



## Cisco ONS 15454 手順ガイド

Release 7.2  
2006 年 5 月



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 適合装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に適合していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 適合装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に適合していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコシステムズの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

- ・干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。
- ・テレビまたはラジオの左右どちらかの側に装置を移動させます。
- ・テレビまたはラジオから離れたところに装置を移動させます。
- ・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) パブリックドメインバージョンの一部として、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的に偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、The Fastest Way to Increase Your Internet Quotient、TransPath は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のもです。「パートナー」という用語を使用しているも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0601R)

このマニュアルで使用されている IP アドレスは、実際のアドレスを意図したものではありません。このマニュアルに含まれる例、コマンド表示出力、図は、例示のみを目的としています。例示の内容に実際の IP アドレスが使用されていたとしても、意図的に使用したのではなく、偶然に一致したものです。

Cisco ONS 15454 手順ガイド

Copyright © 2000–2006 Cisco Systems, Inc.

All rights reserved.



<b>このマニュアルについて</b>	<b>xxiii</b>
マニュアルの目的	xxiii
対象読者	xxiii
マニュアルの構成	xxiv
章 (ディレクタ レベル)	xxiv
DLP	xxiv
関連資料	xxv
表記法	xxvi
安全情報と警告情報の入手先	xxvi
マニュアルの入手方法	xxvii
Cisco.com	xxvii
Product Documentation DVD	xxvii
シスコ光ネットワーク製品の Documentation CD-ROM	xxvii
マニュアルの発注方法	xxvii
シスコ製品のセキュリティ	xxviii
シスコ製品のセキュリティ問題の報告	xxviii
テクニカル サポート	xxix
Cisco Technical Support & Documentation Web サイト	xxix
Japan TAC Web サイト	xxix
Service Request ツールの使用	xxx
問題の重大度の定義	xxx
その他の資料および情報の入手方法	xxx

**CHAPTER 1**

<b>シェルフおよびバックプレーン ケーブルの取り付け</b>	<b>1-1</b>
準備作業	1-1
必要な工具および機器	1-3
シスコが提供する部品	1-3
ユーザが準備する部品	1-3
必要な工具	1-4
テスト機器	1-4
NTP-A1 ONS 15454 シェルフ アセンブリの開梱と検査	1-5

NTP-A2 シェルフ アセンブリの設置	1-6
NTP-A3 前面扉のオープンと取り外し	1-7
NTP-A4 バックプレーン カバーの取り外し	1-8
NTP-A5 EIA の取り付け	1-9
NTP-A6 電源とアースの取り付け	1-11
NTP-A7 ファントレイ アセンブリの取り付け	1-13
NTP-A119 AEP の取り付け	1-15
NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線	1-18
NTP-A120 AEP への外付けワイヤラップ パネルの取り付け	1-19
NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け	1-23
NTP-A10 電気回路ケーブルの配線	1-24
NTP-A11 背面カバーの取り付け	1-25
NTP-A12 フェライトの取り付け	1-31
NTP-A13 シェルフ取り付けの受け入れテスト	1-32

CHAPTER 2

**カードおよび光ファイバケーブルの取り付け** 2-1

準備作業	2-1
NTP-A15 共通コントロール カードの取り付け	2-2
NTP-A16 光カードおよびコネクタの取り付け	2-8
NTP-A17 電気回路カードの取り付け	2-11
NTP-A246 イーサネット カードおよびコネクタの取り付け	2-13
NTP-A274 FC_MR-4 カードの取り付け	2-15
NTP-A316 フィラー カードの取り付け	2-17
NTP-A247 光ファイバケーブルの取り付け	2-18
NTP-A245 光ファイバケーブルの配線	2-22
NTP-A116 カードの取り外しおよび交換	2-23
NTP-A20 前面扉の交換	2-24

CHAPTER 3

**PC の接続と GUI へのログイン** 3-1

準備作業	3-1
NTP-A260 CTC 用コンピュータのセットアップ	3-2
NTP-A234 ONS 15454 へローカルにクラフト接続するための CTC コンピュータのセットアップ	3-4
NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ	3-6
NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ	3-7
NTP-A23 ONS 15454 GUI へのログイン	3-8

## CHAPTER 4

<b>ノードの起動</b>	<b>4-1</b>
準備作業	4-1
NTP-A323 カードの取り付けの確認	4-2
NTP-A30 ユーザの作成とセキュリティの割り当て	4-5
NTP-A25 名前、日付、時刻、連絡先情報の設定	4-6
NTP-A261 電力モニタ スレッシュホールドの設定	4-8
NTP-A169 CTC ネットワーク アクセスの設定	4-9
NTP-A27 ファイアウォール アクセスを目的とした ONS 15454 の設定	4-10
NTP-A28 タイミングの設定	4-11
NTP-A324 保護グループの作成	4-12
NTP-A256 SNMP の設定	4-15
NTP-A318 OSI のプロビジョニング	4-17

## CHAPTER 5

<b>ネットワークの起動</b>	<b>5-1</b>
準備作業	5-1
NTP-A35 ノードの起動の確認	5-3
NTP-A124 ポイントツーポイント ネットワークのプロビジョニング	5-5
NTP-A173 ポイントツーポイント ネットワークの受け入れテスト	5-6
NTP-A38 リニア ADM ネットワークのプロビジョニング	5-9
NTP-A174 リニア ADM ネットワークの受け入れテスト	5-11
NTP-A40 BLSR ノードのプロビジョニング	5-14
NTP-A126 BLSR の作成	5-16
NTP-A175 2 ファイバ BLSR の受け入れテスト	5-17
NTP-A176 4 ファイバ BLSR の受け入れテスト	5-20
NTP-A178 従来型 BLSR DRI のプロビジョニング	5-23
NTP-A179 統合 BLSR DRI のプロビジョニング	5-25
NTP-A44 UPSR ノードのプロビジョニング	5-27
NTP-A177 UPSR の受け入れテスト	5-29
NTP-A216 従来型 UPSR DRI のプロビジョニング	5-32
NTP-A217 統合 UPSR DRI のプロビジョニング	5-34
NTP-A180 従来型 BLSR/UPSR DRI のプロビジョニング	5-36
NTP-A209 統合 BLSR/UPSR DRI のプロビジョニング	5-38
NTP-A224 開放端 UPSR のプロビジョニング	5-40
NTP-A225 開放端 UPSR の受け入れテスト	5-42
NTP-A46 BLSR からの UPSR のサブテンディング	5-45
NTP-A47 UPSR からの BLSR のサブテンディング	5-47
NTP-A48 BLSR からの BLSR のサブテンディング	5-48
NTP-A172 論理ネットワーク マップの作成	5-50

回線と VT トンネルの作成

6-1

準備作業 6-1

NTP-A127 ネットワークの起動の確認 6-5

NTP-A181 自動ルーティングによる DS-1 回線の作成 6-8

NTP-A182 手動ルーティングによる DS-1 回線の作成 6-13

NTP-A183 ドロップが複数ある単方向 DS-1 回線の作成 6-17

NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成 6-22

NTP-A185 手動ルーティングによる DS-3 または EC-1 回線の作成 6-28

NTP-A186 ドロップが複数ある単方向 DS-3 または EC-1 回線の作成 6-31

NTP-A133 自動ルーティングによる VT トンネルの作成 6-35

NTP-A134 手動ルーティングによる VT トンネルの作成 6-38

NTP-A187 VAP の作成 6-40

NTP-A135 電気回線のテスト 6-44

NTP-A343 自動ルーティングによる光回線の作成 6-47

NTP-A344 手動ルーティングによる光回線の作成 6-54

NTP-A314 ドロップが複数ある単方向光回線の作成 6-58

NTP-A62 光回線のテスト 6-63

NTP-A139 BLSR または 1+1 ノードでの半回線の作成 6-65

NTP-A140 UPSR ノードでの半回線の作成 6-67

NTP-A191 E シリーズ EtherSwitch 回線の作成 (マルチカードまたはシングルカードモード) 6-69

NTP-A192 ポートマップモードの E シリーズ カード用回線の作成 6-73

NTP-A142 E シリーズ共有パケット リング イーサネット回線の作成 6-76

NTP-A143 E シリーズカードのハブアンドスポーク イーサネット構成の作成 6-79

NTP-A144 手動による E シリーズ シングルカード EtherSwitch クロスコネクットの作成 6-82

NTP-A145 手動による E シリーズ マルチカード EtherSwitch クロスコネクットの作成 6-85

NTP-A146 E シリーズ回線のテスト 6-89

NTP-A148 手動によるポートマップモードの G シリーズまたは E シリーズ カード用クロスコネクットの作成 6-91

NTP-A241 G シリーズ ポートをトランスポンダモードにするプロビジョニング 6-93

NTP-A149 G シリーズ回線のテスト 6-97

NTP-A264 自動ルーティングによる VCAT 回線の作成 6-99

NTP-A265 手動ルーティングによる VCAT 回線の作成 6-104

NTP-A194 オーバーヘッド回線の作成 6-107

NTP-A167 リングを対象にした STS テスト回線の作成 6-108

NTP-A326 サーバ証跡の作成 6-111

## CHAPTER 7

<b>回線の管理</b>	7-1
準備作業	7-1
NTP-A329 回線の検索と表示	7-2
NTP-A200 クロスコネク トカードのリソース使用率の表示	7-3
NTP-A151 回線の変更と削除	7-5
NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除	7-6
NTP-A78 モニタ回線の作成	7-7
NTP-A328 J0 セクション トレースの作成	7-9
NTP-A79 J1 パス トレースの作成	7-11
NTP-A293 J2 パス トレースの作成	7-12
NTP-A334 トラフィックのブリッジおよびロール	7-15
NTP-A298 回線の再設定	7-16
NTP-A301 回線のマージ	7-17
NTP-A325 VLAN の管理	7-18

## CHAPTER 8

<b>アラームの管理</b>	8-1
準備作業	8-1
NTP-A195 カード、ノード、およびネットワーク プロビジョニングの説明	8-2
NTP-A196 アラーム、履歴、イベント、および状態の表示	8-3
NTP-A68 クリアされたアラームの表示からの削除	8-4
NTP-A69 アラームの影響を受ける回線の表示	8-5
NTP-A70 ノード、スロット、またはポートの LCD のアラーム カウントの表示	8-6
NTP-A71 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	8-8
NTP-A168 アラーム重大度フィルタリングのイネーブル化、変更、またはディセーブル化	8-9
NTP-A72 アラーム抑制の開始と中止	8-10
NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング	8-11

## CHAPTER 9

<b>パフォーマンスのモニタリング</b>	9-1
準備作業	9-1
NTP-A253 PM カウントの表示変更	9-2
NTP-A122 電気回路カードのパフォーマンス モニタリング	9-3
NTP-A198 イーサネット カードのパフォーマンス モニタリング	9-5
NTP-A279 イーサネット RMON スレッシュホールドの作成または削除	9-6
NTP-A250 OC-N カードのパフォーマンス モニタリング	9-7
NTP-A285 FC_MR-4 カードのパフォーマンスのモニタリング	9-8
NTP-A289 FC_MR-4 RMON スレッシュホールドの作成または削除	9-8

CHAPTER 10

**カードの設定変更 10-1**

準備作業 10-1

NTP-A88 電気回路カードを対象にした回線設定と PM パラメータ スレッシュ  
ホールドの変更 10-2

NTP-A89 光カードを対象にした回線設定と PM パラメータ スレッシュホールド  
の変更 10-3

NTP-A118 AIC-I カードの設定変更 10-4

NTP-A91 DS-1 および DS-3 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 10-5

NTP-A315 FC\_MR-4 カードを対象にしたポート設定と PM パラメータ スレッ  
シュホールドの変更 10-6

NTP-A321 カードまたは PPM のサービス状態の変更 10-7

NTP-A322 PPM の管理 10-8

CHAPTER 11

**ノード設定の変更 11-1**

準備作業 11-1

NTP-A81 ノード管理情報の変更 11-2

NTP-A201 CTC ネットワーク アクセスの変更 11-3

NTP-A319 OSI プロビジョニングの変更 11-4

NTP-A202 CTC ネットワーク ビューのカスタマイズ 11-5

NTP-A203 カード保護設定の変更または削除 11-6

NTP-A292 通信チャンネルの終端とプロビジョニング可能なパッチコードの変更ま  
たは削除 11-7

NTP-A85 ノードのタイミング変更 11-8

NTP-A205 ユーザの変更とセキュリティの変更 11-9

NTP-A87 SNMP の設定変更 11-10

CHAPTER 12

**カードとスパンのアップグレード 12-1**

準備作業 12-1

NTP-A220 XCVT カードから XC10G カードへのアップグレード 12-2

NTP-A333 XCVT/XC10G カードから XC-VXC-10G カードへのアップグレード  
12-4

NTP-A296 TCC2 カードから TCC2P カードへのアップグレード 12-6

NTP-A93 DS3-12 カードから DS3-12E カードへのアップグレード 12-8

NTP-A308 低密度電気回路カードから高密度電気回路カードへのアップグレード  
12-10

NTP-A254 DS3-12E/DS3NE カードから DS3-12/DS3N-12 カードへのダウング  
レード 12-14

NTP-A94 OC-N カードおよびスパンの自動アップグレード 12-16

NTP-A95 OC-N スパンの手動アップグレード 12-20



## CHAPTER 13

**ネットワーク構成の変換 13-1**

- 準備作業 13-1
- NTP-A335 1+1 ポイントツーポイント型からリニア ADM への自動変換 13-2
- NTP-A154 1+1 ポイントツーポイント型からリニア ADM への手動変換 13-5
- NTP-A303 非保護ポイントツーポイント型または 1+1 リニア ADM から 2 ファイバ BLSR への自動変換 13-7
- NTP-A155 1+1 ポイントツーポイント型またはリニア ADM から 2 ファイバ BLSR への手動変換 13-10
- NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換 13-13
- NTP-A156 ポイントツーポイント型またはリニア ADM から UPSR への手動変換 13-15
- NTP-A267 UPSR から 2 ファイバ BLSR への自動変換 13-16
- NTP-A210 UPSR から 2 ファイバ BLSR への手動変換 13-19
- NTP-A211 2 ファイバ BLSR から 4 ファイバ BLSR への自動変換 13-21
- NTP-A159 BLSR の変更 13-23

## CHAPTER 14

**ノードの追加と削除 14-1**

- 準備作業 14-1
- NTP-A212 BLSR ノードの追加 14-2
- NTP-A240 BLSR ノードの削除 14-7
- NTP-A105 UPSR ノードの追加 14-11
- NTP-A294 UPSR ノードの削除 14-14
- NTP-A262 リニア ADM へのノードの追加 14-16
- NTP-A323 ウィザードによるリニア ADM へのノードの追加 14-18
- NTP-A313 リニア ADM からの稼働中のノードの削除 14-21

## CHAPTER 15

**ノードのメンテナンス 15-1**

- 準備作業 15-1
- NTP-A107 エアー フィルタの検査、清掃、および交換 15-3
- NTP-A108 データベースのバックアップ 15-6
- NTP-A109 データベースの復元 15-7
- NTP-A320 OSI 情報の表示および管理 15-11
- NTP-A163 ノードの出荷時の設定への復元 15-12
- NTP-A300 監査証跡レコードの表示 15-14
- NTP-A214 監査証跡レコードのオフロード 15-16
- NTP-A306 診断ファイルのオフロード 15-17
- NTP-A302 外部切り替えコマンドの開始またはクリア 15-18
- NTP-A112 ファイバ コネクタの清掃 15-20
- NTP-A332 CTC でのカードのリセット 15-21

NTP-A215 G シリーズ イーサネットのメンテナンス情報表示	15-22
NTP-A239 E シリーズ イーサネットのメンテナンス情報表示	15-23
NTP-A218 ノードのタイミング基準の変更	15-24
NTP-A223 ONS 15454 のタイミング レポート表示	15-25
NTP-A287 稼働中のクロスコネク ト カードの交換	15-28
NTP-A288 FTA の交換	15-30
NTP-A290 AIP の交換	15-33
NTP-A291 プラスチック製の下部バックプレーン カバーの取り付け	15-39
NTP-A162 UBIC-V EIA の交換	15-41
NTP-A336 NE のデフォルト値の編集	15-44
NTP-A337 NE のデフォルト値のインポート	15-46
NTP-A338 NE のデフォルト値のエクスポート	15-48

CHAPTER 16

**ノードの電源切断** 16-1

NTP-A114 ノードの電源切断	16-1
-------------------	------

CHAPTER 17

**DLP A1 ~ A99** 17-1

DLP-A1 シェルフ アセンブリの開梱と確認	17-1
DLP-A2 シェルフ アセンブリの検査	17-2
DLP-A3 19 インチ ( 482.6 mm ) ラックに適合させるためのマウント ブラケットの反転	17-2
DLP-A4 外部ブラケットおよびエアー フィルタの取り付け	17-4
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 )	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 )	17-6
DLP-A7 ラックへの複数のシェルフ アセンブリの取り付け	17-7
DLP-A8 前面扉のオープン	17-8
DLP-A9 前面扉の取り外し	17-9
DLP-A10 下部バックプレーン カバーの取り外し	17-10
DLP-A11 金属製バックプレーン カバーの取り外し	17-11
DLP-A12 BNC または高密度 BNC EIA の取り付け	17-12
DLP-A13 SMB EIA の取り付け	17-14
DLP-A14 AMP Champ EIA の取り付け	17-16
DLP-A16 ONS 15454 へのオフィス アースの接続	17-18
DLP-A17 ONS 15454 シェルフへのオフィス電源の接続	17-19
DLP-A18 オフィス電源の投入と検証	17-22
DLP-A19 バックプレーンへのアラーム ケーブルの取り付け	17-23
DLP-A20 バックプレーンへのタイミング ケーブルの取り付け	17-26
DLP-A21 バックプレーンへの LAN ケーブルの取り付け	17-27

DLP-A22 TL1 クラフト インターフェイスの取り付け	17-28
DLP-A23 電気インターフェイス アダプタ ( バラン ) を使用した DS-1 ケーブルの取り付け	17-29
DLP-A24 AMP Champ EIA への DS-1 AMP Champ ケーブルの取り付け	17-30
DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け	17-33
DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け	17-35
DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け	17-35
DLP-A28 同軸ケーブルの配線	17-37
DLP-A29 DS-1 ツイストペア ケーブルの配線	17-38
DLP-A30 電源コードへのフェライトの取り付け	17-39
DLP-A31 ワイヤラップ ピン フィールドへのフェライトの接続	17-40
DLP-A32 シェルフの取り付けおよび接続の検査	17-41
DLP-A33 電圧の測定	17-41
DLP-A34 最適化 1+1 保護グループの作成	17-42
DLP-A35 最適化 1+1 保護グループの変更	17-43
DLP-A36 TCC2/TCC2P カードの取り付け	17-44
DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け	17-47
DLP-A39 イーサネット カードの取り付け	17-49
DLP-A41 AIC-I カードの取り付け	17-50
DLP-A43 UPSR 構成での光ファイバ ケーブルの取り付け	17-51
DLP-A44 BLSR 構成での光ファイバ ケーブルの取り付け	17-55
DLP-A45 ファイバ ブーツの取り付け	17-57
DLP-A50 スタティック IP アドレスを使用して同一サブネット上の ONS 15454 にクラフト接続するための Windows PC の設定	17-58
DLP-A51 DHCP を使用して ONS 15454 にクラフト接続するための Windows PC の設定	17-61
DLP-A52 自動ホスト検出を使用して ONS 15454 にクラフト接続するための Windows PC の設定	17-63
DLP-A53 ONS 15454 にクラフト接続するための Solaris ワークステーションの設定	17-66
DLP-A54 CTC を使用した CE-100T-8 カードのハードリセット	17-68
DLP-A56 Internet Explorer によるプロキシ サービスのディセーブル化 ( Windows )	17-69
DLP-A57 Netscape によるプロキシ サービスのディセーブル化 ( Windows および UNIX )	17-70
DLP-A60 CTC へのログイン	17-71
DLP-A61 ログイン ノード グループの作成	17-74
DLP-A62 現在のセッションまたはログイン グループへのノードの追加	17-75
DLP-A64 LCD による IP アドレス、デフォルト ルータ、ネットワーク マスク	

の設定	17-76
DLP-A65 スタティック ルートの作成	17-78
DLP-A67 ONS 15454 での IOP リスナー ポートのプロビジョニング	17-79
DLP-A68 CTC コンピュータにおける IOP リスナー ポートのプロビジョニング	17-80
DLP-A69 外部タイミングまたはライン タイミングの設定	17-81
DLP-A70 内部タイミングの設定	17-84
DLP-A71 1:1 保護グループの作成	17-85
DLP-A72 1:N 保護グループの作成	17-86
DLP-A73 1+1 保護グループの作成	17-87
DLP-A74 新規ユーザの作成：単一ノード	17-89
DLP-A75 新規ユーザの作成：複数ノード	17-90
DLP-A83 オーダーワイヤのプロビジョニング	17-91
DLP-A88 1+1 光保護のテスト	17-92
DLP-A89 K3 バイトの再マップ	17-94
DLP-A91 BLSR 切り替えテスト	17-94
DLP-A92 4 ファイバ BLSR のスパン負荷テスト	17-99
DLP-A93 4 ファイバ BLSR のスパン切り替えテスト	17-101
DLP-A94 UPSR の保護切り替えテスト	17-103
DLP-A95 DS-1 回線の送信元と宛先のプロビジョニング	17-104
DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング	17-106
DLP-A97 OC-N 回線の送信元と宛先のプロビジョニング	17-107
DLP-A99 使用可能な VLAN の判別	17-108

## CHAPTER 18

**DLP A100 ~ A199** 18-1

DLP-A111 アラーム履歴のセッション エントリ最大数の変更	18-1
DLP-A112 時間帯に合わせたアラームおよび状態の表示	18-3
DLP-A113 アラームの同期	18-3
DLP-A114 状態の表示	18-4
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	18-6
DLP-A121 ポインタ位置調整カウンターの PM のイネーブル化またはディセーブル化	18-7
DLP-A122 IPPM のイネーブル化またはディセーブル化	18-9
DLP-A124 15 分間隔で行う PM カウントのリフレッシュ	18-11
DLP-A125 1 日間隔で行う PM カウントのリフレッシュ	18-12
DLP-A126 近端側の PM カウントの表示	18-13
DLP-A127 遠端側の PM カウントの表示	18-13
DLP-A129 現在の PM カウントのリセット	18-14
DLP-A131 回線の検索	18-15

DLP-A137 OC-N ポートでのパス トレースのプロビジョニング	18-16
DLP-A140 ノード名、日付、時刻、および連絡先情報の変更	18-17
DLP-A142 スタティック ルートの変更	18-18
DLP-A143 スタティック ルートの削除	18-18
DLP-A144 OSPF のディセーブル化	18-19
DLP-A145 ネットワーク ビューの背景色の変更	18-19
DLP-A148 ドメイン アイコンの作成	18-20
DLP-A149 ドメイン アイコンの管理	18-21
DLP-A150 1:1 保護グループの変更	18-22
DLP-A152 1:N 保護グループの変更	18-23
DLP-A154 1+1 保護グループの変更	18-24
DLP-A155 保護グループの削除	18-25
DLP-A156 SDCC 終端の削除	18-25
DLP-A157 ノードのタイミング ソースの変更	18-26
DLP-A158 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	18-27
DLP-A159 ユーザの削除：単一ノード	18-28
DLP-A160 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	18-29
DLP-A161 ユーザの削除：複数ノード	18-30
DLP-A163 SNMP トラップ宛先の削除	18-30
DLP-A165 DS1-14 または DS1N-14 カードの回線およびスレッシュホールドの設定変更	18-31
DLP-A166 DS3-12 または DS3N-12 カードの回線およびスレッシュホールドの設定変更	18-35
DLP-A167 DS3E-12 または DS3N-12E カードの回線およびスレッシュホールドの設定変更	18-39
DLP-A168 DS3XM-6 カードの回線およびスレッシュホールドの設定変更	18-43
DLP-A169 EC1-12 カードの回線およびスレッシュホールドの設定変更	18-47
DLP-A171 OC-N カードのスレッシュホールドの設定変更	18-50
DLP-A172 SDH への光ポートの変更	18-52
DLP-A176 DS1-14 カードの 1:1 保護から 1:N 保護への変換	18-53
DLP-A177 DS3-12 カードの 1:1 保護から 1:N 保護への変換	18-55
DLP-A178 DS3-12E カードの 1:1 保護から 1:N 保護への変換	18-57
DLP-A189 1+1 現用スロットがアクティブであることの確認	18-59
DLP-A190 UBIC-V EIA の取り付け	18-60
DLP-A191 カードの削除	18-65
DLP-A194 BLSR 強制リング切り替えのクリア	18-65

DLP-A195 縮小されたリングで使用されているタイミングの確認	18-66
DLP-A196 単一ノードからの BLSR の削除	18-67
DLP-A197 UPSR 強制切り替えの開始	18-68
DLP-A198 UPSR 強制切り替えのクリア	18-69

CHAPTER 19

**DLP A200 ~ A299** 19-1

DLP-A201 ロックオンの適用	19-1
DLP-A202 ロックアウトの適用	19-2
DLP-A203 ロックオンまたはロックアウトのクリア	19-3
DLP-A204 アルコールと乾いた布によるファイバ コネクタとアダプタの検査および清掃	19-4
DLP-A205 CLETOP によるファイバ コネクタの清掃	19-5
DLP-A206 ファイバ アダプタの清掃	19-5
DLP-A207 LGX インターフェイスへの光ファイバ ケーブルの取り付け	19-6
DLP-A208 AIC-I カードを使用した外部アラームの変更	19-7
DLP-A209 AIC-I カードを使用した外部制御の変更	19-8
DLP-A210 AIC-I カード オーダーワイヤ設定の変更	19-8
DLP-A212 UDC 回線の作成	19-9
DLP-A214 ポートのサービス状態の変更	19-10
DLP-A217 BLSR の試験リング テスト	19-12
DLP-A218 UPSR セレクタのプロビジョニング	19-14
DLP-A219 VT トンネル ルートのプロビジョニング	19-15
DLP-A220 E シリーズ イーサネット ポートのプロビジョニング	19-15
DLP-A221 VLAN メンバーシップ用の E シリーズ イーサネット ポートのプロビジョニング	19-17
DLP-A222 G シリーズ イーサネット ポートのプロビジョニング	19-18
DLP-A224 CTC を使用した CE-100T-8 カードのソフト リセット	19-19
DLP-A225 アラーム フィルタリングのイネーブル化	19-20
DLP-A227 アラーム フィルタリングのディセーブル化	19-21
DLP-A229 スパンにおける回線の表示	19-21
DLP-A230 回線のサービス状態の変更	19-22
DLP-A231 回線名の編集	19-24
DLP-A232 アクティブ スパンおよびスタンバイ スパンの色の変更	19-25
DLP-A233 UPSR 回線パス セレクタの編集	19-26
DLP-A241 BLSR 手動リング切り替えのクリア	19-27
DLP-A242 単一ノードでの BLSR の作成	19-28
DLP-A244 再初期化ツールの使用によるデータベースのクリアおよびソフトウェアのアップロード (Windows)	19-29
DLP-A245 再初期化ツールの使用によるデータベースのクリアおよびソフト	

ウェアのアップロード (UNIX)	19-31
DLP-A246 E シリーズ イーサネット カードのモードのプロビジョニング	19-32
DLP-A247 OC-N カードの変更	19-33
DLP-A249 IP 設定のプロビジョニング	19-35
DLP-A250 OSPF プロトコルの設定または変更	19-39
DLP-A251 RIP の設定または変更	19-41
DLP-A255 クロスコネク ト カードのサイド切り替えテスト	19-42
DLP-A256 イーサネット PM パラメータの表示：統計情報	19-44
DLP-A257 イーサネット PM パラメータの表示：使用率	19-44
DLP-A258 イーサネット PM パラメータの表示：履歴	19-45
DLP-A259 イーサネット PM カウントのリフレッシュ間隔の変更	19-46
DLP-A260 PM カウントの自動リフレッシュ間隔の設定	19-46
DLP-A261 別ポートの PM カウントのリフレッシュ	19-47
DLP-A262 回線表示のフィルタリング	19-48
DLP-A263 UPSR DRI 回線ホールドオフ タイマーの編集	19-50
DLP-A264 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	19-51
DLP-A265 ログイン時の法的免責事項の説明の変更	19-56
DLP-A266 IP 設定の変更	19-57
DLP-A268 ネットワーク ビューへのカスタム背景マップの適用	19-58
DLP-A269 ダイアログボックス非表示オプションのイネーブル化	19-59
DLP-A271 セキュリティ ポリシーの変更：単一ノード	19-60
DLP-A272 セキュリティ ポリシーの変更：複数ノード	19-61
DLP-A273 SNMP トラップ宛先の修正	19-63
DLP-A293 2 ファイバ BLSR での手動スパン アップグレード	19-64
DLP-A294 4 ファイバ BLSR での手動スパン アップグレード	19-66
DLP-A295 UPSR での手動スパン アップグレード	19-67
DLP-A296 1+1 保護グループでの手動スパン アップグレード	19-69
DLP-A297 非保護スパンでの手動スパン アップグレード	19-70
DLP-A298 ネットワーク上のアラームおよび状態のチェック	19-71
DLP-A299 BLSR スパン ロックアウトの開始	19-72

## CHAPTER 20

**DLP A300 ~ A399** 20-1

DLP-A300 BLSR スパン ロックアウトのクリア	20-1
DLP-A301 BLSR 手動リング切り替えの開始	20-2
DLP-A303 BLSR 強制リング切り替えの開始	20-3
DLP-A309 イーサネット MAC アドレス テーブルの表示	20-4
DLP-A310 イーサネット トランクの使用率の表示	20-5

DLP-A311 BLSR または 1+1 構成での半回線の送信元と宛先のプロビジョニング	20-5
DLP-A312 UPSR での半回線の送信元と宛先のプロビジョニング	20-6
DLP-A313 DCC トンネルの作成	20-7
DLP-A314 ポートへの名前の割り当て	20-9
DLP-A315 ユーザのログアウト：単一ノード	20-9
DLP-A316 ユーザのログアウト：複数ノード	20-10
DLP-A320 ML シリーズ PM パラメータの表示：イーサネット ポート	20-11
DLP-A321 ML シリーズ PM パラメータの表示：POS ポート	20-12
DLP-A322 ノードで使用するタイミング基準の手動または強制切り替え	20-14
DLP-A323 ノードで使用するタイミング基準の手動または強制切り替えのクリア	20-14
DLP-A324 VCAT 回線の送信元と宛先のプロビジョニング	20-15
DLP-A325 VCAT 回線ルートのプロビジョニング	20-16
DLP-A326 BLSR のノード ID の変更	20-17
DLP-A327 CTC Alerts ダイアログボックスの自動ポップアップ設定	20-18
DLP-A328 BLSR ウィザードによる 2 ファイバ BLSR の作成	20-19
DLP-A329 2 ファイバ BLSR の手動作成	20-21
DLP-A330 カード スロットの事前プロビジョニング	20-22
DLP-A332 トンネル タイプの変更	20-22
DLP-A333 回線の削除	20-23
DLP-A334 オーバーヘッド回線の削除	20-25
DLP-A335 VLAN の削除	20-26
DLP-A336 IP トンネルの修復	20-26
DLP-A337 Windows での CTC インストール ウィザードの実行	20-27
DLP-A338 UNIX での CTC インストール ウィザードの実行	20-31
DLP-A339 現在のセッションまたはログイン グループからのノードの削除	20-34
DLP-A340 LCD でのポート ステータスの表示	20-35
DLP-A341 IP カプセル化トンネルの作成	20-36
DLP-A347 E シリーズおよび G シリーズイーサネットカードの PM カウントのリフレッシュ	20-37
DLP-A348 選択した信号の PM カウントのモニタ	20-38
DLP-A349 選択した PM カウントのクリア	20-40
DLP-A350 FC_MR-4 PM パラメータの表示：統計情報	20-41
DLP-A351 FC_MR-4 PM パラメータの表示：使用率	20-42
DLP-A352 FC_MR-4 PM パラメータの表示：履歴	20-43
DLP-A353 FC_MR-4 PM カウントのリフレッシュ間隔の変更	20-44



DLP-A356 TCC2/TCC2P カードのアクティブ / スタンバイ切り替えテスト 20-45	
DLP-A357 FC_MR-4 RMON アラーム スレッシュホールドの作成	20-46
DLP-A358 FC_MR-4 RMON アラーム スレッシュホールドの削除	20-50
DLP-A359 LDCC 終端の削除	20-50
DLP-A362 BLSR ウィザードによる 4 ファイバ BLSR の作成	20-51
DLP-A363 4 ファイバ BLSR の手動作成	20-53
DLP-A364 CTC による TCC2/TCC2P カードのリセット	20-54
DLP-A365 光保護切り替えの開始	20-55
DLP-A366 電気保護切り替えの開始	20-56
DLP-A367 プロビジョニング可能なパッチコードの作成	20-56
DLP-A368 プロビジョニング可能なパッチコードの削除	20-58
DLP-A369 OC-N 回線ルートのプロビジョニング	20-59
DLP-A371 パススルー接続の削除	20-61
DLP-A372 指定したログイン ノード グループからのノードの削除	20-62
DLP-A373 MiniBNC EIA の取り付け	20-63
DLP-A374 SDCC 終端の変更	20-66
DLP-A375 LDCC 終端の変更	20-67
DLP-A376 DS1/E1-56 カードの回線およびスレッシュホールドの設定変更 20-68	
DLP-A377 SDCC 終端のプロビジョニング	20-74
DLP-A378 LDCC 終端のプロビジョニング	20-77
DLP-A379 OC-N カードの回線の伝送設定の変更	20-78
DLP-A380 プロキシ トンネルのプロビジョニング	20-82
DLP-A381 ファイアウォール トンネルのプロビジョニング	20-83
DLP-A382 プロキシ トンネルの削除	20-84
DLP-A383 ファイアウォール トンネルの削除	20-84
DLP-A384 VCAT 回線へのメンバーの追加	20-85
DLP-A385 VCAT 回線からのメンバーの削除	20-89
DLP-A386 UBIC-V EIA での電気回路ケーブルの取り付け	20-90
DLP-A387 DS3XM-12 カードの回線およびスレッシュホールドの設定変更 20-94	
DLP-A388 DS3/EC1-48 カードの回線およびスレッシュホールドの設定変更 20-98	
DLP-A390 アラームの表示	20-102
DLP-A391 CE シリーズ PM パラメータの表示 : イーサネット ポートおよび POS ポートの統計情報	20-103
DLP-A392 CE シリーズ PM パラメータの表示 : イーサネット ポートおよび POS ポートの使用率	20-105
DLP-A393 CE シリーズ PM パラメータの表示 : イーサネット ポートおよび	

POS ポートの履歴	20-106
DLP-A394 DS3XM-12 カード PM パラメータの表示 : DS-N/SONET	20-108
DLP-A395 DS3XM-12 カード PM パラメータの表示 : BFDL	20-109
DLP-A397 手動ルーティングによる UPSR 回線のトポロジーマップアップグレード	20-111
DLP-A398 自動ルーティングによる UPSR 回線のトポロジーマップアップグレード	20-111
DLP-A399 UBIC-H EIA の取り付け	20-113

CHAPTER 21

**DLP A400 ~ A499** 21-1

DLP-A412 DCU シェルフ アセンブリの取り付け	21-1
DLP-A416 回線情報の表示	21-2
DLP-A418 公開鍵セキュリティ証明書のインストール	21-5
DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング	21-6
DLP-A422 BLSR の拡張バイト マッピングの確認	21-7
DLP-A428 1+1 構成での光ファイバ ケーブルの取り付け	21-8
DLP-A430 スパニングツリー情報の表示	21-9
DLP-A431 JRE バージョンの入れ替え	21-10
DLP-A433 ノードのセキュア モードのイネーブル化	21-10
DLP-A434 ノード セキュリティのロック	21-12
DLP-A435 セキュア モードのバックプレーン ポートの IP 設定の修正	21-13
DLP-A436 ノードのセキュリティ モードのディセーブル化	21-14
DLP-A437 VCAT メンバーのサービス状態の変更	21-16
DLP-A438 FC_MR-4 カードにある汎用ポートの設定変更	21-17
DLP-A439 FC_MR-4 カードにあるポートの距離延長設定の変更	21-19
DLP-A440 FC_MR-4 カードにあるポートの拡張 FC/FICON 設定の変更	21-21
DLP-A441 UBIC-H EIA での電気回路ケーブルの取り付け	21-22
DLP-A442 パススルー回線の確認	21-24
DLP-A443 15454_MRC-12 カードへのファイバクリップの取り付け	21-25
DLP-A444 MRC-12 カードでの PPM のプロビジョニング	21-27
DLP-A445 MRC-12 カードでの光回線レートのプロビジョニング	21-28
DLP-A446 MRC-12 カードでの光回線レートの変更	21-29
DLP-A447 MRC-12 または OC192-XFP カードからの PPM の削除	21-29
DLP-A448 DS3XM-6 カードまたは DS3XM-12 カードの 1:1 保護から 1:N 保護への変換	21-30
DLP-A449 GNE 対応 SNMP の設定	21-32
DLP-A450 ENE 対応 SNMP の設定	21-34

DLP-A451 SNMP コマンドまたは演算用の NMS コミュニティ スtringのフォーマット化および入力	21-36
DLP-A452 VLAN の作成	21-37
DLP-A453 サーバ証跡の削除	21-38
DLP-A454 BLSR STS スケルチ テーブルの表示	21-38
DLP-A455 BLSR VT スケルチ テーブルの表示	21-40
DLP-A456 ノードへの RADIUS 認証の設定	21-41
DLP-A457 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	21-43
DLP-A459 OC-192 および MRC-12 カードの光スレッシュホールド設定の変更	21-44
DLP-A460 CTC でのトラフィック カードのリセット	21-46
DLP-A461 SFP または XFP デバイスの事前プロビジョニング	21-47
DLP-A462 アクティブ ログインの表示および終了	21-48
DLP-A463 特定の光回線の送信元または宛先のロール	21-49
DLP-A464 光回線間での単一クロスコネクットのロール	21-52
DLP-A465 自動ルーティングを使用した単一光回線への 2 つのクロスコネクットのロール	21-54
DLP-A466 手動ルーティングを使用した単一光回線への 2 つのクロスコネクットのロール	21-58
DLP-A467 光回線間での 2 つのクロスコネクットのロール	21-61
DLP-A468 ロールの削除	21-63
DLP-A469 GBIC または SFP/XFP デバイスの取り付け	21-64
DLP-A470 GBIC または SFP/XFP デバイスの取り外し	21-68
DLP-A489 ロールのキャンセル	21-69
DLP-A495 ネットワーク ビューでのリンクの統合	21-69
DLP-A498 TDM と DWDM のネットワーク ビューの切り替え	21-73

## CHAPTER 22

**DLP A500 ~ A599** 22-1

DLP-A507 OC-N PM パラメータの表示	22-1
DLP-A509 CE-1000-4 イーサネット ポートのプロビジョニング	22-3
DLP-A510 DS-3 回線の送信元と宛先のプロビジョニング	22-4
DLP-A512 ノード アクセスと PM クリア権限の変更	22-5
DLP-A513 CE-100T-8 イーサネット ポートのプロビジョニング	22-7
DLP-A514 CE-100T-8 および CE-1000-4 POS ポートのプロビジョニング	22-8
DLP-A517 アラーム履歴またはイベント履歴の表示	22-9
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	22-11
DLP-A519 アラーム プロファイルのポートへの適用	22-15
DLP-A520 アラーム重大度プロファイルの削除	22-17
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	22-18

DLP-A522	アラーム レポートの抑制	22-21
DLP-A523	アラーム抑制の中止	22-22
DLP-A524	アラーム重大度プロファイルのダウンロード	22-23
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	22-25
DLP-A527	OC-N カード ALS メンテナンス設定の変更	22-29
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	22-31
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	22-32
DLP-A530	固定棒の取り付け	22-33
DLP-A531	CTC データの印刷	22-34
DLP-A532	CTC データのエクスポート	22-35
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	22-37
DLP-A534	OSI ルーティング モードのプロビジョニング	22-43
DLP-A535	TARP 動作パラメータのプロビジョニングまたは変更	22-45
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	22-47
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	22-48
DLP-A538	TARP MAT エントリの追加	22-48
DLP-A539	OSI ルータのプロビジョニング	22-49
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	22-50
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	22-51
DLP-A542	IP-Over-CLNS トンネルの作成	22-52
DLP-A543	TARP MAT エントリの削除	22-53
DLP-A544	OSI ルーティング モードの変更	22-54
DLP-A545	OSI ルータ設定の編集	22-55
DLP-A546	OSI サブネットワーク接続ポイントの編集	22-56
DLP-A547	IP-Over-CLNS トンネルの編集	22-57
DLP-A548	IP-Over-CLNS トンネルの削除	22-58
DLP-A549	IS-IS RIB の表示	22-58
DLP-A550	ES-IS RIB の表示	22-59
DLP-A551	TDC の管理	22-60
DLP-A552	JVM ヒープ サイズの調整	22-61
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	22-62

CTC ウィンドウの管理	A-5
CTC のメニューとツールバーのオプション	A-5
CTC マウス オプション	A-9
ノード ビューのショートカット	A-10
ネットワーク ビューで行う作業	A-11
テーブル表示オプション	A-12
装置インベントリ	A-13





# このマニュアルについて

---

ここでは、このマニュアルの目的、対象読者、構成、表記法、およびその他の情報を説明します。  
ここでは、次の内容について説明します。

- [マニュアルの目的](#)
- [対象読者](#)
- [マニュアルの構成](#)
- [関連資料](#)
- [表記法](#)
- [安全情報と警告情報の入手先](#)
- [マニュアルの入手方法](#)
- [シスコ製品のセキュリティ](#)
- [テクニカル サポート](#)
- [その他の資料および情報の入手方法](#)

## マニュアルの目的

このマニュアルでは、ONS 15454 ノードおよび ONS 15454 ネットワークの設置、起動、プロビジョニング、受け入れの手順を説明します。

## 対象読者

このマニュアルを使用するには、シスコまたは同等の光伝送ハードウェア製品とそのケーブル接続、テレコミュニケーションハードウェアとそのケーブル接続、電気回路とその配線に精通している必要があります。また、電子通信技術者としての経験があることが望まれます。

## マニュアルの構成

このマニュアルの構成には、シスコが推奨する新しいインストレーションワークフローが反映されています。また、既存のインストレーションの修正に使用する手順と作業も簡単に参照できるようになっています。契約ベンダーが物理的な設置を完了してから、検証、プロビジョニング、起動、および受け入れを実行する技術担当者に実際の設置場所を任せることができるよう、必要に応じて検証手順を示します。

このマニュアルの前付は、次の順番で示されます。

1. タイトル ページ
2. 目次
3. 図のリスト
4. 表のリスト
5. 手順のリスト
6. 作業のリスト

このマニュアルの情報は、次に説明する要素を使用して、作業内容に基づいて階層表示されています。

## 章 (ディレクタ レベル)

このマニュアルは、手順内のディレクタ エントリの機能を果たす論理作業グループ (章) で構成されています。たとえば、請負業者がシェルフ ハードウェアを設置したあとに設置場所に到着したユーザは、第 2 章「カードおよび光ファイバ ケーブルの取り付け」へ進み、設置の検証とカードの取り付けを行います。作業は章の順序に従って進めるか (推奨)、各章の最初のページに示される手順のリストから実行する作業を選択する (あるいは目次または索引を参照する) こともできます。

各 Non-Trouble Procedure (NTP; 手順) は、特定の手続きを完了するためのステップのリストです。各ステップを実行して、手順を完了してください。詳細な作業指示が必要な場合は、手順に指定されている Detailed-Level Procedure (DLP; 作業) を参照してください。



(注)

このマニュアルでは、NTP を「手順」と呼び、DLP を「作業」と呼びます。各手順への参照には NTP 番号が示されています。また、各作業への参照には DLP 番号が示されています。

## DLP

DLP は、NTP を実行する際に必要となる詳細な作業内容です。DLP では、ステップを順に実行すると作業を完了することができます。一部のステップでは、確認のために機器の表示を調べる必要があります。機器が正しく応答しない場合のために、問題を解決するためのリファレンスが示されています。



## 関連資料

『Cisco ONS 15454 手順ガイド』は、次の関連マニュアルと併せて参照してください。

- 『Cisco ONS 15454 Reference Manual』  
カードの仕様、ハードウェアおよびソフトウェア機能の説明、ネットワーク トポロジー情報、およびネットワーク要素の詳細を示します。
- 『Cisco ONS 15454 Troubleshooting Guide』  
アラームの説明、アラームと一般的なトラブルシューティング手順、エラー メッセージ、および一時的な状態を示します。
- 『Cisco ONS SONET TL1 Command Guide』  
Cisco ONS 15454、ONS 15327、ONS 15600、ONS 15310-CL、および ONS 15310-MA システムのパラメータ、AID、条件、修飾子など、完全な TL1 コマンドおよび自律メッセージ セットのリストを示します。
- 『Cisco ONS SONET TL1 Reference Guide』  
Cisco ONS 15454、ONS 15327、ONS 15600、ONS 15310-CL、および ONS 15310-MA システムでの TL1 に関する一般情報、手順、およびエラーを示します。
- 『Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327』  
すべてのイーサネット カードのソフトウェア機能、および ML シリーズ カードの Cisco IOS 設定情報を示します。
- 『Release Notes for the Cisco ONS 15454 Release 7.2』  
注意事項、解決済みの問題、新機能および機能に関する情報が記載されています。

廃止および販売終了に関する注意事項の更新については、

[http://cisco.com/en/US/products/hw/optical/ps2006/prod\\_eol\\_notices\\_list.html](http://cisco.com/en/US/products/hw/optical/ps2006/prod_eol_notices_list.html) を参照してください。

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが入力する引数は、イタリック体で示しています。
[ ]	角カッコ内の要素は、省略可能です。
{ x   x   x }	どれかを選択しなければならないキーワード (x の部分) は、波カッコで囲み、縦棒で区切って示しています。ユーザはこの中からキーワードを 1 つ選択する必要があります。
Ctrl	Ctrl キーを表します。たとえば、Ctrl+D の場合は、Ctrl キーを押しながら D キーを押すことを表します。
screen フォント	画面に表示される情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
< >	モジュール固有のコードで置き換える必要があるコマンドパラメータを表します。



(注) 「注釈」です。役立つ情報やこのマニュアル以外の参照資料などを紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

これらの注意事項を保存しておいてください。

## 安全情報と警告情報の入手先

安全情報と警告情報については、本製品に付属している『Cisco Optical Transport Products Safety and Compliance Information』を参照してください。このマニュアルでは、Cisco ONS 15454 システムの国際機関への準拠性および安全性に関する情報を説明しています。このマニュアルには、ONS 15454 システムのマニュアルに示されている安全に関する警告の各国語訳も含まれています。

## マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

### Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

<http://www.cisco.com/jp>

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルの総合的なライブラリです。DVD では、シスコのハードウェアおよびソフトウェア製品のインストール、設定、コマンド ガイドの複数バージョンにアクセスできます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じ HTML 形式のマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単一製品として、またはサブスクリプションとして入手できます。Cisco.com ( Cisco Direct Customers ) に登録されている場合、次の URL の Cisco Marketplace から Product Documentation DVD ( Customer Order Number DOC-DOCDVD= または DOC-DOCDVD=SUB ) を発注できます。

<http://www.cisco.com/go/marketplace/>

### シスコ光ネットワーク製品の Documentation CD-ROM

Cisco ONS 15xxx 製品のマニュアルを含む、光ネットワーク関連のマニュアルは、製品に付属の CD-ROM パッケージでご利用いただけます。光ネットワーク製品の Documentation CD-ROM は、定期的に更新されるので、印刷資料よりも新しい情報が得られます。

### マニュアルの発注方法

Cisco.com に登録されている場合、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

<http://www.cisco.com/go/marketplace/>

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

## シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトから、次の手順についての情報を検索できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告、セキュリティの注意事項、およびセキュリティ応答のリストが次の URL で確認できます。

<http://www.cisco.com/go/psirt>

セキュリティ勧告、セキュリティの注意事項、およびセキュリティの応答の更新をリアルタイムで参照するには、Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードを購読してください。PSIRT RSS フィードの購読方法に関する情報は、次の URL で確認できます。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 — [security-alert@cisco.com](mailto:security-alert@cisco.com)  
緊急度の高い問題とは、システムが激しい攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 — [psirt@cisco.com](mailto:psirt@cisco.com)

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532



### ヒント

お客様が第三者に知られたくない情報をシスコに送信する場合、Pretty Good Privacy (PGP) または PGP と互換性のある製品(たとえば GnuPG)を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.x ~ 9.x で暗号化した情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の URL の Security Vulnerability Policy ページの Contact Summary でリンクされている有効な公開鍵を使用してください。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このページのリンクには、現在使用中の PGP キー ID があります。

PGP を所有していない、または使用しない場合は、機密情報をお送りになる前に、前述の電子メールアドレスまたは電話番号で PSIRT に連絡し、別のデータ暗号化方法をご利用ください。

## テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center (TAC) のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

### Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。この Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

<http://www.cisco.com/techsupport>

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification (CPI) ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Documentation Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する show コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

### Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register/>

## Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカルサポートを受けられます(ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合)。状況をご説明いただくと、TAC Service Request ツールが推奨される解決方法を自動的に提供します。これらの推奨リソースを使用しても問題が解決しない場合は、シスコの技術者が対応します。TAC Service Request ツールは次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください(運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合)。S1 および S2 の問題にはシスコの技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカルサポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋 : +61 2 8446 7411 (オーストラリア : 1 800 805 227)

EMEA : +32 2 704 55 55

米国 : 1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

<http://www.cisco.com/techsupport/contacts>

## 問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

重大度 1 (S1) — ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

重大度 2 (S2) — ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

重大度 3 (S3) — ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

重大度 4 (S4) — シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

## その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- 『Cisco Product Quick Reference Guide』は、チャネル パートナー経由で販売されているほとんどのシスコ製品に関する簡単な製品概要、重要機能、サンプル部品番号、および簡単な技術仕様が掲載された、手軽で小型の参照ツールです。年に 2 回更新され、シスコが提供する最新情報が収録されます。『Cisco Product Quick Reference Guide』についての詳細および注文方法は、次の URL をご覧ください。

<http://www.cisco.com/go/guide>

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com>

- 『Packet』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『Packet』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

- 『iQ Magazine』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

または次の URL でデジタル版をご覧ください。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>

- シスコシステムズが提供するネットワーク製品およびカスタマー サポート サービスについては、次の URL にアクセスしてください。

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection は、ネットワークング専門家がネットワークング製品やネットワークング技術に関する質問、提案、情報をシスコの専門家および他のネットワークング専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

<http://www.cisco.com/discuss/networking>

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>







# シェルフおよびバックプレーン ケーブルの取り付け

この章では、Cisco ONS 15454 の設置手順を示します。設置に必要な工具と機器の概要については、「必要な工具および機器」(p.1-3) を参照してください。

## 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A1 ONS 15454 シェルフ アセンブリの開梱と検査 \(p.1-5\)](#)— 「[NTP-A2 シェルフ アセンブリの設置 \(p.1-6\)](#)」へ進む前に、この手順を実行します。
2. [NTP-A2 シェルフ アセンブリの設置 \(p.1-6\)](#)— ラックにシェルフ アセンブリを設置する場合は、この手順を実行します。
3. [NTP-A3 前面扉のオープンと取り外し \(p.1-7\)](#)— 機器を使用できるようにする場合は、他の手順へ進む前に、この手順を実行します。
4. [NTP-A4 バックプレーン カバーの取り外し \(p.1-8\)](#)— バックプレーンを使用できるようにする場合は、他の手順へ進む前に、この手順を実行します。
5. [NTP-A5 EIA の取り付け \(p.1-9\)](#)— 電気回路カードを取り付ける計画がある場合は、この手順を実行します。この手順は、「[NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け \(p.1-23\)](#)」を行う場合は必ず実行します。
6. [NTP-A6 電源とアースの取り付け \(p.1-11\)](#)— 「[NTP-A7 ファントレイ アセンブリの取り付け \(p.1-13\)](#)」へ進む前に、この手順を実行します。
7. [NTP-A7 ファントレイ アセンブリの取り付け \(p.1-13\)](#)— シェルフにファントレイ アセンブリを取り付ける場合は、この手順を実行します。
8. [NTP-A119 AEP の取り付け \(p.1-15\)](#)— 取り付けようとしている Alarm Interface Controller-International (AIC-I) カードのアラーム コンタクト数を増やす場合は、この手順を実行します。
9. [NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線 \(p.1-18\)](#)— ワイヤラップ ピン接続を設定する場合は、必要に応じてこの手順を実行します。
10. [NTP-A120 AEP への外付けワイヤラップ パネルの取り付け \(p.1-19\)](#)— 外付けワイヤラップ パネルを Alarm Expansion Panel (AEP) に接続する場合は、この手順を実行します。
11. [NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け \(p.1-23\)](#)— 電気回路カード ケーブルを取り付ける計画がある場合は、この手順を実行します。

12. [NTP-A10 電気回路ケーブルの配線 \(p.1-24\)](#)— バックプレーンに取り付けられた電気回路ケーブルを配線する場合は、必要に応じてこの手順を実行します。
13. [NTP-A11 背面カバーの取り付け \(p.1-25\)](#)— 背面カバーを取り付ける場合は、この手順を実行します。
14. [NTP-A13 シェルフ取り付けの受け入れテスト \(p.1-32\)](#)— この章の他のすべての手順を正しく実行したかどうかを確認する場合は、この手順を実行します。

**警告**

この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

**警告**

この装置は、出入りが制限された場所に設置されることを想定しています。出入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段によって、保守担当者以外の侵入が禁止されている区域のことです。出入りが制限された場所は、責任者が管理します。

**警告**

設置場所として適しているのは、コンクリートなど不燃性の接地面のみです。

**警告**

カバーは製品の安全設計に必要な部品です。カバーを外した状態で装置を稼働させないでください。

## 必要な工具および機器

ONS 15454 を設置およびテストするには、次の工具と機器が必要です。

### シスコが提供する部品

次の部品は、ONS 15454 シェルフに付属している必須の部品です（プラスチックで保護されています）。カッコ内の数字は、パッケージに付属の各部品の数量を示します。

- #12-24 x 3/4 プラス ヘッド ネジ (48-1004-XX、48-1007-XX)(8)
- #12-24 x 3/4 ソケット固定ネジ (48-1003-XX)(2)
- 固定ネジ用 T ハンドル #12-24 六角レンチ (1)
- 1.8 m (6 フィート) の静電気防止用リストストラップ (1)
- タイラップ (10)
- 前面扉用ピン付き六角 (アレン) キー (1)
- スペーサ (50-1193-XX)(4)
- スペーサ マウント ブラケット (2)
- クリア プラスチック背面カバー (1)
- ファントレイ エアー フィルタ用の外付け (底部) ブラケット
- シェルフ アクセサリ キット (53-2329-XX)(オプション)
  - 取り付けバー (700-19701-XX)(2)
  - 1 インチ スタンドオフ (50-1193-01)(4)
  - 1 3/8 インチ スタンドオフ (50-1492-01)(4)
  - 2 インチ スタンドオフ (50-1453-01)(8)
  - 6-32 x 0.5 のフラットヘッド ネジ (48-2116-01)(4)
- スタンドオフキット (53-0795-XX)
  - プラスチック ファイバ マネジメント ガイド (2)
  - ファン フィルタ ブラケット ネジ (53-48-0003)(6)

オプションのエアー ランプを取り付ける場合は、次の部品が必要です。カッコ内の数字は、パッケージに付属の各部品の数量を示します。

- M4.0 x 8mm の SS プラスチックベネジ (2)
- 19 インチ (482.6 mm)、23 インチ (584.2 mm) のマウント ブラケット (2)

### ユーザが準備する部品

次の部品や工具が必要ですが、これらは ONS 15454 には付属していません。

- 次に示す装置ラック (1 つまたは複数)
  - 19 インチ ANSI 標準 (Telcordia GR-63-CORE)(482.6 mm) ラック (合計幅 22 インチ [558.8 mm])
  - 23 インチ ANSI 標準 (Telcordia GR-63-CORE)(584.2 mm) ラック (合計幅 26 インチ [660.4 mm])
- ヒューズ パネル
- 電源コード (ヒューズ アラーム パネルからアセンブリまで) #10 AWG、銅コンダクタ、90°C (194°F)



(注) 15454-SA-NEBS3E、15454-SA-NEBS3、または 15454-SA-R1 に電源装置を取り付ける場合は、部品番号 800-07149 のシェルフ アセンブリ、#10 ~ #12 AWG 電源コードが必要です。

- ストランドアースケーブル #6 AWG



(注) 15454-SA-NEBS3E、15454-SA-NEBS3、または 15454-SA-R1 に電源装置を取り付ける場合は、部品番号 800-07149 のシェルフ アセンブリ、#10 AWG アースケーブルが必要です。

- すべてのアラーム接続用のアラーム ケーブル ペア、#22 または #24 AWG( 0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup> )、メッキ済み
- 100 シールド付き Building Integrated Timing Supply ( BITS ) クロック ケーブル ペア #22 または #24 AWG ( 0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup> ) ツイストペア T1 タイプ
- 光 ( OC-N ) カードの UPC 光沢剤 ( 55 dB 以上 ) を含むシングル モード SC ファイバジャンパ
- SMB または BNC コネクタで終端された、DS-3 カード用シールド付き同軸ケーブル
- #22 または #24 AWG ( 0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup> ) アース ケーブルを含む、AMP Champ コネクタで終端された ( DS1N-14 カードの場合、終端されていない ) シールド付き ABAM ケーブル ( 通常、長さは約 2 フィート [61 cm] )
- 6 ペア #29 AWG 二重シールド ケーブル
- タイラップまたは締めひも
- ラベル
- リストされている圧着端子コネクタ ( 通常はデュアル端子タイプ )。コネクタは、スタッド サイズおよび間隔が装置ラックの仕様に基づく #6 AWG 銅コンダクタに適したものを使用する必要があります。オフィス アース接続には、通常、現地の規約に従って H-TAP 圧着コネクタを使用します。

## 必要な工具

ONS 15454 を取り付ける場合は、次の工具が必要です。

- #2 プラス ドライバ
- 中型スロット ヘッド ネジ用ドライバ
- 小型スロット ヘッド ネジ用ドライバ
- ワイヤ ラッパー
- ワイヤ カッター
- ワイヤ ストリッパ
- 圧着工具
- BNC 取り付け工具

## テスト機器

ONS 15454 を取り付ける場合は、次のテスト機器が必要です。

- 電圧計
- 光パワーメータ ( 光ファイバの場合だけ使用 )
- BER ( ビット エラー レート ) テスター、DS-1 および DS-3

## NTP-A1 ONS 15454 シェルフ アセンブリの開梱と検査

目的	この手順では、ONS 15454 の梱包を解き、内容を確認します。
工具 / 機器	前面扉用ピン付き六角（アレン）キー
事前準備手順	なし
必須 / 適宜	必須
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)** ONS 15454 高密度シェルフ (15454-SA-HD) は、高密度電気回路カード (DS3/EC1-48 および DS1/E1-56 カード) を使用する場合に必要です。

- 
- ステップ 1** 「[DLP-A1 シェルフ アセンブリの開梱と確認](#)」(p.17-1) を実行します。
- ステップ 2** 「[DLP-A2 シェルフ アセンブリの検査](#)」(p.17-2) を実行します。
- ステップ 3** 「[NTP-A2 シェルフ アセンブリの設置](#)」(p.1-6) へ進んでください。

終了：この手順は、これで完了です。

---

## NTP-A2 シェルフ アセンブリの設置

目的	この手順では、マウント ブラケットを反転させて、シェルフ アセンブリをラックに取り付けます。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ ピン付き六角キー 固定ネジ (48-1003-XX) (2)
事前準備手順	<a href="#">NTP-A1 ONS 15454 シェルフ アセンブリの開梱と検査 (p.1-5)</a>
必須 / 適宜	必須
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



警告

システムの過熱を防止するため、周囲温度が推奨範囲の上限 (131°F [55°C]) を超える場所では使用しないでください。



警告

また、通気を妨げないように、通気口の周囲に 1 インチ (25.4 mm) 以上のスペースを確保してください。



警告

ラックに装置を取り付けたり、ラック内の装置のメンテナンス作業を行ったりする場合は、事故を防ぐため、装置が安定した状態で置かれていることを十分に確認してください。安全を確保するために、次の注意事項を守ってください。

- ラックに設置する装置が 1 台だけの場合は、ラックの一番下に取り付けます。
- ラックに複数の装置を設置する場合は、最も重い装置を一番下に設置して、下から順番に取り付けます。
- ラックにスタビライザが付いている場合は、スタビライザを取り付けてから、ラックにスイッチを設置したり、ラック内のスイッチを保守してください。



警告

ONS 15454 のファン吸気口にエアフローを取り入れるには、設置されたシェルフ アセンブリの下に 1 インチ (25.4 mm) 隙間が必要です。この隙間はエアー ランプ (シェルフ アセンブリの上部にある、角付きの板金状部品) によって確保されます。どのような方法でも、エアー ランプの位置を変更しないでください。



(注)

ONS 15454 XC10G、OC-192、および OC-48 Any Slot (AS) カードには、10 Gbps の互換性のあるシェルフ アセンブリ (15454-SA-10G) およびファントレイ アセンブリ (15454-FTA3) が必要です。

- ステップ 1** 23 インチ( 584.2 mm )ラックを 19 インチ( 482.6 mm )ラックに変更する必要がある場合は、「DLP-A3 19 インチ ( 482.6 mm ) ラックに適合させるためのマウント ブラケットの反転」(p.17-2) を実行します。
- ステップ 2** ファントレイ アセンブリの下でなく、シェルフの底部にエア フィルタを取り付ける場合は、「DLP-A4 外部ブラケットおよびエア フィルタの取り付け」(p.17-4) を実行します。
- ステップ 3** 必要なラック取り付け作業を実行します。
- 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)
  - DLP-A7 ラックへの複数のシェルフ アセンブリの取り付け (p.17-7)
- ステップ 4** 「NTP-A3 前面扉のオープンと取り外し」(p.1-7) へ進んでください。
- 終了：この手順は、これで完了です。

## NTP-A3 前面扉のオープンと取り外し

目的	この手順では、機器に触れることができるように前面扉を開けて取り外します。
工具 / 機器	オープンエンド レンチ ピン付き六角キー
事前準備手順	NTP-A2 シェルフ アセンブリの設置 (p.1-6)
必須 / 適宜	必須
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** 「DLP-A8 前面扉のオープン」(p.17-8) を実行します。
- ステップ 2** 必要に応じて、「DLP-A9 前面扉の取り外し」(p.17-9) を行います。
- ステップ 3** 「NTP-A4 バックプレーン カバーの取り外し」(p.1-8) へ進んでください。
- 終了：この手順は、これで完了です。

## NTP-A4 バックプレーン カバーの取り外し

目的	この手順では、カバーを取り外して、バックプレーンを扱う方法について説明します。バックプレーンには金属製のカバーが2つ（両側に1つずつ）およびバックプレーン カバーが底部に1つ付いています。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	<a href="#">NTP-A2 シェルフ アセンブリの設置 (p.1-6)</a> <a href="#">NTP-A3 前面扉のオープンと取り外し (p.1-7)</a>
必須 / 適宜	必須
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



### 警告

カバーは製品の安全設計に必要な部品です。カバーを外した状態で装置を稼働させないでください。

- 
- ステップ 1** 「[DLP-A10 下部バックプレーン カバーの取り外し](#)」(p.17-10) を実行します。
- ステップ 2** 「[DLP-A11 金属製バックプレーン カバーの取り外し](#)」(p.17-11) を実行します。
- ステップ 3** Electrical Interface Assembly( EIA; 電気インターフェイス アセンブリ )を取り付ける場合は、「[NTP-A5 EIA の取り付け](#)」(p.1-9) へ進みます。取り付けない場合は、「[NTP-A6 電源とアースの取り付け](#)」(p.1-11)へ進みます。

終了：この手順は、これで完了です。

---



## NTP-A5 EIA の取り付け

目的	この手順では、EIA の取り付け方法を示します。通常、EIA パネルは製造時にバックプレーンに取り付けられますが、個別に注文することもできます。EIA の詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺に取り付けるネジ (9) 内側に取り付けるネジ (12) バックプレーン カバー ネジ (5)
事前準備手順	EIA カード (SMB、BNC、AMP Champ、UBIC-V、UBIC-H、MiniBNC)
必須 / 適宜	NTP-A4 バックプレーン カバーの取り外し (p.1-8) ノードで電気信号を使用する場合は必須
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



### 注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。



### (注)

EIA は通常出荷時に取り付けられます。シェルフ アセンブリに正しい EIA が取り付けられていることを確認します。正しい EIA が取り付けられていない場合は、正しい EIA を取り付けます。



### (注)

EIA の取り外しまたは取り付けを行う前に、シェルフの電源を切断する必要はありません。すべての電気トラフィック (DS-1、DS-3、DS3XM-6、および EC-1) が反対側で搬送されている場合は、EIA (A 側または B 側) を稼働中にアップグレードできます。

- ステップ 1** 必要に応じて、「[DLP-A12 BNC または高密度 BNC EIA の取り付け](#)」(p.17-12) を行います。BNC はロック コネクタです。高密度 BNC を使用すると、すべてのカードのすべてのポートにアクセスできます。
- ステップ 2** 必要に応じて、「[DLP-A373 MiniBNC EIA の取り付け](#)」(p.20-63) を行います。MiniBNC を使用すると、ONS 15454 の両側にそれぞれ最大 96 個の DS-3 回路を装着できます。
- ステップ 3** 必要に応じて、「[DLP-A13 SMB EIA の取り付け](#)」(p.17-14) を行います。SMB を使用すると、すべてのカードのすべてのポートにアクセスでき、スペースおよびケーブルを効率的に使用できます。

## ■ NTP-A5 EIA の取り付け

- ステップ4** 必要に応じて、「[DLP-A14 AMP Champ EIA の取り付け](#)」(p.17-16)を行います。AMP Champs と DS-1 ケーブルを同時に使用することはできません。
- ステップ5** 必要に応じて、「[DLP-A190 UBIC-V EIA の取り付け](#)」(p.18-60)を行います。UBIC-V (垂直) EIA では、高密度電気回路カードを使用できます。UBIC-V EIA は SCSI コネクタを提供します。
- ステップ6** 必要に応じて、「[DLP-A399 UBIC-H EIA の取り付け](#)」(p.20-113)を行います。UBIC-H (水平) EIA では、高密度電気回路カードを使用できます。UBIC-H EIA は SCSI コネクタを提供します。



(注) EIA にケーブルを接続するには、「[NTP-A9 バックプレーンでの電気回路カードケーブルの取り付け](#)」(p.1-23)を参照してください。

- ステップ7** 「[NTP-A6 電源とアースの取り付け](#)」(p.1-11)へ進んでください。

終了：この手順は、これで完了です。

---

## NTP-A6 電源とアースの取り付け

目的	この手順では、ONS 15454 に電源装置とアースを取り付けます。
工具 / 機器	<p>#2 プラス ドライバ</p> <p>中型スロット ヘッド ネジ用ドライバ</p> <p>小型スロット ヘッド ネジ用ドライバ</p> <p>ネジ</p> <p>電源コード (ヒューズ アラーム パネルからアセンブリまで)、#10 AWG、銅コンダクタ、90°C (194°F)</p> <p>ストランド アース ケーブル (機器フレームからオフィス アースまで)、#6 AWG</p> <p>リストされている圧着端子コネクタ (通常はデュアル端子タイプ)。コネクタは、スタッドサイズおよび間隔が装置ラックの仕様に基づく #6 AWG 銅コンダクタに適したものを使用する必要があります。オフィス アース接続には、通常、現地の規約に従って H-TAP 圧着コネクタを使用します。</p> <p>ワイヤ カッター</p> <p>ワイヤ ストリッパ</p> <p>圧着工具</p> <p>ヒューズ パネル</p>
事前準備手順	<a href="#">NTP-A4 バックプレーン カバーの取り外し (p.1-8)</a>
必須 / 適宜	必須
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



警告

以下の作業を行う前に、DC 回路に電気が流れていないことを確認します。



警告

この装置は、アースされていることが前提になっています。通常の使用時には必ず装置がアースされているようにしてください。



警告

必ず、銅の導体を使用してください。



警告

この装置は、安全規格に基づく IEC 60950 の Safety Extra-Low Voltage (SELV; 安全特別低電圧) 要件を満たす DC 電源にだけ接続してください。

**警告**

この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。一般および地域の電気規格に適合するように設置する必要があります。

**警告**

固定配線内の手の届く場所に二極切断装置を組み込む必要があります。

**警告**

この装置に複数の電源装置が接続されている場合があります。すべての接続を取り外してから、装置の電源をオフにしてください。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**ステップ 1** 次のいずれかを確認します。

- 15454-SA-ANSI または 15454-SA-HD シェルフを使用している場合は、100 A ヒューズ パネル（シェルフごとに最低 30 A のヒューズ）が取り付けられていること。取り付けられていない場合、製造元の指示に従って取り付けてください。
- 15454-SA-NEBS3 シェルフを使用している場合は、標準の 80 A ヒューズ パネル（シェルフごとに最低 20 A のヒューズ）が取り付けられていること。取り付けられていない場合、製造元の指示に従って取り付けてください。

**ステップ 2** 「DLP-A16 ONS 15454 へのオフィス アースの接続」(p.17-18) を実行します。

**ステップ 3** 「DLP-A17 ONS 15454 シェルフへのオフィス電源の接続」(p.17-19) を実行します。

**ステップ 4** 「DLP-A18 オフィス電源の投入と検証」(p.17-22) を実行します。

**ステップ 5** 「NTP-A7 ファントレイ アセンブリの取り付け」(p.1-13) へ進んでください。

**終了：**この手順は、これで完了です。

## NTP-A7 ファントレイ アセンブリの取り付け

目的	この手順では、ファントレイ アセンブリを取り付けます。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	<a href="#">NTP-A3 前面扉のオープンと取り外し (p.1-7)</a> <a href="#">NTP-A6 電源とアースの取り付け (p.1-11)</a>
必須 / 適宜	必須
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



### 注意

ファントレイ エアー フィルタを取り付けずに ONS 15454 を動作させないでください。Telcordia GR-78-CORE に適合させるには、ファントレイ エアー フィルタを取り付ける必要があります。ただし、外部プラント キャビネット内で使用する場合は除きます。



### 注意

15454-FTA3 ファントレイ アセンブリを取り付けることができるのは、ONS 15454 Release 3.1 以降のアセンブリ (15454-SA-ANSI、800-19857 または 15454-SA-HD、800-24848) のみです。エアー フィルタにはピンが付いているため、ONS 15454 Release 3.1 より前にリリースされた ONS 15454 シェルフ アセンブリ (15454-SA-NEBS3E、15454-SA-NEBS3、および 15454-SA-R1、部品番号 800-0714915454) に取り付けることはできません。15454-FTA3 を適合しないシェルフ アセンブリに取り付けると、Alarm Interface Panel (AIP) に障害が発生し、ファントレイ アセンブリの電源が切断されることがあります。



### 注意

エアー フィルタの上部にファントレイを取り付ける場合は、ファントレイ アセンブリのコンパートメントの前面と同一面になるようにエアー フィルタのエッジを配置する必要があります。そのように配置しないと、フィルタやファントレイ、またはその両方が破損することがあります。



### 注意

ファントレイ アセンブリを無理に押し込まないでください。ファントレイのコネクタまたはシェルフ アセンブリの背面パネルにあるコネクタ (あるいはその両方) が破損することがあります。



### (注)

ONS 15454 を外部プラント キャビネットに取り付けている場合は、エアー フィルタを取り外してください。これにより、冷却能力は最大になり、Telcordia GR-487-CORE に適合するようになります。



### (注)

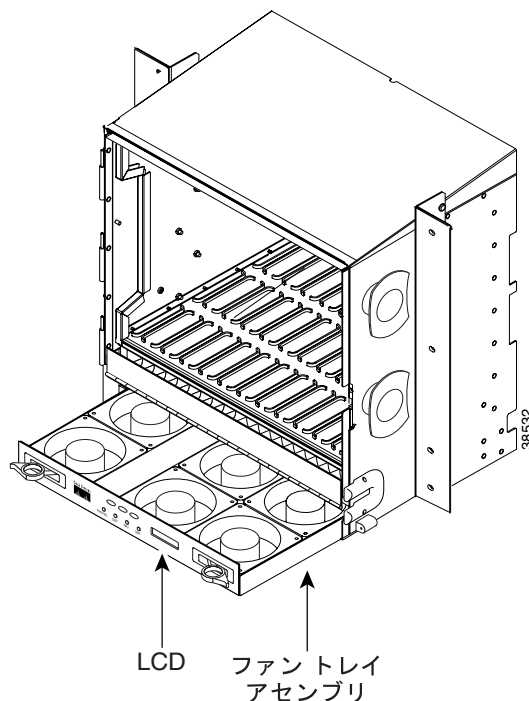
ファントレイ アセンブリを取り付ける場合に、ケーブル マネジメント ファシリティを移動する必要はありません。

## ■ NTP-A7 ファントレイアセンブリの取り付け

- ステップ1** エアーフィルタを取り付けます。エアーフィルタは、ファントレイとシェルフアセンブリの間の内側に取り付けるか、シェルフアセンブリの下部にエアーフィルタブラケットを取り付けて外側に取り付けることができます。エアーフィルタをブラケットにスライドします。
- ステップ2** ファントレイをシェルフアセンブリ内にスライドさせて、トレイの背面にある電気プラグをバックプレーン上の対応するレセプタクルに差し込みます。
- ステップ3** トレイがバックプレーンに差し込まれたことを確認するには、ファントレイを見ながらファンが動作していることを音で確認します。

図 1-1 に、ファントレイの位置を示します。

図 1-1 ファントレイアセンブリの取り付け



- ステップ4** AEP を取り付ける場合は、「NTP-A119 AEP の取り付け」(p.1-15) へ進みます。取り付けない場合は、「NTP-A8 アラーム、タイミング、LAN、およびクラフトピン接続のための配線」(p.1-18) へ進みます。

終了：この手順は、これで完了です。

## NTP-A119 AEP の取り付け

目的	この手順では、15454-SA-ANSI または 15454-SA-HD シェルフ バックプレーンに AEP を取り付けます。AEP は、AIC-I カードが提供する 16 のほかに、アラーム コンタクトも提供します。通常、AEP は ONS 15454 の発注時に取り付けられた状態で出荷されますが、個別に発注することもできます。AEP を装備すると使用可能になるアラーム コンタクトをプロビジョニングするには、事前に AIC-I カードを取り付けておく必要があります。
工具 / 機器	#2 プラス ドライバ  中型スロット ヘッド ネジ用ドライバ  小型スロット ヘッド ネジ用ドライバ  ワイヤラッパー  スタンドオフ (4)
事前準備手順	<a href="#">DLP-A10 下部バックプレーン カバーの取り外し (p.17-10)</a>
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

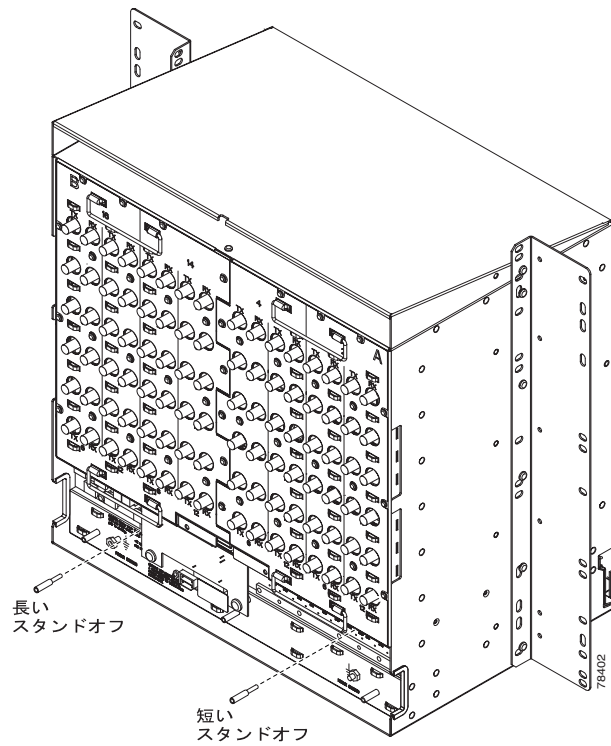


(注)

AIC-I カードは、ダイレクトアラーム コンタクト (外部アラーム入力および外部制御出力) を提供します。ANSI シェルフでは、これらの AIC-I アラーム コンタクトはバックプレーンを介してワイヤラップ ピンに配線されます。ワイヤラップ ピンは、シェルフ背面から取り扱うことができます。AEP を取り付けただけの場合は、ダイレクト AIC-I アラーム コンタクトを使用できません。使用できるのは、AEP アラーム コンタクトのみです。

- ステップ 1** 2 本のバックプレーン ネジを取り外します。2 本のネジをスタンドオフと交換します。左側に長いスタンドオフ、右側に短いスタンドオフを差し込みます ( [図 1-2](#) )。

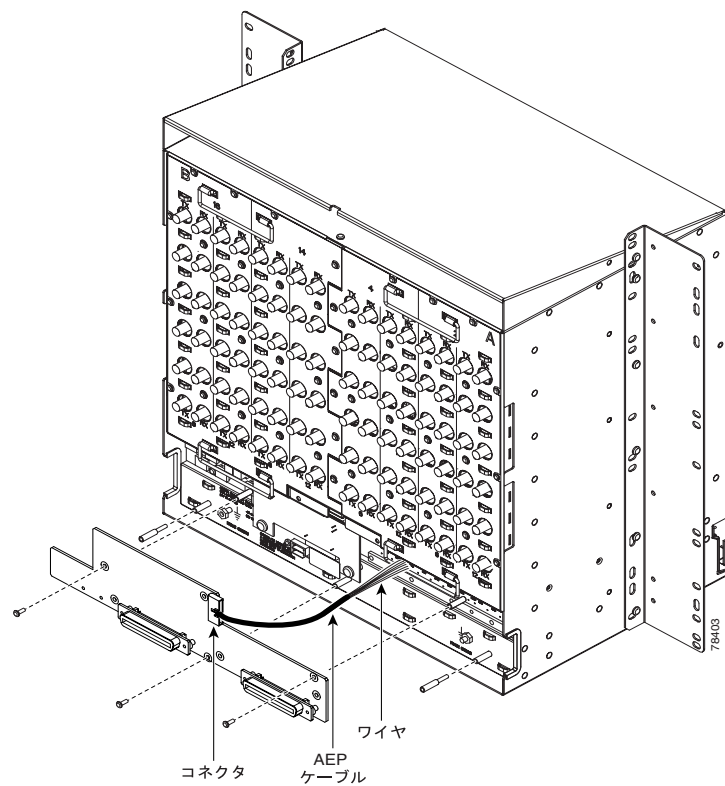
図 1-2 バックプレーン ネジとスタンドオフの交換



**ステップ 2** バックプレーンの両側に、残りの 2 つのスタンドオフを取り付けます ( 図 1-3 )。

**ステップ 3** AEP ボードをスタンドオフの上に合わせます。

図 1-3 スタンドオフおよび AEP の取り付け





**ステップ 4** 3本のネジを差し込んで締めて、AEPをバックプレーンに固定します。

**ステップ 5** AEPケーブルをバックプレーンおよびAEPに接続します。

- a. バックプレーンのワイヤラップピンに10本の色分けされたワイヤを接続します。図1-4に、ケーブル線の接続場所を示します。表1-1に、各ワイヤが伝送するAEP信号およびAIC-I信号を示します。
- b. AEPケーブルの反対側をAEPコネクタポートに差し込みます。ブラウンのピンが一番上になります。

図1-4 AEPワイヤラップとバックプレーンピンの接続

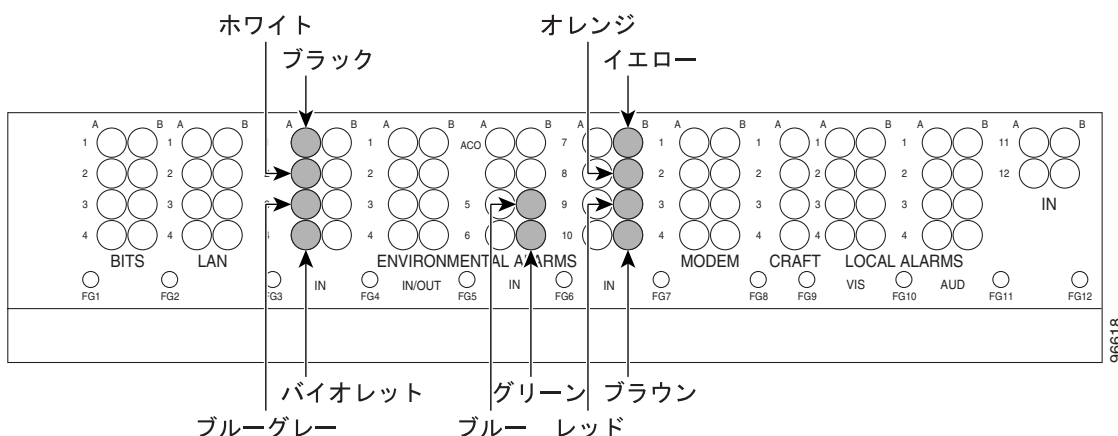


表1-1 AEPのピン割り当て

AEPケーブル線	バックプレーンピン	AIC-I信号	AEP信号
ブラック	A1	GND	AEP_GND
ホワイト	A2	AE_+5	AEP_+5
ブルーグレー	A3	VBAT-	VBAT-
バイオレット	A4	VB+	VB+
ブルー	A5	AE_CLK_P	AE_CLK_P
グリーン	A6	AE_CLK_N	AE_CLK_N
イエロー	A7	AE_DIN_P	AE_DOUT_P
オレンジ	A8	AE_DIN_N	AE_DOUT_N
レッド	A9	AE_DOUT_P	AE_DIN_P
ブラウン	A10	AE_DOUT_N	AE_DIN_N

**ステップ 6** 「NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線」(p.1-18)へ進んでください。

終了：この手順は、これで完了です。

## NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線

目的	この手順では、アラーム、タイミング、LAN、およびクラフト線を取り付けます。
工具 / 機器	ワイヤ ラッパー
事前準備手順	#22 または #24 AWG (0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) アラーム線 NTP-A4 バックプレーン カバーの取り外し (p.1-8)
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



### 警告

カバーは製品の安全設計に必要な部品です。カバーを外した状態で装置を稼働させないでください。

- ステップ 1** AIC-I カードを使用していて、AEP を使用していない場合は、「DLP-A19 バックプレーンへのアラーム ケーブルの取り付け」(p.17-23) を実行します。
- ステップ 2** 必要に応じて、「DLP-A20 バックプレーンへのタイミング ケーブルの取り付け」(p.17-26) を行います。外部タイミングを設定するには、タイミング ケーブルが必要です。
- ステップ 3** 必要に応じて、「DLP-A21 バックプレーンへの LAN ケーブルの取り付け」(p.17-27) を行います。外部 LAN 接続を作成するには、LAN 線 (または TCC2/TCC2P の LAN ポート) が必要です。
- ステップ 4** 必要に応じて、「DLP-A22 TL1 クラフト インターフェイスの取り付け」(p.17-28) を行います。クラフト インターフェイスを使用して TL1 にアクセスするには、クラフト線 (または TCC2/TCC2P の EIA/TIA-232 ポート) が必要です。



### 注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

- ステップ 5** 次のいずれかを行います。
- AEP が取り付けられている場合は、「NTP-A120 AEP への外付けワイヤラップ パネルの取り付け」(p.1-19) に進みます。
  - AEP が取り付けられていない状態で、電気回路カードを取り付ける予定がある場合は、「NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け」(p.1-23) へ進みます。
  - AEP が取り付けられていない状態で、電気回路カードを取り付ける予定もない場合は、「NTP-A11 背面カバーの取り付け」(p.1-25) へ進みます。

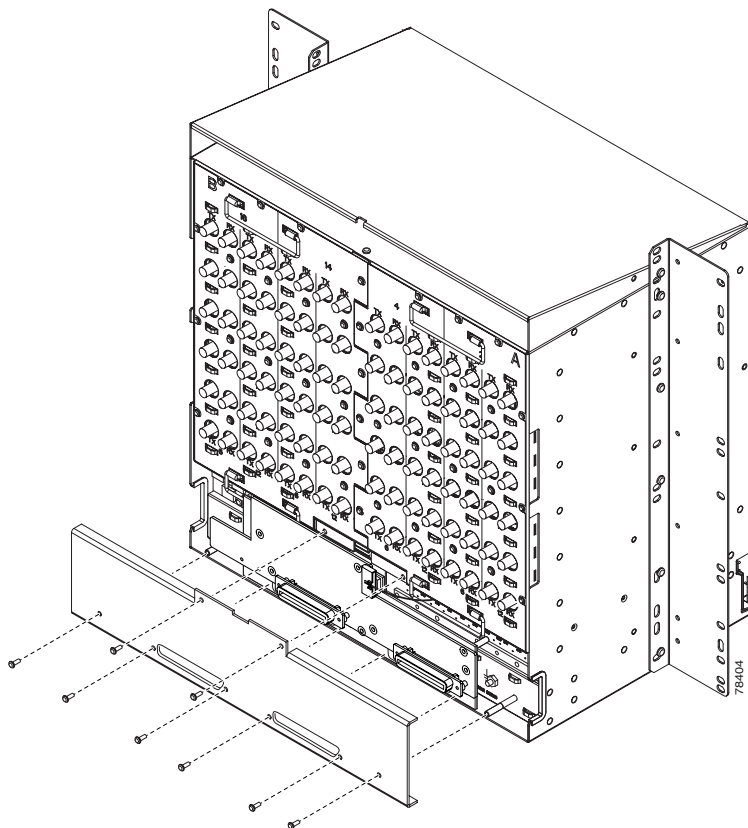
終了：この手順は、これで完了です。

## NTP-A120 AEP への外付けワイヤラップパネルの取り付け

目的	この手順では、AEP に外付けワイヤラップパネルを接続して、AEP の物理アラーム コンタクトを実現します。
工具 / 機器	外付けワイヤラップパネル
事前準備手順	<a href="#">NTP-A119 AEP の取り付け (p.1-15)</a>
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** 下部カバーを AEP の上に合わせます。AEP AMP Champ コネクタが下部カバーの穴から突き出ていることを確認します ( [図 1-5](#) )。

**図 1-5** AEP カバーの取り付け



- ステップ 2** 8本のネジを差し込んで締めて、AEP カバーを AEP に固定します。

- ステップ 3** 外付けワイヤラップパネルと AEP 上の AMP Champ コネクタをケーブル接続します。 [表 1-2](#) に、アラーム入力ピンの割り当てを示します。

表 1-2 アラーム入力ピンの割り当て

AMP Champ ピン	信号名	AMP Champ ピン	信号名
1	ALARM_IN_1-	27	GND
2	GND	28	ALARM_IN_2-
3	ALARM_IN_3-	29	ALARM_IN_4-
4	ALARM_IN_5-	30	GND
5	GND	31	ALARM_IN_6-
6	ALARM_IN_7-	32	ALARM_IN_8-
7	ALARM_IN_9-	33	GND
8	GND	34	ALARM_IN_10-
9	ALARM_IN_11-	35	ALARM_IN_12-
10	ALARM_IN_13-	36	GND
11	GND	37	ALARM_IN_14-
12	ALARM_IN_15-	38	ALARM_IN_16-
13	ALARM_IN_17-	39	GND
14	GND	40	ALARM_IN_18-
15	ALARM_IN_19-	41	ALARM_IN_20-
16	ALARM_IN_21-	42	GND
17	GND	43	ALARM_IN_22-
18	ALARM_IN_23-	44	ALARM_IN_24-
19	ALARM_IN_25-	45	GND
20	GND	46	ALARM_IN_26-
21	ALARM_IN_27-	47	ALARM_IN_28-
22	ALARM_IN_29-	48	GND
23	GND	49	ALARM_IN_30-
24	ALARM_IN_31-	50	—
25	ALARM_IN_+	51	GND1
26	ALARM_IN_0-	52	GND2

