）を使用します。Common Object Request Broker Architecture（CORBA）のデフォルト ポート番号です。
- **Other Constant** — デフォルト ポートを使用しない場合は、ファイアウォール管理者が指定する IIOP または SSLIOP ポートを入力します。

ステップ 8　SNMP Access 領域で、SNMP（簡易ネットワーク管理プロトコル）アクセス状態を Non-Secure または Disabled（SNMP アクセスをディセーブル化）に設定します。

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-A513 CE-100T-8 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 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-A60 CTC へのログイン（p.17-71）
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 カードへの SONET 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 ポートと POS ポート（またはどちらか一方）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-A343 自動ルーティングによる光回線の作成」（p.6-47）または「NTP-A264 自動ルーティングによる VCAT 回線の作成」（p.6-99）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 — ポートにラベルを付ける場合は、ポート名を入力します。
- Admin State — ポートを稼働状態にするには、**IS** 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** 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 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。
- 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、ポートのデュプレックスの自動ネゴシエーションがイネーブルになり、CE-100T-8 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。
- 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 は接続先デバイスと対称型の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 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 は IP Type-Of-Service（ToS; サービス タイプ）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、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　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-A514 CE-100T-8 および CE-1000-4 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 または CE-1000-4 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-A60 CTC へのログイン（p.17-71）
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 または CE-1000-4 カードへの SONET 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 ポートと POS ポート（またはどちらか一方）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-A343 自動ルーティングによる光回線の作成」（p.6-47）または「NTP-A264 自動ルーティングによる VCAT 回線の作成」（p.6-99）を参照してください。

ステップ 1　ノード ビューで、CE-100T-8 または CE-1000-4 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 または CE-1000-4 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 — ポートにラベルを付ける場合は、ポート名を入力します。
- Admin State — ポートを稼働状態にするには、**IS** 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、CRC など、Optical Networking System（ONS）イーサネット カードのインターオペラビリティの詳細については、『*Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*』の「POS on ONS Ethernet Cards」の章を参照してください。

（注） CE-100T-8 および CE-1000-4 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-A517 アラーム履歴またはイベント履歴の表示

目的	この作業は、カード、ノード、またはネットワーク レベルで、クリア済みまたはクリアされていない ONS 15454 アラーム メッセージを表示するのに使用します。この作業は、アラームで示されている、設定、トラフィック、または接続の問題をトラブルシューティングするときに役立ちます。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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、ネットワーク、またはカードのどのレベルでアラーム メッセージの履歴を表示するかを決定します。

ステップ 2　ノードのアラーム履歴を表示する場合は、次の手順を実行します。

a. 現在のセッション中に発生したアラームおよび状態（イベント）を表示する場合は、**History > Session** タブをクリックします。

b. **History > Shelf** タブをクリックします。

Alarms チェックボックスをオンにすると、ノードのアラーム履歴が表示されます。**Events** チェックボックスをオンにすると、ノードの Not Alarmed および一時的なイベントの履歴が表示されます。両方のチェックボックスをオンにすると、ノードのアラームとイベントの両方の履歴が表示されます。

c. History > Shelf タブのすべてのメッセージを表示する場合は、**Retrieve** をクリックします。

（注）　アラームは、いずれかのタブにある Filter ボタンを使用して表示の対象外にすると、報告されなくなります。詳細については、「DLP-A225 アラーム フィルタリングのイネーブル化」（p.19-20）を参照してください。

ヒント　アラーム メッセージに対応したビューを表示する場合は、アラーム テーブル内のアラームまたは履歴テーブル内のイベント（状態）メッセージをダブルクリックします。たとえば、カード アラームをダブルクリックすると、カード ビューが表示されます。ネットワーク ビューでノード アラームをダブルクリックすると、ノード ビューが表示されます。

ステップ 3　ネットワークのアラーム履歴を表示する場合は、ノード ビューで次の手順を実行します。

a. View メニューで、**Go to Network View** を選択します。

b. **History** タブをクリックします。

現在のセッション中に発生したアラームおよび状態（イベント）が表示されます。

ステップ 4　ノード ビューからカードのアラーム履歴を表示する場合は、次の手順を実行します。

a. View メニューから **Go to Previous View** を選択します。

b. シェルフ図でカードをダブルクリックし、カードレベルのビューを開きます。

（注）　TCC2/TCCP カードとクロスコネクト（XCVT、XC10G、または XC-VXL-10G）カードには、カード ビューがありません。

c. 現在のセッション中に発生したアラーム メッセージを表示する場合は、**History > Session** タブをクリックします。

d. カードのすべてのアラーム メッセージを検索する場合は、**History > Card** タブをクリックし、**Retrieve** をクリックします。

Alarms チェックボックスをオンにすると、ノードのアラーム履歴が表示されます。**Events** チェックボックスをオンにすると、ノードの Not Alarmed および一時的なイベントの履歴が表示されます。両方のチェックボックスをオンにすると、ノードのアラームとイベントの両方の履歴が表示されます。

（注） ONS 15454 は、640 件までの Critical アラーム メッセージ、640 件までの Major アラーム メッセージ、640 件までの Minor アラーム メッセージ、および 640 件までの状態メッセージを格納できます。これらのいずれかの上限値に達すると、ONS 15454 はそのカテゴリの中で最も古いイベントを廃棄します。

生成およびクリアされたアラーム メッセージ（および選択した場合はイベント）が表示されます。

ステップ 5　元の手順（NTP）に戻ります。

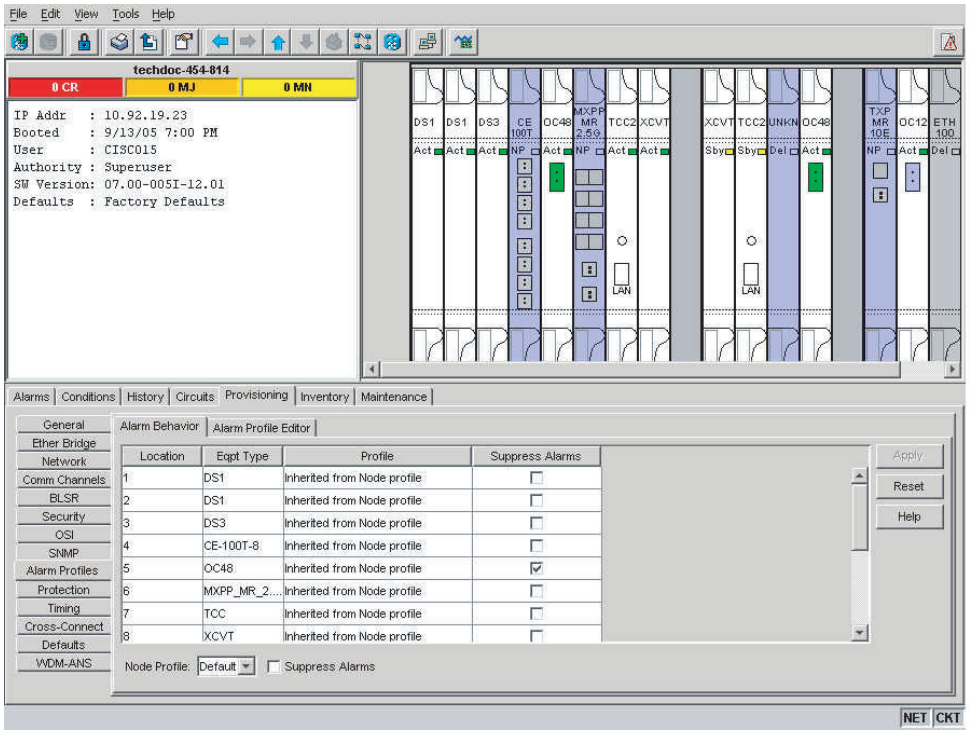
DLP-A518 アラーム重大度プロファイルの新規作成または複製

目的	この作業では、カスタム重大度プロファイルの作成と、デフォルト重大度プロファイルの複製および変更を行います。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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　ネットワーク ビューからアラーム プロファイル エディタにアクセスする場合は、**Provisioning > Alarm Profiles** タブをクリックします。

ステップ 2　ノード ビューからプロファイル エディタにアクセスする場合は、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします（図 22-2）。

図 22-2　ノード ビューのアラーム プロファイル エディタ



ステップ 3　カード ビューからプロファイル エディタにアクセスする場合は、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします。

ステップ 4　使用中のデフォルト プロファイルを基にして新しいプロファイルを作成する場合は、**New** をクリックして、ステップ 10 へ進みます。

ステップ 5　ノードに存在するプロファイルを使用してプロファイルを作成する場合は、Load Profile(s) ダイアログボックスで **Load** および **From Node** をクリックします。

a. Node Names リストで、ログイン中のノード名をクリックします。

b. Profile Names リストで、**Default** などの既存のプロファイル名をクリックします。ステップ 7 へ進みます。

ステップ 6　ローカルに、またはネットワーク ドライブに格納されているファイルのプロファイルを使用してプロファイルを作成する場合は、Load Profile(s) ダイアログボックスで **From File** をクリックします。

a. **Browse** をクリックします。

b. **Open** ダイアログボックスでファイルの格納場所に移動します。

c. **Open** をクリックします。

（注）　デフォルトまたはユーザ定義で重大度が Critical（CR）または Major（MJ）に設定されているものでも、サービスに影響しない（NSA）ものはすべて、Telcordia GR-474 の定義に従って Minor（MN）に格下げされます。

ステップ 7　**OK** をクリックします。

Alarm Profiles ウィンドウにアラーム重大度プロファイルが表示されます。アラーム プロファイル リストには、混合ノード ネットワークで使用されるアラームのマスター リストが含まれています。これらのアラームの中には、ONS ノードでは使用されないものもあります。

ステップ 8　プロファイル カラムで任意の場所を右クリックして、プロファイル編集のショートカット メニューを表示します（Default プロファイルの詳細については、ステップ 11 を参照してください）。

ステップ 9　ショートカット メニューから **Clone** をクリックします。

ヒント　ロードまたは複製に使用可能なものも含めて、すべてのプロファイルをリスト表示する場合は、Available をクリックします。プロファイルを複製する場合は、先にプロファイルをロードしておく必要があります。

ステップ 10　New Profile または Clone Profile ダイアログボックスで、New Profile Name フィールドに名前を入力します。

プロファイル名は一意でなければなりません。別のプロファイルと同じ名前のプロファイルをインポートしたり、指定したりしようとすると、CTC は接尾辞を付けて新しい名前を作成します。長いファイル名もサポートされています。

ステップ 11　**OK** をクリックします。

新しいアラーム プロファイル（ステップ 10 で指定）が作成されます。このプロファイルはデフォルト プロファイルの重大度を複製したもので、Alarm Profiles ウィンドウでは、以前のプロファイル カラムの右側に表示されます。このプロファイルは、選択して別の場所にドラッグできます。

（注）　2 つの予約済みプロファイル（Inherited と Default）も含めて、最大 10 個のプロファイルを CTC に格納できます。

Default プロファイルでは、重大度が Telcordia GR-253-CORE の標準設定に合わせて設定されています。アラームに Inherited プロファイルがある場合は、上位レベルの同じアラームからその重大度を継承（コピー）します。たとえば、ネットワーク ビューで Inherited プロファイルを選択すると、下位レベルの重大度（ノード、カード、およびポート）は、この選択内容からコピーされます。Inherited アラーム プロファイルが設定されているカードには、そのカードのあるノードで使用している重大度がコピーされます（プロファイルを作成する場合は、あらゆるレベルで個別に適用できます。そのためには、「DLP-A117 カードおよびノードへのアラーム プロファイルの適用」（p.18-6）を実行します）。

ステップ 12　次の手順で、新しいアラーム プロファイルを変更（カスタマイズ）します。

a. 新しいアラーム プロファイルのカラムで、プロファイルをカスタマイズするときに変更するアラーム重大度をクリックします。

b. ドロップダウン リストから重大度を選択します。

c. カスタマイズする重大度ごとにステップ a と b を繰り返します。変更したあとにアラームや状態を表示するときは、次の注意事項を参照してください。

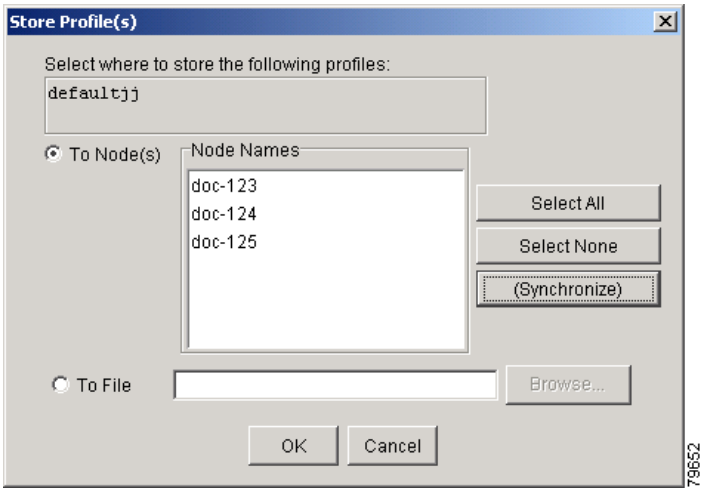
- デフォルトまたはユーザ定義で重大度が Critical（CR）または Major（MJ）に設定されているものでも、サービスに影響しない（NSA）ものはすべて、Telcordia GR-474 の定義に従って Minor（MN）に格下げされます。
- 新しいプロファイルを作成して適用するまでは、デフォルトの重大度がすべてのアラームおよび状態に適用されます。
- 重大度を継承（I）または未設定（U）に変更しても、アラームの重大度は変化しません。

ステップ 13　新しいアラーム プロファイルをカスタマイズしたあと、そのプロファイルのカラムを右クリックして選択します。

ステップ 14　**Store** をクリックします。

ステップ 15　Store Profile(s) ダイアログボックスで、**To Node(s)** をクリックしてステップ a に進むか、**To File** をクリックしてステップ b に進みます（図 22-3）。

図 22-3　Store Profiles ダイアログボックス



a.　プロファイルを保存するノードを選択します。

- 1 つのノードにだけプロファイルを保存する場合は、Node Names リストでそのノードをクリックします。
- すべてのノードにプロファイルを保存する場合は、**Select All** をクリックします。
- どのノードにもプロファイルを保存しない場合は、**Select None** を選択します。
- アラーム プロファイルの情報を更新する場合は、**(Synchronize)** をクリックします。

b.　プロファイルを保存します。

- **Browse** をクリックしてプロファイルの保存先を指定します。
- File name フィールドに名前を入力します。
- **Select** をクリックして、この名前と場所を選択します。長いファイル名もサポートされています。CTC は *.pfl という接尾辞を付けてファイルを格納します。
- **OK** をクリックしてプロファイルを保存します。

ステップ 16　必要に応じて次の操作を行います。

- 重大度の異なる行を表示するように Alarm Profiles ウィンドウを設定する場合は、**Hide Identical Rows** チェックボックスをクリックします。
- Default プロファイルと一致しない重大度を表示するように Alarm Profiles ウィンドウを設定する場合は、**Hide Reference Values** チェックボックスをクリックします。
- サービスに影響しない Minor アラームと一部の Major アラームを表示しないように Alarm Profiles ウィンドウを設定する場合は、**Only show service-affecting severities** チェックボックスをオンにします。

ステップ 17　元の NTP（手順）に戻ります。

DLP-A519 アラーム プロファイルのポートへの適用

目的	この作業では、カスタムまたはデフォルトのアラーム重大度プロファイルを 1 つまたは複数のポートに適用します。
工具 / 機器	なし
事前準備手順	DLP-A518 アラーム重大度プロファイルの新規作成または複製（p.22-11） DLP-A60 CTC へのログイン（p.17-71）
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 ビューでカードをダブルクリックして、カード ビューを開きます。

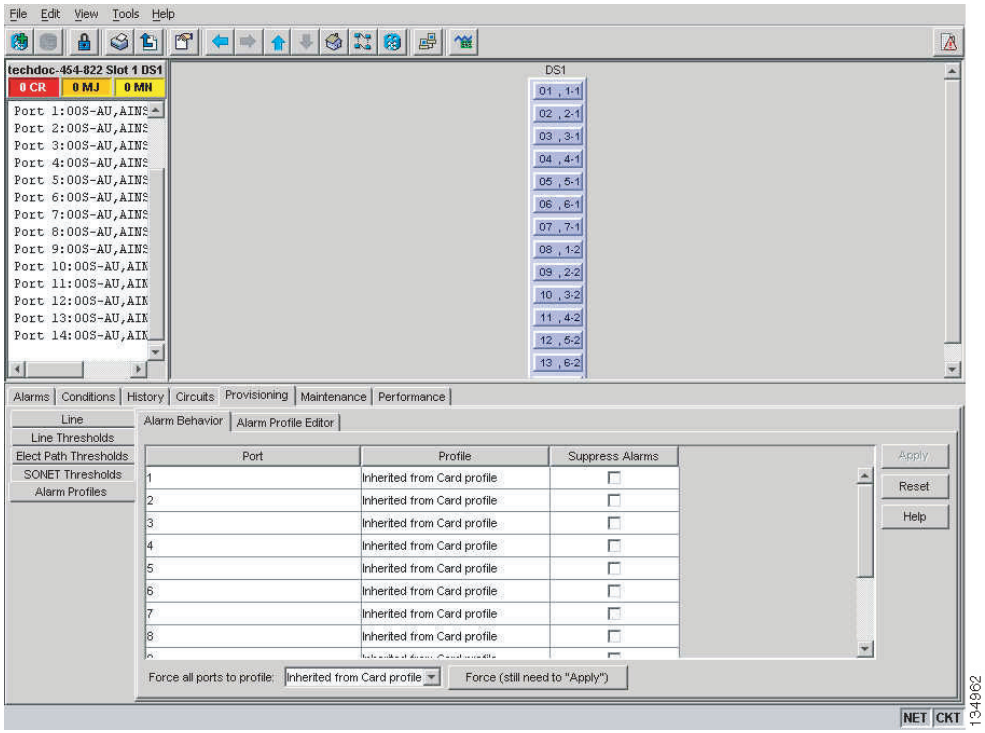
（注）　「DLP-A117 カードおよびノードへのアラーム プロファイルの適用」（p.18-6）を行うことでも、アラーム プロファイルをカードに適用できます。

（注）　TCC2/TCCP またはクロスコネクト カードでは、カード ビューを利用できません。

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

図 22-4 に、DS1/E1-56 カード ポートのアラーム プロファイルを示します。CTC は、[Parent Card Profile: Inherited] を示しています。

図 22-4　DS1-N-14 Card Alarm Behavior タブ



プロファイルを適用するポートが 1 つの場合は、ステップ 3 へ進みます。カード上のすべてのポートにプロファイルを適用する場合は、ステップ 4 へ進みます。

ステップ 3　ポート単位で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 ビューの Profile カラムで対象となるポートの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 4　カード上のすべてのポート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 ビューで、ウィンドウの下にある **Force all ports to profile** ドロップダウン メニューの矢印をクリックします。