表 1-3 に、アラーム出力ピンの割り当てを示します。

表 1-3 アラーム出力ピンの割り当て

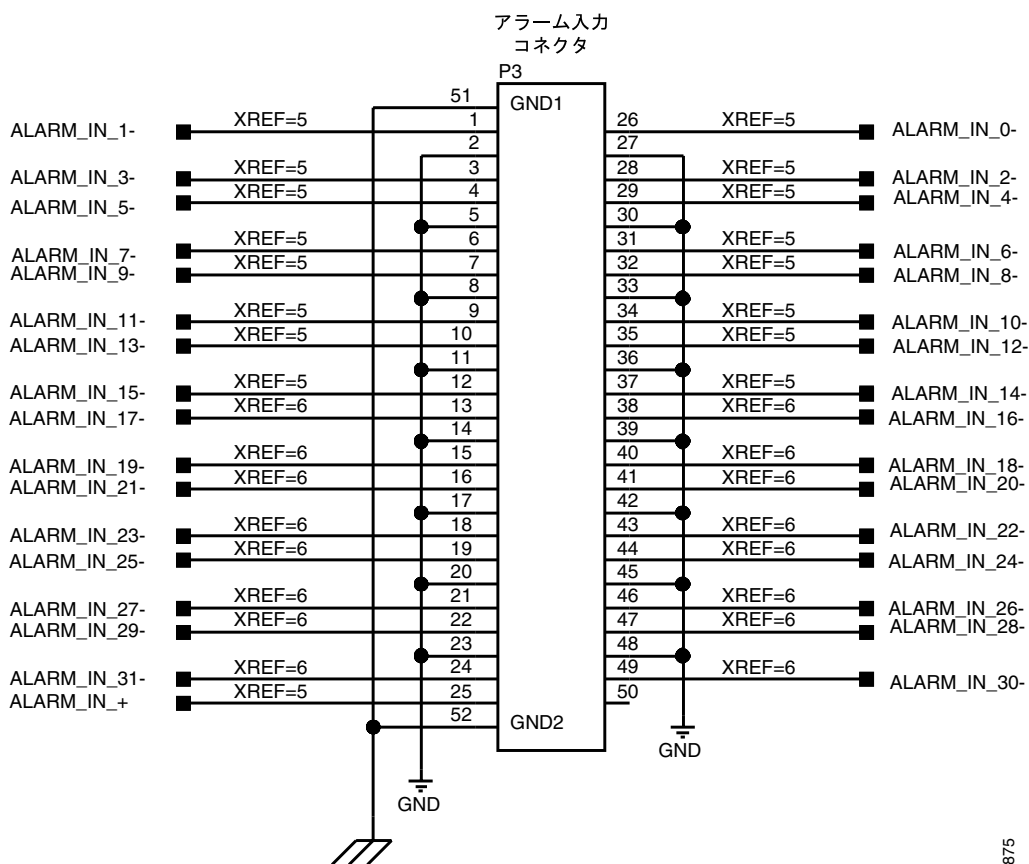
AMP Champ ピン	信号名	AMP Champ ピン	信号名
1	—	27	COM_0
2	COM_1	28	—
3	NO_1	29	NO_2
4	—	30	COM_2
5	COM_3	31	—
6	NO_3	32	NO_4
7	—	33	COM_4
8	COM_5	34	—
9	NO_5	35	NO_6
10	—	36	COM_6

表 1-3 アラーム出力ピンの割り当て (続き)

AMP Champ ピン	信号名	AMP Champ ピン	信号名
11	COM_7	37	—
12	NO_7	38	NO_8
13	—	39	COM_8
14	COM_9	40	—
15	NO_9	41	NO_10
16	—	42	COM_10
17	COM_11	43	—
18	NO_11	44	NO_12
19	—	45	COM_12
20	COM_13	46	—
21	NO_13	47	NO_14
22	—	48	COM_14
23	COM_15	49	—
24	NO_15	50	—
25	—	51	GND1
26	NO_0	52	GND2

図 1-6 に、アラーム入力コネクタを示します。

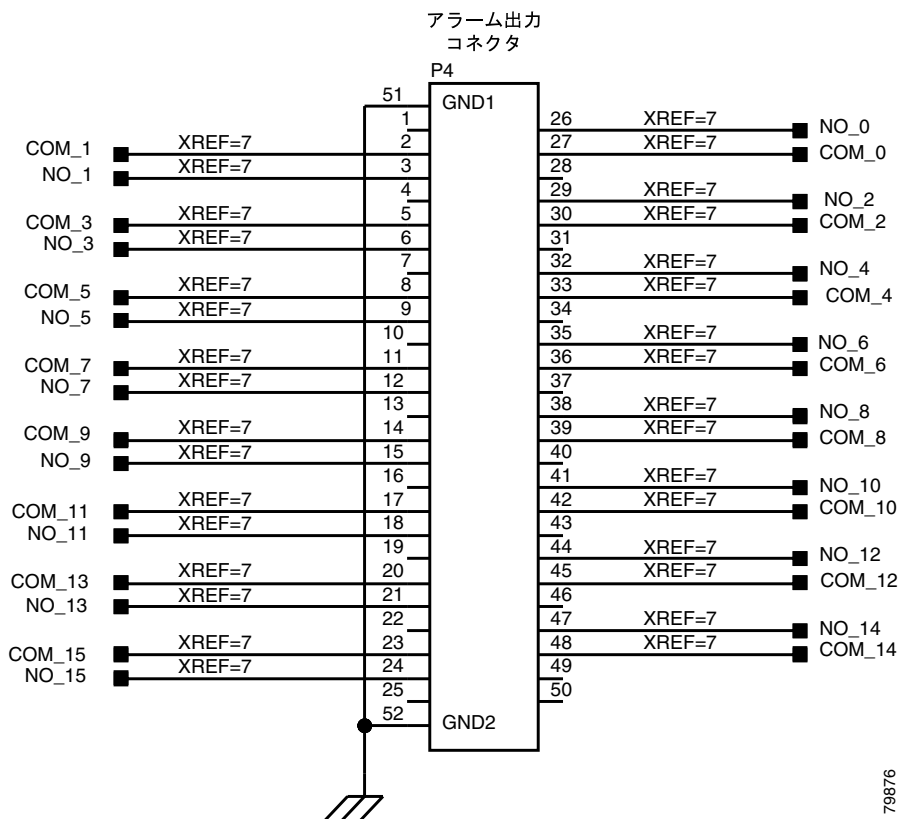
図 1-6 アラーム入力コネクタ



79875

図 1-7 に、アラーム出力コネクタを示します。

図 1-7 アラーム出力コネクタ



**ステップ 4** 次のいずれかを行います。

- 電気回路カードを取り付ける場合は、「[NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け](#)」(p.1-23)へ進みます。
- 電気回路カードを取り付けない場合は、「[NTP-A11 背面カバーの取り付け](#)」(p.1-25)へ進みます。

**終了**：この手順は、これで完了です。

## NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け

目的	オプションの EIA バックプレーン カバーは、通常、ONS 15454 の発注時に取り付けられた状態で出荷されます。次の手順は、バックプレーンに電気回路カードのケーブルを取り付ける方法を示します。出荷されたシェルフに正しい EIA インターフェイスが取り付けられていない場合は、正しい EIA を発注して、取り付ける必要があります。
工具 / 機器	ワイヤ ラッパー ツイストペア ケーブル BNC 取り付け工具 SMB ケーブル コネクタ #2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ DS-1 および DS-3 ケーブル (必要に応じて) 固定棒 (必要に応じて)
事前準備手順	<a href="#">NTP-A5 EIA の取り付け (p.1-9)</a>
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



### 注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。



### (注)

EIA の詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。

- ステップ 1** 取り付ける電気回路ケーブルを配線する場合は、必要に応じて「[DLP-A530 固定棒の取り付け \(p.22-33\)](#)」を実行します。
- ステップ 2** 必要に応じて、「[DLP-A23 電気インターフェイス アダプタ \(バラン\)](#)」を使用した DS-1 ケーブルの[取り付け \(p.17-29\)](#)を行います。DS-1 信号を適切に終端するには、SMB EIA でバランを使用する必要があります。
- ステップ 3** AMP Champ ケーブルを使用して DS-1 ケーブルを取り付ける場合は、「[DLP-A24 AMP Champ EIA への DS-1 AMP Champ ケーブルの取り付け \(p.17-30\)](#)」を実行します。
- ステップ 4** 必要に応じて、「[DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け \(p.17-33\)](#)」を行います。
- ステップ 5** 必要に応じて、「[DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け \(p.17-35\)](#)」を行います。

## ■ NTP-A10 電気回路ケーブルの配線

- ステップ 6** 必要に応じて、「DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け」(p.17-35)を行います。
- ステップ 7** 必要に応じて、「DLP-A386 UBIC-V EIA での電気回路ケーブルの取り付け」(p.20-90)を行います。
- ステップ 8** 必要に応じて、「DLP-A441 UBIC-H EIA での電気回路ケーブルの取り付け」(p.21-22)を行います。
- ステップ 9** 「NTP-A10 電気回路ケーブルの配線」(p.1-24)へ進んでください。

終了：この手順は、これで完了です。

---

## NTP-A10 電気回路ケーブルの配線

目的	この手順では、電気回路（バックプレーン）ケーブルを配線および管理します。
工具 / 機器	RG179、RG59（735A）#26 AWG ケーブル、または RG59（734A）#20 AWG ケーブル
事前準備手順	NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け (p.1-23)
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** 必要に応じて、「DLP-A28 同軸ケーブルの配線」(p.17-37)を行います。
- ステップ 2** 必要に応じて、「DLP-A29 DS-1 ツイストペア ケーブルの配線」(p.17-38)を行います。
- ステップ 3** 「NTP-A11 背面カバーの取り付け」(p.1-25)へ進んでください。

終了：この手順は、これで完了です。

---



## NTP-A11 背面カバーの取り付け

目的	この手順では、背面カバーを取り付けます。
工具 / 機器	#2 プラス ドライバ 5/16 インチ ナット ドライバ シェルフ アクセサリ キット (53-2329-XX) <ul style="list-style-type: none"> <li>取り付けバー (700-19701-XX)(2)</li> <li>1 インチ スタンドオフ (50-1193-01)(4)</li> <li>1 3/8 インチ スタンドオフ (50-1492-01)(4)</li> <li>2 インチ スタンドオフ (50-1453-01)(8)</li> <li>6-32 x 0.5 のフラットヘッド ネジ (48-2116-01)(4)</li> </ul> プラスチック背面カバー (700-06029-XX)
事前準備手順	<a href="#">NTP-A3 前面扉のオープンと取り外し (p.1-7)</a>
必須 / 適宜	必須
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** 背面カバーを取り付ける EIA のタイプを識別します。

**ステップ 2** [表 1-4](#) に従って、目的の EIA タイプの拡張スタンドオフを組み立てます。1 3/8 インチ スタンドオフに別のスタンドオフをつなげて、拡張スタンドオフを作成します。2 本の拡張スタンドオフを互いに組み合わせて、シェルフごとに合計 4 本の拡張スタンドオフを作成する必要があります。

表 1-4 EIA タイプに必要なスタンドオフ

EIA タイプ	1 本の拡張スタンドオフに必要なスタンドオフ	シェルフごとに必要なスタンドオフの総数
<i>UBIC-V</i>	1 3/8 インチ (1) 2 インチ (2)	1 3/8 インチ (4) 2 インチ (8)
<i>UBIC-H</i>	1 3/8 インチ (1) 2 インチ (1)	1 3/8 インチ (4) 2 インチ (4)
<i>MiniBNC</i>	1 3/8 インチ (1) 2 インチ (1)	1 3/8 インチ (4) 2 インチ (4)
<i>BNC</i>	1 3/8 インチ (1)	1 3/8 インチ (4)
<i>High-Density BNC</i>	1 インチ (1)	1 インチ (4)
SMB		
AMP Champ		

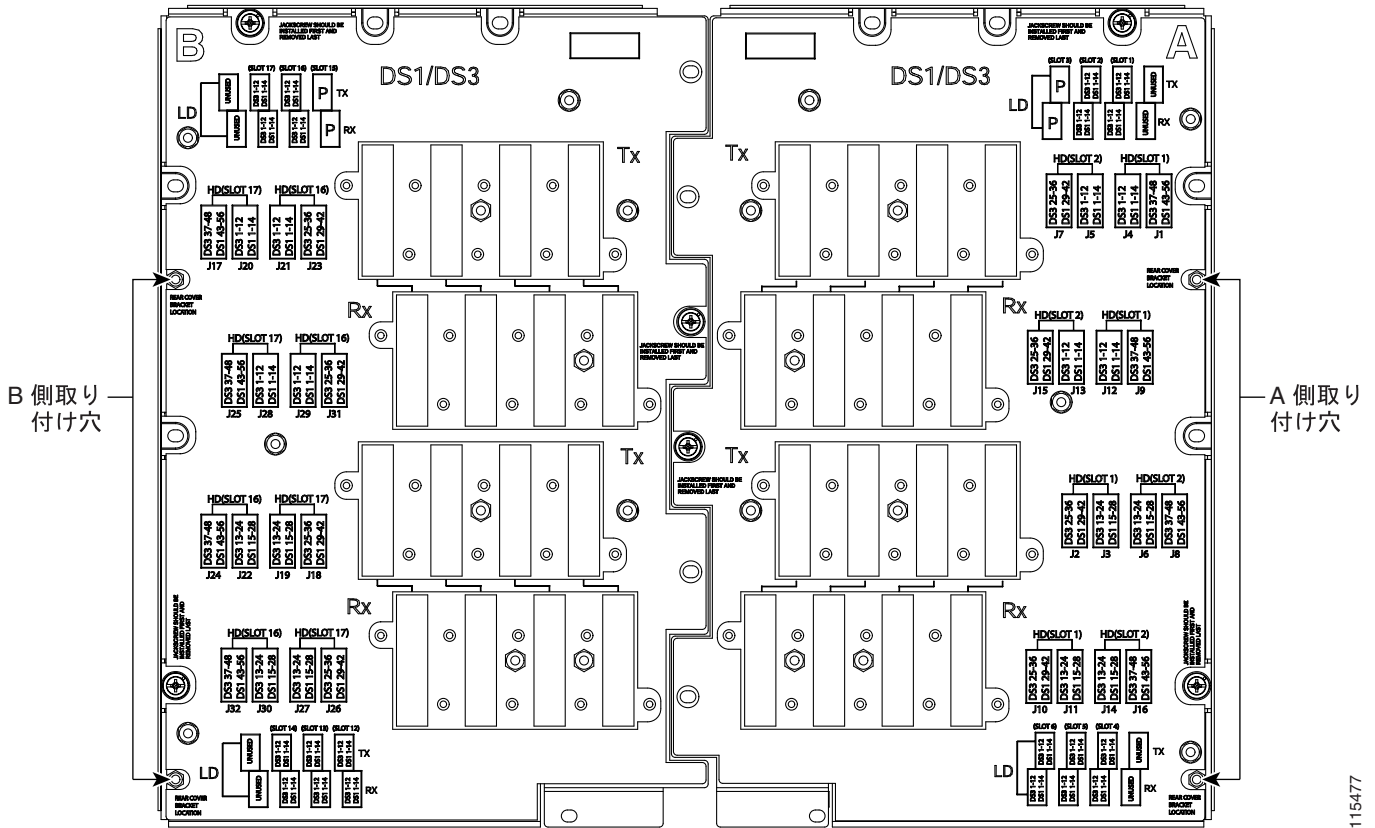


**(注)** 設置場所固有のケーブル マネジメント要件に適合させるために、必要に応じて、拡張スタンドオフにさらにスタンドオフをつなげてください。

NTP-A11 背面カバーの取り付け

**ステップ3** 使用している EIA 上で、スタンドオフの取り付け穴を確認します。図 1-8 に、UBIC-V の取り付け穴を示します。図 1-9 に、UBIC-H の取り付け穴を示します。図 1-10 に、残りの EIA タイプ (MiniBNC、SMB など) の取り付け穴を示します。すべての EIA の取り付け穴は、REAR COVER BRACKET LOCATION のラベルで識別できます。

図 1-8 UBIC-V EIA の取り付け穴



115477

図 1-9 UBIC-H の取り付け穴

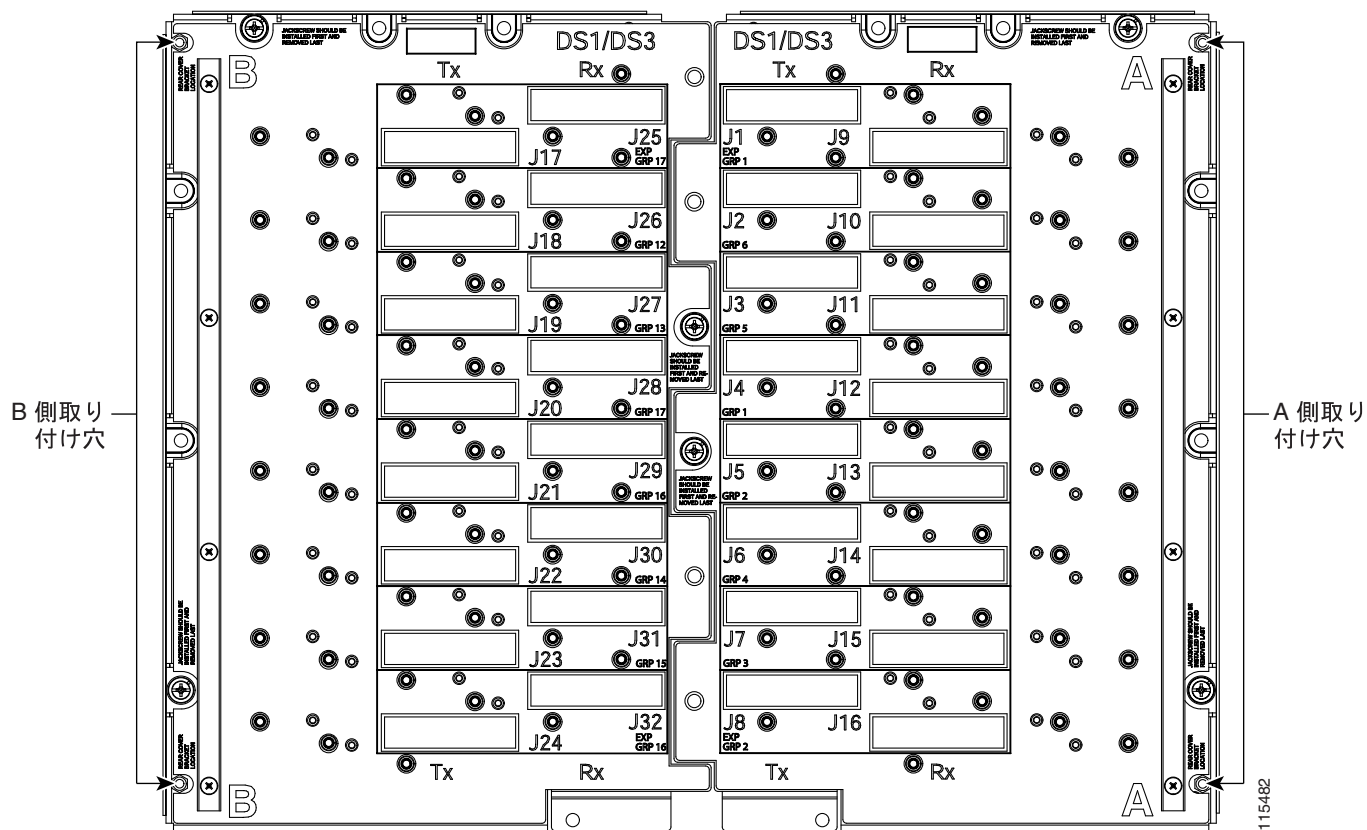
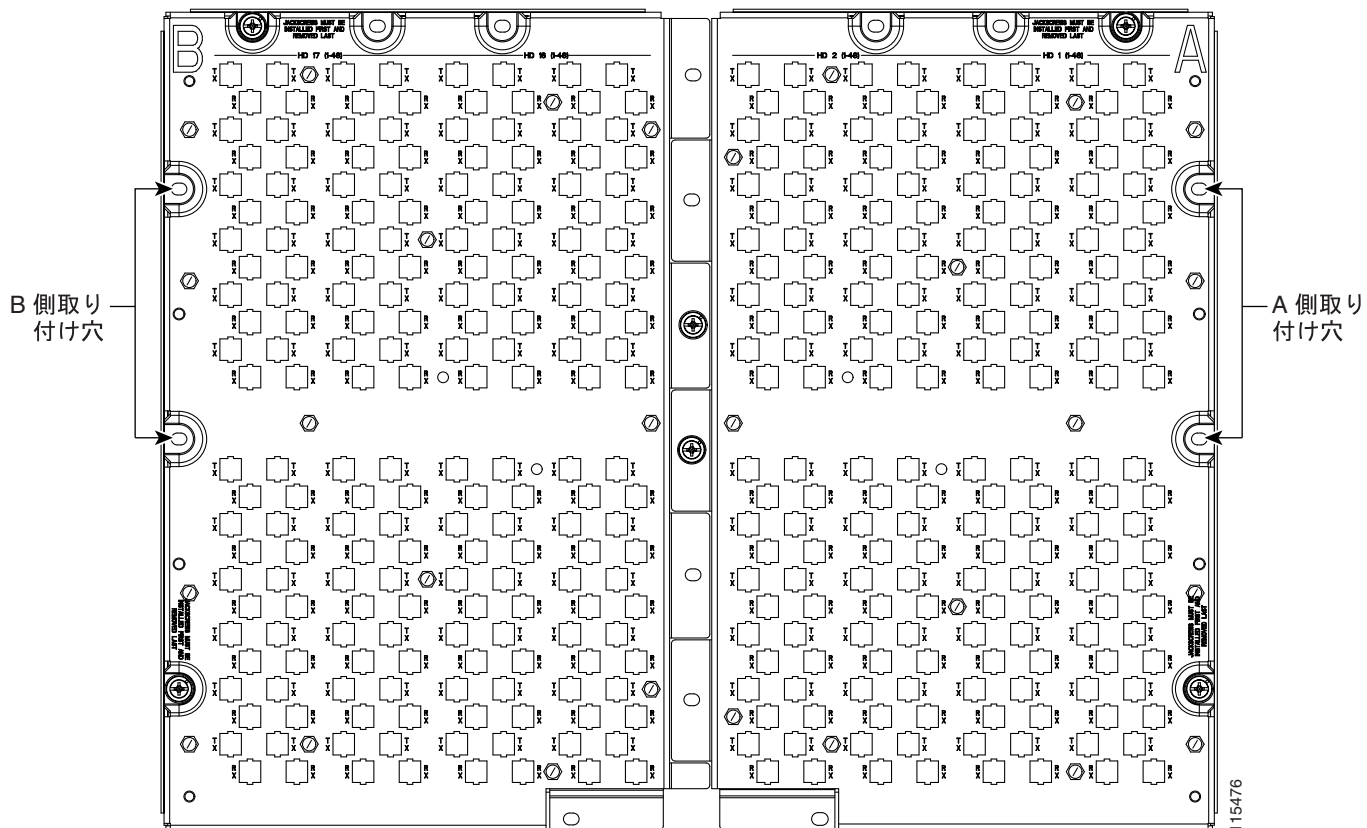


図 1-10 その他のすべての EIA タイプの取り付け穴

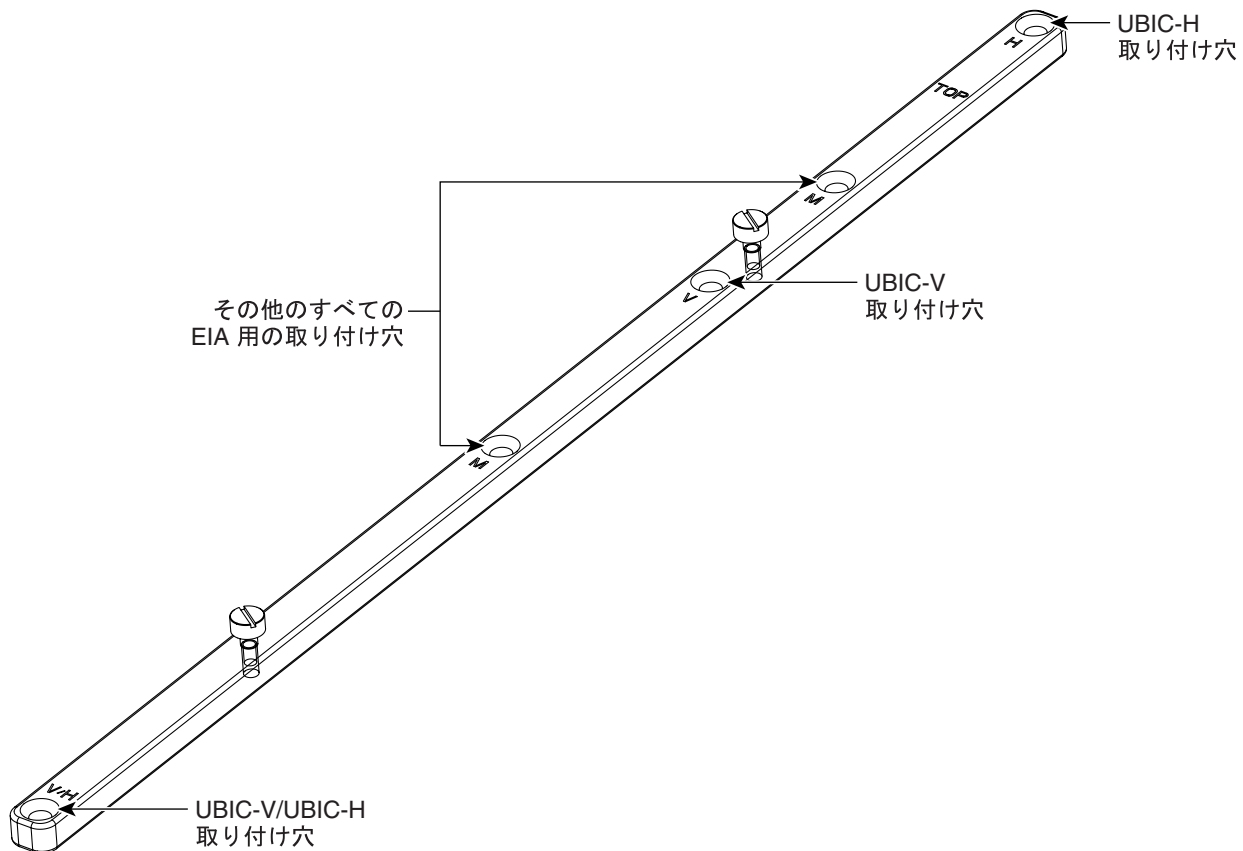


## ■ NTP-A11 背面カバーの取り付け

**ステップ4** 拡張スタンドオフを取り付け穴に取り付けるには、5/16 インチ ナットドライバを使用します。

**ステップ5** いずれかの取り付けバー（700-19701-XX）にある *TOP* ラベルを確認し、EIA の該当する穴の位置を拡張スタンドオフに合わせます（[図 1-11](#)）。

図 1-11 取り付けバーの EIA ラベル

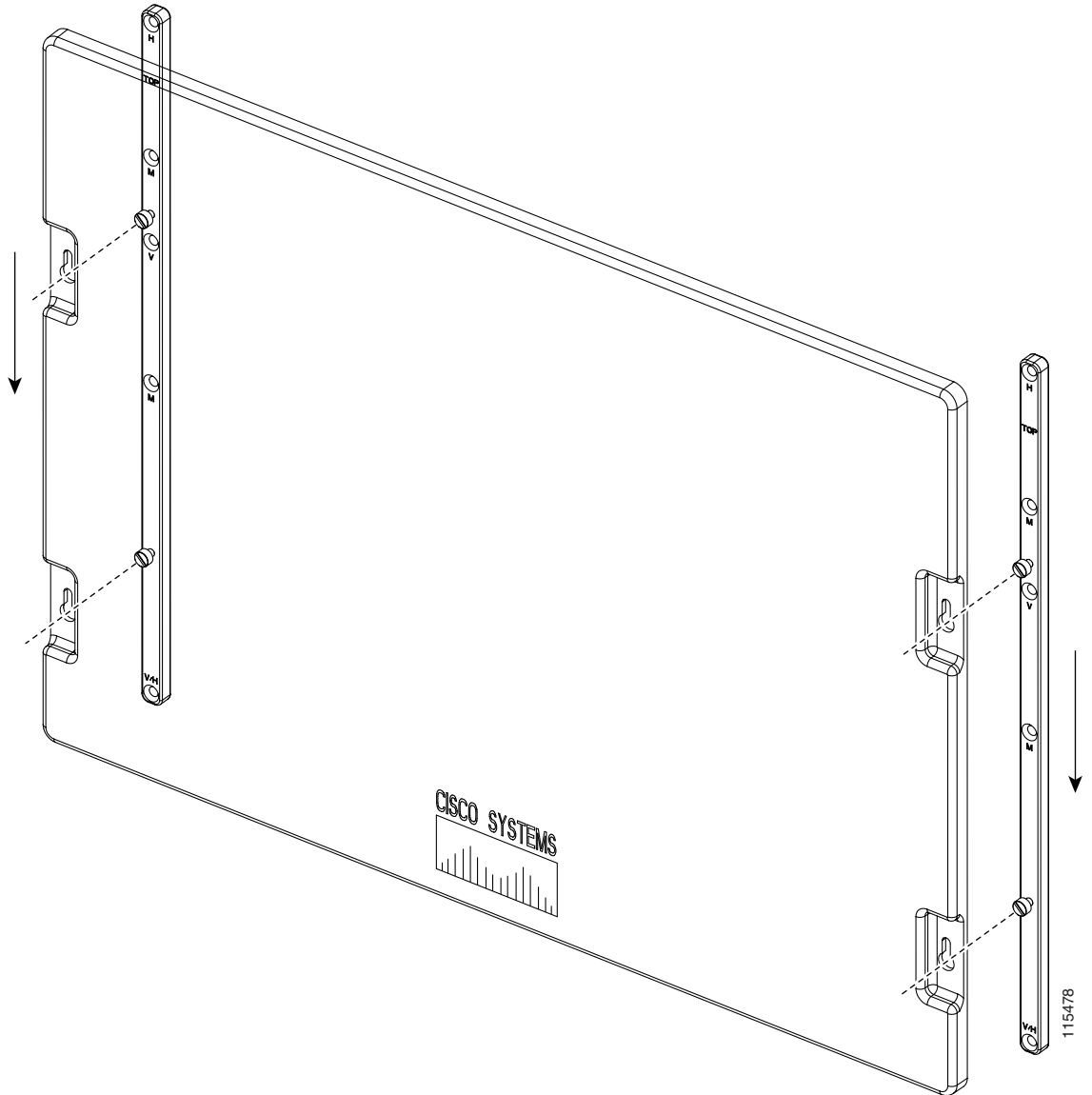


**ステップ6** 各取り付けバーの2本のネジ（48-2116-01）を締めます。

**ステップ7** 別の取り付けバーに、5 ~ 6を繰り返します。

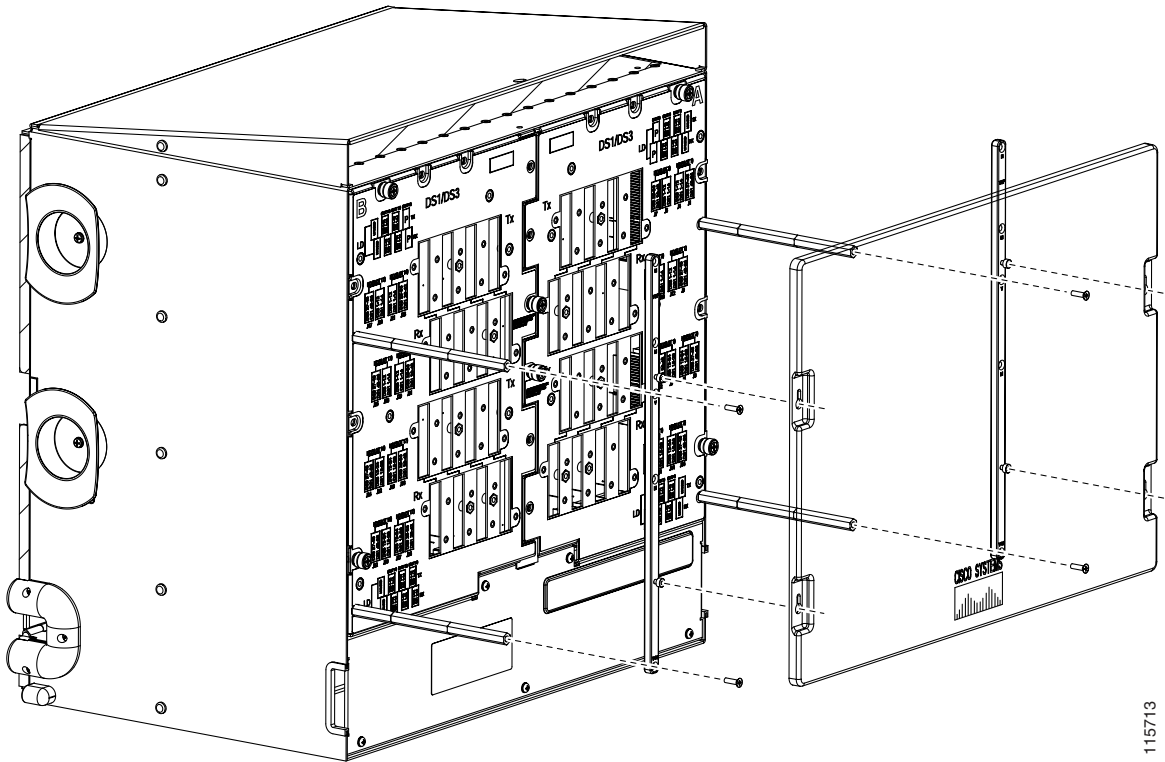
**ステップ 8** 背面カバー（700-06029-XX）を取り付けます。そのためには、取り付けバーの背面にある取り付けネジに背面カバーを引っ掛けて、引き下げて所定位置にしっかりと固定します（[図 1-12](#)）。または、スタンドオフを使用します（[図 1-13](#)）。

**図 1-12** 取り付けバーへの背面カバーの取り付け



## ■ NTP-A11 背面カバーの取り付け

図 1-13 スタンドオフを使用した背面カバーの取り付け



終了：この手順は、これで完了です。

## NTP-A12 フェライトの取り付け

目的	この手順では、フェライトを取り付けます。
工具 / 機器	クランプ型フェライトおよびブロック フェライト
事前準備手順	NTP-A6 電源とアースの取り付け (p.1-11) NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線 (p.1-18)
必須 / 適宜	必須
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** 必要に応じて、「DLP-A30 電源コードへのフェライトの取り付け」(p.17-39) を行います。
- ステップ 2** 必要に応じて、「DLP-A31 ワイヤラップ ピン フィールドへのフェライトの接続」(p.17-40) を行います。
- ステップ 3** 「NTP-A13 シェルフ取り付けの受け入れテスト」(p.1-32) へ進んでください。

終了：この手順は、これで完了です。

---

## NTP-A13 シェルフ取り付けの受け入れテスト

目的	この手順では、シェルフ取り付けの受け入れテストを実行します。
工具 / 機器	電圧計
事前準備手順	第1章の適切な手順
必須 / 適宜	必須
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



### 警告

カバーは製品の安全設計に必要な部品です。カバーを外した状態で装置を稼働させないでください。

**ステップ1** 必要な各手順が完了したことを確認して、[表 1-5](#) を完成させます。

**表 1-5 シェルフ取り付け作業の概要**

内容	完了
<a href="#">NTP-A1 ONS 15454 シェルフ アセンブリの開梱と検査 (p.1-5)</a>	
<a href="#">NTP-A2 シェルフ アセンブリの設置 (p.1-6)</a>	
<a href="#">NTP-A3 前面扉のオープンと取り外し (p.1-7)</a>	
<a href="#">NTP-A4 バックプレーン カバーの取り外し (p.1-8)</a>	
<a href="#">NTP-A5 EIA の取り付け (p.1-9)</a>	
<a href="#">NTP-A6 電源とアースの取り付け (p.1-11)</a>	
<a href="#">NTP-A7 ファントレイ アセンブリの取り付け (p.1-13)</a>	
<a href="#">NTP-A119 AEP の取り付け (p.1-15)</a>	
<a href="#">NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線 (p.1-18)</a>	
<a href="#">NTP-A120 AEP への外付けワイヤラップ パネルの取り付け (p.1-19)</a>	
<a href="#">NTP-A9 バックプレーンでの電気回路カード ケーブルの取り付け (p.1-23)</a>	
<a href="#">NTP-A10 電気回路ケーブルの配線 (p.1-24)</a>	
<a href="#">NTP-A11 背面カバーの取り付け (p.1-25)</a>	

**ステップ2** 「[DLP-A32 シェルフの取り付けおよび接続の検査](#)」(p.17-41) を実行します。

**ステップ3** 「[DLP-A33 電圧の測定](#)」(p.17-41) を実行します。

**ステップ4** 第2章「[カードおよび光ファイバケーブルの取り付け](#)」へ進みます。

終了：この手順は、これで完了です。





# カードおよび光ファイバ ケーブルの 取り付け

この章では、Cisco ONS 15454 カードおよび光ファイバ ケーブルの取り付け方法について説明します。

## 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A15 共通コントロール カードの取り付け \(p.2-2\)](#)— この手順は、その他のカードを取り付ける前に行います。
2. [NTP-A16 光カードおよびコネクタの取り付け\(p.2-8\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A17 電気回路カードの取り付け \(p.2-11\)](#)— 必要に応じて、この手順を実行します。
4. [NTP-A246 イーサネット カードおよびコネクタの取り付け \(p.2-13\)](#)— 必要に応じて、この手順を実行します。
5. [NTP-A274 FC\\_MR-4 カードの取り付け \(p.2-15\)](#)— 必要に応じて、この手順を実行します。
6. [NTP-A316 フィラー カードの取り付け \(p.2-17\)](#)— 必要に応じて、この手順を実行します。
7. [NTP-A247 光ファイバ ケーブルの取り付け \(p.2-18\)](#)— 光カードに光ファイバ ケーブルを取り付ける場合は、この手順を実行します。
8. [NTP-A245 光ファイバ ケーブルの配線 \(p.2-22\)](#)— 必要に応じて、この手順を実行します。
9. [NTP-A116 カードの取り外しおよび交換 \(p.2-23\)](#)— Cisco Transport Controller (CTC) からカードを取り外したり、カードのプロビジョニングを保持したまま OC-N カードを変更したりするなど、カードの取り外しや交換を行う場合は、必要に応じてこの手順を実行します。
10. [NTP-A20 前面扉の交換 \(p.2-24\)](#)— 前面扉が取り外されている場合は、カードと光ファイバ ケーブルを取り付けたあと、前面扉およびアース ストラップを交換する場合は、この手順を実行します。



警告

この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

**警告**

フィルターカードには3つの重要な機能があります。シャーシ内の危険な電圧および電流による感電を防ぐこと、他の装置へのEMI（電磁波干渉）の影響を防ぐこと、およびシャーシ内の空気の流れを適切な状態に保つことです。必ずすべてのカードおよび前面プレートを正しく取り付けられた状態で、システムを運用してください。

## NTP-A15 共通コントロールカードの取り付け

目的	この手順では、共通コントロールカードの取り付け方法について説明します。
工具 / 機器	冗長 TCC2/TCC2P カード 冗長 XCVT、XC10G、または XC-VXC-10G（クロスコネクト）カード AIC-I カード（オプション）
事前準備手順	<a href="#">NTP-A13 シェルフ取り付けの受け入れテスト（p.1-32）</a>
必須 / 適宜	必須
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

**警告**

作業中は、カードの ESD 破壊を防ぐため、必ず静電気防止用リストストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフアセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**(注)**

カードのバックプレーンコネクタに保護クリップが取り付けられている場合は、カードを取り付ける前に、クリップを取り外してください。

**(注)**

カードが正しく取り付けられなかった場合は、FAIL LED が連続して点滅します。

**ステップ 1** XCVT カードを取り付ける場合は、[表 2-1](#) でカードとスロットの互換性を確認してください。XC10G または XC-VXC-10G カードを取り付ける場合は、[表 2-2](#) でカードとスロットの互換性を確認してください。

**ステップ 2** 「[DLP-A36 TCC2/TCC2P カードの取り付け](#)」(p.17-44) を実行します。

**ステップ 3** 「[DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け](#)」(p.17-47) を実行します。

**ステップ4** 必要に応じて、「DLP-A41 AIC-Iカードの取り付け」(p.17-50)を行います。



(注) スロットに誤ったカードを取り付けた場合は、「NTP-A116 カードの取り外しおよび交換」(p.2-23)を参照してください。

**ステップ5** トラフィックカードを取り付けます。各カードに適した手順を判別するには、「準備作業」(p.2-1)のNTPリストを参照してください。

表2-1内の「」は、カードがそのスロットでサポートされていることを示します。マルチサービス(トラフィック)スロットのスロット1～6および12～17には、その他のマルチサービススロットの4倍の帯域幅を持つ4つのスロット(スロット5、6、12、および13)が含まれています。



(注) XCカードは、ほとんどのカードと互換性がありますが、Release 5.0以降の新規機能はサポートしていません。XCカードの互換性の詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。



(注) 各カード固有のスロット制限事項については、『Cisco ONS 15454 Reference Manual』の各カードのカードリファレンスセクションを参照してください。

表2-1 XCVTカードのカードとスロットの互換性

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
TCC2/TCC2P																	
XCVT																	
AIC-I																	
DS1-14																	
DS1N-14 <sup>1</sup>		3		3	3	3						3	3	3		3	3
DS1/E1-56	XCVTカードではサポートされない。XC10GまたはXC-VXC-10Gカードが必要。																
DS3-12						2						2					
DS3-12E						2						2					
DS3N-12	3	3		3	3								3	3		3	3
						3,2						3,2					
DS3N-12E	3	3		3	3								3	3		3	3
						3,2						3,2					
DS3I-N-12 <sup>3</sup>	3	3		3	3	3						3	3	3		3	3
DS3XM-6						2						2					
DS3XM-12						2						2					
DS3/EC1-48	XCVTカードではサポートされない。XC10GまたはXC-VXC-10Gカードが必要。																
EC1-12						2						6					
E100T-12																	

## ■ NTP-A15 共通コントロールカードの取り付け

表 2-1 XCVT カードのカードとスロットの互換性 (続き)

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
E1000-2																	
E100T-G																	
E1000-2-G																	
CE-100T-8																	
CE-1000-4																	
G1K-4																	
ML100-12																	
ML1000-2																	
ML100X-8	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
OC3 IR 4/STM1 SH 1310																	
OC3IR/STM1SH 1310-8	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
OC12 IR STM4 SH 1310																	
OC12 LR/STM4 LH 1310																	
OC12 LR/STM4 LH 1550																	
OC12 IR/STM4 SH 1310-4	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
OC48 IR 1310																	
OC48 LR 1550																	
OC48 IR/STM16 SH AS 1310 <sup>4</sup>																	
OC48 LR/STM16 LH AS 1550 <sup>4</sup>																	
OC48-ELR/STM16 EH 100 GHz																	
OC48 ELR 200 GHz																	
OC192 SR/STM64 IO 1310	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
OC192 IR/STM64 SH 1550	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
OC192 LR/STM64 LH 1550	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																
MRC-12																	
OC192SR1/STM64IO Short Reach および OC192/STM64 Any Reach ( OC192-XFP カード )	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																

表 2-1 XCVT カードのカードとスロットの互換性 (続き)

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
FC_MR-4																	
OC192 LR/STM64 LH ITU 15xx.xx	XCVT カードではサポートされない。XC10G または XC-VXC-10G カードが必要。																

1. 特定のスロットに装着された場合に、標準の DS1 または DS3 カードとして動作する 1:N カードを識別します。
2. この DS3 カードを高密度 Electrical Interface Assembly (EIA; 電気インターフェイス アセンブリ) と組み合わせて使用したり、1:N 設定で使用する場合、このスロットに装着して使用できません。
3. このカードは、XCVT カードとのみ併用できます。XC カードとは併用できません。
4. OC48AS は、R3.4 ~ R4.6 の XC/XCVT のスロット 5、6、12、および 13 で動作します。OC48AS は、R5.0 以降の XCVT のスロット 5、6、12、および 13 で動作します。Release R3.3 以前の XC/XCVT では、OC48AS はサポートされていません。

表 2-2 内の「」は、カードがそのスロットでサポートされていることを示します。マルチサービス (トラフィック) スロットのスロット 1 ~ 6 および 12 ~ 17 には、その他のマルチサービス スロットの 4 倍の帯域幅を持つ 4 つのスロット (スロット 5、6、12、および 13) が含まれています。XC10G および XC-VXC-10G カードには、ANSI シェルフ (5454-SA-ANSI) または高密度シェルフ (15454-SA-HD) が必要です。



(注)

各カード固有のスロット制限事項については、『Cisco ONS 15454 Reference Manual』の各カードのカードリファレンス セクションを参照してください。

表 2-2 XC10G および XC-VXC-10G カードのタイプとスロットの互換性

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
TCC2/TCC2P																	
XC10G																	
XC-VXC-10G																	
AIC-I																	
DS1-14	2	2	2	2	2	2						2	2	2	2	2	2
DS1N-14	1,2	1,2	2	1,2	1,2	1,2						1,2	1,2	1,2		1,2	1,2
DS1/E1-56																	
DS3-12	2	2	2	2	2	2						2	2	2	2	2	2
DS3-12E	2	2	2	2	2	2						2	2	2	2	2	2
DS3N-12	1,2	1,2	2	1,2	1,2	1,2						1,2	1,2	1,2		1,2	1,2
DS3N-12E	1,2	1,2	2	1,2	1,2	1,2						1,2	1,2	1,2		1,2	1,2
DS3XM-6	2	2	2	2	2	2						2	2	2	2	2	2
DS3XM-12	2	2	2	2	2	2						2	2	2	2	2	2
DS3/EC1-48																	
EC1-12	2	2	2	2	2	1,2						2	2	2	2	2	2

## ■ NTP-A15 共通コントロールカードの取り付け

表 2-2 XC10G および XC-VXC-10G カードのタイプとスロットの互換性 (続き)

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
E100T-12	XC10G または XC-VXC-10G カードではサポートされない。																
E1000-2	XC10G または XC-VXC-10G カードではサポートされない。																
E100T-G																	
E1000-2-G																	
CE-100T-8																	
CE-1000-4																	
G1K-4																	
ML100-12																	
ML1000-2																	
ML100X-8																	
OC3 IR 4/STM1 SH 1310																	
OC3IR/STM1SH 1310-8																	
OC12 IR STM4 SH 1310																	
OC12 LR/STM4 LH 1310																	
OC12 IR/STM4 SH 1310-4																	
OC12 LR/STM4 LH 1550																	
OC48 IR 1310																	
OC48 LR 1550																	
OC48 IR/STM16 SH AS 1310																	
OC48 LR/STM16 LH AS 1550																	
OC48-ELR/STM16 EH 100 GHz																	
OC48 ELR 200 GHz																	
OC192 SR/STM64 IO 1310																	
OC192 IR/STM64 SH 1550																	
OC192 LR/STM64 LH 1550																	
OC192 LR/STM64 LH ITU 15xx.xx																	
FC_MR-4																	

表 2-2 XC10G および XC-VXC-10G カードのタイプとスロットの互換性 (続き)

スロット	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
タイプ	MS	MS	MS	MS	MS	MS	TCC	XC	AIC-I	XC	TCC	MS	MS	MS	MS	MS	MS
OC192SR1/STM64IO Short Reach および OC192/STM64 Any Reach ( OC192-XFP カード )																	
MRC_12																	

1. 特定のスロットに装着された場合に、標準の DS1 または DS3 カードとして動作する 1:N カードを識別します。

終了：この手順は、これで完了です。

## NTP-A16 光カードおよびコネクタの取り付け

目的	この手順では、光カード (OC-3、OC-12、OC-48、OC-192、および MRC-12) の取り付け方法を示します。15454_MRC-12 (マルチレート)、OC192SR1/STM64IO Short Reach、および OC192/STM64 Any Reach (CTC では OC192-XFP) カードには、ファイバインターフェイスを装備するための Small Form-Factor Pluggable (SFP)/XFP が必要です。その他のすべての光カードでは、ファイバをカードに直接取り付けます。サイト計画が入手可能な場合は、それに従って取り付けます。
工具 / 機器	OC-3、OC-12、OC-48、OC-192、および MRC-12 カード (装着可能な場合)
事前準備手順	<a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a>
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



警告

作業中は、カードの ESD 破壊を防ぐため、必ず静電気防止用リストストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。



警告

クラス I (CDRH) およびクラス 1M (IEC) レーザー製品です。



警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器 (ルーペ、拡大鏡、顕微鏡など) で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。



警告

指定外の制御機器や調整機器を使用したり、指定外の手順を実行したりすると、有害な放射線にさらされる恐れがあります。

次に示す警告は、安全キーの付いた OC-192 カードにのみ適用されます。



警告

カードの起動時、および安全キーがオンの位置 (ラベル 1) の場合は、レーザーがオンになっています。ポートが稼働していなくても、レーザーはオンになります。安全キーがオフ (ラベル 0) の場合はレーザーもオフになります。



注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。





(注) カードのバックプレーン コネクタに保護クリップが取り付けられている場合は、カードを取り付ける前に、クリップを取り外してください。



(注) Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) から Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング) への変換とノード追加を簡素化するために、高速イースト (スロット 12 および 13) およびウエスト (スロット 5 および 6) の構成に従って光カードを取り付けます。この構成は必須ではありません。



(注) ブート処理中に、Out-of-Service (OOS) OC-N ポートから任意の In-Service (IS) 遠端側レシーバーに Line Alarm Indication Signal (AIS-L; 回線アラーム検出信号) が出力されます。AIS-L 条件の詳細については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 1** XCVT カードを取り付ける場合は、表 2-1 でカードとスロットの互換性を確認してください。XC10 または XC-VXC-10G カードを取り付けた場合は、表 2-2 でカードとスロットの互換性を確認してください。

最初に容量の大きいカードを取り付けます。たとえば、OC-192 カードを取り付けてから、OC-48 カードを取り付けます。各カードのブートを完了してから、次のカードを取り付けます。



(注) OC192-XFP カードの前面プレートには、[OC192SR1/STM64IO Short Reach] および [OC192/STM64 Any Reach] と表示されていますが、CTC では、[OC192-XFP] と省略して表示されます。

MRC-12 カードを取り付ける前に、表 2-3 を参照して、カードを取り付けるスロットごとの帯域幅制限、およびシェルフに装着されたクロスコネクタカードのタイプを確認してください。

表 2-3 さまざまなクロスコネクタ構成における MRC-12 のシェルフ スロット別最大帯域幅

XC カード タイプ	スロット 1 ~ 4 および 12 ~ 17 の最大帯域幅	スロット 5、6、12、または 13 の最大帯域幅
XCVT	OC-12	OC-48
XC10G/XC-VXC-10G	OC-48	OC-192

スロットおよび帯域幅の制限の詳細については、『Cisco ONS 15454 Reference Manual』の「Optical Cards」の章で、該当するカードのリファレンス セクションを参照してください。

**ステップ 2** カードのラッチまたはイジェクタを開きます。

**ステップ 3** ラッチまたはイジェクタを使用して、ガイド レールに沿って光カードをしっかりとスライドさせ、スロットの後方のレセプタクルに光カードを取り付けます。カードが正しく取り付けられなかった場合は、FAIL LED が連続して点滅します。



(注) スロットに誤ったカードを取り付けた場合は、「[NTP-A116 カードの取り外しおよび交換](#)」(p.2-23)を行ってください。

**ステップ4** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まることがあります。カードをそれ以上挿入できないことを確かめてください。

**ステップ5** LEDの動作を確認します。

- レッドの FAIL LED が 20 ~ 30 秒間点灯します。
- レッドの FAIL LED が 35 ~ 45 秒間点滅します。
- すべての LED が一度点滅してから、5 ~ 10 秒間消灯します。
- ACT または ACT/STBY LED がオレンジに点灯します。Signal Fail (SF; 信号障害) LED は、すべてのカードポートがそれぞれの遠端の相手先に接続されて、信号が発生するまで点灯しません。

**ステップ6** カードが適切にブートされない場合、または LED の動作が**ステップ5**のとおりにならない場合は、次の点を調べてください。

- 物理的なカードタイプが、CTC でそのスロット用にプロビジョニングされたカードのタイプに一致していない場合、カードがブートされない可能性があります。光カードがブートされない場合、カードの欠陥であると判断する前に、CTC をオープンし、スロットが別のカードタイプ用にプロビジョニングされていないかを確認してください。
- レッドの FAIL LED が点灯しない場合は、電源を調べてください。
- 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。
- レッドの FAIL LED が連続して点灯したり、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、**ステップ2 ~ 5**を繰り返してください。

**ステップ7** 光ファイバインターフェイスを装備するには、MRC-12 カードの場合は SFP、OC192SR1/STM64IO Short Reach および OC192/STM64 Any Reach (OC192-XFP) カードの場合は XFP が必要です。これらのカードのいずれかを取り付ける前に、「[DLP-A469 GBIC または SFP/XFP デバイスの取り付け](#)」(p.21-64)を実行します。これらを取り付ける前に、SFP または XFP をプロビジョニングする場合は、「[DLP-A461 SFP または XFP デバイスの事前プロビジョニング](#)」(p.21-47)を実行します。

**ステップ8** 光ファイバを取り付ける準備ができたなら、「[NTP-A247 光ファイバケーブルの取り付け](#)」(p.2-18)に進みます。

終了：この手順は、これで完了です。

## NTP-A17 電気回路カードの取り付け

目的	この手順では、電気回路カード( DS-1、DS-3、DS3XM、および EC-1EIA )の取り付け方法を示します。
工具 / 機器	電気回路カード
事前準備手順	<a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a>
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

**警告**

作業中は、カードの ESD 破壊を防ぐため、必ず静電気防止用リストストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**注意**

シェルフの DS3/EC1-48 カードと同じ側に、低密度 DS-1 カードを取り付けしないでください。

**注意**

スロット 3 に MXP\_2.5G\_10G カードが搭載してある場合は、スロット 1 または 2 に DS3/EC1-48 カードを搭載しないでください。同様に、スロット 5 に MXP\_2.5G\_10G カードが搭載してある場合は、スロット 16 または 17 に DS3/EC1-48 を搭載しないでください。このようにすると、カードが相互作用し、DS-3 ビットエラーが発生します。

**(注)**

カードのバックプレーン コネクタに保護クリップが取り付けられている場合は、カードを取り付ける前に、クリップを取り外してください。

**(注)**

最初に容量の大きいカードを取り付けます。たとえば、DS-3 カードを取り付けてから、DS-1 カードを取り付けます。各カードのブートを完了してから、次のカードを取り付けます。

**(注)**

OC-N、トランスポンダ (TXP) またはマックスポンダ (MXP) カードを取り付ける場合は、これらを取り付けてから、必要に応じて電気回路カードを取り付けることを推奨します。

- ステップ 1** XC または XCVT カードを取り付ける場合は、表 2-1 でカードとスロットの互換性を確認してください。XC10 または XC-VXC-10G カードを取り付けた場合は、表 2-2 でカードとスロットの互換性を確認してください。
- ステップ 2** カードのラッチまたはイジェクタを開きます。
- ステップ 3** ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをしっかりとスライドさせ、スロットの後方のレセプタクルにカードを取り付けます。



**(注)** スロットに誤ったカードを取り付けた場合は、「NTP-A116 カードの取り外しおよび交換」(p.2-23) を行ってください。

- ステップ 4** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



**(注)** カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

- ステップ 5** LED の動作を確認します。

- レッドの FAIL LED が 10 ~ 15 秒間点灯します。
- レッドの FAIL LED が 30 ~ 40 秒間点滅します。
- すべての LED が一度点滅してから、1 ~ 5 秒間消灯します。
- ACT または ACT/STBY LED が点灯します。SF LED は、すべてのカード ポートがそれぞれの遠端の相手先に接続されて、信号が発生するまで点灯します。

- ステップ 6** カードが適切にブートされない場合、または LED の動作がステップ 5 のとおりにならない場合は、次の点を調べてください。

- レッドの FAIL LED が点灯しない場合は、電源を調べてください。
- 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。
- レッドの FAIL LED が連続して点灯したり、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 2 ~ 5 を繰り返してください。

- ステップ 7** 必要に応じて、「NTP-A246 イーサネット カードおよびコネクタの取り付け」(p.2-13) へ進みます。

**終了：**この手順は、これで完了です。

## NTP-A246 イーサネット カードおよびコネクタの取り付け

目的	この手順では、イーサネットカード (E100T-12、E100T-G、E1000-2、E1000-2-G、G1K-4、ML100T-12、ML1000-2、ML100X-8、CE-100T-8、および CE-1000-4) の取り付け方法を示します。
工具 / 機器	イーサネットカード
事前準備手順	<a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a>
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

**警告**

作業中は、カードの ESD 破壊を防ぐため、必ず静電気防止用リストストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。

**警告**

クラス I (CDRH) およびクラス 1M (IEC) レーザー製品です。

**警告**

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器 (ルーペ、拡大鏡、顕微鏡など) で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。

**警告**

指定外の制御機器や調整機器を使用したり、指定外の手順を実行したりすると、有害な放射線にさらされる恐れがあります。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**(注)**

カードのバックプレーン コネクタに保護クリップが取り付けられている場合は、カードを取り付ける前に、クリップを取り外してください。

**(注)**

OC-N、TXP、または MXP カードを取り付ける場合は、これらを取り付けてから、イーサネットカードを取り付けることを推奨します。

## ■ NTP-A246 イーサネット カードおよびコネクタの取り付け

**ステップ 1** XC または XCVT カードを取り付ける場合は、[表 2-1](#) でカードとスロットの互換性を確認してください。XC10 または XC-VXC-10G カードを取り付けた場合は、[表 2-2](#) でカードとスロットの互換性を確認してください。

**ステップ 2** 「[DLP-A39 イーサネット カードの取り付け](#)」(p.17-49) を実行します。各カードのブートを完了してから、次のカードを取り付けます。



**(注)** スロットに誤ったカードを取り付けた場合は、「[NTP-A116 カードの取り外しおよび交換](#)」(p.2-23) を行ってください。

**ステップ 3** E1000-2、E1000-2-G、ML1000-2、ML100X-8、または CE-1000-4 カードを使用している場合は、「[DLP-A469 GBIC または SFP/XFP デバイスの取り付け](#)」(p.21-64) を行います。



**(注)** GBIC または SFP/XFP を取り外す必要がある場合は、「[DLP-A470 GBIC または SFP/XFP デバイスの取り外し](#)」(p.21-68) を行います。

**ステップ 4** 必要に応じて、「[NTP-A274 FC\\_MR-4 カードの取り付け](#)」(p.2-15) へ進みます。

**終了：**この手順は、これで完了です。

## NTP-A274 FC\_MR-4 カードの取り付け

目的	この手順では、ファイバチャネル(FC_MR-4)カードを取り付けます。
工具 / 機器	FC_MR-4 カード
事前準備手順	<a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a>
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

**警告**

作業中は、カードの ESD 破壊を防ぐため、必ず静電気防止用リストストラップを着用してください。感電する危険があるので、手や金属工具がバックプレーンに直接触れないようにしてください。

**警告**

クラス I (CDRH) およびクラス 1M (IEC) レーザー製品です。

**警告**

終端していない光ファイバケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器（ルーペ、拡大鏡、顕微鏡など）で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。

**警告**

指定外の制御機器や調整機器を使用したり、指定外の手順を実行したりすると、有害な放射線にさらされる恐れがあります。

**警告**

カード上の高性能デバイスは、動作中に高温になることがあります。カードを取り外すときは、前面プレートと下端を持ってください。それ以外の箇所に触ったり、静電気防止用袋にカードを入れたりする場合は、カードが冷えてからにしてください。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフアセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**(注)**

カードのバックプレーンコネクタに保護クリップが取り付けられている場合は、カードを取り付ける前に、クリップを取り外してください。

**ステップ 1** XCVT カードを取り付ける場合は、表 2-1 でカードとスロットの互換性を確認してください。XC10 または XC-VXC-10G カードを取り付けた場合は、表 2-2 でカードとスロットの互換性を確認してください。

**ステップ 2** カードのラッチまたはイジェクタを開きます。

**ステップ 3** ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをしっかりとスライドさせ、スロットの後方のレセプタクルにカードを取り付けます。



**(注)** スロットに誤ったカードを取り付けた場合は、「NTP-A116 カードの取り外しおよび交換」(p.2-23)を行ってから、正しいカードを取り付けてください。

**ステップ 4** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



**(注)** カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

**ステップ 5** LED の動作を確認します。

- レッドの FAIL LED が 20 ~ 30 秒間点灯します。ACT LED が 3 ~ 5 秒間オレンジに点灯します。
- レッドの FAIL LED が最大 2 分間点滅します。
- FAIL LED と ACT LED が一度点滅してから、1 ~ 5 秒間消灯します。
- ACT LED がグリーンに点灯します。



**(注)** レッドの FAIL LED が点灯しない場合は、電源を調べてください。



**(注)** 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

**ステップ 6** 「DLP-A469 GBIC または SFP/XFP デバイスの取り付け」(p.21-64)を行って、FC\_MR-4 カードに GBIC を取り付けます。




**(注)** GBIC または SFP/XFP を取り外す必要がある場合は、「DLP-A470 GBIC または SFP/XFP デバイスの取り外し」(p.21-68)を行います。

**ステップ 7** 「NTP-A247 光ファイバケーブルの取り付け」(p.2-18)へ進んでください。

**終了：**この手順は、これで完了です。



## NTP-A316 フィラー カードの取り付け

目的	この手順では、未使用のトラフィック カード スロットまたは AIC-I カード スロット (スロット 1 ~ 6、9、および 12 ~ 17) にフィラー カードを取り付ける方法について説明します。フィラー カードは前面プレートの付いたカードです。
	 <p>(注) フィラー カードには次の 2 種類があります。1 つは CTC で検出できない、前面プレートにラベルのないタイプです。もう 1 つは CTC で検出可能な、前面プレートに FILLER ラベルの付いたタイプです。</p>
工具 / 機器	<p>フィラー カード</p> <p>シスコ部品番号 15454-FILLER (検出可能)</p> <p>シスコ部品番号 15454-BLANK (検出不可能)</p>
事前準備手順	<p><a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a></p> <p><a href="#">NTP-A16 光カードおよびコネクタの取り付け (p.2-8)</a></p> <p><a href="#">NTP-A17 電気回路カードの取り付け (p.2-11)</a></p> <p><a href="#">NTP-A246 イーサネット カードおよびコネクタの取り付け (p.2-13)</a></p> <p><a href="#">NTP-A274 FC_MR-4 カードの取り付け (p.2-15)</a></p>
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



### 警告

フィラー カードには 3 つの重要な機能があります。シャーシ内の危険な電圧および電流による感電を防ぐこと、他の装置への EMI (電磁波干渉) の影響を防ぐこと、およびシャーシ内の冷気の流れを適切な状態に保つことです。必ずすべてのカードおよび前面プレートを正しく取り付けられた状態で、システムを運用してください。



### 注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンド ケーブルを接続し、シェルフ アセンブリが正しくアースされていることを確認します。

- ステップ 1** カードのイジェクタを開きます。
- ステップ 2** カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- ステップ 3** イジェクタを閉じます。
- ステップ 4** 残りの未使用カード スロットに上記手順を繰り返します。

## ■ NTP-A247 光ファイバケーブルの取り付け

**ステップ 5** CTC にログインしたら、検出可能なフィルアードカードが CTC ノード ビューに正しく表示されているか確認します。検出不可能なフィルアードカードは、CTC ノード ビューに表示されません。

終了：この手順は、これで完了です。

## NTP-A247 光ファイバケーブルの取り付け

目的	この手順では、トポロジーに従って、光カードに光ファイバケーブルを取り付けます。GBIC、SFP、または XFP に光ファイバケーブルを取り付ける場合は、「 <a href="#">DLP-A469 GBIC または SFP/XFP デバイスの取り付け</a> 」(p.21-64)を参照してください。
工具 / 機器	光ファイバケーブル ファイバブーツ ファイバクリップ
事前準備手順	<a href="#">NTP-A16 光カードおよびコネクタの取り付け</a> (p.2-8) <a href="#">NTP-A112 ファイバコネクタの清掃</a> (p.15-20)
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



警告

クラス I (CDRH) およびクラス 1M (IEC) レーザー製品です。



警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器 (ルーペ、拡大鏡、顕微鏡など) で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。



警告

指定外の制御機器や調整機器を使用したり、指定外の手順を実行したりすると、有害な放射線にさらされる恐れがあります。

次に示す警告は、安全キーの付いた OC-192 カードにのみ適用されます。



警告

カードの起動時、および安全キーがオンの位置 (ラベル 1) の場合は、レーザーがオンになっています。ポートが稼働していなくても、レーザーはオンになります。安全キーがオフ (ラベル 0) の場合はレーザーもオフになります。

**警告**

レーザー光線によって目に見えない事故が発生することがあります。そのため、作業する場合は、レーザー光線が目や体に照射されないように注意してください。この機器に関する作業は、相応の資格がある担当者がレーザーの安全手順を遵守して担当してください。また、この機器に関する作業を始める前に、適切に目を保護してください。

**注意**

20 dB 減衰器を使用している場合以外は、OC192LR/STM64 LH 1550 または OC192LR/STM64 LH ITU 15xx.xx カードでファイバループバックを使用しないでください。ファイバループバックを直接接続しないでください。ファイバループバックを使用すると、OC192 LR/STM64 LH 1550 または OC192 LR/STM64 LH ITU 15xx.xx カードに修復不可能な損傷を引き起こすことがあります。

**注意**

5 dB 減衰器を使用している場合以外は、OC192 IR/STM64 SH 1550 カードでファイバループバックを使用しないでください。非減衰ファイバループバックを直接接続しないでください。非減衰ファイバループバックを使用すると、OC192 IR/STM64 SH 1550 カードに修復不可能な損傷を引き起こすことがあります。

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフアセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**(注)**

OC192 カードまたは OC48 AS カードの場合は、光ポートの角度が下向きになっているため、ファイバブーツを使用しないでください。

**(注)**

カードを取り付けると、ただちに光ファイバケーブルを取り付けることができます。あるいは、ネットワークを立ち上げる準備ができるまで待ちます。第5章「ネットワークの起動」を参照してください。

**ステップ 1**

取り付けたカードの光受信レベルをテストして、それに応じて減衰させます。最小レベルと最大レベルについては、表 2-4 を参照してください。

**(注)**

15454\_MRC-12、OC192SR1/STM64IO Short Reach、および OC192/STM64 Any Reach (OC192-XFP) カードのレベルは、ポートに取り付けられた特定の SFP/XFP によって決まります。表 2-4 では、これらのカードの SFP/XFP をカッコ内に示しています。

表 2-4 光カードの送受信レベル

カード	送信		受信	
	最小	最大	最小	最大
OC3 IR 4/STM1 SH 1310	-15 dBm	-8 dBm	-28 dBm	-8 dBm
OC3IR/STM1SH 1310-8	-15 dBm	-8 dBm	-28 dBm	-8 dBm
OC12 IR/STM4 SH 1310	-15 dBm	-8 dBm	-28 dBm	-8 dBm
OC12 LR/STM4 LH 1310	-3 dBm	+2 dBm	-28 dBm	-8 dBm
OC12 LR/STM4 LH 1550	-3 dBm	+2 dBm	-28 dBm	-8 dBm
OC12 IR/STM4 SH 1310-4	-15 dBm	-8 dBm	-30 dBm	-8 dBm
OC48 IR 1310	-5 dBm	0 dBm	-18 dBm	0 dBm
OC48 LR 1550	-2 dBm	+3 dBm	-28 dBm	-8 dBm
OC48 IR/STM16 SH AS 1310	-5 dBm	0 dBm	-18 dBm	0 dBm
OC48 LR/STM16 LH AS 1550	-2 dBm	+3 dBm	-28 dBm	-8 dBm
OC48 ELR/STM16 EH 100 GHz	-2 dBm	0 dBm	-27 dBm (1E-12 BER の 場合)	-9 dBm
OC48 ELR/STM16 EH 200 GHz	-2 dBm	0 dBm	-28 dBm	-8 dBm
OC192 SR/STM64 IO 1310	-6 dBm	-1 dBm	-11 dBm	-1 dBm
OC192 IR/STM64 SH 1550	-1 dBm	+2 dBm	-14 dBm	-1 dBm
OC192 LR/STM64 LH 1550	+7 dBm	+10 dBm	-19 dBm	-10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	+3 dBm	+6 dBm	-22 dBm	-9 dBm
15454_MRC-12 (ONS-SI-2G-S1)	-10 dBm	-3 dBm	-18 dBm	-3 dBm
15454_MRC-12 (ONS-SI-2G-I1)	-5 dBm	0 dBm	-18 dBm	0 dBm
15454_MRC-12 (ONS-SI-2G-L1)	-2 dBm	3 dBm	-27 dBm	-9 dBm
15454_MRC-12 (ONS-SI-2G-L2)	-2 dBm	3 dBm	-28 dBm	-9 dBm
15454_MRC-12 (ONS-SC-2G-30.3 ~ ONS-SC-2G-60.6)	0 dBm	4 dBm	-28 dBm	-9 dBm
15454_MRC-12 (ONS-SI-622-I1)	-15 dBm	-8 dBm	-28 dBm	-8 dBm
15454_MRC-12 (ONS-SI-622-L1)	-3 dBm	2 dBm	-28 dBm	-8 dBm
15454_MRC-12 (ONS-SI-622-L2)	-3 dBm	2 dBm	-28 dBm	-8 dBm
15454_MRC-12 (ONS-SE-622-1470 ~ ONS-SE-622-1610)	0 dBm	5 dBm	-28 dBm	-3 dBm
15454_MRC-12 (ONS-SI-155-I1)	-15 dBm	-8 dBm	-30 dBm	-8 dBm
15454_MRC-12 (ONS-SI-155-L1)	-5 dBm	0 dBm	-34 dBm	-10 dBm
15454_MRC-12 (ONS-SI-155-L2)	-5 dBm	0 dBm	-34 dBm	-10 dBm
15454_MRC-12 (ONS_SE-155-1470 ~ ONS-SE-155-1610)	0 dBm	5 dBm	-34 dBm	-3 dBm
OC192SR1/STM64IO Short Reach (ONS-XC-10G-S1)	-6 dBm	-1 dBm	-11 dBm	-1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-S1)	-6 dBm	-1 dBm	-11 dBm	-1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-I2)	-1 dBm	2 dBm	-14 dBm	2 dBm
OC192/STM64 Any Reach (ONS-XC-10G-L2)	0 dBm	4 dBm	-24 dBm	-7 dBm

- ステップ 2** 必要に応じて、「DLP-A207 LGX インターフェイスへの光ファイバケーブルの取り付け」(p.19-6)を行います。
- ステップ 3** 必要に応じて、「DLP-A428 1+1 構成での光ファイバケーブルの取り付け」(p.21-8)を行います。
- ステップ 4** 必要に応じて、「DLP-A43 UPSR 構成での光ファイバケーブルの取り付け」(p.17-51)を行います。
- ステップ 5** 必要に応じて、「DLP-A44 BLSR 構成での光ファイバケーブルの取り付け」(p.17-55)を行います。
- ステップ 6** 「NTP-A245 光ファイバケーブルの配線」(p.2-22)へ進んでください。

終了：この手順は、これで完了です。

---

## NTP-A245 光ファイバケーブルの配線

目的	この手順では、ファイバブーツやファイバクリップの取り付けなど、ONS 15454 シェルフからの光ファイバケーブルの配線方法を示します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A247 光ファイバケーブルの取り付け (p.2-18)</a>
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** 必要に応じて、「[DLP-A45 ファイバブーツの取り付け](#)」(p.17-57)を行います。OC-192、OC192SR1/STM64IO Short Reach、OC192/STM64 Any Reach (OC192-XFP) および OC-48 AS カードを除くすべての OC-N カードに、ファイバブーツが必要です。
- ステップ 2** ケーブル マネジメント トレイの折畳式前面扉を開きます。
- ステップ 3** カードの前面プレート上の光ファイバ ケーブルを、前面プレート上のファイバ クリップ (付属している場合)を通して配線します。
- ステップ 4** 15454\_MRC-12 カードを取り付ける場合は、「[DLP-A443 15454\\_MRC-12 カードへのファイバクリップの取り付け](#)」(p.21-25)を実行します。15454\_MRC-12 カードを除く光カードの前面プレートには、出荷時にファイバクリップが取り付けられています。15454\_MRC-12 カードには、前面プレートに装着する 2 種類のファイバクリップが同梱されています。
- ステップ 5** 光ファイバケーブルをケーブル マネジメント トレイに配線します。
- ステップ 6** 光ファイバ ケーブルを、シェルフ アセンブリのそれぞれの側にある切り欠き部を通して、ケーブル マネジメント トレイのいずれかの側から外部に配線します。方向反転可能なファイバ ガイドを使用して、希望する側から外部にケーブルを配線します。
- ステップ 7** 前面のコンパートメント内のすべての光ファイバケーブルが適切に配線されたら、折畳式の前面扉を閉めます。

**終了：**この手順は、これで完了です。

---

## NTP-A116 カードの取り外しおよび交換

目的	この手順では、ONS 15454 シェルフおよびラック内のすべてのカードを取り外して、取り付けます。
工具 / 機器	なし
事前準備手順	カードの取り付け手順
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** CTC にログインせずにカードを取り外す必要がある場合は、[ステップ 3](#) で説明されている手順に従ってカードを取り外します。CTC にログインする場合は、『Cisco ONS 15454 SDH Troubleshooting Guide』を参照して、Mismatched Equipment Alarm (MEA) のトラブルシューティングを行います。

**ステップ 2** CTC にログインしている場合は、次のいずれかを行います。

- 「[DLP-A191 カードの削除](#)」(p.18-65) を行って、[ステップ 3](#) へ進みます。
- 「[DLP-A247 OC-N カードの変更](#)」(p.19-33) を行ってカードを削除し、既存のプロビジョニングを維持しながら別の OC-N カードと交換します。

**ステップ 3** カードを取り外します。

- a. カードのラッチまたはイジェクタを開きます。
- b. ラッチまたはイジェクタを使用してカードを前に引き出し、シェルフから取り出します。

**ステップ 4** 適宜、次のいずれかの手順を使用して、新しいカードを挿入します。

- [NTP-A15 共通コントロールカードの取り付け](#) (p.2-2)
- [NTP-A16 光カードおよびコネクタの取り付け](#) (p.2-8)
- [NTP-A17 電気回路カードの取り付け](#) (p.2-11)
- [NTP-A246 イーサネットカードおよびコネクタの取り付け](#) (p.2-13)
- [NTP-A274 FC\\_MR-4 カードの取り付け](#) (p.2-15)

**ステップ 5** 必要に応じて、「[NTP-A247 光ファイバケーブルの取り付け](#)」(p.2-18) へ進みます。

**終了：**この手順は、これで完了です。

## NTP-A20 前面扉の交換

目的	この手順では、カードおよび光ファイバケーブルを取り付けたあとに、前面扉と扉のアースストラップを交換します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	NTP-A3 前面扉のオープンと取り外し (p.1-7)
必須 / 適宜	必須
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

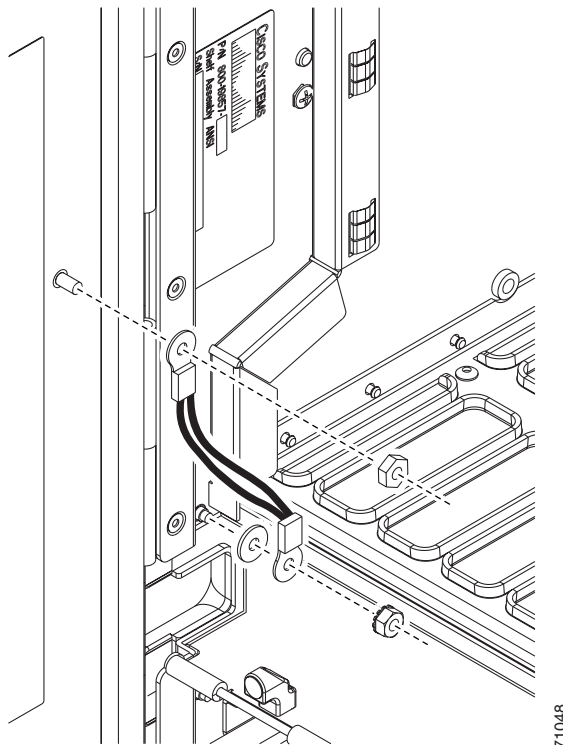


(注) 光カードに接続されている光ファイバケーブルを圧迫しないように注意してください。ファイバブーツが付属していないものもあります。

**ステップ 1** 前面扉をシェルフ アセンブリのヒンジに挿入します。

**ステップ 2** アースストラップ圧着端子 (72-3622-01) の一端を、扉内のオススタッドに取り付けます。オープンエンドレンチを使用して #6 ケブナット (49-0600-01) を取り付け、締めます (図 2-1)。

図 2-1 扉のアースストラップ改良キットの取り付け



71048



**ステップ3** ファイバガイドの長い方のネジに、アースストラップの他端を取り付けます。

- a. ロックワッシャを取り付けます。
- b. 圧着端子を取り付けます。
- c. オープンエンドレンチを使用して圧着端子に #4 ケブナット (49-0337-01) を取り付け、締めます。



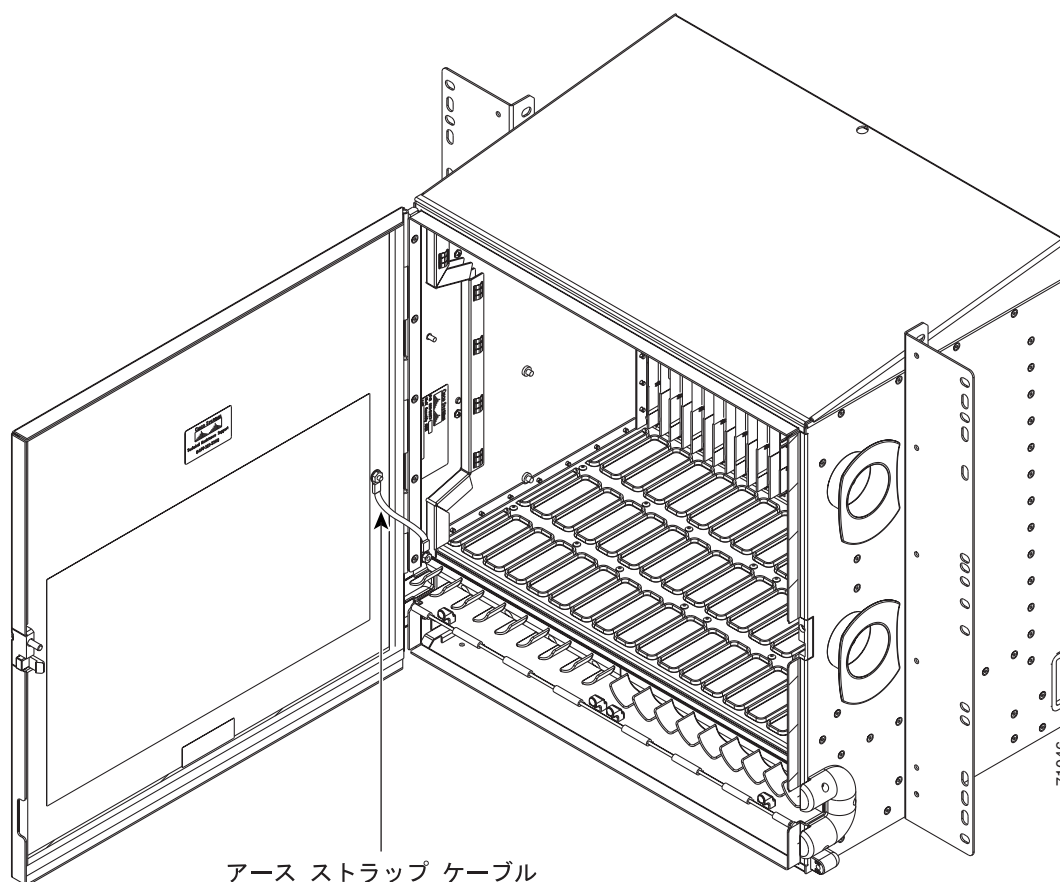
**(注)** トラフィック (回線) の干渉を防止するために、扉が開いている場合は、アースストラップがフラットな位置になっていることを確認します。アースストラップをフラットな位置に移動するには、圧着端子を左回りに回してから、ケブナットを締めます。

**ステップ4** 左側のケーブル配線チャンネルを交換します。

**ステップ5** プラスドライバを使用して、ケーブル配線チャンネルのネジを差し込んで、締めます。

図 2-2 に、前面扉およびアースストラップが取り付けられたシェルフアセンブリを示します。

**図 2-2** 扉のアースストラップ改良キットが取り付けられたシェルフアセンブリ



**ステップ6** 扉を閉めます。



(注) ONS 15454 には、前面扉をロックおよびロック解除するピン付き六角キーが付属しています。キーを左回りに回転させると扉がロック解除され、右回りに回転させるとロックされます。

終了：この手順は、これで完了です。

---



## PC の接続と GUI へのログイン

この章では、Cisco ONS 15454 に PC とワークステーションを接続する方法と、Cisco ONS 15454 の Operation, Administration, Maintenance and Provisioning (OAM&P) ユーザ インターフェイスである Cisco Transport Controller (CTC) ソフトウェアへログインする方法について説明します。TL1 を使用して ONS 15454 に接続する手順については、『Cisco ONS SONET TL1 Reference Guide』を参照してください。

### 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A260 CTC 用コンピュータのセットアップ \(p.3-2\)](#)— PC またはワークステーションをこれまで ONS 15454 に接続したことがない場合は、この手順を実行します。
2. [NTP-A234 ONS 15454 へローカルにクラフト接続するための CTC コンピュータのセットアップ \(p.3-4\)](#)— ONS 15454 にオンサイトでクラフト接続するようにコンピュータを設定する場合は、この手順を実行します。
3. [NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ \(p.3-6\)](#)— 社内 LAN を介して ONS 15454 に接続するようにコンピュータを設定する場合は、この手順を実行します。
4. [NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ \(p.3-7\)](#)— ONS 15454 にリモート モデムを介してアクセスするようにコンピュータを設定する場合は、この手順を実行します。
5. [NTP-A23 ONS 15454 GUI へのログイン \(p.3-8\)](#)— CTC にログインする場合は、この手順を実行します。

## NTP-A260 CTC用コンピュータのセットアップ

目的	この手順では、CTCを実行するようにPCまたはUNIXワークステーションを設定します。
工具 / 機器	Cisco ONS 15454 Release 7.2 ソフトウェアまたは Documentation CD
事前準備手順	<a href="#">第1章「シェルフおよびバックプレーンケーブルの取り付け」</a>
必須 / 適宜	必須
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)

ソフトウェアリリース 7.2 を実行中のノードへログインする場合は、JRE 1.4.2 または JRE 5.0 が必要です。4.5 以前のリリースを実行中のノードへログインする場合は、JRE 1.4.1 または 5.0 をアンインストールしてから、JRE 1.3.1\_2 をインストールする必要があります。必要に応じて、「[DLP-A431 JRE バージョンの入れ替え](#)」(p.21-10) を実行してください。

- ステップ 1** コンピュータに適切なブラウザがインストールされていない場合は、次の操作を実行してください。
- Netscape 7.x をインストールする場合は、次のサイトからブラウザをダウンロードします。  
<http://channels.netscape.com/ns/browsers/default.jsp>
  - PC に Internet Explorer 6.x をインストールする場合は、次のサイトからブラウザをダウンロードします。  
<http://www.microsoft.com>
- ステップ 2** CTC のパフォーマンスを向上させるために、JVM ヒープのサイズを小さくするには、「[DLP-A552 JVM ヒープサイズの調整](#)」(p.22-61) を実行します。
- ステップ 3** コンピュータが Windows PC の場合は、「[DLP-A337 Windows での CTC インストールウィザードの実行](#)」(p.20-27) を行ってから **ステップ 5** へ進んでください。
- ステップ 4** コンピュータが UNIX ワークステーションの場合は、「[DLP-A338 UNIX での CTC インストールウィザードの実行](#)」(p.20-31) を行ってください。
- ステップ 5** PC またはワークステーションが準備できている場合は、ネットワークに合わせて次のセットアップ手順を実行してください。
- [NTP-A234 ONS 15454 へローカルにクラフト接続するための CTC コンピュータのセットアップ](#) (p.3-4)
  - [NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ](#) (p.3-6)
  - [NTP-A236 ONS 15454 へのリモートアクセス接続のセットアップ](#) (p.3-7)



(注) シスコの光機器へのアクセスに使用するコンピュータでは、ユーザ ID またはパスワードのキャッシュをディセーブルにするようにブラウザを設定することを推奨します。

Internet Explorer では、[ ツール ] > [ インターネット オプション ] > [ コンテンツ ] をクリックします。[ オートコンプリート ] をクリックし、[ フォームのユーザ名およびパスワード ] オプションをオフにします。

Netscape 7.0 では、[ 編集 ] > [ 設定 ] > [ プライバシーとセキュリティ ] > [ フォーム ] をクリックし、フォーム データの保存に関するオプションをオフにします。パスワードについては、[ 編集 ] > [ 設定 ] > [ プライバシーとセキュリティ ] > [ パスワード ] をクリックし、パスワードの保存に関するオプションをオフにします。パスワードは、暗号化して保存できます。Netscape 6.0 より前のバージョンでは、ユーザ ID とパスワードをキャッシュに保存できません。

終了：この手順は、これで完了です。

---

# NTP-A234 ONS 15454 ヘローカルにクラフト接続するためのCTC コンピュータのセットアップ

目的	この手順では、ONS 15454 にオンサイトでローカル クラフト接続するように Windows PC または Solaris ワークステーションをセットアップします。
工具 / 機器	Network Interface Card (NIC)、イーサネット カードとも呼ばれています。  ストレート型 (CAT5) LAN ケーブル
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
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

**ステップ 1** [表 3-1](#) に示す CTC コンピュータのセットアップ作業の中から、CTC の接続環境に合わせて必要なものを実行してください。

**表 3-1 ONS15454 ヘローカルにクラフト接続するためのCTC コンピュータのセットアップ**



CTC の接続環境	CTC コンピュータのセットアップ作業
<ul style="list-style-type: none"> <li>• Windows PC から接続する。</li> <li>• アクセスするすべてのノードで Release 3.3 より前のソフトウェアが実行されている。</li> <li>• 1 台の ONS 15454 に接続する。</li> <li>• ONS 15454 には備わっていないアプリケーション (ping や tracert [トレース ルート] など) へアクセスする必要がある。</li> </ul>	<a href="#">DLP-A50 スタティック IP アドレスを使用して同一サブネット上の ONS 15454 にクラフト接続するための Windows PC の設定 (p.17-58)</a>
<ul style="list-style-type: none"> <li>• Windows PC から接続する。</li> <li>• CTC コンピュータが Dynamic Host Configuration Protocol (DHCP) 向けにプロビジョニングされている。</li> <li>• ONS 15454 で DHCP フォワーディングがイネーブルになっている。</li> <li>• ONS 15454 が DHCP サーバに接続されている。</li> </ul>	<a href="#">DLP-A51 DHCP を使用して ONS 15454 にクラフト接続するための Windows PC の設定 (p.17-61)</a>
<p> <b>(注)</b> ONS 15454 は、IP アドレスを提供しません。DHCP をイネーブルにした場合は、DCHP 要求を外部の DHCP サーバに渡します。</p>	<p> <b>(注)</b> 最初のノードを立ち上げるときには、この作業を使用しないでください。この作業は、ONS 15454 で DHCP フォワーディングがイネーブルになっている場合にだけ使用してください。デフォルトでは、DHCP がディセーブルになっています。イネーブルにする場合は、「<a href="#">NTP-A169 CTC ネットワーク アクセスの設定</a>」(p.4-9) を参照してください。</p>

表 3-1 ONS15454 ヘローカルにクラフト接続するためのCTC コンピュータのセットアップ (続き)

CTC の接続環境	CTC コンピュータのセットアップ作業
<ul style="list-style-type: none"> <li>Windows PC から接続する。</li> <li>アクセスするすべてのノードでソフトウェア Release 3.3 以降が実行されている。</li> <li>別々の場所にある ONS 15454 ノードに何度も接続するが、そのたびに PC の IP を再設定しなくてもすむようにしたい。</li> <li>ONS 15454 には備わっていないアプリケーション (ping や tracert [トレース ルート] など) へアクセスしたり、使用したりしない。</li> <li>ONS 15454 TCC2/TCC2P イーサネット ポートまたは FMEC LAN ピンに直接接続するか、ハブを介して接続する。</li> </ul>	DLP-A52 自動ホスト検出を使用して ONS 15454 にクラフト接続するための Windows PC の設定 (p.17-63)
<ul style="list-style-type: none"> <li>Solaris ワークステーションから接続する。</li> <li>1 台の ONS 15454 に接続する。</li> <li>ONS 15454 には備わっていないアプリケーション (ping や traceroute など) へアクセスする必要がある。</li> </ul>	DLP-A53 ONS 15454 にクラフト接続するための Solaris ワークステーションの設定 (p.17-66)