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.　**Force (still need to "Apply")** をクリックします。

d.　**Apply** をクリックします。

ノード ビューの Port Level Profiles カラムに、[exist (1)] のような注記の付いたポートレベルのプロファイルが示されます（図 18-3 [p.18-6]）。

ステップ 5　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 6　元の NTP（手順）に戻ります。

DLP-A520 アラーム重大度プロファイルの削除

目的	この作業では、カスタムまたはデフォルトのアラーム重大度プロファイルを削除します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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　ネットワーク　ビューからアラーム　プロファイル　エディタにアクセスする場合は、ネットワーク ビューに移動して、**Provisioning > Alarm Profiles** タブをクリックします。

ステップ 2　ノード ビューからプロファイル エディタにアクセスする場合は、ノード ビューに移動して、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします。

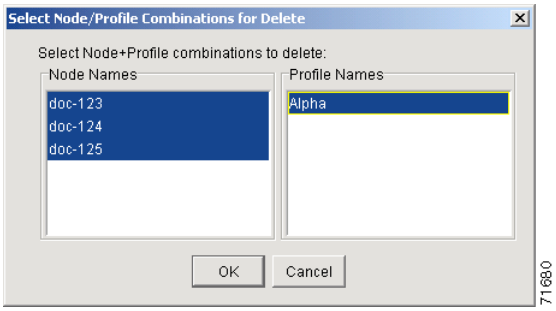
ステップ 3　カード　ビューからプロファイル　エディタにアクセスする場合は、カードをダブルクリックしてカード ビューを表示してから、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします。

ステップ 4　削除するプロファイルをクリックして、選択します。

ステップ 5　**Delete** をクリックします。

Select Node/Profile Combination for Delete ダイアログボックスが表示されます（図 22-5）。

図 22-5　Select Node/Profile Combination for Delete ダイアログボックス



（注）　Inherited または Default アラーム プロファイルは削除できません。

（注）　以前に作成したアラーム プロファイルは、ノードに格納されていないかぎり削除できません。プロファイルが Alarm Profiles タブに表示されていても、Select Node/Profile Combinations to Delete ダイアログボックスにリストされていない場合は、ステップ 9 へ進みます。

ステップ 6　Node Names リストでノード名をクリックして、プロファイルの場所を選択します。

ヒント　Shift キーを押したままにすると、ノード名を連続して選択できます。Ctrl キーを押したままにすると、ノードの任意の組み合わせを選択できます。

ステップ 7　Profile Names リストで削除するプロファイル名をクリックします。

ステップ 8　**OK** をクリックします。

Delete Alarm Profile ダイアログボックスで **Yes** をクリックします。

（注）　ノードからプロファイルを削除しても、次の手順を実行して削除しないかぎり、ネットワーク ビューの Provisioning > Alarm Profile Editor ウィンドウでは表示されたままになります。

ステップ 9　このウィンドウからアラーム プロファイルを削除する場合は、削除したプロファイルのカラムを右クリックし、ショートカット メニューから **Remove** を選択します。

（注）　ノードとプロファイルの組み合わせを選択しても、その組み合わせが存在しないと、[One or more of the profile(s) selected do not exist on one or more of the node(s) selected.] という警告が表示されます。たとえば、ノード A にはプロファイル 1 のみ格納されている場合、ユーザがプロファイル 1 とプロファイル 2 をノード A から削除しようとすると、この警告が表示されます。ただし、この処理でプロファイル 1 がノード A から削除されます。

（注）　Default と Inherited は、特殊なプロファイルなので削除できません。また、Select Node/Profile Combination for Delete ウィンドウにも表示されません。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A521 アラーム、状態、および履歴フィルタのパラメータ変更

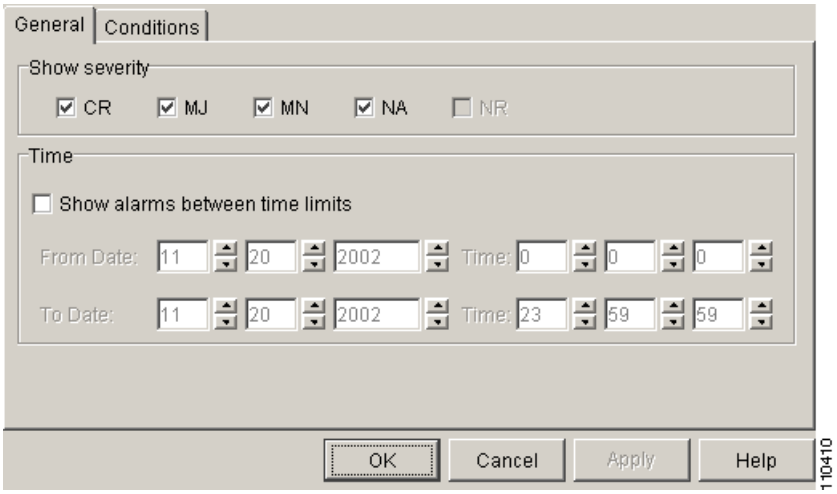
目的	この作業では、すべてのネットワーク ノードについて、そのアラームおよび状態の報告を変更します。
工具 / 機器	なし
事前準備手順	DLP-A225 アラーム フィルタリングのイネーブル化（p.19-20） DLP-A60 CTC へのログイン（p.17-71）
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

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

ステップ 2　下部にあるツールバーで左下にある **Filter** ボタンをクリックします。

フィルタのダイアログボックスが General タブを選択した状態で表示されます。図 22-6 に、Alarm Filter ダイアログボックスを示します。Conditions タブと History タブにも同様のダイアログボックスがあります。

図 22-6　Alarm Filter ダイアログボックスの General タブ



General タブの Show Severity ボックスでは、アラーム フィルタにかけて表示するアラーム重大度と、フィルタを通過したアラームの表示期間を指定することができます。フィルタにかけるアラーム重大度を変更する場合は、ステップ 3 へ進みます。アラームの表示期間フィルタを変更する場合は、ステップ 4 へ進みます。

ステップ 3　Show Severity 領域で、ネットワーク レベルで報告する重大度（Critical [CR]、Major [MJ]、Minor [MN]、または Not Alarmed [NA]）のチェックボックスをオンにします。重大度を表示しない場合は、重大度チェックボックスの選択をすべて解除（オフに）します。

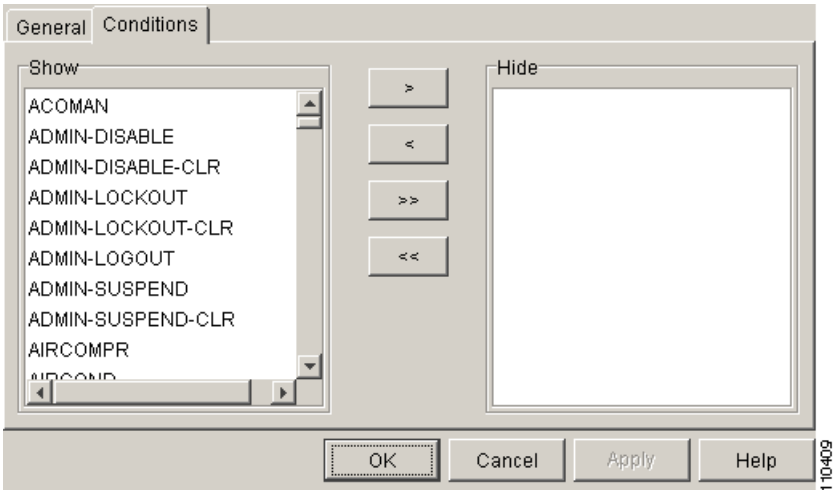
アラーム フィルタをディセーブルにすると、すべてのアラームが表示されます。

ステップ 4　Time 領域で、**Show alarms between time limits** チェックボックスをオンにして、イネーブル化します。From Date、To Date、および Time の各フィールドにある上下の矢印をクリックして、アラームの表示期間を変更します。

状態フィルタのパラメータを変更する場合は、ステップ 5 へ進みます。変更の必要がない場合は、ステップ 6 へ進みます。

ステップ 5　フィルタのダイアログボックスで **Conditions** タブをクリックします（図 22-7）。

図 22-7　Alarm Filter ダイアログボックスの Conditions タブ



フィルタがイネーブルになっているときは、Show リストに状態が表示され、Hide リストには状態が表示されません。

- 状態を Show リストから Hide リストへ個別に移動する場合は、> ボタンをクリックします。
- 状態を Hide リストから Show リストへ個別に移動する場合は、< ボタンをクリックします。
- 状態を Show リストから Hide リストへまとめて移動する場合は、>> ボタンをクリックします。
- 状態を Hide リストから Show リストへまとめて移動する場合は、<< ボタンをクリックします。

（注）　状態にはアラームも含まれます。

ステップ 6　**Apply** をクリックしてから **OK** をクリックします。

アラーム フィルタと状態フィルタのパラメータは、アラーム フィルタをイネーブルにすると強制的に適用され（「DLP-A225 アラーム フィルタリングのイネーブル化」[p.19-20] を参照）、アラーム フィルタをディセーブルにすると解除されます（「DLP-A227 アラーム フィルタリングのディセーブル化」[p.19-21] を参照）。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A522 アラーム レポートの抑制

目的	この作業では、ノード、カード、またはポート レベルで ONS 15454 のアラーム レポートを抑制します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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　複数の CTC/TL1 セッションが開かれている場合に 1 つのセッションのアラームを抑制すると、その他の開いているセッションでもアラームが抑制されます。

（注）　ノード レベルのアラーム抑制よりも、カードまたはポート レベルのアラーム抑制の方が優先されます。抑制は、3 つのエンティティについてそれぞれ別個に設定することができます。つまり、各エンティティごとに Alarms Suppressed by User Command（AS-CMD）アラームが発生するということです。

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

ステップ 2　ノード全体でアラームを抑制する場合は、次の手順を実行します。

a. **Suppress Alarms** チェックボックスをオンにします。

b. **Apply** をクリックします。

Alarms ウィンドウに表示されているそのノードのアラームの色がすべてホワイトに変わり、ステータスがクリア済みに変わります。アラームを抑制したあと、Alarms ウィンドウで **Synchronize** をクリックすると、ウィンドウからクリア済みのアラームが削除されます。ただし、ノードまたはカード ビューに AS-CMD アラームが表示され、ノードレベルでアラームが抑制されていることを示します。Object カラムに System と表示されます。

（注）　BITS、電源、またはシステム アラームを抑制するには、ノード全体のアラームを抑制するしかありません。これらのアラームは、個別に抑制できません。ただし、シェルフのバックプレーンは可能です。

ステップ 3　カードごとにアラームを抑制する場合は、次の手順を実行します。

a. 対象となるカードの行を特定します(スロット番号の Location カラムまたは装置名の Eqpt Type カラムを使用)。

b. その行の **Suppress Alarms column** チェックボックスをオンにします。

そのカードに抑制が直接適用されて、アラームの外観が、ステップ 2 で説明したように変わります。たとえば、スロット 16 の OC-48 カードで発生するアラームを抑制した場合、このカードで発生したアラームのノード ビューまたはカード ビューでの表示方法が変わります。つまり、AS-CMD アラームが表示されて、そこに Object 番号としてスロット番号が示されます。スロット 16 の OC-48 カードのアラームを抑制した場合は、AS-CMD オブジェクトは [SLOT-16] になります。

Apply をクリックします。

ステップ 4　カードのポートごとにアラームを抑制する場合は、ノード ビューでそのカードをダブルクリックします。

ステップ 5　**Provisioning> Alarm Profiles> Alarm Behavior** タブをクリックします。

ステップ 6　アラームを抑制するポートの行で **Suppress Alarms** カラムのチェックボックスをオンにします（図 22-4）。

ステップ 7　**Apply** をクリックします。

このポートに抑制が直接適用されて、アラームの外観がステップ 2 で説明したように変わります（ただし、カード全体にわたって発生しているアラームは表示されたままです）。いずれかのアラーム ウィンドウに AS-CMD アラームが表示され、オブジェクトとしてそのポートが示されます。たとえば、スロット 16 のポート 1 にある OC-48 カードのアラームを抑制した場合は、アラーム オブジェクトに [FAC-16-1] と表示されます。

ステップ 8　元の NTP（手順）に戻ります。

DLP-A523 アラーム抑制の中止

目的	この作業では、アラームの抑制を中止し、ポート、カード、またはノードで行うアラームの報告を再びイネーブルにします。
工具 / 機器	なし
事前準備手順	DLP-A522 アラーム レポートの抑制（p.22-21） DLP-A60 CTC へのログイン（p.17-71）
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　複数の CTC セッションが開かれている場合に 1 つのセッションのアラームを抑制すると、その他のセッションでもアラームが抑制されます。

ステップ 1　ノード全体でアラームの抑制を中止する場合は、次の手順を実行します。

a.　ノード ビューで、**Provisioning > Alarm Profiles > Alarm Behavior** タブをクリックします。

b.　**Suppress Alarms** チェックボックスをオフにします。

抑制されていたアラームが、Alarms ウィンドウに再び表示されます（これらのアラームは Synchronize ボタンによってウィンドウから消去されていた可能性があります）。システム オブジェクト付きで表示されていた AS-CMD アラームが、すべてのビューからクリアされます。

ステップ 2　カードごとにアラーム抑制を中止する場合は、次の手順を実行します。

a. ノード ビューで、**Provisioning > Alarm Profiles > Alarm Behavior** タブをクリックします。

b. スロット リストで、抑制されていたカードを特定します。

c. そのスロットの Suppress Alarms カラムのチェックボックスをオフにします。

d. **Apply** をクリックします。

抑制されていたアラームが、Alarms ウィンドウに再び表示されます（これらのアラームは Synchronize ボタンによってウィンドウから消去されていた可能性があります）。スロット オブジェクト（SLOT-16 など）付きで表示されていた AS-CMD アラームが、すべてのビューからクリアされます。

ステップ 3　ポートのアラーム抑制を中止するには、カードをダブルクリックしてカード ビューを開き、**Provisioning > Alarm Profiles > Alarm Behavior** タブをクリックします。

ステップ 4　抑制を中止するポートの **Suppress Alarms** チェックボックスをオフにします。

ステップ 5　**Apply** をクリックします。

抑制されていたアラームが、Alarms ウィンドウに再び表示されます（これらのアラームは Synchronize ボタンによってウィンドウから消去されていた可能性があります）。ポート オブジェクト（FAC-16-1 など）付きで表示されていた AS-CMD アラームが、すべてのビューからクリアされます。

ステップ 6　元の NTP（手順）に戻ります。

DLP-A524 アラーム重大度プロファイルのダウンロード

目的	この作業では、ネットワークドライブからアクセスできる CD-ROM、フロッピー ディスク、またはハード ディスクから、カスタム アラーム重大度プロファイルをダウンロードします。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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　ネットワーク ビューからアラーム プロファイル エディタにアクセスする場合は、**Provisioning > Alarm Profiles** タブをクリックします。

ステップ 2　ノード ビューからプロファイル エディタにアクセスする場合は、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします。

ステップ 3　カード　ビューからプロファイル　エディタにアクセスする場合は、カードをダブルクリックしてカード ビューを開いてから、**Provisioning > Alarm Profiles > Alarm Profile Editor** タブをクリックします。

ステップ 4　**Load** をクリックします。

ステップ 5　ノードに存在するプロファイルをダウンロードする場合は、Load Profile(s) ダイアログボックスで **From Node** をクリックします。

a. Node Names リストで、ログイン中のノード名をクリックします。

b. Profile Names リストで、**Default** などのプロファイル名をクリックします。

ステップ 6　ローカルに、またはネットワーク ドライブに格納されているプロファイルをダウンロードする場合は、Load Profile(s) ダイアログボックスで **From File** をクリックします。

a. **Browse** をクリックします。

b. **Open** ダイアログボックスでファイルの格納場所に移動します。

c. **Open** をクリックします。

（注）　Default アラーム プロファイル リストには、Telcordia GR-253-CORE のデフォルト値に対応したアラームおよび状態の重大度が含まれています（対応可能な場合のみ）。

（注）　デフォルトまたはユーザ定義で重大度が Critical（CR）または Major（MJ）に設定されているものでも、サービスに影響しない（NSA）ものはすべて、Telcordia GR-474 の定義に従って Minor（MN）に格下げされます。

ステップ 7　**OK** をクリックします。

ダウンロードされたプロファイルは、Alarm Profiles ウィンドウの右側に表示されます。

ステップ 8　ダウンロードされたプロファイル カラムの任意の場所を右クリックして、プロファイル編集ショートカット メニューを表示します。

ステップ 9　**Store** をクリックします。

ステップ 10　Store Profile(s) ダイアログボックスで、**To Node(s)** をクリックします。

a. プロファイルを保存するノードを選択します。
   - 1 つのノードにだけプロファイルを保存する場合は、Node Names リストでそのノードをクリックします。
   - すべてのノードにプロファイルを保存する場合は、**Select All** をクリックします。
   - どのノードにもプロファイルを保存しない場合は、**Select None** を選択します。
   - アラーム プロファイルの情報を更新する場合は、（**Synchronize**）をクリックします。

b. **OK** をクリックします。

ステップ 11　元の NTP（手順）に戻ります。

DLP-A526 DS3i-N-12 カードの回線およびスレッシュホールドの設定変更

目的	この作業では、DS3i-N-12 カードの回線とスレッシュホールドの設定を変更します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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）　ユーザによるプロビジョニング可能なカード設定のデフォルト値およびドメインについては、『*Cisco ONS 15454 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、回線またはスレッシュホールドの設定変更を行う DS3i-N-12 カードをダブルクリックします。

ステップ 2　**Provisioning** タブをクリックします。

ステップ 3　変更が必要な設定に応じて、**Line**、**Line Thresholds**、**Elect Path Thresholds**、または **SONET Thresholds** サブタブをクリックします。

（注）　Alarm Profiles タブの詳細については、第 8 章「アラームの管理」を参照してください。

（注）　スレッシュホールド設定を変更したい場合、利用可能な方向、タイプ、および間隔（15 分、1 日）オプション ボタンをクリックし、次に **Refresh** をクリックします。これにより、希望のスレッシュホールド設定が表示されます。

ステップ 4　変更したいフィールドをクリックして、そのサブタブの下にある設定を変更します。一部のフィールドでは、ドロップダウン リストからオプションを選択し、その他のフィールドには値を入力します。

ステップ 5　**Apply** をクリックします。

ステップ 6　プロビジョニングするパラメータのあるサブタブごとに、ステップ 3 ～ 5 を繰り返します。

回線設定の定義については、表 22-1 を参照してください。回線スレッシュホールドの設定の定義については、表 22-2 を参照してください。電気回路パス スレッシュホールドの設定の定義については、表 22-3 を参照してください。SONET スレッシュホールドの設定の定義については、表 22-4 を参照してください。