**ステップ 2** ストレート型 (CAT-5) LAN ケーブルを PC または Solaris ワークステーションの NIC から次のどれかに直接接続します。

- アクティブまたはスタンバイ TCC2/TCC2P カード上の RJ-45 (LAN) ポート
- ONS 15454 を物理的に接続するハブまたはスイッチ上の RJ-45 (LAN) ポート



**(注)** 独自のストレート型 (CAT-5) LAN ケーブルを圧着する方法については、『Cisco ONS 15454 SDH Troubleshooting Guide』を参照してください。



**(注)** シェルフを最初に立ち上げる場合は、PC を ONS15454 の TCC2/TCC2P カードの LAN ポートに直接接続する必要があります。

**ステップ 3** CTC コンピュータのセットアップを終えたら、必要に応じて「NTP-A23 ONS 15454 GUI へのログイン」(p.3-8)に進みます。

**終了:** この手順は、これで完了です。

## NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ

目的	この手順では、社内 LAN を介して ONS 15454 にアクセスするようにコンピュータをセットアップします。
工具 / 機器	NIC。イーサネットカードとも呼ばれています。
事前準備手順	ストレート型 (CAT5) LAN ケーブル <ul style="list-style-type: none"> <li>• <a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a></li> <li>• ONS 15454 に LAN の接続に必要な情報 (IP アドレス、サブネットマスク、デフォルトゲートウェイなど) がプロビジョニングされていること</li> <li>• ONS 15454 が社内 LAN に物理的に接続されていること</li> <li>• CTC コンピュータを、ONS 15454 SDH に接続可能な社内 LAN に接続しておくこと</li> </ul>
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

**ステップ 1** コンピュータが社内 LAN にすでに接続されている場合は、[ステップ 3](#) へ進みます。ONS 15454 へクラフトアクセスするようにコンピュータのネットワーク設定を変更した場合は、設定内容を社内 LAN へアクセスする設定に戻します。通常は、次の操作を実行します。

- TCP/IP ダイアログボックスにある IP アドレスを [ [IP アドレスを自動的に取得](#) ] (Windows 98、2000、または XP の場合) または [ [DHCP サーバから IP アドレスを取得する](#) ] (Windows NT の場合) に設定します。
- 使用している LAN で Domain Name System (DNS; ドメインネームシステム) または Windows Internet Naming Service (WINS) をイネーブルにする必要がある場合は、TCP/IP ダイアログボックスの [ [DNS 設定](#) ] タブまたは [ [WINS 設定](#) ] タブで設定を変更します。

**ステップ 2** ストレート型 (CAT-5) LAN ケーブルを PC または Solaris ワークステーションの NIC カードから社内 LAN ポートに直接接続します。

**ステップ 3** コンピュータがプロキシサーバに接続されている場合は、プロキシサービスをディセーブルにするか、または ONS 15454 ノードを例外として追加します。プロキシサービスをディセーブルにする場合は、使用している Web ブラウザに応じて次のいずれかの作業を行います。

- [DLP-A56 Internet Explorer によるプロキシサービスのディセーブル化 \(Windows\) \(p.17-69\)](#)
- [DLP-A57 Netscape によるプロキシサービスのディセーブル化 \(Windows および UNIX\) \(p.17-70\)](#)

**ステップ 4** 「[NTP-A23 ONS 15454 GUI へのログイン](#)」(p.3-8) へ進んでください。

終了：この手順は、これで完了です。



## NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ

目的	この手順では、LAN モデムを介して CTC コンピュータを ONS 15454 に接続します。
工具 / 機器	モデムおよびモデムのマニュアル。
事前準備手順	<ul style="list-style-type: none"><li>• <a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a></li><li>• モデムを ONS 15454 に接続する必要があります。</li><li>• ONS 15454 に対応するようにモデムをプロビジョニングする必要があります。CTC を実行するには、イーサネット アクセスに対応するようにモデムをプロビジョニングする必要があります。</li></ul>
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** TCC2/TCC2P カード上の RJ-45 (LAN) ポートまたは ONS 15454 バックプレーンの LAN ピンにモデムを接続します。

**ステップ 2** モデムのマニュアルを参照しながら次の作業を行って、ONS 15454 用にモデムをプロビジョニングします。

- CTC アクセスの場合は、イーサネット アクセス用にモデムを設定します。
- モデムに ONS 15454 と同じサブネット上の IP アドレスを割り当てます。
- モデムから CTC コンピュータに割り当てる IP アドレスは、そのモデムおよび ONS 15454 と同じサブネット上に存在しなければなりません。



**(注)** 特定のモデムをプロビジョニングする際のサポートについては、Cisco Technical Assistance Center (TAC) に連絡してください。詳細については、「[テクニカル サポート](#)」(p.xxix) を参照してください。

**ステップ 3** 「[NTP-A23 ONS 15454 GUI へのログイン](#)」(p.3-8) へ進んでください。

終了：この手順は、これで完了です。

## NTP-A23 ONS 15454 GUIへのログイン

目的	この手順では、CTC (ONS 15454 の管理に使用する GUI [グラフィカル ユーザ インターフェイス] ソフトウェア) へログインします。この手順には、任意のノード ログイン作業が含まれています。
工具 / 機器	なし
事前準備手順	NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)  次の手順のいずれかを実行します。 <ul style="list-style-type: none"> <li>• NTP-A234 ONS 15454 へローカルにクラフト接続するための CTC コンピュータのセットアップ (p.3-4)</li> <li>• NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ (p.3-6)</li> <li>• NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ (p.3-7)</li> </ul>
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** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。



(注) CTC 内をナビゲートする方法については、付録 A 「CTC の情報およびショートカット」を参照してください。

ネットワーク トポロジーの検出時に、CTC はネットワークの各ノードでポーリングを行い、CTC ソフトウェアの最新バージョンがあるノードを判別します。CTC により、現在実行中のバージョンより新しいバージョンの CTC ソフトウェアがあるネットワークのノードが検出されると、CTC はネットワークに新しいバージョンの CTC が見つかったことを示すメッセージを生成し、CTC ソフトウェアのアップグレードのインストールを提示します。ネットワーク調査がディセーブルになっている場合、CTC による最新バージョンのソフトウェアの検索は行われません。アップグレード検出には、到達不能なノードは含まれません。



(注) CTC ソフトウェアのアップグレードを行うと、既存のソフトウェアは上書きされます。アップグレードが完了したら、CTC を再起動する必要があります。

**ステップ 2** 必要に応じて、「DLP-A61 ログイン ノードグループの作成」(p.17-74) を行います。ログイン ノードグループを使用することにより、Data Communication Channel (DCC; データ通信チャネル) を介してログイン ノードに接続されていないノードを管理できます。

**ステップ 3** 必要に応じて、「DLP-A62 現在のセッションまたはログイン グループへのノードの追加」(p.17-75) を行います。

**ステップ 4** 必要に応じて、「DLP-A339 現在のセッションまたはログイン グループからのノードの削除」(p.20-34) を行います。

- ステップ5** 必要に応じて、「[DLP-A372 指定したログイン ノード グループからのノードの削除](#)」(p.20-62)を行います。
- ステップ6** 必要に応じて、「[DLP-A327 CTC Alerts ダイアログボックスの自動ポップアップ設定](#)」(p.20-18)を行います。

**終了：**この手順は、これで完了です。

---





# ノードの起動

この章では、単一の Cisco ONS 15454 ノードをプロビジョニングし、運用に向けて起動する方法について説明します。具体的にはノード名、日時、タイミング基準、IP アドレスやデフォルト ルータなどのネットワーク アトリビュート、ユーザとユーザ セキュリティ、カード保護グループなどの割り当て方法を説明します。

## 準備作業

次の章に記載されている作業の中から、サイト計画に合った作業を実行します。

- [第 1 章「シェルフおよびバックプレーン ケーブルの取り付け」](#)
- [第 2 章「カードおよび光ファイバケーブルの取り付け」](#)
- [第 3 章「PC の接続と GUI へのログイン」](#)

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A323 カードの取り付けの確認 \(p.4-2\)](#)— 最初にこの手順を実行します。
2. [NTP-A30 ユーザの作成とセキュリティの割り当て \(p.4-5\)](#)— Cisco Transport Controller (CTC) のユーザを作成してセキュリティ レベルを割り当てる場合は、この手順を実行します。
3. [NTP-A25 名前、日付、時刻、連絡先情報の設定 \(p.4-6\)](#)— ノード名、日付、時刻、場所、連絡方法を設定する場合は、この手順へ進みます。
4. [NTP-A261 電力モニタ スレッシュホールドの設定 \(p.4-8\)](#)— ノードのバッテリー電力スレッシュホールドを設定する場合は、この手順へ進みます。
5. [NTP-A169 CTC ネットワーク アクセスの設定 \(p.4-9\)](#)— IP アドレス、デフォルト ルータ、サブネット マスク、ネットワークの構成設定をプロビジョニングする場合は、この手順へ進みます。
6. [NTP-A27 ファイアウォール アクセスを目的とした ONS 15454 の設定 \(p.4-10\)](#)— ファイアウォールの背後にある ONS 15454 へアクセスする場合は、この手順へ進みます。
7. [NTP-A28 タイミングの設定 \(p.4-11\)](#)— ノードの SONET タイミング基準を設定する場合は、この手順へ進みます。
8. [NTP-A324 保護グループの作成 \(p.4-12\)](#)— 1:1、1:N、1+1、または Y 字ケーブル保護グループを ONS 15454 電気回路カードと光カードに対して設定する場合は、必要に応じてこの手順を実行します。
9. [NTP-A256 SNMP の設定 \(p.4-15\)](#)— SNMP (簡易ネットワーク管理プロトコル) を使用してネットワークをモニタする場合は、この手順を実行します。

10. **NTP-A318 OSI のプロビジョニング(p.4-17)**— ONS 15454 が、Open Systems Interconnection( OSI; 開放型システム間相互接続)プロトコル スタックに基づく Network Element( NE; ネットワーク要素)とネットワーク接続されている場合は、この手順を実行します。この手順では、TARP、OSI ルータ、マニュアルエリア アドレス、サブネットワーク接続ポイント、および IP over OSI トンネルをプロビジョニングします。

## NTP-A323 カードの取り付けの確認

目的	この手順では、SONET 用にプロビジョニングされた ONS 15454 ノードの立ち上げ準備が整っているかどうかを確認します。
工具 / 機器	ONS 15454 カードの取り付け方法を説明した、エンジニアリングの作業順序、サイト計画、またはその他の文書
事前準備手順	<a href="#">第1章「シェルフおよびバックプレーン ケーブルの取り付け」</a> <a href="#">第2章「カードおよび光ファイバケーブルの取り付け」</a>
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	検索以上のレベル

**ステップ 1** 2 枚の TCC2/TCC2P カードがスロット 7 と 11 に取り付けられていることを確認します。

**ステップ 2** 一方の TCC2/TCC2P カードで緑色の ACT(アクティブ)LED が、またもう一方の TCC2/TCC2P カードでオレンジの STBY(スタンバイ)LED がそれぞれ点灯していることを確認します。



**(注)** TCC2/TCC2P カードが取り付けられていない場合や、LED が正しく点灯していない場合は、作業を続行しないでください。「[DLP-A36 TCC2/TCC2P カードの取り付け](#)」(p.17-44)を繰り返すか、『Cisco ONS 15454 Troubleshooting Guide』を参照して取り付けに関する問題を解決してから、[ステップ 3](#)へ進みます。

**ステップ 3** クロスコネクタカード(XCVT、XC10G、または XC-VXC-10G)がスロット 8 と 10 に取り付けられていることを確認します。クロスコネクタカードは同じタイプである必要があります。

**ステップ 4** 一方のクロスコネクタカードで緑色の ACT(アクティブ)LED が、またもう一方のクロスコネクタカードでオレンジの STBY(スタンバイ)LED がそれぞれ点灯していることを確認します。



**(注)** クロスコネクタカードが取り付けられていない場合や、LED が正しく動作していない場合は、作業を続行しないでください。「[DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け](#)」(p.17-47)を繰り返すか、『Cisco ONS 15454 Troubleshooting Guide』を参照して取り付けに関する問題を解決してから、[ステップ 5](#)へ進みます。

**ステップ 5** サイト計画の要件に Alarm Interface Controller-International(AIC-I)カードが含まれている場合は、AIC-Iカードがスロット 9 に取り付けられ、ACT(アクティブ)LED がグリーンに点灯していることを確認します。

**ステップ6** DS-1、DS-3、EC-1、および DS3XM カードが、取り付け計画で指定されたおりにスロット 1 ~ 6 または 12 ~ 17 に取り付けられているかを確認します。



**(注)** DS1/E1-56 および DS3/EC1-48 カードを取り付けることができるのは、スロット 3 またはスロット 15 ~ 17 のみです。

**ステップ7** イーサネット カードが取り付けられている場合は、正しいクロスコネクタ カードがスロット 8 および 10 に取り付けられていることを確認します。

- E100T-12-G および E1000-2-G カードには、XC10G または XC-VXC-10G カードが必要です。
- G1K-4、ML1000-2、ML100X-8、ML100T-12、CE-1000-4 カードがスロット 1 ~ 6 または 12 ~ 17 に取り付けられている場合は、XC10G または XC-VXC-10G カードが必要です。スロット 5、6、11、および 12 に取り付けられている場合は、任意のクロスコネクタ カードを取り付けることができます。

**ステップ8** E1000-2、E1000-2-G、G1000-4、ML100X-8、ML1000-2、または CE-1000-4 イーサネット カードが取り付けられている場合は、GBIC(ギガビット インターフェイス コンバータ)か Small Form-Factor Pluggable(SFP)が取り付けられていることを確認します。取り付けられていない場合は、「[DLP-A469 GBIC または SFP/XFP デバイスの取り付け](#)」(p.21-64)を参照してください。

**ステップ9** OC-N カード(OC-3、OC-3-8、OC-12、OC-12-4、OC-48、OC-48 Any Slot [AS]、OC-192、および MRC-12)が、サイト計画で指定されたスロットに取り付けられていることを確認します。

- OC-3、OC-12、OC-48 AS、および MRC-12 カードは、スロット 1 ~ 6 または 12 ~ 17 に取り付けすることができます。
- OC-3-8 および OC-12-4 カードは、スロット 1 ~ 4 または 14 ~ 17 に取り付けすることができます。
- OC-48 および OC-192 カードは、スロット 5、6、12、または 13 に取り付けすることができます。

**ステップ10** クロスコネクタ カードがスロット 8 および 10 に取り付けられていることを確認します。

- OC-192、OC-12-4、または OC-3-8 カードが取り付けられている場合は、XC10G カードを取り付ける必要があります。
- OC-48 AS カードがスロット 1 ~ 4 または 14 ~ 17 に取り付けられている場合は、XC10G カードを取り付ける必要があります。XC カードまたは XCVT カードが取り付けられている場合、OC-48 AS を取り付けることができるのは、スロット 5、6、12 または 13 のみです。

**ステップ11** 取り付けられているすべての OC-N カードの STBY LED がオレンジに点灯していることを確認します。

**ステップ12** トランスポンダ(TXP)カードまたはマックスポンダ(MXP)カード(TXP\_MR\_10G、TXP\_MR\_2.5G、TXPP\_MR\_2.5G、MXP\_MR\_2.5G、MXPP\_MR\_2.5G、MXP\_2.5G\_10G、TXP\_MR\_10E、TXP\_MR\_10E\_L、TXP\_MR\_10E\_C、および MXP\_2.5G\_10E、MXP\_2.5G\_10E\_C、MXP\_2.5G\_10E\_L、MXP\_MR\_10DME\_L、または MXP\_MR\_10DME\_C)が取り付けられている場合は、これらのカードがスロット 1 ~ 6 または 12 ~ 17 に取り付けられていることと、それらに GBIC か SFP コネクタが付いていることを確認します。TXP および MXP カードの取り付けおよびプロビジョニングについては、『[Cisco ONS 15454 DWDM Procedure Guide](#)』を参照してください。

**ステップ 13** ファイバチャネルカード (FC-MR-4) が取り付けられている場合は、次のいずれかを確認します。

- XC10G クロスコネクタカードが取り付けられている場合は、FC\_MR-4 がスロット 1 ~ 6 か 12 ~ 17 に取り付けられ、ACT (アクティブ) LED がグリーンに点灯していることを確認します。
- XCVT クロスコネクタカードが取り付けられている場合は、FC\_MR-4 がスロット 5 ~ 6 か 12 ~ 13 に取り付けられ、ACT (アクティブ) LED がグリーンに点灯していることを確認します。

**ステップ 14** 光ファイバケーブル (ファイバ) が取り付けられ、サイト計画で指定された場所に接続されていることを確認します。ファイバが取り付けられていない場合は、「[NTP-A247 光ファイバケーブルの取り付け](#)」(p.2-18) を行います。

**ステップ 15** ファイバがシェルフ アセンブリに正しく配線され、ファイバブーツが適切に取り付けられていることを確認します。ファイバがシェルフ アセンブリに配線されていない場合は、「[NTP-A245 光ファイバケーブルの配線](#)」(p.2-22) を実行します。ファイバブーツが取り付けられていない場合は、「[DLP-A45 ファイバブーツの取り付け](#)」(p.17-57) を行います。

**ステップ 16** LCD に表示されているソフトウェア リリースが、サイト計画で指定されたソフトウェア リリースと一致していることを確認します。リリースが一致していない場合は、次のいずれかの手順を実行します。

- Cisco ONS 15454 のソフトウェア CD を使用して、ソフトウェアをアップグレードします。手順については、リリースに固有のソフトウェア アップグレード マニュアルを参照してください。
- TCC2/TCC2P カードを、正しいリリースを含むカードと交換します。『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**終了** : この手順は、これで完了です。

---



## NTP-A30 ユーザの作成とセキュリティの割り当て

目的	この手順では、ONS 15454 ユーザを作成し、セキュリティ レベルを割り当てます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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** ユーザを作成するノードで「[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。



(注) ユーザを作成して追加するには、スーパーユーザとしてログインする必要があります。各 ONS 15454 が提供する CISCO15 ユーザは、他の ONS 15454 ユーザの設定に使用できます。1 つの ONS 15454 にユーザを 500 人まで追加できます。

- ステップ 2** 必要に応じて、「[DLP-A74 新規ユーザの作成：単一ノード](#)」(p.17-89)または「[DLP-A75 新規ユーザの作成：複数ノード](#)」(p.17-90)を行います。



(注) ユーザがアクセスするノードごとに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 3** 必要に応じて、「[DLP-A456 ノードへの RADIUS 認証の設定](#)」(p.21-41)を行います。Remote Authentication Dial In User Service (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。

- ステップ 4** パスワード有効期限やアイドル ユーザのタイムアウト ポリシーなどのセキュリティ ポリシーの設定を変更する場合は、「[NTP-A205 ユーザの変更とセキュリティの変更](#)」(p.11-9)を実行します。

終了：この手順は、これで完了です。

## NTP-A25 名前、日付、時刻、連絡先情報の設定

目的	この手順では、ノードの識別情報をプロビジョニングします（ノード名、担当者名、電話番号、ノードの場所、日付、時刻、時間帯など）。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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** 起動するノードで、「[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** Provisioning > General タブをクリックします。

**ステップ 3** 表示されたフィールドに次の情報を入力します。

- Node Name — ノードの名前を入力します。Transaction Language 1 (TL1) に適合させるために、名前は英字で始め、最大 20 文字までの英数字 (a ~ z, A ~ Z, 0 ~ 9) で指定する必要があります。
- Contact — (任意) ノードの担当者の名前と電話番号を 255 文字以内で入力します。
- Latitude — (任意) ノードの緯度を N (北緯) または S (南緯)、度、分で入力します。
- Longitude — (任意) ノードの経度を E (東経) または W (西経)、度、分で入力します。



### ヒント

ネットワーク ビューのマップ上で、手動でノードを配置することもできます。Ctrl キーを押しながら、ノードのアイコンをドラッグアンドドロップします。すべての ONS 15454 ユーザに表示可能な同じネットワーク マップを作成するには、「[NTP-A172 論理ネットワーク マップの作成](#)」(p.5-50) を実行します。

CTC では、ネットワーク ビューのマップへ ONS 15454 アイコンを配置するときに緯度と経度を使用します。度で表示された座標を度と分に変換するには、小数点以下の数値に 60 を掛けます。たとえば、緯度 38.250739 は 38 度 15 分に変換されます ( $0.250739 \times 60 = 15.0443$ 、整数に四捨五入)。

- Description — ノードの説明を入力します。説明は、255 文字以内で指定します。
- Use NTP/SNTP Server — CTC で Network Time Protocol (NTP) または Simple Network Time Protocol (SNTP) サーバを使用してノードの日付と時間を設定する場合に、このボックスをオンにします。

SNTP サーバまたは NTP サーバを使用しない場合は、Date フィールドと Time フィールドに入力してください。ONS 15454 では、これらのフィールドをアラームの日付と時間に使用します。デフォルトでは、整合性を保つために、すべてのアラームが CTC コンピュータの時間帯で表示されます。表示をノードの時間帯に変更するには、「[DLP-A112 時間帯に合わせたアラームおよび状態の表示](#)」(p.18-3) を行います。



### (注)

NTP サーバまたは SNTP サーバを使用すると、すべての ONS 15454 ネットワーク ノードで同じ日付と時間基準が使用されます。このサーバは、停電やソフトウェアのアップグレード後にノードの時刻を同期させます。

Use NTP/SNTP Server チェックボックスをオンにした場合は、次のいずれかの IP アドレスを入力します。

- ONS 15454 に接続された NTP/SNTP サーバ
- ONS 15454 に接続された、NTP/SNTP がイネーブルな別の ONS 15454

ONS 15454 SOCKS プロキシ サーバの Gateway Network Element ( GNE; ゲートウェイ ネットワーク エlement ) を選択した場合 ( 「DLP-A249 IP 設定のプロビジョニング」 [p.19-35] を参照 ) 外部 ONS 15454 はゲートウェイ ONS 15454 で NTP/SNTP タイミングを参照する必要があります。ONS 15454 ゲートウェイの設定については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

**注意**

NTP/SNTP サーバとして別の ONS 15454 を参照している場合は、2 番目の ONS 15454 が 1 番目の ONS 15454 ではなく NTP/SNTP サーバを参照していることを確認してください (つまり、NTP/SNTP タイミング ループを作成したときに、2 つの ONS 15454 ノードが互いを参照し合わないようししてください)。

- Date — Use NTP/SNTP Server がオフの場合に、現在の日付を mm/dd/yyyy の形式で入力します (たとえば、2002 年 9 月 24 日であれば 09/24/2002 となります)。
- Time — Use NTP/SNTP Server がオフの場合に、hh:mm:ss の形式で現在の時間を入力します。たとえば、11:24:58 のように入力します。ONS 15454 では 24 時間表示が使用されるため、午後 10:00 は 22:00:00 と入力します。
- Time Zone — フィールドをクリックして、ドロップダウン メニューから指定した時間帯の都市を選択します。リストには -11 から 0 (GMT) を通って +14 まで 80 の時間帯が表示されます。米国の時間帯は GMT-05:00 (東海岸)、GMT-06:00 (中西部)、GMT-07:00 (山岳部) および GMT-08:00 (太平洋) になります。
- Use Daylight Savings Time — 選択した時間帯でサマータイムを使用する場合は、このチェックボックスをオンにします。
- Insert AIS-V on STS-1 SD-P — STS-1 が Signal Degrade Path (SD-P) BER (ビット エラー レート) スレッシュホールドを超過したときに、STS-1 で伝送される VT 回線に Alarm Indication Signal Virtual Tributary (AIS-V) 条件を挿入する場合は、このチェックボックスをオンにします。保護されている回線では、トラフィックが切り替わります。切り替えを実行できないか、または回線が保護されない場合は、STS-1 SD-P BER スレッシュホールドに達するとトラフィックが廃棄されます。
- SD-P BER — Insert AIS-V を選択した場合は、SD-P BER ドロップダウン リストから SD-P BER レベルを選択できます。

**ステップ 4** Apply をクリックします。

**ステップ 5** 確認用ダイアログボックスで、Yes をクリックします。

**ステップ 6** ノード情報を確認します。訂正が必要な場合は、ステップ 3 ~ 5 を繰り返して訂正します。情報が正しい場合は、「NTP-A261 電力モニタ スレッシュホールドの設定」(p.4-8) へ進みます。

**終了:** この手順は、これで完了です。

## NTP-A261 電力モニタ スレッシュホールドの設定

目的	この手順では、-48 Volts Direct Current (VDC; 直流電圧) 環境での極高、高、極低、および低の入力バッテリー電力スレッシュホールドをプロビジョニングします。このスレッシュホールドを超えると、TCC2/TCC2P によって CTC に警告アラームが生成されます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
必須 / 適宜	必須
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** 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** ノード ビューで、**Provisioning > General > Power Monitor** タブをクリックします。
- ステップ 3** バッテリーの極低電圧スレッシュホールドを 0.5 VDC の増分で変更する場合は、ELWBATVG(Vdc) ドロップダウン リストから電圧を選択します。
- ステップ 4** バッテリーの低電圧スレッシュホールドを 0.5 VDC の増分で変更する場合は、LWBATVG(Vdc) ドロップダウン リストから電圧を選択します。
- ステップ 5** バッテリーの高電圧スレッシュホールドを 0.5 VDC の増分で変更する場合は、HIBATVG(Vdc) ドロップダウン リストから電圧を選択します。
- ステップ 6** バッテリーの極高電圧スレッシュホールドを 0.5 VDC の増分で変更する場合は、EHIBATVG(Vdc) ドロップダウン リストから電圧を選択します。
- ステップ 7** **Apply** をクリックします。

**終了:** この手順は、これで完了です。

---

## NTP-A169 CTC ネットワーク アクセスの設定

目的	この手順では、ノードのネットワーク アクセスをプロビジョニングします。具体的には、サブネット マスク、デフォルト ルータ、Dynamic Host Configuration Protocol (DHCP) サーバ、Internet Inter-Orb Protocol (IOP) リスナー ポート、SOCKS プロキシ サーバ設定、デュアル IP アドレス設定、スタティック ルート、Open Shortest Path First (OSPF) プロトコル、および Routing Information Protocol (RIP) を設定します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
必須 / 適宜	必須
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[DLP-A249 IP 設定のプロビジョニング](#)」(p.19-35) を行って、ONS 15454 の IP アドレス、サブネット マスク、デフォルト ルータ、DHCP サーバ、IOP リスナー ポート、および SOCKS プロキシ サーバの設定をプロビジョニングします。



**ヒント** ノードにログインできない場合は、ONS 15454 ファントレイ アセンブリの LCD を使用して、IP アドレス、デフォルト ルータ、およびネットワーク マスクを変更できます (LCD プロビジョニングが抑制されていない場合)。手順については、「[DLP-A64 LCD による IP アドレス、デフォルト ルータ、ネットワーク マスクの設定](#)」(p.17-76) を参照してください。ただし、LCD でその他のネットワーク設定をプロビジョニングすることはできません。

- ステップ 3** TCC2P カードが取り付けられている場合に、ノードに 2 つの IP アドレスをプロビジョニングできるようになるセキュア モードを ONS 15454 でオンにするには、「[DLP-A433 ノードのセキュア モードのイネーブル化](#)」(p.21-10) を行います。セキュア モードの詳細については、『*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** スタティック ルートが必要な場合は、「[DLP-A65 スタティック ルートの作成](#)」(p.17-78) を行います。スタティック ルートの詳細については、『*Cisco ONS 15454 Reference Manual*』の「Management Network Connectivity」の章を参照してください。
- ステップ 5** OSPF を使用する LAN または WAN に ONS 15454 が接続されており、LAN または WAN と ONS ネットワークの間でルーティング情報を共有する場合は、「[DLP-A250 OSPF プロトコルの設定または変更](#)」(p.19-39) を行います。
- ステップ 6** RIP を使用する LAN または WAN に ONS 15454 が接続されている場合は、「[DLP-A251 RIP の設定または変更](#)」(p.19-41) を行います。

終了：この手順は、これで完了です。

## NTP-A27 ファイアウォールアクセスを目的とした ONS 15454 の設定

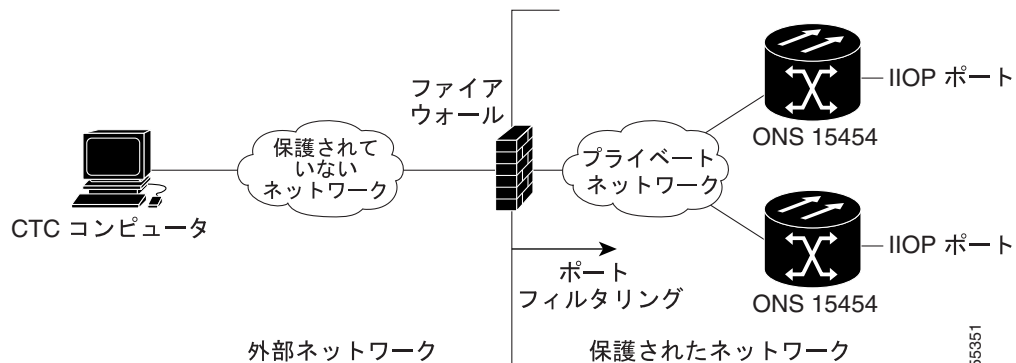
目的	この手順では、ONS 15454 および CTC コンピュータにファイアウォールを介してアクセスするためのプロビジョニングを行います。
工具 / 機器	LAN 管理者またはファイアウォール管理者が指定する IOP リスナーポート番号
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

**ステップ 1** ファイアウォールの背後にあるノードにログインします。手順については、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を参照してください。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** 「[DLP-A67 ONS 15454 での IOP リスナー ポートのプロビジョニング](#)」(p.17-79) を実行します。

図 4-1 は、ONS 15454 が保護ネットワーク内にあり、CTC コンピュータが外部ネットワークにあるケースを示しています。コンピュータから ONS 15454 にアクセスするには、ファイアウォール管理者が指定した IOP リスナー ポートを ONS 15454 上でプロビジョニングする必要があります。

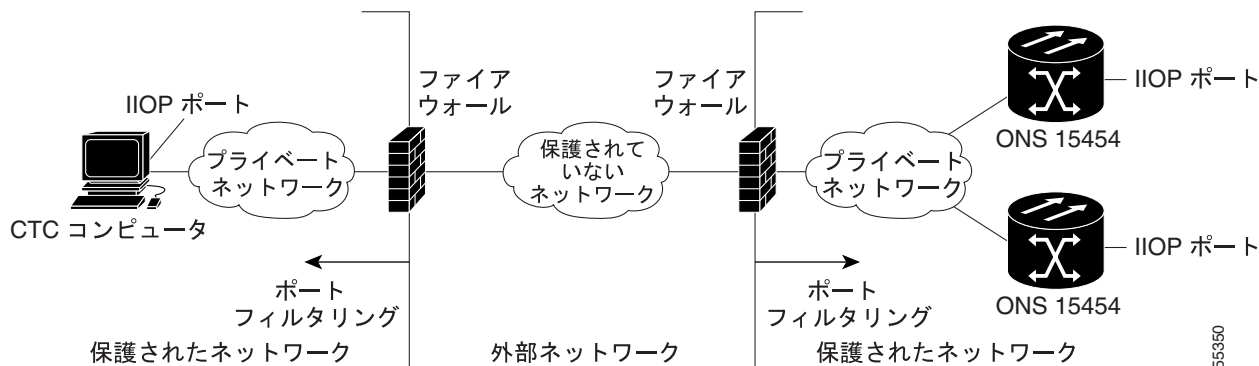
図 4-1 ファイアウォールの背後にあるノード



**ステップ 3** CTC コンピュータがファイアウォールの背後にある場合は、「[DLP-A68 CTC コンピュータにおける IOP リスナー ポートのプロビジョニング](#)」(p.17-80) を行います。

図 4-2 は、CTC コンピュータと ONS 15454 がファイアウォールの背後にあるケースを示しています。コンピュータから ONS 15454 にアクセスするには、CTC コンピュータと ONS 15454 上で IOP ポートをプロビジョニングする必要があります。

図 4-2 ファイアウォールの背後にある CTC コンピュータ と ONS 15454



終了：この手順は、これで完了です。

## NTP-A28 タイミングの設定

目的	この手順では、ONS 15454 のタイミングをプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
必須 / 適宜	必須
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** タイミング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** 外部 Building Integrated Timing Supply (BITS) ソースを使用できる場合は、「[DLP-A69 外部タイミングまたはライン タイミングの設定](#)」(p.17-81)を行います。SONET のタイミング設定には、この手順を使用するのが一般的です。
- ステップ 3** [ステップ 2](#) を完了できない場合 (外部 BITS ソースを使用できない場合) は、「[DLP-A70 内部タイミングの設定](#)」(p.17-84)を行います。この作業で設定できるのは Stratum 3 タイミングだけです。



(注) SONET のタイミングについては、『Cisco ONS 15454 Reference Manual』の「Timing」の章または Telcordia GR-253-CORE を参照してください。

終了：この手順は、これで完了です。

## NTP-A324 保護グループの作成

目的	この手順では、ONS 15454 カードの保護グループを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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** 保護グループを作成するノードで、「[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。

[表 4-1](#) に、ONS 15454 で使用できる保護タイプを示します。

**表 4-1 保護タイプ**

タイプ	カード	説明および取り付け要件
1:1	DS1-14 DS3-12 DS3-12E EC1-12 DS3XM-6 DS3XM-12 DS3/EC1-48	1 枚の現用カードと 1 枚の保護カードのペア。保護カードが奇数番号スロットに、現用カードが保護スロットの TCC2/TCC2P 側の隣の偶数番号スロットに取り付けられている必要があります。たとえば、保護カードがスロット 1 のときは、現用カードがスロット 2 に、保護カードがスロット 3 のときは、現用カードがスロット 4 に、保護カードがスロット 15 のときは、現用カードがスロット 14 に、それぞれ取り付けられている必要があります。1:1 保護は、リバーティブまたは非リバーティブに設定できます。詳細については、『Cisco ONS 15454 Reference Manual』の「Card Protection」の章およびカード固有の参照情報を参照してください。
1:N	DS1N-14 DS3N-12 DS3N-12E DS3XM-12 DS3/EC1-48 DS1/E1-56	複数の現用カードに保護カードを 1 枚割り当てます。最大で 1:5 の割り当てが可能です。これらの保護カードはスロット 3 または 15 に、保護の対象となるカードはシェルフの同じ側に取り付ける必要があります。  保護カードと保護対象カードが一致している必要があります。たとえば、DS1N-14 が保護できるのは、DS1-14 カードまたは DS1N-14 カードのみです。障害が解消されて、復元時間が経過すると、トラフィックは現用カードに復元します。  詳細については、『Cisco ONS 15454 Reference Manual』の「Card Protection」の章およびカード固有の参照情報を参照してください。



表 4-1 保護タイプ (続き)

タイプ	カード	説明および取り付け要件
1+1	任意の OC-N	1つの現用 OC-N カード / ポートと 1つの保護 OC-N カード / ポートのペア。マルチポート OC-N カードでは、保護ポートを現用カードの現用ポートに一致させる必要があります。たとえば、OC-3 カードのポート 1 は、別の OC-3 カードのポート 1 でだけ保護できます。マルチポートカードのポートは、現用ポートまたは保護ポートである必要があります。同じカードに現用ポートと保護ポートを混在させることはできません。カードは、隣接するスロットに取り付ける必要はありません。1:1 保護は、リバーティプまたは非リバーティプ、単方向または双方向に設定できます。
最適化 1+1	OC-3-4 OC-3-8	SDH に対応するようにポートをプロビジョニングする必要があります。最適化 1+1 保護は、主にリニア 1+1 双方向保護方式のネットワークで使用します。最適化 1+1 は、2つの回線 (現用と保護) を使用するリニアレベル保護方式です。2つの回線の 1つがプライマリチャネルの役割を果たして、トラフィックの選択元となります。もう 1つのポートはセカンダリチャネルの役割を果たし、プライマリチャネルを保護します。外部切り替えコマンドまたは回線状態に基づいて、トラフィックはプライマリチャネルからセカンダリチャネルに切り替わります。切り替えの原因となった回線状態または外部切り替えコマンドがクリアされると、2つの回線の役割が元に戻ります。
Y 字ケーブル	MXP_2.5_10G MXP_2.5_10E MXP_2.5G_10E_C MXP_2.5G_10E_L MXP_MR_10DME_L MXP_MR_10DME_C TXP_MR_10G TXP_MR_10E TXP_MR_10E_L TXP_MR_10E_C MXP_2.5G_10E MXP_MR_2.5G	1つの現用トランスポンダカード / ポートまたは現用マックスポンダカード / ポートと 1つの保護トランスポンダカード / ポートまたは保護マックスポンダカード / ポートのペア。保護ポートは現用ポートと異なるカードにある必要があります。現用ポートと同じカードタイプである必要があります。現用ポートと保護ポートの数は同じにする必要があります。つまり、ポート 1 ではポート 1 だけが保護され、ポート 2 ではポート 2 だけが保護されます。詳細については、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。

表 4-1 保護タイプ(続き)

タイプ	カード	説明および取り付け要件
スプリッタ	TXPP_MR_2.5G MXPP_MR_2.5G	スプリッタ保護では、自動的に TXPP_MR_2.5G および MXPP_MR_2.5G カードが使用されます。詳細については、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。
非保護	任意	カードに障害または信号エラーが発生した場合、非保護カードは信号損失の原因になる可能性があります。ただし、保護用に予約されたカード スロットがないため、非保護スキームの ONS 15454 ではサービスを最大限に使用できます。非保護がデフォルトの保護タイプです。

**ステップ 2** 作成する保護グループに応じて、次の作業を 1 つまたは複数実行します。

- [DLP-A71 1:1 保護グループの作成 \(p.17-85\)](#)
- [DLP-A72 1:N 保護グループの作成 \(p.17-86\)](#)
- [DLP-A73 1+1 保護グループの作成 \(p.17-87\)](#)
- [DLP-A34 最適化 1+1 保護グループの作成 \(p.17-42\)](#)



**(注)** 保護カードが取り付けられていない場合は、『[DLP-A330 カード スロットの事前プロビジョニング](#)』(p.20-22) を実行して、カード保護のプロビジョニングを実行できます。



**(注)** TXP および MXP カードに Y 字ケーブル保護グループを作成する場合は、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。

終了：この手順は、これで完了です。

## NTP-A256 SNMP の設定

目的	この手順では、ONS 15454 で SNMP 管理用ソフトウェアを使用できるように、SNMP パラメータを設定します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
必須 / 適宜	インストール時に SNMP を使用する場合は必須
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** SNMP 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** ノード ビューで、**Provisioning > SNMP** タブをクリックします。

**ステップ 3** Trap Destinations 領域で、**Create** をクリックします。

**ステップ 4** Create SNMP Trap Destination ダイアログボックスで次のフィールドを入力します ([図 4-3](#))。

- Destination IP Address — Network Management System (NMS; ネットワーク管理システム) の IP アドレスを入力します。ログインしているノードが End Network Element (ENE) の場合は、宛先アドレスを GNE に設定します。
- Community — SNMP コミュニティ名を入力します。SNMP のコミュニティ名の詳細については、『*Cisco ONS 15454 Reference Manual*』の「SNMP」の章を参照してください。



**(注)** コミュニティ名は、認証とアクセス制御を組み合わせた形式で指定します。ONS 15454 に割り当てるコミュニティ名は、大文字と小文字を区別し、NMS のコミュニティ名と一致させる必要があります。

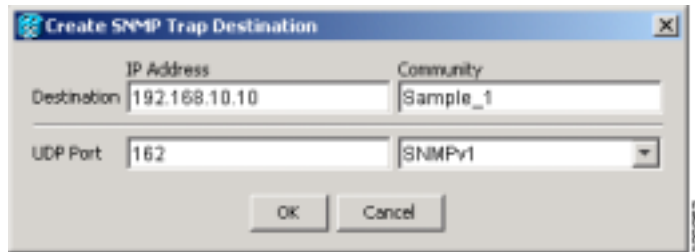
- UDP Port — SNMP のデフォルトの UDP ポートは 162 です (UDP ポートのプロビジョニングの詳細については、「[DLP-A449 GNE 対応 SNMP の設定](#)」 [p.21-32] および「[DLP-A450 ENE 対応 SNMP の設定](#)」 [p.21-34] も参照)。



**(注)** ノードで SOCKS プロキシ サーバがイネーブルになっていて、ENE としてプロビジョニングされている場合は、UDP ポートを GNE の SNMP リレー ポート (391) に設定する必要があります。

- 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。

図 4-3 SNMP トラップの作成



**ステップ 5** 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 6** 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 7** Gateway Node Element ( GNE )および End Node Element ( ENE )に SNMP Remote Monitoring ( RMON )を設定する場合は、作成する保護グループに応じて、必要に応じて次の作業を実行する必要があります。

- [DLP-A449 GNE 対応 SNMP の設定 \( p.21-32 \)](#)
- [DLP-A450 ENE 対応 SNMP の設定 \( p.21-34 \)](#)
- [DLP-A451 SNMP コマンドまたは演算用の NMS コミュニティ スtringのフォーマット化および入力 \( p.21-36 \)](#)

**ステップ 8** Apply をクリックします。

**終了 :** この手順は、これで完了です。

---

## NTP-A318 OSI のプロビジョニング

目的	この手順では、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) 通信を行うその他のベンダー NE とネットワーク接続できるように、ONS 15454 をプロビジョニングします。この手順では、TARP、OSI ルータ、マニュアル エリア アドレス、サブネットワーク接続ポイント、および IP over OSI トンネルをプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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

この手順を実行するには、OSI のプロトコル、パラメータ、および機能についての理解が必要です。手順を開始する前に、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章の OSI リファレンス セクションを参照してください。



注意

OSI および IP ネットワークでの ONS 15454 の役割を決定してから、この手順を開始してください。



(注)

この手順では、ルータやサードパーティ製 NE を含む非 ONS 機器をプロビジョニングする必要があります。このプロビジョニングを実行できるようになるまでは、この手順を開始しないでください。

**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** 必要に応じて次の作業を行います。

- [DLP-A534 OSI ルーティング モードのプロビジョニング \(p.22-43\)](#)— 最初にこの作業を実行します。
- [DLP-A535 TARP 動作パラメータのプロビジョニングまたは変更 \(p.22-45\)](#)— 次にこの作業を実行します。
- [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 \(p.22-47\)](#)— 必要に応じて、この作業を実行します。
- [DLP-A538 TARP MAT エントリの追加 \(p.22-48\)](#)— 必要に応じて、この作業を実行します。
- [DLP-A539 OSI ルータのプロビジョニング \(p.22-49\)](#)— 必要に応じて、この作業を実行します。
- [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 \(p.22-50\)](#)— 必要に応じて、この作業を実行します。
- [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 \(p.22-51\)](#)— 必要に応じて、この作業を実行します。
- [DLP-A542 IP-Over-CLNS トンネルの作成 \(p.22-52\)](#)— 必要に応じて、この作業を実行します。

終了：この手順は、これで完了です。

---



# ネットワークの起動

この章では、Cisco ONS 15454 ネットワークを起動して、テストする方法について説明します。対象となるネットワークは、ポイントツーポイント ネットワーク、リニア Add Drop Multiplexer( ADM; 分岐挿入装置)、Unidirectional Path Switched Ring ( UPSR; 単方向パス スイッチ型リング)、および Bidirectional Line Switched Ring ( BLSR; 双方向ライン スイッチ型リング) です。

## 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A35 ノードの起動の確認 \(p.5-3\)](#)— ネットワークの起動を開始する前に、この手順を実行します。
2. [NTP-A124 ポイントツーポイント ネットワークのプロビジョニング \(p.5-5\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A173 ポイントツーポイント ネットワークの受け入れテスト \(p.5-6\)](#)— ポイントツーポイント ネットワークをプロビジョニングしたあとに、この手順を実行します。
4. [NTP-A38 リニア ADM ネットワークのプロビジョニング \(p.5-9\)](#)— 必要に応じて、この手順を実行します。
5. [NTP-A174 リニア ADM ネットワークの受け入れテスト \(p.5-11\)](#)— リニア ADM をプロビジョニングしたあとに、この手順を実行します。
6. [NTP-A40 BLSR ノードのプロビジョニング \(p.5-14\)](#)— 2 ファイバまたは 4 ファイバの BLSR で ONS 15454 をプロビジョニングする場合は、この手順を実行します。
7. [NTP-A126 BLSR の作成 \(p.5-16\)](#)— BLSR ノードをプロビジョニングしたあとに、この手順を実行します。
8. [NTP-A175 2 ファイバ BLSR の受け入れテスト \(p.5-17\)](#)— 2 ファイバ BLSR を作成したあとに、この手順を実行します。
9. [NTP-A176 4 ファイバ BLSR の受け入れテスト \(p.5-20\)](#)— 4 ファイバ BLSR を作成したあとに、この手順を実行します。
10. [NTP-A178 従来型 BLSR DRI のプロビジョニング \(p.5-23\)](#)— BLSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
11. [NTP-A179 統合 BLSR DRI のプロビジョニング \(p.5-25\)](#)— BLSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
12. [NTP-A44 UPSR ノードのプロビジョニング \(p.5-27\)](#)— 必要に応じて、この手順を実行します。
13. [NTP-A177 UPSR の受け入れテスト \(p.5-29\)](#)— UPSR を作成したあとに、この手順を実行します。

14. [NTP-A216 従来型 UPSR DRI のプロビジョニング \(p.5-32\)](#)— UPSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
15. [NTP-A217 統合 UPSR DRI のプロビジョニング \(p.5-34\)](#)— UPSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
16. [NTP-A180 従来型 BLSR/UPSR DRI のプロビジョニング \(p.5-36\)](#)— UPSR および BLSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
17. [NTP-A209 統合 BLSR/UPSR DRI のプロビジョニング \(p.5-38\)](#)— UPSR および BLSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
18. [NTP-A224 開放端 UPSR のプロビジョニング \(p.5-40\)](#)— UPSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
19. [NTP-A225 開放端 UPSR の受け入れテスト \(p.5-42\)](#)— 開放端 UPSR をプロビジョニングしたあとで、必要に応じてこの手順を実行します。
20. [NTP-A46 BLSR からの UPSR のサブテンディング \(p.5-45\)](#)— 必要に応じて、この手順を実行します。
21. [NTP-A47 UPSR からの BLSR のサブテンディング \(p.5-47\)](#)— 必要に応じて、この手順を実行します。
22. [NTP-A48 BLSR からの BLSR のサブテンディング \(p.5-48\)](#)— 必要に応じて、この手順を実行します。
23. [NTP-A172 論理ネットワーク マップの作成 \(p.5-50\)](#)— 必要に応じて、この手順を実行します。



## NTP-A35 ノードの起動の確認

目的	この手順では、ネットワークに ONS 15454 を追加する前に、ネットワークの起動準備ができていることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">第4章「ノードの起動」</a>
必須 / 適宜	必須
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** テスト対象ネットワークで「[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** Alarms タブをクリックします。
- 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-A227 アラームフィルタリングのディセーブル化](#)」(p.19-21)を参照してください。
  - 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 3** ノードビューのステータス領域に表示されている SW Version フィールドと Defaults フィールドの値が、サイト計画に示されているソフトウェアバージョンと Network Element (NE; ネットワーク要素)のデフォルト値に一致していることを確認します。どちらかが一致していない場合は、必要に応じて次の手順を実行します。
- ソフトウェアのバージョンが正しくない場合は、Cisco ONS 15454 のソフトウェア CD から正しいバージョンのソフトウェアをインストールします。アップグレード手順については、リリース固有のソフトウェアアップグレードマニュアルを参照してください。最新のソフトウェアリリースを搭載した TCC2/TCC2P カードを注文することもできます。
  - ノードのデフォルト値が正しくない場合は、NE のデフォルト値をインポートします。『*Cisco ONS 15454 Reference Manual*』の付録「Network Element Defaults」を参照してください。
- ステップ 4** Provisioning > General タブをクリックします。一般ノード情報のすべての設定がサイト計画の設定と一致していることを確認します。一致していない場合は、「[NTP-A81 ノード管理情報の変更](#)」(p.11-2)を参照してください。
- ステップ 5** Provisioning > Timing タブをクリックします。タイミングの設定がサイト計画の設定と一致していることを確認します。一致していない場合は、「[NTP-A85 ノードのタイミング変更](#)」(p.11-8)を参照してください。
- ステップ 6** Provisioning > Network タブをクリックします。IP の設定と他の CTC ネットワークアクセス情報が正しいことを確認します。一致していない場合は、「[NTP-A201 CTC ネットワークアクセスの変更](#)」(p.11-3)を参照してください。
- ステップ 7** Provisioning > Protection タブをクリックします。すべての保護グループがサイト計画に従って作成されていることを確認します。一致していない場合は、「[NTP-A203 カード保護設定の変更または削除](#)」(p.11-6)を参照してください。

- ステップ 8** Provisioning > Security タブをクリックします。すべてのユーザが作成されていて、各ユーザのセキュリティ レベルやポリシーがサイト計画に示された設定と一致していることを確認します。一致していない場合は、「[NTP-A205 ユーザの変更とセキュリティの変更](#)」(p.11-9)を参照してください。
- ステップ 9** ノードで SNMP (簡易ネットワーク管理プロトコル) がプロビジョニングされている場合は、Provisioning > SNMP タブをクリックします。すべての SNMP 設定がサイト計画の設定と一致していることを確認します。一致していない場合は、「[NTP-A87 SNMP の設定変更](#)」(p.11-10)を参照してください。
- ステップ 10** 「[準備作業](#)」(p.5-1) に説明されている適切な手順を使用して、ネットワークをプロビジョニングします。

終了：この手順は、これで完了です。

---

## NTP-A124 ポイントツーポイント ネットワークのプロビジョニング

目的	この手順では、1+1 ポイントツーポイント（端末）ネットワーク内で2つの ONS 15454 をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** ポイントツーポイント構成をプロビジョニングするネットワークの ONS 15454 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** Provisioning > Protection タブをクリックします。OC-N カードに 1+1 保護が作成されていることを確認します。保護が作成されていない場合は、「[DLP-A73 1+1 保護グループの作成](#)」(p.17-87)を行います。
- ステップ 3** 2 番めのポイントツーポイント ノードについて、ステップ 1 と 2 を繰り返します。
- ステップ 4** 1+1 保護グループ内の現用カードと保護カードがノード間の物理ファイバ接続に対応していることを確認します。つまり、一方のノードにある現用カードが他方のノードの現用カードに接続され、一方のノードにある保護カードが他方のノードの保護カードに接続されていることを確認します。
- ステップ 5** 両方のポイントツーポイント ノードにある現用側の OC-N ポートについて、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74)を行います。CTC の管理に必要な帯域幅が不足している場合は、「[DLP-A378 LDCC 終端のプロビジョニング](#)」(p.20-77)を行って追加します。



(注) 保護ポートには DCC の終端を設定しません。



(注) ポイントツーポイント ノードが LAN に接続されていない場合は、そのノードに直接(クラフト)接続して DCC の終端を作成する必要があります。リモートプロビジョニングが可能になるのは、ネットワーク内のすべてのノードの DCC 終端が稼働中の OC-N ポートにプロビジョニングされたあとのみです。

- ステップ 6** 「[DLP-A214 ポートのサービス状態の変更](#)」(p.19-10)を行い、保護カードを稼働状態にします。
- ステップ 7** 必要に応じて、「[DLP-A380 プロキシ トンネルのプロビジョニング](#)」(p.20-82)を行います。
- ステップ 8** 必要に応じて、「[DLP-A381 ファイアウォール トンネルのプロビジョニング](#)」(p.20-83)を行います。
- ステップ 9** 必要に応じて、「[DLP-A367 プロビジョニング可能なパッチコードの作成](#)」(p.20-56)を行います。

## ■ NTP-A173 ポイントツーポイント ネットワークの受け入れテスト

**ステップ 10** 両方のポイントツーポイント ノードでタイミングが設定されていることを確認します。設定されていない場合は、一方または両方のノードについて「[NTP-A28 タイミングの設定](#)」(p.4-11) を実行します。ノードでライン タイミングを使用する場合は、現用側の OC-N カードをタイミング ソースに指定します。対応する保護 OC-N カードが保護タイミング ソースとして自動的に選択されます。その結果は、Maintenance > Timing タブをクリックすると確認できます。

**ステップ 11** 「[NTP-A173 ポイントツーポイント ネットワークの受け入れテスト](#)」(p.5-6) を実行します。

終了：この手順は、これで完了です。

## NTP-A173 ポイントツーポイント ネットワークの受け入れテスト

目的	この手順では、ポイントツーポイント ネットワークをテストします。
工具 / 機器	作成するテスト回線に適したテスト セットとケーブル
事前準備手順	<a href="#">NTP-A124 ポイントツーポイント ネットワークのプロビジョニング</a> (p.5-5)
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

トラフィックを伝送するノードでこの手順を実行すると、サービスが影響を受けることがあります。

**ステップ 1** いずれかのポイントツーポイント ノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。ノード (デフォルト) ビューが表示されます。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** View メニューから **Go to Network View** を選択します。

**ステップ 3** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- c. 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、アラーム データをエクスポートします。

**ステップ 4** Conditions タブをクリックします。

- a. 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

- b. 「DLP-A532 CTC データのエクスポート」(p.22-35)を行い、状態の情報をエクスポートします。

**ステップ5** ネットワーク マップ上で1つのポイントツーポイント ノードをダブルクリックし、ノード ビューで表示します。

**ステップ6** ログイン ノードから他のポイントツーポイント ノードまでのテスト回線を作成します。

- DS-1 回線の場合 — 「NTP-A181 自動ルーティングによる DS-1 回線の作成」(p.6-8)を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。
- DS-3 回線の場合 — 「NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成」(p.6-22)を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。
- OC-N 回線について、「NTP-A343 自動ルーティングによる光回線の作成」(p.6-47)を行います。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。

**ステップ7** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ8** このテストで使用する各パッチ ケーブルの一方の端をテスト セットの送信 (Tx) コネクタに接続し、もう一方の端をテスト セットの受信 (Rx) コネクタに接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認してから **ステップ9** へ進みます。

**ステップ9** 回線の宛先カードで物理的にループバックを作成します。ループバックを作成するには、パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続し、もう一方の端をこのポートの受信 Rx コネクタに接続します。

**ステップ10** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の送信元カードの Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の送信元カードの Tx コネクタに接続します。

**ステップ11** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ 6 ~ 10 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

## ■ NTP-A173 ポイントツーポイントネットワークの受け入れテスト

**ステップ 12** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

**ステップ 13** テスト セットから BIT エラーを発生させます。テスト セットにエラーが表示されることを確認します。エラーが表示される場合は、エンドツーエンドの回線が正しく設定されています。

**ステップ 14** 「DLP-A356 TCC2/TCC2P カードのアクティブ/スタンバイ切り替えテスト」(p.20-45)を実行します。

**ステップ 15** 「DLP-A255 クロスコネク ト カードのサイド切り替えテスト」(p.19-42)を実行します。

**ステップ 16** 「DLP-A88 1+1 光保護のテスト」(p.17-92)を実行します。

**ステップ 17** BER (ビット エラー レート) テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ 18** すべてのテストが完了したら、ノードからループバック、スイッチ、またはテスト セットを取り外します。

**ステップ 19** View メニューから Go to Network View を選択します。

**ステップ 20** 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-A227 アラーム フィルタリングのディセーブル化」(p.19-21)を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- c. 「DLP-A532 CTC データのエクスポート」(p.22-35)を行い、アラーム情報をエクスポートします。

**ステップ 21** 他のポイントツーポイント ノードについて、ステップ 9 ~ 20 を繰り返します。

**ステップ 22** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

**ステップ 23** テスト回線を削除します。「DLP-A333 回線の削除」(p.20-23)を参照してください。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。

**終了：この手順は、これで完了です。**

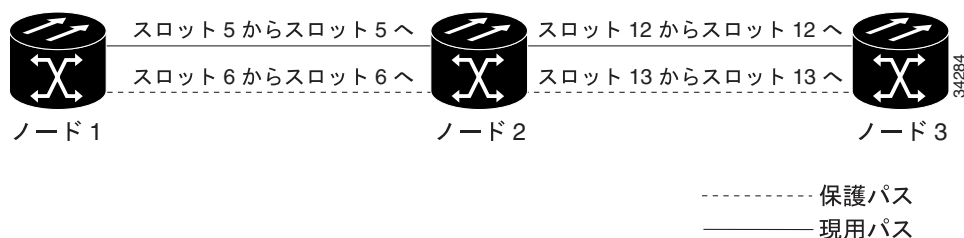
## NTP-A38 リニア ADM ネットワークのプロビジョニング

目的	この手順では、リニア ADM 構成で 3 つ以上の ONS 15454 をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** リニア ADM ネットワークをプロビジョニングする ONS 15454 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。

図 5-1 に、リニア ADM 構成の 3 つの ONS 15454 を示します。この例では、現用トラフィックがノード 1 のスロット 5 からノード 2 のスロット 5 へ、またノード 2 のスロット 12 からノード 3 のスロット 12 へそれぞれ送信されます。スロット 6 と 13 には、保護 OC-N カードが取り付けられています。スロット 5 と 6、およびスロット 12 と 13 の構成は、1+1 保護です。

図 5-1 リニア ADM 構成



- ステップ 2** **Provisioning > Protection** タブをクリックします。ノードの OC-N カードに 1+1 保護が作成されていることを確認します。保護グループが作成されていない場合は、「[DLP-A73 1+1 保護グループの作成 \(p.17-87\)](#)」を行います。
- ステップ 3** リニア ADM に含める他のすべてのノードについて、ステップ 1 と 2 を繰り返します。
- ステップ 4** 1+1 保護グループ内の現用カードと保護カードが、ノード間の物理的なファイバ接続に対応していることを確認します。つまり、現用カード同士と保護カード同士がファイバで接続されていることを確認します。
- ステップ 5** 各リニア ADM ノードの OC-N 現用ポートについて、「[DLP-A377 SDCC 終端のプロビジョニング \(p.20-74\)](#)」を行います。CTC の管理に必要な帯域幅が不足している場合は、「[DLP-A378 LDCC 終端のプロビジョニング \(p.20-77\)](#)」を行って追加します。



**(注)** リニア ADM ノードが LAN に接続されていない場合は、そのノードに直接 (クラフト) 接続して DCC の終端を作成する必要があります。リモート プロビジョニングが可能になるのは、LAN に接続されていないすべてのノードの DCC 終端が稼働中の OC-N ポートにプロビジョニングされたあとのみです。



(注) 終端ノード (図 5-1 のノード 1 と 3) には DCC の終端を 1 つ設定し、中継ノード (図 5-1 のノード 2) には DCC の終端 (この例ではスロット 5 と 12) を 2 つ設定します。

- ステップ 6** 必要に応じて、「[DLP-A380 プロキシ トンネルのプロビジョニング](#)」(p.20-82) を行います。
- ステップ 7** 必要に応じて、「[DLP-A381 ファイアウォール トンネルのプロビジョニング](#)」(p.20-83) を行います。
- ステップ 8** 必要に応じて、「[DLP-A367 プロビジョニング可能なパッチコードの作成](#)」(p.20-56) を行います。
- ステップ 9** 各リニアノードでタイミングが設定されていることを確認します。設定されていない場合は、「[NTP-A28 タイミングの設定](#)」(p.4-11) を実行します。ノードでライン タイミングを使用する場合は、現用側の OC-N カードをタイミングソースとして指定します。
- ステップ 10** 「[NTP-A174 リニア ADM ネットワークの受け入れテスト](#)」(p.5-11) を実行します。

終了：この手順は、これで完了です。

---



## NTP-A174 リニア ADM ネットワークの受け入れテスト

目的	この手順では、リニア ADM ネットワークをテストします。
工具 / 機器	作成するテスト回線に適したテストセットとケーブル
事前準備手順	<a href="#">NTP-A38 リニア ADM ネットワークのプロビジョニング (p.5-9)</a>
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** テストするリニア ADM ネットワークのノードで「[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** View メニューから、**Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21)を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、アラーム情報をエクスポートします。
- ステップ 4** Conditions タブをクリックします。
- 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、状態の情報をエクスポートします。
- ステップ 5** ネットワーク マップ上で、テスト対象となるリニア ADM のノードをダブルクリックして、ノードビューを開きます。
- ステップ 6** そのノードから隣接するリニア ADM ノードまでのテスト回線を作成します。
- DS-1 回線の場合 — 「[NTP-A181 自動ルーティングによる DS-1 回線の作成](#)」(p.6-8)を実行します。回線の状態を設定する場合は、**IS** を選択し、**Apply to drop ports** チェックボックスをオンにします。
  - DS-3 回線の場合 — 「[NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成](#)」(p.6-22)を実行します。回線の状態を設定する場合は、**IS** を選択し、**Apply to drop ports** チェックボックスをオンにします。
  - OC-N 回線について、「[NTP-A343 自動ルーティングによる光回線の作成](#)」(p.6-47)を行います。回線の状態を設定する場合は、**IS** を選択し、**Apply to drop ports** チェックボックスをオンにします。

**ステップ7** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ8** このテストで使用する各パッチ ケーブルの一方の端をテスト セットの Tx コネクタに接続し、もう一方の端をテスト セットの Rx コネクタに接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、次のステップへ進む前に、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。

**ステップ9** 回線の宛先カードで物理的にループバックを作成します。ループバックを作成するには、パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続し、もう一方の端を宛先ポートの受信 Rx コネクタに接続します。

**ステップ10** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の Tx コネクタに接続します。

**ステップ11** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ 6 ~ 10 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ12** テスト セットから BIT エラーを発生させます。テスト セットにエラーが表示されることを確認します。エラーが表示される場合は、エンドツーエンドの回線が正しく設定されています。

**ステップ13** 「DLP-A356 TCC2/TCC2P カードのアクティブ/スタンバイ切り替えテスト」(p.20-45)を実行します。

**ステップ14** 「DLP-A255 クロスコネク ト カードのサイド切り替えテスト」(p.19-42)を実行します。

**ステップ15** 「DLP-A88 1+1 光保護のテスト」(p.17-92)を行い、OC-N ポートの保護グループ切り替えをテストします。

**ステップ16** BER テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ17** すべてのテストが完了したら、ノードからループバック、スイッチ、またはテスト セットを取り外します。

**ステップ 18** ネットワーク 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 19** テスト回線を削除します。「[DLP-A333 回線の削除](#)」(p.20-23) を参照してください。

**ステップ 20** テストする次のリニア ADM ノードに、ステップ 6 ~ 19 を繰り返します。

**ステップ 21** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。

**終了**：この手順は、これで完了です。

---

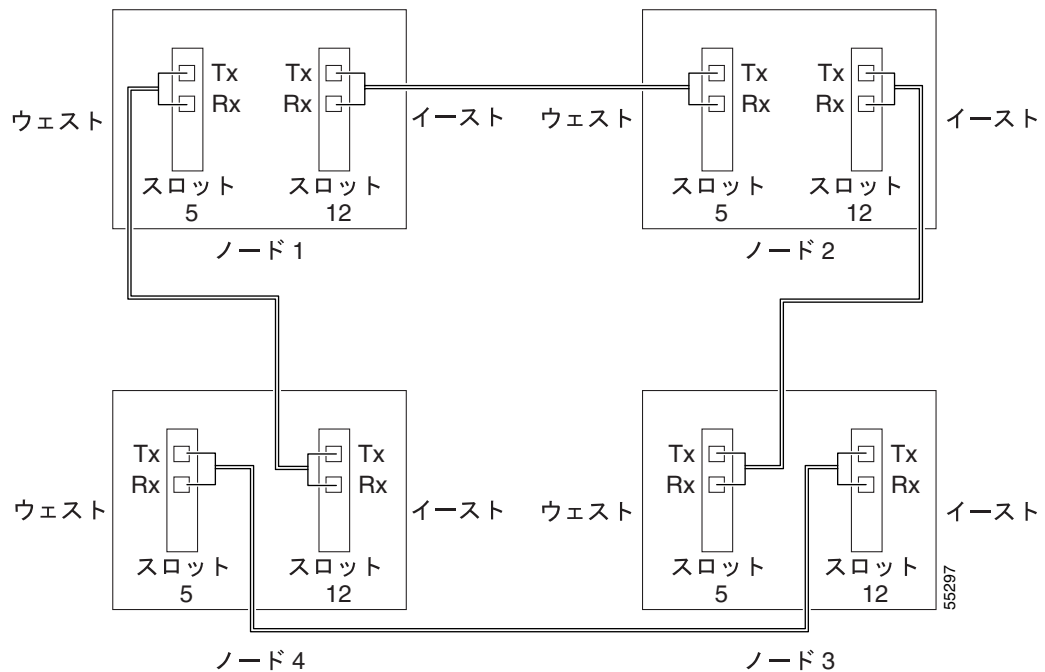
## NTP-A40 BLSR ノードのプロビジョニング

目的	この手順では、ONS 15454 ノードを BLSR 用にプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** 「[DLP-A44 BLSR 構成での光ファイバケーブルの取り付け \(p.17-55\)](#)」を行い、次の規則が守られていることを確認します。

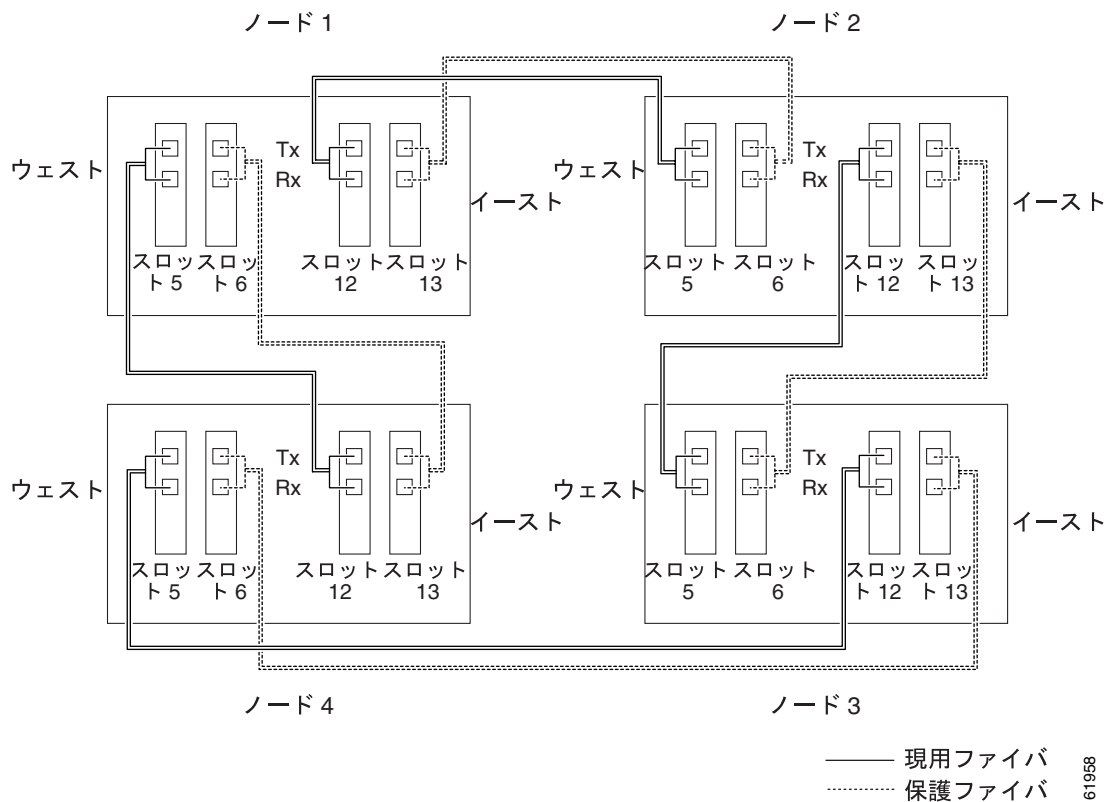
- 1 つのノードのイースト ポートが隣接ノードのウェスト ポートに接続されていることを確認します。イースト ポートとウェスト ポートの間でのこの接続は、[図 5-2](#) のようにすべての BLSR ノードで使用されます。この図では、シェルフの左側にある OC-N ドロップ カードがウェスト ポートで、シェルフの右側にあるドロップカードがイースト ポートです。

**図 5-2 4 ノード、2 ファイバ構成の BLSR ファイバ接続の例**



- 4 ファイバの BLSR について、[図 5-3](#) のように、現用ファイバと保護ファイバでイースト ポートからウェスト ポートまでに同じ接続が使用されていることを確認します。現用カードと保護カードの接続が混同されていないことを確認します。現用カードは、DCC の終端をプロビジョニングするカードです。

図 5-3 4 ノード、4 ファイバ構成の BLSR ファイバ接続の例



**ステップ 2** BLSR で設定する ONS 15454 にログインします。「[DLP-A60 CTC へのログイン](#)」(p.17-71) を参照してください。すでにログインしている場合は、ステップ 3 へ進みます。

**ステップ 3** 「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を実行します。ノードで BLSR ポートとして機能する 2 つのポート（カード）をプロビジョニングします。4 ファイバ BLSR については、現用トラフィックを伝送する OC-N カードで DCC の終端をプロビジョニングします。保護カードで、DCC をプロビジョニングしないでください。



**(注)** ONS 15454 を社内 LAN に接続していない場合は、このノードに直接（クラフト）接続して DCC をプロビジョニングする必要があります。リモート プロビジョニングが可能になるのは、ネットワーク内のすべてのノードの DCC OC-N が IS-NR ポートにプロビジョニングされたあとのみです。

**ステップ 4** 4 ファイバ BLSR について「[DLP-A214 ポートのサービス状態の変更](#)」(p.19-10) を行い、保護 OC-N カードまたはポートを稼働状態にします。

**ステップ 5** BLSR に組み込む各ノードで、ステップ 2 ~ 4 を繰り返します。リング内のすべてのノードで DCC を設定したあとに、EOC（DCC 終端エラー）と Loss of Signal（LOS; 信号損失）がクリアされていることを確認します。

**ステップ 6** 必要に応じて、「[DLP-A380 プロキシ トンネルのプロビジョニング](#)」(p.20-82) を行います。

**ステップ 7** 必要に応じて、「[DLP-A381 ファイアウォール トンネルのプロビジョニング](#)」(p.20-83) を行います。

- ステップ 8** 必要に応じて、「[DLP-A367 プロビジョニング可能なパッチコードの作成](#)」(p.20-56)を行います。
- ステップ 9** BLSR のスパンが、K3 バイトを透過的に転送できないサードパーティ製機器を経由する場合は、「[DLP-A89 K3 バイトの再マップ](#)」(p.17-94)を行います。通常は、この作業は不要です。
- ステップ 10** 「[NTP-A126 BLSR の作成](#)」(p.5-16)を実行します。

終了：この手順は、これで完了です。

---

## NTP-A126 BLSR の作成

目的	この手順では、BLSR をプロビジョニングした各ノードで BLSR を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A40 BLSR ノードのプロビジョニング</a> (p.5-14)
必須 / 適宜	適宜。BLSR のプロビジョニングを完了する場合必須
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** BLSR を作成するネットワーク上のノードで、「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。

**ステップ 2** 次のいずれかの作業を行います。

- [DLP-A328 BLSR ウィザードによる 2 ファイバ BLSR の作成](#) (p.20-19) — CTC の BLSR ウィザードを使用して 2 ファイバの BLSR を作成する場合は、この作業を行います。BLSR ウィザードを使用すると、各ノードが BLSR のプロビジョニングを開始できる状態であるかどうかを確認されて、すべてのノードが同時にプロビジョニングされます。BLSR ウィザードの使用を推奨します。
- [DLP-A362 BLSR ウィザードによる 4 ファイバ BLSR の作成](#) (p.20-51) — CTC の BLSR ウィザードを使用して 4 ファイバの BLSR を作成する場合は、この作業を行います。BLSR ウィザードを使用すると、各ノードが BLSR のプロビジョニングを開始できる状態であるかどうかを確認されて、すべてのノードが同時にプロビジョニングされます。BLSR ウィザードの使用を推奨します。
- [DLP-A329 2 ファイバ BLSR の手動作成](#) (p.20-21) — BLSR に組み込む各ノードで 2 ファイバの BLSR を手動でプロビジョニングする場合は、この作業を行います。
- [DLP-A363 4 ファイバ BLSR の手動作成](#) (p.20-53) — BLSR に組み込む各ノードで 4 ファイバの BLSR を手動でプロビジョニングする場合は、この作業を行います。

**ステップ 3** 「[NTP-A175 2 ファイバ BLSR の受け入れテスト](#)」(p.5-17) または 「[NTP-A176 4 ファイバ BLSR の受け入れテスト](#)」(p.5-20)を実行します。

終了：この手順は、これで完了です。

---

## NTP-A175 2 ファイバ BLSR の受け入れテスト

目的	この手順では、2 ファイバ BLSR をテストします。
工具 / 機器	テスト回線に適したテスト セットとケーブル
事前準備手順	<a href="#">NTP-A40 BLSR ノードのプロビジョニング (p.5-14)</a> <a href="#">NTP-A126 BLSR の作成 (p.5-16)</a>
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)

この手順では、リングの周囲にテスト回線を作成して、リングを切り替えます。わかりやすいように、手順を開始するログイン ノードを「ノード 1」とします。ノード 1 のイースト OC-N トランク (スパン) カードに接続されたノードを「ノード 2」とします。

- ステップ 1** テスト対象の BLSR にある 1 つの ONS 15454 で、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います(このノードをノード 1 と呼びます)。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** View メニューから **Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、アラーム情報をエクスポートします。
- ステップ 4** Conditions タブをクリックします。
- 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、状態の情報をエクスポートします。
- ステップ 5** ネットワーク ビューで、Node 1 をダブルクリックします。
- ステップ 6** 「[DLP-A217 BLSR の試験リング テスト](#)」(p.19-12) を実行します。
- ステップ 7** ノード 1 から、ノード 1 のイースト OC-N トランク (スパン) カードに接続されたノード (このノードをノード 2 と呼びます) までのテスト回線を作成します。
- DS-1 回線の場合 — 「[NTP-A181 自動ルーティングによる DS-1 回線の作成](#)」(p.6-8) を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。
  - DS-3 回線の場合 — 「[NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成](#)」(p.6-22) を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。

- OC-N 回線について、「[NTP-A343 自動ルーティングによる光回線の作成](#)」(p.6-47)を行います。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。

**ステップ 8** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ 9** このテストで使用する各パッチ ケーブルでテスト セットの Tx コネクタとテスト セットの Rx コネクタを接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、次のステップへ進む前に、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。

**ステップ 10** 回線の宛先カードで物理的にループバックを作成します。ループバックを作成するには、パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続し、もう一方の端をこのポートの受信 Rx コネクタに接続します。

**ステップ 11** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の Tx コネクタに接続します。

**ステップ 12** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ 7 ~ 11 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ 13** テスト セットから BIT エラーを発生させます。テスト セットにエラーが表示されることを確認します。エラーが表示される場合は、エンドツーエンドの回線が正しく設定されています。

**ステップ 14** 「[DLP-A356 TCC2/TCC2P カードのアクティブ/スタンバイ切り替えテスト](#)」(p.20-45)を実行します。

**ステップ 15** 「[DLP-A255 クロスコネク トカードのサイド切り替えテスト](#)」(p.19-42)を実行します。

60 ミリ秒未満のサービスの中断が発生することがありますが、テスト回線は、切り替えの実行前、実行中、実行後に関係なく同様に機能します。回線が停止した場合は、作業を中断し、次のレベルのサポートに問い合わせます。

**ステップ 16** ノード 1 で「[DLP-A91 BLSR 切り替えテスト](#)」(p.17-94)を行います。



**ステップ 17** テスト回線で BER テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ 18** テスト回線について、「[DLP-A333 回線の削除](#)」(p.20-23)を行います。

**ステップ 19** BLSR 内のノード 2 以降のノードについて、ステップ 5 ~ 18 を繰り返し、リング内の各ノードとスパンをテストします。連続する 2 つのノード間すべてで、テスト回線を作成します。

**ステップ 20** リング全体をテストしたあとで、ノードからすべてのループバックとテストセットを取り外します。

**ステップ 21** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。[第 6 章「回線と VT トンネルの作成」](#)へ進みます。

**終了：この手順は、これで完了です。**

---

## NTP-A176 4 ファイバ BLSR の受け入れテスト

目的	この手順では、4 ファイバ BLSR をテストします。
工具 / 機器	作成するテスト回線に適したテストセットとケーブル
事前準備手順	<a href="#">NTP-A40 BLSR ノードのプロビジョニング (p.5-14)</a> <a href="#">NTP-A126 BLSR の作成 (p.5-16)</a>
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

トラフィックを伝送するノードでこの手順を実行すると、サービスが影響を受けることがあります。



### (注)

この手順では、テスト回線を作成し、リングを切り替えます。わかりやすいように、手順を開始するログインノードを「ノード1」とします。ノード1のイースト OC-N トランク (スパン) カードに接続されたノードを「ノード2」、ノード2のイースト OC-N トランクカードに接続されたノードを「ノード3」という順番でノードを表します。

- ステップ 1** テストする BLSR で「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います (このノードをノード 1 と呼びます)。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** View メニューから、**Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、アラーム情報をエクスポートします。
- ステップ 4** Conditions タブをクリックします。
- 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、状態の情報をエクスポートします。
- ステップ 5** ネットワーク ビューで、Node 1 をダブルクリックします。
- ステップ 6** 「[DLP-A92 4 ファイバ BLSR のスパン負荷テスト](#)」(p.17-99) を実行します。
- ステップ 7** 「[DLP-A217 BLSR の試験リングテスト](#)」(p.19-12) を実行します。

**ステップ 8** ノード 1 とノード 2 の間にテスト回線を作成します。

- DS-1 回線の場合 — 「[NTP-A181 自動ルーティングによる DS-1 回線の作成](#)」( p.6-8 ) を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。
- DS-3 回線の場合 — 「[NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成](#)」( p.6-22 ) を実行します。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。
- OC-N 回線について、「[NTP-A343 自動ルーティングによる光回線の作成](#)」( p.6-47 ) を行います。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。

**ステップ 9** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ 10** このテストで使用する各パッチ ケーブルの一方の端をテスト セットの Tx コネクタに接続し、もう一方の端をテスト セットの Rx コネクタに接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、次へ進む前に、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。

**ステップ 11** 回線の宛先カードで物理的にループバックを作成します。ループバックを作成するには、パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続し、もう一方の端をこのポートの受信 Rx コネクタに接続します。

**ステップ 12** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の Tx コネクタに接続します。

**ステップ 13** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ 6 ~ 12 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ 14** テスト セットからグローバル BIT エラーを発生させます。テスト セットにエラーが表示されることを確認します。エラーが表示される場合は、エンドツーエンドの回線が正しく設定されています。

**ステップ 15** 「[DLP-A356 TCC2/TCC2P カードのアクティブ / スタンバイ切り替えテスト](#)」( p.20-45 ) を実行します。

**ステップ 16** 「DLP-A255 クロスコネク トカードのサイド切り替えテスト」(p.19-42) を実行します。

**ステップ 17** 「DLP-A91 BLSR 切り替えテスト」(p.17-94) を行い、ノード 1 で BLSR の保護切り替えをテストします。

**ステップ 18** ノード 1 で「DLP-A93 4 ファイバ BLSR のスパン切り替えテスト」(p.17-101) を行います。

**ステップ 19** ノード 1 と 2 の間のテスト回線で BER テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ 20** テスト回線について、「DLP-A333 回線の削除」(p.20-23) を行います。

**ステップ 21** ノード 2 でステップ 5 ~ 20 を繰り返し、ノード 2 と、ノード 2 のイースト OC-N トランク (スパン) カードに接続されたノード (ノード 3) との間にテスト回線を作成します。BLSR にある連続した 2 つのノード間すべてでテスト回線を作成し、このリングをテストします。

**ステップ 22** リング全体をテストしたあとで、ノードからすべてのループバックとテスト セットを取り外します。

**ステップ 23** 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-A227 アラーム フィルタリングのディセーブル化」(p.19-21) を参照してください。
- b. 説明のつかないアラームが表示されていないことを確認します。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- c. 「DLP-A532 CTC データのエクスポート」(p.22-35) を行い、アラーム情報をエクスポートします。

**ステップ 24** Conditions タブをクリックします。

- a. 説明のつかない状態が表示されていないことを確認します。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- b. 「DLP-A532 CTC データのエクスポート」(p.22-35) を行い、状態の情報をエクスポートします。

**ステップ 25** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。第 6 章「回線と VT トンネルの作成」へ進みます。

**終了**：この手順は、これで完了です。

## NTP-A178 従来型 BLSR DRI のプロビジョニング

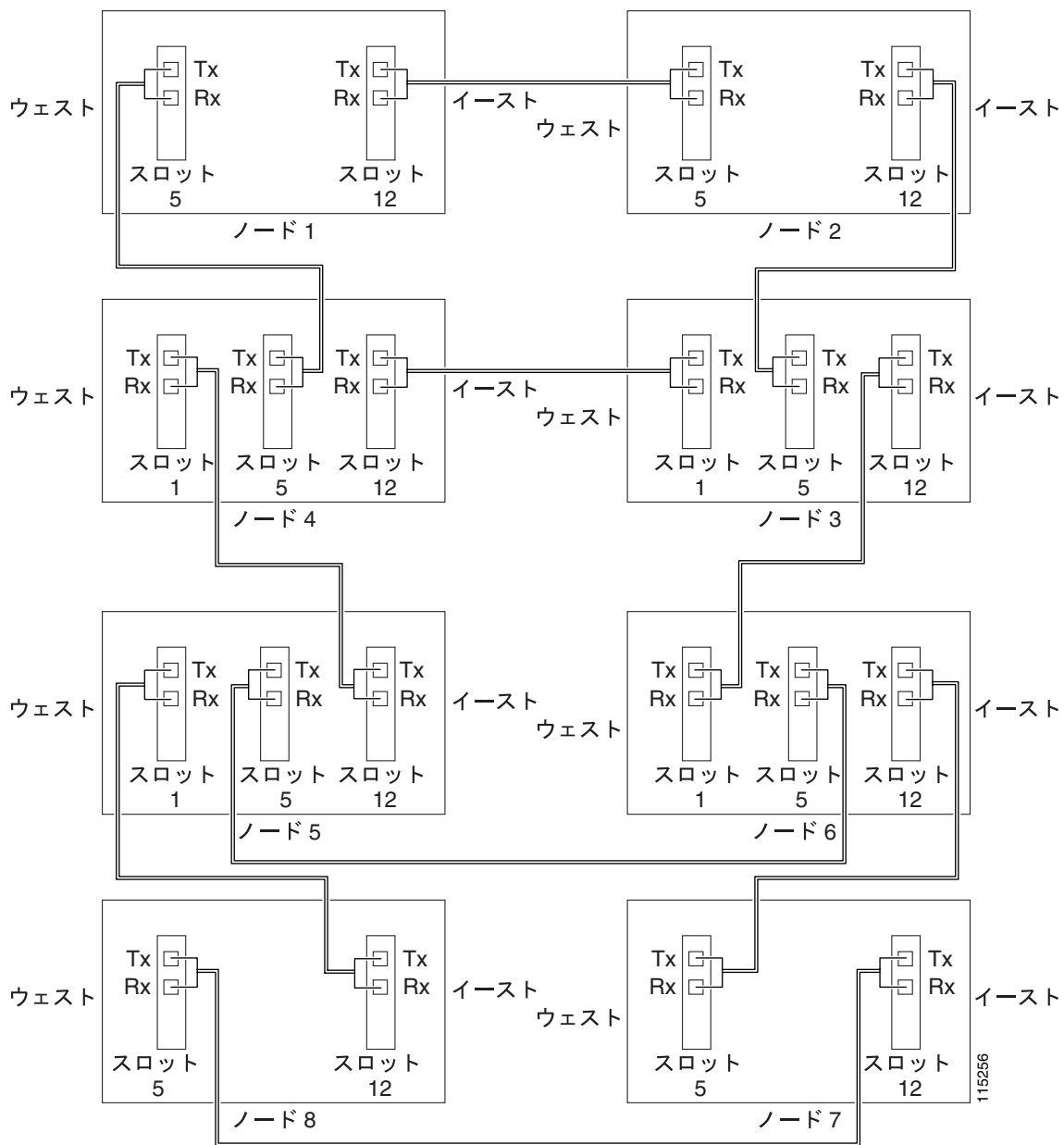
目的	この手順では、従来型 Dual-Ring Interconnect (DRI; デュアル リング相互接続) トポロジーの BLSR をプロビジョニングします。DRI で 2 つ以上の BLSR を相互接続すれば、保護を強化することができます。従来型の BLSR DRI ネットワークでは、2 ファイバおよび 4 ファイバの BLSR を混在させることができます。
工具 / 機器	なし
事前準備手順	NTP-A35 ノードの起動の確認 (p.5-3)
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル

**(注)**

回線を DRI にルーティングする場合は、回線作成時に Dual Ring Interconnect チェックボックスをオンにする必要があります。

- ステップ 1** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** BLSR DRI で相互接続する BLSR をプロビジョニングしていない場合は、次のステップを行います。BLSR がすでに作成されている場合は、ステップ 3 へ進みます。
- 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行して、BLSR をプロビジョニングします。
  - 「NTP-A126 BLSR の作成」(p.5-16) を実行して、BLSR を作成します。
  - 「NTP-A175 2 ファイバ BLSR の受け入れテスト」(p.5-17) を実行して、2 ファイバ BLSR をテストします。
  - 「NTP-A176 4 ファイバ BLSR の受け入れテスト」(p.5-20) を実行して、4 ファイバ BLSR をテストします。
- ステップ 3** BLSR DRI で相互接続するノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。
- 相互接続ノードには、BLSR を接続するための OC-N カードが取り付けられている必要があります。
  - 相互接続ノードは、ファイバ接続されている必要があります。図 5-4 に、従来型の 2 ファイバ BLSR DRI について、そのファイバ接続例を示します。

図 5-4 従来型の 2 ファイバ BLSR DRI のファイバ接続例



終了：この手順は、これで完了です。

## NTP-A179 統合 BLSR DRI のプロビジョニング

目的	この手順では、統合 DRI トポロジーの BLSR をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** BLSR DRI ネットワークにあるノードで、「[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。

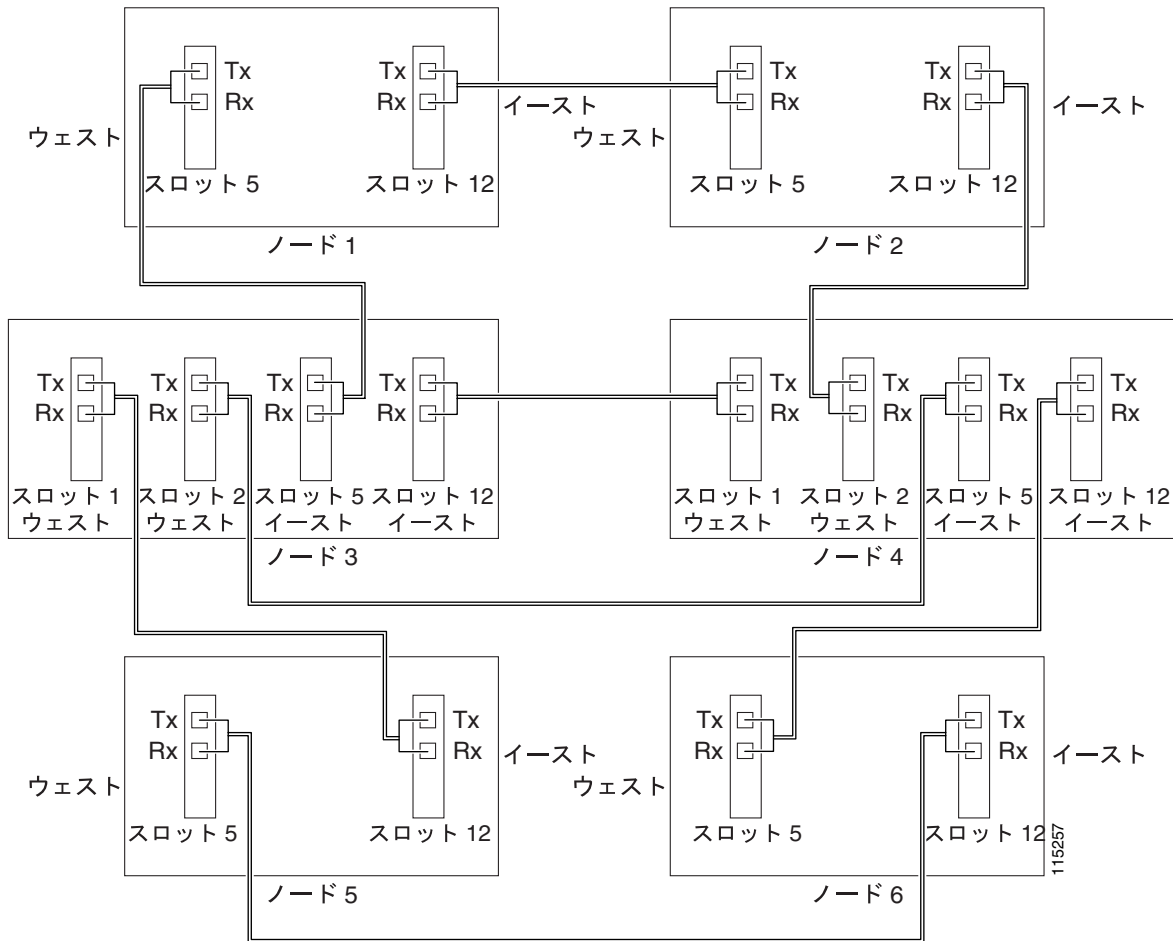
**ステップ 2** BLSR DRI で相互接続する BLSR をプロビジョニングしていない場合は、次のステップを行います。BLSR がすでに作成されている場合は、ステップ 3 へ進みます。

- a. 「[NTP-A40 BLSR ノードのプロビジョニング](#)」(p.5-14)を実行して、BLSR をプロビジョニングします。
- b. 「[NTP-A126 BLSR の作成](#)」(p.5-16)を実行して、BLSR を作成します。
- c. 「[NTP-A175 2 ファイバ BLSR の受け入れテスト](#)」(p.5-17)を実行して、2 ファイバ BLSR をテストします。
- d. 「[NTP-A176 4 ファイバ BLSR の受け入れテスト](#)」(p.5-20)を実行して、4 ファイバ BLSR をテストします。

**ステップ 3** BLSR DRI ノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。

- 2つの相互接続ノードに、BLSR を接続するための OC-N カードが取り付けられている必要があります。
- 2つの相互接続ノードは、ファイバで正しく接続されている必要があります。[図 5-5](#)に、統合 2 ファイバ BLSR DRI 構成の例を示します。

図 5-5 統合 2 ファイバ BLSR DRI 構成の例



終了：この手順は、これで完了です。



## NTP-A44 UPSR ノードのプロビジョニング

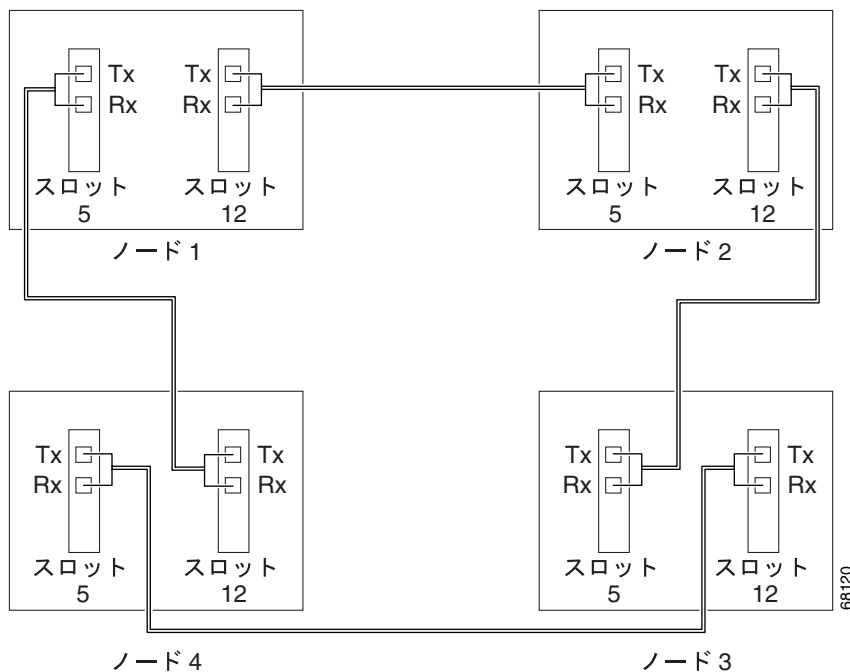
目的	この手順では、UPSR に組み込むノードをプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	プロビジョニング以上のレベル



**(注)** UPSR は、ONS 15454 のデフォルトのトポロジーになっています。UPSR OC-N カードを取り付け、OC-N ファイバを接続して、DCC の終端を作成すると、すぐに使用できます。BLSR と異なり、ONS 15454 UPSR は、明示的に設定する必要がありません。

**ステップ 1** [図 5-6](#) のように、ファイバが UPSR トランク (スパン) OC-N カードに正しく接続されていることを確認します。「[DLP-A43 UPSR 構成での光ファイバケーブルの取り付け](#)」(p.17-51) を参照してください。

**図 5-6 UPSR ファイバ接続の例**



**ステップ 2** 起動する UPSR で ONS 15454 にログインします。「[DLP-A60 CTC へのログイン](#)」(p.17-71) を参照してください。すでにログインしている場合は、ステップ 3 へ進みます。

**ステップ 3** ノードで UPSR ポートとして機能する 2 つのカードまたはポート、たとえばノード 1 のスロット 5 (OC-48) とノード 1 のスロット 12 (OC-48) などについて、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74)を行います(または、CTC の管理のために帯域幅の追加が必要な場合は、「[DLP-A378 LDCC 終端のプロビジョニング](#)」[p.20-77]を行います)。



**(注)** ONS 15454 を社内 LAN に接続していない場合は、このノードに直接(クラフト)接続して DCC または LDCC をプロビジョニングする必要があります。リモート プロビジョニングが可能になるのは、ネットワーク内のすべてのノードの DCC または LDCC の終端が稼働中の OC-N ポートにプロビジョニングされたあとのみです。

**ステップ 4** UPSR 内の各ノードについて、ステップ 2 ~ 3 を繰り返します。

**ステップ 5** 必要に応じて、「[DLP-A380 プロキシ トンネルのプロビジョニング](#)」(p.20-82)を行います。

**ステップ 6** 必要に応じて、「[DLP-A381 ファイアウォール トンネルのプロビジョニング](#)」(p.20-83)を行います。

**ステップ 7** 必要に応じて、「[DLP-A367 プロビジョニング可能なパッチコードの作成](#)」(p.20-56)を行います。

**ステップ 8** 「[NTP-A177 UPSR の受け入れテスト](#)」(p.5-29)を実行します。

**終了:** この手順は、これで完了です。

---

## NTP-A177 UPSR の受け入れテスト

目的	この手順では、UPSR をテストします。
工具 / 機器	作成するテスト回線に適したテストセットとケーブル
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a>
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

トラフィックを伝送するノードでこの手順を実行すると、サービスが影響を受けることがあります。

- ステップ 1** テスト対象の UPSR にある 1 つの ONS 15454 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** View メニューから **Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、アラーム情報をエクスポートします。
- ステップ 4** Conditions タブをクリックします。
- 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行い、状態の情報をエクスポートします。
- ステップ 5** ステップ 1 でログインしたノードをネットワーク マップ上でダブルクリックします。
- ステップ 6** そのノードから隣接する次の UPSR ノードまでのテスト回線を作成します。
- DS-1 回線の場合 — 「[NTP-A181 自動ルーティングによる DS-1 回線の作成](#)」(p.6-8) を実行します。回線の状態を設定する場合は、IS を選択し、**Apply to drop ports** チェックボックスをオンにします。
  - DS-3 回線の場合 — 「[NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成](#)」(p.6-22) を実行します。回線の状態を設定する場合は、IS を選択し、**Apply to drop ports** チェックボックスをオンにします。
  - OC-N 回線について、「[NTP-A343 自動ルーティングによる光回線の作成](#)」(p.6-47) を行います。回線の状態を設定する場合は、IS を選択し、**Apply to drop ports** チェックボックスをオンにします。

**ステップ7** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ8** このテストで使用する各パッチ ケーブルの一方の端をテスト セットの Tx コネクタに接続し、もう一方の端をテスト セットの Rx コネクタに接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、次へ進む前に、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。

**ステップ9** 回線の宛先カードで物理的にループバックを作成します。

- a. パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続します。
- b. もう一方の端をポートの Rx コネクタに接続します。

**ステップ10** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の Tx コネクタに接続します。

**ステップ11** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ 6 ~ 10 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ12** テスト セットから BIT エラーを発生させます。エンドツーエンド回線が完全であることを確認するために、テスト セットにエラーが表示されることを確認します。

**ステップ13** 「[DLP-A356 TCC2/TCC2P カードのアクティブ/スタンバイ切り替えテスト \(p.20-45\)](#)」を実行します。

**ステップ14** 「[DLP-A255 クロスコネクタ カードのサイド切り替えテスト \(p.19-42\)](#)」を実行します。

**ステップ15** View メニューから **Go to Network View** を選択します。

**ステップ16** 回線の送信元ノードに接続された2つのスパンのうちの1つをクリックします。

**ステップ17** 「[DLP-A94 UPSR の保護切り替えテスト \(p.17-103\)](#)」を行い、このスパンで UPSR 保護切り替えをテストします。

**ステップ 18** ネットワーク ビューで、回線のもう一方の送信元スパンをクリックし、[ステップ 17](#) を繰り返します。

**ステップ 19** BER テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ 20** テスト回線について、「[DLP-A333 回線の削除](#)」(p.20-23)を行います。

**ステップ 21** すべてのテストが完了したら、ノードからループバック、スイッチ、またはテスト セットを取り外します。

**ステップ 22** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21)を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- c. 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、アラーム情報をエクスポートします。

**ステップ 23** Conditions タブをクリックします。

- a. 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- b. 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、状態の情報をエクスポートします。

**ステップ 24** ネットワーク内の各ノードについて、[ステップ 5 ~ 23](#) を繰り返します。

**ステップ 25** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。[第 6 章「回線と VT トンネルの作成」](#)へ進みます。

**終了**：この手順は、これで完了です。

## NTP-A216 従来型 UPSR DRI のプロビジョニング

目的	この手順では、従来型 DRI トポロジーの UPSR をプロビジョニングします。DRI で 2 つ以上の UPSR を相互接続すると、保護を強化することができます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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) 回線を DRI にルーティングする場合は、回線作成時に Dual Ring Interconnect チェックボックスをオンにする必要があります。

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** UPSR DRI で相互接続する UPSR をプロビジョニングしていない場合は、次のステップを行います。UPSR がすでに作成されている場合は、ステップ 3 へ進みます。

- a. 「[NTP-A44 UPSR ノードのプロビジョニング](#)」(p.5-27) を実行して、UPSR をプロビジョニングします。
- b. 「[NTP-A177 UPSR の受け入れテスト](#)」(p.5-29) を実行して、UPSR をテストします。

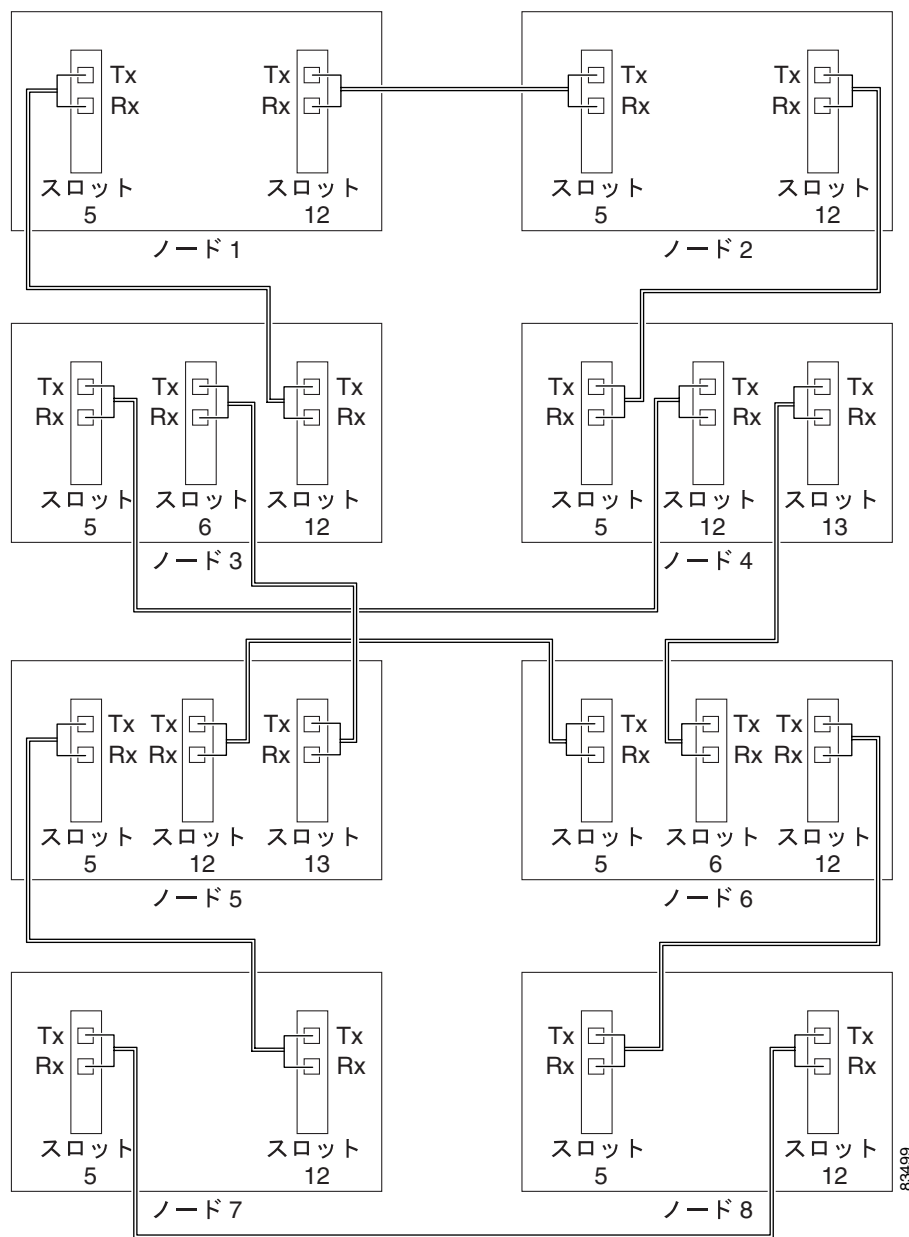


(注) 相互接続するすべての UPSR で OC-N のレートが同じである必要があります。

**ステップ 3** UPSR DRI で相互接続するノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。

- 相互接続ノードには、UPSR を接続するための OC-N カードが取り付けられている必要があります。UPSR ノード内の OC-N カードと相互接続ノードは、同じタイプである必要があります。
- 相互接続ノードは、ファイバで接続されている必要があります。図 5-7 に例を示します。この例では、2 つのリング (ノード 1 ~ 4 とノード 5 ~ 8) を UPSR DRI で相互接続しています。OC-N カードが、ノード 4 のスロット 13 に追加されていて、ノード 6 のスロット 6 にある OC-N カードに接続されています。ノード 3 と 5 は、ノード 3 のスロット 6 とノード 5 のスロット 13 にある OC-N カードで相互接続されています。

図 5-7 従来型 UPSR DRI ファイバ接続の例



終了：この手順は、これで完了です。

83499

## NTP-A217 統合 UPSR DRI のプロビジョニング

目的	この手順では、統合 DRI トポロジーの UPSR をプロビジョニングします。統合 DRI では、両方の UPSR で UPSR OC-N トランクカードを同じシェルフに取り付けます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** UPSR DRI ネットワークにあるノードで、「[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** UPSR DRI で相互接続する UPSR をプロビジョニングしていない場合は、次のステップを行います。UPSR がすでに作成されている場合は、ステップ 3 へ進みます。

- a. 「[NTP-A44 UPSR ノードのプロビジョニング](#)」(p.5-27)を実行して、UPSR をプロビジョニングします。
- b. 「[NTP-A177 UPSR の受け入れテスト](#)」(p.5-29)を実行して、UPSR をテストします。



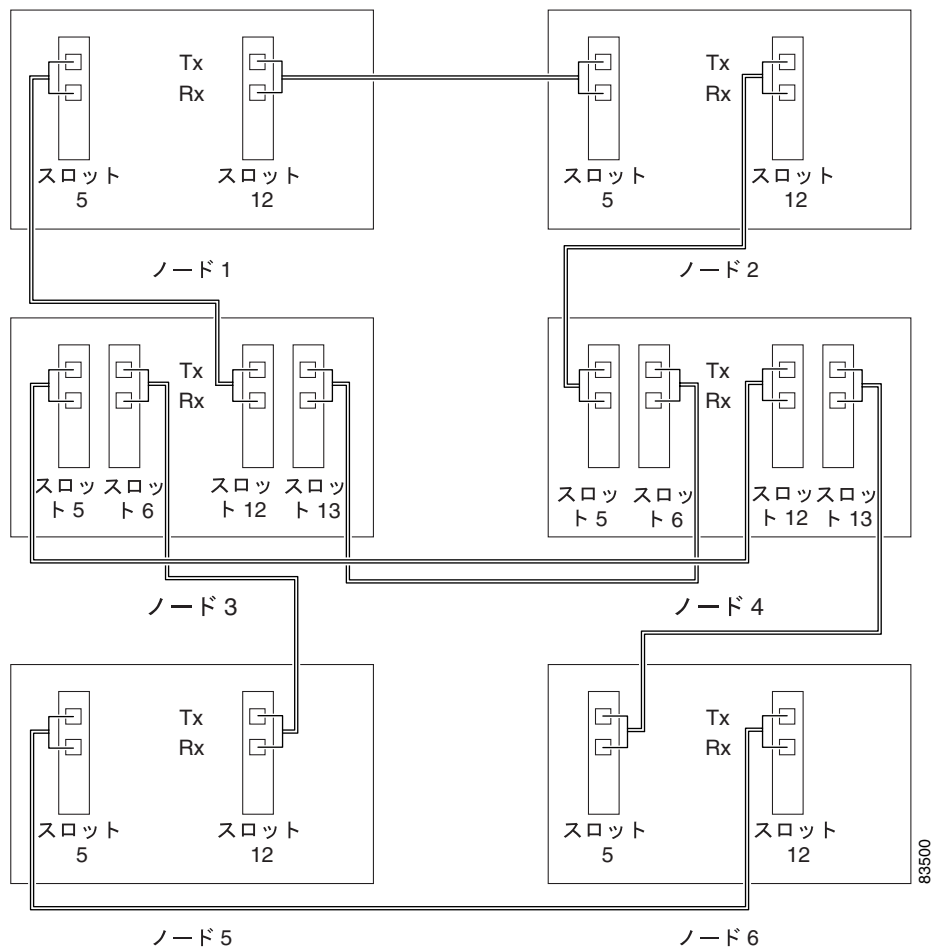
**(注)** 相互接続するすべての UPSR で OC-N のレートが同じである必要があります。

**ステップ 3** UPSR DRI で相互接続するノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。

- 相互接続ノードには、UPSR を接続するための OC-N カードが取り付けられている必要があります。UPSR ノード内の OC-N カードと相互接続ノードは、同じタイプである必要があります。
- 相互接続ノードは、ファイバで正しく接続されている必要があります。[図 5-8](#) に例を示します。この例では、UPSR DRI で 2 つのリングを相互接続しています。



図 5-8 統合 UPSR DRI の例



終了：この手順は、これで完了です。

## NTP-A180 従来型 BLSR/UPSR DRI のプロビジョニング

目的	この手順では、従来型 DRI トポロジーの BLSR および UPSR をプロビジョニングします。DRI でリング トポロジーを相互接続すれば、保護を強化することができます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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)

回線を DRI にルーティングする場合は、回線作成時に Dual Ring Interconnect チェックボックスをオンにする必要があります。

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 従来型 DRI で相互接続する BLSR および UPSR をプロビジョニングしていない場合は、次のステップを行います。BLSR および UPSR がすでに作成されている場合は、ステップ 3 へ進みます。

a. 次の手順を実行し、BLSR をプロビジョニングしてテストします。

- [NTP-A40 BLSR ノードのプロビジョニング \(p.5-14\)](#)
- [NTP-A126 BLSR の作成 \(p.5-16\)](#)
- [NTP-A175 2 ファイバ BLSR の受け入れテスト \(p.5-17\)](#)
- [NTP-A176 4 ファイバ BLSR の受け入れテスト \(p.5-20\)](#)

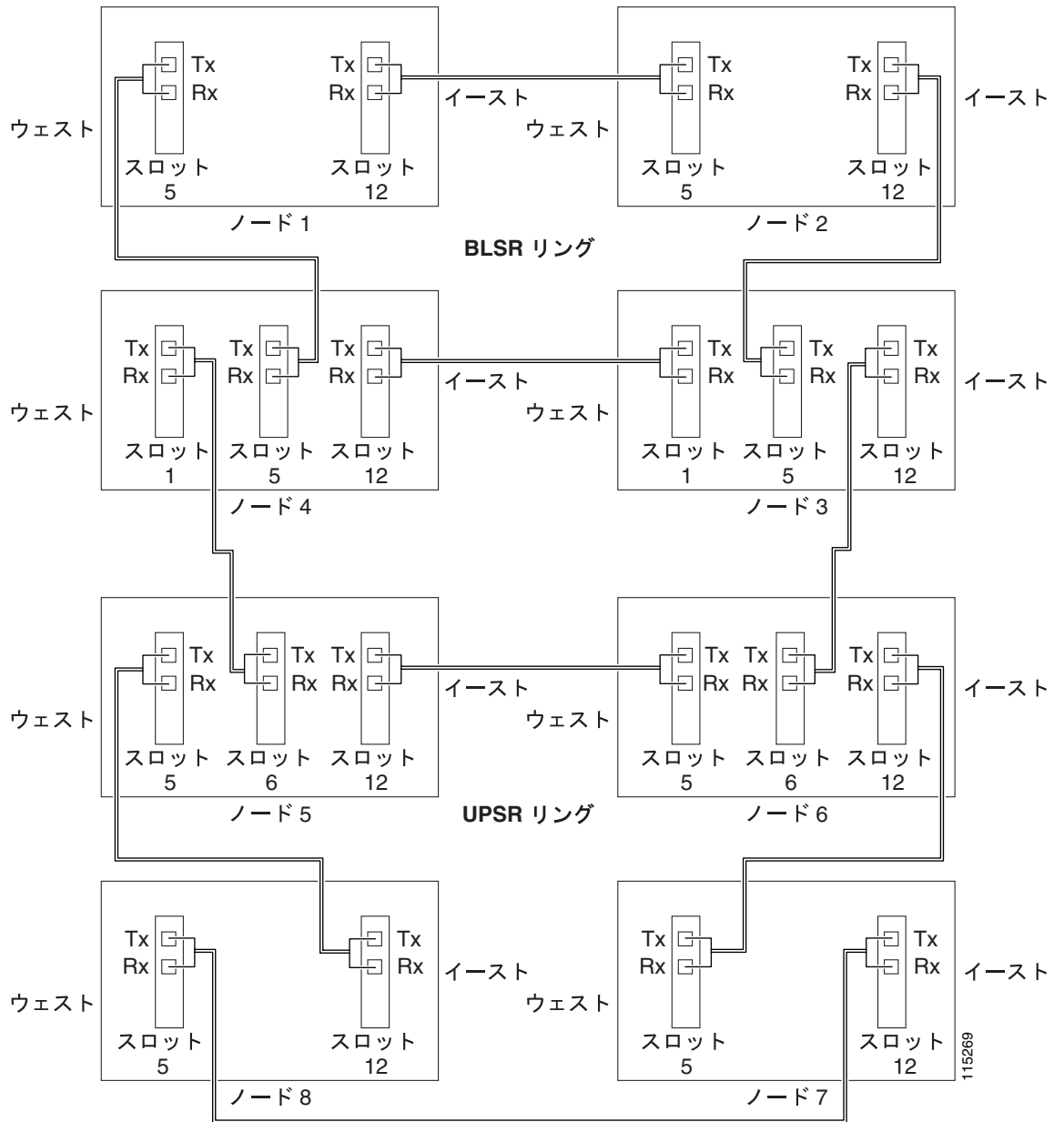
b. 次の手順を実行し、UPSR をプロビジョニングしてテストします。

- [NTP-A44 UPSR ノードのプロビジョニング \(p.5-27\)](#)
- [NTP-A177 UPSR の受け入れテスト \(p.5-29\)](#)

**ステップ 3** DRI で相互接続するノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。

- 相互接続ノードには、BLSR および UPSR を接続するための OC-N カードが取り付けられている必要があります。UPSR ノード内の OC-N カードと相互接続ノードは、同じタイプである必要があります。
- 相互接続ノードは、ファイバで接続されている必要があります。[図 5-9](#) に例を示します。

図 5-9 従来型 BLSR/UPSR DRI のファイバ接続の例



終了：この手順は、これで完了です。

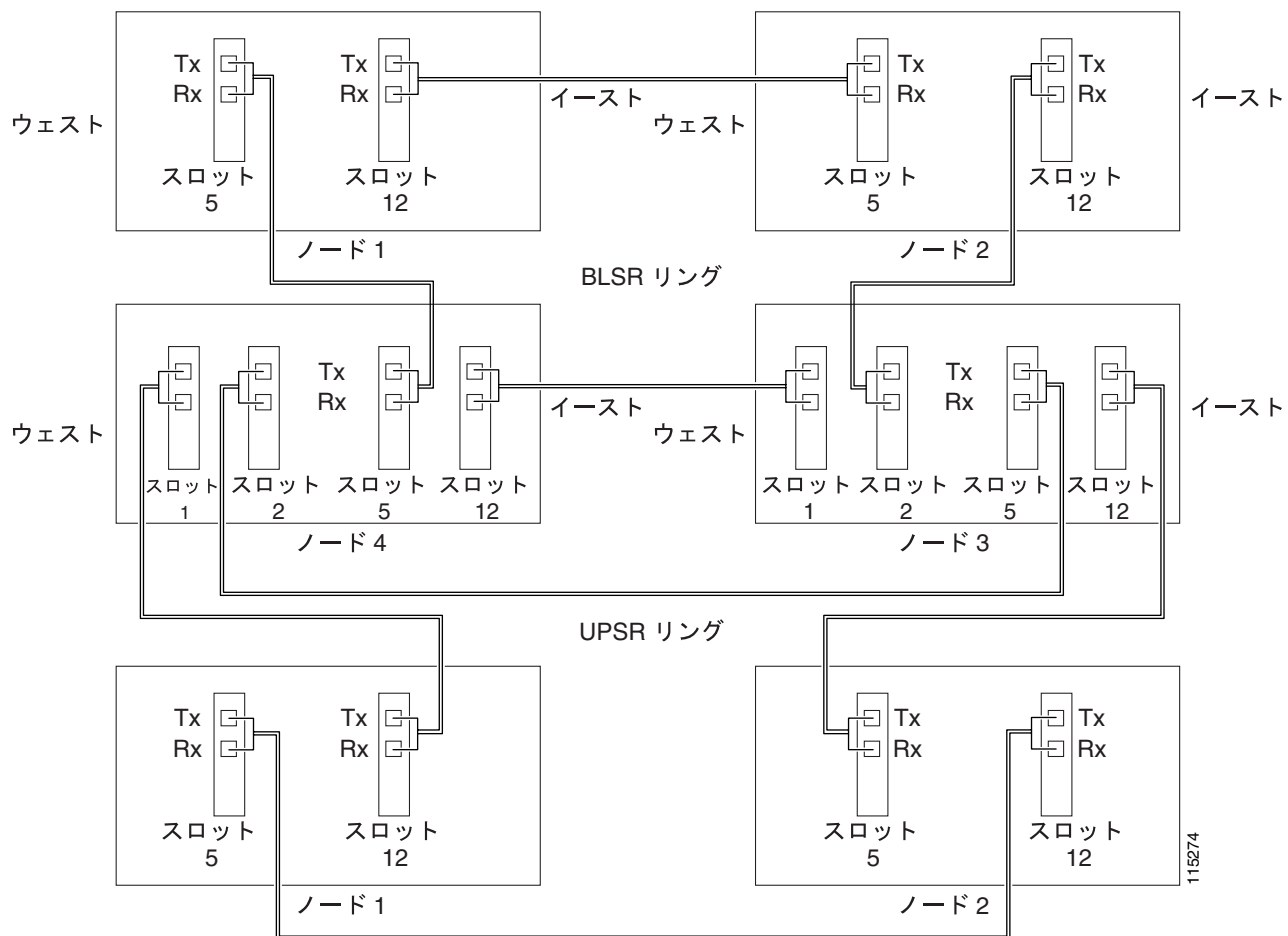
115269

## NTP-A209 統合 BLSR/UPSR DRI のプロビジョニング

目的	この手順では、統合 DRI トポロジーの BLSR および UPSR をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** BLSR および UPSR DRI ネットワークにあるノードで、「[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** 統合 DRI で相互接続する BLSR および UPSR をプロビジョニングしていない場合は、次のステップを行います。BLSR および UPSR がすでに作成されている場合は、ステップ 3 へ進みます。
- a. 次の手順を実行し、BLSR をプロビジョニングしてテストします。
    - [NTP-A40 BLSR ノードのプロビジョニング \(p.5-14\)](#)
    - [NTP-A126 BLSR の作成 \(p.5-16\)](#)
    - [NTP-A175 2 ファイバ BLSR の受け入れテスト \(p.5-17\)](#)
    - [NTP-A176 4 ファイバ BLSR の受け入れテスト \(p.5-20\)](#)
  - b. 次の手順を実行し、UPSR をプロビジョニングしてテストします。
    - [NTP-A44 UPSR ノードのプロビジョニング \(p.5-27\)](#)
    - [NTP-A177 UPSR の受け入れテスト \(p.5-29\)](#)
- ステップ 3** BLSR および UPSR DRI で相互接続するノードに OC-N カードが取り付けられていることと、相互にファイバで接続されていることを確認します。
- 相互接続ノードには、BLSR および UPSR を接続するための OC-N カードが取り付けられている必要があります。UPSR ノード内の OC-N カードと相互接続ノードは、同じタイプである必要があります。
  - 相互接続ノードは、ファイバで正しく接続されている必要があります。[図 5-10](#) に例を示します。

図 5-10 統合 BLSR/UPSR DRI の例



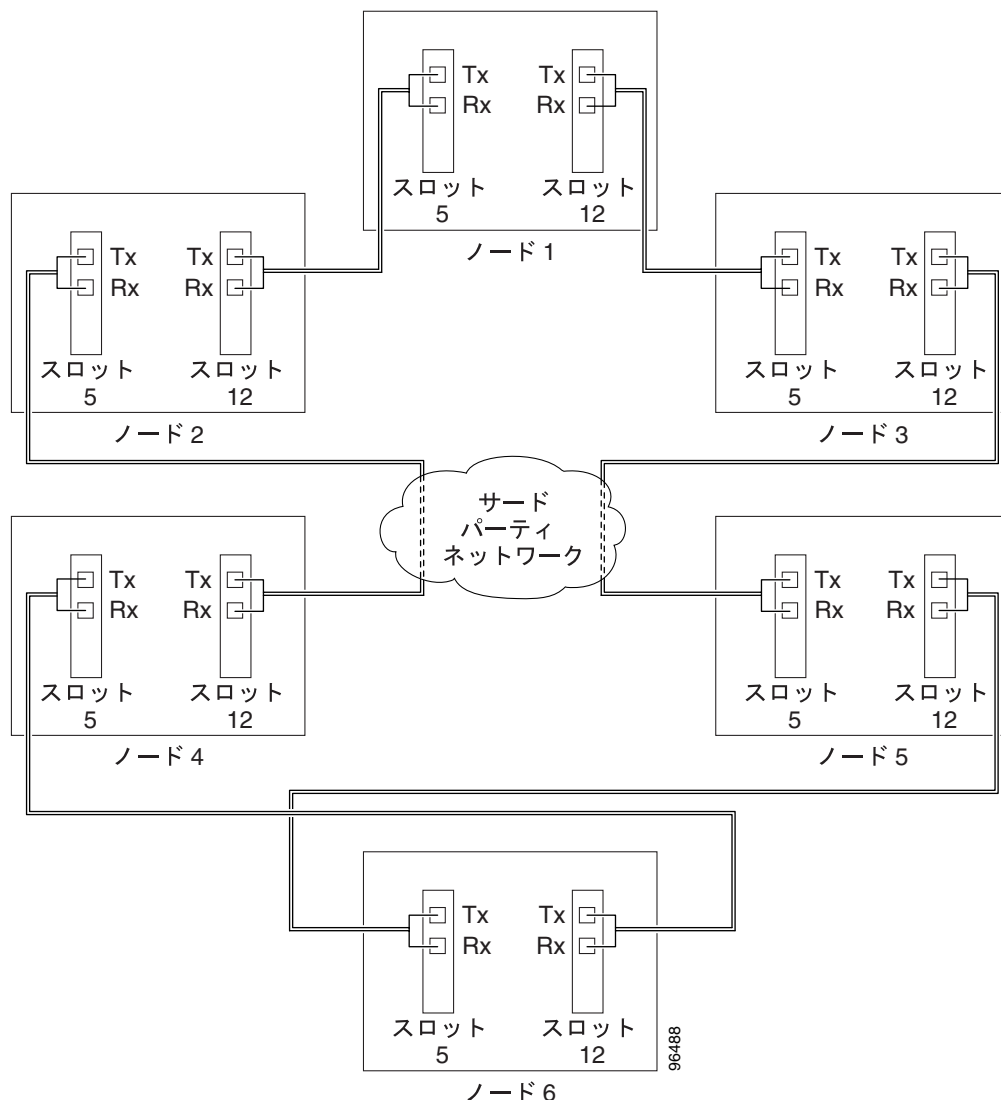
終了：この手順は、これで完了です。

## NTP-A224 開放端 UPSR のプロビジョニング

目的	この手順では、サードパーティベンダーのネットワークに接続する開放端 UPSR 内で ONS 15454 ノードをプロビジョニングします。このトポロジーでは、サードパーティのネットワークを経由して ONS 15454 ネットワーク間に回線をルーティングできます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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** すべての開放端 UPSR ノードで、UPSR トランク (スパン) OC-N カードにファイバが正しく接続されていることを確認します。図 5-11 に例を示します。ノード 1 は、ONS 15454 のノード 2 (スロット 12) とノード 3 (スロット 5) に接続されています。ノード 2 と 3 のトランク カードは、サードパーティベンダーの機器に接続されています。

図 5-11 ONS 15454 の開放端 UPSR ファイバ接続の例



**ステップ2** ONS 15454 トランク カードに接続されているサードパーティ製のカードの OC-N レートが、ONS 15454 トランク カードの OC-N レートと同じであることを確認します。サードパーティのタイム スロットは、接続されている ONS 15454 カードのタイム スロットと同じである必要があります。たとえば、トランク カードが OC-48 の場合、サードパーティ ベンダー製のカードまたはユニットで、STS の 1 ~ 48 を使用できる必要があります。

**ステップ3** 起動する UPSR で ONS 15454 にログインします。「[DLP-A60 CTC へのログイン](#)」(p.17-71) を参照してください。すでにログインしている場合は、ステップ4へ進みます。

**ステップ4** 他の ONS 15454 に接続されている ONS 15454 カードまたはポートについて、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を行います (CTC の管理に必要な帯域幅が不足している場合は、「[DLP-A378 LDCC 終端のプロビジョニング](#)」[p.20-77] を行います)。サードパーティ製の機器に接続されているカードまたはポートに対しては DCC の終端も LDCC の終端も作成しないでください。たとえば、[図 5-11](#) では、DCC の終端を次のカードまたはポートに作成します。

- ノード1 および6 : スロット5 およびスロット12
- ノード2 および5 : スロット12
- ノード3 および4 : スロット5



**(注)** ONS 15454 を社内 LAN に接続していない場合は、このノードに直接 (クラフト) 接続して DCC または LDCC をプロビジョニングする必要があります。リモート プロビジョニングが可能になるのは、ネットワーク内のすべてのノードの DCC または LDCC の終端が稼働中の OC-N ポートにプロビジョニングされたあとのみです。

**ステップ5** UPSR 内の各ノードについて、ステップ3 ~ 4 を繰り返します。

**ステップ6** 必要に応じて、「[DLP-A380 プロキシ トンネルのプロビジョニング](#)」(p.20-82) を行います。

**ステップ7** 必要に応じて「[DLP-A381 ファイアウォール トンネルのプロビジョニング](#)」(p.20-83) を行います。

**ステップ8** サードパーティ ベンダーの提供しているマニュアルに従って、一方の端にある ONS 15454 接続からもう一方の端にある ONS 15454 接続までの光ループをプロビジョニングします。つまり、サードパーティ製機器用の手順を使用して、開放端 UPSR を作成します。

**ステップ9** 「[NTP-A225 開放端 UPSR の受け入れテスト](#)」(p.5-42) を実行します。

**終了 :** この手順は、これで完了です。

## NTP-A225 開放端 UPSR の受け入れテスト

目的	この手順では、開放端 UPSR リングをテストします。
工具 / 機器	作成するテスト回線に適したテストセットとケーブル
事前準備手順	<a href="#">NTP-A224 開放端 UPSR のプロビジョニング (p.5-40)</a>
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

トラフィックを伝送するノードでこの手順を実行すると、サービスが影響を受けることがあります。

- ステップ 1** サードパーティのネットワークを通過するトラフィックの送信元ノードで「[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** View メニューから **Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラームフィルタリングのディセーブル化](#)」(p.19-21)を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、アラーム情報をエクスポートします。
- ステップ 4** Conditions タブをクリックします。
- 説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35)を行い、状態の情報をエクスポートします。
- ステップ 5** [ステップ 1](#) でログインしたノードをネットワークマップ上でダブルクリックします。
- ステップ 6** このノードから、サードパーティのネットワークに接続するノードにある OC-N トランク (スパン) カードまでのテスト回線を作成します。たとえば、[図 5-11](#) では、ノード 1 からノード 2 のスロット 5 にある OC-N カードまでの間に回線が作成されます。セカンダリ回線の宛先は、ノード 3 のスロット 12 にある OC-N カードに作成されます。回線を作成するには、次のいずれかの作業を行います。
- DS-1 回線の場合 — 「[NTP-A181 自動ルーティングによる DS-1 回線の作成](#)」(p.6-8)を実行します。回線の状態を設定する場合は、**IS** を選択し、**Apply to drop ports** チェックボックスをオンにします。
  - DS-3 回線の場合 — 「[NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成](#)」(p.6-22)を実行します。回線の状態を設定する場合は、**IS** を選択し、**Apply to drop ports** チェックボックスをオンにします。



- OC-N 回線について、「NTP-A343 自動ルーティングによる光回線の作成」(p.6-47)を行います。回線の状態を設定する場合は、IS を選択し、Apply to drop ports チェックボックスをオンにします。

**ステップ7** サードパーティのネットワーク内で、両方の UPSR スパンにある ONS 15454 の接続ポートから ONS 15454 接続ポートのセカンダリ セットまでの間に回線を作成します。回線の作成手順については、サードパーティ製機器のマニュアルを参照してください。

**ステップ8** ステップ6 を繰り返して、サードパーティ ネットワークの反対側にある終端ノードにセカンダリ回線を作成します。図 5-11 でこれに該当するのはノード6です。ただし、この回線には2つの送信元(ノード4のポート12とノード5のポート5)を設定します。宛先は、ノード6のドロップカードです。

**ステップ9** 作成したテスト回線のタイプに合わせてテスト セットを設定します。

- DS-1 — 多重化されていない DS-1 をテストする場合は、ONS 15454 に DSX-1 パネルまたはダイレクト DS-1 インターフェイスが必要です。DS-1 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS-3 — クリア チャネル DS-3 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。クリア チャネル DS-3 に対応するようにテスト セットを設定してください。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードで DS-1 をテストする場合は、ONS 15454 に DSX-3 パネルまたはダイレクト DS-3 インターフェイスが必要です。多重化 DS-3 に対応するようにテスト セットを設定してください。次に、多重化 DS-3 でテストする DS-1 を選択します。テスト セットの設定方法については、テスト セットのユーザ ガイドを参照してください。
- OC-N — OC-N 回線をテストする場合は、適用可能な回線サイズに対応するようにテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ10** このテストで使用する各パッチ ケーブルの一方の端をテスト セットの Tx コネクタに接続し、もう一方の端をテスト セットの Rx コネクタに接続して、すべてのケーブルが完全であることを確認します。テスト セットが正常に動作しない場合は、次へ進む前に、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。

**ステップ11** 回線の宛先カードで物理的にループバックを作成します。

- a. パッチ ケーブルの一方の端を宛先ポートの Tx コネクタに接続します。
- b. もう一方の端をポートの Rx コネクタに接続します。

**ステップ12** 回線の送信元カードで、次の作業を行います。

- a. テスト セットの Tx コネクタを回線の Rx コネクタに接続します。
- b. テスト セットの Rx コネクタを回線の Tx コネクタに接続します。

**ステップ13** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ6 ~ 12 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ14** テスト セットから BIT エラーを発生させます。エンドツーエンド回線が完全であることを確認するために、テスト セットにエラーが表示されることを確認します。

**ステップ 15** 「DLP-A356 TCC2/TCC2P カードのアクティブ / スタンバイ切り替えテスト」(p.20-45)を実行します。

**ステップ 16** 「DLP-A255 クロスコネク ト カードのサイド切り替えテスト」(p.19-42)を実行します。

60 ミリ秒未満のサービスの中断が発生することがありますが、テスト回線は、切り替えの実行前、実行中、実行後に関係なく同様に機能します。回線が停止した場合は、作業を中断し、次のレベルのサポートに問い合わせます。

**ステップ 17** View メニューから **Go to Network View** を選択します。

**ステップ 18** 回線の送信元ノードに接続されている 2 つのスパンのうちの 1 つをクリックします。

**ステップ 19** 「DLP-A94 UPSR の保護切り替えテスト」(p.17-103)を行い、このスパンで UPSR 保護切り替えをテストします。

**ステップ 20** ネットワーク ビューで、回線のもう一方の送信元スパンをクリックし、**ステップ 19** を繰り返します。

**ステップ 21** BER テストを設定して実行します。テスト期間については、既存の設定を使用し、サイトの要件に従います。テスト結果と設定を記録します。

**ステップ 22** テスト回線について、「DLP-A333 回線の削除」(p.20-23)を行います。

**ステップ 23** すべてのテストが完了したら、ノードからループバック、スイッチ、またはテスト セットを取り外します。

**ステップ 24** ネットワーク 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-A227 アラーム フィルタリングのディセーブル化」(p.19-21)を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- c. 「DLP-A532 CTC データのエクスポート」(p.22-35)を行い、アラーム情報をエクスポートします。

**ステップ 25** ネットワーク ビューで、**Conditions** タブをクリックします。

- a. 説明のつかない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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- b. 「DLP-A532 CTC データのエクスポート」(p.22-35)を行い、状態の情報をエクスポートします。

**ステップ 26** サードパーティのネットワークを通過する回線の送信元または宛先となる各ノードについて、**ステップ 6 ~ 25** を繰り返します。

**ステップ 27** いずれかのテストでエラーが発生したノードについては、設定および構成が正しいことを確認して、テストを繰り返します。それでもエラーが発生する場合は、次のレベルのサポートに問い合わせます。

すべてのテストが正常に終了し、アラームがネットワーク上に発生しなくなったら、ネットワークの準備は終了です。**第 6 章「回線と VT トンネルの作成」**へ進みます。

終了：この手順は、これで完了です。

## NTP-A46 BLSR からの UPSR のサブテンディング

目的	この手順では、既存の BLSR から UPSR をサブテンドします。
工具 / 機器	BLSR ノードには、OC-N カードと、UPSR を伝送するためのファイバが必要です。
事前準備手順	<a href="#">NTP-A175 2 ファイバ BLSR の受け入れテスト (p.5-17)</a> または <a href="#">NTP-A176 4 ファイバ BLSR の受け入れテスト (p.5-20)</a>
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



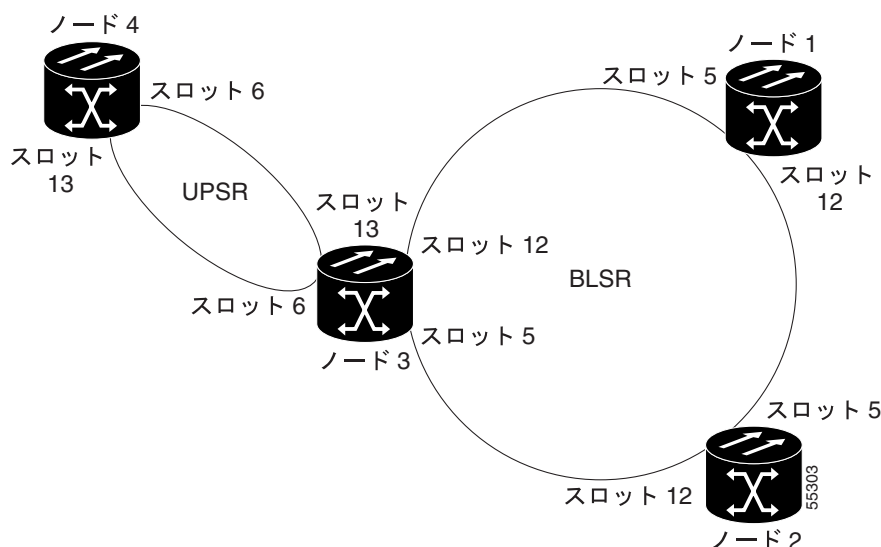
(注)

UPSR は、ONS 15454 のデフォルトのトポロジーになっています。UPSR OC-N カードを取り付け、OC-N ファイバを接続して、DCC の終端を作成すると、すぐに使用できます。BLSR と異なり、ONS 15454 UPSR は、明示的に設定する必要がありません。

**ステップ 1** UPSR をサブテンドするノード ( [図 5-12](#) のノード 3 ) に、UPSR トランク ( スパン ) カードとして機能する 2 つの OC-N カード ( ノード 3 のスロット 6 と 13 ) を取り付けます。「[NTP-A16 光カードおよびコネクタの取り付け](#)」( p.2-8 ) を参照してください。カードがすでに取り付けられている場合は、[ステップ 2](#) へ進みます。

**ステップ 2** これらのカードから、隣接する UPSR ノードの UPSR トランク カードにファイバを接続します。[図 5-12](#) では、ノード 3 のスロット 6 とノード 4 のスロット 13 が、またノード 3 のスロット 13 とノード 4 のスロット 6 がそれぞれ接続されています。

図 5-12 BLSR からの UPSR のサブテンディング



- ステップ 3** UPSR をサブテンドする ONS 15454 (この例ではノード 3) で、「DLP-A60 CTC へのログイン」(p.17-71) を行います。
- ステップ 4** UPSR を伝送する各 OC-N カードについて、「DLP-A377 SDCC 終端のプロビジョニング」(p.20-74) を行います。CTC の管理に必要な帯域幅が不足している場合は、「DLP-A378 LDCC 終端のプロビジョニング」(p.20-77) を行って追加します。
- ステップ 5** **ステップ 3** のノードに接続している UPSR ノードにログインします(図 5-12 では、ノード 4 が UPSR 内にある唯一のその他のノードです)。
- ステップ 6** UPSR のトラフィックを伝送する各 OC-N カードについて、「DLP-A377 SDCC 終端のプロビジョニング」(p.20-74) を行います。CTC の管理に必要な帯域幅が不足している場合は、「DLP-A378 LDCC 終端のプロビジョニング」(p.20-77) を行って追加します。
- ステップ 7** UPSR の各ノードについて、**ステップ 6** を繰り返します。
- ステップ 8** 必要に応じて、「DLP-A380 プロキシ トンネルのプロビジョニング」(p.20-82) を行います。
- ステップ 9** 必要に応じて、「DLP-A381 ファイアウォール トンネルのプロビジョニング」(p.20-83) を行います。
- ステップ 10** View メニューから **Go To Network View** を選択し、サブテンディング リングを表示します。
- ステップ 11** 「NTP-A177 UPSR の受け入れテスト」(p.5-29) を実行します。

終了：この手順は、これで完了です。

---

## NTP-A47 UPSR からの BLSR のサブテンディング

目的	この手順では、既存の UPSR から BLSR をサブテンドします。
工具 / 機器	UPSR ノードには、BLSR を伝送するための OC-N カードとファイバが必要です。
事前準備手順	<a href="#">NTP-A177 UPSR の受け入れテスト (p.5-29)</a>
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** BLSR をサブテンドする UPSR ノードに、BLSR トランク (スパン) カードとして機能する 2 つの OC-N カードを取り付けます ( [図 5-12](#) ではノード 3 のスロット 5 と 12 )。 [「NTP-A16 光カードおよびコネクタの取り付け」\(p.2-8\)](#) を参照してください。
- ステップ 2** [ステップ 1](#) のカードから他の BLSR ノードにある BLSR トランク カードまでをファイバで接続します。 [図 5-12](#) では、ノード 3 のスロット 5 とノード 2 のスロット 12 が、またノード 3 のスロット 12 とノード 1 のスロット 5 がそれぞれ接続されています。
- ステップ 3** BLSR をサブテンドする ONS 15454 (ステップ 1 のノード) にログインします。 [「DLP-A60 CTC へのログイン」\(p.17-71\)](#) を参照してください。すでにログインしている場合は、 [ステップ 4](#) へ進みます。
- ステップ 4** BLSR のトラフィックを伝送する両方の OC-N トランク カード (イーストとウェスト) で DCC を作成します。 [「DLP-A377 SDCC 終端のプロビジョニング」\(p.20-74\)](#) を参照してください。CTC の管理に必要な帯域幅が不足している場合は、 [「DLP-A378 LDCC 終端のプロビジョニング」\(p.20-77\)](#) を行って追加します。
- ステップ 5** サブテンディング BLSR を作成します。
- BLSR に組み込む各ノードについて、 [「NTP-A40 BLSR ノードのプロビジョニング」\(p.5-14\)](#) を実行します。BLSR がすでに設定されている場合は、サブテンディング ノードに対してだけこの手順を実行します。
  - [「NTP-A126 BLSR の作成」\(p.5-16\)](#) を実行します。 [ステップ 3](#) のノード (BLSR をサブテンドするノード) を BLSR に追加します。
- ステップ 6** View メニューから **Go to the Network View** を選択して、サブテンディングリングを表示します。

終了 : この手順は、これで完了です。

---

## NTP-A48 BLSR からの BLSR のサブテンディング

目的	この手順では、既存の BLSR から BLSR をサブテンドします。
工具 / 機器	BLSR ノードには、もう 1 つの BLSR を伝送するための OC-N カードとファイバが必要です。
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
セキュリティ レベル	プロビジョニング以上のレベル

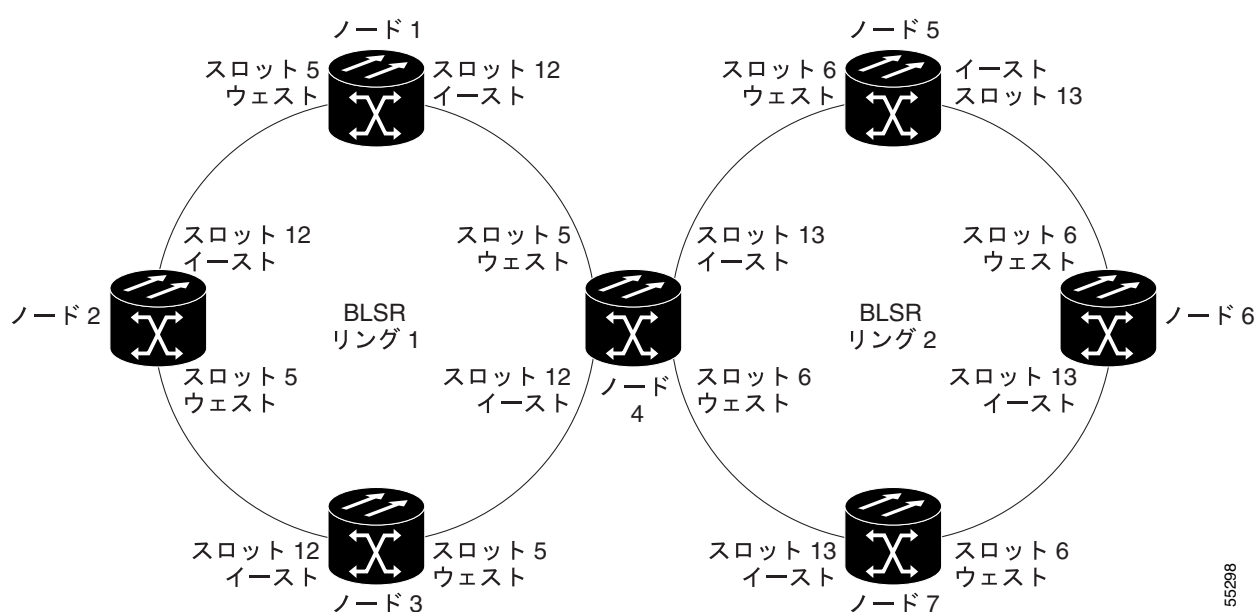


(注) この手順は、すべてのノードを BLSR 用に設定することを前提としています。BLSR にノードを追加する必要がある場合は、「[NTP-A212 BLSR ノードの追加](#)」(p.14-2) を参照してください。

- ステップ 1** BLSR をサブテンドするノードで ( [図 5-13](#) のノード 4 ) 「[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** BLSR トランク (スパン) カードとして機能する OC-N カードを取り付けていない場合は、これらのカードを取り付けます。「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を参照してください。

[図 5-13](#) に、ONS 15454 で共有される 2 つの BLSR を示します。リング 1 には、ノード 1、2、3、および 4 が含まれています。リング 2 には、ノード 4、5、6、および 7 が含まれています。リング 2 は、この手順で追加するサブテンディングリングです。ノード 4 には、2 つの BLSR リング (リング 1 とリング 2) が設定されています。リング 1 では、スロット 5 とスロット 12 のカードを使用し、リング 2 では、スロット 6 と 13 のカードを使用しています。

図 5-13 BLSR からの BLSR のサブテンディング



55298

- ステップ3** サブテンディング ノードのトランク カードから 2 つの近接 BLSR ノードの BLSR トランク カードまでをファイバで接続します。図 5-13 では、ノード 4 のスロット 6 とノード 7 のスロット 13 が、またノード 4 のスロット 13 とノード 5 のスロット 6 がそれぞれ接続されています。「DLP-A44 BLSR 構成での光ファイバケーブルの取り付け」(p.17-55) を参照してください。
- ステップ4** BLSR のトラフィックを伝送する最初の OC-N カードで DCC を作成します。「DLP-A377 SDCC 終端のプロビジョニング」(p.20-74) を参照してください。CTC の管理に必要な帯域幅が不足している場合は、「DLP-A378 LDCC 終端のプロビジョニング」(p.20-77) を行って追加します。
- ステップ5** BLSR のトラフィックを伝送する 2 番めの OC-N トランク カードについて、ステップ 4 を繰り返します。
- ステップ6** BLSR に組み込む各ノードについて、「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行します。BLSR がすでに設定されている場合は、サブテンディング ノードに対してだけこの手順を実行します。
- ステップ7** サブテンディング BLSR が作成されていない場合は、「NTP-A126 BLSR の作成」(p.5-16) を実行して、新しい BLSR をプロビジョニングします。サブテンディング BLSR のリング名には、最初の BLSR のリング名と異なる名前を指定する必要があります。



- (注) サブテンディング ノードには、両方の BLSR に使用する 1 つのノード ID を指定することも、BLSR ごとに個別のノード ID を指定することもできます。たとえば、同じノードを BLSR 1 ではノード 4 として、BLSR 2 ではノード 2 として設定できます。

- ステップ8** View メニューから Go to Network View を選択して、サブテンディング リングを表示します。

図 5-14 に 2 つのサブテンディング BLSR の例を示します。

図 5-14 ネットワーク マップに表示されたサブテンディング BLSR



終了：この手順は、これで完了です。

## NTP-A172 論理ネットワーク マップの作成

目的	この手順では、ネットワーク ビュー内にノードを配置します。スーパーユーザはこの手順を使用して、ネットワーク上のすべてのノードに対して一貫したネットワーク ビューを作成できるようにします。
工具	なし
事前準備手順	この手順は、ネットワークの起動が完了していることを前提としています。
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	スーパーユーザ

**ステップ 1** ネットワーク マップを作成するネットワーク上の ONS 15454 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** View メニューから、**Go to Network View** を選択します。

**ステップ 3** サイト計画に基づいて、ネットワーク ビューに表示されているノードの位置を変更します。

- a. ノードをクリックして選択し、Ctrl キーを押しながら、そのノードアイコンを新しい場所にドラッグアンドドロップします。
- b. ネットワーク マップ領域のブランク部分をクリックして、選択されたノードの選択を解除します。
- c. 配置の必要がある各ノードについて、**ステップ a**を繰り返します。

**ステップ 4** ネットワーク ビューのマップを右クリックして、**Save Node Position** を選択します。

**ステップ 5** Save Node Position ダイアログボックスで **Yes** をクリックします。

CTC に進行バーが表示され、新しいノードの場所が保存されます。



**(注)** ネットワーク マップでノードを移動することは検索、プロビジョニング、メンテナンスユーザでもできますが、ネットワーク マップの設定を保存できるのは、スーパーユーザだけです。以前に保存したバージョンのネットワーク マップ ビューを復元するには、そのネットワーク ビュー マップを右クリックし、**Reset Node Position** を選択します。

**終了** : この手順は、これで完了です。





## 回線と VT トンネルの作成

この章では、Cisco ONS 15454 の電気回線、トンネル、光回線、イーサネット回線、および Virtual Concatenated (VCAT; 仮想連結) 回線について、その作成方法を説明します。ONS 15454 回線の詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

### 準備作業

次の手順を実行する前に、すべてのアラームを調べて、問題をすべて解決しておいてください。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A127 ネットワークの起動の確認 \(p.6-5\)](#)— この手順は、回線を作成する前に行います。
2. [NTP-A181 自動ルーティングによる DS-1 回線の作成 \(p.6-8\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A182 手動ルーティングによる DS-1 回線の作成 \(p.6-13\)](#)— 必要に応じて、この手順を実行します。
4. [NTP-A183 ドロップが複数ある単方向 DS-1 回線の作成 \(p.6-17\)](#)— 必要に応じて、この手順を実行します。
5. [NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成 \(p.6-22\)](#)— 必要に応じて、この手順を実行します。
6. [NTP-A185 手動ルーティングによる DS-3 または EC-1 回線の作成 \(p.6-28\)](#)— 必要に応じて、この手順を実行します。
7. [NTP-A186 ドロップが複数ある単方向 DS-3 または EC-1 回線の作成 \(p.6-31\)](#)— 必要に応じて、この手順を実行します。
8. [NTP-A133 自動ルーティングによる VT トンネルの作成 \(p.6-35\)](#)— 必要に応じて、この手順を実行します。
9. [NTP-A134 手動ルーティングによる VT トンネルの作成 \(p.6-38\)](#)— 必要に応じて、この手順を実行します。
10. [NTP-A187 VAP の作成 \(p.6-40\)](#)— 必要に応じて、この手順を実行します。
11. [NTP-A135 電気回線のテスト \(p.6-44\)](#)— 電気回線を作成したあとに、この手順を実行します。
12. [NTP-A343 自動ルーティングによる光回線の作成 \(p.6-47\)](#)— 必要に応じて、この手順を実行します。

13. NTP-A344 手動ルーティングによる光回線の作成 (p.6-54) — 必要に応じて、この手順を実行します。
14. NTP-A314 ドロップが複数ある単方向光回線の作成 (p.6-58) — 必要に応じて、この手順を実行します。
15. NTP-A62 光回線のテスト (p.6-63) — 光回線を作成したあとに、この手順を実行します。
16. NTP-A139 BLSR または 1+1 ノードでの半回線の作成 (p.6-65) — Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) または 1+1 トポロジーの宛先として OC-N カードまたは G シリーズ カードを使用して半回線を作成する場合に、必要に応じてこの手順を実行します。
17. NTP-A140 UPSR ノードでの半回線の作成 (p.6-67) — Unidirectional Path Switched Ring (UPSR; 単方向パススイッチ型リング) の宛先として OC-N カードまたは G シリーズ カードを使用して半回線を作成する場合に、必要に応じてこの手順を実行します。
18. NTP-A191 E シリーズ EtherSwitch 回線の作成 (マルチカードまたはシングルカード モード) (p.6-69) — 必要に応じて、この手順を実行します。
19. NTP-A192 ポートマップモードの E シリーズ カード用回線の作成 (p.6-73) — 必要に応じて、この手順を実行します。
20. NTP-A142 E シリーズ共有パケットリングイーサネット回線の作成 (p.6-76) — 必要に応じて、この手順を実行します。
21. NTP-A143 E シリーズ カードのハブアンドスポークイーサネット構成の作成 (p.6-79) — 必要に応じて、この手順を実行します。
22. NTP-A144 手動による E シリーズ シングルカード EtherSwitch クロスコネクットの作成 (p.6-82) — 必要に応じて、この手順を実行します。
23. NTP-A145 手動による E シリーズ マルチカード EtherSwitch クロスコネクットの作成 (p.6-85) — 必要に応じて、この手順を実行します。
24. NTP-A146 E シリーズ回線のテスト (p.6-89) — E シリーズ SONET 回線を作成したあとに、この手順を実行します。
25. NTP-A148 手動によるポートマップモードの G シリーズまたは E シリーズ カード用クロスコネクットの作成 (p.6-91) — 必要に応じて、この手順を実行します。
26. NTP-A241 G シリーズ ポートをトランスポンダモードにするプロビジョニング (p.6-93) — 必要に応じて、この手順を実行します。
27. NTP-A149 G シリーズ回線のテスト (p.6-97) — G シリーズ SONET 回線を作成したあとに、この手順を実行します。
28. NTP-A264 自動ルーティングによる VCAT 回線の作成 (p.6-99) — 必要に応じて、この手順を実行します。
29. NTP-A265 手動ルーティングによる VCAT 回線の作成 (p.6-104) — 必要に応じて、この手順を実行します。
30. NTP-A194 オーバーヘッド回線の作成 (p.6-107) — Data Communication Channel (DCC; データ通信チャンネル) トンネルの作成、IP カプセル化トンネルの作成、オーダーワイヤのプロビジョニング、または User Data Channel (UDC) 回線の作成を行う場合に、必要に応じて、この手順を実行します。
31. NTP-A167 リングを対象にした STS テスト回線の作成 (p.6-108) — 必要に応じて、この手順を実行します。
32. NTP-A326 サーバ証跡の作成 (p.6-111) — 必要に応じて、この手順を実行します。

表 6-1 に、ONS 15454 回線を作成するための条件とオプションを示します。

表 6-1 ONS 15454 回線オプション

回線オプション	内容
送信元	回線の送信元は、回線が ONS 15454 ネットワークに入る場所です。
宛先	回線の宛先は、回線が ONS 15454 ネットワークを出る場所です。
回線の自動ルーティング	Cisco Transport Controller (CTC) は、ルーティングパラメータと帯域幅の Availability に基づいて、使用可能な最も短いパスに回線を自動的にルーティングします。
回線の手動ルーティング	手動ルーティングを使用すると、自動ルーティングによって選択される最も短いパス以外に、特定のパスを選択できます。Telcordia Trunk Information Record Keeping System (TIRKS) のような Operations Support System (OSS; オペレーションサポートシステム) に用意されている作業指示に従い、回線セグメントごとに特定の Synchronous Transport Signal (STS; 同期転送信号) または Virtual Tributary (VT) を選択して、回線を作成することができます。
VT トンネル	VT トンネルを使用すれば、クロスコネクタカード (XC、XCVT、XC10G、XC-VXC-10G) リソースを利用しなくても、ONS 15454 に VT1.5 回線をパススルーさせることができます。VT トンネルを使用する VT 回線は、送信元ノードと宛先ノードでだけクロスコネクタの伝送容量を使用します。1 つの VT トンネルは VT1.5 回線 28 本または VT2 回線 21 本のトラフィックを伝送できます。
VAP	VT Aggregation Point (VAP) を使用すると、VT 回線を 1 つの STS に集約して、Interoffice Facility (IOF) スイッチ、Digital Access Cross-Connect System (DACCS) など、ONS 15454 以外のネットワークや機器につなぐことができます。VAP により、VT が STS に集約されるノードでの VT マトリクスリソースの利用率が低下します。このノードは STS グルーミング エンドといいます。STS グルーミング エンドには、EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N カードが必要です。VAP は、BLSR、1+1、または非保護ノードで作成できますが、UPSR ノードでは作成できません。

ONS 15454 回線には、VT 回線と STS 回線があります。表 6-2 に、VT 回線の送信元および宛先のオプションを示します。

表 6-2 VT 回線に対する CTC 回線の送信元と宛先に関するオプション

カード	ポート	STS	VT	DS-1
DS1-14、DS1N-14	—	—	—	14
DS3XM-6	6	—	—	ポートごとに 28
DS3XM-12	12	—	—	ポートごとに 28
DS3/EC1-48	48	—	—	ポートごとに 28
EC1-12	12	—	ポートごとに VT1.5 が 28、VT2 が 21	—
DS1/E1-56	56	—	—	56
OC3 IR 4/STM1 SH 1310	4	ポートごとに 3	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—
OC3 IR/STM1 SH 1310-8	8	ポートごとに 3	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—

表 6-2 VT 回線に対する CTC 回線の送信元と宛先に関するオプション (続き)

カード	ポート	STS	VT	DS-1
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—
OC12 IR/STM4 SH 1310-4	4	ポートごとに 12	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—
すべての OC-48 カード (ML シリーズカードを含まない)	—	48	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—
すべての OC-192 カード	—	192	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—
FC_MR-4	4	—	—	—
MRC-12	12	ポートごとに 3、 12、または 48 <sup>1</sup>	STS ごとに VT1.5 が 28、ポートごとに VT2 が 21	—

1. ポートで使用されている SFP、および使用可能なバックプレーンの幅やプロビジョニングされた既存回線によって決まります。詳細については、『Cisco ONS 15454 Reference Manual』の「Optical Cards」の章を参照してください。

表 6-3 に、STS 回線の送信元および宛先のオプションを示します。

表 6-3 STS 回線に対する CTC 回線の送信元と宛先に関するオプション

カード	ポート	STS
DS1-14、DS1N-14 <sup>1</sup>	—	—
DS3-12、DS3N-12、DS3-12E、DS3N-12E	12	—
DS3XM-6	6	—
DS3XM-12	12、または 6 ~ 12 の「ポート レス」 <sup>2</sup>	—
DS3i-N-12	12	ポートごとに 1
DS3/EC1-48	48	ポートごとに 1
EC1-12	12	—
DS1/E1-56	56	—
OC3 IR 4/STM1	4	ポートごとに 3
OC3-8	8	ポートごとに 3
OC12 IR/STM4 SH 1310 OC12 LR/STM4 LH 1310 OC12 LR/STM4 LH 1550	—	12
OC12 IR/STM4 SH 1310-4	4	ポートごとに 12
すべての OC-48 カード (ML シリーズ カードを含む)	—	48
すべての OC-192 カード	—	192

表 6-3 STS 回線に対する CTC 回線の送信元と宛先に関するオプション (続き)

カード	ポート	STS
FC_MC-4	4	—
MRC-12	12	ポートごとに 3、12、または 48 <sup>3</sup>

- 1つの DS1 カードで STS 回線を 1 つルーティングし、この STS 内で 14 個のポートのトラフィックをすべて伝送することができます。ただし、14 個の VT1.5 は利用されません。
- 「ポートレス」インターフェイスの数は、システム構成によって決まります。XCVT ドロップ スロットでは、最大 6 つのポートレス トランスマックス インターフェイスがサポートされます。XCVT トランク スロット、XC10G と XC-VXC-10G Any Slot では、最大 12 個のポートレス トランスマックス インターフェイスがサポートされます。
- ポートで使用されている SFP、および使用可能なバックプレーンの幅やプロビジョニングされた既存回線によって決まります。詳細については、『Cisco ONS 15454 Reference Manual』の「Optical Cards」の章を参照してください。

## NTP-A127 ネットワークの起動の確認

目的	この手順では、ONS 15454 ネットワークで回線をプロビジョニングするための準備ができていることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">第 5 章「ネットワークの起動」</a>
必須 / 適宜	必須
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-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** View メニューから、[Go to Network View](#) を選択します。ネットワークに属しているノードがネットワーク マップにすべて表示されるのを待ちます (大規模なネットワークでは、すべてのノードが表示されるまでに数分かかることがあります)。



**(注)** コンピュータをこの ONS 15454 ネットワークに初めて接続したときは、ノードアイコンが図領域の左側に重なっていて、見えないことがあります。その場合は、ネットワーク マップの下にあるスクロールバーを使用して、アイコンが見える位置までスクロールしてください。また、Ctrl キーを押しながらアイコンを新しい場所にドラッグアンドドロップして、アイコンが 1 つ 1 つ見えるように移動してください。すべてのノードが図領域に表示されるまで繰り返します。

**ステップ 3** ノードにアクセスできることを確認します。ネットワーク ビューで、すべてのノードアイコンがグリーン、イエロー、オレンジ、またはレッドになっている必要があります。

数分経過してもすべてのネットワークアイコンが表示されないか、ノードアイコンがグレーのままに [Unknown] が表示される場合は、中止してください。ウィンドウの右下隅にある Net ボックスを確認してください。Net ボックスがグレーになっている場合は、再度ログインして、CTC Login ダイアログボックスの Disable Network チェックボックスがオフになっていることを確認します。問題が解消されない場合は、[第 5 章「ネットワークの起動」](#)を参照して、ネットワークの起動手順がネットワークのトポロジーに合っているかどうかを確認するか、『Cisco ONS 15454 Troubleshooting Guide』のトラブルシューティング手順を参照してください。

- ステップ 4** DCC の接続を確認します。すべてのノードが緑色の線で接続されている必要があります。回線が存在しないかグレーになっている場合は、中止してください。第5章「ネットワークの起動」を参照して、ネットワークトポロジーに合ったネットワーク起動手順を実行してください。続行する前に、すべてのノードがDCCで接続できるようになっていることを確認します。
- ステップ 5** Alarms タブをクリックして、アラームの説明を表示します。必要に応じて、すべての Critical アラーム（レッドのノードアイコン）または Major アラーム（オレンジのノードアイコン）を調べて解決します。続行する前に『Cisco ONS 15454 Troubleshooting Guide』を参照して、アラームを解決してください。
- ステップ 6** View メニューから、Go to Home View を選択します。ノードがサイト計画またはエンジニアリング計画に従ってプロビジョニングされていることを確認します。
- シェルフ マップにあるカードを表示します。指定のスロットに ONS 15454 カードが表示されていることを確認します。
  - Provisioning > General タブをクリックします。ノード名、連絡先、日付、時刻、および Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) サーバの IP アドレス（使用する場合）が正しくプロビジョニングされていることを確認します。必要に応じて、「NTP-A25 名前、日付、時刻、連絡先情報の設定」(p.4-6) を行って訂正します。
  - Network タブをクリックします。IP アドレス、サブネットマスク、デフォルト ルータ、Prevent LCD IP Config、およびゲートウェイの設定が正しくプロビジョニングされていることを確認します。正しくプロビジョニングされていない場合は、「NTP-A169 CTC ネットワーク アクセスの設定」(p.4-9) を実行して訂正します。
  - Protection タブをクリックします。保護グループがサイト計画に従って作成されていることを確認します。保護グループが作成されていない場合は、「NTP-A324 保護グループの作成」(p.4-12) を実行します。
  - BLSR のノードで、BLSR タブをクリックします（BLSR にノードがない場合は、ステップ f に進みます）。次の項目がサイト計画に従ってプロビジョニングされていることを確認します。
    - BLSR のタイプ（2 ファイバまたは 4 ファイバ）
    - BLSR のリング ID とノード ID
    - リング復元時間
    - イーストカードとウェストカードの割り当て
    - 4 ファイバ BLSR：スパンの復元とイースト/ウェスト保護カードの割り当て
 訂正が必要な場合は、「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を参照してください。
  - Security タブをクリックします。ユーザとアクセス レベルが指定どおりにプロビジョニングされていることを確認します。指定どおりにプロビジョニングされていない場合は、「NTP-A30 ユーザの作成とセキュリティの割り当て」(p.4-5) を参照して、その情報を訂正します。
  - SNMP（簡易ネットワーク管理プロトコル）を使用している場合は、SNMP タブをクリックして、トラップと宛先の情報を確認します。情報が間違っている場合は、「NTP-A87 SNMP の設定変更」(p.11-10) を参照して、その情報を訂正します。
  - Comm Channels タブをクリックします。該当する OC-N スロットとポート（Time Division Multiplexing [TDM; 時分割多重] ノード）および Optical Service Channel (OSC) スロットとポート（Dense Wavelength Division Multiplexing [DWDM; 高密度波長分割多重] ノード）に DCC が作成されていることを確認します。該当する OC-N または OSC スロットおよびポートに DCC が作成されていない場合は、第5章「ネットワークの起動」を参照して、ネットワークトポロジーに合った起動手順を実行します。OSC ポートのプロビジョニングについては、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。

- i. **Timing** タブをクリックします。タイミングが指定どおりにプロビジョニングされていることを確認します。タイミングが指定どおりにプロビジョニングされていない場合は、「[NTP-A85 ノードのタイミング変更](#)」(p.11-8)を参照して変更します。
- j. **Alarm Profiles** タブをクリックします。オプションのアラーム プロファイルをプロビジョニングした場合は、アラーム プロファイルが指定どおりにプロビジョニングされていることを確認します。アラーム プロファイルが指定どおりにプロビジョニングされていない場合は、「[NTP-A71 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.8-8)を参照して、その情報を変更します。
- k. ノード ビューのウィンドウで、ステータス領域にリストされている Network Element( NE; ネットワーク要素)のデフォルト値が正しいことを確認します。

**ステップ7** ネットワーク内の各ノードについて、[ステップ6](#)を繰り返します。

**ステップ8** 「[準備作業](#)」(p.6-1)のNTPリストから、該当する回線作成手順を選んで実行します。

**終了**：この手順は、これで完了です。

---


## NTP-A181 自動ルーティングによる DS-1 回線の作成

目的	この手順では、ルーティング（ルートの設定）を自動的に行う DS-1 回線を作成します。つまり、CTC が、指定したパラメータとソフトウェアバージョンに基づいて、回線ルートを自動的に選択します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — VT または STS を選択します。VT のクロスコネクトによって、ONS 15454 ネットワーク上に DS-1 回線のトラフィックが伝送されます。
  - Number of Circuits — 作成する DS-1 回線数を入力します。デフォルトは 1 です。同じスロットでポート番号の連続する回線を複数作成する場合は、Auto-ranged を使用して回線を自動的に作成します。
  - Auto-ranged — このチェックボックスは、Number of Circuits フィールドに 1 より大きい値を入力すると、自動的にオンになります。オートレンジ機能をオンにすると、送信元と宛先の同じ回線が連続して自動的に作成されます。CTC に連続した回線を自動的に作成させない場合は、このチェックボックスをオフにします。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します (  6-1 )。
- Name — 回線に名前を付けます。名前には、48 文字（スペースを含む）以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — VT 回線の場合は、VT1.5 を選択します。STS 回線の場合は、STS-1 を選択します。
  - Bidirectional — この回線はオンのままにします（デフォルト）。



- Create cross-connects only( TL1-like )— 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- Diagnostic — オフのままにします。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を In-Service and Normal ( IS-NR ) にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を Out-of-Service and Management, Disabled ( OOS-MA,DSBLD ) にします。トラフィックは回線を通ってできません。
  - IS,AINS — 回線のクロスコネクトを Out-of-Service and Autonomous, Automatic In-Service ( OOS-AU,AINS ) サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクトのサービス状態を Out-of-Service and Management, Maintenance ( OOS-MA,MT ) にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」( p.19-22 ) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

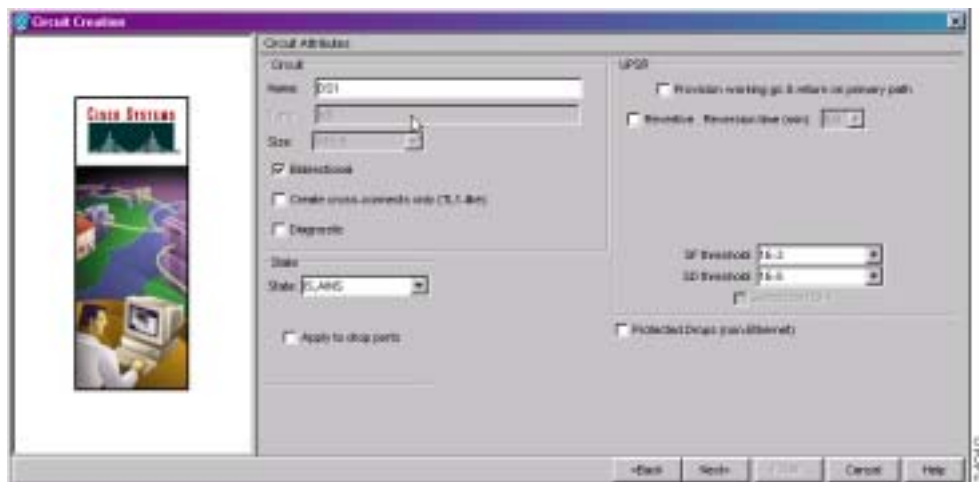
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、Loss of Signal( LOS; 信号損失 ) アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードとポートだけが表示されます。

図 6-1 DS-1 回線のアトリビュート設定



**ステップ 8** 回線を UPSR にルーティングする場合は、「DLP-A218 UPSR セレクタのプロビジョニング (p.19-14)」を行います。それ以外の場合は、次のステップへ進みます。

**ステップ 9** Next をクリックします。

**ステップ 10** 「DLP-A95 DS-1 回線の送信元と宛先のプロビジョニング」(p.17-104) を実行します。

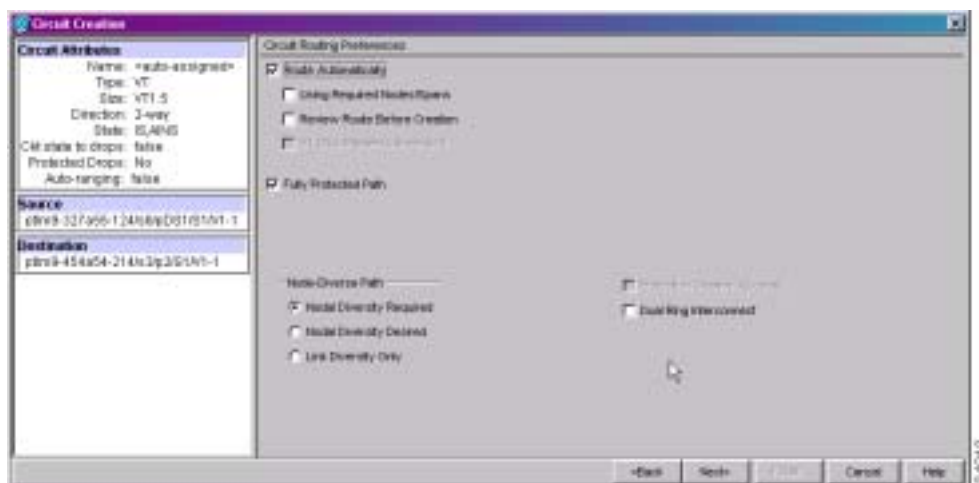
**ステップ 11** Circuit Routing Preferences 領域 (図 6-2) で、Route Automatically をオンにします。使用できるオプションは 2 つあります。設定に応じて、どちらか一方または両方を選択するか、またはどちらも選択しないようにします。

- Using Required Nodes/Spans — CTC の作成する回線ルートに、ノードとスパンを指定して追加または除外する場合は、このチェックボックスをオンにします。

含めるように指定したノードとスパンは、確実にその回線の現用パスに含まれます(保護パスには含まれません)。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。

- Review Route Before Creation — 回線を作成する前にその回線を確認して編集する場合は、このチェックボックスをオンにします。

図 6-2 DS-1 回線の回線ルーティングのプリファレンス設定



**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたまま **ステップ 13** へ進みます。CTC では、選択したパス ダイバーシティ オプションに基づいて、完全に保護された回線ルートを作成します。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして **ステップ 15** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで **Yes** をクリックして **ステップ 15** へ進みます。

**注意**

BLSR の保護チャンネルにルーティングした回線は保護されません。そのため、それらの回線は BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 13** **ステップ 12** で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パスがノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 14** **ステップ 12** で Fully Protected Path を選択して、回線を UPSR Dual-Ring Interconnect (DRI; デュアルリング相互接続)へルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

**ステップ 15** **ステップ 11** で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。それ以外の場合は、**ステップ 17** へ進みます。

- a. **Next** をクリックします。
- b. Circuit Route Constraints 領域の回線マップで、ノードまたはスパンをクリックします。
- c. 回線にそのノードまたはスパンを含める場合は、**Include** をクリックします。回線からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。含めるノードとスパンは、回線をルーティングする順序で選択します。回線の方向を変更する場合は、スパンを 2 回クリックします。
- d. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b と c を繰り返します。
- e. 回線のルートを確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストでノードを選択し、**Up** または **Down** ボタンをクリックして、回線のルーティング順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。

**ステップ 16** Next をクリックします。VT Matrix Optimization ページの Create 領域で、次のいずれかを選択します。

- Create VT tunnel on transit nodes — このオプションは、DS-1 回線が VT トンネルのないノードをパススルーするように設定する場合や、既存の VT トンネルが満杯の場合に使用します。VT トンネルを使用すれば、クロスコネクタカードのリソースを使用しなくても、ONS 15454 に VT 回線をパススルーさせることができます。VT トンネルは 28 本の VT1.5 回線のトラフィックを伝送できます。送信元と宛先の同じ VT 回線を数多く作成する場合は、特別なことがないかぎり、VT トンネルを作成することを推奨します。詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。
- Create VT aggregation point — このオプションは、DS-1 回線の送信元または宛先が、BLSR ノード、1+1 ノード、または保護されていないノードの EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N ポートである場合に使用できます。VAP は STS 上の DS-1 を集約して、IOF、スイッチ、DACS など、ONS 15454 以外のネットワークまたは機器へ接続します。また、クロスコネクタマトリクス上で VT 接続を複数使用しなくても、クロスコネクタカードの STS 接続を 1 つだけ使用して、VT1.5 回線をノードにルーティングすることができます。作成中の DS-1 回線を他の回線と一緒に STS へ集約して、ONS 15454 ネットワークから外部へ出て行くようにする場合は、次のいずれかを選択します。
  - STS grooming node is *source node*, VT grooming node is *destination node* — DS-1 回線の送信元ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の送信元が EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。
  - STS grooming node is *destination node*, VT grooming node is *source node* — DS-1 回線の宛先ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の宛先が EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。
- None — VT トンネルと VAP をどちらも作成しない場合に、このオプションを選択します。このオプションは、CTC が VT トンネルも VAP も作成できない場合にだけ使用できます。

**ステップ 17** [ステップ 11](#) で Review Route Before Creation を選択した場合は、次のサブステップを実行します。それ以外の場合は、[ステップ 18](#) へ進みます。

- a. Next をクリックします。
- b. 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include** をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- c. プロビジョニングした回線が予定のルートと設定を反映していない場合は **Back** をクリックし、回線の情報を確認して変更します。回線を別のパスにルーティングする必要がある場合は、『[NTP-A182 手動ルーティングによる DS-1 回線の作成](#)」(p.6-13) を参照してください。

**ステップ 18** Finish をクリックします。Circuit Creation ダイアログボックスの Number of Circuits フィールドで回線を複数入力した場合は、次のいずれかになります。

- Auto-ranged を選択した場合は、Number of Circuits フィールドに入力された数の回線が自動的に作成されます。送信元または宛先で連続ポートを使用できないなど、何らかの理由によってオートレンジで一部またはすべての回線を完成できない場合は、ダイアログボックスが表示されます。残りの回線に新しい送信元または宛先を設定し、**Finish** をクリックしてオートレンジを続行します。回線が完成すると、Circuits ウィンドウが表示されます。
- Auto-ranged を選択しなかった場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとに [ステップ 5 ~ 17](#) を繰り返します。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 19** Circuits ウィンドウで、回線リストに新しい回線が表示されていることを確認します。

**ステップ 20** 「NTP-A135 電気回線のテスト」(p.6-44) を実行します。テスト回線を作成した場合は、このステップを省略します。

終了：この手順は、これで完了です。

## NTP-A182 手動ルーティングによる DS-1 回線の作成

目的	この手順では、DS-1 回線を作成して、回線のルートを提供できるようにします。
工具 / 機器	なし
事前準備手順	NTP-A127 ネットワークの起動の確認 (p.6-5)
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** 回線を作成するノードで「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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「DLP-A314 ポートへの名前の割り当て」(p.20-9) を行います。それ以外の場合は、**ステップ 3** へ進みます。

**ステップ 3** View メニューから、Go to Network View を選択します。

**ステップ 4** Circuits タブをクリックして、Create をクリックします。

**ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — VT または STS を選択します。VT のクロスコネクタによって、ONS 15454 ネットワーク上に DS-1 回線のトラフィックが伝送されます。
- Number of Circuits — 作成する DS-1 回線数を入力します。デフォルトは 1 です。
- Auto-ranged — (自動ルーティング対象の回線にのみ適用) Circuit Creation ダイアログボックスの Number of Circuits フィールドに 1 より大きい値を入力した場合は、このチェックボックスをオフにします (このチェックボックスは、Number of Circuits フィールドに入力した回線の数 が 1 の場合は使用できません)。

**ステップ 6** Next をクリックします。

**ステップ 7** 回線のアトリビュートを定義します (図 6-1)。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — VT 回線の場合は、VT1.5 を選択します。STS 回線の場合は、STS-1 を選択します。
- Bidirectional — この回線はオンのままにします (デフォルト)。

- Create cross-connects only( TL1-like )— 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通できません。
  - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」( p.19-22 ) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードとポートだけが表示されます。

**ステップ 8** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング](#)」( p.19-14 ) を行います。それ以外の場合は、次のステップへ進みます。

**ステップ 9** Next をクリックします。

**ステップ 10** 「[DLP-A95 DS-1 回線の送信元と宛先のプロビジョニング](#)」( p.17-104 ) を実行します。

**ステップ 11** Circuit Routing Preferences 領域 (  6-2 ) で Route Automatically をオフにします。

**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、Fully Protected Path をオンにしたまま [ステップ 13](#) へ進みます。完全に保護されているパスには ( プライマリ パスと代替パスを持つ ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます ( 存在している場合 )。

- 保護されていない回線を作成する場合は、Fully Protected Path をオフにしてステップ 16 へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は Fully Protected Path をオフにし、Protection Channel Access をオンにしたあと、Warning ダイアログボックスで Yes をクリックしてステップ 16 へ進みます。

**注意**

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 13** ステップ 12 で Fully Protected Path を選択して回線を UPSR ヘルルーティングするようにした場合は、Node-Diverse Path オプションを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 14** ステップ 12 で Fully Protected Path を選択して回線を UPSR DRI ヘルルーティングするようにした場合は、Dual Ring Interconnect チェックボックスをオンにします。

**ステップ 15** Next をクリックします。VT Matrix Optimization ページの Create 領域で、次のいずれかを選択します。

- Create VT tunnel on transit nodes — このオプションは、DS-1 回線が VT トンネルのないノードをパススルーするように設定する場合や、既存の VT トンネルが満杯の場合に使用します。VT トンネルを使用すれば、クロスコネク トカードのリソースを使用しなくても、ONS 15454 に VT 回線をパススルーさせることができます。VT トンネルは 28 本の VT1.5 回線のトラフィックを伝送できます。送信元と宛先の同じ VT 回線を数多く作成する場合は、特別なことがないかぎり、VT トンネルを作成することを推奨します。詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。
- Create VT aggregation point — このオプションは、DS-1 回線の送信元または宛先が、BLSR ノード、1+1 ノード、または保護されていないノードの EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N ポートである場合に使用できます。VAP は STS 上の DS-1 を集約して、IOF、スイッチ、DACS など、ONS 15454 以外のネットワークまたは機器へ接続します。また、クロスコネク トマトリクス上で VT 接続を複数使用しなくても、クロスコネク トカードの STS 接続を 1 つだけ使用して、VT1.5 回線をノードにルーティングすることができます。作成中の DS-1 回線を他の回線と一緒に STS へ集約して、ONS 15454 ネットワークから外部へ出て行くようにする場合は、次のいずれかを選択します。
  - STS grooming node is source node, VT grooming node is destination node — DS-1 回線の送信元ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の送信元が EC1、DS3、DS3E、DS3i-N-12、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。
  - STS grooming node is destination node, VT grooming node is source node — DS-1 回線の宛先ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の宛先が EC1、DS3、DS3E、DS3i-N-12、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。
- None — VT トンネルと VAP をどちらも作成しない場合に、このオプションを選択します。このオプションは、CTC が VT トンネルも VAP も作成できない場合にだけ使用できます。