表 22-1 に、DS3i-N-12 カードに対する Provisioning > Line タブの値を示します。

表 22-1　DS3i-N-12 カードの回線オプション

パラメータ	内容	オプション
Port	（表示専用）ポート番号	1 ～ 12
Port Name	ポート名を設定します。	ユーザが 32 文字以下の英数字または特殊文字で定義します。デフォルトはブランクです。 「DLP-A314 ポートへの名前の割り当て」（p.20-9）を参照してください。
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
Line Type	ライン フレーミング タイプを指定します。	• Unframed • M13 • C Bit • Auto Provisioned
Detected Line Type	検出された回線のタイプを表示します。	• M13 • C Bit • Unframed • Unknown
Line Coding	（表示専用）DS3E 伝送符号化タイプを定義します。	B3ZS
Line Length	バックプレーン接続から次の終端地点までの距離（フィート単位）を指定します。	• 0 ～ 225（デフォルト） • 226 ～ 450

表 22-1　DS3i-N-12 カードの回線オプション（続き）

パラメータ	内容	オプション
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。	• IS — ポートを稼働状態にします。ポートのサービス状態は IS-NR に変化します。 • IS,AINS — ポートを自動稼働状態にします。ポートのサービス状態は OOS-AU,AINS に変化します。 • OOS,DSBLD — 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 OOS-MA,DSBLD に変化します。 • OOS,MT — 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 OOS-MA,MT に変化します。
Service State	（表示専用）自律的に生成され、ポートの全体的な状態を示すサービス状態を識別します。サービス状態は、Primary State-Primary State Qualifier、Secondary State という形式で表示されます。	• IS-NR —（In-Service and Normal）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。 • OOS-AU,AINS —（Out-Of-Service and Autonomous, Automatic In-Service）ポートは停止中ですが、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、エラーなし信号をモニタします。エラーなし信号を検出したあと、ポートはソーク時間の間 OOS-AU,AINS 状態に留まります。ソーク時間が過ぎると、ポートのサービス状態は IS-NR に変化します。 • OOS-MA,DSBLD —（Out-of-Service and Management, Disabled）ポートは停止中でトラフィックを伝送できません。 • OOS-MA,MT —（Out-of-Service and Management, Maintenance）ポートはメンテナンスのために停止しています。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	自動稼働のソーク時間を設定します。	• 入力信号が有効であり続ける時間を hh:mm の形式で表します。この時間が経過すると、カードが自動的に稼働状態（IS）へ変わります。 • 0 ～ 48 時間、15 分刻み

表 22-2 に、DS3i-N-12 カードに対する Provisioning > Line Thresholds タブのパラメータを示します。

表 22-2　DS3i-N-12 カードの回線スレッシュホールド オプション

パラメータ	内容
Port	（表示専用）ポート番号（1 ～ 12）
CV	符号化違反数。
ES	エラー秒数
SES	重大エラー秒数
LOSS	Loss of Signal（LOS; 信号損失）秒数。1 つまたは複数の LOS 障害が発生した 1 秒数の間隔です。
15 Min オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、15 分間隔で表示されます。
1 Day オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、1 日間隔で表示されます。

表 22-3 に、DS3i-N-12 カードに対する Provisioning > Elect Path Thresholds タブのパラメータを示します。

表 22-3　DS3i-N-12 カードの電気回路パス オプション

パラメータ	内容
Port	（表示専用）ポート番号（1 ～ 12）
CVP	符号化違反数 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
ESP	エラー秒数 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
SESP	重大エラー秒数 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
SASP	重大エラー フレーム / アラーム表示信号 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
UASP	使用不可秒数 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
AISSP	Alarm Indication Signal（AIS; アラーム表示信号）秒数 — パス。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit 用、近端および遠端。
15 Min オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、15 分間隔で表示されます。
1 Day オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、1 日間隔で表示されます。

表 22-4 に、DS3i-N-12 カードに対する Provisioning > SONET Thresholds タブの値を示します。

表 22-4　DS3i-N-12 カードの SONET スレッシュホールド オプション

パラメータ	内容
Port	（表示専用）ポート番号（1 ～ 12）
CV	符号化違反数
ES	エラー秒数
FC	障害カウント

表 22-4　DS3i-N-12 カードの SONET スレッシュホールド オプション（続き）

パラメータ	内容
SES	重大エラー秒数
UAS	使用不可秒数
15 Min オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、15 分間隔で表示されます。
1 Day オプション ボタン	このオプション ボタンをクリックし、次に Refresh をクリックすると、このタブのスレッシュホールド値が、1 日間隔で表示されます。

（注）　スレッシュホールドは、回線が作成されたあとで表示されます。

ステップ 7　元の NTP（手順）に戻ります。

DLP-A527 OC-N カード ALS メンテナンス設定の変更

目的	この作業では、OC-N カードの Automatic Laser Shutdown（ALS; 自動レーザー シャットダウン）メンテナンス設定を変更します。この機能は、OC3-8 カード、OC-192 カード、および MRC-12 カードで使用できます。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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）　ユーザによるプロビジョニング可能なカード設定のデフォルト値およびドメインについては、『*Cisco ONS 15454 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、ALS メンテナンス設定を変更する OC-N カードをダブルクリックします。

ステップ 2　**Maintenance > ALS** 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 22-5 にある設定を変更します。一部のフィールドでは、ドロップダウン リストからオプションを選択し、その他のフィールドには値を入力するか、チェックボックスをオン / オフします。表のオプション カラムにプロビジョニング可能なパラメータが表示されます。

ステップ 4　**Apply** をクリックします。変更内容がトラフィックに影響する場合、警告メッセージが表示されます。**Yes** をクリックして、変更を完了します。

表 22-5　OC-N メンテナンス設定

パラメータ	内容	オプション
ポート番号	（表示専用）ポート番号	—
ALS Mode	ALS モード。ALS では、RX が LOS を検出したとき、TX レーザーをシャットダウンできます。	ドロップダウン リストから、次のいずれかを選択します。 • Disable — ALS を無効にします。 • Auto Restart —（デフォルト）ALS はアクティブです。電源は必要に応じて自動的にシャットダウンされ、障害の原因が修復されるまで、プローブ パルスを使用して自動的に再起動を試みます。 • Manual Restart — ALS はアクティブですが、電源供給停止を引き起こした状態を解決したときに、レーザーを手動で再起動する必要があります。 • Manual Restart for Test — テストのため、レーザーを手動で再起動します。
Recovery Pulse Duration	レーザーのシャットダウン後、光電源パルスの初期リカバリのためのリカバリ レーザー パルス時間を秒単位で設定します。	数値。ユーザによるプロビジョニング可能なカード設定のデフォルト値およびドメインについては、『*Cisco ONS 15454 Reference Manual*』の付録「Network Element Defaults」を参照してください。
Recovery Pulse Interval	リカバリ レーザー パルス間隔を秒単位で設定します。この間隔は、リカバリ パルスが繰り返される前に経過する必要がある時間です。	数値。ユーザによるプロビジョニング可能なカード設定のデフォルト値およびドメインについては、『*Cisco ONS 15454 Reference Manual*』の付録「Network Element Defaults」を参照してください。
Currently Shutdown	（表示専用）レーザーの現在の状態を表示します。	数値。ユーザによるプロビジョニング可能なカード設定のデフォルト値およびドメインについては、『*Cisco ONS 15454 Reference Manual*』の付録「Network Element Defaults」を参照してください。
Request Laser Restart	オンになっている場合、メンテナンス用にレーザーを再起動できます。 **（注）** レーザーを再起動すると、トラフィックに影響を与えることがあります。	オンまたはオフ

ステップ 5　元の NTP（手順）に戻ります。

DLP-A528 ネットワーク ビューのデフォルト背景マップの変更

目的	この作業は、CTC ネットワーク ビューのデフォルト マップを変更します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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

（注） 背景イメージを変更する場合、変更はコンピュータの 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　Edit メニューから **Preferences > Map** を選択し、**Use Default Map** チェックボックスをオンにします。

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

ステップ 3　Defaults Selector 領域で **CTC** を選択し、次に **network** を選択します。

ステップ 4　**Default Value** フィールドをクリックし、ドロップダウン リストからデフォルトのマップを選択します。マップには、ドイツ、日本、オランダ、韓国、英国、および米国（デフォルト）があります。

ステップ 5　**Apply** をクリックします。新しいネットワーク マップが表示されます。

ステップ 6　**OK** をクリックします。

ステップ 7　ONS 15454 のアイコンが表示されていない場合は、ネットワーク ビューを右クリックして、**Zoom Out** を選択します。ONS 15454 のすべてのアイコンが表示されるまで繰り返します（**Fit Graph to Window** を選択することもできます）。

ステップ 8　ノード アイコンの位置を変更するには、アイコンをマップ上の新しい場所に 1 つずつドラッグ アンド ドロップします。

ステップ 9　アイコンの表示倍率を変更する場合は、ネットワーク ビューを右クリックして、**Zoom In** を選択します。ONS 15454 のアイコンが希望の倍率で表示されるまで繰り返します。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A529 イーサネットの RMON アラーム スレッシュホールドの削除

目的	この作業では、イーサネット ポートの Remote Monitoring（RMON）スレッシュホールド超過アラームを削除します。
工具 / 機器	なし
事前準備手順	DLP-A533 イーサネットの RMON アラーム スレッシュホールドの作成（p.22-37） DLP-A60 CTC へのログイン（p.17-71）
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） ONS 15454 ML シリーズ カードでは、Cisco IOS CLI（コマンドライン インターフェイス）を使用して、RMON を管理します。

ステップ 1　RMON アラームのスレッシュホールドを削除するイーサネット カードをダブルクリックします。

ステップ 2　カード ビューで **Provisioning > Ether Ports > RMON Thresholds** タブをクリックします。

（注） CE シリーズの場合、**Provisioning > Ether Ports > RMON Thresholds** タブまたは **Provisioning > POS Ports > RMON Thresholds** タブをクリックします。