- ステップ 16** Next をクリックします。Route Review and Edit 領域に、回線を手動でルーティングできるようにノードアイコンが表示されます。回線の送信元ノードは選択されています。送信元ノードから他のネットワークノードまでを示す緑色の矢印は、回線のルーティングに使用できるスパンを表しています。
- ステップ 17** 作成する DS-1 回線について、「[DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング](#)」(p.17-106)を行います。
- ステップ 18** Finish をクリックします。CTC によって、手動でプロビジョニングした回線ルートと、[ステップ 13](#) で選択したパスダイバーシティオプションが比較されます。指定したパスダイバーシティ要件を当該パスが満たしていない場合は、CTC によってエラーメッセージが表示されるので、回線のパスを変更します。
- ステップ 19** Circuit Creation ダイアログボックスの Number of Circuits フィールドに 1 より大きい数値を入力した場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとに [ステップ 5 ~ 18](#) を繰り返します。
- ステップ 20** すべての回線を作成すると、Circuits ウィンドウが表示されます。作成した回線が正しいことを確認します。
- ステップ 21** 「[NTP-A135 電気回線のテスト](#)」(p.6-44)を実行します。テスト回線を作成した場合は、このステップを省略します。

終了：この手順は、これで完了です。

---



## NTP-A183 ドロップが複数ある単方向 DS-1 回線の作成

目的	この手順では、ドロップ（宛先）が複数ある単方向 DS-1 回線を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て \(p.20-9\)](#)」を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — VT または STS を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — Number of Circuits フィールドの値が 1 の場合は使用できません。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します ([図 6-3](#))。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — VT 回線の場合は、VT1.5 を選択します。STS 回線の場合は、STS-1 を選択します。
  - Bidirectional — この回線はオフにします。
  - Create cross-connects only (TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
  - Diagnostic — オフのままにします。
  - State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
    - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
    - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
    - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。

- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS、AINS、または OOS,DSBLD に変更します。「DLP-A230 回線のサービス状態の変更」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

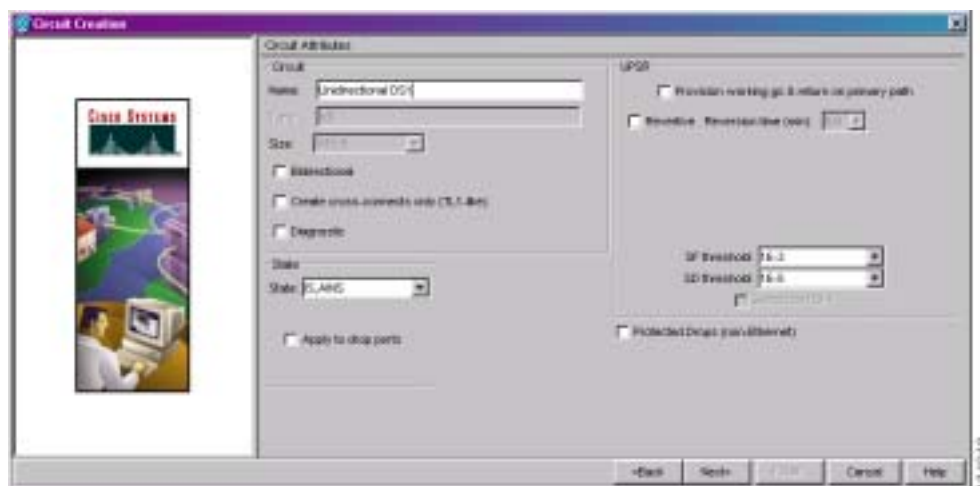
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

図 6-3 単方向 DS-1 回線のアトリビュート設定



**ステップ 8** Next をクリックします。

**ステップ 9** 「DLP-A95 DS-1 回線の送信元と宛先のプロビジョニング」(p.17-104) を実行します。

**ステップ 10** Circuit Routing Preferences 領域で、Route Automatically をオフにします。Route Automatically をオフにすると、Using Required Nodes/Spans チェックボックスと Review Route Before Circuit Creation チェックボックスは使用できません。

**ステップ 11** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、Fully Protected Path をオンにしたままで **ステップ 12** へ進みます。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、Fully Protected Path をオフにして **ステップ 16** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は Fully Protected Path をオフにし、Protection Channel Access をオンにしたあと、Warning ダイアログボックスで Yes をクリックして **ステップ 16** へ進みます。



**注意**

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 12** **ステップ 11** で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 13** **ステップ 11** で Fully Protected Path を選択して回線を UPSR DRI にルーティングするようにした場合は、Dual Ring Interconnect チェックボックスをクリックします。

**ステップ 14** Next をクリックします。VT Matrix Optimization ページの Create 領域で、次のいずれかを選択します。

- Create VT tunnel on transit nodes — このオプションは、DS-1 回線が VT トンネルのないノードをパススルーするように設定する場合や、既存の VT トンネルが満杯の場合に使用します。VT トンネルを使用すれば、クロスコネクタカードのリソースを使用しなくても、ONS 15454 に VT 回線をパススルーさせることができます。VT トンネルは 28 本の VT1.5 回線のトラフィックを伝送できます。送信元と宛先の同じ VT 回線を数多く作成する場合は、特別なことがないかぎり、VT トンネルを作成することを推奨します。詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。
- Create VT aggregation point — このオプションは、DS-1 回線の送信元または宛先が、BLSR ノード、1+1 ノード、または保護されていないノードの EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、DS3XM-12、または OC-N ポートである場合に使用できます。VAP は STS 上の DS-1 を集約して、IOF、スイッチ、DACS など、ONS 15454 以外のネットワークまたは機器へ接続します。また、クロスコネクタマトリクス上で VT 接続を複数使用しなくても、クロスコネクタカードの STS 接続を 1 つだけ使用して、VT1.5 回線をノードにルーティングすることができます。作成中の DS-1 回線を他の回線と一緒に STS へ集約して、ONS 15454 ネットワークから外部へ出て行くようにする場合は、次のいずれかを選択します。
  - STS grooming node is source node, VT grooming node is destination node — DS-1 回線の送信元ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の送信元が EC1、DS3、DS3E、DS3i-N-12、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。

- STS grooming node is *destination node*, VT grooming node is *source node* — DS-1 回線の宛先ノードに VAP を作成します。このオプションを使用できるのは、DS-1 回線の宛先が EC1、DS3、DS3E、DS3i-N-12、DS3XM-6、DS3XM-12、または OC-N カードである場合のみです。
- None — VT トンネルと VAP をどちらも作成しない場合に、このオプションを選択します。このオプションは、CTC が VT トンネルも VAP も作成できない場合にだけ使用できます。

**ステップ 15** Next をクリックします。Route Review and Edit 領域に、回線を手動でルーティングできるようにノードアイコンが表示されます。回線の送信元ノードは選択されています。送信元ノードから他のネットワークノードまでを示す緑色の矢印は、回線のルーティングに使用できるスパンを表しています。

**ステップ 16** 作成する DS-1 回線について、「[DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング](#)」(p.17-106)を行います。

**ステップ 17** Finish をクリックします。CTC が回線を完成すると、Circuits ウィンドウが表示されます。

**ステップ 18** Circuits ウィンドウで、複数のドロップにルーティングする回線をクリックします。Delete ボタン、Edit ボタン、Search ボタンが有効になります。

**ステップ 19** Edit をクリックします(または、回線の行をダブルクリックします)。選択した Edit Circuit ウィンドウの General タブが表示されます。

DCC ネットワークのすべてのノードがネットワークマップに表示されます。回線の送信元と宛先の情報が送信元ノードと宛先ノードの下に表示されます。回線の詳細を表示する場合は、**Show Detailed Map** をクリックします。ノードアイコンを再配置する場合は、ノードを選択して、Ctrl キーを押しながら、アイコンを新しい場所にドラッグアンドドロップします。

**ステップ 20** Edit Circuit ダイアログボックスで、**Drops** タブをクリックします。既存のドロップがリストで表示されます。

**ステップ 21** Create をクリックします。

**ステップ 22** Define New Drop ダイアログボックスで、新しいドロップを定義します。

- a. Node — 回線のドロップ対象ノードを選択します。
- b. Slot — ターゲットカードおよびスロットを選択します。
- c. Port、STS、VT、または DS1 — Port、STS、VT、または DS1 ドロップダウンリストからポート、STS、VT、または DS-1 を選択します。ステップ b で選択したカードによって、表示されるフィールドが決まります。オプションのリストは [表 6-2](#) を参照してください。
- d. 新しいドロップのルーティング設定は、元の回線の設定と同じです。ただし、次のオプションが使用できる場合は、設定を変更できます。
  - 保護された UPSR パスに元の回線がルーティングされていた場合は、Nodal Diversity Required、Nodal Diversity Desired、または Link Diversity Only のノードダイバーシティオプションを変更できます。オプションの説明については、[ステップ 12](#) を参照してください。
  - 保護されていないパスに元の回線がルーティングされていなかった場合は、PCA オプションを使用できます。[ステップ 11](#) の PCA オプションの説明を参照してください。
- e. 回線状態を変更する場合は、Target Circuit Admin State ドロップダウンリストから回線状態を選択します。選択された状態は、回線全体に適用されます。

- f. Target Circuit Admin State で選択した状態を回線の送信元ポートと宛先ドロップに適用する場合は、**Apply to drop ports** をオンにします。ドロップポートにサービス状態を適用するための要件については、『Cisco ONS 15454 Reference Manual』を参照してください。
- g. **Finish** をクリックします。新しいドロップが Drops リストに表示されます。

**ステップ 23** ドロップを作成して回線に追加する必要がある場合は、ステップ 21 と 22 を繰り返します。

**ステップ 24** **Close** をクリックします。Circuits ウィンドウが表示されます。

**ステップ 25** 編集した回線の Destination カラムに新しいドロップが表示されていることを確認します。表示されていない場合は、オプションがすべて正しく設定されていることを確認して、ステップ 5 ~ 24 を繰り返します。

**ステップ 26** 「NTP-A135 電気回線のテスト」(p.6-44) を実行します。テスト回線を作成した場合は、このステップを省略します。

**終了：**この手順は、これで完了です。

---

## NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成

目的	この手順では、自動ルーティングされる DS-3 または EC-1 回線を作成します。また、ポートレス トランスマックス インターフェイスのペアを通る回線の作成方法も示します。CTC は回線作成パラメータおよびソフトウェア バージョンに基づいて、回線を自動的に作成します。
工具 / 機器	ポートレス トランスマックス構成の場合は、回線が経由するノードに DS3XM-12 を取り付ける必要があります。  VT2 回線では、XC-VXC-10G カードと EC1 カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** View メニューから、**Go to Network View** を選択します。
- ステップ 4** Circuits タブをクリックして、**Create** をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — VT または STS を選択します。STS のクロスコネクトによって、ONS 15454 ネットワーク上に DS-3 または EC-1 回線のトラフィックが伝送されます。
  - Number of Circuits — 作成する DS-3 または EC-1 の回線数を入力します。デフォルトは 1 です。送信元と宛先ポートが連続する複数の回線を作成する場合は、Auto-ranged を使用して、回線を自動的に作成できます。
  - Auto-ranged — このチェックボックスは、Number of Circuits フィールドに 1 より大きい値を入力すると、自動的にオンになります。送信元と宛先が同じ複数の DS-3 または EC-1 回線を作成する場合に CTC を使用して回線を自動的に作成するときは、このチェックボックスをオンのままにします。CTC に連続した回線を自動的に作成させない場合は、このチェックボックスをオフにします。
- ステップ 6** **Next** をクリックします。

### ステップ7 回線のアトリビュートを定義します (図 6-4)。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — DS3i-N-12 カードの回線の場合は、STS-3c を選択します。このようにすると、任意の時刻に、3 つのポートを使用してポート 1、4、7、および 10 のポート グループが設定されます。EC1 カードの VT2 回線の場合は、VT2 を選択します。他のすべての回線の場合は、STS-1 を選択します。
- Bidirectional — この回線はオンのままにします (デフォルト)。
- Create cross-connects only (TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
  - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

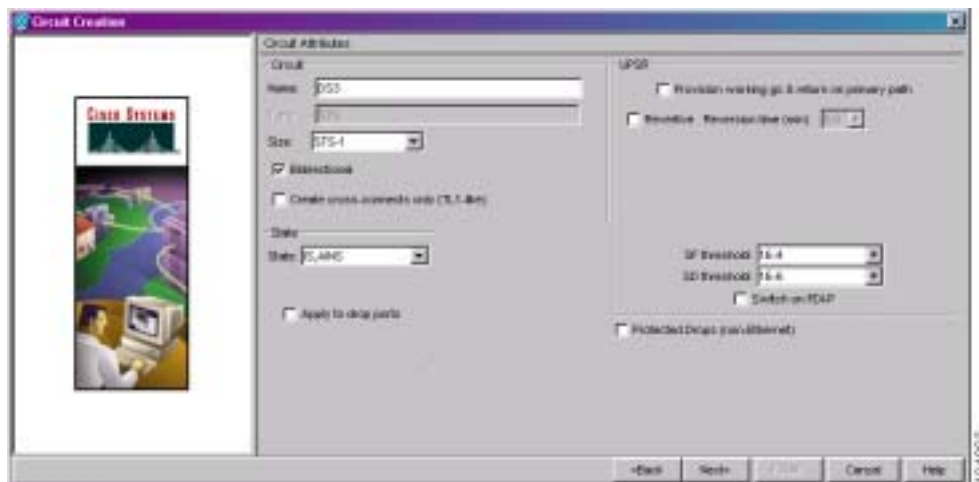
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードとポートだけが表示されます。

図 6-4 DS-3 または EC-1 回線のアトリビュート設定



**ステップ 8** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング](#) (p.19-14) を行います。

**ステップ 9** Next をクリックします。

**ステップ 10** 「[DLP-A510 DS-3 回線の送信元と宛先のプロビジョニング](#)」(p.22-4) を実行します。

**ステップ 11** Circuit Routing Preferences 領域 ( [図 6-5](#) ) で、**Route Automatically** をオンにします。使用できるオプションは 3 つあります。設定に応じて選択してください。

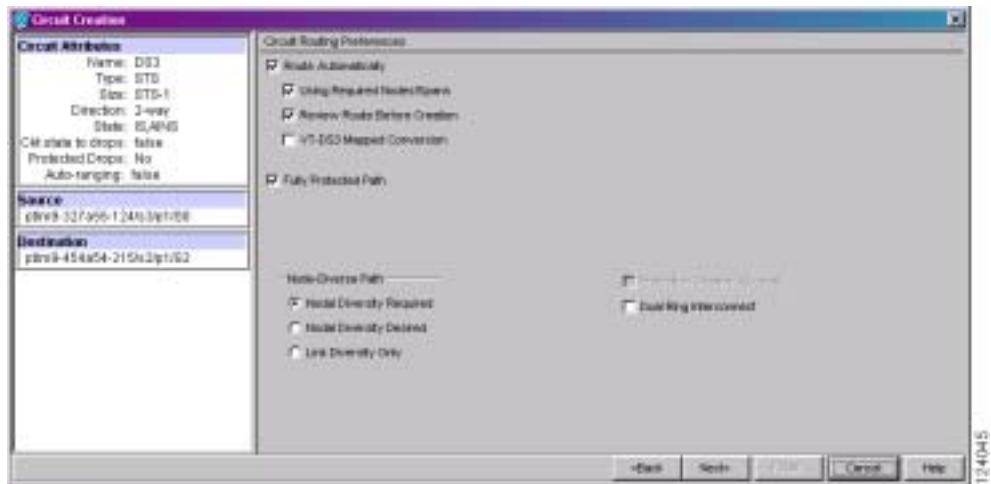
- Using Required Nodes/Spans — CTC の作成する回線ルートに、ノードとスパンを指定して含める、または除外する場合は、このチェックボックスをオンにします。

含めるように指定したノードとスパンは、確実にその回線の現用パスに含まれます ( 保護パスには含まれません )。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。

- Review Route Before Creation — 回線を作成する前にその回線を確認して編集する場合は、このチェックボックスをオンにします。
- VT-DS3 Mapped Conversion — DS3XM-12 カードのポートレス トランスマックス インターフェイスを使用して回線を作成する場合は、このチェックボックスをオンにします。



図 6-5 DS-3 または EC-1 回線の回線ルーティング プリファレンス設定



**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたままで **ステップ 13** へ進みます。CTC では、選択したパス ダイバーシティ オプションに基づいて、完全に保護された回線ルートを作成します。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして **ステップ 15** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで **Yes** をクリックして **ステップ 15** へ進みます。



#### 注意

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 13** **ステップ 12** で **Fully Protected Path** を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required** — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired** — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバースパスが作成されます。
- Link Diversity Only** — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 14** **ステップ 12** で **Fully Protected Path** を選択して回線を UPSR DRI へルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

**ステップ 15** **ステップ 11** で VT-DS3 Mapped Conversion を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 16** へ進みます。

- a. **Next** をクリックします。
- b. Conversion Circuit Route Constraints 領域で、次の項目を指定します。
  - Node — DS3XM-12 カードが取り付けられているノードを選択します。
  - Slot — DS3XM-12 カードが取り付けられているスロットを選択します。
  - DS3 Mapped STS — 該当する場合に **Circuit Dest** を選択して、STS が回線の宛先であることを示すか、**Circuit Source** を選択して、STS が回線の送信元であることを示します。

**ステップ 16** **ステップ 11** で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 17** に進みます。

- a. **Next** をクリックします。
- b. Circuit Route Constraints 領域の回線マップで、ノードまたはスパンをクリックします。
- c. 回線にそのノードまたはスパンを含める場合は、**Include** をクリックします。回線からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。含めるノードとスパンを選択した順序によって、回線の順序が決まります。回線の方向を変更する場合は、スパンを 2 回クリックします。
- d. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b と c を繰り返します。
- e. 回線のルートを確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Notes Links リストでノードを選択し、**Up** ボタンまたは **Down** ボタンをクリックします。ノードまたはスパンを削除する場合は、**Remove** をクリックします。



**(注)** ノードまたはスパンがグレーのままの場合、このノードまたはスパンは必須です。

**ステップ 17** **ステップ 11** で Review Route Before Creation を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 18** へ進みます。

- a. **Next** をクリックします。
- b. 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include** をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- c. プロビジョニングした回線が予定のルートと設定を反映していない場合は **Back** をクリックし、回線の情報を確認して変更します。回線を別のバスにルーティングする必要がある場合は、「[NTP-A185 手動ルーティングによる DS-3 または EC-1 回線の作成](#)」(p.6-28) を参照してください。

**ステップ 18** **Finish** をクリックします。Circuit Creation ダイアログボックスの Number of Circuits フィールドで回線を複数入力した場合は、次のいずれかになります。

- Auto-ranged を選択した場合は、Number of Circuits フィールドに入力された数の回線が自動的に作成されます。送信元または宛先で連続ポートを使用できないなど、何らかの理由によってオートレンジで一部またはすべての回線を完成できない場合は、ダイアログボックスが表示されます。残りの回線に新しい送信元または宛先を設定し、**Finish** をクリックしてオートレンジを続行します。回線が完成すると、Circuits ウィンドウが表示されます。

- Auto-ranged を選択しなかった場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 5 ~ 17 を繰り返します。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 19** Circuits ウィンドウで、回線リストに作成した回線が表示されていることを確認します。


**ステップ 20** 「[NTP-A135 電気回線のテスト](#)」(p.6-44) を実行します。テスト回線を作成した場合は、このステップを省略します。

**終了：**この手順は、これで完了です。

---

## NTP-A185 手動ルーティングによる DS-3 または EC-1 回線の作成

目的	この手順では、DS-3 または EC-1 回線を作成して、回線のルートをプロビジョニングできるようにします。
工具 / 機器	VT2 回線では、XC-VXC-10G カードと EC1 カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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 3](#)へ進みます。
- ステップ 2** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 4](#)へ進みます。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — STS を選択します。STS のクロスコネクトによって、ONS 15454 ネットワーク上に DS-3 または EC-1 回線のトラフィックが伝送されます。
  - Number of Circuits — 作成する DS-3 または EC-1 の回線数を入力します。デフォルトは 1 です。
  - Auto-ranged — (自動ルーティング対象の回線にのみ適用) Number of Circuits フィールドに 1 より大きい値を入力した場合は、このチェックボックスをオフにします (このチェックボックスは、Number of Circuits フィールドに入力した回線の数 が 1 の場合は使用できません)。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します (  )。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — DS3i-N-12 カードの回線の場合は、STS-3c を選択します。このようにすると、任意の時刻に、3 つのポートを使用してポート 1、4、7、および 10 のポートグループが設定されます。EC1 カードの VT2 回線の場合は、VT2 を選択します。他のすべての回線の場合は、STS-1 を選択します。
  - Bidirectional — このフィールドはオンのままにします (デフォルト)。
  - Create cross-connects only( TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
  - State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
    - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
    - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。

- IS,AINS — 回線のクロスコネクタを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
- OOS,MT — 回線のクロスコネクタのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS, IS,AINS、または OOS,DSBLD に変更します。「DLP-A230 回線のサービス状態の変更」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

**ステップ 8** 回線を UPSR にルーティングする場合は、「DLP-A218 UPSR セレクタのプロビジョニング」(p.19-14) を行います。

**ステップ 9** Next をクリックします。

**ステップ 10** 「DLP-A510 DS-3 回線の送信元と宛先のプロビジョニング」(p.22-4) を実行します。

**ステップ 11** Circuit Routing Preferences 領域(図 6-5)で **Route Automatically** をオフにします。Route Automatically をオフにすると、Using Required Nodes/Spans チェックボックス、Review Route Before Circuit Creation チェックボックス、および VT-DS3 Mapped Conversion チェックボックスは使用できません。

**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたままで **ステップ 13** へ進みます。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして **ステップ 15** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで Yes をクリックして **ステップ 15** へ進みます。

**注意**

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 13** [ステップ 12](#) で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 14** [ステップ 12](#) で Fully Protected Path を選択して回線を UPSR DRI ヘルルーティングするようにした場合は、Dual Ring Interconnect チェックボックスをオンにします。

**ステップ 15** Next をクリックします。Route Review and Edit 領域に、回線を手動でルーティングできるようにノード アイコンが表示されます。選択されたノードから他のネットワークノードまでを示すグリーンの矢印は、回線のルーティングに使用できるスパンを表しています。

**ステップ 16** 作成する DS-3 または EC-1 回線について、「[DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング](#)」(p.17-106)を行います。

**ステップ 17** Finish をクリックします。

**ステップ 18** Circuit Creation ダイアログボックスの Number of Circuits フィールドに 1 より大きい数値を入力した場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとに [ステップ 5 ~ 17](#) を繰り返します。

**ステップ 19** すべての回線を作成すると、Circuits ウィンドウが表示されます。ウィンドウに作成した回線が表示されていることを確認します。

**ステップ 20** 「[NTP-A135 電気回線のテスト](#)」(p.6-44)を実行します。テスト回線を作成した場合は、このステップを省略します。

**終了**：この手順は、これで完了です。

## NTP-A186 ドロップが複数ある単方向 DS-3 または EC-1 回線の作成

目的	この手順では、ドロップが複数ある単方向 DS-3 または EC-1 回線を作成します。
工具 / 機器	VT2 回線では、XC-VXC-10G カードと EC1 カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — STS を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — Number of Circuits フィールドの値が 1 の場合は使用できません。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します ( [図 6-6](#) )。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — DS3i-N-12 カードの回線の場合は、STS-3c を選択します。EC1 カードの VT 回線の場合は、VT2 を選択します。他のすべての回線の場合は、STS-1 を選択します。
  - Bidirectional — この回線はオフにします。
  - Create cross-connects only( TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
  - State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
    - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
    - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。
    - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。

- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「DLP-A230 回線のサービス状態の変更」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

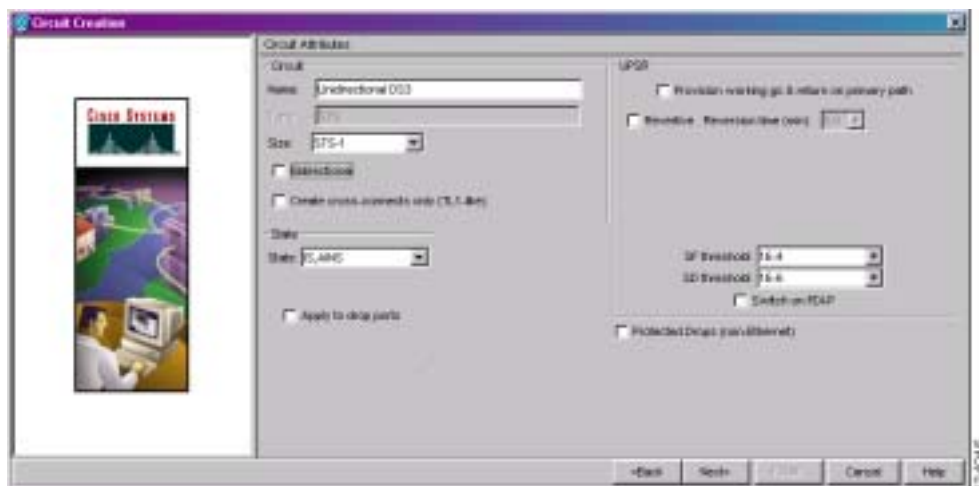
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

図 6-6 単方向 DS-3 または EC-1 回線のアトリビュート設定



**ステップ 8** 回線を UPSR にルーティングする場合は、「DLP-A218 UPSR セレクタのプロビジョニング」(p.19-14) を行います。

**ステップ 9** Next をクリックします。

**ステップ 10** 「DLP-A510 DS-3 回線の送信元と宛先のプロビジョニング」(p.22-4) を実行します。



**ステップ 11** **Route Automatically** をオフにします。Route Automatically をオフにすると、Using Required Nodes/Spans チェックボックス、Review Route Before Circuit Creation チェックボックス、および VT-DS3 Mapped Conversion チェックボックスは使用できません。

**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたまま **ステップ 13** へ進みます。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして **ステップ 15** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで **Yes** をクリックして **ステップ 15** へ進みます。

**注意**

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 13** **ステップ 12** で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 14** **ステップ 12** で Fully Protected Path を選択して回線を UPSR DRI へルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

**ステップ 15** **Next** をクリックします。Route Review and Edit 領域に、回線を手動でルーティングできるようにノードアイコンが表示されます。回線の送信元ノードは選択されています。送信元ノードから他のネットワーク ノードまでを示すグリーンの矢印は、回線のルーティングに使用できるスパンを表しています。

**ステップ 16** 作成する DS-3 または EC-1 回線について、「**DLP-A96 DS-1 または DS-3 回線ルートのプロビジョニング**」(p.17-106)を行います。

**ステップ 17** **Finish** をクリックします。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 18** Circuits ウィンドウで、複数のドロップにルーティングする回線をクリックします。Delete ボタン、Edit ボタン、Search オプション ボタンが有効になります。

**ステップ 19** Edit をクリックします。選択した Edit Circuit ウィンドウの General タブが表示されます。DCC ネットワークのすべてのノードがネットワーク マップに表示されます。回線の送信元と宛先の情報が送信元ノードと宛先ノードの下に表示されます。回線の詳細を表示する場合は、**Show Detailed Map** をクリックします。ノード アイコンの位置を変更する場合は、**Ctrl** キーを押したままで、左マウス ボタンでノードを選択し、アイコンを新しい位置にドラッグします。

**ステップ 20** Edit Circuit ダイアログボックスで、**Drops** タブをクリックします。既存のドロップがリストで表示されます。

**ステップ 21** Create をクリックします。

**ステップ 22** Define New Drop ダイアログボックスで、新しいドロップを定義します。

- a. Node — 回線のドロップ対象ノードを選択します。
- b. Slot — ターゲット カードおよびスロットを選択します。
- c. Port、VC4 — Port および STS の各ドロップダウン リストからポートおよび STS (またはどちらか一方) を選択します。ステップ b で選択したカードによって、ポートと STS のいずれが表示されるか、または両方が表示されるかが決まります。オプションのリストは [表 6-2](#) を参照してください。
- d. 新しいドロップのルーティング設定は、元の回線の設定と同じです。ただし、次のオプションが使用できる場合は、設定を変更できます。
  - 保護された UPSR パスに元の回線がルーティングされていた場合は、Nodal Diversity Required、Nodal Diversity Desired、または Link Diversity Only のノード ダイバーシティ オプションを変更できます。[ステップ 13](#) のオプション説明を参照してください。
  - 保護されていないパスに元の回線がルーティングされていなかった場合は、PCA オプションを使用できます。[ステップ 12](#) の PCA オプションの説明を参照してください。
- e. 回線状態を変更する場合は、Target Circuit Admin State ドロップダウン リストから回線状態を選択します。選択された状態は、回線全体に適用されます。
- f. Target Circuit Admin State で選択した状態を回線の送信元ポートと宛先ドロップに適用する場合は、**Apply to drop ports** をオンにします。ドロップ ポートにサービス状態を適用するための要件については、『Cisco ONS 15454 Reference Manual』を参照してください。
- g. **Finish** をクリックします。新しいドロップが Drops リストに表示されます。

**ステップ 23** ドロップを作成して回線に追加する必要がある場合は、[ステップ 21](#) と [22](#) を繰り返します。

**ステップ 24** Close をクリックします。Circuits ウィンドウが表示されます。

**ステップ 25** 編集した回線の Destination カラムに新しいドロップが表示されていることを確認します。表示されない場合は、オプションがすべて正しく設定されていることを確認して、[ステップ 21](#) ~ [24](#) を繰り返します。

**ステップ 26** 「[NTP-A135 電気回線のテスト](#)」(p.6-44) を実行します。テスト回線を作成した場合は、このステップを省略します。

**終了** : この手順は、これで完了です。

## NTP-A133 自動ルーティングによるVTトンネルの作成

目的	この手順では、送信元ノードから宛先ノードまでのルーティングを自動的に行うVTトンネルを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。



(注)

VTトンネルを使用すれば、クロスコネクタカードのVTマトリクスリソースを使用しなくても、中間のONS 15454にVT回線をパススルーさせることができます。VTトンネルは28本のVT1.5回線のトラフィックを伝送できます。送信元と宛先の同じVT回線を数多く作成する場合は、特別なことがないかぎり、VTトンネルを作成することを推奨します。詳細については、『Cisco ONS 15454 SDH Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- ステップ 1** VTトンネルを作成するノードで、「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** Viewメニューから、**Go to Network View**を選択します。
- ステップ 4** Circuitsタブをクリックして、**Create**をクリックします。
- ステップ 5** Circuit Creationダイアログボックスで、Circuit Type リストから **VT Tunnel**を選択します。
- ステップ 6** **Next**をクリックします。
- ステップ 7** 回線のアトリビュートを定義します ([図 6-7](#))。

- Name — VTトンネルに名前を付けます。名前には、48文字(スペースを含む)以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を43文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTCによってデフォルトの名前がトンネルに割り当てられます。
- Size — VTトンネルでは使用できません。
- Bidirectional — VTトンネルでは使用できません。
- State — VTトンネル内のすべてのクロスコネクタに適用する管理状態を選択します。
  - IS — 回線のクロスコネクタのサービス状態をIS-NRにします。

- OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
- IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

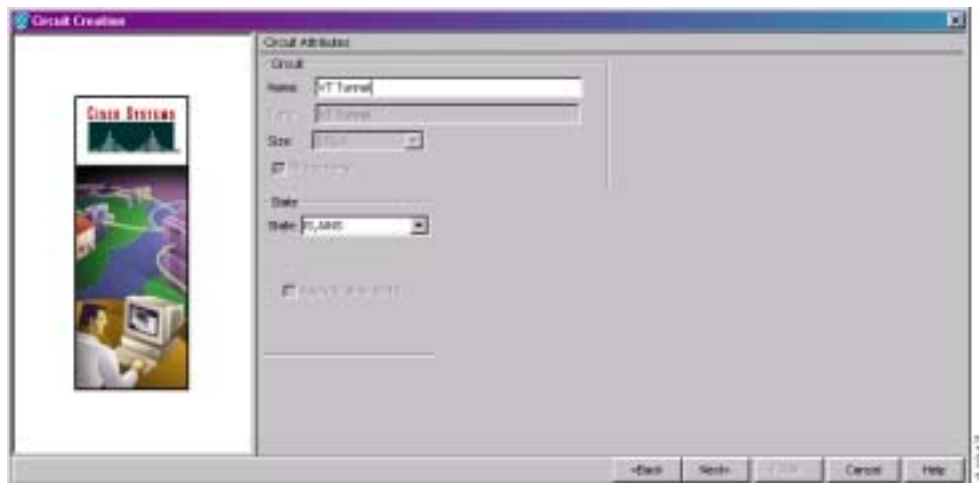


(注) VT回線を作成すると、VTトンネルは自動的にISサービス状態に移行します。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — VTトンネルでは使用できません。

図 6-7 VTトンネルのアトリビュート設定



**ステップ 8** Next をクリックします。

**ステップ 9** Circuit Source 領域で、Node ドロップダウン リストから、VTトンネルの送信元になるノードを選択します。

**ステップ 10** Next をクリックします。

**ステップ 11** Circuit Destination 領域で、Node ドロップダウン リストから、VTトンネルの宛先になるノードを選択します。

**ステップ 12** Next をクリックします。

**ステップ 13** Circuit Routing Preferences 領域で、**Route Automatically** を選択します。使用できるオプションは2つあります。設定に応じて、どちらか一方または両方を選択するか、またはどちらも選択しないようにします。

- Using Required Nodes/Spans — CTC が生成したトンネル ルートに、ノードとスパンを指定して含める、または除外する場合は、このチェックボックスをオンにします。  
含めるように指定したノードとスパンは、確実にその回線の現用パスに含まれます(保護パスには含まれません)。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。
- Review Route Before Creation — 回線を作成する前に VT トンネルのルートを確認して編集する場合は、このチェックボックスをオンにします。ステップ 15 に進みます。

**ステップ 14** ステップ 13 で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。

- a. Next をクリックします。
- b. Circuit Route Constraints 領域の VT トンネル マップで、スパンをクリックします。
- c. ノードまたはスパンを VT トンネルに含める場合は、**Include** をクリックします。VT トンネルからそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。トンネルに含めるノードとスパンの選択順によって、VT トンネルの順序が決まります。回線の変更に伴ってスパンを2回クリックします。
- d. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b と c を繰り返します。
- e. VT トンネルのルートを確認します。トンネルのルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストからノードを選択し、Up ボタンまたは Down ボタンをクリックします。ノードまたはスパンを削除する場合は、**Remove** をクリックします。ステップ 16 に進みます。

**ステップ 15** ステップ 13 で Review Route Before Creation を選択した場合は、次のサブステップを実行します。

- a. Next をクリックします。
- b. トンネルのルートを確認します。トンネルのスパンを追加または削除する場合は、トンネルのルートにあるノードを選択します。ブルーの矢印でトンネルのルートが示されます。グリーン  
の矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include**  
をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- c. プロビジョニングしたトンネルが予定のルートと設定を反映していない場合は **Back** をクリッ  
クし、トンネルの情報を確認して変更します。

**ステップ 16** **Finish** をクリックします。Circuits ウィンドウが表示されます。

**ステップ 17** 回線のリストに作成したトンネルが表示されていることを確認します。VT トンネルは、Type カラムが VTT になっています。

**終了**：この手順は、これで完了です。

## NTP-A134 手動ルーティングによるVTトンネルの作成

目的	この手順では、送信元ノードから宛先ノードまでのルーティングを手動で行うVTトンネルを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

VTトンネルを使用すれば、クロスコネク トカードのVTマトリクスリソースを使用しなくても、中間のONS 15454にVT回線をパススルーさせることができます。VTトンネルは28本のVT1.5回線のトラフィックを伝送できます。送信元と宛先の同じVT回線を数多く作成する場合は、特別なことがないかぎり、VTトンネルを作成することを推奨します。詳細については、『Cisco ONS 15454 SDH Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- ステップ 1** VTトンネルを作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** Viewメニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、Circuit Type リストから VT Tunnel を選択します。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します ([図 6-7](#))。

- Name — VTトンネルに名前を付けます。名前には、48文字(スペースを含む)以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を43文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTCによってデフォルトの名前がトンネルに割り当てられます。
- Size — VTトンネルでは使用できません。
- Bidirectional — VTトンネルでは使用できません。
- State — VTトンネル内のすべてのクロスコネク トに適用する管理状態を選択します。
  - IS — 回線のクロスコネク トのサービス状態をIS-NRにします。
  - OOS,DSBLD — 回線のクロスコネク トのサービス状態をOOS-MA,DSBLDにします。トラフィックは回線を通できません。
  - IS,AINS — 回線のクロスコネク トをOOS-AU,AINSサービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的にIS-NRになります。

- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS、AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。



**(注)** VT 回線を作成すると、VT トンネルは自動的に IS サービス状態に移行します。

回線の詳細なサービス状態については、『*Cisco ONS 15454 Reference Manual*』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — VT トンネルでは使用できません。

**ステップ 8** Next をクリックします。

**ステップ 9** Circuit Source 領域で、Node ドロップダウン リストから、VT トンネルの送信元になるノードを選択します。

**ステップ 10** Next をクリックします。

**ステップ 11** Circuit Destination 領域で、Node ドロップダウン リストから、VT トンネルの宛先になるノードを選択します。

**ステップ 12** Next をクリックします。

**ステップ 13** Circuit Routing Preferences 領域で、**Route Automatically** をオフにします。

**ステップ 14** Next をクリックします。Route Review and Edit 領域に、トンネルをルーティングできるようにノードアイコンが表示されます。回線の送信元ノードは選択されています。送信元ノードから他のネットワークノードまでを示す緑色の矢印は、トンネルのルーティングに使用できるスパンを表しています。

**ステップ 15** 作成しているトンネルに対して、「[DLP-A219 VT トンネルルートのプロビジョニング](#)」(p.19-15)を行います。Circuits ウィンドウが表示されます。

**ステップ 16** 回線のリストに作成したトンネルが表示されていることを確認します。VT トンネルは、Type カラムが VTT になっています。

**終了：**この手順は、これで完了です。

## NTP-A187 VAP の作成

目的	この手順では、VAPを作成します。VAPを使用すると、複数のDS-1 (VT1.5) 回線をOC-N、EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、またはDS3XM-12カードの単一のSTSに集約できます。また、クロスコネクタカードのVTマトリクスリソースを利用しなくても、クロスコネクタカードに複数のVT1.5回線をパススルーさせることができます。ポートレストランスマックスインターフェイスを通るように回線をルーティングすることもできます。
工具 / 機器	ポートレストランスマックス構成の場合は、ネットワーク内のノードにDS3XM-12カードを取り付ける必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)** この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。



**(注)** VAPを作成できるのはBLSRノード、1+1ノード、または保護されていないノードの回線です。UPSRノードの回線にはVAPを作成できません。



**(注)** 作成できるVAPの最大数は、ノード保護のトポロジーとノードで終端するVT1.5回線の数によって異なります。ノードで終端するVT1.5回線がほかになければ、1つのノードで終端できるVAPの最大数は、1+1保護で8、BLSR保護で12です。

- ステップ 1** VAPを作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** Viewメニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、Circuit Type リストから VT Aggregation Point を選択します。
- ステップ 6** Next をクリックします。



### ステップ7 回線のアトリビュートを定義します (図 6-8)。

- Name — VAP に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が VAP に割り当てられます。
- Size — VAP では使用できません。
- Bidirectional — VAP では使用できません。
- State — 回線内のすべてのクロスコネク트에適用する管理状態を選択します。
  - IS — 回線のクロスコネク트의サービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネク트의サービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。
  - IS,AINS — 回線のクロスコネクートを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクートのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

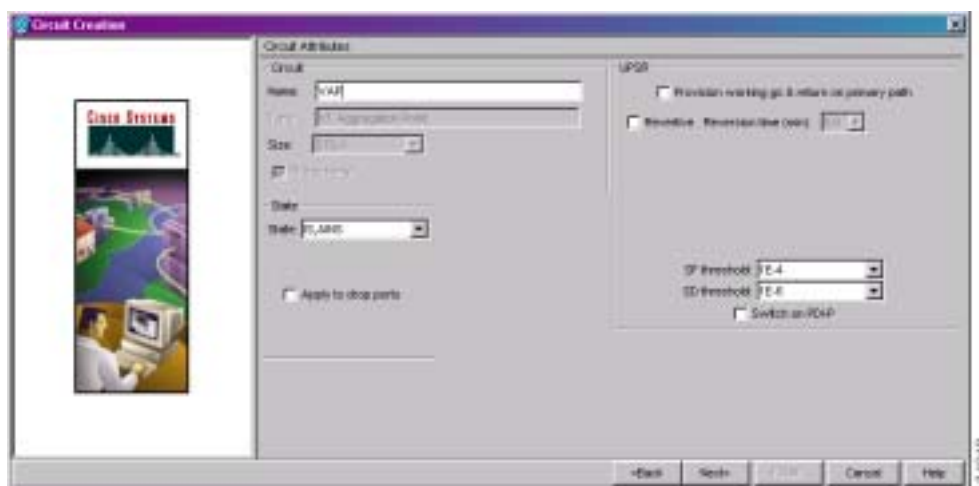


(注) VAP を作成すると、VT トンネルは自動的に IS サービス状態に移行します。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — このボックスはオフにします。

図 6-8 VAP のアトリビュート設定



### ステップ8 Next をクリックします。

**ステップ 9** Circuit Source 領域で、VAP の送信元ノード、スロット、ポート、および STS を選択します。VAP 送信元は、DS-1 (VT1.5) 回線が単一の STS に集約される場所です。VAP の宛先が DS-1 回線の送信元になります。

- a. Node ドロップダウン リストから、VAP の始点にするノードを選択します。
- b. Slot ドロップダウン リストから、VAP の始点になる OC-N、EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、または DS3XM-12 カードが入っているスロットを選択します。
- c. ポートまたは STS を選択します。
  - EC1、DS3、DS3E、DS3i-N-12、DS3/EC1-48、DS3XM-6、または DS3XM-12 カードを選択した場合は、Port ドロップダウン リストから送信元ポートを選択します。
  - STS ドロップダウン リストから OC-N カードを選択した場合は、送信元 STS を選択します。

**ステップ 10** Next をクリックします。

**ステップ 11** Circuit Destination 領域の Node ドロップダウン リストから、VAP に集約する VT 回線が終端するノードを選択します。

**ステップ 12** Next をクリックします。

**ステップ 13** Circuit Routing Preferences 領域で、**Route Automatically** を選択します。必要に応じて、次の手順を行います。

- Using Required Nodes/Spans — CTC が生成したトンネル ルートに、ノードとスパンを指定して含める、または除外する場合は、このチェックボックスをオンにします。  
含めるように指定したノードとスパンは、確実にその回線の現用パスに含まれます (保護パスには含まれません)。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。
- Review Route Before Creation — 回線を作成する前に VT トンネルのルートを確認して編集する場合は、このチェックボックスをオンにします。
- VT-DS3 Mapped Conversion — ポートレス トランスマックス インターフェイスを通るように VT トンネルをルーティングする場合は、このチェックボックスをオンにします。**ステップ 9** で VAP 送信元として DS3、DS3E、DS3i-N-12、DS3XM-6、または DS3XM-12 カードを選択した場合は、このチェックボックスを使用できません。

**ステップ 14** **ステップ 13** で VT-DS3 Mapped Conversion を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 15** へ進みます。

- a. Next をクリックします。
- b. Conversion Circuit Route Constraints 領域で、次の項目を指定します。
  - Node — DS3XM-12 カードが取り付けられているノードを選択します。
  - Slot — DS3XM-12 カードが取り付けられているスロットを選択します。
  - DS3 Mapped STS — 該当する場合に **Circuit Dest** を選択して、STS が回線の宛先であることを示すか、**Circuit Source** を選択して、STS が回線の送信元であることを示します。

**ステップ 15** **ステップ 13** で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。

- a. Next をクリックします。
- b. Circuit Route Constraints 領域の VAP マップで、スパンをクリックします。

- c. ノードまたはスパンを VAP に含める場合は、**Include** をクリックします。VAP からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。VAP に含めるノードとスパンを選択した順序によって、VAP の順序が設定されます。回線の方向を変更する場合は、スパンを2回クリックします。
- d. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b と c を繰り返します。
- e. VAP のルートを確認します。トンネルのルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストからノードを選択し、Up ボタンまたは Down ボタンをクリックします。ノードまたはスパンを削除する場合は、**Remove** をクリックします。

**ステップ 16** [ステップ 13](#) で Review Route Before Creation を選択した場合は、次のサブステップを実行します。

- a. **Next** をクリックします。
- b. トンネルのルートを確認します。トンネルのスパンを追加または削除する場合は、トンネルのルートにあるノードを選択します。ブルーの矢印でトンネルのルートが示されます。グリーン  
の矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include**  
をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- c. プロビジョニングしたトンネルが予定のルートと設定を反映していない場合は **Back** をクリッ  
クし、トンネルの情報を確認して変更します。

**ステップ 17** **Finish** をクリックします。Circuits ウィンドウが表示されます。

**ステップ 18** 回線のリストに作成した VAP が表示されていることを確認します。VAP は、Type カラムで識別  
できます。VAP トンネルは自動的に IS-NR サービス状態に移行します。

**終了**：この手順は、これで完了です。

---

## NTP-A135 電気回線のテスト

目的	この手順では、DS-1 回線および DS-3 回線または EC-1 回線をテストします。
工具 / 機器	テスト セットとすべての適切なケーブル
事前準備手順	この手順では、送信元と宛先になっている ONS 15454 から Digital Signal Cross-Connect( DSX )までのファイバとケーブルがファシリティ ループバックによってテスト済みであること、および回線が次のいずれかの手順で作成されていることが前提になっています。  <a href="#">NTP-A139 BLSR または 1+1 ノードでの半回線の作成 (p.6-65)</a> <a href="#">NTP-A140 UPSR ノードでの半回線の作成 (p.6-67)</a> <a href="#">NTP-A181 自動ルーティングによる DS-1 回線の作成 (p.6-8)</a> <a href="#">NTP-A182 手動ルーティングによる DS-1 回線の作成 (p.6-13)</a> <a href="#">NTP-A183 ドロップが複数ある単方向 DS-1 回線の作成 (p.6-17)</a> <a href="#">NTP-A184 自動ルーティングによる DS-3 または EC-1 回線の作成 (p.6-22)</a> <a href="#">NTP-A185 手動ルーティングによる DS-3 または EC-1 回線の作成 (p.6-28)</a> <a href="#">NTP-A186 ドロップが複数ある単方向 DS-3 または EC-1 回線の作成 (p.6-31)</a>
必須 / 適宜	必須
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** 電気回線をテストするノードで、「[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** View メニューから、**Go to Network View** を選択します。
- ステップ 3** **Circuits** タブをクリックします。
- ステップ 4** 「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を行い、回線および回線ポートをメンテナンス サービス状態 (OOS-MA,MT) に設定します。あとで元の状態に戻すので、最初の状態を記録しておいてください。
- ステップ 5** 送信元および宛先の DS1 または DS3 カードの回線長を設定します。
- ネットワーク ビューで、送信元ノードをダブルクリックします。
  - 回線の送信元カードをダブルクリックして、**Provisioning > Line** タブを選択します。
  - 回線の送信元ポートの Line Length ドロップダウン リストから、DSX (使用している場合) または回線終端ポイントと送信元 ONS 15454 の間の回線長 (フィート) を選択します。
  - Apply** をクリックします。
  - View メニューから、**Go to Network View** を選択します。
  - 宛先ノード回線長について [ステップ a ~ e](#) を繰り返します。

**ステップ6** 回線の宛先側カード（宛先ノード）にループバックケーブルを接続します。

- a. ループバックケーブルをテストセットの送信（Tx）コネクタからテストセットの受信（Rx）コネクタに接続してループさせ、ループバックケーブルの完全性を確認します。テストセットが正常に動作しない場合は、ケーブルに損傷がないことと、テストセットが正しく設定されていることを確認してからステップbへ進みます。
- b. テストするポートにループバックケーブルを接続します。TxコネクタをポートのRxコネクタに接続します。

**ステップ7** 回線の送信元ノードにループバックケーブルを接続します。

- a. ループバックケーブルをテストセットのTxコネクタからテストセットのRxコネクタに接続してループさせ、ループバックケーブルの完全性を確認します。テストセットが正常に動作しない場合は、ケーブルに損傷がないことと、テストセットが正しく設定されていることを確認してからステップbへ進みます。
- b. テストするポートにループバックケーブルを接続します。テストセットを回線の送信元ポートに接続します。テストセットのTxポートを回線のRxポートに接続し、テストセットのRxポートを回線のTxポートに接続します。

**ステップ8** テストする回線の送信元であるONS 15454カードに合わせて、次のようにテストセットを設定します。

- DS-1 — 多重化されていないDS-1をテストする場合は、ONS 15454にDSX-1ページまたはダイレクトDS-1インターフェイスが必要です。DS-1に対応するようにテストセットを設定してください。テストセットの設定方法については、テストセットのユーザガイドを参照してください。
- DS-3 — クリアチャンネルDS-3をテストする場合は、ONS 15454にDSX-3ページまたはダイレクトDS-3インターフェイスが必要です。クリアチャンネルDS-3に対応するようにテストセットを設定してください。テストセットの設定方法については、テストセットのユーザガイドを参照してください。
- DS3XM — DS3XM-6 または DS3XM-12 カードでDS-1をテストする場合は、ONS 15454にDSX-3ページまたはダイレクトDS-3インターフェイスが必要です。多重DS-3に対応するようにテストセットを設定してください。多重DS-3を選択したら、多重DS-3でテストするDS-1を選択します。テストセットの設定方法については、テストセットのユーザガイドを参照してください。
- EC-1 — EC1カードでDS-1をテストする場合は、ONS 15454にDSX-3ページまたはダイレクトDS-3インターフェイスが必要です。STS-1に対応するようにテストセットを設定してください。STS-1を選択したら、STS-1をテストするDS-1を選択します。テストセットの設定方法については、テストセットのユーザガイドを参照してください。

**ステップ9** テストセットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されない場合は、ステップ2～8を繰り返して、テストセットとケーブルが正しく設定されていることを確認します。

**ステップ10** テストセットからエラーを発生させます。送信元ノードと宛先ノードにエラーが表示されることを確認します。

**ステップ11** テストしたポートのPerformance Monitoring（PM; パフォーマンス モニタリング）カウントをクリアします。手順については、「DLP-A349 選択したPMカウントのクリア」（p.20-40）を参照してください。

**ステップ12** 「DLP-A230 回線のサービス状態の変更」（p.19-22）を行って、回線と回線ポートをテスト開始時のサービス状態に戻します。

**ステップ 13** 次のように、SONET のトポロジーに合った保護切り替えテストを実行します。

- UPSR の場合は、「[DLP-A94 UPSR の保護切り替えテスト](#)」(p.17-103) を実行します。
- BLSR の場合は、「[DLP-A91 BLSR 切り替えテスト](#)」(p.17-94) を実行します。

**ステップ 14** Bit Error Rate Test (BERT) を 12 時間行います。この時間について設置場所に固有の要件があれば、その要件に従ってテストを行います。テストセットを BERT 用に設定する方法については、テストセットのユーザガイドを参照してください。

**ステップ 15** BERT が終了したら、結果を印刷するか、ディスクに保存して、あとで参照できるようにします。テスト結果の印刷または保存については、テストセットのユーザガイドを参照してください。

**終了：**この手順は、これで完了です。

---

## NTP-A343 自動ルーティングによる光回線の作成

目的	この手順では、ルーティングを自動的に行なう双方向または単方向の光回線を作成します。STS-1 および連結された STS-3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、STS-192c の速度などが含まれます。
工具 / 機器	E シリーズ カードを除く OC-N カードおよびすべてのイーサネットカード。  G シリーズ回線の場合は、G シリーズ カードまたは ML シリーズ カードが回線の反対側に取り付けられている必要があります。  VT2 回線の場合は、XC-VXC-10G カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** 回線を作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** 必要に応じて次の手順を実行します(イーサネットポートまたは Packet-Over-SONET [POS] ポートのプロビジョニングは、STS 回線を作成する前にまたはあとに実行できます)。
- イーサネットポートを CE-1000-4 回線用にプロビジョニングするには、「[DLP-A509 CE-1000-4 イーサネットポートのプロビジョニング](#)」(p.22-3)を実行します。
  - イーサネットポートを CE-100T-8 回線用にプロビジョニングするには、「[DLP-A513 CE-100T-8 イーサネットポートのプロビジョニング](#)」(p.22-7)を実行します。
  - POS ポートを CE-100T-8 または CE-1000-4 回線用にプロビジョニングするには、「[DLP-A514 CE-100T-8 および CE-1000-4 POS ポートのプロビジョニング](#)」(p.22-8)を実行します。
  - G シリーズ回線の G シリーズ イーサネットポートをイネーブルにするには、「[DLP-A222 G シリーズイーサネットポートのプロビジョニング](#)」(p.19-18)を行います。
  - ML シリーズカード用のカードモードをプロビジョニングする場合は、「[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](#)」(p.22-62)を行います。
  - G シリーズまたは CE-1000-4 回線のフロー制御のデフォルト設定を変更する場合は、「[DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング](#)」(p.21-6)を行います。
- ステップ 4** View メニューから、Go to Network View を選択します。

**ステップ 5** Circuits タブをクリックして、Create をクリックします。

**ステップ 6** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — STS を選択します。
- Number of Circuits — 作成する光回線数を入力します。デフォルトは 1 です。同じ始点と終点で複数の回線を作成する場合は、オートレンジングの機能を使用して、回線を自動的に作成します。
- Auto-ranged — このチェックボックスは、Number of Circuits フィールドに 1 より大きい値を入力すると、自動的にオンになります。同じ送信元と宛先で複数の光回線を作成する場合に CTC を使用して回線を自動的に作成するときは、このチェックボックスをオンのままにします。CTC に回線を自動的に作成させない場合は、このチェックボックスをオフにします。

**ステップ 7** Next をクリックします。

**ステップ 8** 回線のアトリビュートを定義します (図 6-9)。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — VT2、STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、または STS-192c から回線サイズを選択します。G シリーズ回線の有効な回線サイズは、STS-1、STS-3c、STS6c、STS-9c、STS-12c、STS-24c、および STS-48c です。



**(注)** プロビジョニングされた回線サイズの 1 つが STS-24c の場合、G シリーズカードでの複数回線のプロビジョニングは制限されます。詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。

- Bidirectional — この回線はオンのままにします (デフォルト)。
- Create cross-connects only (TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
  - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「DLP-A230 回線のサービス状態の変更」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。



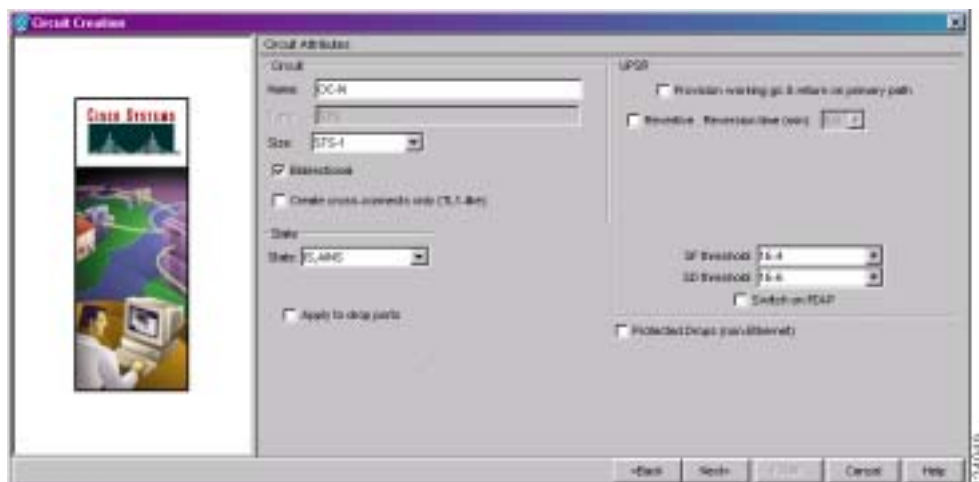
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

図 6-9 光回線のアトリビュート設定



**ステップ 9** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。

**ステップ 10** Next をクリックします。

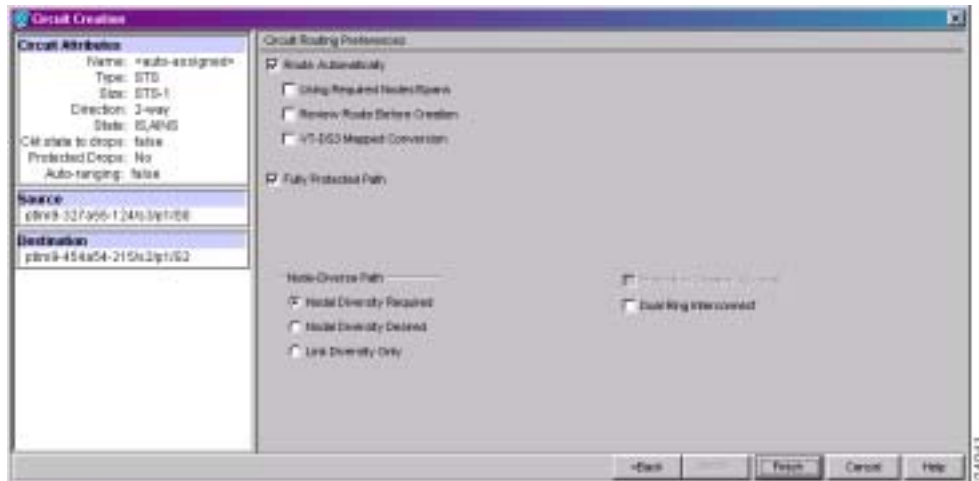
**ステップ 11** 作成している光回線に対して、「[DLP-A97 OC-N 回線の送信元と宛先のプロビジョニング \(p.17-107\)](#)」を行います。

**ステップ 12** Circuit Routing Preferences 領域 ( [図 6-10](#) ) で、**Route Automatically** をオンにします。使用できるオプションは 3 つあります。設定に応じて選択してください。

- Using Required Nodes/Spans — CTC の作成する回線ルートに、ノードとスパンを指定して含める、または除外する場合は、このチェックボックスをオンにします。  
含めるように指定したノードとスパンは、確実にその回線の現用パスに含められます (保護パスには含められません)。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。

- Review Route Before Creation — 回線を作成する前にその回線を確認して編集する場合は、このチェックボックスをオンにします。
- VT-DS3 Mapped Conversion — DS3XM-12 カードのポートレス トランスマックス インターフェイスを使用して回線を作成する場合は、このチェックボックスをオンにします。

図 6-10 光回線の回線ルーティングのプリファレンス設定



**ステップ 13** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたままで **ステップ 14** へ進みます。CTC では、選択したパス ダイバーシティ オプションに基づいて、完全に保護された回線ルートを作成します。完全に保護されているパスには (プライマリ パスと代替パスを持つ) UPSR パス セグメントがある場合とない場合がありますが、パス ダイバーシティ オプションは、UPSR パス セグメントだけに適用されます (存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして **ステップ 16** へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで **Yes** をクリックして **ステップ 16** へ進みます。

**ステップ 14** **ステップ 13** で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバースパスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 15** **ステップ 13** で Fully Protected Path を選択して回線を BLSR DRI または UPSR DRI へルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

**ステップ 16** Next をクリックします。

**ステップ 17** [ステップ 12](#) で VT-DS3 Mapped Conversion を選択した場合は、次のサブステップを実行します。それ以外の場合は [ステップ 18](#) へ進みます。

- a. Next をクリックします。
- b. Conversion Circuit Route Constraints 領域で、次の項目を指定します。
  - Node — DS3XM-12 カードが取り付けられているノードを選択します。
  - Slot — DS3XM-12 カードが取り付けられているスロットを選択します。
  - DS3 Mapped STS — 該当する場合に **Circuit Dest** を選択して、STS が回線の宛先であることを示すか、**Circuit Source** を選択して、STS が回線の送信元であることを示します。
- c. Next をクリックします。

**ステップ 18** [ステップ 12](#) で Using Required Nodes/Spans チェックボックスをオンにした場合、または [ステップ 15](#) で Dual Ring Interconnect チェックボックスをオンにした場合は、次のサブステップを実行します。BLSR の Dual Ring Interconnect チェックボックスをオンにした場合は、このステップを省略して、[ステップ 19](#) へ進みます。これらのオプションを選択しなかった場合は、[ステップ 20](#) へ進みます。

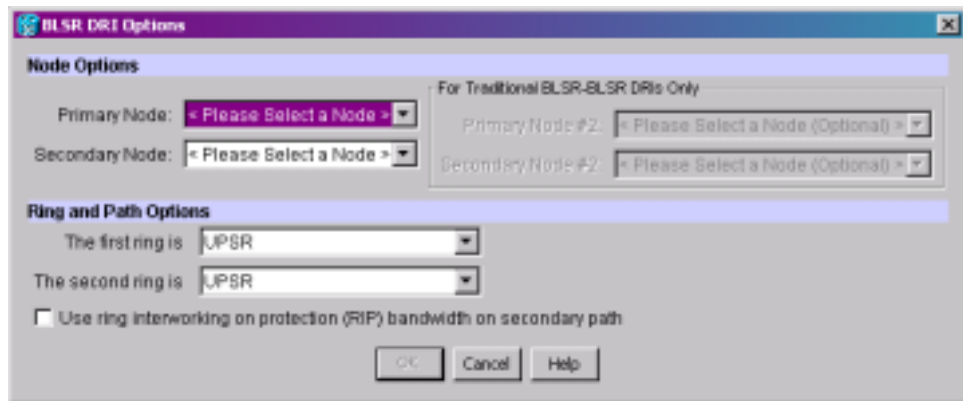
- a. Circuit Constraints for Automatic Routing 領域で、回線マップ上のノードまたはスパンをクリックします。
- b. ノードまたはスパンを回線に含める場合は、**Include** をクリックします。回線からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。含めるノードとスパンは、回線をルーティングする順序で選択します。回線の方向を変更する場合は、スパンを 2 回クリックします。
- c. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b を繰り返します。
- d. 回線のルートを確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストでノードを選択し、Up または Down ボタンをクリックして、回線のルーティング順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。

**ステップ 19** [ステップ 15](#) で BLSR の Dual Ring Interconnect チェックボックスをオンにした場合は、次のサブステップを実行して、プライマリ ノードおよびセカンダリ ノードを割り当てます。

- a. Circuit Constraints for Automatic Routing 領域で、**Add BLSR DRI** をクリックします。
- b. 確認ウィンドウで、**OK** をクリックします。
- c. BLSR DRI Options ダイアログボックスの Node Options 領域で、次のサブステップを実行します ([図 6-11](#))。
  - Primary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するプライマリ ノードを選択します。
  - Secondary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するセカンダリ ノードを選択します。プライマリ ノードのルートで障害が発生すると、このルートが使用されます。
  - Primary Node #2 — リングの相互接続に 2 つのプライマリ ノードが必要な従来型 BLSR DRI について、2 番目のプライマリ ノードを選択します。
  - Secondary Node #2 — 2 つのセカンダリ ノードが必要な従来型 BLSR DRI について、2 番目のセカンダリ ノードを選択します。
- d. Ring and Path Options 領域で、次の項目を指定します。
  - The first ring is — ドロップダウン リストから UPSR または BLSR を選択します。
  - The second ring is — ドロップダウン リストから UPSR または BLSR を選択します。

- Use ring interworking protection (RIP) on secondary path — 保護チャンネルでセカンダリ スパンのデータを伝送する場合は、このチェックボックスをオンにします。これらのスパンは、リング / スパンの切り替え中に優先使用されます。

図 6-11 BLSR DRI のプライマリ ノードとセカンダリ ノードの割り当ての選択



- OK をクリックします。ノードの情報が Required Nodes/Lines リストに表示され、マップの図にプライマリ ノードとセカンダリ ノードが表示されます。
- Circuit Constraints for Automatic Routing 領域で、回線マップ上のノードまたはスパンをクリックします。
- Include をクリックしてそのノードまたはスパンを回線に含めるか、Exclude をクリックして回線から除外します。含めるノードとスパンは、回線をルーティングする順序に合わせて選択します。回線の方向を変更する場合は、スパンを 2 回クリックします。UPSR から BLSR を結ぶ従来のハンドオフを作成する場合は、プライマリ ノードをセカンダリ ノードへ接続している非保護リンクを除外します。UPSR と BLSR を結ぶ統合ハンドオフを作成する場合は、UPSR セグメントにある不要な DRI を除外します。
- 回線の制約を確認します。回線ルートの変更する場合は、Required Nodes/Lines リストからノードを選択し、Up ボタンまたは Down ボタンをクリックして、回線ルートの順序を変更します。ノードまたはスパンを削除する場合は、Remove をクリックします。

**ステップ 20** ステップ 12 で Review Route Before Creation を選択した場合は、次のサブステップを実行します。それ以外の場合は [ステップ 21](#) へ進みます。

- Next をクリックします。
- 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、Include をクリックしてスパンを含めるか、Remove をクリックしてスパンを削除します。
- プロビジョニングした回線が予定のルートと設定を反映していない場合は Back をクリックし、回線の情報を確認して変更します。回線を別のパスにルーティングする必要がある場合は、[「NTP-A344 手動ルーティングによる光回線の作成」\(p.6-54\)](#) を参照して、回線ルートを自分で割り当てます。

**ステップ 21** **Finish** をクリックします。Circuit Creation ダイアログボックスの Number of Circuits フィールドで回線を複数入力した場合は、次のいずれかになります。

- Auto-ranged を選択した場合は、Number of Circuits フィールドに入力された数の回線が自動的に作成されます。送信元または宛先で連続ポートを使用できないなど、何らかの理由によってオートレンジで一部またはすべての回線を完成できない場合は、ダイアログボックスが表示されます。残りの回線に新しい送信元または宛先を設定し、**Finish** をクリックしてオートレンジを続行します。回線が完成すると、Circuits ウィンドウが表示されます。
- Auto-ranged を選択しなかった場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 6 ~ 20 を繰り返します。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 22** Circuits ウィンドウで、回線リストに作成した回線が表示されていることを確認します。

**ステップ 23** 必要に応じて、次の手順を行います。テスト回線を作成した場合は、このステップを省略します。

- a. 「[NTP-A62 光回線のテスト](#)」(p.6-63) を実行します。
- b. 「[NTP-A149 G シリーズ回線のテスト](#)」(p.6-97) を実行します。

**終了** : この手順は、これで完了です。

---

## NTP-A344 手動ルーティングによる光回線の作成

目的	この手順では、ルーティングを手動で行なう双方向または単方向の光回線を作成します。STS-1 または連結された STS-3c、STS-6c、STS-9c、STS-12c、STS-24c、STS-48c、STS-192c の速度などが含まれます。
工具 / 機器	E シリーズ カードを除く OC-N カードおよびすべてのイーサネットカード。  G シリーズ回線の場合は、G シリーズ カードまたは ML シリーズ カードが回線の反対側に取り付けられている必要があります。  VT2 回線の場合は、XC-VXC-10G カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** 必要に応じて次の手順を実行します（イーサネット ポートまたは POS ポートのプロビジョニングは、STS 回線を作成する前にまたはあとに実行できます）。
- イーサネット ポートを CE-1000-4 回線用にプロビジョニングするには、「[DLP-A509 CE-1000-4 イーサネット ポートのプロビジョニング](#)」(p.22-3)を実行します。
  - イーサネット ポートを CE-100T-8 回線用にプロビジョニングするには、「[DLP-A513 CE-100T-8 イーサネット ポートのプロビジョニング](#)」(p.22-7)を実行します。
  - POS ポートを CE-100T-8 または CE-1000-4 回線用にプロビジョニングするには、「[DLP-A514 CE-100T-8 および CE-1000-4 POS ポートのプロビジョニング](#)」(p.22-8)を実行します。
  - G シリーズ回線の G シリーズ イーサネット ポートをイネーブルにするには、「[DLP-A222 G シリーズ イーサネット ポートのプロビジョニング](#)」(p.19-18)を行います。
  - ML シリーズ カード用のカード モードをプロビジョニングする場合は、「[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](#)」(p.22-62)を行います。
  - G シリーズまたは CE-1000-4 回線のフロー制御のデフォルト設定を変更する場合は、「[DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング](#)」(p.21-6)を行います。
- ステップ 4** View メニューから、**Go to Network View** を選択します。
- ステップ 5** Circuits タブをクリックして、**Create** をクリックします。
- ステップ 6** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — **STS** を選択します。
  - Number of Circuits — 作成する光回線数を入力します。デフォルトは 1 です。
  - Auto-ranged — (自動ルーティング対象の回線にのみ適用) Number of Circuits フィールドに 1 より大きい値を入力した場合は、このチェックボックスをオフにします（このチェックボックスは、Number of Circuits フィールドに入力した回線の数が 1 の場合は使用できません）。

**ステップ7** Next をクリックします。

**ステップ8** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48文字（スペースを含む）以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を43文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTCによってデフォルトの名前が回線に割り当てられます。
- Size — VT2、STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、またはSTS-192cから回線サイズを選択します。Gシリーズ回線の有効な回線サイズは、STS-1、STS-3c、STS6c、STS-9c、STS-12c、STS-24c、およびSTS-48cです。



**(注)** プロビジョニングされた回線サイズの1つがSTS-24cの場合、Gシリーズカードでの複数回線のプロビジョニングは制限されます。詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。

- Bidirectional — この回線はオンのままにします（デフォルト）。
- Create cross-connects only( TL1-like) — 1つまたは複数のクロスコネクトを作成してTL1によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VTトンネル、および、Ethergroupの送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態をIS-NRにします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態をOOS-MA,DSBLDにします。トラフィックは回線を通じてできません。
  - IS,AINS — 回線のクロスコネクトをOOS-AU,AINSサービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的にIS-NRになります。
  - OOS,MT — 回線のクロスコネクトのサービス状態をOOS-MA,MTにします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、このOOS,MTを使用します。テストが完了したら、管理状態をIS、IS,AINS、またはOOS,DSBLDに変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートにStateフィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTCで管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことがWarningダイアログボックスに表示されます。このチェックボックスをオフにすると、CTCでは送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS管理状態になっているポートで信号が受信されていない場合は、LOSアラームが生成され、ポートサービス状態がOOS-AU,FLTに移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

**ステップ 9** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。

**ステップ 10** Next をクリックします。

**ステップ 11** 作成している光回線に対して、「[DLP-A97 OC-N 回線の送信元と宛先のプロビジョニング \(p.17-107\)](#)」を行います。

**ステップ 12** Circuit Routing Preferences 領域 ([図 6-10](#)) で、**Route Automatically** をオフにします。

**ステップ 13** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたまま [ステップ 14](#) へ進みます。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして [ステップ 16](#) へ進みます。
- BLSR の保護チャンネルに回線をルーティングする場合は **Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warning ダイアログボックスで **Yes** をクリックして [ステップ 16](#) へ進みます。



#### 注意

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 14** [ステップ 13](#) で Fully Protected Path を選択して回線を UPSR にルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバースパスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 15** [ステップ 13](#) で Fully Protected Path を選択して回線を BLSR DRI または UPSR DRI へルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

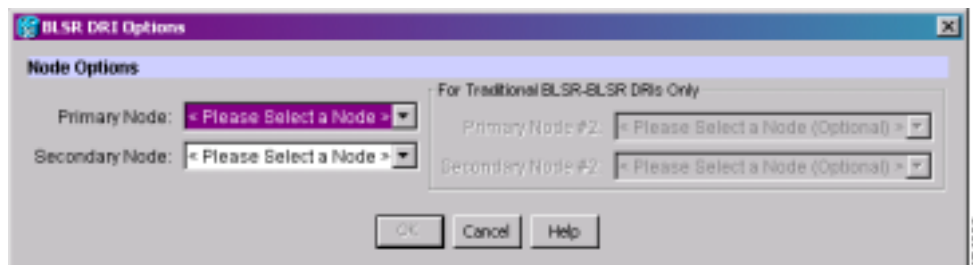
**ステップ 16** Next をクリックします。Route Review/Edit 領域にノード アイコンが表示されるので、回線を手動でルーティングします。BLSR の Dual Ring Interconnect チェックボックスをオンにした場合は、[ステップ 17](#) へ進みます。それ以外の場合は、[ステップ 18](#) へ進みます。



**ステップ 17** **ステップ 15** で BLSR DRI の Dual Ring Interconnect チェックボックスをオンにした場合は、次のサブステップを実行して、プライマリ ノードおよびセカンダリ ノードを割り当てます。

- a. Route/Review Edit 領域で、**BLSR-DRI Nodes** タブをクリックします。
- b. **Add BLSR DRI** をクリックします。
- c. BLSR DRI Options ダイアログボックスで、次の情報を入力します (図 6-12)。
  - Primary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するプライマリ ノードを選択します。
  - Secondary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するセカンダリ ノードを選択します。プライマリ ノードのルートで障害が発生すると、このルートが使用されます。
  - Primary Node #2 — リングの相互接続に 2 つのプライマリ ノードが必要な従来型 BLSR DRI について、2 番めのプライマリ ノードを選択します。
  - Secondary Node #2 — 2 つのセカンダリ ノードが必要な従来型 BLSR DRI について、2 番めのセカンダリ ノードを選択します。
- d. **OK** をクリックします。
- e. 回線の制約を確認します。回線ルートの順序を変更する場合は、Required Nodes/Lines リストからノードを選択し、**Up** ボタンまたは **Down** ボタンをクリックして、回線ルートの順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。
- f. **Included Spans** タブをクリックして、**ステップ 18** へ進みます。

図 6-12 BLSR DRI のプライマリ ノードとセカンダリ ノードの割り当ての設定 (手動ルーティング)



**ステップ 18** 「DLP-A369 OC-N 回線ルートのプロビジョニング」(p.20-59) を実行します。

**ステップ 19** **Finish** をクリックします。指定したパス ダイバーシティ要件を当該パスが満たしていない場合は、CTC によってエラー メッセージが表示されるので、回線のパスを変更します。Circuit Creation ダイアログボックスの Number of Circuits フィールドに 1 より大きい数値を入力した場合は、回線作成後に Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 6 ~ 18 を繰り返します。

**ステップ 20** すべての回線を作成すると、Circuits ウィンドウが表示されます。ウィンドウに作成した回線が表示されていることを確認します。

**ステップ 21** 必要に応じて、次の手順を行います。テスト回線を作成した場合は、このステップを省略します。


- a. 「NTP-A62 光回線のテスト」(p.6-63) を実行します。

b. 「NTP-A149 G シリーズ回線のテスト」(p.6-97) を実行します。

終了：この手順は、これで完了です。

## NTP-A314 ドロップが複数ある単方向光回線の作成

目的	この手順では、トラフィックのドロップ（回線の宛先）が複数ある単方向光回線を作成します。
工具 / 機器	VT2 回線の場合は、XC-VXC-10G カードが回線の送信元および宛先ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9) を行います。それ以外の場合は、[ステップ 3](#) へ進みます。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — STS を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — Number of Circuits フィールドの値が 1 の場合は使用できません。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します (  )。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — VT2、STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、または STS-192c から回線サイズを選択します。
  - Bidirectional — この回線ではチェックボックスをオフにします。
  - Create cross-connects only( TL1-like ) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。

- State — 回線内のすべてのクロスコネク트에適用する管理状態を選択します。
  - IS — 回線のクロスコネク트의サービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネク트의サービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通りできません。
  - IS,AINS — 回線のクロスコネク트를 OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネク트의サービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

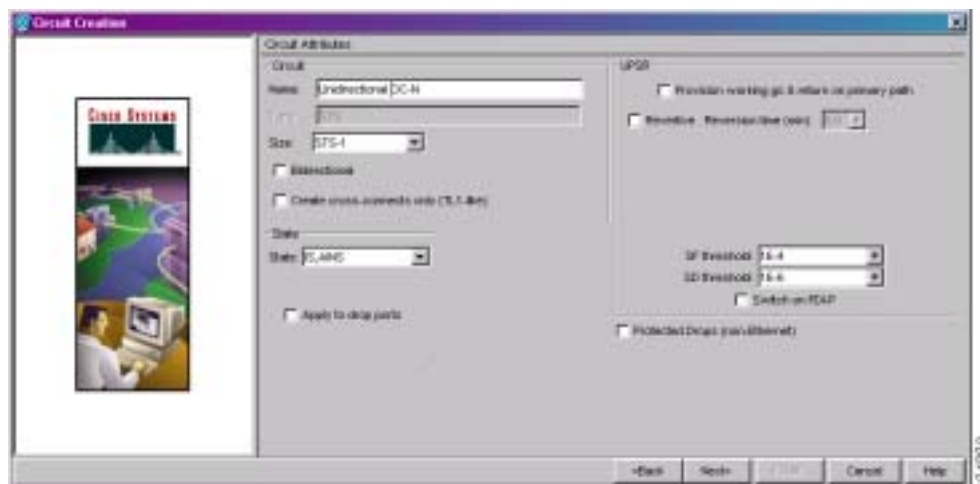
- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

図 6-13 単方向光回線のアトリビュート設定



**ステップ 8** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セクタのプロビジョニング](#)」(p.19-14)を行います。

**ステップ 9** Next をクリックします。

**ステップ 10** 作成している回線に対して、「[DLP-A97 OC-N 回線の送信元と宛先のプロビジョニング](#)」(p.17-107)を行います。

**ステップ 11** **Route Automatically** をオフにします。Route Automatically をオフにすると、Using Required Nodes/Spans チェックボックスと Review Route Before Circuit Creation チェックボックスは使用できません。

**ステップ 12** 回線パスを保護するように設定する場合は、次のいずれかを行います。

- 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにしたままで**ステップ 13**へ進みます。完全に保護されているパスには(プライマリパスと代替パスを持つ)UPSRパスセグメントがある場合とない場合がありますが、パスダイバーシティオプションは、UPSRパスセグメントだけに適用されます(存在している場合)。
- 保護されていない回線を作成する場合は、**Fully Protected Path** をオフにして**ステップ 15**へ進みます。
- BLSRの保護チャンネルに回線をルーティングする場合は**Fully Protected Path** をオフにし、**Protection Channel Access** をオンにしたあと、Warningダイアログボックスで**Yes**をクリックして**ステップ 15**へ進みます。



**注意**

BLSRの保護チャンネルにルーティングされた回線は保護されません。そのため、BLSRを切り替えている最中に優先使用されてしまいます。

**ステップ 13** **ステップ 12**でFully Protected Pathを選択して回線をUPSRにルーティングするようにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスのUPSR部分にあるプライマリパスと代替パスを、ノードダイバースにします。
- Nodal Diversity Desired — ノードダイバーシティを優先するように指定します。ただし、ノードダイバースにできない場合は、CTCによって、完全回線パスのUPSR部分にファイバダイバースパスが作成されます。
- Link Diversity Only — 完全回線パスのUPSR部分にあるプライマリパスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノードダイバースになっていても、CTCではそのことをチェックしません。



**(注)** 手動でルートを設定する回線では、パスダイバーシティの選択オプションを手動でプロビジョニングすると、CTCでそのパスがチェックされます。指定したパスダイバーシティの要件をパスが満たしていないと、エラーメッセージが表示されます。


**ステップ 14** **ステップ 12**でFully Protected Pathを選択して回線をBLSR DRIまたはUPSR DRIへルーティングするようにした場合は、**Dual Ring Interconnect** チェックボックスをオンにします。

**ステップ 15** Next をクリックします。Route Review/Edit領域にノードアイコンが表示されるので、回線を手動でルーティングします。

- a. 回線マップでノードまたはスパンをクリックします。

- b. ノードまたはスパンを回線に含める場合は、**Include** をクリックします。回線からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。含めるノードとスパンは、回線をルーティングする順序で選択します。回線の方向を変更する場合は、スパンを2回クリックします。
- c. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ a と b を繰り返します。
- d. 回線の制約を確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストでノードを選択し、**Up** または **Down** ボタンをクリックして、回線のルーティング順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。
- e. BLSR の Dual Ring Interconnect チェックボックスをオンにした場合は、**ステップ 16** へ進みます。Dual Ring Interconnect チェックボックスをオンにしなかった場合は、**ステップ 17** へ進みます。

**ステップ 16** **ステップ 14** で BLSR DRI の Dual Ring Interconnect チェックボックスをオンにした場合は、次のサブステップを実行して、プライマリ ノードおよびセカンダリ ノードを割り当てます。それ以外の場合は、**ステップ 17** へ進みます。

- a. Route/Review Edit 領域で、**BLSR-DRI Nodes** タブをクリックします。
- b. **Add BLSR DRI** をクリックします。
- c. BLSR DRI Options ダイアログボックスの Node Options 領域で、次のサブステップを実行します (  )。
  - Primary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するプライマリ ノードを選択します。
  - Secondary Node — 従来型 BLSR DRI または統合 BLSR DRI について、リングを回線で相互接続するセカンダリ ノードを選択します。プライマリ ノードのルートで障害が発生すると、このルートが使用されます。
  - Primary Node #2 — リングの相互接続に2つのプライマリ ノードが必要な従来型 BLSR DRI について、2番めのプライマリ ノードを選択します。
  - Secondary Node #2 — 2つのセカンダリ ノードが必要な従来型 BLSR DRI について、2番めのセカンダリ ノードを選択します。
- d. Ring and Path Options 領域で、次の項目を指定します。
  - The first ring is — ドロップダウン リストから UPSR または BLSR を選択します。
  - The second ring is — ドロップダウン リストから UPSR または BLSR を選択します。
  - Use ring interworking protection (RIP) on secondary path — 保護チャンネルでセカンダリ スパンのデータを伝送する場合は、このチェックボックスをオンにします。これらのスパンは、リング/スパンの切り替え中に優先使用されます。
- e. **OK** をクリックします。
- f. 回線の制約を確認します。回線ルートの順序を変更する場合は、Required Nodes/Lines リストからノードを選択し、**Up** ボタンまたは **Down** ボタンをクリックして、回線ルートの順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。
- g. **Included Spans** タブをクリックして、**ステップ 18** へ進みます。

**ステップ 17** 「DLP-A369 OC-N 回線ルートのプロビジョニング」(p.20-59) を実行します。

**ステップ 18** **Finish** をクリックします。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 19** Circuits ウィンドウで、複数のドロップにルーティングする回線をクリックします。Delete ボタン、Edit ボタン、Search ボタンが有効になります。

**ステップ 20** Edit をクリックします。選択した Edit Circuit ウィンドウの General タブが表示されます。DCC ネットワークのすべてのノードがネットワーク マップに表示されます。回線の送信元と宛先の情報が送信元ノードと宛先ノードの下に表示されます。回線の詳細を表示する場合は、**Show Detailed Map** をクリックします。アイコンの位置を変更する場合は、Ctrl キーを押したままでノード アイコンを新しい位置にドラッグアンドドロップします。

**ステップ 21** Edit Circuit ダイアログボックスで、**Drops** タブをクリックします。既存のドロップがリストで表示されます。

**ステップ 22** Create をクリックします。

**ステップ 23** Define New Drop ダイアログボックスで、新しいドロップを定義します。

- a. Node — 回線のドロップ対象ノードを選択します。
- b. Slot — ターゲット カードおよびスロットを選択します。
- c. Port、VC4 — Port および STS の各ドロップダウン リストからポートおよび STS (またはどちらか一方) を選択します。これらのメニューでどのような選択を行うかは、ステップ b で選択したカードによって異なります。表 6-2 のオプション リストを参照してください。
- d. 新しいドロップのルーティング設定は、元の回線の設定と同じです。ただし、次のオプションが使用できる場合は、設定を変更できます。
  - 保護された UPSR パスに元の回線がルーティングされていた場合は、Nodal Diversity Required、Nodal Diversity Desired、または Link Diversity Only のノード ダイバーシティ オプションを変更できます。ステップ 13 のオプション説明を参照してください。
  - 保護されていないパスに元の回線がルーティングされていなかった場合は、PCA オプションを使用できます。ステップ 12 の PCA オプションの説明を参照してください。
- e. 回線状態を変更する場合は、Target Circuit Admin State ドロップダウン リストから回線状態を選択します。選択された状態は、回線全体に適用されます。
- f. Target Circuit Admin State で選択した状態を回線の送信元ポートと宛先ドロップに適用する場合は、**Apply to drop ports** をオンにします。ドロップ ポートにサービス状態を適用するための要件については、『Cisco ONS 15454 Reference Manual』を参照してください。
- g. **Finish** をクリックします。新しいドロップが Drops リストに表示されます。

**ステップ 24** ドロップを作成して回線に追加する場合は、ステップ 21 ~ 23 を繰り返します。

**ステップ 25** Close をクリックします。Circuits ウィンドウが表示されます。

**ステップ 26** 編集した回線の Destination カラムに新しいドロップが表示されていることを確認します。表示されていない場合は、オプションがすべて正しく設定されていることを確認して、ステップ 22 ~ 25 を繰り返します。

**ステップ 27** 「NTP-A62 光回線のテスト」(p.6-63) を実行します。

**終了**：この手順は、これで完了です。

## NTP-A62 光回線のテスト

目的	この手順では、光回線をテストします。光回線を作成した場合は、この手順が必須です。
工具 / 機器	光学的な伝送速度、対応するファイバ、減衰器をテストできるテストセット
事前準備手順	送信元と宛先になっている ONS 15454 からファイバ分散ページまたは DSX までのファイバとケーブルがファシリティ ループバックによってテスト済みであること、および次のいずれかの手順が完了していることが前提になっています。  <a href="#">NTP-A343 自動ルーティングによる光回線の作成 (p.6-47)</a> <a href="#">NTP-A344 手動ルーティングによる光回線の作成 (p.6-54)</a> <a href="#">NTP-A314 ドロップが複数ある単方向光回線の作成 (p.6-58)</a>
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** 回線を作成するノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 2** View メニューから、**Go to Network View** を選択します。
- ステップ 3** Circuits タブをクリックします。
- ステップ 4** 「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を行い、回線および回線ポートを OOS-MA,MT 状態に設定します。
- ステップ 5** 宛先ノードにパッチ ケーブルを取り付けます。
- 一方の端をテスト セットの Tx ポートに、またもう一方の端をテスト セットの Rx ポートにそれぞれ接続して、パッチ ケーブルをテストします。テスト セットが正常に動作しない場合は、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。
  - テストするポートにループバック ケーブルを接続します。テストするポートの Rx コネクタに Tx コネクタを接続します。
- ステップ 6** 送信元ノードにパッチ ケーブルを取り付けます。
- 一方の端をテスト セットの Tx ポートに、またもう一方の端をテスト セットの Rx ポートにそれぞれ接続して、ループバック ケーブルをテストします。テスト セットが正常に動作しない場合は、ケーブルに損傷がないことと、テスト セットが正しく設定されていることを確認します。
  - テストする送信元ノードのポートにループバック ケーブルを接続します。テスト セットを回線の送信元ポートに接続します。テスト セットの Tx ポートを回線の Rx ポートに接続し、テスト セットの Rx ポートを回線の Tx ポートに接続します。

**ステップ7** 送信元の ONS 15454 カードに合わせてテスト セットを設定します。

- OC-3 カード — OC-3c または多重 OC-3 をテストします。OC-3c をテストする場合は、OC-3c に合わせてテスト セットを設定します。多重 OC-3 をテストする場合は、多重 OC-3 に合わせてテスト セットを設定し、テストする DS-3 または DS-1 を選択します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。
- OC-12 カード — OC-12c または多重 OC-12 をテストします。OC-12c をテストする場合は、OC-12c に合わせてテスト セットを設定します。多重 OC-12 をテストする場合は、多重 OC-12 に合わせてテスト セットを設定し、テストする DS-3 または DS-1 を選択します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。
- OC-48 カード — OC-48c または多重 OC-48 をテストします。OC-48c をテストする場合は、OC-48c に合わせてテスト セットを設定します。多重 OC-48 をテストする場合は、多重 OC-48 に合わせてテスト セットを設定し、テストする DS-3 または DS-1 を選択します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。
- OC-192 カード — OC-192c または多重 OC-192 をテストします。OC-192c をテストする場合は、OC-192c に合わせてテスト セットを設定します。多重 OC-192 をテストする場合は、多重 OC-192 に合わせてテスト セットを設定し、テストする DS-3 または DS-1 を選択します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ8** テスト セットにクリーンな信号が表示されていることを確認します。クリーンな信号が表示されていない場合は、ステップ 2 ~ 7 を繰り返して、テスト セットとケーブルが正しく設定されていることを確認します。

**ステップ9** テスト セットからエラーを発生させます。送信元ノードと宛先ノードにエラーが表示されることを確認します。

**ステップ10** テストしたポートの PM カウントをクリアします。手順については、「[DLP-A349 選択した PM カウントのクリア](#)」(p.20-40) を参照してください。

**ステップ11** SONET トポロジーに合った保護切り替えテストを実行します。

- UPSR の場合は、「[DLP-A94 UPSR の保護切り替えテスト](#)」(p.17-103) を参照してください。
- BLSR の場合は、「[DLP-A91 BLSR 切り替えテスト](#)」(p.17-94) を参照してください。

**ステップ12** BERT を 12 時間行います。この時間について設置場所に固有の要件があれば、その要件に従ってテストを行います。テスト セットを BERT 用に設定する方法については、テスト セットのユーザ ガイドを参照してください。

**ステップ13** BERT が終了したら、結果を印刷するか、ディスクに保存して、あとで参照できるようにします。テスト結果の印刷または保存については、テスト セットのユーザ ガイドを参照してください。

**ステップ14** 「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を行い、回線と回線ポートのサービス状態を OOS-MA,MT から元のサービス状態へ戻します。

**終了**：この手順は、これで完了です。



## NTP-A139 BLSR または 1+1 ノードでの半回線の作成

目的	この手順では、BLSR または 1+1 のトポロジーにある同じノード内で、ドロップカードから OC-N または G シリーズ トランク カードまでの DS-1、DS-3、または光回線を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 半回線を作成するネットワーク上のノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。

**ステップ 3** View メニューから、Go to Network View を選択します。

**ステップ 4** Circuits タブをクリックして、Create をクリックします。

**ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — DS-1 回線の場合は、VT を選択します。VT のクロスコネクタによって、ONS 15454 ネットワーク上に DS-1 回線のトラフィックが伝送されます。DS-3 回線または光回線の場合は、STS を選択します。STS のクロスコネクタによって、ONS 15454 ネットワーク上に DS-3 回線のトラフィックが伝送されます。
- Number of Circuits — 作成する回線数を入力します。デフォルトは 1 です。
- Auto-ranged — オフにします。このチェックボックスは、Number of Circuits フィールドに 1 より大きい値を入力すると、自動的にオンになります。

**ステップ 6** Next をクリックします。

**ステップ 7** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — DS-3 回線または光回線の場合は、STS-1 を選択します。DS-1 回線の場合は、VT1.5 がデフォルトです。変更はできません。
- Bidirectional — この回線はオンのままにします (デフォルト)。
- Create cross-connects only( TL1-like) — 1 つまたは複数のクロスコネクタを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクタに適用する管理状態を選択します。
  - IS — 回線のクロスコネクタのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクタのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。

- IS,AINS — 回線のクロスコネクートを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
- OOS,MT — 回線のクロスコネクートのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — このボックスはオフにします。

**ステップ 8** Next をクリックします。

**ステップ 9** 「[DLP-A311 BLSR または 1+1 構成での半回線の送信元と宛先のプロビジョニング](#)」(p.20-5) を実行します。

**ステップ 10** Finish をクリックします。Circuit Creation ダイアログボックスの Number of Circuits フィールドで回線を複数入力した場合は、次のいずれかになります。

- Auto-ranged を選択した場合は、Number of Circuits フィールドに入力された数の回線が自動的に作成されます。送信元または宛先で連続ポートを使用できないなど、何らかの理由によってオートレンジで一部またはすべての回線を完成できない場合は、ダイアログボックスが表示されます。残りの回線に新しい送信元または宛先を設定し、Finish をクリックしてオートレンジを続行します。回線が完成すると、Circuits ウィンドウが表示されます。
- Auto-ranged を選択しなかった場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 5 ~ 9 を繰り返します。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 11** Circuits ウィンドウで、回線リストに新しい回線が表示されていることを確認します。

**ステップ 12** 必要に応じて、「[NTP-A135 電気回線のテスト](#)」(p.6-44)または「[NTP-A62 光回線のテスト](#)」(p.6-63)を行います。テスト回線を作成した場合は、このステップを省略します。

**終了**：この手順は、これで完了です。

## NTP-A140 UPSR ノードでの半回線の作成

目的	この手順では、同じ UPSR ノード内で、ドロップカードから OC-N または G シリーズラインカードまでの DS-1、DS-3、または光回線を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。

**ステップ 3** View メニューから、**Go to Network View** を選択します。

**ステップ 4** **Circuits** タブをクリックして、**Create** をクリックします。

**ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — DS-1 回線の場合は、**VT** を選択します。VT のクロスコネクトによって、ONS 15454 ネットワーク上に DS-1 回線のトラフィックが伝送されます。DS-3 回線または光回線の場合は、**STS** を選択します。STS のクロスコネクトによって、ONS 15454 ネットワーク上に DS-3 回線のトラフィックが伝送されます。
- Number of Circuits — 作成する回線数を入力します。デフォルトは 1 です。
- Auto-ranged — オフにします。このチェックボックスは、Number of Circuits フィールドに 1 より大きい値を入力すると、自動的にオンになります。

**ステップ 6** **Next** をクリックします。

**ステップ 7** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — DS-1 回線の場合は、VT1.5 がデフォルトです。変更はできません。DS-3 回線または光回線の場合は、**STS-1** を選択します。
- Bidirectional — この回線はオンのままにします (デフォルト)。
- Create cross-connects only (TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。

- IS,AINS — 回線のクロスコネクタを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
- OOS,MT — 回線のクロスコネクタのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「DLP-A230 回線のサービス状態の変更」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — このチェックボックスはオフのままにします。

**ステップ 8** UPSR パス セレクタを設定します。「DLP-A218 UPSR セレクタのプロビジョニング」(p.19-14) を参照してください。

**ステップ 9** Next をクリックします。

**ステップ 10** 「DLP-A312 UPSR での半回線の送信元と宛先のプロビジョニング」(p.20-6) を実行します。

**ステップ 11** Finish をクリックします。Circuit Creation ダイアログボックスの Number of Circuits フィールドで回線を複数入力した場合は、次のいずれかになります。

- Auto-ranged を選択した場合は、Number of Circuits フィールドに入力された数の回線が自動的に作成されます。送信元または宛先で連続ポートを使用できないなど、何らかの理由によってオートレンジで一部またはすべての回線を完成できない場合は、ダイアログボックスが表示されます。残りの回線に新しい送信元または宛先を設定し、Finish をクリックしてオートレンジを続行します。回線が完成すると、Circuits ウィンドウが表示されます。
- Auto-ranged を選択しなかった場合は、Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 5 ~ 10 を繰り返します。回線が完成すると、Circuits ウィンドウが表示されます。

**ステップ 12** Circuits ウィンドウで、回線リストに新しい回線が表示されていることを確認します。

**ステップ 13** 必要に応じて、「NTP-A135 電気回線のテスト」(p.6-44)または「NTP-A62 光回線のテスト」(p.6-63)を行います。テスト回線を作成した場合は、このステップを省略します。

**終了：**この手順は、これで完了です。

## NTP-A191 E シリーズ EtherSwitch 回線の作成 (マルチカードまたはシングルカード モード)

目的	この手順では、マルチカードまたはシングルカードの EtherSwitch 回線を作成します。この手順は、ポートマップ モードの E シリーズ カードには適用できません。ポートマップ モードの回線を作成する場合は、「 <a href="#">NTP-A192 ポートマップ モードの E シリーズ カード用回線の作成</a> 」(p.6-73)を参照してください。
工具 / 機器	E シリーズ イーサネット カード (E100T-12/E100T-G、E1000-2/E1000-2-G)がイーサネット回線の両端に取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認</a> (p.6-5)
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** EtherSwitch 回線を作成するノードで「[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** ネットワークですでに多数の VLAN (仮想 LAN) が使用されている場合は、「[DLP-A99 使用可能な VLAN の判別](#)」(p.17-108)を行って、VLAN の伝送容量が十分にあることを確認します (あとで回線を作成するときに VLAN を作成します)。
- ステップ 3** 使用できる VLAN の伝送容量が十分でない場合は、「[DLP-A335 VLAN の削除](#)」(p.20-26)を行ってスペースを解放します。
- ステップ 4** 回線の送信元と宛先になるイーサネット カードが、作成する回線のモード (マルチカードまたはシングルカード) に合わせてプロビジョニングされていることを確認します。「[DLP-A246 E シリーズ イーサネット カードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 5** イーサネット ポートをプロビジョニングしてイネーブルにします。「[DLP-A220 E シリーズ イーサネット ポートのプロビジョニング](#)」(p.19-15)を参照してください。
- ステップ 6** View メニューから **Go to Network View** を選択します。
- ステップ 7** **Circuits** タブをクリックして、**Create** をクリックします。
- ステップ 8** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
  - Circuit Type — **STS** を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — 使用できません。

**ステップ 9** Next をクリックします。

**ステップ 10** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — 回線サイズを選択します。イーサネット マルチカード回線で利用できる回線のサイズは、STS-1、STS-3c、および STS6c です。イーサネット シングルカード回線で利用できる回線のサイズは、STS-1、STS-3c、STS6c、および STS12c です。
- Bidirectional — デフォルトを変更しません (オン)。
- Create cross-connects only (TL1-like) — このチェックボックスはオフにします。イーサネット回線には適用されません。
- State — IS (稼働中) を選択します。Ethergroup 回線はステートレスであり、常に稼働中です。
- Apply to drop ports — このチェックボックスはオフにします。状態は E シリーズ イーサネットカード ポートに適用できません。
- Protected Drops — 変更しないで、デフォルト (オフ) のままにしておきます。

**ステップ 11** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。



**注意**

レイヤ 1 の SONET 保護は、UPSR のマルチカード EtherSwitch 回線にまでは及びません。



**注意**

TCC2/TCC2P カードをリセットすると、シングルカード Etherswitch 回線とマルチカード Etherswitch 回線のサービスは 45 秒 ~ 2 分の間中断します。この間に、新しく有効となった TCC2/TCC2P カードでスパニング ツリートポロジーが作成されます。

**ステップ 12** Next をクリックします。

**ステップ 13** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、EtherSwitch 回線のエンド ノードを 1 つ選択します (どちらのエンド ノードを EtherSwitch 回線の送信元にしてもかまいません)。
- b. Slot ドロップダウン リストから、次のいずれかを選択します。
  - マルチカード EtherSwitch 回線を作成している場合は、**Ethergroup** を選択します。
  - シングルカード EtherSwitch 回線を作成している場合は、シングルカード EtherSwitch をイネーブルにしたイーサネットカードを選択します。

**ステップ 14** Next をクリックします。

**ステップ 15** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから、EtherSwitch 回線のもう一方のエンド ノードを選択します。
- b. Slot ドロップダウン リストから、次のいずれかを選択します。

- マルチカード EtherSwitch 回線を作成している場合は、**Ethergroup** を選択します。
- シングルカード EtherSwitch 回線を作成している場合は、シングルカード EtherSwitch をイネーブルにしたイーサネットカードを選択します。

**ステップ 16** Next をクリックします。

**ステップ 17** Circuit VLAN Selection 領域で、**New VLAN** をクリックします。目的の VLAN がすでに存在している場合は、**ステップ 20** へ進みます。

**ヒント**

**Tools > Manage VLANs** を選択して、ネットワーク ビューに VLAN を追加することもできます。All VLANs ダイアログボックスで、**Create** ボタンをクリックして Define New VLAN ダイアログボックスを開きます。

**ステップ 18** Define New VLAN ダイアログボックスで、次のように設定します。

- VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。
- VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザ プロビジョニング可能な VLAN の最大数は 509 です。
- Topology Host — ドロップダウン リストからトポロジー ホストとして機能するノードを選択します。

**ステップ 19** OK をクリックします。

**ステップ 20** Circuit VLAN Selection 領域で VLAN の名前を強調表示し、矢印ボタン (>>) をクリックして、使用可能な VLAN を Circuit VLANs カラムに移動します。

**ステップ 21** シングルカード EtherSwitch 回線を作成しているときにこの回線でスパンニングツリーの保護をディセーブルにする場合は、Disabling Spanning Tree ダイアログボックスで **Enable Spanning Tree** チェックボックスをオフにして、**OK** をクリックします。Enable Spanning Tree チェックボックスは、次のシングルカード ポイントツーポイント イーサネット回線を作成する際にも、ここで設定したオンまたはオフの状態が保たれています。

**注意**

スパンニングツリーの保護をディセーブルにすると、イーサネット ネットワーク上で論理ループの発生する確率が高くなります。

**注意**

回線単位でスパンニングツリーをオフにすると、ONS 15454 でイーサネット回線が保護されなくなるため、その回線はイーサネット ネットワークの別のメカニズムによって保護する必要があります。

**注意**

スパンニングツリーの保護がイネーブルになっている回線が複数ある場合は、それらの回線が同じ E シリーズカードを通して同じ VLAN を使用していると、ブロッキングが発生します。

**(注)**

回線が VLAN 割り当ての一定の条件を満たしていない場合は、スパニングツリーの規則によって、新しい回線を作成したり既存の回線を修正したりすることができません。新しい回線の VLAN セットが既存の回線と重複している場合は、同じスパニングツリーがすべての回線で使用されます。新しい回線の VLAN セットと、スパニングツリーの異なる既存回線の VLAN セットが重複している場合は、VLAN を割り当てることができません。そのため、VLAN の割り当てでは VLAN セットが大きくて重複の可能性が高い回線を先に追加することを推奨します。つまり、追加する回線の VLAN セットが重複していると、その回線は同じスパニングツリーにマッピングされます。スパニングツリーにマッピングされた回線とそれらの VLAN 割り当てを表示する方法については、「DLP-A430 スパニングツリー情報の表示」(p.21-9) を参照してください。

**(注)**

回線単位でスパニングツリーの保護をディセーブルまたはイネーブルにできるのは、シングルカードのポイントツーポイントイーサネット回線だけです。他の E シリーズイーサネットでは、ポート単位でしかディセーブルまたはイネーブルにできません。

**ステップ 22** Next をクリックします。

**ステップ 23** Circuit Attributes 領域で、次の情報が正しいことを確認します。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- ONS ノード

**ステップ 24** 情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 8 ~ 23 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 25** Finish をクリックします。

**ステップ 26** 「DLP-A221 VLAN メンバーシップ用の E シリーズイーサネットポートのプロビジョニング」(p.19-17) を実行します。

**ステップ 27** 「NTP-A146 E シリーズ回線のテスト」(p.6-89) を実行します。

終了：この手順は、これで完了です。



## NTP-A192 ポートマップモードのEシリーズカード用回線の作成

目的	この手順では、ポートマップモードのEシリーズカードを使用して、Eシリーズポイントツーポイント SONET 回線を作成します。
工具 / 機器	Eシリーズイーサネットカードが回線の両端に取り付けられていて、ポートマップモードに設定されている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** 回線を作成するノードで「[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 4**へ進みます。
- ステップ 2** 回線のトラフィックを伝送するイーサネットカードをポートマップモードにプロビジョニングします。「[DLP-A246 E シリーズイーサネットカードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 3** 「[DLP-A220 E シリーズイーサネットポートのプロビジョニング](#)」(p.19-15)を実行します。
- ステップ 4** View メニューから、Go to Network View を選択します。
- ステップ 5** Circuits タブをクリックして、Create をクリックします。
- ステップ 6** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — STS を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — 使用できません。
- ステップ 7** Next をクリックします。
- ステップ 8** 回線のアトリビュートを定義します。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — 回線サイズを選択します。E シリーズ回線で利用できる回線のサイズは、STS-1、STS-3c、STS6c、および STS12c です。
  - Bidirectional — デフォルトを変更しません (オン)。
  - Create cross-connects only (TL1-like) — このチェックボックスはオフにします。

- State — 回線内のすべてのクロスコネク트에適用する管理状態を選択します。
  - IS — 回線のクロスコネク트의サービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネク트의サービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通できません。
  - IS,AINS — 回線のクロスコネク트를 OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネク트의サービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — イーサネット回線の送信元ポートと宛先ポートに State フィールドで選択した状態 (IS または OOS-MT の場合だけ) を適用する場合は、このチェックボックスをオンにします。E シリーズ イーサネット カード ポートには OOS-AINS を適用できません。CTC で回線の状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がドロップポートを使用する最初の回線である場合だけです。それ以外の場合は、回線の状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートの状態を変更しません。ドロップポートにサービス状態を適用するための要件については、『Cisco ONS 15454 Reference Manual』を参照してください。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Auto-ranged — 使用できません。
- Protected Drops — 変更しないで、デフォルト (オフ) のままにしておきます。

**ステップ 9** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング](#)」(p.19-14) を行います。

**ステップ 10** Next をクリックします。

**ステップ 11** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、回線の送信元ノードを選択します。どちらのエンド ノードをポイントツーポイント回線の送信元にしてもかまいません。
- b. Slot ドロップダウン リストから、ポイントツーポイント回線の一方の端に使用する E シリーズ カードが取り付けられているスロットを選択します。
- c. 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 12** Next をクリックします。

**ステップ 13** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから、回線の宛先ノードを選択します。

- b. Slot ドロップダウン リストから、ポイントツーポイント回線のもう一方の端に使用する E シリーズカードが取り付けられているスロットを選択します。
- c. 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 14** Next をクリックします。

**ステップ 15** Circuit Attributes 領域で、次の情報が正しいことを確認します。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- ONS ノード

**ステップ 16** 情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 6 ~ 15 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 17** Finish をクリックします。

**ステップ 18** 「NTP-A146 E シリーズ回線のテスト」(p.6-89) を実行します。

**終了** : この手順は、これで完了です。

---

## NTP-A142 E シリーズ共有パケットリングイーサネット回線の作成

目的	この手順では、共有パケットリングイーサネット回線を作成します。この手順は、ポートマップモードのEシリーズカードには適用できません。
工具 / 機器	Eシリーズイーサネットカード (E100T-12/E100T-G、E1000-2/E1000-2-G) がイーサネット回線の両方のエンドポイントノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** ネットワークですでに多数の VLAN が使用されている場合は、「[DLP-A99 使用可能な VLAN の判別](#)」(p.17-108)を行って、VLAN の伝送容量が十分であることを確認します (あとで回線を作成するときに VLAN を作成します)。
- ステップ 3** 回線のトラフィックを伝送するイーサネットカードがマルチカード EtherSwitch グループ用にプロビジョニングされていることを確認します。「[DLP-A246 E シリーズイーサネットカードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 4** イーサネットポートをプロビジョニングしてイネーブルにします。「[DLP-A220 E シリーズイーサネットポートのプロビジョニング](#)」(p.19-15)を参照してください。
- ステップ 5** View メニューから **Go to Network View** を選択します。
- ステップ 6** **Circuits** タブをクリックして、**Create** をクリックします。
- ステップ 7** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — **STS** を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — 使用できません。
- ステップ 8** **Next** をクリックします。
- ステップ 9** 回線のアトリビュートを定義します。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
  - Size — 回線サイズを選択します。共有パケットリング回線の有効なサイズは STS-1、STS-3c、および STS6c です。
  - Bidirectional — デフォルトを変更しません (オン)。

- Create cross-connects only ( TL1-like )— このチェックボックスはオフにします。イーサネット回線には適用されません。
- State — 回線は稼働中です ( デフォルト )。
- Apply to drop ports — このチェックボックスはオフにします。状態は E シリーズ ポートに適用できません。
- Protected Drops — 変更しないで、デフォルト ( オフ ) のままにしておきます。

**ステップ 10** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \( p.19-14 \)](#)」を行います。

**注意**

レイヤ 1 の SONET 保護は、UPSR のマルチカード EtherSwitch 回線にまでは及びません。

**ステップ 11** Next をクリックします。

**ステップ 12** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、共有パケットリング回線のエンドポイント ノードを 1 つ選択します ( どちらのエンド ノードを共有パケットリング回線の送信元にしてもかまいません )。
- b. Slot ドロップダウン リストから **Ethergroup** を選択します。

**ステップ 13** Next をクリックします。

**ステップ 14** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから、共有パケットリング回線のもう一方のエンドポイント ノードを選択します。
- b. Slot ドロップダウン リストから **Ethergroup** を選択します。

**ステップ 15** Next をクリックします。

**ステップ 16** Available VLANs リストで VLAN を確認します。使用する VLAN が表示されている場合は、[ステップ 17](#) へ進みます。新しい VLAN を作成する必要がある場合は、次のステップを実行します。

- a. **New VLAN** ボタンをクリックします。
- b. Define New VLAN ダイアログボックスで、次のように設定します。
  - VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。
  - VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザ プロビジョニング可能な VLAN の最大数は 509 です。
  - Topology Host — ドロップダウン リストからトポロジー ホストの ID を選択します。
- c. **OK** をクリックします。

**ヒント**

**Tools > Manage VLANs** を選択して、ネットワーク ビューに VLAN を追加することもできます。All VLANs ダイアログボックスで、**Create** ボタンをクリックして Define New VLAN ダイアログボックスを開きます。

**ステップ 17** Available VLANs カラムで使用する VLAN をクリックし、矢印ボタン (>>) をクリックしてその VLAN を Circuit VLANs カラムに移動します。



**(注)** Available VLANs にある VLAN を Circuit VLANs に移動すると、すべての VLAN トラフィックに、作成中の共有パケットリングが強制的に使用されます。

**ステップ 18** Next をクリックします。

**ステップ 19** Circuit Routing Preferences 領域で、Route Automatically チェックボックスをオフにし、Next をクリックします。

**ステップ 20** Route Review and Edit 領域で、送信元ノードをクリックしたあと、送信元ノードから外側へ向かうスパン (緑色の矢印) をクリックします。

スパンがホワイトになります。

**ステップ 21** Add Span をクリックします。

スパンがブルーになります。CTC によって、Included Spans リストにスパンが追加されます。

**ステップ 22** ブルーのスパンの終端ノードをクリックします。

**ステップ 23** ステップ 22 で選択したノードに参加している緑色のスパンをクリックします。

スパンがホワイトになります。

**ステップ 24** Add Span をクリックします。

スパンがブルーになります。

**ステップ 25** リング内のすべてのノードに対して、ステップ 21 ~ 24 を繰り返します。

**ステップ 26** Route Review and Edit 領域で、新しい回線が正しく設定されていることを確認します。回線情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 7 ~ 25 を繰り返します。



**(注)** 回線が正しくない場合は、Finish をクリックし、完成した回線を削除して、手順を最初から始めることもできます。

**ステップ 27** Finish をクリックします。

**ステップ 28** 回線を伝送する各ノードに対して「DLP-A220 E シリーズイーサネットポートのプロビジョニング」(p.19-15) を行います。

**ステップ 29** 回線を伝送する各ノードに対して「DLP-A221 VLAN メンバーシップ用の E シリーズイーサネットポートのプロビジョニング」(p.19-17) を行います。

**ステップ 30** 「NTP-A146 E シリーズ回線のテスト」(p.6-89) を実行します。

終了：この手順は、これで完了です。

## NTP-A143 E シリーズカードのハブアンドスポークイーサネット構成の作成

目的	この手順では、ハブアンドスポークイーサネット構成を作成します。この構成では同じエンドポイントを複数の回線で共有します。この手順は、ポートマップモードのEシリーズカードには適用できません。
工具 / 機器	Eシリーズイーサネットカード (E100T-12/E100T-G、E1000-2/E1000-2-G) がイーサネット回線のすべてのエンドポイントノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** ハブ ノード (共通エンドポイント) 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** 「DLP-A99 使用可能な VLAN の判別」(p.17-108) を行って、使用できる VLAN の伝送容量が十分であることを確認します (あとで回線を作成するときに VLAN を作成します)。
- ステップ 3** ノード ビューを表示します。
- ステップ 4** ハブアンドスポーク回線のトラフィックを伝送するイーサネットカードが、シングルカード EtherSwitch グループ用にプロビジョニングされていることを確認します。「DLP-A246 E シリーズイーサネットカードのモードのプロビジョニング」(p.19-32) を参照してください。
- ステップ 5** イーサネット ポートをプロビジョニングしてイネーブルにします。「DLP-A220 E シリーズイーサネットポートのプロビジョニング」(p.19-15) を参照してください。
- ステップ 6** スポーク エンドポイント ノードにログインして、宛先イーサネットカードに対して**ステップ 3 ~ 5** を繰り返します (ハブ ノードがシングルカード EtherSwitch 用にプロビジョニングされていることは1度だけ確認する必要があります)。
- ステップ 7** Circuits タブをクリックして、Create をクリックします。

**ステップ 8** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — STS を選択します。
- Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
- Auto-ranged — 使用できません。

**ステップ 9** Next をクリックします。

**ステップ 10** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — 回線サイズを選択します。
- Bidirectional — デフォルトを変更しません (オン)。
- Create cross-connects only (TL1-like) — このチェックボックスはオフにします。イーサネット回線には適用されません。
- State — 回線は稼働中です (デフォルト)。
- Apply to drop ports — このチェックボックスはオフにします。状態は E シリーズ ポートに適用できません。
- Protected Drops — 変更しないで、デフォルト (オフ) のままにしておきます。

**ステップ 11** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。

**ステップ 12** Next をクリックします。

**ステップ 13** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、ハブ ノードを選択します。
- b. Slot ドロップダウン リストから、シングルカード EtherSwitch がイネーブルになっているイーサネットカードを選択します。

**ステップ 14** Next をクリックします。

**ステップ 15** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから EtherSwitch 回線のエンドポイント ノードを選択します。
- b. Slot ドロップダウン リストから、シングルカード EtherSwitch がイネーブルになっているイーサネットカードを選択します。

**ステップ 16** Next をクリックします。

**ステップ 17** Available VLANs リストで VLAN を確認します。使用する VLAN が表示されている場合は、[ステップ 19](#) へ進みます。新しい VLAN を作成する必要がある場合は、次のステップを実行します。

- a. New VLAN ボタンをクリックします。
- b. Define New VLAN ダイアログボックスで、次のように設定します。
  - VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。



- VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザプロビジョニング可能な VLAN の最大数は 509 です。
- Topology Host — ドロップダウン リストからトポロジー ホストの ID を選択します。

c. OK をクリックします。



**ヒント** Tools > Manage VLANs を選択して、ネットワーク ビューに VLAN を追加することもできます。All VLANs ダイアログボックスで、Create ボタンをクリックして Define New VLAN ダイアログボックスを開きます。

**ステップ 18** Available VLANs カラムで使用する VLAN をクリックし、矢印ボタン (>>) をクリックしてその VLAN を Circuit VLANs カラムに移動します。



**(注)** Available VLANs にある VLAN を Circuit VLANs に移動すると、すべての VLAN トラフィックに、作成中の共有パケット リングが強制的に使用されます。

**ステップ 19** Next をクリックします。

**ステップ 20** Circuit Attributes 領域で、次の情報が正しいことを確認します。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- VLAN の名前
- ONS ノード

**ステップ 21** 回線情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 8 ~ 20 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 22** Finish をクリックします。

**ステップ 23** 回線を伝送する各ノードに対して「DLP-A220 E シリーズイーサネット ポートのプロビジョニング」(p.19-15) を行います。

**ステップ 24** 「DLP-A221 VLAN メンバーシップ用の E シリーズイーサネット ポートのプロビジョニング」(p.19-17) を実行します。

**ステップ 25** 回線を伝送する各ノードに対して「NTP-A146 E シリーズ回線のテスト」(p.6-89) を行います。

**ステップ 26** ステップ 2 ~ 25 を繰り返して残りの回線 (スポーク) を作成します。

**終了:** この手順は、これで完了です。

## NTP-A144 手動による E シリーズ シングルカード EtherSwitch クロスコネクットの作成

目的	この手順では、E シリーズ イーサネット カードと、ONS 以外の機器に接続された OC-N カードとの間を接続するためのシングルカード EtherSwitch クロスコネクットを、手動で作成します。
工具 / 機器	E シリーズ イーサネット カード (E100T-12/E100T-G、E1000-2/E1000-2-G) が回線の送信元ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)** この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。



**(注)** この手順で説明しているクロスコネクットは、同じノード内のイーサネット カードと、サードパーティ製機器に接続された OC-N カードとの間に作成する回線接続のことを指します。サードパーティ製の機器を通してイーサネット回線を送信元から宛先までルーティングできるように、送信元ノードと宛先ノードでクロスコネクットを作成します。

- ステップ 1** 回線を作成するノードで「[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** 回線を作成する前に回線の送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。
- ステップ 3** ネットワークですでに多数の VLAN が使用されている場合は、「[DLP-A99 使用可能な VLAN の判別](#)」(p.17-108)を行って、VLAN の伝送容量が十分であることを確認します (あとで回線を作成するときに VLAN を作成します)。
- ステップ 4** ノード ビューで、クロスコネクットの作成対象となるイーサネット カードをダブルクリックします。
- ステップ 5** 回線のトラフィックを伝送するイーサネット カードがシングルカード EtherSwitch 用にプロビジョニングされていることを確認します。「[DLP-A246 E シリーズ イーサネット カードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 6** View メニューから **Go to Network View** を選択します。
- ステップ 7** Circuits タブをクリックして、**Create** をクリックします。

**ステップ 8** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — STS を選択します。
- Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。

**ステップ 9** Next をクリックします。

**ステップ 10** 回線のアトリビュートを定義します。

- Name — クロスコネクットに名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってクロスコネクットにデフォルトの名前が割り当てられます。
- Size — クロスコネクットのサイズを選択します。シングルカード EtherSwitch で使用できるサイズは、STS-1、STS-3c、STS6c、および STS12c です。
- Bidirectional — デフォルトを変更しません (オン)。
- Create cross-connects only (TL1-like) — このチェックボックスはオフにします。
- State — 回線は稼働中です (デフォルト)。
- Apply to drop ports — このボックスはオフにします。
- Protected Drops — 変更しないで、デフォルト (オフ) のままにしておきます。

**ステップ 11** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。

**ステップ 12** Next をクリックします。

**ステップ 13** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、クロスコネクットの送信元ノードを選択します。
- b. Slot ドロップダウン リストから、[ステップ 5](#) でシングルカード EtherSwitch をイネーブルにしたイーサネットカードを選択します。

**ステップ 14** Next をクリックします。

**ステップ 15** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから、[ステップ 13](#) で選択したクロスコネクットの送信元ノードを選択します (イーサネットクロスコネクットの場合、送信元ノードと宛先ノードは同じです)。
- b. Slot ドロップダウン リストから、ONS 以外の機器に接続されている OC-N カードを選択します。
- c. OC-N カードに応じて、Port ドロップダウン リストと STS ドロップダウン リストからポートまたは STS を選択します。

**ステップ 16** Next をクリックします。

**ステップ 17** Available VLANs リストで VLAN を確認します。使用する VLAN が表示されている場合は、[ステップ 18](#) へ進みます。新しい VLAN を作成する必要がある場合は、次のステップを実行します。

- a. New VLAN ボタンをクリックします。

- b. Define New VLAN ダイアログボックスで、次のように設定します。
- VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。
  - VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザ プロビジョニング可能な VLAN の最大数は 509 です。
  - Topology Host — ドロップダウン リストからトポロジー ホストの ID を選択します。
- c. OK をクリックします。



**ヒント** Tools > Manage VLANs を選択して、ネットワーク ビューに VLAN を追加することもできます。All VLANs ダイアログボックスで、Create ボタンをクリックして Define New VLAN ダイアログボックスを開きます。

**ステップ 18** Available VLANs カラムで使用する VLAN をクリックし、矢印 (>>) ボタンをクリックしてその VLAN を Circuit VLANs カラムに移動します。

**ステップ 19** Next をクリックします。

**ステップ 20** Circuit Attributes 領域で、手動で作成するシングルカード EtherSwitch クロスコネクットについて、次の情報が正しいことを確認します (この作業の「回線」は、イーサネット クロスコネクットのことを指しています)。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- VLAN の名前
- ONS ノード

**ステップ 21** 情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 8 ~ 20 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 22** Finish をクリックします。

**ステップ 23** 回線を伝送する各ノードに対して「DLP-A220 E シリーズイーサネット ポートのプロビジョニング」(p.19-15) を行います。

**ステップ 24** 回線を伝送する各ノードに対して「DLP-A221 VLAN メンバーシップ用の E シリーズイーサネット ポートのプロビジョニング」(p.19-17) を行います。

**終了** : この手順は、これで完了です。

## NTP-A145 手動による E シリーズ マルチカード EtherSwitch クロスコネクットの作成

目的	この手順では、E シリーズ イーサネット カードと、ONS 以外の機器に接続された OC-N カードとの間を接続するためのマルチカード EtherSwitch クロスコネクットを、手動で作成します。
工具 / 機器	E シリーズ イーサネット カード (E100T-12/E100T-G、E1000-2/E1000-2-G) が回線の送信元ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順で説明しているクロスコネクットは、同じノード内のイーサネット カードと、サードパーティ製機器に接続された OC-N カードとの間に作成する回線接続のことを指します。サードパーティ製の機器を通してイーサネット回線を送信元から宛先までルーティングできるように、送信元ノードと宛先ノードでクロスコネクットを作成します。



(注)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** 回線を作成するノードで「[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** 「[DLP-A99 使用可能な VLAN の判別](#)」(p.17-108)を行って、使用できる VLAN の伝送容量が十分であることを確認します (あとで回線を作成するときに VLAN を作成します)。
- ステップ 3** 回線のトラフィックを伝送するイーサネット カードがマルチカード EtherSwitch グループ用にプロビジョニングされていることを確認します。「[DLP-A246 E シリーズ イーサネット カードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 4** イーサネット ポートをプロビジョニングしてイネーブルにします。「[DLP-A220 E シリーズ イーサネット ポートのプロビジョニング](#)」(p.19-15)を参照してください。
- ステップ 5** View メニューから **Go to Network View** を選択します。
- ステップ 6** **Circuits** タブをクリックして、**Create** をクリックします。
- ステップ 7** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — **STS** を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。

- Auto-ranged — 使用できません。

**ステップ 8** Next をクリックします。

**ステップ 9** 回線のアトリビュートを定義します。

- Name — 送信元クロスコネクットに名前を付けます。名前には、48 文字（スペースを含む）以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によって送信元クロスコネクットにデフォルトの名前が割り当てられます。
- Size — クロスコネクットによって伝送される回線のサイズを選択します。マルチカード EtherSwitch 回線で利用できるサイズは、STS-1、STS-3c、および STS6c です。
- Bidirectional — オンのままにします（デフォルト）。
- Create cross-connects only (TL1-like) — このチェックボックスはオフにします。
- State — 回線は稼働中です（デフォルト）。
- Apply to drop ports — このボックスはオフにします。
- Protected Drops — 変更しないで、デフォルト（オフ）のままにしておきます。

**ステップ 10** 回線を UPSR にルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。

**ステップ 11** Next をクリックします。

**ステップ 12** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、クロスコネクットの送信元ノードを選択します。
- b. Slot ドロップダウン リストから **Ethergroup** を選択します。

**ステップ 13** Next をクリックします。

**ステップ 14** Destination 領域の下にある Node ドロップダウン リストから、[ステップ 12](#) で選択したクロスコネクットの送信元ノードを選択します（イーサネットクロスコネクットの場合、送信元ノードと宛先ノードは同じです）。

Slot フィールドは、自動的に Ethergroup 用にプロビジョニングされています。

**ステップ 15** Next をクリックします。

**ステップ 16** Available VLANs リストで VLAN を確認します。使用する VLAN が表示されている場合は、[ステップ 18](#) へ進みます。新しい VLAN を作成する必要がある場合は、次のステップを実行します。

- a. New VLAN ボタンをクリックします。
- b. Define New VLAN ダイアログボックスで、次のように設定します。
  - VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。
  - VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザプロビジョニング可能な VLAN の最大数は 509 です。
  - Topology Host — ドロップダウン リストからトポロジー ホストの ID を選択します。

c. OK をクリックします。



**ヒント** Tools > Manage VLANs を選択して、ネットワーク ビューに VLAN を追加することもできます。All VLANs ダイアログボックスで、Create ボタンをクリックして Define New VLAN ダイアログボックスを開きます。

**ステップ 17** Available VLANs カラムで使用する VLAN をクリックし、矢印ボタン (>>) をクリックしてその VLAN を Circuit VLANs カラムに移動します。

**ステップ 18** Next をクリックします。

**ステップ 19** Circuit Attributes 領域で、次の情報が正しいことを確認します。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- VLAN
- ONS ノード

**ステップ 20** 情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 7 ~ 19 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 21** Finish をクリックします。

**ステップ 22** 「DLP-A220 E シリーズ イーサネット ポートのプロビジョニング」(p.19-15) を実行します。

**ステップ 23** 「DLP-A221 VLAN メンバーシップ用の E シリーズ イーサネット ポートのプロビジョニング」(p.19-17) を実行します。

**ステップ 24** View メニューから Go to Home View を選択します。

**ステップ 25** Circuits タブをクリックします。

**ステップ 26** 回線を選択して、Edit をクリックします。

Edit Circuit ダイアログボックスが表示されます。

**ステップ 27** Edit Circuit ダイアログボックスで、Drops タブをクリックします。既存のドロップがリストで表示されます。

**ステップ 28** Create をクリックします。

**ステップ 29** Define New Drop ダイアログボックスで、新しいドロップを定義します。

- a. Node — 回線のドロップ対象ノードを選択します。
- b. Slot — ONS 15454 を ONS 15454 以外の機器にリンクする OC-N カードを選択します。
- c. Port、VC4 — Port および STS の各ドロップダウン リストからポートおよび STS (またはどちらか一方) を選択します。

- d. 新しいドロップのルーティング設定は、元の回線の設定と同じです。ただし、次のオプションが使用できる場合は、設定を変更できます。
  - 保護された UPSR パスに元の回線がルーティングされていた場合は、Nodal Diversity Required、Nodal Diversity Desired、または Link Diversity Only のノード ダイバーシティ オプションを変更できます。
  - 保護されていないパスに元の回線がルーティングされていなかった場合は、PCA オプションを使用できます。
- e. 回線状態を変更する場合は、Target Circuit Admin State ドロップダウン リストから回線状態を選択します。選択された状態は、回線全体に適用されます。
- f. Target Circuit Admin State で選択した状態を回線の送信元ポートと宛先ドロップに適用する場合は、Apply to drop ports をオンにします。ドロップ ポートにサービス状態を適用するための要件については、『Cisco ONS 15454 Reference Manual』を参照してください。
- g. Finish をクリックします。新しいドロップが Drops リストに表示されます。

**ステップ 30** Edit Circuit ダイアログボックスに表示される回線の情報を確認して、Close をクリックします。

**ステップ 31** 手動で作成するイーサネット クロスコネクットのもう一方のエンドポイントで、ステップ 2 ~ 30 を繰り返します。

手動で作成した最初および 2 番目のイーサネット クロスコネクット エンドポイントは、OC-N STS クロスコネクット回線でブリッジングされます。



**(注)** 手動で作成したイーサネット クロスコネクットの 2 つのエンドポイントを接続するには、ONS 以外の機器に適切な STS 回線が存在している必要があります。



#### 注意

手動で作成したイーサネット クロスコネクットで CARLOSS アラームが繰り返し表示されてクリアされる場合は、2 つのイーサネット回線の間でサイズが一致していない可能性があります。たとえば、最初の ONS 15454 に STS-3c の回線サイズ、2 番目の ONS 15454 に STS-12c の回線サイズが設定されています。アラームが発生する場合は、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 32** 「NTP-A146 E シリーズ回線のテスト」(p.6-89) を実行します。

終了：この手順は、これで完了です。



## NTP-A146 E シリーズ回線のテスト

目的	この手順では、マルチカード EtherSwitch 用、シングルカード EtherSwitch 用、またはポートマップ モード用にプロビジョニングされている E シリーズ イーサネット カードで作成した回線をテストします。
工具 / 機器 事前準備手順	イーサネットのテストセットと、対応するファイバ送信元と宛先になっている ONS 15454 からファイバ分散ページまたは DSX までのファイバとケーブルがファシリティ ループバックによってテスト済みであること、および次のいずれかの手順が完了していることが前提になっています。  <a href="#">NTP-A191 E シリーズ EtherSwitch 回線の作成 (マルチカードまたはシングルカードモード)</a> (p.6-69)  <a href="#">NTP-A192 ポートマップ モードの E シリーズ カード用回線の作成</a> (p.6-73)  <a href="#">NTP-A142 E シリーズ共有パケットリングイーサネット回線の作成</a> (p.6-76)  <a href="#">NTP-A143 E シリーズカードのハブアンドスポークイーサネット構成の作成</a> (p.6-79)  <a href="#">NTP-A145 手動による E シリーズ マルチカード EtherSwitch クロスコネクットの作成</a> (p.6-85)
必須 / 適宜 オンサイト / リモート セキュリティ	適宜 オンサイト プロビジョニング以上のレベル

**ステップ 1** ONS 15454 の送信元イーサネット ノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。

**ステップ 2** シェルフ図で、回線の送信元になっているカードをダブルクリックします。

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

**ステップ 4** 次のように設定されていることを確認します。

- Mode — Auto、10 Half、10 Full、100 Half、または 100 Full
- Enabled — オン
- Priority — 回線計画またはサイト計画に示されているプライオリティ レベル。ポートマップモードの E シリーズ カードには、プライオリティが適用されません。
- Stp State — (Spanning-Tree Protocol [STP; スパニングツリー プロトコル] が回線に対してイネーブルになっている場合) オン。ポートマップモードの E シリーズ カードには、STP が適用されません。

**ステップ 5** VLAN タブをクリックします。E シリーズ カードがポートマップ モードになっていない場合は、送信元ポートが宛先ポートと同じ VLAN 上にあることを確認します。

**ステップ 6** 宛先ノードについてステップ 1 ~ 5 を繰り返します。

**ステップ7** イーサネットのテストセットを宛先ノードの宛先ポートに接続して、イーサネットのトラフィックが正しく送受信できるようにテストセットを設定します。



**(注)** この時点では、まだイーサネットのトラフィックを送受信できません。

**ステップ8** イーサネットのテストセットを送信元ノードの送信元ポートに接続し、イーサネットのトラフィックが正しく送受信できるようにテストセットを設定します。

**ステップ9** 両方のテストセットの間で、イーサネットフレームを伝送します。これらのノード間でイーサネットのトラフィックを送受信できない場合は、ステップ1～8を繰り返して、イーサネットポートとテストセットが正しく設定されていることを確認します。

**ステップ10** SONET トポロジーに合った保護切り替えテストを実行します。

- UPSR の場合は、「[DLP-A94 UPSR の保護切り替えテスト](#)」(p.17-103)を参照してください。
- BLSR の場合は、「[DLP-A91 BLSR 切り替えテスト](#)」(p.17-94)を参照してください。

現地の状況に合わせてテストセットを設定します。テストセットの設定については、テストセットのユーザガイドを参照してください。

**ステップ11** イーサネットのテストが完了したら、結果を印刷するか、ディスクに保存してあとで参照できるようにします。テスト結果の印刷または保存については、テストセットのユーザガイドを参照してください。

**終了：**この手順は、これで完了です。

---

## NTP-A148 手動によるポートマップモードのGシリーズまたはEシリーズカード用クロスコネクットの作成

目的	この手順では、ポートマップモードのGシリーズイーサネットカードまたはEシリーズイーサネットカードと、ONS以外の機器に接続されたOC-Nカードとの間に、手動でクロスコネクットを作成します。
工具 / 機器	GシリーズカードまたはEシリーズカードが回線の送信元ノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)** この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。



**(注)** この手順で説明しているクロスコネクットは、同じノード内のイーサネットカードと、サードパーティ製機器に接続されたOC-Nカードとの間に作成する回線接続のことを指します。サードパーティ製の機器を通してイーサネット回線を送信元から宛先までルーティングできるように、送信元ノードと宛先ノードでクロスコネクットを作成します。

- ステップ 1** クロスコネクットを作成するノードで「[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** E シリーズ カードをプロビジョニングする場合は、回線のトラフィックを伝送するイーサネットカードがポートマップモード用にプロビジョニングされていることを確認します。「[DLP-A246 E シリーズイーサネットカードのモードのプロビジョニング](#)」(p.19-32)を参照してください。
- ステップ 3** G シリーズカードをプロビジョニングする場合は、「[DLP-A222 G シリーズイーサネットポートのプロビジョニング](#)」(p.19-18)を行います。
- ステップ 4** フロー制御のデフォルト設定を変更する場合は、「[DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング](#)」(p.21-6)を行います。
- ステップ 5** Circuits タブをクリックして、Create をクリックします。
- ステップ 6** Circuit Creation ダイアログボックスで、次のフィールドを設定します。
- Circuit Type — STS を選択します。
  - Number of Circuits — 変更しないで、デフォルト (1) のままにしておきます。
  - Auto-ranged — 使用できません。
- ステップ 7** Next をクリックします。

**ステップ 8** 回線のアトリビュートを定義します。

- Name — 送信元クロスコネクットに名前を付けます。名前には、48文字（スペースを含む）以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を43文字以下にする必要があります。このフィールドを空白のままにしておくと、CTCによって送信元クロスコネクットにデフォルトの名前が割り当てられます。
- Size — クロスコネクットによって伝送される回線のサイズを選択します。Gシリーズ回線の有効な回線サイズは、STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-24c、およびSTS-48cです。ポートマップモードのEシリーズカードで使用できるサイズは、STS-1、STS-3c、STS-6c、およびSTS12cです。
- Bidirectional — デフォルトを変更しません（オン）。
- Create cross-connects only (TL1-like) — このチェックボックスはオフにします。
- State — 回線は稼働中です（デフォルト）。
- Apply to drop ports — このボックスはオフにします。
- Protected Drops — 変更しないで、デフォルト（オフ）のままにしておきます。

**ステップ 9** 回線をUPSRにルーティングする場合は、「[DLP-A218 UPSR セレクタのプロビジョニング \(p.19-14\)](#)」を行います。**ステップ 10** Next をクリックします。**ステップ 11** 次のサブステップを実行して、回線の送信元をプロビジョニングします。

- a. Node ドロップダウン リストから、回線の送信元ノードを選択します。
- b. Slot ドロップダウン リストから、クロスコネクットの送信元になるイーサネットカードを選択します。
- c. Port ドロップダウン リストからクロスコネクットの送信元ポートを選択します。

**ステップ 12** Next をクリックします。**ステップ 13** 次のサブステップを実行して、回線の宛先をプロビジョニングします。

- a. Node ドロップダウン リストから、[ステップ 11](#) で選択したクロスコネクットの送信元ノードを選択します（イーサネットクロスコネクットの場合、送信元ノードと宛先ノードは同じです）。
- b. Slot ドロップダウン リストから、ONS以外の機器に接続しているOC-Nカードを選択します。
- c. OC-Nカードに応じて、Port ドロップダウン リストとSTS ドロップダウン リストからポートまたはSTSを選択します。

**ステップ 14** Next をクリックします。**ステップ 15** Circuit Attributes 領域で、次の情報が正しいことを確認します。

- 回線の名前
- 回線のタイプ
- 回線のサイズ
- ONS ノード

**ステップ 16** 情報が正しくない場合は Back ボタンをクリックし、正しい情報を使用してステップ 5 ~ 15 を繰り返します。情報が正しい場合は、Route Automatically をオンにします。

**ステップ 17** Finish をクリックします。

**ステップ 18** 「NTP-A149 G シリーズ回線のテスト」(p.6-97) を実行します。

終了：この手順は、これで完了です。

## NTP-A241 G シリーズ ポートをトランスポンダ モードにするプロビジョニング

目的	この手順では、G シリーズ ポートをトランスポンダ モードにプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A222 G シリーズイーサネット ポートのプロビジョニング (p.19-18)</a>
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** G シリーズ ポート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、G シリーズ 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 3** Provisioning > Port タブをクリックします。

**ステップ 4** G シリーズ カードのポート ペアを 2 ポート双方向トランスポンダ モードにする場合は、次のサブステップを実行します ( [図 6-14](#) )。



(注) [ステップ 4](#) は、ペアの最初のポートを「ポート A」で、またペアの 2 番目のポートを「ポート B」でそれぞれ表しています。2 ポート双方向トランスポンダ モードでは、G シリーズ カード上の任意の 2 つのポートをペアにすることができます。

- ポート A の行 (ポート 1 など) をクリックします。
- TXP Port カラムで、ポート A を反映するポート番号 (Port 1 など) を選択します。
- TXP Mode カラムで、ドロップダウン リストから TX/RX を選択します。
- ポート B の行 (ポート 2 など) をクリックします。
- TXP Port カラムで、ドロップダウン リストからポート A (Port 1 など) を選択します。
- TXP Mode カラムで、ドロップダウン リストから TX/RX を選択します。
- Apply をクリックします。

カード ビュー内のポートに、いくつかの矢印と、ポートの背面どうしを接続する線が表示されます。

図 6-14 2 ポート双方向トランスポンダ モード

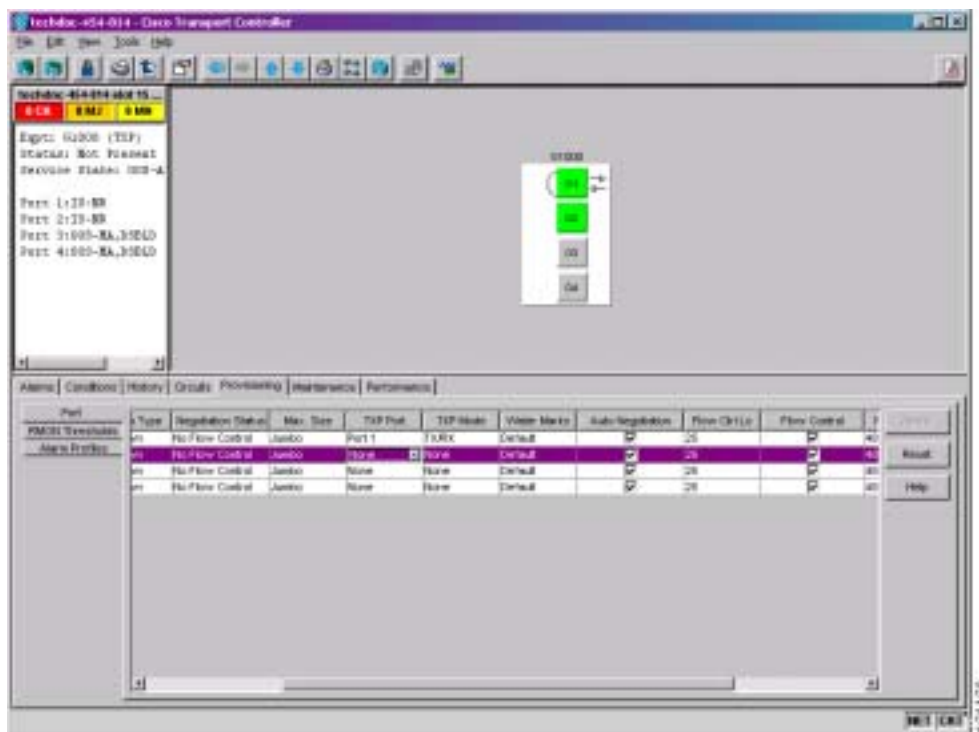


**ステップ 5** G シリーズ カードのポートを 1 ポート双方向トランスポンダ モードにする場合は、次のサブステップを実行します (図 6-15)。

- a. 対象となるポートの行 (ポート 1 など) をクリックします。
- b. TXP Port カラムで、ドロップダウン リストから対象となるポート (ポート 1 など) を選択します。
- c. TXP Mode カラムで、ドロップダウン リストから TX/RX を選択します。
- d. Apply をクリックします。

カード ビュー内の対象ポートに、いくつかの矢印が表示されます。また、ポートの背面に曲線が表示されます。

図 6-15 1 ポート双方向トランスポンダ モード



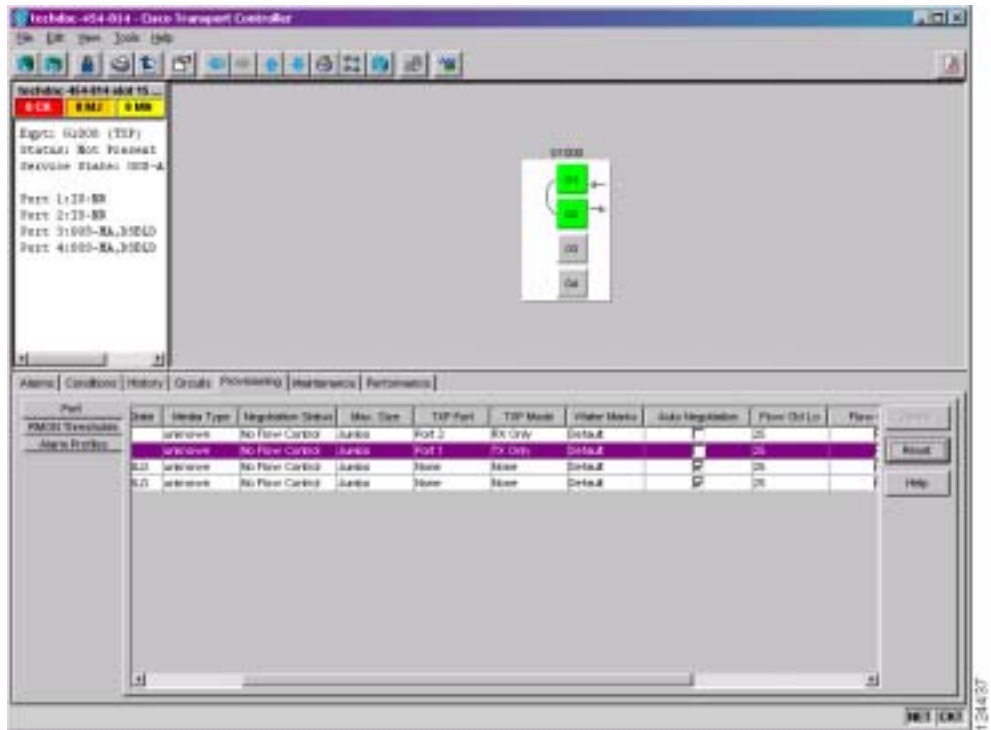
**ステップ 6** 2ポート単方向トランスポンダモードをプロビジョニングする場合は、次のサブステップを実行します（図 6-16）。

**(注)** ステップ 6 は、ペアの最初のポートを「ポート A」で、またペアの 2 番目のポートを「ポート B」でそれぞれ表しています。2ポート単方向トランスポンダモードでは、G シリーズカード上の任意の 2 つのポートをペアにすることができます。

- ポート A の行（ポート 1 など）をクリックします。
- Auto Negotiation チェックボックスをオフにします。自動ネゴシエーションがイネーブルになっている場合は、ポートを単方向トランスポンダモードにプロビジョニングすることはできません。
- TXP Port カラムで、ドロップダウン リストからポート B（ポート 2 など）を選択します。
- TXP Mode カラムで、ドロップダウン リストから **RX Only** を選択します。CTC によって、ポート B の TXP Port に Port A が設定され、TXP Mode に TX Only が設定されます。
- ポート B の行をクリックして Auto Negotiation をオフにします。
- Apply をクリックします。

CTC のカード レベル ビューにあるポートに、いくつかの矢印と、2 つのポートを接続する線が表示されます。

図 6-16 2ポート単方向トランスポンダモード




終了：この手順は、これで完了です。



## NTP-A149 G シリーズ回線のテスト

目的	この手順では、G シリーズ カード上に作成した回線をテストします。
工具 / 機器	イーサネットのテストセットと、対応するファイバ
事前準備手順	送信元と宛先になっている ONS 15454 からファイバ分散ページまたは DSX までのファイバとケーブルがファシリティ ループバックによってテスト済みであること、および次のいずれかの手順が完了していることが前提になっています。
	<a href="#">NTP-A343 自動ルーティングによる光回線の作成 (p.6-47)</a>
	<a href="#">NTP-A344 手動ルーティングによる光回線の作成 (p.6-54)</a>
	<a href="#">NTP-A148 手動によるポートマップ モードの G シリーズまたは E シリーズ カード用クロスコネクタの作成 (p.6-91)</a>
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** 回線を作成するノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 2** 「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を行い、回線および回線ポートを OOS-MA,MT 状態に変更します。
- ステップ 3** シェルフ図で、回線の送信元になっているカードをダブルクリックします。
- ステップ 4** Provisioning > Port タブをクリックします。
- ステップ 5** 次のように設定されていることを確認します。
- State — OOS,MT
  - Flow Control Neg — 回線計画またはサイト計画に示されている仕様（オンまたはオフ）
  - Max Size — Jumbo または 1548（回線計画またはサイト計画に従う）
  - Media Type — SX、LX、ZX、CWDM、または DWDM
- ステップ 6** 宛先ノードについてステップ 1 ~ 5 を繰り返します。
- ステップ 7** イーサネットのテストセットを宛先ノードの宛先ポートに接続して、イーサネットのトラフィックが正しく送受信できるようにテストセットを設定します。
-  **(注)** この時点では、まだイーサネットのトラフィックを送受信できません。
- 
- ステップ 8** イーサネットのテストセットを送信元ノードの送信元ポートに接続し、イーサネットのトラフィックが正しく送受信できるようにテストセットを設定します。
- ステップ 9** 両方のテストセットの間で、イーサネットフレームを伝送します。これらのノード間でイーサネットのトラフィックを送受信できない場合は、ステップ 1 ~ 8 を繰り返して、イーサネットポートとテストセットが正しく設定されていることを確認します。

**ステップ 10** SONET トポロジーに合った保護切り替えテストを実行します。

- UPSR の場合は、「[DLP-A94 UPSR の保護切り替えテスト](#)」(p.17-103) を実行します。
- BLSR の場合は、「[DLP-A91 BLSR 切り替えテスト](#)」(p.17-94) を実行します。

現地の状況に合わせてテスト セットを設定します。テスト セットの設定については、テスト セットのユーザ ガイドを参照してください。

**ステップ 11** 「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を行い、回線および回線ポートを IS-NR サービス状態に変更します。

**ステップ 12** 回線テストが完了したら、結果を印刷するか、ディスクに保存してあとで参照できるようにします。テスト結果の印刷または保存については、テスト セットのユーザ ガイドを参照してください。

**終了**：この手順は、これで完了です。

---

## NTP-A264 自動ルーティングによる VCAT 回線の作成

目的	この手順では、ルーティングを自動的にこなす VCAT 回線を作成します。VCAT 回線の詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
工具 / 機器	CE-100T-8、CE-1000-4、FC_MR-4、または ML シリーズ カードが VCAT 回線に使用するノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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)

この手順には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** VCAT 回線を作成するノードで「[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** 必要に応じて次の手順を実行します (イーサネット ポートまたは POS ポートのプロビジョニングは、VCAT 回線を作成する前にまたはあとに実行できます)。
- イーサネット ポートを CE-1000-4 回路用にプロビジョニングするには、「[DLP-A509 CE-1000-4 イーサネット ポートのプロビジョニング](#)」(p.22-3)を実行します。
  - イーサネット ポートを CE-100T-8 回路用にプロビジョニングするには、「[DLP-A513 CE-100T-8 イーサネット ポートのプロビジョニング](#)」(p.22-7)を実行します。
  - POS ポートを CE-100T-8 または CE-1000-4 回路用にプロビジョニングするには、「[DLP-A514 CE-100T-8 および CE-1000-4 POS ポートのプロビジョニング](#)」(p.22-8)を実行します。
- ステップ 3** View メニューから、Go to Network View を選択します。
- ステップ 4** Circuits タブをクリックして、Create をクリックします。
- ステップ 5** Circuit Creation ダイアログボックスで、Circuit Type ドロップダウン リストから STS-V または VT-V を選択します。VT-V 回線を作成するには、CE-100T-8 または CE-1000-4 カードを取り付けるか、事前にプロビジョニングする必要があります。
- ステップ 6** Next をクリックします。
- ステップ 7** 回線のアトリビュートを定義します (図 6-17)。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
  - Type — [ステップ 5](#) で選択した回線の種類が表示されます。変更はできません。

- Bidirectional — オンになっている状態がデフォルトです。変更はできません。
- Create cross-connects only( TL1-like ) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。
- State — IS を選択します。
- Apply to drop ports — 回線の送信元ポートと宛先ポートに管理状態として IS を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



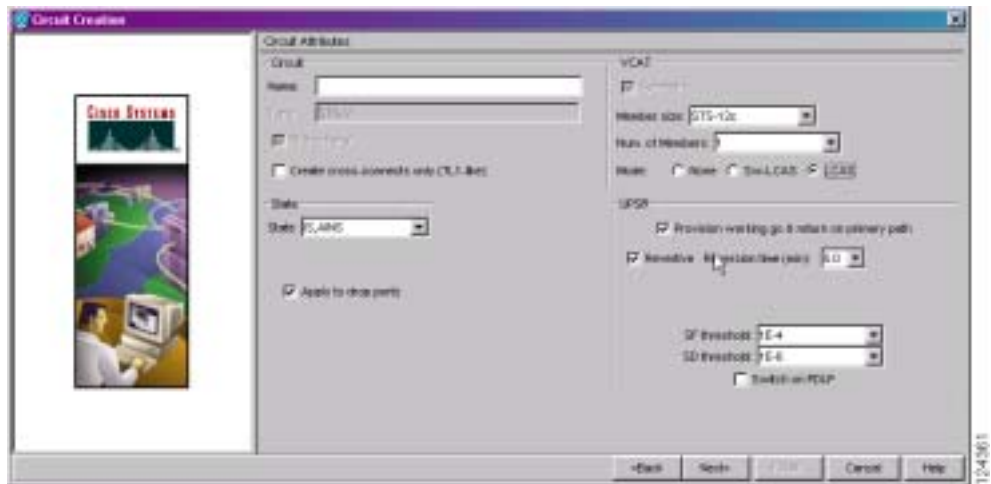
(注) IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Symmetric — オンになっている状態がデフォルトです。変更はできません。
- Member size — メンバー サイズを選択します。各カードでサポートされているメンバー サイズの詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
- Num. of members — メンバーの数を選択します。各カードでサポートされているメンバー数の詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
- Mode — VCAT 回線の保護モードを選択します。
  - None — 保護しません。1 つのメンバーで障害が発生すると、VCAT 回線全体で障害が発生します。CE-100T-8 または CE-1000-4 カードの場合は、保護されていない VCAT 回線を作成したあとに、メンバーを追加したり削除することができます。メンバーの追加中または削除中(数秒 ~ 数分間)は、VCAT 回線全体でトラフィックを伝送できません。その他のすべてのカードでは、保護モードが None の場合、メンバーを追加したり削除することができません。
  - SW-LCAS — (Software Link Capacity Adjustment Scheme [LCAS]) VCAT 回線がメンバーの障害に適応して、障害の発生したあとに狭い帯域幅でトラフィックの流れを維持するようにします。SW-LCAS では、Path Alarm Indication Signal (AIS-P) や Path Remote Defect Indication (RDI-P) のような従来の SONET 障害表示を使用してメンバーの障害を検出します。
  - LCAS — LCAS を使用するように VCAT 回線を設定します。LCAS を使用すると、関係のないメンバーの動作を中断することなく、メンバーの追加や削除を行うことができます。また LCAS では、メンバーに障害が発生しても、VCAT 回線から障害メンバーを一時的に切り離すだけです。障害が回復するまでは、残りのメンバーでトラフィックが伝送されます。



(注) ML シリーズ カードと相互運用する必要のない CE-100T-8 カードでは、LCAS を使用することを推奨します。

図 6-17 VCAT 回線のアトリビュート設定



**ステップ 8** Next をクリックします。

**ステップ 9** 作成中の VCAT 回線に対して「[DLP-A324 VCAT 回線の送信元と宛先のプロビジョニング \(p.20-15\)](#)」を行います。

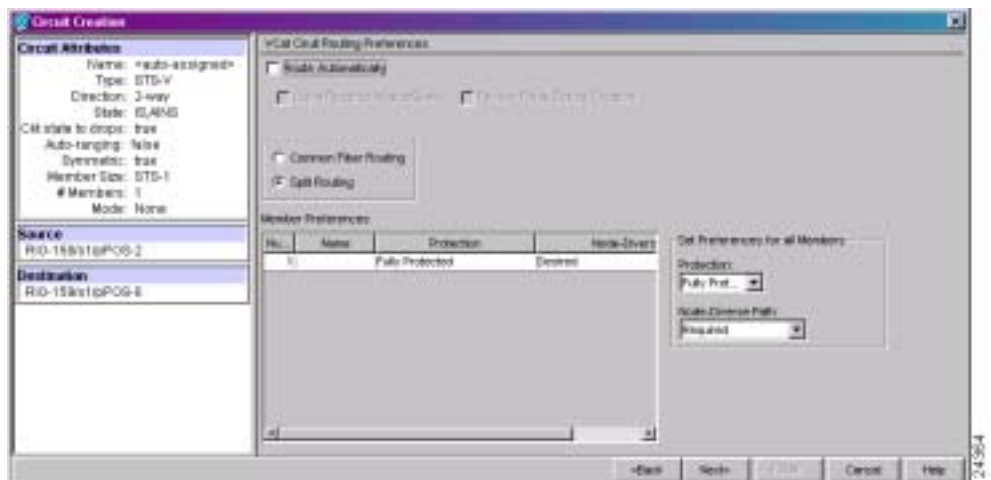
**ステップ 10** VCAT Circuit Routing Preferences 領域 (図 6-18) で、**Route Automatically** をオンにします。使用できるオプションは 2 つあります。設定に応じて、どちらか一方または両方を選択するか、またはどちらも選択しないようにします。

- Using Required Nodes/Spans — CTC の作成する回線ルートに、ノードとスパンを指定して含める、または除外する場合は、このチェックボックスをオンにします。

含めるように指定したノードとスパンは、確実にその回線の現用パスに含まれます (保護パスには含まれません)。トンネルから除外するように指定したノードとスパンは、確実にその回線の現用パスと保護パスから除外されます。

- Review Route Before Creation — 回線を作成する前にその回線を確認して編集する場合は、このチェックボックスをオンにします。

図 6-18 VCAT 回線の自動ルーティング



**ステップ 11** VCAT 回線の送信元または宛先が CE-100T-8 または CE-1000-4 カード上にある場合は、次のルーティングタイプのいずれかを選択します。

- Common Routing — 同じファイバ上にメンバーをルーティングします。
- Split Routing — 各メンバーを異なるファイバ上でルーティングしたり、各メンバーに異なるルーティング制約を設定することができます。UPSR を通る回線を作成する場合は、スプリットルーティングが必要です。

VCAT 回線の送信元または宛先が CE-100T-8 または CE-1000-4 カード上にない場合は、共通のルーティングが自動的に選択され、変更できなくなります。

**ステップ 12** メンバーごとにプリファレンスを設定する場合は、Member Preferences 領域で次の項目を指定します。各メンバーに作業を繰り返します。すべてのメンバーに同じプリファレンスを設定する場合は、このステップを省略して、[ステップ 13](#) へ進みます。

- Number — ドロップダウン リストから、メンバーを識別する番号 (1 ~ 256) を選択します。
- Name — メンバーを識別するための一意な名前を入力します。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — 回線を BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリットルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリットルーティングのみ) Fully Protected が選択されている場合に、各メンバーが利用できます。

**ステップ 13** すべてのメンバーに同じプリファレンスを設定する場合は、Set Preferences for All Members 領域で次の選択を行います。

- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — メンバーを BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリットルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリットルーティングのみ) Fully Protected が選択されている場合に、利用できます。

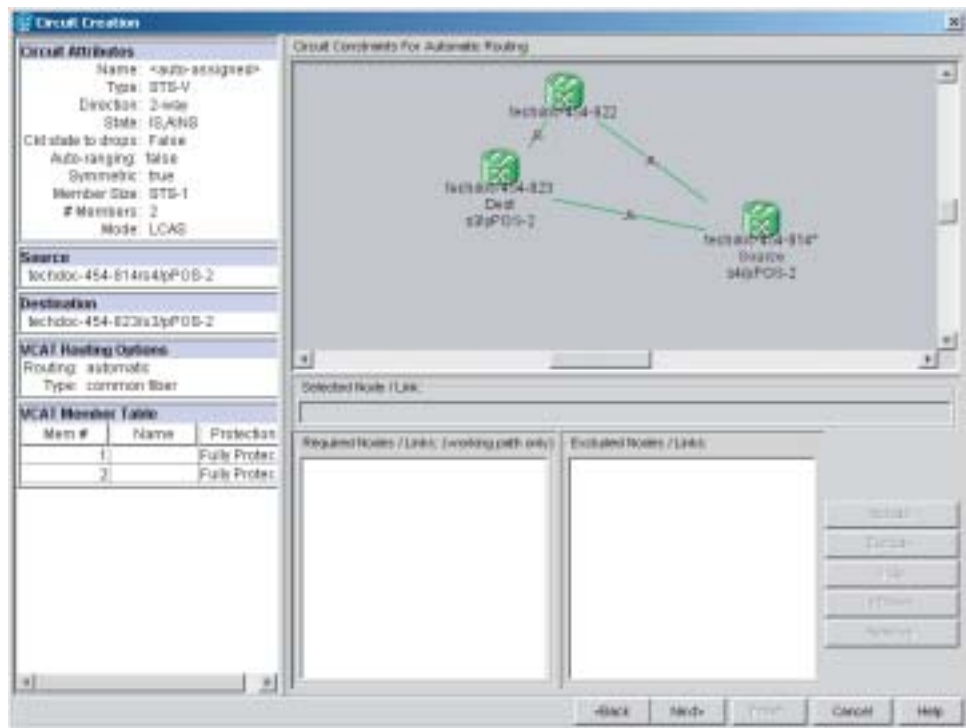
**ステップ 14** Next をクリックします。Fully Protected または PCA を選択した場合は、OK をクリックして続けます。それ以外の場合は、次のステップへ進みます。

**ステップ 15** [ステップ 10](#) で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。それ以外の場合は、[ステップ 16](#) へ進みます。

- a. Circuit Constraints 領域 ([図 6-19](#)) で、Route member number ドロップダウン リストから、ルーティングするメンバーを選択します。
- b. 回線マップでノードまたはスパンをクリックします。
- c. 回線にノードまたはスパンを含める場合は **Include** をクリックし、回線から除外する場合は **Exclude** をクリックします。含めるノードとスパンは、回線をルーティングする順序で選択します。回線の方向を変更する場合は、スパンを 2 回クリックします。

- d. 回線に含めたり除外したりするノードまたはスパンごとに、ステップ b と c を繰り返します。
- e. 回線のルートを確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストでノードを選択し、Up または Down ボタンをクリックして、回線のルーティング順序を変更します。ノードまたはスパンを削除する場合は、Remove をクリックします。
- f. 各メンバーについてステップ a ~ e を繰り返します。

図 6-19 VCAT 回線ルートの制約



**ステップ 16** ステップ 10 で Review Route Before Creation を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 17** へ進みます。

- a. Route Review/Edit 領域で、Route member number ドロップダウン リストから、ルーティングするメンバーを選択します。
- b. 回線マップでノードまたはスパンをクリックします。
- c. 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、Include をクリックしてスパンを含めるか、Remove をクリックしてスパンを削除します。
- d. プロビジョニングした回線が予定のルートと設定を反映していない場合は Back をクリックし、回線の情報を確認して変更します。回線を別のパスにルーティングする必要がある場合は、「NTP-A265 手動ルーティングによる VCAT 回線の作成」(p.6-104) を参照して、回線ルートを自分で割り当てます。
- e. 各メンバーについてステップ a ~ d を繰り返します。

**ステップ 17** Finish をクリックします。Circuits ウィンドウが表示されます。



(注) ネットワークの複雑さとメンバーの数によっては、VCAT 回線の作成処理に数分かかることがあります。

**ステップ 18** Circuits ウィンドウで、回線リストに作成した回線が表示されていることを確認します。

終了：この手順は、これで完了です。

## NTP-A265 手動ルーティングによる VCAT 回線の作成

目的	この手順では、ルーティングを手動で行なう VCAT 回線を作成します。VCAT 回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
工具 / 機器	CE-100T-8、CE-1000-4、FC_MR-4、または ML シリーズ カードが VCAT 回線に使用するノードに取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。

**ステップ 3** 必要に応じて次の手順を実行します（イーサネット ポートまたは POS ポートのプロビジョニングは、VCAT 回線を作成する前にまたはあとに実行できます）。

- イーサネット ポートを CE-1000-4 回線用にプロビジョニングするには、「[DLP-A509 CE-1000-4 イーサネット ポートのプロビジョニング](#)」(p.22-3)を実行します。
- イーサネット ポートを CE-100T-8 回線用にプロビジョニングするには、「[DLP-A513 CE-100T-8 イーサネット ポートのプロビジョニング](#)」(p.22-7)を実行します。
- POS ポートを CE-100T-8 または CE-1000-4 回線用にプロビジョニングするには、「[DLP-A514 CE-100T-8 および CE-1000-4 POS ポートのプロビジョニング](#)」(p.22-8)を実行します。

**ステップ 4** View メニューから、Go to Network View を選択します。

**ステップ 5** Circuit Creation ダイアログボックスで、Circuit Type ドロップダウン リストから STS-V または VT-V を選択します。VT-V 回線を作成するには、CE-100T-8 または CE-1000-4 カードを取り付けるか、事前にプロビジョニングする必要があります。

**ステップ 6** Next をクリックします。



**ステップ7** 回線のアトリビュートを定義します (図 6-17)。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておく、CTC によってデフォルトの名前が回線に割り当てられます。
- Type — **ステップ5** で選択した回線の種類が表示されます。変更はできません。
- Bidirectional — オンになっている状態がデフォルトです。変更はできません。
- Create cross-connects only (TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成される回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。
- State — **IS** を選択します。
- Apply to drop ports — 回線の送信元ポートと宛先ポートに管理状態として IS を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートの状態を変更しません。
- Symmetric — オンになっている状態がデフォルトです。変更はできません。
- Member size — メンバー サイズを選択します。各カードでサポートされているメンバー サイズの詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
- Num. of members — メンバーの数を選択します。各カードでサポートされているメンバー数の詳細については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。
- Mode — VCAT 回線の保護モードを選択します。
  - None — 保護しません。1 つのメンバーで障害が発生すると、VCAT 回線全体で障害が発生します。CE-100T-8 または CE-1000-4 カードの場合は、保護されていない VCAT 回線を作成したあとに、メンバーを追加したり削除することができます。メンバーの追加中または削除中 (数秒 ~ 数分間) は、VCAT 回線全体でトラフィックを伝送できません。その他のすべてのカードでは、保護モードが None の場合、メンバーを追加したり削除することができません。
  - Sw-LCAS — VCAT 回線がメンバーの障害に適応して、障害の発生したあとも狭い帯域幅でトラフィックの流れを維持するようにします。Sw-LCAS では、AIS-P や RDI-P のような従来の SONET 障害表示を使用してメンバーの障害を検出します。
  - LCAS — LCAS を使用するように VCAT 回線を設定します。LCAS を使用すると、関係のないメンバーの動作を中断することなく、メンバーの追加や削除を行うことができます。また LCAS では、メンバーに障害が発生しても、VCAT 回線から障害メンバーを一時的に切り離すだけです。障害が回復するまでは、残りのメンバーでトラフィックが伝送されます。



**(注)** ML シリーズ カードと相互運用する必要のない CE-T100-8 カードでは、LCAS を使用することを推奨します。

**ステップ8** Next をクリックします。

**ステップ9** 作成中の VCAT 回線に対して「[DLP-A324 VCAT 回線の送信元と宛先のプロビジョニング \(p.20-15\)](#)」を行います。

**ステップ10** Circuit Routing Preferences 領域 (図 6-18) で **Route Automatically** をオフにします。

**ステップ 11** VCAT 回線の送信元または宛先が CE-100T-8 または CE-1000-4 カード上にある場合は、次のルーティングタイプのいずれかを選択します。

- Common Routing — 同じファイバ上にメンバーをルーティングします。
- Split Routing — 各メンバーを異なるファイバ上でルーティングしたり、各メンバーに異なるルーティング制約を設定することができます。UPSR を通る回線を作成する場合は、スプリットルーティングが必要です。

VCAT 回線の送信元または宛先が CE-100T-8 または CE-1000-4 カード上にない場合は、共通のルーティングが自動的に選択され、変更できなくなります。

**ステップ 12** メンバーごとにプリファレンスを設定する場合は、Member Preferences 領域で次の項目を指定します。各メンバーに作業を繰り返します。すべてのメンバーに同じプリファレンスを設定する場合は、このステップを省略して、[ステップ 13](#) へ進みます。

- Number — ドロップダウン リストから、メンバーを識別する番号 (1 ~ 256) を選択します。
- Name — メンバーを識別するための一意な名前を入力します。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — メンバーを BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリットルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリットルーティングのみ) Fully Protected が選択されている場合に、各メンバーが利用できます。

**ステップ 13** すべてのメンバーに同じプリファレンスを設定する場合は、Set Preferences for All Members 領域で次の選択を行います。

- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — メンバーを BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリットルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリットルーティングのみ) Fully Protected が選択されている場合に、利用できます。

**ステップ 14** Next をクリックします。Fully Protected または PCA を選択した場合は、OK をクリックして続けません。それ以外の場合は、次のステップへ進みます。

**ステップ 15** Route Review and Edit 領域に、回線を手動でルーティングできるようにノードアイコンが表示されます。

**ステップ 16** 「[DLP-A325 VCAT 回線ルートのプロビジョニング](#)」(p.20-16) を実行します。

**ステップ 17** Finish をクリックします。指定したパス ダイバーシティ要件を当該パスが満たしていない場合は、CTC によってエラーメッセージが表示されるので、回線のパスを変更します。



(注) ネットワークの複雑さとメンバーの数によっては、VCAT 回線の作成処理に数分かかることがあります。

**ステップ 18** すべての回線を作成すると、Circuits ウィンドウが表示されます。ウィンドウに作成した回線が表示されていることを確認します。

終了：この手順は、これで完了です。

## NTP-A194 オーバーヘッド回線の作成

目的	この手順では、ONS 15454 ネットワーク上でオーバーヘッド回線を作成します。オーバーヘッド回線には、DCC トンネル、IP カプセル化トンネル、Alarm Interface Controller-International (AIC-I) カード オーダーワイヤ、および AIC-I カード UDC が含まれます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** オーバーヘッド回線を作成するノードで「[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** View メニューから **Go to Network View** を選択します。

**ステップ 3** 必要に応じて、「[DLP-A313 DCC トンネルの作成](#)」(p.20-7)を行います。

**ステップ 4** 必要に応じて、「[DLP-A341 IP カプセル化トンネルの作成](#)」(p.20-36)を行います。

**ステップ 5** 必要に応じて、「[DLP-A83 オーダーワイヤのプロビジョニング](#)」(p.17-91)を行います。

**ステップ 6** 必要に応じて、「[DLP-A212 UDC 回線の作成](#)」(p.19-9)を行います。

終了：この手順は、これで完了です。

## NTP-A167 リングを対象にした STS テスト回線の作成

目的	この手順では、同じノードの異なるポートにある送信元と宛先を使用して、リングのトラフィックをルーティングする STS テスト回線を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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** 回線を作成するノードで「[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** 回線を作成する前にトンネルの送信元ポートと宛先ポートに名前を割り当てる場合は、「[DLP-A314 ポートへの名前の割り当て](#)」(p.20-9)を行います。それ以外の場合は、[ステップ 3](#)へ進みます。

**ステップ 3** View メニューから、**Go to Network View** を選択します。

**ステップ 4** Circuits タブをクリックして、**Create** をクリックします。

**ステップ 5** Circuit Creation ダイアログボックスで、次のフィールドを設定します。

- Circuit Type — **STS** を選択します。
- Number of Circuits — 作成する回線数を入力します。デフォルトは 1 です。
- Auto-ranged — (自動ルーティング対象の回線のみ) Number of Circuits フィールドに 1 より大きい値を入力した場合は、このチェックボックスをオフにします (このチェックボックスは、Number of Circuits フィールドに入力した回線の数が 1 の場合は使用できません)。

**ステップ 6** **Next** をクリックします。

**ステップ 7** 回線のアトリビュートを定義します。

- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。モニタ回線を作成できるようにしておく場合は、回線の名前を 43 文字以下にする必要があります。このフィールドをブランクのままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Size — 回線サイズを選択します。STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、および STS-192c から選択します。
- Bidirectional — この回線はオンのままにします (デフォルト)。
- Create cross-connects only( TL1-like) — 1 つまたは複数のクロスコネクトを作成して TL1 によって生成された回線に対する信号パスを完成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、VT トンネル、および、Ethergroup の送信元と宛先は使用できません。
- State — 回線内のすべてのクロスコネクトに適用する管理状態を選択します。
  - IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
  - OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通じてできません。
  - IS,AINS — 回線のクロスコネクトを OOS-AU,AINS サービス状態にして、アラームおよび状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。

- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS、AINS、または OOS,DSBLD に変更します。「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22) を参照してください。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

- Apply to drop ports — 回線の送信元ポートと宛先ポートに State フィールドで選択した管理状態を適用する場合は、このチェックボックスをオンにします。CTC で管理状態がポートに適用されるのは、回線の帯域幅がポートの帯域幅と同じか、または、ポートの帯域幅が回線の帯域幅より大きくても、その回線がポートを使用する最初の回線である場合だけです。それ以外の場合は、管理状態をポートに適用できないことが Warning ダイアログボックスに表示されます。このチェックボックスをオフにすると、CTC では送信元ポートと宛先ポートに管理状態を適用しません。



**(注)** IS 管理状態になっているポートで信号が受信されていない場合は、LOS アラームが生成され、ポート サービス状態が OOS-AU,FLT に移行します。

- Protected Drops — 保護されているドロップ、つまり 1:1、1:N、1+1、または最適化 1+1 で保護されている ONS 15454 カードだけに回線をルーティングする場合は、この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ンにすると、CTC からは、送信元と宛先の選択肢として、保護されているカードだけが表示されます。

**ステップ 8** Next をクリックします。

**ステップ 9** 次のサブステップを実行して、回線の送信元を選択します。

- Node ドロップダウン リストから、回線の始点となるノードを選択します。
- Slot ドロップダウン リストから、回線の始点になるカードが取り付けられているスロットを選択します。(伝送容量を使い切っているカードは、リストに表示されません)。
- 回線の送信元カードに応じて、Port ドロップダウン リストと STS ドロップダウン リストから送信元ポートまたは STS を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS は、別の回線によってすでに使用されている場合は、表示されません。



**(注)** 表示される STS は、カード、回線のサイズ、および保護方式によって異なります。

**ステップ 10** Next をクリックします。

**ステップ 11** 回線の宛先を選択します。



**(注)** 宛先ポートは、回線の送信元ポートと同じノードにある必要があります。

- Node ドロップダウン リストから、[ステップ 9a](#) で選択したノードを選択します。
- Slot ドロップダウン リストから、回線が終端するカード(宛先カード)が入っているスロットを選択します(伝送容量を使い切っているカードは、リストに表示されません)。

- c. ステップ b で選択したカードに合わせて、Port ドロップダウン リストと STS ドロップダウン リストから、宛先ポートまたは STS を選択します。Port ドロップダウン リストは、カードに複数のポートがある場合にだけ使用できます。表示される STS は、カード、回線のサイズ、および保護方式によって異なります。

**ステップ 12** Next をクリックします。

**ステップ 13** Circuit Routing Preferences 領域で **Route Automatically** をオフにします。

**ステップ 14** ルーティングするテスト回線の送信元ポートと宛先ポートが同じノードにある場合は、Fully Protected Path チェックボックスが自動的にディセーブルとなります。次のいずれかのオプションを選択します。

- テスト回線を保護しない場合は、**ステップ 15** へ進みます。
- テスト回線を BLSR の保護チャンネルにルーティングする場合は、**Protection Channel Access** をオンにし、Warning ダイアログボックスで Yes をクリックして、**ステップ 15** へ進みます。



**注意**

BLSR の保護チャンネルにルーティングされた回線は保護されません。そのため、BLSR を切り替えている最中に優先使用されてしまいます。

**ステップ 15** Next をクリックします。

**ステップ 16** Route Review/Edit 領域にノード アイコンが表示されるので、回線を手動でルーティングします。

- a. Route Review/Edit 領域で送信元ノードのアイコンがまだ選択されていない場合は、そのアイコンをクリックして選択します。
- b. 送信元ノードにあるスパンから開始して、回線を通させるスパンの矢印をクリックしていきます。矢印の方向を反対にするには、矢印を 2 回クリックします。
- c. 矢印がホワイต์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。送信元 STS が表示されます。発信元 STS を変更する場合は、Source STS フィールドを変更します。変更しない場合は、ステップ d へ進みます。
- d. **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。
- e. 中継ノードも含めて回線が送信元から宛先まですべてプロビジョニングされるまで、ステップ b ~ d を繰り返します。

**ステップ 17** **Finish** をクリックします。指定したパス ダイバーシティ要件を当該パスが満たしていない場合は、CTC によってエラー メッセージが表示されるので、回線のパスを変更します。Circuit Creation ダイアログボックスの Number of Circuits フィールドに 1 より大きい数値を入力した場合は、回線作成後に Circuit Creation ダイアログボックスが表示されるので、残りの回線を作成します。追加する回線ごとにステップ 7 ~ 16 を繰り返します。

**ステップ 18** すべての回線を作成すると、Circuits ウィンドウが表示されます。ウィンドウに作成した回線が表示されていることを確認します。

**終了**：この手順は、これで完了です。

## NTP-A326 サーバ証跡の作成

目的	この手順では、ONS からサードパーティのネットワーク間の接続を行うサーバ証跡を作成します。2つの光ポート間またはDS-3ポート間にサーバ証跡を作成できます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a>
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 リンクを使用するポートではサーバ証跡を作成できません。

**ステップ 1** 回線を作成するノードで「[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** View メニューから、Go to Network View を選択します。

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

**ステップ 4** Create をクリックします。

**ステップ 5** Server Trail Creation ダイアログボックスで、次のフィールドを設定します。

- Type — VT または STS を選択します。
- Size — 選択したタイプによって、サーバ証跡のサイズを選択します。VT の場合、VT1.5 または VT2 を選択します。STS の場合、STS1、STS-3s、STS-6c、STS-12c、STS-48c、STS-192c から選択します。
- Protection Type — 次の保護タイプのいずれかを選択します。Preemptible、Unprotected、Fully Protected。サーバ証跡の保護では、サーバを通過する回線の保護タイプが設定されます。
- Number of Trails — サーバ証跡の数を入力します。同一ポートから複数のサーバ証跡を作成できます。最大数は、ポート上で特定のサーバ証跡サイズの回線がサポートされる数で決まります（たとえば、1つのOC-12ポートから、12個のSTS-1サーバ証跡を作成できます）。
- SRLG — 共有リソース リンク グループ (SRLG; Shared Resource Link Group) の値を入力します。SRLG は、Cisco Transport Manager (CTM) がリンク ダイバーシティの指定に使用します。SRLG フィールドには制限がありません。1つのポートから複数のサーバ証跡を作成する場合、同一ポートを起点としていることを示すように、すべてのリンクに同じ SRLG 値を割り当てることができます。

**ステップ 6** Next をクリックします。

**ステップ 7** Source 領域で、次の手順を実行します。

- Node ドロップダウン リストから、サーバ証跡の始点にするノードを選択します。
- Slot ドロップダウン リストから、サーバ証跡の始点になるカードが取り付けられているスロットを選択します（伝送容量を使い切っているカードは、リストに表示されません）。

- 送信元カードに応じて、Port リストと STS リストから送信元ポートまたは STS またはその両方を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS は、別の回線によってすでに使用されている場合は、表示されません。

**ステップ 8** Next をクリックします。

**ステップ 9** Destination 領域で、次の手順を実行します。

- Node ドロップダウン リストから宛先ノードを選択します。
- Slot ドロップダウン リストから、サーバ証跡が終端するカード（宛先カード）が入っているスロットを選択します（伝送容量を使い切っているカードは、リストに表示されません）。
- 選択したカードに合わせて、Port ドロップダウン リストと STS ドロップダウン リストから、宛先ポートまたは STS またはその両方を選択します。Port ドロップダウン リストは、カードに複数のポートがある場合にだけ使用できます。表示される STS は、カード、回線のサイズ、および保護方式によって異なります。

**ステップ 10** Finish をクリックします。

終了：この手順は、これで完了です。

---





## 回線の管理

この章では、Cisco ONS 15454 の電気回線、光 (OC-N) 回線、イーサネット回線、および Virtual Concatenated (VCAT; 仮想連結) 回線について、その管理方法を説明します。