ステップ 3　削除する RMON アラームのスレッシュホールドをクリックします。

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

ステップ 5　**Yes** をクリックして、スレッシュホールドを削除します。

ステップ 6　元の NTP（手順）に戻ります。

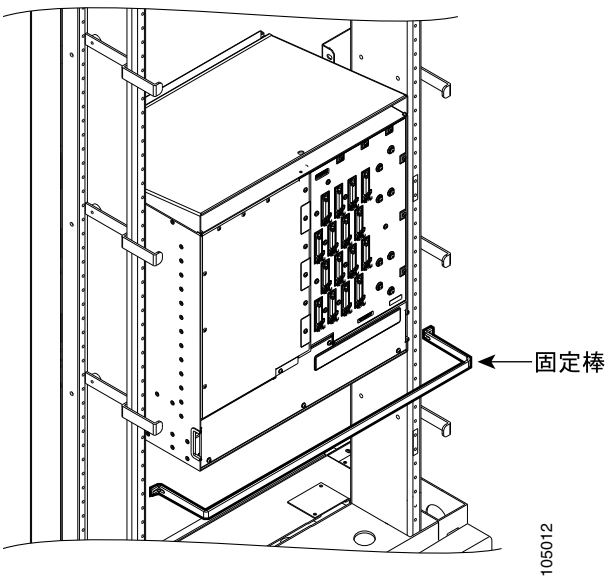
DLP-A530 固定棒の取り付け

目的	この作業では、ONS 15454 の背面のケーブル接続を固定するために使用される固定棒を取り付けます。固定棒を使用することにより、冗長電源装置とケーブルにダイバース パスを提供できます。
工具 / 機器	固定棒 ネジ（4）
事前準備手順	DLP-A5 ラックへのシェルフ アセンブリの取り付け（1 人で作業する場合）（p.17-5） DLP-A6 ラックへのシェルフ アセンブリの取り付け（2 人で作業する場合）（p.17-6）
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

ステップ 1　固定棒の端を、ONS 15454 の 1 RU 下にある 4 本のネジ穴に合わせます。

図 22-8 は、固定棒、ONS 15454、およびラックを示します。

図 22-8　固定棒



ステップ 2　ラックに 4 本のネジを取り付けます。

ステップ 3　元の NTP（手順）に戻ります。

DLP-A531 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のデータをグラフ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-A60 CTC へのログイン（p.17-71）
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。

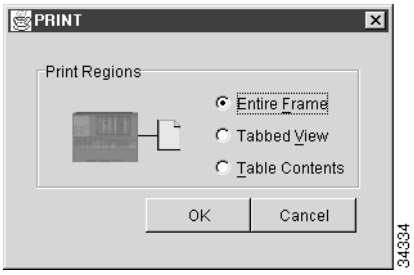
ステップ 3　Print ダイアログボックスで、印刷オプションをクリックします（図 22-9）。

- 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、またはタブの図を除いて、CTC データを表形式で印刷します。このオプションは、次のウィンドウには適用されません。
  - Provisioning > General タブ（General、Power Monitor、および Multishelf Config）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 > Cross-Connect ウィンドウ
  - Provisioning > OSI > Main Setup、TARP 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

  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、ノード、およびカードの各ビューはまったく同じですが、ネットワーク ビューには Inventory タブまたは Performance タブがありません。

図 22-9　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-A532 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 ウィンドウからもデータをエクスポートできます。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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　詳細回線情報をエクスポートする場合は、次の手順を実行します。

a.　Circuits ウィンドウで回線を選択し、**Edit** をクリックして Edit Circuits ウィンドウ内で開きます。

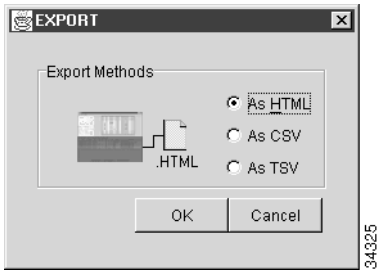
b.　Edit Circuit ウィンドウで、Drops、UPSR Selectors、UPSR Switch Counts、State、または Merge のいずれかのタブをクリックします（設定によっては、これらのうち一部のタブが表示されないことがあります）。

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 22-10）。

- **As HTML** — 図を含まない単純な 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（カンマ区切り形式）で保存します。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（タブ区切り形式）で保存します。

図 22-10　エクスポートの対象にする CTC データの選択



ステップ 5　テキスト エディタまたはワープロ アプリケーションでファイルを開く場合、それぞれで手順が異なります。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、カンマ区切りやタブ区切りも含めて、エクスポートされた形式のままでデータをフォーマットします。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フォーマットできます。

ステップ 6　スプレッドシートおよび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、それぞれで手順が異なります。通常は、アプリケーションを開いたあと、File > Import を選択して区切られたファイルを選択し、データをセルにフォーマットします。

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、次の表形式（TSV として保存）データには適用されません。

- Circuits（Edit オプション、General および Monitor ウィンドウ）
- Provisioning > General > General、Power Monitor、および Multishelf Config 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 および BITS FAcilities ウィンドウ

- Provisioning > OSI > Main Setup ウィンドウおよび OSI > TARP > Config ウィンドウ
- Provisioning > Cross-Connect 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、次のいずれかの形式を使用して名前を入力します。

- *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を指定します。

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-A533 イーサネットの RMON アラーム スレッシュホールドの作成

目的	この手順では、RMON をセットアップして、ネットワーク管理システムでイーサネット ポートをモニタできるようにします。
工具 / 機器	なし
事前準備手順	NTP-A323 カードの取り付けの確認（p.4-2）
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）　ONS 15454 ML シリーズ カードでは、Cisco IOS CLI を使用して、RMON を管理します。

ステップ 1　RMON を設定するノードで「DLP-A60 CTC へのログイン」（p.17-71）を行います。すでにログインしている場合は、ステップ 2 へ進みます。

ステップ 2　RMON アラームのスレッシュホールドを作成するイーサネット カードをダブルクリックします。

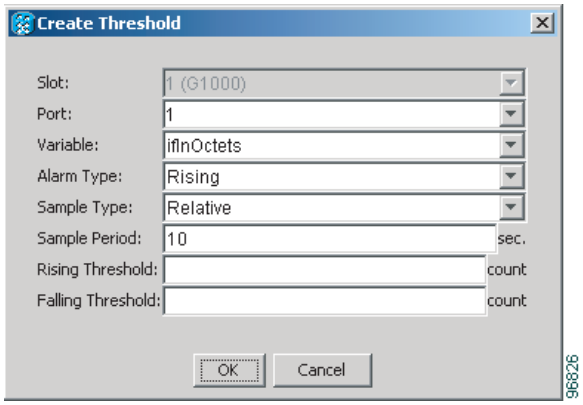
ステップ 3　カード ビューで **Provisioning > RMON Thresholds** タブをクリックします。

（注）　CE シリーズ カードおよび ML シリーズ カードの場合、**Provisioning > Ether Ports > RMON Thresholds** タブまたは **Provisioning > POS Ports > RMON Thresholds** タブをクリックします。

ステップ 4　**Create** をクリックします。

Create Ether Threshold ダイアログボックスが表示されます（図 22-11）。

図 22-11　RMON スレッシュホールドの作成



ステップ 5　Port ドロップダウン リストで、選択したイーサネット カードで利用できるポートを選択します。

ステップ 6　Variable ドロップダウン リストで変数を選択します。このフィールドで選択できるイーサネットおよび POS スレッシュホールド変数については、表 22-6 および表 22-7 を参照してください。

表 22-6　イーサネットのスレッシュホールド変数（MIB）

変数	定義
ifInOctets	インターフェイスで受信したオクテットの総数（フレーミング オクテットを含む）。
ifInUcastPkts	対応するプロトコルに配送されたユニキャスト パケットの総数
ifInMulticastPkts	（G シリーズ、CE シリーズ、ML シリーズのみ）正常に受信したマルチキャスト フレームの数
ifInBroadcastPkts	（G シリーズ、CE シリーズ、ML シリーズのみ）このサブレイヤのブロードキャスト アドレスを使用してこのサブレイヤから上位（サブ）レイヤに渡されたパケットの数
ifInDiscards	（G シリーズ、CE シリーズ、ML シリーズのみ）正常に受信したが、上位レイヤのプロトコルに渡されないように廃棄された着信パケットの数
ifInErrors	エラーがあるために廃棄された着信パケットの数
ifOutOctets	送信オクテットの総数（フレーミング パケットを含む）。

表 22-6　イーサネットのスレッシュホールド変数（MIB）（続き）

変数	定義
ifOutUcastPkts	単一のアドレスへ送信するように要求されたユニキャスト パケットの総数
ifOutMulticastPkts	（G シリーズ、CE シリーズ、ML シリーズのみ）正常に送信したマルチキャスト フレームの数
ifOutBroadcastPkts	（G シリーズ、CE シリーズ、ML シリーズのみ）上位プロトコルから送信するように要求されたパケットで、このサブレイヤのブロードキャスト アドレスを使用したパケットの総数（廃棄、未送信も含む）。
ifOutDiscards	（G シリーズのみ）エラーはないが、送信されないように廃棄されたパケットの数
dot3statsAlignmentErrors	アライメント エラーがあったフレームの数。つまり、長さがオクテットの整数倍でないために、Frame Check Sequence（FCS）テストに合格できなかったフレームの数
dot3StatsFCSErrors	フレーム チェック エラーがあったフレームの数。つまり、長さはオクテットの整数倍であったが FCS テストで問題の判明したフレームの数
dot3StatsSingleCollisionFrames	（E シリーズまたは G シリーズ以外）衝突に 1 回だけ遭遇して、正常に送信されたフレームの数
dot3StatsMutlipleCollisionFrames	（E シリーズまたは G シリーズ以外）衝突に複数回遭遇して、正常に送信されたフレームの数
dot3StatsDeferredTransmissions	（E シリーズまたは G シリーズ以外）メディアが混雑していたために最初の送信が遅れた回数
dot3StatsLateCollisions	（E シリーズまたは G シリーズ以外）64 オクテットを送信したあとに衝突が検出された回数（衝突カウントにも追加）
dot3StatsExcessiveCollisions	（E シリーズまたは G シリーズ以外）衝突回数が多すぎて送信に失敗したフレームの数
dot3StatsCarrierSenseErrors	（G シリーズのみ）他のインターフェイスではカウントされていない、特定インターフェイス上の送信エラーの数
dot3StatsSQETestErrors	（G シリーズのみ）特定のインターフェイスの PLS 副層で SQE TEST ERROR メッセージが生成された回数
etherStatsBroadcastPkts	正常に受信したブロードキャスト パケットの合計数。（マルチキャスト パケットを含まない）。