### 準備作業

回線の作成については、第 6 章「回線と VT トンネルの作成」を参照してください。

アラームや問題を解決する際には、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A329 回線の検索と表示 \(p.7-2\)](#)— 必要に応じて、この手順を実行します。
2. [NTP-A200 クロスコネク トカードのリソース使用率の表示 \(p.7-3\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A151 回線の変更と削除 \(p.7-5\)](#)— 回線名の編集、アクティブスパンとスタンバイスパンを表す色の変更、Signal Fail (SF; 信号障害) と Signal Degrade (SD; 信号劣化) のスレッシュホールド、復元時間、Unidirectional Path Switch Ring (UPSR; 単方向パススイッチ型リング) 回線の Path Payload Defect Indication (PDI-P; ペイロード障害表示パス) 設定の変更、あるいは VCAT メンバーの追加または削除を行う場合は、必要に応じて、この手順を実行します。
4. [NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除 \(p.7-6\)](#)— トンネルタイプの変更、IP 回線の修復、およびオーバーヘッド回線の削除を行う場合は、必要に応じてこの手順を実行します。
5. [NTP-A78 モニタ回線の作成 \(p.7-7\)](#)— プライマリ側の双方向回線上を流れるトラフィックをモニタする場合は、必要に応じてこの手順を実行します。
6. [NTP-A328 J0 セクショントレースの作成 \(p.7-9\)](#)— 回線トラフィックの中断や変更をモニタする場合は、必要に応じてこの手順を実行します。
7. [NTP-A79 J1 パストレースの作成 \(p.7-11\)](#)— 回線トラフィックの中断や変更をモニタする場合は、必要に応じてこの手順を実行します。
8. [NTP-A293 J2 パストレースの作成 \(p.7-12\)](#)— 回線トラフィックの中断や変更をモニタする場合は、必要に応じてこの手順を実行します。
9. [NTP-A334 トラフィックのブリッジおよびロール \(p.7-15\)](#)— トラフィックをブリッジまたはロールする場合は、必要に応じてこの手順を実行します。
10. [NTP-A298 回線の再設定 \(p.7-16\)](#)— 回線を再設定する場合は、必要に応じてこの手順を実行します。

11. [NTP-A301 回線のマージ \(p.7-17\)](#)— 回線をマージする場合は、必要に応じてこの手順を実行します。
12. [NTP-A325 VLAN の管理 \(p.7-18\)](#)— 必要に応じて実行し、VLAN (仮想 LAN) を表示、作成、または削除します。

## NTP-A329 回線の検索と表示

目的	この手順では、回線とスパニング ツリー情報を検索して表示します。また、Circuits ウィンドウおよび Edit Circuits ウィンドウから回線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	<a href="#">第6章「回線とVTトンネルの作成」</a> の回線作成手順
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** 回線を表示するネットワーク上のノードで「[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。



- (注)** Login ダイアログボックスでは Disable Circuit Management のチェックボックスをオンにしないでください。このオプションのチェックボックスをオンにすると、回線がまったく表示されなくなります。

- ステップ 2** 必要に応じて、「[DLP-A416 回線情報の表示 \(p.21-2\)](#)」を行います。
- ステップ 3** 必要に応じて、「[DLP-A131 回線の検索 \(p.18-15\)](#)」を行います。
- ステップ 4** 必要に応じて、「[DLP-A262 回線表示のフィルタリング \(p.19-48\)](#)」を行います。
- ステップ 5** 必要に応じて、「[DLP-A229 スパンにおける回線の表示 \(p.19-21\)](#)」を行います。
- ステップ 6** 必要に応じて、「[DLP-A454 BLSR STS スケルチ テーブルの表示 \(p.21-38\)](#)」を行います。
- ステップ 7** 必要に応じて、「[DLP-A455 BLSR VT スケルチ テーブルの表示 \(p.21-40\)](#)」を行います。
- ステップ 8** 必要に応じて、「[DLP-A430 スパニングツリー情報の表示 \(p.21-9\)](#)」を行います。
- ステップ 9** 必要に応じて、「[DLP-A532 CTC データのエクスポート \(p.22-35\)](#)」を行います。

終了：この手順は、これで完了です。

## NTP-A200 クロスコネク ト カードのリソース使用率の表示

目的	この手順では、ONS 15454 を経由する回線または終端とする回線で使用しているクロスコネク ト カードのリソース使用率(パーセント)を表示します。
工具 / 機器	XCVT、XC10G、または XC-VXC-10G カードを取り付ける必要があります。
事前準備手順	<a href="#">DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け (p.17-47)</a>
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** クロスコネク ト カードのリソース使用率を表示するノードで、「[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** Maintenance > Cross-Connect > Resource Usage タブをクリックします。

**ステップ 3** Resources Usage タブの Summary 領域に、次の情報が表示されます。

- STS-1 Matrix — クロスコネク ト カードで使用されている STS-1 パス リソースの割合 (パーセント) が表示されます。XCVT カードでは 288 本の STS-1 パスを使用できます。XC10G および XC-VXC-10G カードでは 1152 本の STS-1 パスを使用できます。
- VT Matrix Ports — クロスコネク ト カードで使用されている VT マトリクス ポートの数の割合 (パーセント) が表示されます。各ポートのサイズは STS 1 つ分であり、それぞれ 28 本の VT1.5 回線または 21 本の VT2 回線のトラフィックを伝送できます。XCVT および XC10G カードでは 24 個の VT マトリクス ポートを使用できます。XC-VXC-10G カードでは 96 個の VT マトリクス ポートを使用できます。
- VT Matrix — 使用されている VT マトリクス リソースの割合 (パーセント) が表示されます。XCVT および XC10G カードでは、672 を使用できます (672 は VT マトリクス ポートの個数 [24] に、1 つの STS における VT1.5 の数 [28] を掛けた値です)。XC-VXC-10G の VT マトリクスには、2688 本の VT1.5 終端 (1344 本の VT1.5 双方向回線) または 2016 VT2 終端 (1008 本の VT2 双方向回線) の容量があります。

**ステップ 4** VT Matrix Port Detail セクションでは、VT Matrix Port の使用率の詳細を表示できます。

- Drop — 送信元スロット、ポート、および STS を識別します。
- Tunnel Name — ポートが VT トンネルによって使用されている場合は、そのトンネル名が表示されます。VT トンネルは トンネルの送信元ノードおよび宛先ノードの VT マトリクス ポートを使用します (VT トンネルはパススルー ノードのマトリクス リソースを使用しません)。
- % Used — マトリクス ポートの使用率を示します。たとえば、各マトリクス ポートは 28 本の VT1.5 のトラフィックを伝送できるため、1 つの STS が 7 本の VT1.5 回線のトラフィックを伝送する場合、マトリクス ポートの使用率は 25% になります。
- Usage — ポート使用率を示します。たとえば、1 つの STS が 7 本の VT1.5 回線のトラフィックを伝送する場合、マトリクス ポートは、28 本の VT1.5 回線のうち 7 本が使用されていることを示します。

**ステップ 5** 必要に応じて次の操作を行います。

- 更新された XC Resources ビューを表示する場合は、**Refresh** ボタンをクリックします。たとえば、XC Resources タブを表示しているときに他のユーザが回線を作成した場合、これらの回線が VT マトリクスの使用率に与える影響を表示するには、**Refresh** をクリックします。
- VT マトリクス リソースを使用しているにもかかわらず VT 回線のデータを伝送していない STS を削除する場合は、**Delete** ボタンをクリックします。このような状況は、一定期間に多くの VT 回線を追加、削除した場合にときどき発生します。孤立状態になった STS は、VT Matrix Port Detail 領域に使用率が 0% として表示されます。孤立状態の STS が表示された場合は、その STS をクリックしてから **Delete** をクリックして、VT マトリクス容量を解放します。



(注) Delete ボタンの操作には、スーパーユーザのセキュリティ レベルが必要です。



(注) VT トンネルは、使用容量が 0% の STS として表示されることがあります。これらの STS は削除できません。

終了：この手順は、これで完了です。

## NTP-A151 回線の変更と削除

目的	この手順では、ONS 15454 回線およびトンネルを変更したり、削除したりします。
工具 / 機器	なし
事前準備手順	ネットワーク上に回線が存在している必要があります。回線の作成手順については、第6章「回線とVTトンネルの作成」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	プロビジョニング以上のレベル

- 
- ステップ 1** 変更する回線があるノードで、「[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** 必要に応じて、「[DLP-A230 回線のサービス状態の変更](#)」(p.19-22)を行います。
- ステップ 3** 必要に応じて、「[DLP-A231 回線名の編集](#)」(p.19-24)を行います。
- ステップ 4** 必要に応じて、「[DLP-A232 アクティブ スパンおよびスタンバイ スパンの色の変更](#)」(p.19-25)を行います。
- ステップ 5** 必要に応じて、「[DLP-A233 UPSR 回線パス セレクタの編集](#)」(p.19-26)を行います。
- ステップ 6** 必要に応じて、「[DLP-A263 UPSR DRI 回線ホールドオフ タイマーの編集](#)」(p.19-50)を行います。
- ステップ 7** 必要に応じて、「[DLP-A333 回線の削除](#)」(p.20-23)を行います。
- ステップ 8** 必要に応じて、「[DLP-A437 VCAT メンバーのサービス状態の変更](#)」(p.21-16)を行います。
- ステップ 9** 必要に応じて、「[DLP-A384 VCAT 回線へのメンバーの追加](#)」(p.20-85)を行います。
- ステップ 10** 必要に応じて、「[DLP-A385 VCAT 回線からのメンバーの削除](#)」(p.20-89)を行います。

**終了：**この手順は、これで完了です。

---

## NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除

目的	この手順では、トンネルタイプの変更、IP回線の修復、およびオーバーヘッド回線とサーバ証跡の削除を行います。
工具 / 機器	なし
事前準備手順	ネットワーク上に回線が存在している必要があります。第6章「回線とVTトンネルの作成」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	プロビジョニング以上のレベル



### 注意

回線の削除はサービスに影響するので、保守時間中に作業を行ってください。

- ステップ 1** 回線を削除するネットワーク上のノードで、「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** 必要に応じて、「DLP-A332 トンネルタイプの変更」(p.20-22)を行います。
- ステップ 3** 必要に応じて、「DLP-A336 IP トンネルの修復」(p.20-26)を行います。
- ステップ 4** 必要に応じて、「DLP-A334 オーバーヘッド回線の削除」(p.20-25)を行います。
- ステップ 5** 必要に応じて、「DLP-A453 サーバ証跡の削除」(p.21-38)を行います。

終了：この手順は、これで完了です。

## NTP-A78 モニタ回線の作成

目的	この手順では、モニタ回線を作成します。このモニタ回線は、プライマリ側双方向回線上を流れるトラフィックをモニタするためのものです。
工具 / 機器	なし
事前準備手順	双方向（二方向）回線がネットワーク上に存在している必要があります。回線の作成手順については、第6章「回線とVTトンネルの作成」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	プロビジョニング以上のレベル



(注) モニタ回線と EtherSwitch 回線は一緒に使用できません。



(注) 単方向回線の場合は、テスト機器が接続されているポートへのドロップを作成します。

- ステップ 1** モニタ回線を作成するネットワーク上のノードで「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** View メニューから **Go to Network View** を選択します。
- ステップ 3** Circuits タブをクリックします。
- ステップ 4** モニタリングの対象となる双方向（二方向）回線を選択して、**Edit** をクリックします。
- ステップ 5** 回線名が 44 文字を超えていないことを確認します。モニタ回線の場合は回線名に [MON] が追加されています。回線名が 44 文字を超えている場合、Name フィールドで名前を編集したあと、**Apply** をクリックします。
- ステップ 6** Edit Circuit ウィンドウで、**Monitors** タブをクリックします。

Monitors タブに、回線のモニタリングに使用できるポートが表示されます。



(注) Monitors タブを使用できるのは、この回線のステータスが DISCOVERED になっている場合だけです。

- ステップ 7** Monitors タブで、モニタ送信元ポートを選択します。モニタ回線には、選択したポートからノードに入ってくるトラフィックが表示されます。



(注) 図 7-1 で、DS1-14 カード (DS1-14 のノード 2 に入る回線トラフィックをテストする場合) またはノード 1 の OC-N カード (OC-N カードのノード 1 に入る回線のトラフィックをテストする場合) を選択します。

**ステップ 8** Create Monitor Circuit をクリックします。

**ステップ 9** Circuit Creation ウィザードの Circuit Destination セクションで、モニタする回線の宛先となるノード、スロット、ポート、および必要に応じて STS、VT、または DS1 を選択します。



(注) 図 7-1 では、EC1-12 カードのポート 2 がモニタ回線の宛先になっています。

**ステップ 10** Next をクリックします。

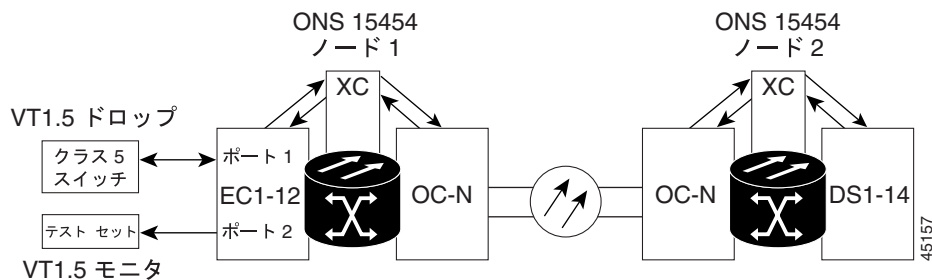
**ステップ 11** Circuit Routing Preferences 領域で、モニタ回線の情報を確認します。モニタ回線が Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) の保護チャンネルを通るようにルートを選択する場合は、Protection Channel Access をクリックします。

**ステップ 12** Finish をクリックします。

**ステップ 13** Edit Circuit ウィンドウで、Close をクリックします。Circuits タブに新しいモニタ回線が表示されません。

図 7-1 に、モニタ回線の設定例を示します。VT1.5 トラフィックは、ノード 1 の EC1-12 カードのポート 1 で受信されます。VT1.5 トラフィックをモニタするには、テスト機器を EC1-12 カードのポート 2 に装着し、ポート 2 に接続されたモニタ回線を CTC でプロビジョニングします (回線のモニタリングは一方方向です)。この例では、回線がすでに作成されていると想定します。

図 7-1 EC1-12 ポートで受信する VT1.5 モニタ回線



終了：この手順は、これで完了です。



## NTP-A328 J0 セクション トレースの作成

目的	この手順では、固定長の繰り返し文字列を作成します。この文字列はノード間のトラフィックの中断または変化をモニタするために使用します。
工具 / 機器	少なくとも、MRC-12 または OC192-XFP のいずれか 1 つが取り付けられている必要があります。
事前準備手順	なし
必須 / 適宜	適宜 (パストレースが設定されている場合は任意)
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** セクション トレースを作成するネットワーク上のノードで、「[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 MRC-12 または OC192-XFP カードをダブルクリックします。
- ステップ 3** Provisioning > Line > Section Trace タブをクリックします。
- ステップ 4** Port ドロップダウン リストからセクション トレース用のポートを選択します。
- ステップ 5** Trace Mode ドロップダウン リストで、Auto または Manual を選択して、セクション トレースの予測文字列をイネーブルにします。
- Auto — 送信元ポートから受信された最初の文字列が、現在の予測文字列として自動的にプロビジョニングされます。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せん。
  - Manual — Current Expected String フィールドに入力された文字列がベースラインになります。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。
- ステップ 6** Section Trace String Size 領域で、1 byte、16 byte、または 64 byte をクリックします。New Transmit String フィールドで、送信する文字列を入力します。入力する文字列は、ノードの IP アドレス、ノード名、その他の文字列など、宛先ポートが容易に識別できるものにします。New Transmit String フィールドを空白のままにしておくと、J0 はヌル文字列を送信します。
- ステップ 7** Section Trace Mode フィールドを Manual に設定した場合、宛先ポートが送信元ポートから受信する文字列を New Expected String フィールドに入力します。Section Trace Mode 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** STS Section Trace Identifier Mismatch Path (TIM-P) アラームが検出された場合に、Alarm Indication Signal (AIS; アラーム表示信号) および Remote Defect Indication (RDI; リモート障害表示) を抑制する場合は、**Disable AIS and RDI if TIM-P is detected** チェックボックスをクリックします。アラームおよび状態の説明については、『Cisco ONS 15454 Troubleshooting Guide』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** セクショントレースを設定すると、Received フィールドに受信した文字列が表示されます。次のオプションを指定します。

- セクショントレースを 16 表記で表示する場合は、**Hex Mode** ボタンをクリックします。ボタンの名前が ASCII Mode に変わります。セクショントレースを ASCII 表記に戻す場合は、このボタンをクリックします。
- ポートから値を再度読み取る場合は、**Reset** ボタンをクリックします。
- セクショントレースのデフォルト設定に戻す場合は、**Default** をクリックします ( Section Trace Mode は Off に、New Transmit String と New Expected String はヌルに設定されます )。

**注意**

---

他端のポートに異なる文字列がプロビジョニングされている場合に Default をクリックすると、アラームが発生します。

---

Section Trace Mode フィールドを Auto または Manual に設定した場合、予測文字列と受信文字列は数秒ごとに更新されます。

**終了：この手順は、これで完了です。**

---

## NTP-A79 J1 パストレースの作成

目的	この手順では、固定長の繰り返し文字列を作成します。この文字列は回線トラフィックの中断または変化をモニタするために使用します。
工具 / 機器	パストレースを送信または受信できる ONS 15454 カードが取り付けられている必要があります。カードのリストは <a href="#">表 19-3 (p.19-52)</a> を参照してください。
事前準備手順	パストレースをプロビジョニングできるのは、OC-N (STS) 回線のみです。OC-N 回線の作成手順については、 <a href="#">第 6 章「回線と VT トンネルの作成」</a> 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	プロビジョニング以上のレベル



(注) TL1 と同様な回線には J1 パストレースを作成できません。

**ステップ 1** パストレースを作成するネットワーク上のノードで、「[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** 必要に応じて、次の作業を行います。

- 必要に応じて、「[DLP-A264 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.19-51) を行います。
- 必要に応じて、「[DLP-A137 OC-N ポートでのパストレースのプロビジョニング](#)」(p.18-16) を行います。

**終了：**この手順は、これで完了です。

## NTP-A293 J2 パス トレースの作成

目的	この手順では、固定長の繰り返し文字列を作成します。この文字列は回線トラフィックの中断または変化をモニタするために使用します。
工具 / 機器	DS3XM-12 カードまたは DS1/E1-56 カード
事前準備手順	DS-3 回線の作成手順については、第6章「回線と VT トンネルの作成」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	プロビジョニング以上のレベル



(注) TL1 と同様な回線には J2 パス トレースを作成できません。



(注) この手順では、双方向回線上にパス トレースを設定することと、回線の送信元および宛先に送信文字列を設定することを前提としています。

**ステップ 1** パス トレースを作成するネットワーク上のノードで、「[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** View メニューから **Go to Network View** を選択します。

**ステップ 3** **Circuits** タブをクリックします。

**ステップ 4** モニタする VT 回線で、送信元ポートと宛先ポートの存在するカードでパス トレースの文字列を送受信できることを確認します。



(注) どちらのポートも送受信カード上に存在しない場合、この手順を完了することはできません。片方のポートが送受信カード上にあり、もう片方が受信専用カード上にある場合、送信文字列を送受信ポートで、受信文字列を受信専用ポートでそれぞれ設定できます。ただし、双方向に送信することはできません。

**ステップ 5** トレースする VT 回線を選択し、**Edit** をクリックします。

**ステップ 6** Edit Circuit ウィンドウで、ウィンドウ下部にある **Show Detailed Map** チェックボックスをクリックします。送信元ポートと宛先ポートの詳細マップが表示されます。

**ステップ 7** 回線の送信元が送信する文字列を、次の手順でプロビジョニングします。

- a. 詳細な回線マップで、回線の送信元ポート（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 J2 Path Trace (port)** を選択します。

- b. New Transmit String フィールドで、回線の送信元が送信する文字列を入力します。入力する文字列は、ノードの IP アドレス、ノード名、回線名、その他の文字列など、送信元のポートが容易に識別できるものにします。New Transmit String フィールドを空白のままにしておくと、J2 はヌル文字列を送信します。
- c. Apply をクリックしてから Close をクリックします。

**ステップ 8** 回線の宛先が送信する文字列を、次の手順でプロビジョニングします。

- a. 詳細な回線マップで、回線の宛先ポートを右クリックし、ショートカット メニューから **Edit Path Trace** を選択します。
- b. New Transmit String フィールドで、回線の宛先から送信する文字列を入力します。入力する文字列は、ノードの IP アドレス、ノード名、回線名、その他の文字列など、宛先ポートが容易に識別できるものにします。New Transmit String フィールドを空白のままにしておくと、J2 はヌル文字列を送信します。
- c. Apply をクリックします。

**ステップ 9** 回線の宛先で受信する予測文字列を、次の手順でプロビジョニングします。

- a. 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 — 送信元ポートから受信された最初の文字列が、現在の予測文字列として自動的にプロビジョニングされます。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。
  - Manual — Current Expected String フィールドに入力された文字列がベースラインになります。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。
- b. Path Trace Mode フィールドを Manual に設定した場合、回線の宛先が回線の送信元から受信する文字列を New Expected String フィールドに入力します。Path Trace Mode 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。
- c. (チェックボックスの表示は選択したカードにより異なります) C2 の不一致が発生したときに AIS を抑制する場合は、**Disable AIS on C2 Mis-Match** チェックボックスをクリックします。
- d. Apply をクリックしてから Close をクリックします。



**(注)** 回線の宛先で受信する予測文字列に関しては、形式 (16 バイトまたは 64 バイト) を設定する必要はありません。パストレースの処理で自動的に形式が判別されるからです。

**ステップ 10** 回線の送信元で受信する予測文字列を、次の手順でプロビジョニングします。

- a. Edit Circuit ウィンドウで (Show Detailed Map を選択して) 回線の送信元ポートを右クリックし、ショートカットメニューから **Edit Path Trace** を選択します。
- b. 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 — ベースライン文字列として、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。
  - 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。

- c. Path Trace Mode フィールドを Manual に設定した場合は、回線の宛先が回線の送信元から受信する文字列を New Expected String フィールドに入力します。Path Trace Mode 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。
- d. (チェックボックスの表示は選択したカードにより異なります) C2 の不一致が発生したときに AIS を抑制する場合は、**Disable AIS on C2 Mis-Match** チェックボックスをクリックします。
- e. **Apply** をクリックします。



(注) 回線の送信元で受信する予測文字列に関しては、形式(16バイトまたは64バイト)を設定する必要はありません。パストレースの処理で自動的に形式が判別されるからです。

**ステップ 11** パストレースを設定すると、パストレース設定ウィンドウの Received フィールドに受信した文字列が表示されます。次のオプションを指定します。

- パストレースを 16 進表記で表示する場合は、**Hex Mode** ボタンをクリックします。ボタンの名前が ASCII Mode に変わります。パストレースを ASCII 表記に戻す場合は、このボタンをクリックします。
- ポートから値を再度読み取る場合は、**Reset** ボタンをクリックします。
- パストレースのデフォルト設定に戻す場合は、**Default** をクリックします (Path Trace Mode は Off に、New Transmit String と New Expected String はヌルに設定されます)。



**注意**

他端のポートに異なる文字列がプロビジョニングされている場合に Default をクリックすると、アラームが発生します。

Path Trace Mode フィールドを Auto または Manual に設定した場合、予測文字列と受信文字列は数秒ごとに更新されます。

**ステップ 12** Close をクリックします。

詳細な回線マップでは、回線の送信元ポートと宛先ポートにパストレースが M (マニュアルパストレース) または A (自動パストレース) という文字で表示されます。

**終了:** この手順は、これで完了です。

## NTP-A334 トラフィックのブリッジおよびロール

目的	この手順では、サービスの中断なしにライブトラフィックを再ルーティングします。Bridge and Roll ウィザードを使用すると、カードの交換やロードバランスなどの機能をメンテナンスできます。回線は1つの送信元ファシリティ、1つ以上の宛先ファシリティ、および中間ファシリティ（パス）で構成されます。
工具 / 機器	なし
事前準備手順	<ul style="list-style-type: none"> <li>• ネットワーク上に回線が存在している必要があります。回線の作成手順については、<a href="#">第6章「回線とVTトンネルの作成」</a>を参照してください。</li> <li>• 保護ポートに回線をルーティングするには、「<a href="#">DLP-A73 1+1 保護グループの作成</a>」(p.17-87)または「<a href="#">NTP-A126 BLSR の作成</a>」(p.5-16)を使用して、保護グループを作成する必要があります。</li> <li>• ロールに2つの回線が関与する場合は、Data Communication Channel (DCC; データ通信チャネル) 接続を確立する必要があります。「<a href="#">DLP-A377 SDCC 終端のプロビジョニング</a>」(p.20-74)を参照してください。</li> <li>• 「<a href="#">NTP-A329 回線の検索と表示</a>」(p.7-2)を使用して、計画した Roll To パスが稼働中であることを確認します。計画した Roll To および Roll From パスが Roll Pending ステータスでなく、テストアクセスまたはループバックに使用されていることを確認します。アラームのクリア方法については、『<a href="#">Cisco ONS 15454 Troubleshooting Guide</a>』を参照してください。</li> </ul>
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)

ブリッジおよびロール機能を使用すると、保護されていない回線を完全に保護された回線にアップグレードしたり、完全に保護された回線を保護されていない回線にダウングレードすることができません。



注意

STS192C でブリッジおよびロールを実行すると、50 ミリ秒以下のトラフィックの中断が発生することがあります。

- ステップ 1** ONS 15454 回線の送信元ノードで「[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** 必要に応じて「[DLP-A463 特定の光回線の送信元または宛先のロール](#)」(p.21-49)を行います。
- ステップ 3** 必要に応じて、「[DLP-A464 光回線間での単一クロスコネクットのロール](#)」(p.21-52)を行います。
- ステップ 4** 必要に応じて、「[DLP-A465 自動ルーティングを使用した単一光回線への2つのクロスコネクットのロール](#)」(p.21-54)または「[DLP-A466 手動ルーティングを使用した単一光回線への2つのクロスコネクットのロール](#)」(p.21-58)を行います。
- ステップ 5** 必要に応じて、「[DLP-A467 光回線間での2つのクロスコネクットのロール](#)」(p.21-61)を行います。

**ステップ6** 必要に応じて、「[DLP-A489 ロールのキャンセル](#)」(p.21-69)を行います。

**ステップ7** 必要に応じて、「[DLP-A468 ロールの削除](#)」(p.21-63)を行います。このオプションを選択する場合は、注意してください。ルールを削除するのは、ルールを完了できないか、またはキャンセルできない場合に限定してください。このオプションが選択されている場合、回線は PARTIAL ステータスになることがあります。

終了：この手順は、これで完了です。

## NTP-A298 回線の再設定

目的	この手順では、回線を作成し直します。この作業は、ステータスが PARTIAL になっている回線が多数ある場合に必要となることがあります。
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71)を実行します。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** Circuits タブをクリックします。

**ステップ3** 再設定する回線を選択します。

**ステップ4** Tools メニューから、Circuits > Reconfigure Circuits を選択します。

**ステップ5** 確認用のダイアログボックスで Yes をクリックして、次へ進みます。

**ステップ6** 通知ボックスで、再設定の結果を表示します。Ok をクリックします。

終了：この手順は、これで完了です。



## NTP-A301 回線のマージ

目的	この手順では、2つの回線をマージします。対象となる回線は、経路的には連続的な1本のパスを形成しているものの、回線IDが異なるかまたはパラメータが競合するために個別の回線として扱われている回線です。マージでは、1本のマスター回線に1本以上の回線を結合します。
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71)を実行します。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** Circuits タブをクリックします。

**ステップ 3** マージのマスター回線として使用する回線をクリックします。

**ステップ 4** Edit をクリックします。

**ステップ 5** Edit Circuit ウィンドウで、Merge タブをクリックします。

**ステップ 6** マスター回線にマージする回線を選択します。

**ステップ 7** Merge をクリックします。

**ステップ 8** 確認用のダイアログボックスで Yes をクリックして、次へ進みます。

**ステップ 9** 通知ボックスで、マージの結果を表示します。Ok をクリックします。

**終了 :** この手順は、これで完了です。

## NTP-A325 VLAN の管理

目的	この手順により、VLAN を表示、作成、または削除できます。
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** Tools メニューから、**Manage VLANs** を選択します。All VLANs ダイアログ ボックスが表示され、ネットワークのすべての VLAN トポロジーが一覧表示されます。

**ステップ 3** 必要に応じて、次の手順を行います。

- VLAN を追加するには、「[DLP-A452 VLAN の作成](#)」(p.21-37) を実行します。
- VLAN を削除するには、「[DLP-A335 VLAN の削除](#)」(p.20-26) を実行します。

**終了：**この手順は、これで完了です。

---



## アラームの管理

この章では、Cisco ONS 15454 でアラームおよび状態を表示および管理する方法について説明します。

Cisco Transport Controller (CTC) では、Cisco ONS 15454 および Optical Networking System (ONS) ネットワークで生成されたアラームを検出して報告します。CTC を使用することで、カード、ノード、またはネットワークの各レベルでアラームをモニタおよび管理できます。LCD 前面パネルにアラーム カウントを表示することもできます。

### 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A195 カード、ノード、およびネットワーク プロビジョニングの説明 \(p.8-2\)](#) — ノードデータを印刷またはエクスポートする場合は、必要に応じてこの手順を実行します。
2. [NTP-A196 アラーム、履歴、イベント、および状態の表示 \(p.8-3\)](#) — ノードに発生しているアラームおよび状態を表示したり、アラームおよび状態の完全なメッセージ履歴を表示したりする場合は、必要に応じてこの手順を実行します。
3. [NTP-A68 クリアされたアラームの表示からの削除 \(p.8-4\)](#) — クリアされたアラームの情報を削除する場合は、必要に応じてこの手順を実行します。
4. [NTP-A69 アラームの影響を受ける回線の表示 \(p.8-5\)](#) — 特定のアラームまたは状態によって影響を受ける回線を見つける場合は、必要に応じてこの手順を実行します。
5. [NTP-A70 ノード、スロット、またはポートの LCD のアラーム カウントの表示 \(p.8-6\)](#) — スロットまたはポートで発生したアラームの統計カウントを表示する場合は、必要に応じてこの手順を実行します。
6. [NTP-A71 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 \(p.8-8\)](#) — 特定のアラームについてデフォルトの重大度を変更したり、ポート、カード、またはノードに新しい重大度を割り当てたり、アラーム プロファイルを削除したりする場合は、必要に応じてこの手順を実行します。
7. [NTP-A168 アラーム重大度フィルタリングのイネーブル化、変更、またはディセーブル化 \(p.8-9\)](#) — Conditions、Alarms、または History 画面に表示されるアラームの重大度フィルタリングをノード レベルまたはネットワーク レベルでイネーブル化、ディセーブル化、または変更する場合は、必要に応じてこの手順を実行します。
8. [NTP-A72 アラーム抑制の開始と中止 \(p.8-10\)](#) — ポート、カード、またはノード レベルでアラームのレポートを抑制したり、抑制コマンドをディセーブルにして通常のアラーム報告を再開したりする場合は、必要に応じてこの手順を実行します。

9. [NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング \(p.8-11\)](#) — Alarm Interface Controller-International (AIC-I) カードに外部アラームおよび制御をプロビジョニングする場合は、必要に応じてこの手順を実行します。

## NTP-A195 カード、ノード、およびネットワーク プロビジョニングの説明

目的	この手順では、Windows でプロビジョニングされているプリンタへ、カード、ノード、およびネットワークの CTC 情報を図または表形式で印刷します。この手順は、ネットワークに関する記録やトラブルシューティングに便利です。
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	<a href="#">第4章「ノードの起動」</a>
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** データを記録または保存しているノードで、「[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** 必要に応じて「[DLP-A531 CTC データの印刷](#)」(p.22-34) を行います。

**ステップ 3** 必要に応じて、「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を行います。

終了：この手順は、これで完了です。

## NTP-A196 アラーム、履歴、イベント、および状態の表示

目的	この手順では、カード、ノード、またはネットワークに現在存在しているアラームおよび状態を表示したり、その履歴を表示したりします。この情報は、ハードウェアとソフトウェアのイベントをモニタしたり、トラブルシューティングしたりする際に役立ちます。
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

- 
- ステップ 1** 表示したいアラーム 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** 必要に応じて、「[DLP-A390 アラームの表示](#)」(p.20-102)を行います。
- ステップ 3** 必要に応じて、「[DLP-A517 アラーム履歴またはイベント履歴の表示](#)」(p.22-9)を行います。
- ステップ 4** 必要に応じて、「[DLP-A111 アラーム履歴のセッション エントリ最大数の変更](#)」(p.18-1)を行います。
- ステップ 5** 必要に応じて、「[DLP-A112 時間帯に合わせたアラームおよび状態の表示](#)」(p.18-3)を行います。
- ステップ 6** 必要に応じて、「[DLP-A113 アラームの同期](#)」(p.18-3)を行います。
- ステップ 7** 必要に応じて、「[DLP-A114 状態の表示](#)」(p.18-4)を行います。

**終了：**この手順は、これで完了です。

---

## NTP-A68 クリアされたアラームの表示からの削除

目的	この手順では、Alarms ウィンドウから、ステータスが「クリア (C)」になっているアラームを削除します。また、CTC の History ウィンドウから一時メッセージを削除します。
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	検索以上のレベル

**ステップ 1** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** ノードレベルで、クリアされているアラームを削除する場合は、次の手順を実行します。

- a. ノード ビューで、Alarms タブをクリックします。
- b. 次の規則を参考にして、Delete Cleared Alarms をクリックします。
  - Autodelete Cleared Alarms チェックボックスがオンになっている場合 — アラームをクリアするとウィンドウから消去されます。
  - Autodelete Cleared Alarms チェックボックスがオンでない場合 — アラームをクリアしても、ウィンドウには表示されたままです。この状態のアラームはウィンドウにホワイトで表示され、重大度としてクリア (C) のマークが付けられています。Delete Cleared Alarms ボタンをクリックすると、このアラームを削除できます。

このアクションによって、Alarms タブから、クリアされているすべての ONS 15454 アラームが削除されます。クリアされたアラームの行は、色がホワイトになるとともに、ステータス (ST) カラムに C と表示されます。

**ステップ 3** カードレベルで、クリアされているアラームを削除する場合は、次の手順を実行します。

- a. ノード ビューで、開きたいカードの図をダブルクリックします。
- b. Alarms タブをクリックし、**ステップ 2** の規則を参考にして Delete Cleared Alarms をクリックします。

**ステップ 4** ネットワークレベルで、クリアされているアラームを削除する場合は、次の手順を実行します。

- a. ノード ビューで、View > Go to Network View をクリックします。
- b. Alarms タブをクリックし、**ステップ 2** の規則を参考にして Delete Cleared Alarms をクリックします。

**ステップ 5** History ウィンドウから一時的なメッセージを削除する場合は、Delete Cleared Alarms をクリックします。一時的なメッセージは単一のメッセージで、発生とクリアのペアではありません (したがって、クリアされたことを示すメッセージもありません)。

**終了:** この手順は、これで完了です。

## NTP-A69 アラームの影響を受ける回線の表示

目的	この手順では、アラームまたは状態によって影響を受ける回線をすべて表示します。
工具 / 機器	なし
事前準備手順	NTP-A196 アラーム、履歴、イベント、および状態の表示 (p.8-3)
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** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。すでにログインしている場合は、**ステップ 2** へ進みます。

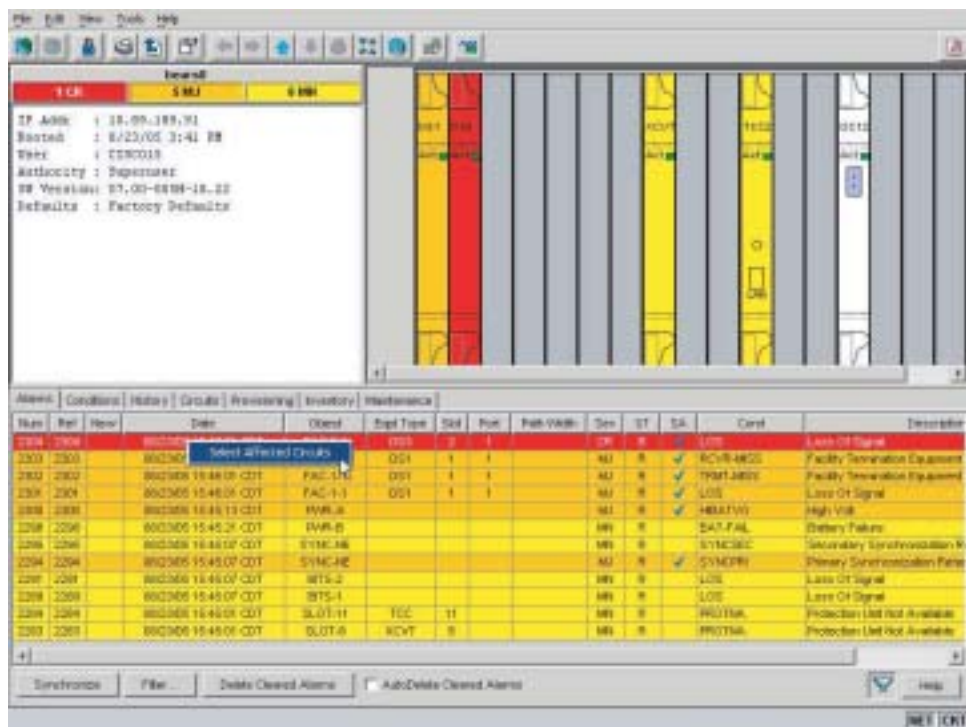
**ステップ 2** ネットワーク、ノード、またはカード ビューで、Alarms タブまたは Conditions タブをクリックし、アクティブなアラームまたは状態の行を右クリックします。行の中であれば、どこをクリックしてもかまいません。



**(注)** デフォルトのビューはノード ビューですが、ネットワーク ビューまたはカード ビューの Alarms タブに移動してステップ 2 を実行することもできます。

ショートカットメニューに Select Affected Circuit オプションが表示されます (図 8-1)。

図 8-1 Select Affected Circuits オプション



**ステップ 3** Select Affected Circuits を左クリックまたは右クリックします。

Circuits ウィンドウが表示され、影響を受ける回線が強調表示されます。

**ステップ 4** 特定の回線を検索する場合は、「[DLP-A131 回線の検索](#)」(p.18-15) を参照してください。

終了：この手順は、これで完了です。

## NTP-A70 ノード、スロット、またはポートの LCD のアラーム カウントの表示

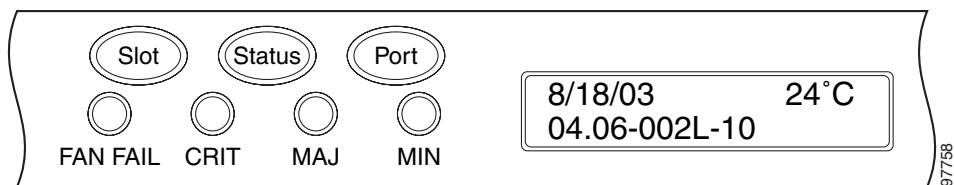
目的	この手順では、CTC を使用しないでノード、スロット、またはポートのアラーム概要を表示します。
工具 / 機器	なし
事前準備手順	なし
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

- ステップ 1** ノードの全体的なアラーム概要を表示する場合は、LCD に [Node] という文字が表示されるまで、LCD パネルの Slot ボタンまたは Port ボタンを押します。そこには、「Status=Alm Ct」という文字も表示されます。ここで、[ステップ 2](#) の指示に従って Status ボタンを押せば、ノードのアラーム カウントを表示できます。
- ステップ 2** ノードに関するアラームと重大度の概要を表示する場合は、Status ボタンを押します。[Alm CT: 2: MJ:2 MN:2] のようなメッセージが表示されます。これは、2 つの Critical アラーム、2 つの Major アラーム、および 2 つの Minor アラームがあることを意味しています。
- ステップ 3** スロット 2 にある OC-3 カードのアラームのように、特定スロットのアラーム カウントを確認する場合は、LCD に [Slot-3] という文字が表示されるまで Slot ボタンを押します。そこには、「Status=Alm Ct」という文字が表示されます。
- ステップ 4** スロットに関するアラームと重大度の概要を表示する場合は、Status ボタンを押します。たとえば、[Slot-3 Alm CT:0 MJ:1 MN:2] のように表示されます。このメッセージは、スロットに Critical アラームはなく、Major アラームが 1 つ、Minor アラームが 2 つあることを意味します。
- ステップ 5** カード上のポートに関するアラームを表示する場合は、Port ボタンを押します。たとえば、以前に表示した OC-3 カード上のポート 3 のアラームを表示する場合は、[Port-3 Status=Alm Ct] という文字が表示されるまで Port ボタンを押します。
- ステップ 6** Status ボタンを押して、ポートのアラーム カウントを表示します。[Port-3 Alm CT:0 MJ:1 MN:0] のようなメッセージが表示されます。このメッセージは、このポートに Major アラームが 1 つあることを意味しています。

 [図 8-2](#) にシェルフの LCD パネルを示します。




図 8-2 シェルフの LCD パネル



Port 画面から前のビューに戻る場合は、スロット上のすべてのポートの表示が一巡するまで **Port** ボタンを押し続けます。たとえば、OC-3 カードで Slot 4 を過ぎるまで Port ボタンを押し続けると、表示が一巡して最初の [Slot] が表示されます。

Slot 画面から ノード メニューに戻る場合は、すべてのスロットが一巡して [Node] が表示されるまで **Slot** ボタンを押し続けます。

どのボタンも押さないと、LCD はデフォルトのノード名を表示した状態に戻ります。ただし、オプションを一巡してノード ステータスに戻らなかった場合は、最後にステータスをチェックしたスロットまたはポートが表示されます。

 **(注)** Alarm Interface Panel (AIP) ボードのヒューズが飛ぶと、LCD はブランクになります。この場合は、次のレベルのサポートに問い合わせます。詳細については、「[テクニカル サポート](#)」(p.xxix) を参照してください。

終了：この手順は、これで完了です。

## NTP-A71 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

目的	この手順では、ネットワーク、ノード、またはカードレベルでアラームのプロファイルを作成し、カスタマイズします。また、ポート、カード、またはノードごとにカスタム重大度を割り当てる方法や、アラームプロファイルを削除する方法を示す作業へのリンクも提供します。
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** アラームのプロファイルを作成するノードで、「[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**へ進んで、アラームのプロファイルを作成、複製、または変更するか、**ステップ 3**へ進んでダウンロードします。
- ステップ 2** 「[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)を実行します。この作業では、現在のアラームプロファイルを複製して新しいプロファイルを作成し、その名前を変更したあと、カスタマイズします。
- ステップ 3** 「[DLP-A524 アラーム重大度プロファイルのダウンロード](#)」(p.22-23)を実行します。この作業では、CDまたはノードからアラーム重大度プロファイルをダウンロードします。



**(注)** 作成またはダウンロードしたアラームプロファイルを格納したあと、そのノードに移動して(そのノードにログインするか、またはネットワークビューからそのノードをクリックする)アラームプロファイルをシェルフ、カード、またはポートに適用して有効にする必要があります。

- ステップ 4** 必要に応じて「[DLP-A519 アラームプロファイルのポートへの適用](#)」(p.22-15)または「[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)を行います。
- ステップ 5** 必要に応じて、「[DLP-A520 アラーム重大度プロファイルの削除](#)」(p.22-17)を行います。

終了：この手順は、これで完了です。

## NTP-A168 アラーム重大度フィルタリングのイネーブル化、変更、またはディセーブル化

目的	この手順では、すべてのネットワーク ノードの Alarms、Conditions、および History の各ウィンドウで、アラーム重大度に対するフィルタリングを開始、変更、または停止します。
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	検索以上のレベル

- 
- ステップ 1** アラーム重大度のフィルタリングをイネーブルにするノードで、「[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** 必要に応じて「[DLP-A225 アラーム フィルタリングのイネーブル化](#)」(p.19-20)を行います。この作業では、ネットワーク内のすべてのノードのカード、ノード、およびネットワーク ビューでアラーム フィルタリングをイネーブルにします。アラーム フィルタリングは、アラーム、状態、またはイベントに対してイネーブルにできます。
- ステップ 3** 必要に応じて「[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](#)」(p.22-18)を行い、ネットワーク ノードのアラーム フィルタリングを変更して、特定のアラームまたは状態を表示または非表示にします。
- ステップ 4** 必要に応じて、「[DLP-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21)を行い、すべてのネットワーク ノードでアラーム プロファイルのフィルタリングをディセーブルにします。

**終了：**この手順は、これで完了です。

---

## NTP-A72 アラーム抑制の開始と中止

目的	この手順では、アラームまたは状態が発生していてもそれらを表示する必要がない場合に、ポート、カード、またはノードからそれらのアラームがレポートされないようにします。また、抑制を中断して通常のアラーム報告を再開する方法を示す作業へのリンクも提供します。
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** ノードに特定のアラームをクリアする自律メッセージを送信させて、Conditions ウィンドウにアラームが表示されないように抑制する場合は、「[DLP-A522 アラーム レポートの抑制](#)」(p.22-21) を行います。



**(注)** アラームを抑制すると、それらのアラームは Alarm ウィンドウや History ウィンドウだけでなく、その他のクライアントにも表示されなくなります。抑制コマンドを実行した場合は、Conditions ウィンドウにそれらのアラームが重大度とサーピスに影響するステータスとともに色分け（重大度別）されて表示されます。

**ステップ 3** アラームの抑制を中止して通常のアラーム報告を再開する場合は、「[DLP-A523 アラーム抑制の中止](#)」(p.22-22) を行います。

**終了：**この手順は、これで完了です。

# NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング

目的	この手順では、AIC-I カードの外部（環境）アラームおよび外部制御を作成します。
工具 / 機器	AIC-I カードがスロット 9 に取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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)

AIC-I カード アラームには、バックプレーンを介してワイヤラップ ピンに配線されるダイレクトアラーム コンタクト（外部アラーム入力および外部制御出力）が備わっています。ワイヤラップピンは、シェルフ背面から取り扱うことができます。Alarm Expansion Panel (AEP) を取り付けた場合は、AIC-I アラーム コンタクトを使用できません。使用できるのは、AEP アラーム コンタクトのみです。AEP の詳細については、「[NTP-A119 AEP の取り付け \(p.1-15\)](#)」および「[NTP-A120 AEP への外付けワイヤラップ パネルの取り付け \(p.1-19\)](#)」を参照してください。



(注)

AIC-I アラーム、制御、および仮想ワイヤの詳細については、『*Cisco ONS 15454 Reference Manual*』を参照してください。

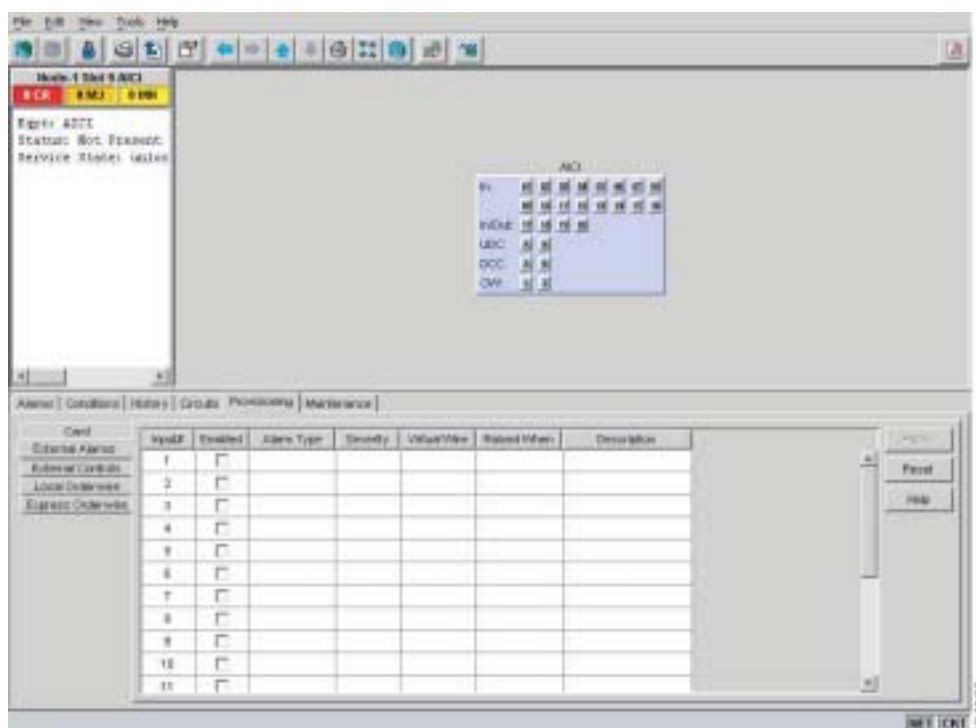
- ステップ 1** 次の手順を実行して、バックプレーンの配線を確認します。AEP を使用している場合は、「[NTP-A119 AEP の取り付け \(p.1-15\)](#)」を参照してください。それ以外の場合は、「[NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線 \(p.1-18\)](#)」で ONS 15454 バックプレーン ピンの情報を参照してください。
- 外部アラームについては、外部デバイス リレー が ENVIR ALARMS IN バックプレーン ピンに配線されていることを確認します。
  - 外部制御については、外部デバイス リレー が ENVIR ALARMS OUT バックプレーン ピンに配線されていることを確認します。
- ステップ 2** 「[DLP-A60 CTC へのログイン \(p.17-71\)](#)」を実行します。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 3** ノード ビューのシェルフ図にある AIC-I 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 4** Provisioning > Card タブをクリックします。
- ステップ 5** AEP を使用している場合は、Alarm Contacts 領域で、Add Extension オプション ボタンをクリックします。このオプションをクリックすると、External Alarm の入出力タイプおよび AEP 拡張タイプが選択されます。16 個の外部アラーム コンタクトにアクセスできます。

**ステップ 6** Add Extension をクリックしなかった場合は、Input/Output 領域で External Alarm または External Control を選択します（ステップ 5 の説明にあるように、External Alarm によって入出力オプションが制限されます）。External Control を選択すると、外部アラームと外部制御が両方もイネーブルになります。これにより 4 つの外部アラーム コンタクトが外部制御に変換され、使用可能な外部制御コンタクト数は 12 になります。両方のオプションの拡張タイプは AEP です。

**ステップ 7** Apply をクリックします。

**ステップ 8** 外部アラームをプロビジョニングしている場合は、External Alarms タブをクリックします（図 8-3）。外部アラームをプロビジョニングしていない場合は、ステップ 9 ~ 11 を省略してステップ 12 へ進みます。

図 8-3 AIC-I カードでの外部アラームのプロビジョニング



**ステップ 9** 外部アラームで次のフィールドを設定します。

- Enabled — アラーム入力番号の各フィールドを有効にする場合は、このチェックボックスをオンにします。
- Alarm Type — ドロップダウン リストからアラームのタイプを選択します。
- Severity — ドロップダウン リストから重大度を選択します。

重大度によって、Alarms タブと History タブに表示されるアラームの重大度と、LED を有効にするかどうかが決まります。Critical (CR)、Major (MJ)、または Minor (MN) アラームを選択すると、LED は有効になります。Not Alarmed (NA) および Not Reported (NR) を選択すると LED は無効になって、CTC の情報だけが報告されます。

- Virtual Wire — 外部デバイスを仮想ワイヤに割り当てる場合は、ドロップダウン リストから仮想ワイヤの番号を選択します。それ以外の場合は、デフォルトの None を変更しないでください。AIC-I の仮想ワイヤについては、『Cisco ONS 15454 Reference Manual』の「Alarms Monitoring and Management」を参照してください。

- Raised When — ドロップダウン リストから、アラームのトリガーとなる接点の条件（オープンまたはクローズ）を選択します。
- Description — デフォルトの説明が表示されます。必要があれば、別の説明を入力します。

**ステップ 10** プロビジョニングするデバイスがほかにもある場合には、それらの各デバイスについて [ステップ 9](#) を実行します。

**ステップ 11** Apply をクリックします。

**ステップ 12** 外部制御の場合は、**External Controls** タブをクリックして、ONS 15454 バックプレーンに接続されている外部制御ごとに次のフィールドを設定します。

- Enabled — アラーム入力番号の各フィールドを有効にする場合は、このチェックボックスをオンにします。
- Control Type — ドロップダウン リストから、エアコン、エンジン、ファン、ジェネレータ、ヒート、ライト、スプリンクラ、またはその他の制御タイプを選択します。
- Trigger Type — ローカル アラーム（Minor、Major、または Critical）、リモート アラーム（Minor、Major、または Critical）、または、仮想ワイヤのアクティブ化から、トリガーの種類を選択します。
- Description — 説明を入力します。

**ステップ 13** 外部制御をプロビジョニングするデバイスがほかにもある場合は、それらの各デバイスについて [ステップ 12](#) を実行します。

**ステップ 14** Apply をクリックします。



**(注)** 外部アラームをプロビジョニングすると、アラーム オブジェクトは ENV-IN-*nm* となります。変数 *nm* は、指定する名前とは関係なく、外部アラームの番号を指します。



**(注)** 作成して名前を付けた環境アラームは、その NE でローカルに記録されます。アラームの名前と解決はノード固有です。

**終了：**この手順は、これで完了です。







# パフォーマンスのモニタリング

この章では、Cisco ONS 15454 の Performance Monitoring (PM; パフォーマンス モニタリング) 統計情報をイネーブルにして、表示する方法を示します。サービス プロバイダーでは、問題を早期に検出するために、PM パラメータを使用して、パフォーマンスデータの収集と保存、スレッシュホールドの設定、およびレポートの作成を行っています。PM の情報、詳細、および定義については、『Cisco ONS 15454 Reference Manual』を参照してください。

## 準備作業

次の手順を実行する前に、すべてのアラームを調べて、問題をすべて解決しておいてください。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A253 PM カウントの表示変更 \(p.9-2\)](#) — 表示する PM カウントを変更する場合は、必要に応じてこの手順を実行します。
2. [NTP-A122 電気回路カードのパフォーマンス モニタリング \(p.9-3\)](#) — 電気回路カードのパフォーマンスをモニタする場合は、必要に応じてこの手順を実行します。
3. [NTP-A198 イーサネット カードのパフォーマンス モニタリング \(p.9-5\)](#) — イーサネット カードのパフォーマンスをモニタする場合は、必要に応じてこの手順を実行します。
4. [NTP-A279 イーサネット RMON スレッシュホールドの作成または削除 \(p.9-6\)](#) — イーサネットの Remote Monitoring (RMON) スレッシュホールドを作成または削除する場合は、必要に応じてこの手順を実行します。
5. [NTP-A250 OC-N カードのパフォーマンス モニタリング \(p.9-7\)](#) — 光カード (OC-N) のパフォーマンスをモニタする場合は、必要に応じてこの手順を実行します。
6. [NTP-A285 FC\\_MR-4 カードのパフォーマンスのモニタリング \(p.9-8\)](#) — FC\_MR-4 カードのパフォーマンスをモニタする場合は、必要に応じてこの手順を実行します。
7. [NTP-A289 FC\\_MR-4 RMON スレッシュホールドの作成または削除 \(p.9-8\)](#) — FC\_MR-4 の RMON スレッシュホールドを作成または削除する場合は、必要に応じてこの手順を実行します。



(注)

PM パラメータの詳細については、Telcordia の GR-1230-CORE、GR-820-CORE、GR-499-CORE、および GR-253-CORE に関するマニュアルおよび ANSI マニュアル『Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring』で、デジタル伝送サーベイランスのセクションを参照してください。

## NTP-A253 PM カウントの表示変更

目的	この手順では、Performance ウィンドウのドロップダウン リストまたはオプション ボタンを選択して、PM カウントの表示を変更します。
工具 / 機器	なし
事前準備手順	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第6章「回線とVT トンネルの作成」と第11章「ノード設定の変更」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	検索以上のレベル

**ステップ 1** モニタするノードで、「[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、PM カウントを表示する電気回路カード、イーサネット カード、または光(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 3** 必要に応じて次の作業を行い、PM カウントの表示を変更します。

- [DLP-A124 15 分間隔で行う PM カウントのリフレッシュ](#) (p.18-11)
- [DLP-A125 1 日間隔で行う PM カウントのリフレッシュ](#) (p.18-12)
- [DLP-A347 E シリーズおよび G シリーズ イーサネット カードの PM カウントのリフレッシュ](#) (p.20-37)
- [DLP-A126 近端側の PM カウントの表示](#) (p.18-13)
- [DLP-A127 遠端側の PM カウントの表示](#) (p.18-13)
- [DLP-A348 選択した信号の PM カウントのモニタ](#) (p.20-38)
- [DLP-A129 現在の PM カウントのリセット](#) (p.18-14)
- [DLP-A349 選択した PM カウントのクリア](#) (p.20-40)
- [DLP-A260 PM カウントの自動リフレッシュ間隔の設定](#) (p.19-46)
- [DLP-A259 イーサネット PM カウントのリフレッシュ間隔の変更](#) (p.19-46)
- [DLP-A261 別ポートの PM カウントのリフレッシュ](#) (p.19-47)

終了：この手順は、これで完了です。

## NTP-A122 電気回路カードのパフォーマンス モニタリング

目的	この手順では、電気回路カードとそのポートについて、指定したインターバルでモニタした近端または遠端のノード パフォーマンスを表示します。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	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第6章「回線とVTトンネルの作成」と第11章「ノード設定の変更」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	検索以上のレベル

**ステップ 1** モニタするノードで、「[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 3](#)へ進みます。

**ステップ 2** DS3XM-12 カードに対して、次の手順を実行します。

- [DLP-A394 DS3XM-12 カード PM パラメータの表示](#) : DS-N/SONET (p.20-108)
- [DLP-A395 DS3XM-12 カード PM パラメータの表示](#) : BFDL (p.20-109)

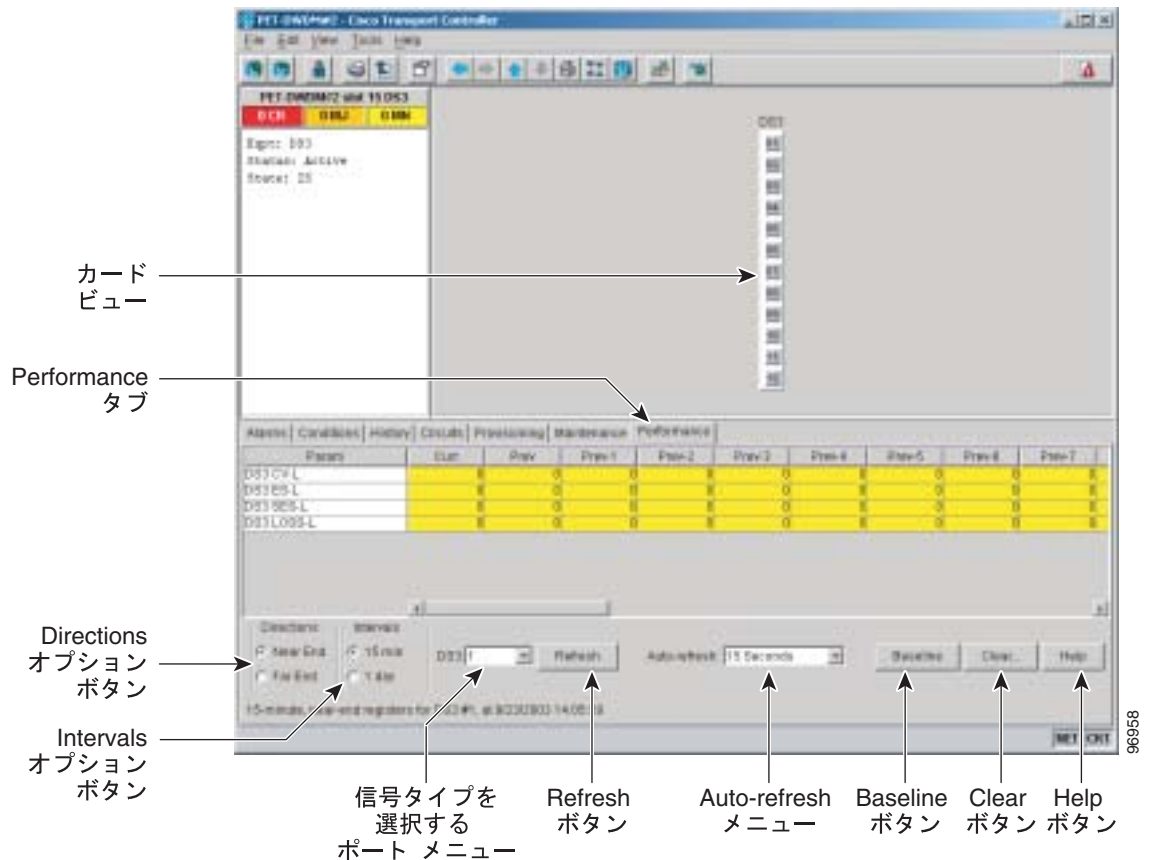
EC-1 カードの場合は、必要に応じて「[DLP-A122 IPPM のイネーブル化またはディセーブル化](#)」(p.18-9)を行い、中間ノードを通る STS トラフィックのモニタリングをイネーブルまたはディセーブルにします。

その他のすべての電気回路カードの場合は、[ステップ 3](#)に進みます。

**ステップ 3** ノード ビューで、PM カウントを表示する電気回路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 4** Performance タブをクリックします ([図 9-1](#))。

図 9-1 電気回路カードの PM 情報の表示



**ステップ 5** 信号タイプを選択するドロップダウン リストで、次のいずれかのオプションをクリックします。

- DS $n$  (カードポート)
- VT $n$  (VTパス)
- STS $n$  (VTパス内のSTS)

**ステップ 6** Refresh をクリックします。

**ステップ 7** 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) カラムと Prev- $n$  (過去) の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。

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-A253 PM カウントの表示変更](#)」(p.9-2)を参照してください。

**終了**：この手順は、これで完了です。

## NTP-A198 イーサネット カードのパフォーマンス モニタリング

目的	この手順では、イーサネット カードとそのポートについて、指定したインターバルでモニタした送信および受信のノード パフォーマンスを表示します。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	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第6章「回線とVTトンネルの作成」と第11章「ノード設定の変更」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
セキュリティ レベル	検索以上のレベル

- 
- ステップ 1** モニタするノードで、「[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** 「[DLP-A256 イーサネット PM パラメータの表示：統計情報](#)」(p.19-44)を実行します。
- ステップ 3** 「[DLP-A257 イーサネット PM パラメータの表示：使用率](#)」(p.19-44)を実行します。
- ステップ 4** 「[DLP-A258 イーサネット PM パラメータの表示：履歴](#)」(p.19-45)を実行します。
- ステップ 5** 「[DLP-A320 ML シリーズ PM パラメータの表示：イーサネット ポート](#)」(p.20-11)を実行します。
- ステップ 6** 「[DLP-A321 ML シリーズ PM パラメータの表示：POS ポート](#)」(p.20-12)を実行します。
- ステップ 7** 「[DLP-A391 CE シリーズ PM パラメータの表示：イーサネット ポートおよび POS ポートの統計情報](#)」(p.20-103)を実行します。
- ステップ 8** 「[DLP-A392 CE シリーズ PM パラメータの表示：イーサネット ポートおよび POS ポートの使用率](#)」(p.20-105)を実行します。
- ステップ 9** 「[DLP-A393 CE シリーズ PM パラメータの表示：イーサネット ポートおよび POS ポートの履歴](#)」(p.20-106)を実行します。

終了：この手順は、これで完了です。

---

## NTP-A279 イーサネット RMON スレッシュホールドの作成または削除

目的	この手順では、ONS 15454 のイーサネット RMON スレッシュホールドを作成または削除します。
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 必要に応じて次の作業を行います。

- [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](#) (p.22-37)
- [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](#) (p.22-32)

**終了** : この手順は、これで完了です。

---

## NTP-A250 OC-N カードのパフォーマンス モニタリング

目的	この手順では、OC-N カードとそのポートについて、指定した時間間隔でモニタした近端または遠端のノード パフォーマンスを表示します。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	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第6章「回線とVT トンネルの作成」と第11章「ノード設定の変更」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	検索以上のレベル

- 
- ステップ 1** モニタするノードで、「[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** 必要に応じて「[DLP-A121 ポインタ位置調整カウンターのPMのイネーブル化またはディセーブル化](#)」(p.18-7)を行い、クロックの同期モニタリングをイネーブルまたはディセーブルにします。
- ステップ 3** 必要に応じて「[DLP-A122 IPPMのイネーブル化またはディセーブル化](#)」(p.18-9)を行い、中間ノードを通る STS トラフィックのモニタリングをイネーブルまたはディセーブルにします。
- ステップ 4** 「[DLP-A507 OC-N PM パラメータの表示](#)」(p.22-1)を実行します。

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-A253 PM カウントの表示変更](#)」(p.9-2)を参照してください。

**終了：**この手順は、これで完了です。

---

## NTP-A285 FC\_MR-4 カードのパフォーマンスのモニタリング

目的	この手順では、FC_MR-4 カードとそのポートについて、指定した時間間隔でモニタした送信および受信のノード パフォーマンスを表示します。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	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第6章「回線とVTトンネルの作成」と第11章「ノード設定の変更」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
セキュリティ レベル	検索以上のレベル

**ステップ 1** モニタするノードで、「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** 「DLP-A350 FC\_MR-4 PM パラメータの表示：統計情報」(p.20-41)を実行します。

**ステップ 3** 「DLP-A351 FC\_MR-4 PM パラメータの表示：使用率」(p.20-42)を実行します。

**ステップ 4** 「DLP-A352 FC\_MR-4 PM パラメータの表示：履歴」(p.20-43)を実行します。

終了：この手順は、これで完了です。

## NTP-A289 FC\_MR-4 RMON スレッシュホールドの作成または削除

目的	この手順では、ONS 15454 の FC_MR-4 RMON スレッシュホールドを作成または削除します。
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** 「DLP-A60 CTC へのログイン」(p.17-71)を実行します。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** 必要に応じて次の作業を行います。

- [DLP-A357 FC\\_MR-4 RMON アラーム スレッシュホールドの作成](#) (p.20-46)
- [DLP-A358 FC\\_MR-4 RMON アラーム スレッシュホールドの削除](#) (p.20-50)

終了：この手順は、これで完了です。





# カードの設定変更

この章では、Cisco ONS 15454 カードの回線プロビジョニング、スレッシュホールド、サービス状態、および回線レートの変更方法について説明します。

## 準備作業

次の手順を実行する前に、すべてのアラームを調べて、問題をすべて解決しておいてください。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A88 電気回路カードを対象にした回線設定と PM パラメータ スレッシュホールドの変更 \(p.10-2\)](#)— すべての電気回路カード (EC-1、DS-1、DS-3、DS3i-N-12、および DS3XM) について回線とスレッシュホールドの設定を変更する場合は、必要に応じてこの手順を実行します。
2. [NTP-A89 光カードを対象にした回線設定と PM パラメータ スレッシュホールドの変更 \(p.10-3\)](#)— すべての光カードについて回線とスレッシュホールドの設定を変更する場合は、必要に応じてこの手順を実行します。
3. [NTP-A118 AIC-I カードの設定変更 \(p.10-4\)](#)— 外部アラームおよび制御とオーダーワイヤの設定を変更する場合は、必要に応じてこの手順を実行します。
4. [NTP-A91 DS-1 および DS-3 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 \(p.10-5\)](#)— DS-1 カードまたは DS-3 カード上で保護タイプを変更する場合は、必要に応じてこの手順を実行します。
5. [NTP-A315 FC\\_MR-4 カードを対象にしたポート設定と PM パラメータ スレッシュホールドの変更 \(p.10-6\)](#)— FC\_MR-4 カードのポートとスレッシュホールドの設定を変更する場合は、必要に応じてこの手順を実行します。
6. [NTP-A321 カードまたは PPM のサービス状態の変更 \(p.10-7\)](#)— カードまたは Pluggable Port Module (PPM) のサービス状態を変更する場合は、必要に応じてこの手順を実行します。
7. [NTP-A322 PPM の管理 \(p.10-8\)](#)— マルチレート PPM のプロビジョニング、光回線レートの割り当てや変更、および PPM の削除を行う場合は、必要に応じてこの手順を実行します。

## NTP-A88 電気回路カードを対象にした回線設定と PM パラメータ スレッシュホールドの変更

目的	この手順では、電気回路カードの回線および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	NTP-A17 電気回路カードの取り付け (p.2-11)
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

カードの設定変更は、サービスに影響することがあります。すべての変更は、スケジュールされた保守時間中に行ってください。

**ステップ 1** 電気回路カードの設定を変更するノードで、「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** 必要に応じて「NTP-A108 データベースのバックアップ」(p.15-6)を行います。

**ステップ 3** 必要に応じて次の作業を行います。

- DLP-A165 DS1-14 または DS1N-14 カードの回線およびスレッシュホールドの設定変更 (p.18-31)
- DLP-A166 DS3-12 または DS3N-12 カードの回線およびスレッシュホールドの設定変更 (p.18-35)
- DLP-A167 DS3E-12 または DS3N-12E カードの回線およびスレッシュホールドの設定変更 (p.18-39)
- DLP-A168 DS3XM-6 カードの回線およびスレッシュホールドの設定変更 (p.18-43)
- DLP-A387 DS3XM-12 カードの回線およびスレッシュホールドの設定変更 (p.20-94)
- 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 (p.22-25)
- DLP-A388 DS3/EC1-48 カードの回線およびスレッシュホールドの設定変更 (p.20-98)
- DLP-A169 EC1-12 カードの回線およびスレッシュホールドの設定変更 (p.18-47)
- DLP-A376 DS1/E1-56 カードの回線およびスレッシュホールドの設定変更 (p.20-68)

**ステップ 4** 必要に応じて、「NTP-A108 データベースのバックアップ」(p.15-6)を行います。

終了：この手順は、これで完了です。

## NTP-A89 光カードを対象にした回線設定と PM パラメータ スレッシュホールドの変更

目的	この手順では、光カード (OC-N) の回線および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	<a href="#">NTP-A16 光カードおよびコネクタの取り付け (p.2-8)</a>
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

カードの設定変更は、サービスに影響することがあります。すべての変更は、スケジュールされた保守時間中に行ってください。

**ステップ 1** OC-N カードの設定を変更するノードで、「[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** 必要に応じて「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A379 OC-N カードの回線の伝送設定の変更](#) (p.20-78)
- [DLP-A171 OC-N カードのスレッシュホールドの設定変更](#) (p.18-50)
- [DLP-A459 OC-192 および MRC-12 カードの光スレッシュホールド設定の変更](#) (p.21-44)
- [DLP-A527 OC-N カード ALS メンテナンス設定の変更](#) (p.22-29)
- [DLP-A172 SDH への光ポートの変更](#) (p.18-52)

**ステップ 4** 必要に応じて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。

終了：この手順は、これで完了です。

## NTP-A118 AIC-I カードの設定変更

目的	この手順では、バックプレーンに配線された外部デバイスからの入力を受信したり、この外部デバイスへ出力を送信するように、Alarm Interface Controller-International (AIC-I) カードをプロビジョニングします (外部アラームや外部制御、または環境アラームといいます)。オーダーワイヤ設定も変更します。
工具 / 機器	なし
事前準備手順	NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング (p.8-11)  DLP-A83 オーダーワイヤのプロビジョニング (p.17-91)
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** AIC-I カードの設定を変更するノードで、「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** 必要に応じて「NTP-A108 データベースのバックアップ」(p.15-6) を行います。

**ステップ 3** 必要に応じて次の作業を行います。

- DLP-A208 AIC-I カードを使用した外部アラームの変更 (p.19-7)
- DLP-A209 AIC-I カードを使用した外部制御の変更 (p.19-8)
- DLP-A210 AIC-I カード オーダーワイヤ設定の変更 (p.19-8)

**ステップ 4** 必要に応じて、「NTP-A108 データベースのバックアップ」(p.15-6) を行います。

**終了** : この手順は、これで完了です。

## NTP-A91 DS-1 および DS-3 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

目的	この手順では、DS-1 および DS-3 保護カードを 1:1 保護から 1:N 保護に変換します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A71 1:1 保護グループの作成 (p.17-85)</a>
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** DS-1 カードと DS-3 カードを 1:1 保護から 1:N 保護に変更するノードで、「[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** 必要に応じて「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A176 DS1-14 カードの 1:1 保護から 1:N 保護への変換 \(p.18-53\)](#)
- [DLP-A177 DS3-12 カードの 1:1 保護から 1:N 保護への変換 \(p.18-55\)](#)
- [DLP-A178 DS3-12E カードの 1:1 保護から 1:N 保護への変換 \(p.18-57\)](#)
- [DLP-A448 DS3XM-6 カードまたは DS3XM-12 カードの 1:1 保護から 1:N 保護への変換 \(p.21-30\)](#)

**ステップ 4** 必要に応じて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。

**終了 :** この手順は、これで完了です。

## NTP-A315 FC\_MR-4 カードを対象にしたポート設定と PM パラメータ スレッシュホールドの変更

目的	この手順では、FC_MR-4 カードを含む Storage Area Network (SAN; ストレージ エリア ネットワーク) カードの回線およびスレッシュホールド設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A274 FC_MR-4 カードの取り付け (p.2-15)</a>
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

カードの設定変更は、サービスに影響することがあります。すべての変更は、スケジュールされた保守時間中に行ってください。

- 
- ステップ 1** OC-N カードの設定を変更するノードで、「[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** 必要に応じて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。
- ステップ 3** 必要に応じて次の作業を行います。
- [DLP-A438 FC\\_MR-4 カードにある汎用ポートの設定変更](#) (p.21-17)
  - [DLP-A439 FC\\_MR-4 カードにあるポートの距離延長設定の変更](#) (p.21-19)
  - [DLP-A440 FC\\_MR-4 カードにあるポートの拡張 FC/FICON 設定の変更](#) (p.21-21)
  - [DLP-A357 FC\\_MR-4 RMON アラーム スレッシュホールドの作成](#) (p.20-46)
  - [DLP-A358 FC\\_MR-4 RMON アラーム スレッシュホールドの削除](#) (p.20-50)
- ステップ 4** 必要に応じて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6)を行います。
- 終了** : この手順は、これで完了です。
-

## NTP-A321 カードまたは PPM のサービス状態の変更

目的	この手順では、カードまたはポートのサービス状態を変更します。この状態は自律生成され、ポートの全体的な状態を表します。
工具 / 機器	なし
事前準備手順	第 2 章「カードおよび光ファイバケーブルの取り付け」
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) OC192-XFP および MRC-12 カードでは、PPM は光ポートと同等です。

- ステップ 1** カードのサービス状態を変更するノードで、「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 2** ノード ビューで、**Inventory** タブをクリックします。
- ステップ 3** 変更したいカードまたは PPM の Admin State ドロップダウン リストから、**IS** (In-Service) または **OOS,MT** (Out-of-Service,Maintenance) のいずれかの Admin state を選択します。
- ステップ 4** **Apply** をクリックします。
- ステップ 5** カードの状態が現在の状態から変更できないことを示すエラー メッセージが表示されたら、**OK** をクリックします。

選択した Admin State に応じて、カードまたはポート /PPM は異なるサービス状態に遷移します。サービス状態およびカード状態の遷移については、『*Cisco ONS 15454 Reference Manual*』の付録「Administrative and Service States」を参照してください。

**終了**：この手順は、これで完了です。

## NTP-A322 PPM の管理

目的	この手順では、MRC-12 および OC192-XFP カードを対象とした PPM のプロビジョニング、変更、および削除を行います (OC-192XFP はシングルレート PPM であるため、削除のみを実行できます)。
工具 / 機器	なし
事前準備手順	DLP-A461 SFP または XFP デバイスの事前プロビジョニング (p.21-47) または DLP-A469 GBIC または SFP/XFP デバイスの取り付け (p.21-64)
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 のプロビジョニング、変更、または削除を行うノードで「[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** View メニューから **Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかない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。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。
  - 「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) 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 4** 必要に応じて、「[DLP-A444 MRC-12 カードでの PPM のプロビジョニング](#)」(p.21-27) を行います。シングルレート PPM ではプロビジョニングは不要です。
- ステップ 5** 必要に応じて「[DLP-A445 MRC-12 カードでの光回線レートのプロビジョニング](#)」(p.21-28) を行い、OC-3、OC-12、または OC-48 回線レートをマルチレート PPM に割り当てます。
- ステップ 6** 必要に応じて「[DLP-A446 MRC-12 カードでの光回線レートの変更](#)」(p.21-29) を行い、マルチレート PPM の回線レートを変更します。シングルレート PPM の光回線レートは変更できません。
- ステップ 7** 必要に応じて、「[DLP-A447 MRC-12 または OC192-XFP カードからの PPM の削除](#)」(p.21-29) を行います。

終了：この手順は、これで完了です。

---





# ノード設定の変更

この章では、Cisco ONS 15454 のノード プロビジョニングを変更する方法について説明します。新しいノードをプロビジョニングする場合は、第4章「ノードの起動」を参照してください。ネットワーク要素のデフォルト設定を変更して、これらの設定を表示する場合は、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。

## 準備作業

次の手順を実行する前に、すべてのアラームを調べて、問題をすべて解決しておいてください。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A81 ノード管理情報の変更 \(p.11-2\)](#)— ノード名、連絡先情報、緯度、経度、日付、時刻、およびログイン時の法的免責事項の説明を変更する場合は、必要に応じてこの手順を実行します。
2. [NTP-A201 CTC ネットワーク アクセスの変更 \(p.11-3\)](#)— IP アドレス、デフォルトルータ、サブネットマスク、ネットワーク構成の設定、およびスタティックルートを変更する場合は、必要に応じてこの手順を実行します。
3. [NTP-A319 OSI プロビジョニングの変更 \(p.11-4\)](#)— Open Systems Interconnection (OSI; 開放型システム間相互接続)ルーティングモード、Target Identifier Address Resolution Protocol (TARP)、ルータ、サブネット、IP over OSI トンネルなど、OSI パラメータを変更する場合は、必要に応じてこの手順を実行します。
4. [NTP-A202 CTC ネットワーク ビューのカスタマイズ \(p.11-5\)](#)— ドメインを作成したりネットワークマップの体裁をカスタマイズしたりする場合は、必要に応じてこの手順を実行します。これらの手順には、異なるデフォルトマップの指定、ドメインの作成、独自マップやイメージの選択、リンクの統合、グローバルおよびローカルのドメイン設定のトグル、背景色の変更などが含まれています。
5. [NTP-A203 カード保護設定の変更または削除 \(p.11-6\)](#)— 必要に応じて、この手順を実行します。
6. [NTP-A292 通信チャンネルの終端とプロビジョニング可能なパッチコードの変更または削除 \(p.11-7\)](#)— Section DCC (SDCC) または Line DCC (LDCC) の終端あるいはプロビジョニング可能なパッチコードを変更または削除する場合は、必要に応じてこの手順を実行します。
7. [NTP-A85 ノードのタイミング変更 \(p.11-8\)](#)— 必要に応じて、この手順を実行します。

8. [NTP-A205 ユーザの変更とセキュリティの変更 \(p.11-9\)](#)— セキュリティ レベルやセキュリティ ポリシーを含むユーザ設定を変更したり、Remote Authentication Dial In User Service (RADIUS) サーバ設定を変更したり、ユーザを削除したりする場合は、必要に応じてこの手順を実行します。
9. [NTP-A87 SNMP の設定変更 \(p.11-10\)](#)— 必要に応じて、この手順を実行します。

## NTP-A81 ノード管理情報の変更

目的	この手順では、ノード名、日付、時刻、連絡先情報、またはログイン時の法的免責事項の説明を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A25 名前、日付、時刻、連絡先情報の設定 (p.4-6)</a>
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-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
  - ステップ 3** 必要に応じて、「[DLP-A140 ノード名、日付、時刻、および連絡先情報の変更](#)」(p.18-17) を行います。
  - ステップ 4** 必要に応じて、「[DLP-A265 ログイン時の法的免責事項の説明の変更](#)」(p.19-56) を行います。
  - ステップ 5** 変更内容を確認したら、「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

終了：この手順は、これで完了です。

---

## NTP-A201 CTC ネットワーク アクセスの変更

目的	この手順では、IP の設定、スタティック ルート、および Open Shortest Path First (OSPF) オプションといった基本的なネットワーク情報を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A169 CTC ネットワーク アクセスの設定 (p.4-9)</a>
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)

IP アドレッシングの例、スタティック ルートのシナリオ、OSPF プロトコルや Routing Information Protocol (RIP) のオプションなど、ONS 15454 のネットワーキングに関するその他の情報と手順については、『Cisco ONS 15454 Reference Manual』を参照してください。

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A266 IP 設定の変更](#) (p.19-57)
- [DLP-A142 スタティック ルートの変更](#) (p.18-18)
- [DLP-A143 スタティック ルートの削除](#) (p.18-18)
- [DLP-A144 OSPF のディセーブル化](#) (p.18-19)
- [DLP-A250 OSPF プロトコルの設定または変更](#) (p.19-39)
- [DLP-A382 プロキシ トンネルの削除](#) (p.20-84)
- [DLP-A383 ファイアウォール トンネルの削除](#) (p.20-84)
- [DLP-A434 ノード セキュリティのロック](#) (p.21-12)
- [DLP-A435 セキュア モードのバックプレーン ポートの IP 設定の修正](#) (p.21-13)
- [DLP-A436 ノードのセキュリティ モードのディセーブル化](#) (p.21-14)

**ステップ 4** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

終了：この手順は、これで完了です。

## NTP-A319 OSI プロビジョニングの変更

目的	この手順では、OSI ルーティング モード、TARP、ルータ、サブネット、および IP over CLNS トンネルなど、ONS 15454 の OSI パラメータを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A318 OSI のプロビジョニング (p.4-17)</a>
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 に実装されている OSI 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 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A535 TARP 動作パラメータのプロビジョニングまたは変更](#) (p.22-45)
- [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](#) (p.22-47)
- [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](#) (p.22-48)
- [DLP-A538 TARP MAT エントリの追加](#) (p.22-48)
- [DLP-A543 TARP MAT エントリの削除](#) (p.22-53)
- [DLP-A544 OSI ルーティング モードの変更](#) (p.22-54)
- [DLP-A545 OSI ルータ設定の編集](#) (p.22-55)
- [DLP-A546 OSI サブネットワーク接続ポイントの編集](#) (p.22-56)
- [DLP-A547 IP-Over-CLNS トンネルの編集](#) (p.22-57)
- [DLP-A548 IP-Over-CLNS トンネルの削除](#) (p.22-58)

**ステップ 4** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

終了：この手順は、これで完了です。

## NTP-A202 CTC ネットワーク ビューのカスタマイズ

目的	この手順では、Cisco Transport Controller( CTC )のネットワーク ビューを変更します。各ノードをドメイン別にグループ化して見やすくしたり、ネットワーク ビューの背景色を変更したり、ネットワーク ビューの背景にカスタム イメージを使用したりすることができます。
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** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** 必要に応じて、次の作業を行います。

- [DLP-A145 ネットワーク ビューの背景色の変更 \( p.18-19 \)](#)
- [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 \( p.22-31 \)](#)
- [DLP-A268 ネットワーク ビューへのカスタム背景マップの適用 \( p.19-58 \)](#)
- [DLP-A148 ドメイン アイコンの作成 \( p.18-20 \)](#)
- [DLP-A149 ドメイン アイコンの管理 \( p.18-21 \)](#)
- [DLP-A269 ダイアログボックス非表示オプションのイネーブル化 \( p.19-59 \)](#)
- [DLP-A498 TDM と DWDM のネットワーク ビューの切り替え \( p.21-73 \)](#)
- [DLP-A495 ネットワーク ビューでのリンクの統合 \( p.21-69 \)](#)

**終了 :** この手順は、これで完了です。

## NTP-A203 カード保護設定の変更または削除

目的	この手順では、カード保護の設定を変更または削除します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A324 保護グループの作成 (p.4-12)</a>
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

保護グループの変更や削除はサービスに影響することがあります。

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A150 1:1 保護グループの変更](#) (p.18-22)
- [DLP-A152 1:N 保護グループの変更](#) (p.18-23)
- [DLP-A154 1+1 保護グループの変更](#) (p.18-24)
- [DLP-A35 最適化 1+1 保護グループの変更](#) (p.17-43)
- [DLP-A155 保護グループの削除](#) (p.18-25)

**ステップ 4** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**終了** : この手順は、これで完了です。

## NTP-A292 通信チャネルの終端とプロビジョニング可能なパッチコードの変更または削除

目的	この手順では、ONS 15454 の SDCC または LDCC 終端を変更または削除します。また、ONS 15454 でプロビジョニング可能なパッチコードを削除します。
工具 / 機器	なし
事前準備手順	DLP-A377 SDCC 終端のプロビジョニング (p.20-74) または DLP-A378 LDCC 終端のプロビジョニング (p.20-77) または DLP-A367 プロビジョニング可能なパッチコードの作成 (p.20-56)
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



### 注意

Data Communications Channel (DCC; データ通信チャネル) の終端を削除すると、DCC がほかに設定されていないノードや、CTC コンピュータにネットワークで接続されていないノードが見えなくなります。

**ステップ 1** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** 必要に応じて次の作業を行い、DCC 設定を変更します。

- DLP-A374 SDCC 終端の変更 (p.20-66)
- DLP-A375 LDCC 終端の変更 (p.20-67)

**ステップ 3** 必要に応じて次の作業を行い、DCC 終端を削除します。

- DLP-A156 SDCC 終端の削除 (p.18-25)
- DLP-A359 LDCC 終端の削除 (p.20-50)

**ステップ 4** 必要に応じて、「DLP-A368 プロビジョニング可能なパッチコードの削除」(p.20-58) を行います。

終了：この手順は、これで完了です。

## NTP-A85 ノードのタイミング変更

目的	この手順では、ONS 15454 に設定されている SONET タイミングを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A28 タイミングの設定 (p.4-11)</a>
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

内部タイミングは Stratum 3 なので、一時的にしか使用しません。ONS 15454 のタイミングは、すべて Stratum 2 以上のプライマリ基準ソースに合わせる必要があります。

- 
- ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 3** 必要に応じて、「[DLP-A157 ノードのタイミングソースの変更](#)」(p.18-26) を行います。
- ステップ 4** 内部タイミングの設定を変更する場合は、変更する設定について「[DLP-A70 内部タイミングの設定](#)」(p.17-84) を参照してください。
- ステップ 5** Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング) または Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) からノードを削除したあとにタイミングの確認が必要な場合は、「[DLP-A195 縮小されたリングで使用されているタイミングの確認](#)」(p.18-66) を参照してください。
- ステップ 6** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

終了 : この手順は、これで完了です。

---



## NTP-A205 ユーザの変更とセキュリティの変更

目的	この手順では、ONS 15454 のユーザ プロパティとセキュリティ プロパティを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A30 ユーザの作成とセキュリティの割り当て (p.4-5)</a>
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A462 アクティブ ログインの表示および終了](#) (p.21-48)
- [DLP-A271 セキュリティ ポリシーの変更：単一ノード](#) (p.19-60)
- [DLP-A272 セキュリティ ポリシーの変更：複数ノード](#) (p.19-61)
- [DLP-A512 ノード アクセスと PM クリア権限の変更](#) (p.22-5)
- [DLP-A457 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](#) (p.21-43)
- [DLP-A158 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](#) (p.18-27)
- [DLP-A160 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](#) (p.18-29)
- [DLP-A159 ユーザの削除：単一ノード](#) (p.18-28)
- [DLP-A161 ユーザの削除：複数ノード](#) (p.18-30)
- [DLP-A456 ノードへの RADIUS 認証の設定](#) (p.21-41) — この作業には、RADIUS サーバの変更や削除に関する説明が含まれています。

**ステップ 4** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**終了：**この手順は、これで完了です。

## NTP-A87 SNMP の設定変更

目的	この手順では、ONS 15454 の SNMP (簡易ネットワーク管理プロトコル) 設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A256 SNMP の設定 (p.4-15)</a>
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-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 必要に応じて次の作業を行います。

- [DLP-A273 SNMP トラップ宛先の修正](#) (p.19-63)
- [DLP-A163 SNMP トラップ宛先の削除](#) (p.18-30)

**ステップ 4** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

終了：この手順は、これで完了です。

---



# カードとスパンのアップグレード

この章では、共通コントロールカード（DS3-12 と DS3N-12 カード）および Cisco ONS 15454 の光スパンをアップグレードする方法について説明します。