表 22-6　イーサネットのスレッシュホールド変数（MIB）（続き）

変数	定義
etherStatsCollisions	このイーサネット セグメントで発生した衝突の推定合計回数。戻り値は、RMON プローブの場所によって異なります。IEEE 802.3 標準のセクション 8.2.1.3（10BASE5）およびセクション 10.3.1.3（10BASE2）には、3 つ以上のステーションが同時に通信を行うと、受信モードのステーションでは 1 回の衝突を検出する旨が記載されています。リピータの各ポートでは、2 つ以上のステーションが同時に通信した場合、1 回の衝突を検出します。したがって、リピータのポートに配置されているプローブには、同じセグメントのステーションに接続されているプローブよりも多くの衝突が記録される可能性があります。 10BaseT の場合は、プローブの場所はそれほど重要ではありません。IEEE 802.3 標準のセクション 14.2.1.4（10BaseT）では、DO 回路と RD 回路で信号が同時に存在している（つまり、同時に送受信している）ことを衝突と定義しています。10BaseT ステーションでは、送信時にしか衝突が検出されません。したがって、ステーションとリピータに配置されたプローブのどちらでも、同じ数の衝突が記録されます。 リピータ内の RMON プローブでは、リピータと他の 1 つまたは複数のホストとの間の衝突（IEEE 802.3k で定義されている送信衝突）と、リピータが接続されている同軸セグメントにおいて検出されたレシーバーの衝突が報告されます。
etherStatsCollisionFrames	このイーサネット セグメントで発生した衝突の推定合計回数。戻り値は、RMON プローブの場所によって異なります。IEEE 802.3 標準のセクション 8.2.1.3（10BASE5）およびセクション 10.3.1.3（10BASE2）には、3 つ以上のステーションが同時に通信を行うと、受信モードのステーションでは 1 回の衝突を検出する旨が記載されています。リピータの各ポートでは、2 つ以上のステーションが同時に通信した場合、1 回の衝突を検出します。したがって、リピータのポートに配置されているプローブには、同じセグメントのステーションに接続されているプローブよりも多くの衝突が記録される可能性があります。 10BaseT の場合は、プローブの場所はそれほど重要ではありません。IEEE 802.3 標準のセクション 14.2.1.4（10Base-T）では、DO 回路と RD 回路で信号が同時に存在している（つまり、同時に送受信している）ことを衝突と定義しています。10BaseT ステーションでは、送信時にしか衝突が検出されません。したがって、ステーションとリピータに配置されたプローブのどちらでも、同じ数の衝突が記録されます。 リピータ内の RMON プローブでは、リピータと他の 1 つまたは複数のホストとの間の衝突（IEEE 802.3k で定義されている送信衝突）と、リピータが接続されている同軸セグメントにおいて検出されたレシーバーの衝突が報告されます。
etherStatsDropEvents	リソース不足が原因で、パケットがプローブによって廃棄されたイベントの合計数。この数値は、必ずしも廃棄パケットの合計数を表すものではなく、このような状況が検出された回数を示します。

表 22-6　イーサネットのスレッシュホールド変数（MIB）（続き）

変数	定義
etherStatsJabbers	ネットワークから受信したデータのオクテット総数（不正なパケットを含む）。
etherStatsMulticastPkts	正常に受信したマルチキャスト パケットの合計数（ブロードキャスト パケットを含まない）。
etherStatsOversizePkts	長さが 1518 オクテットより長い（フレーミング ビットは除き、FCS オクテットは含む）こと以外には、適切に形成されている受信パケットの総数
etherStatsUndersizePkts	64 オクテットより短い受信パケットの数
etherStatsFragments	オクテットが整数倍でないか FCS にエラーのある、64 オクテットより短いパケットの総数
etherStatsPkts64Octets	長さが 64 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsPkts65to127Octets	長さが 65 ～ 172 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsPkts128to255Octets	長さが 128 ～ 255 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsPkts256to511Octets	長さが 256 ～ 511 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsPkts512to1023Octets	長さが 512 ～ 1023 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsPkts1024to1518Octets	長さが 1024 ～ 1518 オクテットの受信パケットの総数（エラー パケットを含む）。
etherStatsJabbers	オクテットが整数倍でないか FCS にエラーのある、1518 オクテットより長いパケットの総数
etherStatsOctets	ネットワークで受信したデータ（不正パケットのデータも含む）のオクテットの総数（フレーミング ビットは除き、FCS オクテットは含む）。
etherStatsCollisions	セグメントで発生した衝突の総数に最も近い推定値
etherStatsCollisionFrames	セグメントで発生したフレーム衝突の合計回数に最も近い推定値
etherStatsCRCAlignErrors	長さが 64 ～ 1518 オクテットで、FCS にエラーがあるか、または長さがオクテットの整数倍でないパケットの総数
receivePauseFrames	（G シリーズのみ）受信した IEEE 802.x ポーズ フレームの数
transmitPauseFrames	（G シリーズのみ）送信した IEEE 802.x ポーズ フレームの数
receivePktsDroppedInternalCongestion	（G シリーズのみ）フレーム バッファのオーバーフローやその他の理由によって廃棄された受信フレームの数
transmitPktsDroppedInternalCongestion	（G シリーズのみ）フレーム バッファのオーバーフローやその他の理由によって廃棄された送信フレームの数
txTotalPkts	送信パケットの総数
rxTotalPkts	受信パケットの総数
mediaIndStatsOversizeDropped	CE-100T-8 RMON スレッシュホールドより大きい受信パケットの数
mediaIndStatsTxFramesTooLong	長さが 1548 を超えていた送信パケットの数

表 22-7　POS スレッシュホールド変数（MIB）

変数	定義
ifInPayloadCrcErrors	SONET の受信（RX）方向から送信される GFP/HDLC ペイロード内のフレームにある CRC エラーの数
ifOutPayloadCrcErrors	SONET の送信（TX）方向から送信される GFP/HDLC ペイロード内のフレームにある CRC エラーの数
ifOutOversizePkts	SONET に送信された 1518 バイトより大きいパケット数。 1600 バイトより大きいパケットは送信されません。
etherStatsDropEvents	ポート レベルで廃棄された受信フレームの数
gfpStatsRxSBitErrors	シングル ビット エラーがある受信フレーム数（cHEC、tHEC、eHEC）
gfpStatsRxMBitErrors	マルチ ビット エラーがある受信フレーム数（cHEC、tHEC、eHEC）
gfpStatsRxTypeInvalid	無効なタイプがある受信フレーム数（PTI、EXI、UPI）
gfpStatsRxCRCErrors	ペイロード CRC エラーがある受信データ フレーム数
gfpStatsRxCIDInvalid	無効な CID がある受信フレーム数
gfpStatsCSFRaised	クライアント信号エラー表示のある受信（Rx）クライアント管理フレームの数
gfpStatsRxFrame	受信データ フレーム数
gfpStatsTxFrame	送信データ フレーム数
gfpStatsRxOctets	受信済みデータ オクテット数
gfpStatsTxOctets	送信データ オクテット数

ステップ 7　Alarm Type ドロップダウン リストで、イベントをトリガーするスレッシュホールドとして、上限スレッシュホールドと下限スレッシュホールドの一方または両方を指定します。

ステップ 8　Sample Type ドロップダウン リストから、**Relative** または **Absolute** を選択します。Relative を指定すると、スレッシュホールドに使用する発生回数が、ユーザ設定のサンプリング周期に制限されます。Absolute を指定すると、スレッシュホールドは周期に関係なく、発生回数の合計を使用するように設定されます。

ステップ 9　Sample Period に適切な秒数を入力します。

ステップ 10　Rising Threshold に適切な発生回数を入力します。

上昇タイプのアラームの場合は、測定値が下限スレッシュホールドより下から上限スレッシュホールドより上に変動したときにアラームが発生します。たとえば、ネットワークの衝突発生回数が 15 秒あたり 1000 回という上限スレッシュホールドを下回っていたときに、ネットワークで問題が発生して、15 秒間に 1001 回の衝突が記録されると、そのこと（衝突の発生回数がスレッシュホールドを超えたということ）がトリガーになってアラームが生成されます。

ステップ 11 Falling Threshold フィールドに適切な発生回数を入力します。多くの場合、下限スレッシュホールドは上限スレッシュホールドより低く設定します。

下限スレッシュホールドと上限スレッシュホールドはペアで使用されます。発生回数が上限スレッシュホールドより高くなって、その後下限スレッシュホールドより下に下がると、上限スレッシュホールドはリセットされます。たとえば、15 分間に 1001 回という衝突を起こしていたネットワークの問題がなくなって、15 分間に 799 回の衝突しか発生しなくなると、発生回数は 800 という下限スレッシュホールドより低くなります。この状態変化によって上限スレッシュホールド値はリセットされ、ネットワークの衝突が再び急増して 15 分間に 1000 回という上限スレッシュホールドを超えると、その時点でまたアラームが生成されます。イベントのトリガーとなるのは、上限スレッシュホールド値を初めて超えたときだけです（そうでないと、1 つのネットワーク障害によって、上限スレッシュホールド値を何度も超えて、イベントが大量に発生してしまうためです）。

ステップ 12 **OK** をクリックしてこの手順を完了します。

ステップ 13 元の NTP（手順）に戻ります。

DLP-A534 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、Open Systems Interconnection（OSI; 開放型システム間相互接続）のルーティング モードをプロビジョニングします。この作業は、ONS 15454 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 Communication 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 Network Element（NE; ネットワーク要素）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	NTP-A323 カードの取り付けの確認（p.4-2）
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 Reference Manual*』にある「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。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せずに、LSP バッファを変更しないでください。

注意　LSP バッファ サイズを、OSI 領域内の LAP-D Maximum Transmission Unit（MTU; 最大伝送ユニット）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 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 Serrice 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　OSI ルーティング モードをプロビジョニングするノードで「DLP-A60 CTC へのログイン」（p.17-71）を行います。すでにログインしている場合は、ステップ 2 へ進みます。

ステップ 2　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 3　ルーティング モードを選択します。

- End System — ONS 15454 は OSI End System（ES; エンド システム）機能を実行し、Intermediate System（IS; 中継システム）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 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 ノードとの通信方法は、IS L1/L2 ノードごとに異なります。
- Intermediate System Level 1/Level 2 — ONS 15454 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、ノードが接続されている。
  - 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、ノードが接続されている。

ステップ 4　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 Protocol Data Unit（PDU; プロトコル データ ユニット）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 5　元の NTP（手順）に戻ります。

DLP-A535 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-A60 CTC へのログイン（p.17-71）
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

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 は受信元の 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 パラメータは使用されません。

- 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 のターゲットでなければ、伝播は発生しますが、PDU は受信元の NE には伝播されません。

（注）　TARP PDUs L2 Propagation パラメータが使用されるのは、Node Routing Area が IS Level1/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（TARP 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/NSAP の更新または訂正）。TARP 3 PDU は Type 1 および Type 2 PDU への応答です。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）　このパラメータを使用するのは、TARP PDUs Origination パラメータがイネーブルである場合のみです。

- L2 TARP Data Cache — オン（デフォルト）の場合、Type 2 の要求を送信している 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。

TDC パラメータは、別の IS Level 1/Level 2 ノードに接続された IS 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 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。

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 パラメータは使用されません。

- 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（デフォルト設定ではオフになっています）。
- 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 タイムは、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 がイネーブルでない場合、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-A536 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-A60 CTC へのログイン（p.17-71）
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 タブにある 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を使用した場合は、**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-A537 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-A60 CTC へのログイン（p.17-71）
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-A538 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 が TARP 機能を持たないルータ間または非 SONET 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-A60 CTC へのログイン（p.17-71）
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、Type2 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を使用した場合は、**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-A539 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-A60 CTC へのログイン（p.17-71）
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 1 をイネーブルにしてからルータ 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してください。

（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（メディア アクセス制御）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 進表記）には 8 ～ 24 文字の英数字（0 ～ 9、a ～ f）を使用できます。

d. **OK** をクリックして、Masked NSAP Entry（使用している場合）、Edit Manual Area Address、および OSI Router Editor の各ダイアログ 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-A540 その他のマニュアル 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。1 つのプライマリ マニュアル エリアおよび 2 つの追加マニュアル 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	DLP-A539 OSI ルータのプロビジョニング（p.22-49） DLP-A60 CTC へのログイン（p.17-71）
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　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 進表記）には 2 ～ 24 文字の英数字（0 ～ 9、a ～ f）を使用できます。

d. **OK** をクリックして、Masked NSAP Entry（使用している場合）、Add Manual Area Address、および OSI Router Editor の各ダイアログ 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-A541 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 サブネットワーク接続ポイ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-A60 CTC へのログイン（p.17-71）
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） DCC を作成すると、DCC 上で OSI サブネットワーク接続ポイントがイネーブルになります。「DLP-A377 SDCC 終端のプロビジョニング」（p.20-74）と「DLP-A378 LDCC 終端のプロビジョニング」（p.20-77）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 サブネットワーク接続ポイ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）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 の 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 Network Element Title（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 間の隣接を確立および維持します。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-A542 IP-Over-CLNS トンネルの作成

目的	この作業では、IP-over-CLNS 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 の通信を可能にします。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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。ONS 15454 にポイントを 1 つ作成します。もう 1 つは、通常、ルータや他の 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 — シスコ仕様の 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 — Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）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。

  シスコ仕様のトンネルでは、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 Open Shortest Path First（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。複数のトンネル ルートを作成し、異なる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、通常 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-A543 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-A60 CTC へのログイン（p.17-71）
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 手動隣接がノード グループとの唯一の通信手段である場合、隣接テーブル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-A544 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-A60 CTC へのログイン（p.17-71）
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、この手順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 Reference Manual*』にある「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 バッファを同じ設定に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。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せずに、LSP バッファを変更しないでください。

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 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 ノードとの通信方法は、IS L1/L2 ノードごとに異なります。
- **Intermediate System Level 1/Level 2** — ONS 15454 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、ノードが接続されている。
  - 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、ノードが接続されている。

（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 Reference Manual*』の「Management Network Connectivity」の章を参照してください。

ステップ 4　LSP 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-A545 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-A60 CTC へのログイン（p.17-71）
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-A546 OSI サブネットワーク接続ポイントの編集

目的	この作業では、OSI サブネット接続ポイントのパラメータを表示して、編集します。パラメータの初期プロビジョニングは、Section DCC（SDCC）、Line 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に行われます。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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 間の隣接を確立および維持します。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、またはイネーブル化するとき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場合は、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-A547 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-A542 IP-Over-CLNS トンネルの作成（p.22-52） DLP-A60 CTC へのログイン（p.17-71）
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 アドレスや 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の確認をとらずにネットワークアドレスを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 タイプを選択します。
  - **Cisco** — シスコ仕様の 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。

  シスコ仕様のトンネルでは、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。複数のトンネル ルートを作成し、異なる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、通常 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-A548 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-A60 CTC へのログイン（p.17-71）
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、接続を回復するために、現地でのプロビジョニングが必要になる場合があります。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-A549 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 トポロジー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-A60 CTC へのログイン（p.17-71）
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 サブネットワーク接続ポイ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 サブネットワーク接続ポイントを示します。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-A550 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-A60 CTC へのログイン（p.17-71）
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 サブネットワーク接続ポイ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 — 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 フィールドでその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-A551 TDC の管理

目的	この作業では、TDC を表示および管理します。TDC によって TID/NSAP マッピング リストを格納して、TARP 処理を容易にします。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン（p.17-71）
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 ターゲット ID です。ONS 15454 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 NSAP または NET です。
- Type — TDC エントリの作成方法を示します。
  - Dynamic — エントリは TARP 伝播プロセスを介して作成されました。
  - Static — エントリは手動で作成され、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 サブタブで TDC がイネーブルでない場合は、TID/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 が見つかった場合は、一致する NSAP が戻されます。見つからない場合、TARP はネットワークを介して PDU を送信します。[check TDC later] メッセージが表示され、あとで TDC に返信が返されます。

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　元の手順（NTP）に戻ります。

DLP-A552 JVM ヒープ サイズの調整

目的	この作業では、CTC パフォーマンスを向上させるため、Java Virtual Memory（JVM）のヒープ サイズをデフォルトの 256 MB から最大の 512 MB に調整します。
工具 / 機器	なし
事前準備手順	なし
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　［**スタート**］> ［**設定**］> ［**コントロール パネル**］をクリックします。Windows の［コントロール パネル］が表示されます。

ステップ 2　［**システム**］をダブルクリックします。［システムのプロパティ］ウィンドウが表示されます。

ステップ 3　［**詳細設定**］タブをクリックします。

ステップ 4　［**環境変数**］をクリックします。［環境変数］ウィンドウが表示されます。

ステップ 5　［ユーザー環境変数］領域で［**新規**］をクリックします。［新しいユーザー変数］ウィンドウが表示されます。

ステップ 6　［変数名］フィールドに「CTC_HEAP」と入力します。

ステップ 7　［変数値］フィールドに「512」と入力します。

ステップ 8　**OK** をクリックします。

ステップ 9　PC をリブートします。

ステップ 10　元の NTP（手順）に戻ります。

DLP-A556 ML シリーズ イーサネット カードのカード モードのプロビジョニング

目的	この作業では、ML シリーズ イーサネット カード（ML100T-12、ML1000-2、および ML100X-8）のカード モード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-A60 CTC へのログイン（p.17-71）
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、ML シリーズ イーサネット 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** > **Card** タブをクリックします。

ステップ 3　ML シリーズ イーサネット カードで、ドロップダウン Mode メニューからオプションを選択します。

- HDLC — High-Level Data Link Control（HDLC; ハイレベル データ リンク制御）（ほとんどのシスコ データ デバイスで標準的な VLAN トランキングをサポートしません）。
- GFP-F — Frame-mapped Generic Framing Procedure（GFP-F）である PDU を基にした適応モードで、クライアント フレームを GFP フレームにマップします。
- RPR 802.17 — IEE 準拠の 802.17 Resilient Packet Ring（RPR）

（注）　ONS イーサネット カードのインターオペラビリティの詳細については、『*Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*』を参照してください。

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。