## 準備作業

この章では次の NTP（手順）について説明します。適用する DLP（作業）については、各手順を参照してください。

1. [NTP-A220 XCVT カードから XC10G カードへのアップグレード \(p.12-2\)](#)— 必要に応じて、この手順を実行します。
2. [NTP-A333 XCVT/XC10G カードから XC-VXC-10G カードへのアップグレード \(p.12-4\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A296 TCC2 カードから TCC2P カードへのアップグレード \(p.12-6\)](#)— 必要に応じて、この手順を実行します。
4. [NTP-A93 DS3-12 カードから DS3-12E カードへのアップグレード \(p.12-8\)](#)— 必要に応じて、この手順を実行します。
5. [NTP-A308 低密度電気回路カードから高密度電気回路カードへのアップグレード \(p.12-10\)](#)— 1:N 設定の低密度カードを高密度カードにアップグレードする場合は、必要に応じてこの手順を実行します。
6. [NTP-A254 DS3-12E/DS3NE カードから DS3-12/DS3N-12 カードへのダウングレード \(p.12-14\)](#)— DS3E カードをダウングレードしたり、DS3-12 から DS3-12E カードへのアップグレードを取り消す場合は、必要に応じてこの手順を実行します。
7. [NTP-A94 OC-N カードおよびスパンの自動アップグレード \(p.12-16\)](#)— Unidirectional Path Switched Ring (UPSR; 単方向バス スイッチ型リング)、Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング)、および 1+1 保護グループ内の OC-N カードをアップグレードする場合は、必要に応じてこの手順を実行します。
8. [NTP-A95 OC-N スパンの手動アップグレード \(p.12-20\)](#)— スパンアップグレードウィザードのエラーを回復したり、スパンアップグレードを取り消したりする（ダウングレードする）場合は、必要に応じて、この手順を実行します。

## NTP-A220 XCVT カードから XC10G カードへのアップグレード

目的	この手順では、XCVT カードを XC10G カードへアップグレードします。
工具 / 機器	XC10G カード (2)
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
セキュリティ レベル	メンテナンス以上のレベル



**注意**

アップグレードには、必ずスタンバイ側のクロスコネクタカードを使用してください。ロックアウトが設定されていない状態でアクティブ側のクロスコネクタカードを取り外すと、保護切り替えが発生します。スタンバイカードのアップグレードでは、ロックアウトが不要です。



**(注)**

XC10G には、15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリが必要です。



**(注)**

ノードに E100T-12 または E1000-2 カードが取り付けられている場合は、クロスコネクタカードをアップグレードしたときに UNEQ-P アラームが表示されます。アラームは、数秒間表示されてからクリアされます。



**(注)**

アップグレード手順の実行中に相互接続機器障害アラームが表示されることがありますが、アップグレードの手順が完了してノードに対応するクロスコネクタカードが取り付けられると、クリアされます。



**(注)**

XC10G カードから XCVT カードへのダウングレードはサポートされておりません。詳細については、Cisco Technical Assistance Center (TAC) にお問い合わせください (「[テクニカル サポート](#)」 [p.xxix] を参照)。

- ステップ 1** アップグレードを実行するノードで「[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** 現地の状況に合わせて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 3** スタンバイ側の XCVT カードを特定します。スタンバイ XCVT カードの ACT/STBY LED はオレンジで、アクティブ XCVT カードの ACT/STBY LED はグリーンです。

**ステップ 4** ONS 15454 のスタンバイ XCVT カードを XC10G カードに交換します。

- a. XCVT カードのイジェクタを開きます。
- b. カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。
- c. XC10G カードのイジェクタを開きます。
- d. XC10G カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- e. イジェクタを閉じます。



**(注)** XC10G カードでは、ACT/STBY LED の上にある FAIL LED がレッドになり、しばらく (20 ~ 30 秒) 点滅してから消えます。ACT/STBY LED はオレンジになり、点灯したままになります。ノード ビューでは、XC10G はスタンバイ XCVT として表示されます。

**ステップ 5** ノード ビューで、Maintenance > Cross-Connect タブをクリックします。

**ステップ 6** Cross Connect Cards メニューから、Switch を選択します。

**ステップ 7** Confirm Switch ダイアログボックスで Yes をクリックします。トラフィックが、**ステップ 4** で装着した XC10G カードに切り替わります。このカードの ACT/STBY LED がオレンジからグリーンに変わります。

**ステップ 8** ONS 15454 からスタンバイ XCVT カードを物理的に取り外し、2 枚めの XC10G カードを空き XCVT カード スロットに挿入します。

- a. XCVT カードのイジェクタを開きます。
- b. XCVT カードをスライドさせてスロットから外します。
- c. XC10G カードのイジェクタを開きます。
- d. XC10G カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- e. イジェクタを閉じます。

2 枚めの XC10G カードが起動してスタンバイ XC10G カードになれば、アップグレードは完了です。ノード ビューのアクティブカードおよびスタンバイカードが、XC10G に変更されます。



**(注)** 最初のカードを変更しても、CTC では引き続き、両方のスロットで XCVT カードが表示されます。XC10G カードを反映するように表示を変更するには、2 枚めのカードをアップグレードし、このスロット内の XC10G カードを起動する必要があります。

**終了：**この手順は、これで完了です。

# NTP-A333 XCVT/XC10G カードから XC-VXC-10G カードへのアップグレード

目的	この手順では、XCVTまたはXC10GカードからXC-VXC-10Gカードにアップグレードします。
工具 / 機器	XC-VXC-10G カード (2)
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
セキュリティ レベル	メンテナンス以上のレベル



(注) XC-VXC-10G には、15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリが必要です。



(注) ノードに E100T-12 または E1000-2 カードが取り付けられている場合は、クロスコネクタカードをアップグレードしたときに UNEQ-P アラームが表示されます。アラームは、数秒間表示されてからクリアされます。



(注) アップグレード手順の実行中に相互接続機器障害アラームが表示されることがありますが、アップグレードの手順が完了してノードに対応するクロスコネクタカードが取り付けられると、クリアされます。



(注) XC-VXC-10G カードから XCVT または XC10G カードへのダウングレードはサポートされておりません。詳細については、Cisco TAC にお問い合わせください (「[テクニカル サポート](#)」 [p.xxix] )。



## 注意

アップグレードには、必ずスタンバイ側のクロスコネクタカードを使用してください。ロックアウトが設定されていない状態でアクティブ側のクロスコネクタカードを取り外すと、保護切り替えが発生します。スタンバイカードのアップグレードでは、ロックアウトが不要です。

- ステップ 1** アップグレードを実行するノードで「[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** 現地の状況に合わせて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 3** スタンバイ側の XCVT または XC10G カードを特定します。スタンバイ XCVT または XC10G カードの ACT/STBY LED はオレンジで、アクティブ XCVT または XC10G カードの ACT/STBY LED はグリーンです。

**ステップ4** ONS 15454 のスタンバイ XCVT または XC10G カードを XC-VXC-10G カードに交換します。

- a. XCVT または XC10G カードのイジェクタを開きます。
- b. カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。
- c. XC-VXC-10G カードのイジェクタを開きます。
- d. XC-VXC-10G カードをガイドレールに沿ってスライドさせて、スロットに取り付けます。
- e. イジェクタを閉じます。



**(注)** XC-VXC-10G カードでは、ACT/STBY LED の上にある FAIL LED がレッドになり、しばらく (20 ~ 30 秒) 点滅してから消えます。ACT/STBY LED はオレンジになり、点灯したままになります。

**ステップ5** ノードビューで、Maintenance > Cross-Connect タブをクリックします。

**ステップ6** Cross Connect Cards メニューから、Switch を選択します。

**ステップ7** Confirm Switch ダイアログボックスで Yes をクリックします。トラフィックが、**ステップ4** で挿入した XC-VXC-10G カードに切り替わります。このカードの ACT/STBY LED がオレンジからグリーンに変わります。

**ステップ8** ONS 15454 からスタンバイ XCVT または XC10G カードを物理的に取り外し、2 枚めの XC-VXC-10G カードを XCVT または XC10G カードの空きスロットに挿入します。

- a. XCVT または XC10G カードのイジェクタを開きます。
- b. XCVT または XC10G カードをスライドさせてスロットから外します。
- c. XC-VXC-10G カードのイジェクタを開きます。
- d. XC-VXC-10G カードをガイドレールに沿ってスライドさせて、スロットに取り付けます。
- e. イジェクタを閉じます。

2 枚めの XC-VXC-10G カードが起動してスタンバイ XC-VXC-10G カードになれば、アップグレードは完了です。ノードビューのアクティブカードおよびスタンバイカードが、XC-VXC-10G に変更されます。



**(注)** 最初のカードを変更しても、CTC では引き続き、両方のスロットで XCVT または XC10G カードが表示されます。XC-VXC-10G カードを反映するように表示を変更するには、2 枚めのカードをアップグレードし、このスロット内の XC-VXC-10G カードを起動する必要があります。

**終了:** この手順は、これで完了です。

## NTP-A296 TCC2 カードから TCC2P カードへのアップグレード

目的	この手順では、TCC2 カードを TCC2P カードへアップグレードします。TCC2 カードと TCC2P カードでは、R4.0 以降の ONS 15454 ソフトウェアがサポートされています。
工具 / 機器	SONET TCC2P カード (2) TCC2 カード (2)
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
セキュリティ レベル	メンテナンス以上のレベル



(注) TCC2P カードから TCC2 カードへのダウングレードはサポートされておりません。詳細については、Cisco TAC にお問い合わせください (「[テクニカル サポート](#)」 [p.xxix] を参照)。

- ステップ 1** バックプレーンの LAN 配線が正しいことを確認します。TCC2 カードでは、LAN 接続に配線ミスがあっても自動的に検出されません。LAN 接続に配線ミスがある場合は、[LAN Connection Polarity Reversed] 状態が表示されます。手順については、「[DLP-A21 バックプレーンへの LAN ケーブルの取り付け](#)」(p.17-27) を参照してください。
- ステップ 2** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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 3** アラームや異常がないことを確認します。手順については、「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を参照してください。
- ステップ 4** アップグレードを始める前に、「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。このノードに R4.0 以降の ONS 15454 ソフトウェアがインストールされていることを確認します。リリースごとのソフトウェア アップグレード マニュアルを参照してください。TCC2 カードと TCC2P カードは、R4.0 より前のソフトウェアとは互換性がありません。
- ステップ 5** ONS 15454 のスタンバイ TCC2 カードを TCC2P カードに交換します。
- 前面プレートの LED を確認します。TCC2 カードの前面プレートにある ACT/STBY LED は、カードがアクティブモードとスタンバイモードのどちらであることを示しています。ACT/STBY LED がグリーンになっている場合はカードがアクティブであることを示し、オレンジになっている場合はカードがスタンバイモードであることを示します。
  - スタンバイ TCC2 カードのイジェクタを開きます。
  - カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。
  - 取り付ける TCC2P カードのイジェクタを開きます。
  - TCC2P カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
  - イジェクタを閉じます。
  - CTC のノード ビューで、新しく取り付けられた TCC2P カードに Ldg (ロード中) の文字が表示されることを確認します。





(注) TCC2 をアップグレードしているときは TCC2 でバックプレーンとの通信が一時的に遮断されるので、CONTBUS-IO-A または CONTBUS-IO-B TCC A (または B) To Shelf Slot Communication Failure アラームが表示されます。このアラームは、特別なことがないかぎり、13 分ほどでクリアされます。一定期間経過後もアラーム状態がクリアされない場合は、<http://www.cisco.com/tac> にログオンして詳細を確認するか、Cisco TAC にお問い合わせください。



(注) データベースをアクティブ側の TCC2 カードから新しく取り付けられた TCC2P カードへ転送するのに、約 10 分かかります。この間、TCC2P カードの LED で Fail が点滅し、そのあとでアクティブ/スタンバイ LED が点滅します。転送が完了すると、TCC2P カードがリブートされ、3 分ほどでスタンバイ モードに変わります。データベースの転送中はシェルフからカードを取り出さないでください。

**注意**

アップグレードの作業で新しい TCC2P カードが完全なスタンバイ モードになる前にアクティブな TCC2 カードがリセットされた場合は、取り付けられた TCC2P カードをすぐに取り出してください。

**ステップ 6** 新しく取り付けられた TCC2P カードがスタンバイ モードになったら、アクティブ側の TCC2 カードに移動して、そのカードを右クリックします。

**ステップ 7** ドロップダウン リストから **Reset Card** をクリックします。

TCC2 カードがリブートされるまで待ちます。ONS 15454 によって、スタンバイ TCC2P カードがアクティブ モードに切り替わります。TCC2 カードは、TCC2P カードと同じデータベースがあるかどうかを確認してから、スタンバイ モードに切り替わります。

**ステップ 8** スロットに残っている TCC2 カードがスタンバイ モードになったこと (ACT/STBY LED がオレンジに変わっていること) を確認します。

**ステップ 9** [ステップ 5](#) を実行して、もう一方の TCC2 カードを 2 枚めの TCC2P カードと交換します。

ONS 15454 によって、2 枚めの TCC2P カードがブートします。2 枚めの TCC2P カードにもデータベースをコピーする必要があります。この作業には、約 10 分かかります。データベースの転送中はシェルフからカードを取り出さないでください。

**ステップ 10** 2 枚めの TCC2P カードを取り付けたあとに電源関連のアラームが発生した場合は、バックプレーンの電圧を調べます。手順については、「[DLP-A33 電圧の測定](#)」(p.17-41) を参照してください。アラームのクリアについては、『[Cisco ONS 15454 Troubleshooting Guide](#)』を参照してください。

**終了** : この手順は、これで完了です。

## NTP-A93 DS3-12 カードから DS3-12E カードへのアップグレード

目的	この手順では、DS3-12 カードを DS3-12E カードに、または DS3N-12 カードを DS3N-12E カードにアップグレードします。この手順を使用すると、シェルフに搭載されている R3.1 以前のソフトウェアを使用する DS3-12E カードの機能をイネーブルにすることもできます。
工具 / 機器	DS3-12E または DS3N-12E カード
事前準備手順	<a href="#">NTP-A17 電気回路カードの取り付け (p.2-11)</a>
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)

アップグレードは、2 枚の N タイプ カード間または 2 枚の N タイプ以外のカード間で実行する必要があります。N タイプカードと N タイプ以外のカード間でアップグレードすることはできません。カードを物理的に交換する場合は、新しいカードを古いカードと同じスロットに装着する必要があります。DS3-12E カードのアップグレードでは、1:1 および 1:N 保護方式がサポートされます。この手順を実行しても、保護カードのサービスには影響しません。アップグレードによって生じる切り替え時間は、50 ミリ秒未満です。



注意

現用カードに設定できる機能は保護カード以下であるため、現用カードより先に保護カードをアップグレードする必要があります。



(注)

アップグレード中に、Minor アラームおよび状態の一部が発生し、自動的にクリアされます。ただし、保護カードのアップグレード中は、サービスに影響するアラーム (SA、Major、または Critical) は、発生しません (保護されていないカードをアップグレードすると、サービスに影響することがあります)。サービスに影響するアラームが表示された場合は、この手順を取り消して元の状態に戻すことを推奨します。「[NTP-A254 DS3-12E/DS3NE カードから DS3-12/DS3N-12 カードへのダウングレード](#)」(p.12-14) を参照してください。

- ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 現地の状況に合わせて、「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 3** アップグレードするカードが保護されているかどうかを決定します。
- 保護されているカードは、**Maintenance > Protection** タブの Protection Groups に表示されます。Selected Group 領域に、各カードのスロット、ポート、およびステータス (Protect/Standby、Working/Active) が表示されます。
  - 保護されていないカードは、**Maintenance > Protection** タブの Protection Groups 領域または Selected Group 領域に表示されません。

**注意**

保護されていないカードのアップグレード中は、トラフィックが失われます。

- ステップ 4** アップグレードするカードが保護されていない場合は、この手順を省略し、保護カードおよび保護スロットに関する記述を無視して、**ステップ 5** に進んでください。アップグレード中のカードが保護されている場合は、保護カードがアクティブでないことを確認してください。カードステータスが Protect/Active である場合は、切り替えを実行して、現用カードをアクティブにします。
- 保護グループをダブルクリックします。
  - Protect/Active カードをクリックします。
  - Switch をクリックします。
  - 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 5** 保護 DS3-12 カードおよび保護 DS3N-12 カードを物理的に取り外します。
- DS3-12 または DS3N-12 カードのイジェクタを開きます。
  - カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。
- ステップ 6** 保護スロットを右クリックして、ドロップダウン リストから **Change Card** を選択します。
- ステップ 7** Change to ドロップダウン リストから、新しいカード (DS3-12E または DS3N-12E) を選択します。
- ステップ 8** OK をクリックします。
- ステップ 9** 新しい DS3-12E または DS3N-12E カードを保護スロットに挿入します。
- DS3-12E または DS3N-12E カードのイジェクタを開きます。
  - DS3-12E または DS3N-12E カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- ステップ 10** イジェクタを閉じます。
- IMPROPRMVL アラームがクリアされ、カードがスタンバイになるまで待ちます。
- ステップ 11** **ステップ 4** でトラフィックを切り替えた場合は、切り替えをクリアします。
- Maintenance > Protection タブで、レポートイング カードを含む保護グループをダブルクリックします。
  - 選択されたグループをクリックします。
  - Clear をクリックし、確認用ダイアログボックスで Yes をクリックします。
- ステップ 12** 現用カードについて **ステップ 3 ~ 11** を繰り返します。
- 終了** : この手順は、これで完了です。

## NTP-A308 低密度電気回路カードから高密度電気回路カードへのアップグレード

目的	この作業では、1:N 保護方式 (N = 1 または 2) の低密度電気回路カードを高密度電気回路カード (DS3/EC1-48、DS1/E1-56、および DS3XM-12 カード) にアップグレードします。低密度カードは、DS-1、DS-12、EC-12、および DS3XM-6 のいずれかとして定義されます。
工具 / 機器	DS3/EC1-48 カード、DS1/E1-56 カード、または DS3XM-12 カード 高密度シェルフ アセンブリ (15454-SA-HD)
事前準備手順	取り付けられた高密度 Electrical Interface Assembly (EIA; 電気インターフェイス アセンブリ) (MiniBNC、UBIC-V、UBIC-H)
必須 / 適宜	NTP-A17 電気回路カードの取り付け (p.2-11) 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**

現用カードの機能は保護カードの機能より低いため、現用カードより先に保護カードをアップグレードする必要があります。

**注意**

DS3XM-6 カードを DS3XM-12 カードにアップグレードしたあと、新しく取り付けられた DS3XM-12 カードは STS-12 モードで稼働します。バックプレーンのスループット レートを変更するには、カードが停止中で、ライブトラフィックを送信していないことを確認してください。稼働中のカードのバックプレーン スループット レートを変更すると、最長 30 秒のトラフィック停止を引き起こす可能性があります。

**(注)**

低密度電気回路カードがスロット 4、5、または 6 (シェルフの B 側のスロット 12、13、または 14) に取り付けられている場合は、電気回路を低密度から高密度にアップグレードできません。高密度電気回路カードにアップグレードできるのは、スロット 1、2、16、および 17 に取り付けられたカードのみです。

**(注)**

この手順では、スロット 1、2、および 3 (15、16、および 17) の電気回路カードを高密度電気回路カードにアップグレードする方法を示します。ただし、保護カード (スロット 3 または 15) を高密度電気回路カードにアップグレードした場合は、スロット 1 および 2 (16 および 17) に低密度 (12 ポート) 電気回路カードと高密度電気回路カードを混在させることができます。

**(注)**

アップグレード中に、Minor アラームおよび状態がいくつか発生し、自動的にクリアされます。ただし、保護カードのアップグレード中は、サービスに影響するアラーム (SA、Major、または Critical) は、発生しません (保護されていないカードをアップグレードすると、サービスに影響することがあります)。サービスに影響するアラームが表示された場合は、この手順を取り消して元の状態に戻すことを推奨します。

- ステップ 1** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** 現地の状況に合わせて、「NTP-A108 データベースのバックアップ」(p.15-6) を実行します。
- ステップ 3** スロット制限に従って、高密度カードにアップグレードする低密度カード (DS-1、DS-3、DS-3E) を決定します。

低密度保護カードをアップグレードする場合は、次の制限が適用されます。

- 保護カードは保護グループに属している必要があります。
- シェルフの A 側のスロット 4、5、または 6 (B 側の 12、13、または 14) に取り付けられた低密度電気回路カードは、保護カードで保護されません。
- 1:N 保護グループ (N=2) の場合 — A 側のスロット 4、5、または 6 (B 側の 12、13、または 14) に電気回路カードが取り付けられている場合は、保護カードをアップグレードできません。
- 1:N 保護グループ (N=1) の場合 — A 側のスロット 3 に保護カードが取り付けられていて、スロット 1 の低密度カードが保護されている場合に、スロット 5 または 6 に電気回路カードが取り付けられているか、事前にプロビジョニングされていると、保護カードをアップグレードできません。B 側のスロット 15 に保護カードが取り付けられていて、スロット 17 の低密度カードが保護されている場合に、スロット 12 または 13 に電気回路カードが取り付けられているか、事前にプロビジョニングされていると、保護カードをアップグレードできません。
- 1:N 保護グループ (N=1) の場合 — A 側のスロット 3 に保護カードが取り付けられていて、スロット 2 の低密度カードが保護されている場合に、スロット 4 に電気回路カードが取り付けられているか、または事前にプロビジョニングされていると、保護カードをアップグレードできません。B 側のスロット 15 に保護カードが取り付けられていて、スロット 16 の低密度カードが保護されている場合に、スロット 14 に電気回路カードが取り付けられているか、または事前にプロビジョニングされていると、保護カードをアップグレードできません。
- DS3XM-12 カードは、シェルフの反対側にある DS3XM-6 または DS3XM-12 カードを保護できませんが、保護されるカードをポートレス モードにしておく必要があります。

保護カードをアップグレードしたあとに現用カードをアップグレードする場合は、次の制限事項が適用されます。

- スロット 5 または 6 (B 側のスロット 12 または 13) に電気回路カードが取り付けられているか、または事前にプロビジョニングされている場合は、A 側のスロット 1 (B 側のスロット 17) に取り付けられた現用カードをアップグレードできません。
- スロット 4 (B 側のスロット 14) に電気回路カードが取り付けられているか、または事前にプロビジョニングされている場合は、A 側のスロット 2 (B 側のスロット 16) に取り付けられた現用カードをアップグレードできません。

- ステップ 4** ノード ビューで、現在の保護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。

シェルフの A 側で作業している場合は、スロット 3 に保護カードが装着されています。シェルフの B 側で作業している場合は、スロット 15 に保護カードが装着されています。

- ステップ 5** 現在の保護カードがアクティブでないことを確認してください。

- a. カード ビューで、Maintenance > Protection タブをクリックします。
- b. 保護カードが属している保護グループを選択します。

**ステップ 6** カード ステータスが Protect/Active である場合は、切り替えを実行して、保護カードをスタンバイにします。

- a. Switch をクリックします。
- 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 7** 物理的にカードを取り外します。

- a. カードのイジェクタを開きます。
- b. カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。

**ステップ 8** 保護スロット (スロット 3 またはスロット 15) を右クリックして、低密度カードを高密度カードに変更します。

- a. ドロップダウン リストから Change Card を選択します。
- b. Change to ドロップダウン リストから、新しいカード タイプ (DS3/EC1-48) を選択します。
- c. OK をクリックします。

**ステップ 9** 新しい高密度電気回路カードを保護スロットに挿入します。カードを取り付ける前に、カード背面のプラスチック製保護カバーが取り外されていることを確認してください。

- a. カードのイジェクタを開きます。
- b. カードをガイドレールに沿ってスライドさせて、スロットに取り付けます。
- c. イジェクタを閉じます。

IMPROPRMVL アラームがクリアされ、カードがスタンバイになるまで待ちます。高密度カードの起動中の LED の動作については、「NTP-A17 電気回路カードの取り付け」(p.2-11) を参照してください。

**ステップ 10** 低密度カードが現在アクティブであるため、A 側で作業している場合はスロット 1、B 側で作業している場合はスロット 17 の低密度カードから、別のカードにトラフィックを切り替えます。

- a. ノード ビューで、スロット 1 またはスロット 17 に取り付けられたカードをダブルクリックします。
- b. Maintenance > Protection タブをクリックします。
- c. スロット 1 または 17 内の現用カードを含む保護グループをダブルクリックします。
- d. スロット 1 またはスロット 17 内のカードをクリックします。
- e. Switch をクリックし、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 11** スロット 1 またはスロット 17 内の低密度カードを物理的に取り外します。

- a. カードのイジェクタを開きます。
- b. カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはアップグレードが完了するとクリアされます。

**ステップ 12** CTC で、低密度カードを高密度カードに変更します。

- a. スロット 1 またはスロット 17 を右クリックして、ドロップダウン リストから Change Card を選択します。

- b. Change to ドロップダウン リストから、新しいカード タイプを選択します。
- c. OK をクリックします。

**ステップ 13** 新しい高密度電気回路カードをスロット 1 またはスロット 17 に挿入します。カードを取り付ける前に、カード背面のプラスチック製保護カバーが取り外されていることを確認してください。

- a. カードのイジェクタを開きます。
- b. カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- c. イジェクタを閉じます。

IMPROPRMVL アラームがクリアされ、カードがスタンバイになるまで待ちます。DS3/EC1-48 カードの起動中の LED の動作については、「[NTP-A17 電気回路カードの取り付け](#)」(p.2-11) を参照してください。

**ステップ 14** [ステップ 10](#) で実行した切り替えをクリアします。

- a. ノード ビューで、スロット 1 またはスロット 17 に取り付けられたカードをダブルクリックします。
- b. Maintenance > Protection タブで、レポータリング カードを含む保護グループをダブルクリックします。
- c. 選択されたグループをクリックします。
- d. Clear をクリックし、確認用ダイアログボックスで Yes をクリックします。

スロット 3 (A 側) またはスロット 15 (B 側) の保護カードがこれでスタンバイになります。



**(注)** DS3XM-12 カードにアップグレードし、UBIC Electrical Interface Adapter (EIA; 電気インターフェイス アダプタ) 付き 734A ケーブルを使用している場合、LBX パネルからの実際の距離 (フィート) にしたがって、ポート 13 ~ 48 の LBO を設定する必要があります。735A ケーブルを使用している場合、次の規則に従ってポート 13 ~ 48 の LBO を設定します。

LBX パネルからの実際の距離が 110 フィート (33.53 m) より短い場合：  
LBO 設定は「0 ~ 225」です。

LBX パネルからの実際の距離が 110 フィート (33.53 m) 以上の場合：  
LBO 設定は「226 ~ 450」です。

**ステップ 15** スロット 2 またはスロット 16 の各について [ステップ 4 ~ 14](#) を繰り返します。

**終了：この手順は、これで完了です。**

## NTP-A254 DS3-12E/DS3NE カードから DS3-12/DS3N-12 カードへのダウングレード

目的	この作業では、DS3-12E または DS3NE カードをダウングレードします。ダウングレードによってアップグレードを取り消すことができます。ダウングレード手順は、Change Card ドロップダウン リストから DS3-12 または DS3N-12 を選択する点を除いて、アップグレード手順と同じです。
工具	なし
事前準備手順	NTP-A17 電気回路カードの取り付け (p.2-11)
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)

すべてのポートを UNFRAMED としてプロビジョニングし、Path Trace をディセーブルにする必要があります。



(注)

保護カードより先に、現用カードをダウングレードする必要があります。



ヒント

ダウングレード手順は、Change Card ドロップダウン リストから DS3-12 または DS3N-12 を選択する点を除いて、アップグレード手順と同じです。

**ステップ 1** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** 現地の状況に合わせて、「NTP-A108 データベースのバックアップ」(p.15-6) を実行します。

**ステップ 3** ダウングレードするカードが保護されているかどうかを判別します。

- 保護されているカードは、Maintenance > Protection タブの Protection Groups 領域に表示されません。Selected Group 領域に、各カードのスロット、ポート、およびステータス (Protect/Standby、Working/Active) が表示されます。
- 保護されていないカードは、Maintenance > Protection タブの Protection Groups 領域または Selected Group 領域に表示されません。



注意

保護されていないカードのアップグレード中は、トラフィックが失われます。



- ステップ 4** アップグレードするカードが保護されていない場合は、この手順を省略し、保護カードおよび保護スロットに関する記述を無視して、[ステップ 5](#)に進んでください。アップグレードするカードが保護されている場合は、保護カードがアクティブでないことを確認してください。カードステータスが Protect/Active である場合は、切り替えを実行して、現用カードをアクティブにします。
- 保護グループをダブルクリックします。
  - Protect/Active カードをクリックします。
  - Switch をクリックし、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 5** DS3-12E 現用カードまたは DS3N-12E 現用カードを物理的に取り外します。
- DS3-12E または DS3N-12E カードのイジェクタを開きます。
  - カードをスライドさせてスロットから外します。その結果、IMPROPRMVL アラームが表示されます。このアラームはダウングレードが完了するとクリアされます。
- ステップ 6** ダウングレードするスロットを右クリックして、ドロップダウン リストから **Change Card** を選択します。
- ステップ 7** Change to ドロップダウン リストから **DS3-12** または **DS3N-12** を選択します。
- ステップ 8** **OK** をクリックします。
- ステップ 9** DS3-12 または DS3N-12 カードを現用スロットに挿入します。
- DS3-12 または DS3N-12 カードのイジェクタを開きます。
  - DS3-12 または DS3N-12 カードをガイド レールに沿ってスライドさせて、スロットに取り付けます。
- ステップ 10** イジェクタを閉じます。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 11** [ステップ 4](#) でトラフィックを切り替えた場合は、切り替えをクリアします。
- Maintenance > Protection タブで、レポートカードを含む保護グループをダブルクリックします。
  - 選択されたグループをクリックします。
  - Clear をクリックし、確認用ダイアログボックスで Yes をクリックします。
- ステップ 12** 必要に応じて [ステップ 3](#) ~ [11](#) を繰り返して、保護カードをダウングレードします。
- 終了**：この手順は、これで完了です。
-

## NTP-A94 OC-N カードおよびスパンの自動アップグレード

目的	この手順では、カード、2 ファイバ BLSR スパン、4 ファイバ BLSR スパン、UPSR スパン、および 1+1 保護グループ スパンをアップグレードします。スパン アップグレード ウィザードでサポートされるのは、OC-N スパン アップグレードのみです。電気回路のアップグレードはサポートされません。
工具 / 機器	高速のカード  アップグレードに必要な互換ハードウェア (XC10G カードや XC-VXC-10G カード、および OC-48 Any Slot [AS] カードなど)
事前準備手順	アプリケーションによっては、減衰器が必要となる場合があります。スパンをアップグレードする場合は、2 人以上の技術者をスパンの両端にそれぞれ配置して、お互いに連絡を取り合えるようにし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
セキュリティ レベル	プロビジョニング以上のレベル



警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



注意

ファシリティや端末のループバックなど、これ以外のメンテナンス操作を実行したり、カードまたはスパンのアップグレード中に回線を追加したりしないでください。



(注)

表 2-4 (p.2-20) にある各カードの仕様で示されているように、OC-N の送受信レベルが許容範囲内にある必要があります。



(注)

アップグレード中に IMPROPRMVL アラームが発生することがあります。このアラームは自動的にクリアされます。



(注)

4 ポート OC-3 から 8 ポート OC-3 へのアップグレード、または 1 ポート OC-12 から 4 ポート OC-12 へのアップグレードを実行できるのは、スロット 1 ~ 4 および 14 ~ 17 のみです。これら以外のスロットには、OC3-8 および OC12-4 カードを取り付けることができないためです。OC3-8 および OC12-4 のスパン アップグレードを実行する前に、OC-3 および OC-12 カードがこれらのスロットに取り付けられていることを確認してください。4 つの OC-3 ポートは 8 ポート OC-3 カードのポート 1 ~ 4 にマッピングされます。OC-12 ポートは、4 ポート OC-12 カードのポート 1 にマッピングされます。



(注)

MRC-12 カードにアップグレードできるのは、1 ポート OC-12 カードまたは 1 ポート OC-48 カードのみです。低速カードのポートは、MRC-12 カードのポート 1 にマッピングされます。



(注)

BLSR PCA 回線が存在していた場合、それらの回線は既存の STS 内にそのまま残されます。そのため、これらの回線はアップグレード スパンの現用パスに配置され、BLSR の完全な保護を受けます。PCA 回線をアップグレード スパン内の保護チャンネルへ移す場合は、スパンをアップグレードしたあとにこれらの回線を削除して、再作成します。たとえば、OC-48 スパンを OC-192 にアップグレードした場合、OC-48 BLSR 内の保護 STS (25 ~ 48) の PCA 回線は、既存の STS (STS 25 ~ 48)、つまり OC-192 BLSR 内で保護されている現用 STS 内にそのまま残されます。OC-48 PCA 回線を削除して再作成すると、回線は OC-192 BLSR 内の STS 96 ~ 192 に移動します。回線の削除については、「[NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除](#)」(p.7-6) を参照してください。回線の作成については、第 6 章「[回線と VT トンネルの作成](#)」を参照してください。

**ステップ 1** 実行する必要があるアップグレードのタイプを判別し、必要なカードが取り付けられているか確認します。有効なカード アップグレードは、次のとおりです。

- 4 ポート OC-3 から 8 ポート OC-3 へ
- 1 ポート OC-12 から 4 ポート OC-12 へ
- OC-48 から MRC-12 へ
- OC-192 から OC192SR1/STM64IO Short Reach または OC192/STM64 Any Reach へ

有効なスパン アップグレードは、次のとおりです。

- 1 ポート OC-12 から OC-48 へ
- 1 ポート OC-12 から OC-192 へ
- 1 ポート OC-12 から 4 ポート OC-12 へ
- 1 ポート OC-12 から 15454\_MRC-12 へ
- OC-48 から OC-192 へ
- OC-48 から 15454\_MRC-12 へ
- OC-192 から OC192SR1/STM64IO Short Reach または OC192/STM64 Any Reach へ



注意

4 ポート OC-12 スパンはアップグレードできません。リングに OC12-4 カードが含まれる場合にリング内のすべてのスパンをアップグレードするときは、OC12-4 カードを 1 ポート OC-12 カードにダウングレードする必要があります (この処理を実行できるのは、OC12-4 カードのポートが 1 つだけ使用されている場合に限られます)。

**ステップ 2** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。すでにログインしている場合は、ステップ 3 へ進みます。



(注) Span Upgrade オプションが表示され、使用可能になるのは、アップグレードに必要なハードウェアが存在する場合のみです。たとえば、スパンの両端のノードに XC10G または XC-VXC-10G カードが取り付けられている場合を除き、OC-48 スパンからのアップグレードは実行できません。

**ステップ 3** 現地の状況に合わせて、「NTP-A108 データベースのバックアップ」(p.15-6) を実行します。

**ステップ 4** (重大度に関係なく) LOS、LOF、AIS-L、Signal Failure (SF; 信号障害)、Signal Degrade (SD; 信号劣化)、FORCED-REQ-RING などのアラームや異常な状態がないことを確認します。手順については、「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を参照してください。



(注) アップグレードまたはダウングレード中は、いくつかの Minor アラームや状態が表示され、自動的にクリアされます。サービスに影響するアラーム (SA、Major、または Critical) は、BLSROSYNC を除いて表示されません。BLSROSYNC は、すべてのノードのアップグレードまたはダウングレードが完了するとクリアされます。サービスに影響するその他のアラームが表示された場合は、この手順を取り消して元の状態に戻すことを推奨します。4 ノードの BLSR では、すべての BLSROSYNC アラームがクリアされるまでに最大で 5 分かかります。大規模な BLSR では、すべての BLSROSYNC アラームがクリアされるまでにさらに時間がかかります。

**ステップ 5** ネットワーク ビューで、アップグレードするスパンを右クリックします。

**ステップ 6** ドロップダウン リストから Span Upgrade を選択します。

**ステップ 7** 最初の Span Upgrade ダイアログボックスが表示されます (図 12-1)。ダイアログボックスの指示に従うと、ウィザードによってスパン アップグレードの残りの手順を実行できます。



(注) Back ボタンを使用できるのは、ウィザードのステップ 2 だけです。このステップよりあとではアップグレードを取り消すことができないため、ウィザードのステップ 2 よりあとでアップグレードを取り消す必要がある場合は、ウィザードを閉じて、手動による手順を実行してください。

図 12-1 スパン アップグレード ウィザード



**注意**

ウィザードでも示されますが、カードを取り付けるときは、次のステップへ進む前に、カードが起動してアクティブになるまで待つ必要があります。

**(注)**

OC-N カードを取り付けたあとに、必ずファイバを接続してください。

**(注)**

スパンをアップグレードすると、回線の CV-L スレッシュホールドが出荷時のデフォルトにリセットされます。これは、スレッシュホールドが回線速度に依存しているために、CV-L スレッシュホールドがリセットされるからです。

**ステップ 8** リングの残りのスパンについてステップ 5 ~ 7 を繰り返します。

**終了：**この手順は、これで完了です。

## NTP-A95 OC-N スパンの手動アップグレード

目的	この手順では、OC-N カードをアップグレードすることで、BLSR、UPSR、および 1+1 保護グループ内の OC-N 速度をアップグレードします。スパン アップグレード ウィザードのエラーを回復したり、スパンのアップグレードを取り消したりする（ダウングレード）必要がある場合は、アップグレード作業を手動で実行します。
工具 / 機器	交換用カード
事前準備手順	手動でスパンをアップグレードする場合は、2 人以上の技術者をスパンの両端にそれぞれ配置し、お互いに連絡を取り合えるようにし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
セキュリティ レベル	プロビジョニング以上のレベル



(注) 表 2-4 (p.2-20) にある各カードの仕様に示されているように、OC-N カードの送受信レベルが許容範囲内にある必要があります。



(注) ここでは、「スパン」という用語で、2 つのノード間の OC-N パスを表しています。また、「スパン エンドポイント」という用語で、スパンの両端のノードを表しています。



(注) スパンのアップグレード中にクロスコネクト カードがリブートした場合は、リング内のすべてのノードで、スパン アップグレード手順が完了したときに各カードをリセットする必要があります。

**ステップ 1** アップグレードする必要があるスパンのタイプを判別し、必要なカードが取り付けられていることを確認します。有効なスパン アップグレードは、次のとおりです。

- 4 ポート OC-3 から 8 ポート OC-3 へ
- 1 ポート OC-12 から 4 ポート OC-12 へ
- 1 ポート OC-12 から OC-48 へ
- 1 ポート OC-12 から OC-192 へ
- 1 ポート OC-12 から 15454\_MRC-12 へ
- OC-48 から OC-192 へ
- OC-192 から OC192SR1/STM64IO Short Reach または OC192/STM64 Any Reach へ



**注意** 4 ポート OC-12 スパンはアップグレードできません。リングに OC12-4 カードが含まれる場合にリング内のすべてのスパンをアップグレードする必要があるときは、OC12-4 カードを 1 ポート OC-12 カードにダウングレードする必要があります（この処理を実行できるのは、OC12-4 カードのポートが 1 つだけ使用されている場合に限られます）。

- ステップ 2** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。すでにログインしている場合は、ステップ 3 へ進みます。
- ステップ 3** 現地の状況に合わせて、「NTP-A108 データベースのバックアップ」(p.15-6) を実行します。
- ステップ 4** (重大度に関係なく) LOS、LOF、AIS-L、SF、SD、FORCED-REQ-RING などのアラームや異常な状態がないことを確認します。手順については、「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を参照してください。



- (注)** アップグレードまたはダウングレード中は、いくつかの Minor アラームや状態が表示され、自動的にクリアされます。サービスに影響するアラーム (SA、Major、または Critical) は、BLSROSYNC を除いて表示されません。BLSROSYNC は、すべてのノードのアップグレードまたはダウングレードが完了するとクリアされます。サービスに影響するその他のアラームが表示された場合は、この手順を取り消して元の状態に戻すことを推奨します。4 ノードの BLSR では、すべての BLSROSYNC アラームがクリアされるまでに最大で 5 分かかります。大規模な BLSR では、すべての BLSROSYNC アラームがクリアされるまでにさらに時間がかかります。アラームの詳細については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

- ステップ 5** 次の中の該当する作業を行います。

- DLP-A293 2 ファイバ BLSR での手動スパン アップグレード (p.19-64)
- DLP-A294 4 ファイバ BLSR での手動スパン アップグレード (p.19-66)
- DLP-A295 UPSR での手動スパン アップグレード (p.19-67)
- DLP-A296 1+1 保護グループでの手動スパン アップグレード (p.19-69)
- DLP-A297 非保護スパンでの手動スパン アップグレード (p.19-70)



- (注)** スパンをアップグレードすると、回線の CV-L スレッシュホールドが出荷時のデフォルトにリセットされます。これは、スレッシュホールドが回線速度に依存しているために、CV-L スレッシュホールドがリセットされるからです。



- (注)** Span Upgrade オプションが表示され、使用可能になるのは、アップグレードに必要なハードウェアが存在する場合のみです。たとえば、スパンの両端のノードに XC10G または XC-VXC-10G カードが取り付けられている場合を除き、OC-48 スパンからのアップグレードは実行できません。



- (注)** 4 ポート OC-3 から 8 ポート OC-3 スパンへのアップグレード、または OC-12 から 4 ポート OC-12 スパンへのアップグレードを実行できるのは、スロット 1 ~ 4 および 14 ~ 17 のみです。これら以外のスロットには、OC3-8 および OC12-4 カードを取り付けることができません。OC3-8 および OC12-4 へのスパン アップグレードを実行する前に、OC-3 および OC-12 カードがこれらのスロットに取り付けられていることを確認してください。4 つの OC-3 ポートは 8 ポート OC-3 カードのポート 1 ~ 4 にマッピングされます。OC-12 ポートは、4 ポート OC-12 カードのポート 1 にマッピングされます。

終了：この手順は、これで完了です。







## ネットワーク構成の変換

この章では、Cisco ONS 15454 ネットワークで SONET トポロジを別のトポロジへ変換する方法について説明します。ネットワークの初期起動については、第 5 章「ネットワークの起動」を参照してください。

### 準備作業

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A335 1+1 ポイントツーポイント型からリニア ADM への自動変換 \(p.13-2\)](#)— 必要に応じて、この手順を実行します。
2. [NTP-A154 1+1 ポイントツーポイント型からリニア ADM への手動変換 \(p.13-5\)](#)— 稼働中のトポロジ アップグレード ウィザードを使用できない場合、またはウィザードを取り消す必要がある場合は、必要に応じてこの手順を実行します。
3. [NTP-A303 非保護ポイントツーポイント型または 1+1 リニア ADM から 2 ファイバ BLSR への自動変換 \(p.13-7\)](#)— 必要に応じて、この手順を実行します。
4. [NTP-A155 1+1 ポイントツーポイント型またはリニア ADM から 2 ファイバ BLSR への手動変換 \(p.13-10\)](#)— 稼働中のトポロジ アップグレード ウィザードを使用できない場合、またはウィザードを取り消す必要がある場合は、必要に応じてこの手順を実行します。
5. [NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換 \(p.13-13\)](#)— 必要に応じて、この手順を実行します。
6. [NTP-A156 ポイントツーポイント型またはリニア ADM から UPSR への手動変換 \(p.13-15\)](#)— 稼働中のトポロジ アップグレード ウィザードを使用できない場合、またはウィザードを取り消す必要がある場合は、必要に応じてこの手順を実行します。
7. [NTP-A267 UPSR から 2 ファイバ BLSR への自動変換 \(p.13-16\)](#)— 必要に応じて、この手順を実行します。
8. [NTP-A210 UPSR から 2 ファイバ BLSR への手動変換 \(p.13-19\)](#)— 稼働中のトポロジ アップグレード ウィザードを使用できない場合、またはウィザードを取り消す必要がある場合は、必要に応じてこの手順を実行します。
9. [NTP-A211 2 ファイバ BLSR から 4 ファイバ BLSR への自動変換 \(p.13-21\)](#)— 必要に応じて、この手順を実行します。
10. [NTP-A159 BLSR の変更 \(p.13-23\)](#)— 必要に応じて実行し、BLSR リング名、リングまたはスパンの復元時間、またはノード ID を変更します。

## NTP-A335 1+1 ポイントツーポイント型からリニア ADM への自動変換

目的	この手順では、トラフィックを損失することなく 1+1 ポイントツーポイント ( 端末 ) 構成 ( 2 ノード ) をリニア Add Drop Multiplexer ( ADM; 分岐挿入装置 ) 構成 ( 3 ノード ) に変換します。
工具 / 機器	互換性のあるハードウェア
事前準備手順	アプリケーションによっては、減衰器が必要となる場合があります。この手順では、追加するノードに到達できる ( CTC と IP 接続されている ) 必要があります。CTC の動作している PC と ONS 15454 ノードが別々の場所にある場合は、2 人の技術者をそれぞれの場所に配置して、アップグレード中にお互いに連絡を取り合えるようにし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
セキュリティ レベル	プロビジョニング以上のレベル



(注) 表 2-4 ( p.2-20 ) にある各カードの仕様で示されているように、OC-N の送受信レベルが許容範囲内にある必要があります。



(注) ネットワークにオーバーヘッド回線が存在している場合は、この手順を実行するとサービスに影響が出ます。この場合、オーバーヘッド回線でトラフィックが廃棄され、アップグレードが完了したときにステータスが PARTIAL になります。

- ステップ 1** 2 つのポイントツーポイント ノードの一方で、「[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** ネットワーク ビューで、新しいノードを追加する 2 つのノード間のスパンを右クリックします。ダイアログボックスが表示されます。
- ステップ 3** Upgrade Protection を選択します。ドロップダウン リストが表示されます。
- ステップ 4** Terminal to Linear を選択すると、Upgrade Protection: Terminal to Linear ウィザードの最初のページが表示されます。
- ステップ 5** ウィザードの最初のページに、新しいノードを追加するために必要な次の条件が表示されます。
- 終端ノードに Critical アラームも Major アラームもない。
  - 追加するノードに Critical アラームも Major アラームもない。
  - そのノードと終端ノードのソフトウェア バージョンに互換性がある。
  - 1+1 保護の速度に合った未使用の光ポートがノードに 4 つ存在し、それら 4 つのポートに通信チャネルがプロビジョニングされていない。
  - 追加するノードを終端ノードに接続するためのファイバがある。
- これらの条件がすべて満たされていて、この手順を続ける場合は、Next をクリックします。

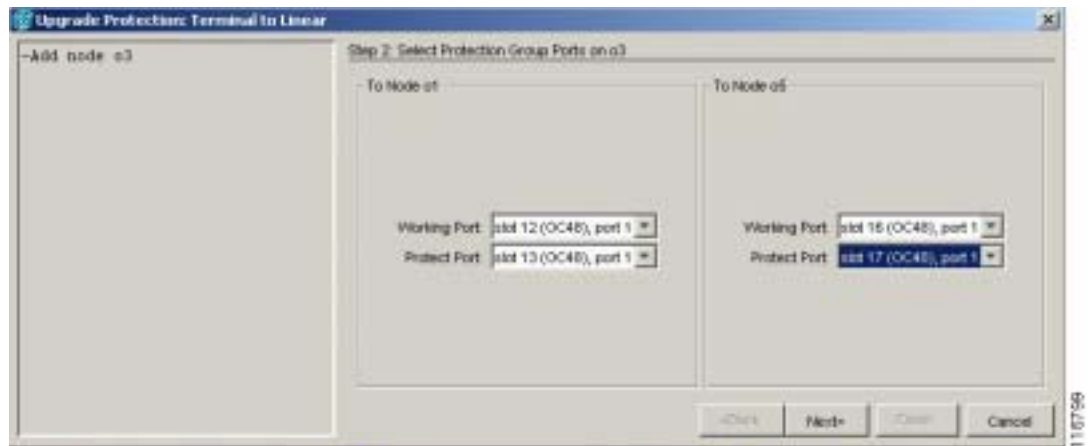


(注) 到達不能なノードを追加する場合は、まず、別の CTC セッションを使用してその到達不能なノードにログインし、そのノードを設定します。次に「DLP-A155 保護グループの削除」(p.18-25) に説明されている方法で、既存の保護グループをすべて削除します。「DLP-A156 SDCC 終端の削除」(p.18-25) および「DLP-A359 LDCC 終端の削除」(p.20-50) に説明されている方法で、既存の Data Communication Channel (DCC; データ通信チャネル) 終端をすべて削除します。

**ステップ 6** ノードのホスト名または IP アドレスを入力するか、ドロップダウン リストで新しいノードの名前を選択します。名前を入力する場合は、実際のノード名を正しく入力してください。ノード名は、大文字と小文字を区別して指定します。

**ステップ 7** Next をクリックします。Select Protection Group Ports ページが表示されます (図 13-1)。

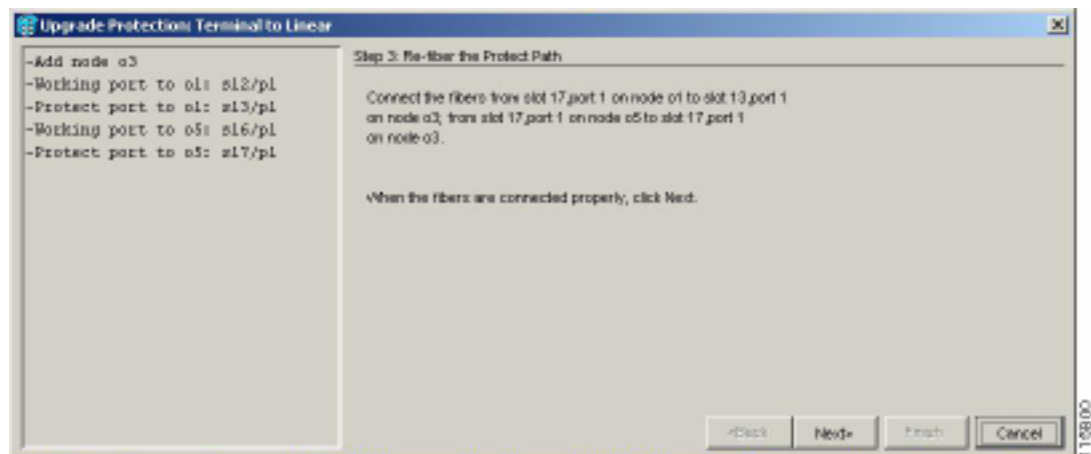
図 13-1 保護グループ ポートの選択



**ステップ 8** 各終端ノードに接続する新しいノードの現用ポートと保護ポートを、ドロップダウン リストから選択します。

**ステップ 9** Next をクリックします。Re-fiber the Protected Path ダイアログボックスが表示されます (図 13-2)。

図 13-2 保護パスのファイバ再接続



**ステップ 10** Re-fiber the Protected Path ダイアログボックスの指示に従って、ノード間をファイバで接続します。

**ステップ 11** ファイバを正しく接続したら、**Next** をクリックします。Update Circuit(s) on *Node-Name* ダイアログボックスが表示されます。



**(注)** ウィザードでは、Back ボタンを使用できません。保護のアップグレード手順をキャンセルする場合は、ここで **Cancel** ボタンをクリックし、**Yes** ボタンをクリックします。光ファイバケーブルを物理的に移動したあとで手順が失敗した場合は、光ファイバケーブルを元の位置に戻し、ノードの現用パスにトラフィックが流れていることを (CTC 経由で) 確認してから、手順を再開します。トラフィックのステータスを確認するには、ノードビューへ進んで、**Maintenance > Protection** タブをクリックします。Protection Groups 領域で、1+1 保護グループをクリックします。Selected Group 領域でトラフィックのステータスを確認できます。

**ステップ 12** Update Circuit(s) on *Node-Name* ページで **Next** をクリックし、手順の実行を続けます。

**ステップ 13** Force Traffic to Protect Path ページに、終端ノードでトラフィックを現用パスから保護パスへ強制的に切り替えようとしていることが表示されます。次へ進む準備ができたなら、**Next** をクリックします。

**ステップ 14** ウィザードの説明に従ってノード間の現用パスをファイバで再接続したあと、トラフィックを現用パスへ強制的に戻すための各手順を実行します。

**ステップ 15** Force Traffic to Working Path ページに、終端ノードでトラフィックを保護パスから現用パスへ強制的に切り替えようとしていることが表示されます。次へ進む準備ができたなら、**Next** をクリックします。

**ステップ 16** Completed ページが表示されます。このページは、この手順の最後のページです。**Finish** をクリックします。

**終了** : この手順は、これで完了です。

## NTP-A154 1+1 ポイントツーポイント型からリニア ADM への手動変換

目的	この手順では、稼働中のトポロジー アップグレード ウィザードを使用しないで、1+1 ポイントツーポイント構成 (2 ノード) をリニア ADM 構成 (3 ノード以上) へ手動でアップグレードします。ウィザードを使用できない場合、またはウィザードをキャンセルして最初から手動で行う場合に、この手順を使用します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A124 ポイントツーポイント ネットワークのプロビジョニング (p.5-5)</a>
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) [表 2-4 \(p.2-20\)](#) にある各カードの仕様に示されているように、光の送受信レベルが許容範囲内にある必要があります。



(注) ポイントツーポイント構成では、2 枚の OC-N カードが、もう一方のノードにある 2 枚の OC-N カードに接続されています。現用の OC-N ポートには DCC の終端があり、OC-N カードは 1+1 保護グループに属しています。

- ステップ 1** 2 つのポイントツーポイント ノードの一方で、「[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** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。
- ステップ 3** ポイントツーポイント構成へ追加するノード (新規ノード) にログインします。



(注) 到達不能なノードを追加する場合は、まず、別の CTC セッションを使用してその到達不能なノードにログインし、そのノードを設定します。次に「[DLP-A155 保護グループの削除](#)」(p.18-25) に説明されている方法で、既存の保護グループをすべて削除します。「[DLP-A156 SDCC 終端の削除](#)」(p.18-25) および「[DLP-A359 LDCC 終端の削除](#)」(p.20-50) に説明されている方法で、既存の DCC 終端をすべて削除します。

- ステップ 4** 「[NTP-A323 カードの取り付けの確認](#)」(p.4-2) を実行して、新規ノードに 2 枚の OC-N カードが取り付けられていることと、それらのカードの速度がポイントツーポイント ノードの速度と同じであることを確認します。
- ステップ 5** 新規ノードに対して、「[NTP-A35 ノードの起動の確認](#)」(p.5-3) を実行します。
- ステップ 6** ポイントツーポイント ノードと新規ノードの間をファイバで物理的に接続します。ファイバは、現用カードと現用カードの間と、保護カードと保護カードの間に接続する必要があります。

**ステップ 7** 新規ノードで、ポイントツーポイント ノードに接続するポイントツーポイント ノード内の OC-N カードに対して 1+1 保護グループを作成します。「[DLP-A73 1+1 保護グループの作成](#)」(p.17-87) を参照してください。

**ステップ 8** リニア ADM ネットワークに接続する新規ノードの現用 OC-N カードに対して、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を行います。CTC の管理に必要な帯域幅が不足している場合は、「[DLP-A378 LDCC 終端のプロビジョニング](#)」(p.20-77) を行って追加します。



(注) **ステップ 9** でポイントツーポイント ノードに DCC の終端を作成するまでは、DCC 障害アラームが表示され続けます。

**ステップ 9** ノード ビューで、新規ノードに接続するポイントツーポイント ノードを表示します。

**ステップ 10** 「[NTP-A323 カードの取り付けの確認](#)」(p.4-2) を実行して、ポイントツーポイント ノードに、新規ノードに接続できる OC-N カードが取り付けられていることを確認します。

**ステップ 11** 新規ノードに接続する OC-N カードに対して 1+1 保護グループを作成します。手順については、「[DLP-A73 1+1 保護グループの作成](#)」(p.17-87) を参照してください。

**ステップ 12** 新規ノードに接続する現用 OC-N カードに DCC 終端を作成します。「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を参照してください。

**ステップ 13** View メニューで **Go to Node View** を選択し、ノード ビュー内に新規ノードを開きます。

**ステップ 14** 新規ノードに対して、「[NTP-A28 タイミングの設定](#)」(p.4-11) を実行します。新規ノードでライン タイミングを使用している場合は、現用 OC-N カードをタイミングソースに設定します。

**ステップ 15** View メニューから **Go to Network View** を選択します。新しく作成したリニア ADM の構成が正しいことを確認します。各リニア ノードの間には、グリーンのスパン ラインが 1 本表示されています。

**ステップ 16** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 17** ここまでの手順を繰り返して、残りのノードをリニア ADM に追加します。

終了：この手順は、これで完了です。

## NTP-A303 非保護ポイントツーポイント型または 1+1 リニア ADM から 2 ファイバ BLSR への自動変換

目的	この手順では、トラフィックを中断することなく、非保護ポイントツーポイント型 (2 ノード) またはリニア ADM (3 ノード以上) を 2 ファイバ Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) へアップグレードします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a>
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) この手順を開始する前に、新しい BLSR を識別するための一意なリング名と、リング上の各ノードに対する一意なノード ID 番号を用意しておく必要があります。



(注) この手順を開始する前に、光の送受信レベルが [表 2-4 \(p.2-20\)](#) に示されている許容範囲内にあることを確認してください。



(注) ネットワークにオーバーヘッド回線が存在している場合は、この手順を実行するとサービスに影響が出ます。この場合、オーバーヘッド回線でトラフィックが廃棄され、アップグレードが完了したときにステータスが PARTIAL になります。

- ステップ 1** ポイントツーポイントまたはリニア ADM 上のノードで、「[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** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。
- ステップ 3** ポイントツーポイント型またはリニア ADM スパンをサポートしているノードで、「[DLP-A155 保護グループの削除](#)」(p.18-25) を行って、存在する可能性のある保護グループをすべて削除します。
- ステップ 4** ポイントツーポイント型またはリニア ADM スパンをサポートしているノードで、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を行います。SDCC の終端リストにない各ノードのスロットをプロビジョニングします。
- ステップ 5** Tools メニューから **Topology Upgrade > Convert UPSR to BLSR** を選択します。Topology Conversion ダイアログボックスで、BLSR プロパティを設定します。
- Ring Type — (表示専用) デフォルトは、2 ファイバです。
  - Speed — OC-12、OC-48、OC-192 から BLSR リングの速度を選択します。速度は BLSR トランク (スパン) カードの OC-N 速度と一致する必要があります。



(注) OC-12 の BLSR を作成しておいて、最終的に OC-48 または OC-192 へアップグレードする場合は、1 ポート OC-12 カード (OC12 IR/STM4 SH 1310、OC12 LR/STM4 SH 1310、または OC12 LR/STM4 LH 1550) を使用します。

- Ring Name — リング名を割り当てます。名前に使用できる文字数は、1 ~ 6 文字です。すべての英数字を大文字と小文字を組み合わせて指定できます。大文字か小文字かに関係なく、文字列 [All] は使用できません。[All] は TL1 のキーワードであるため、拒否されます。すでに他の BLSR に割り当てられている名前も指定できません。
- Reversion time — リングを切り替えたあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。リングの復元を、Never に設定することもできます。

**ステップ 6** Next をクリックします。ネットワークの図が表示されたら、[ステップ 7](#) へ進みます。

取り付けられている光カードの数が不足している場合や、Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) セレクタのある回線が検出された場合などは、BLSR を作成できません。CTC でそうした状況が判明すると、[Cannot Create BLSR] というメッセージが表示されます。このメッセージが表示された場合は、次のステップを実行します。

- OK をクリックします。
- Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- 「[NTP-A40 BLSR ノードのプロビジョニング](#)」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。

**ステップ 7** ネットワークの図で、BLSR のスパン ラインを順番にダブルクリックしていきます。ダブルクリックしたスパン ラインが他の BLSR カードに DCC で接続されていて完全なリングを形成していれば、それらのラインがブルーになります。ラインをダブルクリックしてもまだ完全なリングを形成できていない場合は、完全なリングが作成されるまで別のスパン ラインをダブルクリックしていきます。Next をクリックします。

**ステップ 8** UPSR to BLSR Topology Conversion ダイアログボックスが表示されます。このダイアログボックスに、システムがトラフィックを最短の UPSR パスへ強制的に流すことが表示されます。Next をクリックします。

**ステップ 9** 別のダイアログボックスが開き、トラフィックが最短の UPSR パスに適用されたことが表示されます。Finish をクリックします。

BLSR ウィンドウが開き、作成した BLSR が表示されたら、次のステップへ進みます。[Cannot Create BLSR] または [Error While Creating BLSR] というメッセージが表示された場合は、次の作業を行います。

- OK をクリックします。
- Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。



- d. 「[NTP-A40 BLSR ノードのプロビジョニング](#)」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。



(注) BLSR の設定時には、E-W-MISMATCH、RING MISMATCH、APSCIMP、APSDFLTK、および BLSROSYNC の各アラームのうち一部またはすべてが一時的に表示されることがあります。

**ステップ 10** 次の点を確認します。

- ネットワーク ビューの図で、すべての BLSR ノード間にグリーンのスパン ラインが表示されていること。
- E-W MISMATCH、RING MISMATCH、APSCIMP、DFLTK、および BLSROSYNC の各アラームがすべてクリアされていること。アラームのトラブルシューティングについては、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。



(注) ノード名の後ろにあるかっこ内の数字は、CTC によって割り当てられた BLSR ノード ID です。1 つの BLSR 内の各 ONS 15454 には、0 ~ 31 の一意なノード ID が割り当てられています。ノード ID を変更する場合は、「[DLP-A326 BLSR のノード ID の変更](#)」(p.20-17) を行います。

終了：この手順は、これで完了です。

## NTP-A155 1+1 ポイントツーポイント型またはリニア ADM から 2 ファイバ BLSR への手動変換

目的	この手順では、稼働中のトポロジー アップグレード ウィザードを使用しないで、1+1 ポイントツーポイント構成 (2 ノード) またはリニア ADM 構成 (3 ノード以上) を 2 ファイバ BLSR に手動でアップグレードします。ウィザードを使用できない場合、またはウィザードをキャンセルして最初から手動で行う場合に、この手順を使用します。
工具 / 機器	なし
事前準備手順	NTP-A124 ポイントツーポイント ネットワークのプロビジョニング (p.5-5) または NTP-A38 リニア ADM ネットワークのプロビジョニング (p.5-9)
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)

光の送受信レベルが表 2-4 (p.2-20) に示されている許容範囲内にあることを確認してください。



注意

この手順を実行している間は、トラフィックは保護されません。

- ステップ 1** ポイントツーポイント型または ADM から BLSR に変換するノードの 1 つで、「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** 現地の状況に合わせて、構成に含まれている各ノードに対して「NTP-A108 データベースのバックアップ」(p.15-6) を実行します。
- ステップ 3** 「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を実行します。
- ステップ 4** ネットワーク マップで、現在ログインしているノードの隣接スパンを右クリックします。ショートカット メニューが表示されます。
- ステップ 5** ショートカット メニューで、Circuits をクリックします。Circuits on Span ウィンドウが表示されます。
- ステップ 6** アクティブな STS 回線の合計帯域幅が、スパン帯域幅の 50% を超えていないことを確認します。Circuits カラムには、[Unused] というタイトルの付いたブロックがあります。この数値がスパン帯域幅の 50% を超えている必要があります。

スパンが OC-48 の場合、そのスパンでプロビジョニングできる STS の最大数は 24 です。スパンが OC-192 の場合、そのスパンでプロビジョニングできる STS の最大数は 96 です。スパンが OC-12 の場合、そのスパンでプロビジョニングできる STS の最大数は 6 です。

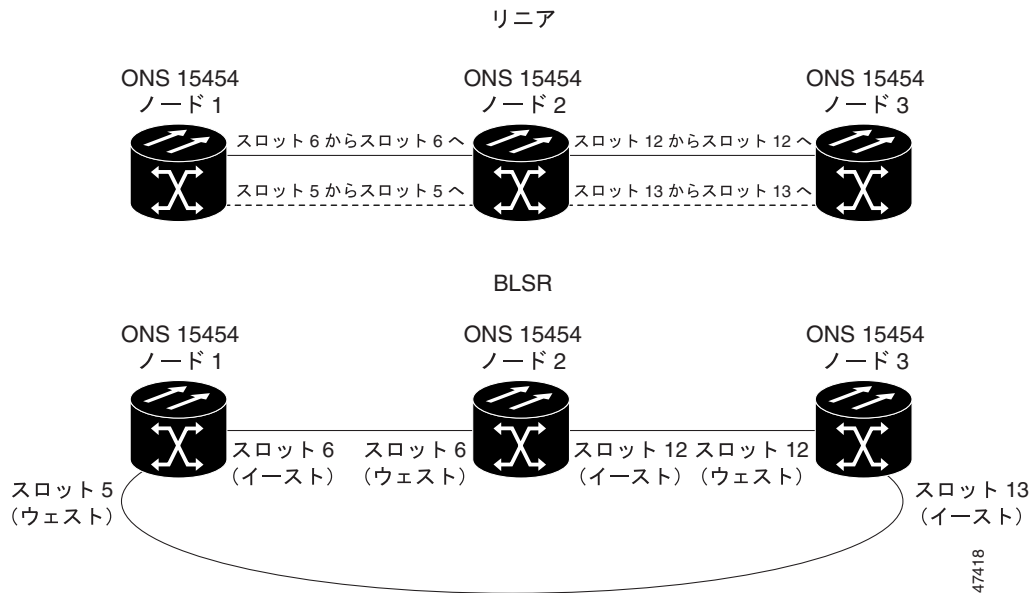


**注意**

上位 STS が使用されている場合は、この手順を実行できません。BLSR に変換するには、まだ割り当てられていない帯域幅が 50% 必要です。これらの要件が満たされていない場合は、ローカル手順を参照して、回線を再配置してください。

- ステップ 7** BLSR に変換するポイントツーポイント型またはリニア ADM 内の各ノードに対して、**ステップ 4 ~ 6** を繰り返します。すべてのノードが**ステップ 6** の要件を満たしていれば、次のステップへ進みます。
- ステップ 8** BLSR に変換するポイントツーポイント型またはリニア ADM ネットワーク内のすべてのノードに対して、次の作業を行います。
- ポイントツーポイント型またはリニア ADM ネットワークでスパンをサポートしているすべての 1+1 保護グループに対して、「**DLP-A189 1+1 現用スロットがアクティブであることの確認**」(p.18-59) を行います。
  - ポイントツーポイント型またはリニア ADM スパンをサポートしている各ポートで、「**DLP-A155 保護グループの削除**」(p.18-25) を行います。
  - ポイントツーポイント型またはリニア ADM スパンをサポートしている各ノードで「**DLP-A214 ポートのサービス状態の変更**」(p.19-10) を行い、保護ポートを停止状態にします。
- ステップ 9** (リニア ADM の場合のみ)リニア ADM 内のすべてのノードから、保護ファイバを物理的に取り外します。たとえば、ノード 2 のスロット 13 からノード 3 のスロット 13 に接続されているファイバを取り外します (図 13-3)。

**図 13-3 リニア ADM から BLSR への変換**



47418

**ステップ 10** 一方のエンド ノードからもう一方のエンド ノードにある保護ポートまで保護ファイバを接続して、リングを作成します。たとえば、ノード 1 のスロット 5 とノード 2 のスロット 5 の間を接続しているファイバを、ノード 1 のスロット 5 とノード 3 のスロット 13 を結ぶようにルーティングしなおします ( [図 13-3](#) を参照 )。



**(注)** シェルフから OC-N カードを取り外す必要がある場合は、この時点で取り外します。この例では、ノード 2 のスロット 5 と 13 のカードを取り外します。「[NTP-A116 カードの取り外しおよび交換](#)」( p.2-23 ) を参照してください。

**ステップ 11** ネットワーク ビューで **Circuits** タブをクリックして「[DLP-A532 CTC データのエクスポート](#)」( p.22-35 ) を行い、回線のデータをハード ドライブ上のファイルに保存します。

**ステップ 12** エンド ノードで「[DLP-A377 SDCC 終端のプロビジョニング](#)」( p.20-74 ) を行います。各ノードで、SDCC の終端リストにまだ含まれていないスロットをプロビジョニングします ( [図 13-3](#) の例では、ノード 1 にあるスロット 5 のポート 1 とノード 3 にあるスロット 13 のポート 1 )。

**ステップ 13** 保護帯域幅の一部となった STS 上にプロビジョニングしてあった各回線を、次の手順で削除して、再作成します ( OC-12 BLSR の場合は STS 7 ~ 12、OC-48 BLSR の場合は STS 25 ~ 48、および OC-192 BLSR の場合は STS 97 ~ 192 )。

- a. 1 本の回線について、「[DLP-A333 回線の削除](#)」( p.20-23 ) を行います。
- b. リニア ADM の保護ファイバとして使用されていたファイバ上で、OC-12 BLSR の場合は STS 1 ~ 6、OC-48 BLSR の場合は STS 1 ~ 24、OC-192 BLSR の場合は STS 1 ~ 96 に回線を作成します。手順については、「[NTP-A344 手動ルーティングによる光回線の作成](#)」( p.6-54 ) を参照してください。
- c. BLSR の保護 STS 上にある残りの回線について、ステップ a と b を繰り返します。

**ステップ 14** 「[NTP-A126 BLSR の作成](#)」( p.5-16 ) を実行して、BLSR にノードを組み入れます。

**終了 :** この手順は、これで完了です。

## NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換

目的	この手順では、トラフィックを中断することなく、ポイントツーポイント型またはリニア ADM を UPSR へアップグレードします。UPSR へアップグレードできるのは、STS、VT、および VT トンネル回線です。このオプションは、1 本の回線を対象にした操作です。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A124 ポイントツーポイント ネットワークのプロビジョニング (p.5-5)</a>
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)** VT トンネルをアップグレードする場合、CTC では VT トンネルを UPSR へ変換する代わりに、代替パスのセカンダリ トンネルを作成します。その結果、代替パスを使用する非保護 VT トンネルが 2 つあることとなります。



**(注)** ネットワークにオーバーヘッド回線が存在している場合は、この手順を実行するとサービスに影響が出ます。この場合、オーバーヘッド回線でトラフィックが廃棄され、アップグレードが完了したときにステータスが PARTIAL になります。

- ステップ 1** ポイントツーポイントまたはリニア ADM 上のノードで、「[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** ポイントツーポイント型またはリニア ADM が 1+1 保護の場合は、「[DLP-A155 保護グループの削除](#)」(p.18-25) を行います。ポイントツーポイント型またはリニア ADM が非保護の場合は、**ステップ 4** へ進みます。
- ステップ 3** UPSR に組み入れるすべてのノードの保護カードで、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を行います。CTC の管理に必要な帯域幅が不足している場合は、「[DLP-A378 LDCC 終端のプロビジョニング](#)」(p.20-77) を行って追加します。
- ステップ 4** ネットワーク ビューまたはノード ビューで、Circuits タブをクリックします。アップグレードする回線をクリックして、選択します。
- ステップ 5** Tools メニューから **Topology Upgrade > Convert Unprotected to UPSR** を選択します。
- ステップ 6** UPSR のパラメータを設定するには、「[DLP-A218 UPSR セクタのプロビジョニング](#)」(p.19-14) を行います。



(注) ポイントツーポイント型またはリニア ADM 回線を UPSR トポロジにアップグレードするとき、Provision working go & return on primary path ルーティング オプションが Circuit Attributes ペインでオンになっていない場合、300 ミリ秒以上のトラフィックの中断が発生します。

**ステップ 7** Next をクリックします。

**ステップ 8** 次のいずれかの作業を行います。

- a. 新しい UPSR 回線を手動でルーティングする場合は、「[DLP-A397 手動ルーティングによる UPSR 回線のトポロジ アップグレード](#)」(p.20-111)を行います。
- b. 新しい UPSR 回線を自動でルーティングする場合は、「[DLP-A398 自動ルーティングによる UPSR 回線のトポロジ アップグレード](#)」(p.20-111)を行います。

**終了** : この手順は、これで完了です。

---

## NTP-A156 ポイントツーポイント型またはリニア ADM から UPSR への手動変換

目的	この手順では、ポイントツーポイント型システムを UPSR へ手動で変換します。稼働中のトポロジー アップグレード ウィザードは使用しません。ウィザードを使用できない場合、またはウィザードをキャンセルして最初から手動で行う場合に、この手順を使用します。
工具 / 機器	なし
事前準備手順	NTP-A124 ポイントツーポイント ネットワークのプロビジョニング (p.5-5) または NTP-A38 リニア ADM ネットワークのプロビジョニング (p.5-9)
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

この手順は、サービスに影響を与えます。すべての回線が削除され、再プロビジョニングされます。

- ステップ 1** ポイントツーポイントまたはリニア ADM 上のノードで、「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** 「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を実行します。
- ステップ 3** 各ノードに対して、「DLP-A189 1+1 現用スロットがアクティブであることの確認」(p.18-59) を行います。
- ステップ 4** ポイントツーポイント型またはリニア ADM スパンをサポートしている各 1+1 保護グループに対して、「DLP-A155 保護グループの削除」(p.18-25) を行います。
- ステップ 5** UPSR に組み入れるすべてのノードの保護カードで、「DLP-A377 SDCC 終端のプロビジョニング」(p.20-74) を行います。CTC の管理に必要な帯域幅が不足している場合は、「DLP-A378 LDCC 終端のプロビジョニング」(p.20-77) を行って追加します。
- ステップ 6** 「DLP-A333 回線の削除」(p.20-23) と 「NTP-A343 自動ルーティングによる光回線の作成」(p.6-47) を行い、回線を一度に 1 つずつ削除して再作成します。



- (注) カードが取り付けられていて、DCC が設定されている場合は、UPSR がデフォルトの設定になります。

終了：この手順は、これで完了です。

## NTP-A267 UPSR から 2 ファイバ BLSR への自動変換

目的	この手順では、トラフィックを中断することなく、UPSR を 2 ファイバ BLSR へ変換します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a>
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) 開放型 UPSR と UPSR Dual-Ring Interconnect (DRI; デュアル リング相互接続) の構成では、稼働中のトポロジー アップグレードをサポートしません。



(注) この手順を開始する前に、新しい BLSR を識別するための一意なリング名と、リング上の各ノードに対する一意なノード ID 番号を用意しておく必要があります。



(注) この手順を開始する前に、光の送受信レベルが表 2-4 (p.2-20) に示されている許容範囲内にあることを確認してください。



(注) ネットワークにオーバーヘッド回線が存在している場合は、この手順を実行するとサービスに影響が出ます。この場合、オーバーヘッド回線でトラフィックが廃棄され、アップグレードが完了したときにステータスが PARTIAL になります。

**ステップ 1** UPSR 上のノードで「[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** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。

**ステップ 3** UPSR to BLSR Topology Conversion ダイアログボックスで、BLSR プロパティを設定します。

- Ring Type — (表示専用) デフォルトは、2 ファイバです。
- Speed — OC-12、OC-48、OC-192 から BLSR リングの速度を選択します。速度は BLSR トランク (スパン) カードの OC-N 速度と一致する必要があります。



(注) OC-12 の BLSR を作成しておいて、最終的に OC-48 または OC-192 へアップグレードする場合は、1 ポート OC-12 カード (OC12 IR/STM4 SH 1310、OC12 LR/STM4 SH 1310、または OC12 LR/STM4 LH 1550) を使用します。



- Ring Name — リング名を割り当てます。名前に使用できる文字数は、1 ~ 6 文字です。すべての英数字を大文字と小文字を組み合わせて指定できます。大文字か小文字かに関係なく、文字列 [All] は使用できません。[All] は TL1 のキーワードであるため、拒否されます。すでに他の BLSR に割り当てられている名前も指定できません。
- Reversion time — リングを切り替えたあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。リングの復元を、Never に設定することもできます。

**ステップ 4** Next をクリックします。ネットワークの図が表示されたら、ステップ 5 へ進みます。

取り付けられている光カードの数が不足している場合や、UPSR セレクタのある回線が検出された場合などは、BLSR を作成できません。CTC でそうした状況が判明すると、[Cannot Create BLSR] というメッセージが表示されます。このメッセージが表示された場合は、次のステップを実行します。

- a. OK をクリックします。
- b. Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- c. 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。

**ステップ 5** ネットワークの図で、BLSR のスパン ラインを順番にダブルクリックしていきます。ダブルクリックしたスパン ラインが他の BLSR カードに DCC で接続されていて完全なリングを形成していれば、それらのラインがブルーになります。ラインをダブルクリックしてもまだ完全なリングを形成できていない場合は、完全なリングが作成されるまで別のスパン ラインをダブルクリックしていきます。Next をクリックします。

**ステップ 6** UPSR to BLSR Topology Conversion ダイアログボックスが表示されます。このダイアログボックスに、システムがトラフィックを最短の UPSR パスへ強制的に流すことが表示されます。Next をクリックします。

**ステップ 7** 別のダイアログボックスが開き、トラフィックが最短の UPSR パスに適用されたことが表示されます。Finish をクリックします。

BLSR ウィンドウが開き、作成した BLSR が表示されたら、ステップ 8 へ進みます。[Cannot Create BLSR] または [Error While Creating BLSR] というメッセージが表示された場合は、次の作業を行います。

- a. OK をクリックします。
- b. Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- c. 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。



(注) BLSR の設定時には、E-W-MISMATCH、RING MISMATCH、APSCIMP、APSDFLTK、および BLSROSYNC の各アラームのうち一部またはすべてが一時的に表示されることがあります。

**ステップ 8** 次の点を確認します。

- ネットワーク ビューの図で、すべての BLSR ノード間にグリーンのスパン ラインが表示されていること。
- E-W MISMATCH、RING MISMATCH、APSCIMP、DFLTK、および BLSROSYNC の各アラームがすべてクリアされていること。アラームのトラブルシューティングについては、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。



(注) ノード名の後ろにあるかっこ内の数字は、CTC によって割り当てられた BLSR ノード ID です。1 つの BLSR 内の各 ONS 15454 には、0 ~ 31 の一意なノード ID が割り当てられています。ノード ID を変更する場合は、「[DLP-A326 BLSR のノード ID の変更](#)」(p.20-17)を行います。

終了：この手順は、これで完了です。

---

## NTP-A210 UPSR から 2 ファイバ BLSR への手動変換

目的	この手順では、UPSR を 2 ファイバ BLSR へ手動で変換します。稼働中のトポロジー アップグレードウィザードは使用しません。ウィザードを使用できない場合、またはウィザードをキャンセルして最初から手動で行う場合に、この手順を使用します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a>
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**

この手順は、サービスに影響を与えます。リング上のすべての回線が削除されて再プロビジョニングされます。



**注意**

変換作業を開始する前に、この手順の説明を最後まで熟読してください。



**(注)**

この手順を開始する前に、新しい BLSR を識別するための一意なリング名と、リング上の各ノードに対する一意なノード ID 番号を用意しておく必要があります。



**(注)**

この手順を開始する前に、光の送受信レベルが表 2-4 (p.2-20) に示されている許容範囲内にあることを確認してください。

- ステップ 1** UPSR 上のノードで「[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** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。
- ステップ 3** ネットワーク マップで、現在ログインしているノードの隣接スパンを右クリックします。ショートカットメニューが表示されます。
- ステップ 4** ショートカットメニューで、**Circuits** をクリックします。Circuits on Span ウィンドウが表示されず。
- ステップ 5** アクティブな STS 回線の合計帯域幅が、スパン帯域幅の 50% を超えていないことを確認します。Circuits カラムには、[Unused] というタイトルの付いたブロックがあります。この数値がスパン帯域幅の 50% を超えている必要があります。

スパンが OC-48 の場合、そのスパンでプロビジョニングできる STS の最大数は 24 です。スパンが OC-192 の場合、そのスパンでプロビジョニングできる STS の最大数は 96 です。スパンが OC-12 の場合、そのスパンでプロビジョニングできる STS の最大数は 6 です。

**注意**

帯域幅の半分以上がすでに使用されている場合は、この手順を実行できません。BLSR に変換するには、まだ割り当てられていない帯域幅が 50% 必要です。これらの要件が満たされていない場合は、ローカル手順を参照して、回線を再配置してください。

**ステップ 6** BLSR に変換する UPSR 内の各ノードについて、ステップ 1 ~ 5 を繰り返します。すべてのノードが **ステップ 5** の要件を満たしていれば、次のステップへ進みます。

**ステップ 7** 次の手順で、すべての回線情報を保存します。

- a. ネットワーク ビューで、**Circuits** タブをクリックします。
- b. 次のいずれかの方法で、回線の情報を記録します。
  - File メニューで **Print** をクリックして、回線の表を印刷する。詳細については、「[DLP-A531 CTC データの印刷](#)」(p.22-34) を参照してください。
  - File メニューで **Export** をクリックして、HTML、CSV (カンマ区切り形式)、または TSV (タブ区切り形式) のいずれかのデータ形式を選択します。OK をクリックして、ファイルを一時ディレクトリに保存します。詳細については、「[DLP-A532 CTC データのエクスポート](#)」(p.22-35) を参照してください。

**ステップ 8** 次の手順で、回線を削除します。

- a. ネットワーク ビューで、**Circuits** タブをクリックします。リング上のすべての回線が表示されます。
- b. Ctrl キーを押したまま、各回線をクリックします。選択された各回線は、ダークブルーに変わります。
- c. すべての回線を選択したら、**Delete** をクリックします。処理には数分かかる場合があります。実際の所要時間は、ネットワーク内の回線数によって異なります。

**ステップ 9** 「[NTP-A126 BLSR の作成](#)」(p.5-16) を実行して、BLSR を作成します。

**ステップ 10** 回線を再作成する場合は、[第 6 章「回線と VT トンネルの作成」](#) を参照し、使用する回線の種類に応じた手順を実行します。



**(注)** BLSR にノードを追加する場合は、「[NTP-A212 BLSR ノードの追加](#)」(p.14-2) を参照してください。

**終了** : この手順は、これで完了です。

## NTP-A211 2 ファイバ BLSR から 4 ファイバ BLSR への自動変換

目的	この手順では、トラフィックを中断することなく、2 ファイバ BLSR を 4 ファイバ BLSR へアップグレードします。アップグレードするすべてのノードで同じイースト設定とウェスト設定が使用されている場合、変換作業が簡単になります。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A126 BLSR の作成 (p.5-16)</a>
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) BLSR DRI 構成は、稼働中のトポロジー アップグレードをサポートしません。



(注) 2 ファイバの OC-48 BLSR と OC-192 BLSR は、4 ファイバの BLSR に変換できます。変換する場合は、2 ファイバ BLSR の各ノードに OC-48 または OC-192 カードを 2 枚追加したあと、CTC にログインして、BLSR を 2 ファイバから 4 ファイバに変換します。2 ファイバ BLSR で帯域幅が現用と保護に分割されていたファイバは、これにより現用 BLSR トラフィックに割り当てられます。スパンのアップグレードは、2 ファイバから 4 ファイバ BLSR へ変換する前に行うことができます。



(注) BLSR Protection Channel Access (PCA) 回線が存在していた場合、それらの回線は既存の STS 内にそのまま残されます。そのため、これらの回線は 4 ファイバ BLSR の現用パスに配置され、BLSR の完全な保護を受けます。PCA 回線を 4 ファイバ BLSR の保護チャンネルへ移す場合は、アップグレードしたあとにこれらの回線を削除して、再作成します。たとえば、2 ファイバの OC-48 BLSR を 4 ファイバへアップグレードした場合、2 ファイバ BLSR の保護 STS (STS 25 ~ 48) にある PCA 回線は、既存の STS、つまり、4 ファイバ BLSR の現用 STS にそのまま残されます。OC-48 の PCA 回線を削除して再作成すると、その回線は、4 ファイバ BLSR の保護帯域幅にある STS 1 ~ 24 に移動します。回線の削除については、「[DLP-A333 回線の削除](#)」(p.20-23) を参照してください。回線の作成については、[第 6 章「回線と VT トンネルの作成」](#) を参照してください。



(注) この手順を開始する前に、光の送受信レベルが[表 2-4 \(p.2-20\)](#) に示されている許容範囲内にあることを確認してください。

- ステップ 1** 変換する 2 ファイバ ノードの一方で、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。
- ステップ 2** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。
- ステップ 3** 「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行して、各 BLSR ノードに 2 枚の OC-48 または OC-192 カードを取り付けます。2 ファイバ BLSR と速度が同じ OC-N カードを取り付ける必要があります。

- ステップ 4** 新しいカードにファイバを接続します。2 ファイバ接続を作成する際に使用したものと同一イースト / ウェスト接続方式を使用してください。「[NTP-A247 光ファイバ ケーブルの取り付け](#)」(p.2-18) を参照してください。
- ステップ 5** すべての新しい OC-N カードに対して「[DLP-A214 ポートのサービス状態の変更](#)」(p.19-10) を行い、ポートを稼働状態にします。
- ステップ 6** 現地の標準作業手順に従って、新しいファイバ接続をテストします。
- ステップ 7** BLSR を変換します。
- ネットワーク ビューを表示して、**Provisioning > BLSR** タブをクリックします。
  - 変換する 2 ファイバ BLSR を選択して、**Upgrade to 4 Fiber** ボタンをクリックします。
  - Upgrade BLSR ダイアログボックスで、切り替えの原因となった条件が解決されたあとにトラフィックが元の現用パスに復帰するまでの時間を設定します。デフォルトは 5 分です。
  - Next** をクリックします。
  - 次の手順で、イースト保護ポートとウェスト保護ポートを割り当てます。
    - West Protect — ウェスト保護ファイバに接続するウェスト側の BLSR ポートを、ドロップダウン リストから選択します。
    - East Protect — イースト保護ファイバに接続するイースト BLSR ポートを、ドロップダウン リストから選択します。
  - Finish** をクリックします。
- ステップ 8** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 9** 「[NTP-A1764 ファイバ BLSR の受け入れテスト](#)」(p.5-20) を実行します。

終了：この手順は、これで完了です。

---

## NTP-A159 BLSR の変更

目的	この手順では、BLSR のリング名、ノード ID、または、リングとスパンの復元時間を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A126 BLSR の作成 (p.5-16)</a>
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** 変更する BLSR のノードで、「[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** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。



**(注)** BLSR の設定時には、E-W-MISMATCH、RING MISMATCH、APSCIMP、APSDFLTK、および BLSROSYNC の各アラームのうち一部またはすべてが表示されることがあります。BLSR のすべてのノードを設定すると、これらのアラームはクリアされます。これらのアラームの定義については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 3** BLSR のリング名や、リングまたはスパンの復元時間を変更する場合は、次のステップを実行します。ノード ID を変更する場合は、[ステップ 4](#) へ進みます。

- a. ネットワーク ビューで、**Provisioning** > **BLSR** タブをクリックします。
- b. 変更する BLSR をクリックして、**Edit** をクリックします。
- c. BLSR ウィンドウで、次のいずれかを変更します。
  - Ring Name — リング名を割り当てます。名前に使用できる文字数は、1 ~ 6 文字です。使用できる文字は、0 ~ 9 と A ~ Z の英数字です。数字と文字を組み合わせたり、大文字と小文字を組み合わせたりすることができます。文字列 [All] は、TL1 のキーワードであるため、大文字でも小文字でも使用できません。すでに他の BLSR に割り当てられている名前も指定できません。
  - Reversion time — 必要に応じて、リングを切り替えてからトラフィックが元の現用パスに復元するまでの時間を変更します。
  - Span Reversion — (4 ファイバ BLSR の場合のみ) 必要に応じて、スパンを切り替えてからトラフィックが元の現用パスに復元するまでの時間を変更します。
- d. **Apply** をクリックします。
- e. リング名を変更した場合は、BLSR ウィンドウが自動的に閉じます。復元時間だけを変更した場合は、File メニューで **Close** を選択してウィンドウを閉じます。

**ステップ 4** 必要に応じて、「[DLP-A326 BLSR のノード ID の変更](#)」(p.20-17) を行います。必要がない場合は、[ステップ 5](#) へ進みます。

**ステップ 5** ネットワーク ビューで、次の点を確認します。

- すべての BLSR ノード間に、グリーンのスパン ラインが表示されている。
- E-W MISMATCH、RING MISMATCH、APSCIMP、DFLTK、BLSROSYNC、および Node ID Mismatch の各アラームがすべてクリアされている。



(注) これらのアラームの定義については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

---

終了：この手順は、これで完了です。

---





## ノードの追加と削除

この章では、Bidirectional Line Switched Ring( BLSR; 双方向ライン スイッチ型リング )、Unidirectional Path Switched Ring( UPSR; 単方向パス スイッチ型リング ) およびリニア Add Drop Multiplexer( ADM; 分岐挿入装置 ) ネットワークに対して Cisco ONS 15454 ノードを追加または削除する方法について説明します。

### 準備作業

次の手順を実行する前に、「[NTP-A195 カード、ノード、およびネットワーク プロビジョニングの説明](#)」(p.8-2) を実行します。また、すべてのアラームを調べて、問題を解決しておいてください。必要に応じて、『[Cisco ONS 15454 Troubleshooting Guide](#)』を参照してください。

この章では次の NTP (手順) について説明します。適用する DLP (作業) については、各手順を参照してください。

1. [NTP-A212 BLSR ノードの追加](#) (p.14-2) — 必要に応じて、この手順を実行します。
2. [NTP-A240 BLSR ノードの削除](#) (p.14-7) — 必要に応じて、この手順を実行します。
3. [NTP-A105 UPSR ノードの追加](#) (p.14-11) — 必要に応じて、この手順を実行します。
4. [NTP-A294 UPSR ノードの削除](#) (p.14-14) — 必要に応じて、この手順を実行します。
5. [NTP-A262 リニア ADM へのノードの追加](#) (p.14-16) — リニア ADM の終端にノードを追加する場合は、必要に応じてこの手順を実行します。この手順は、2 つの ADM ノード間でノードを追加する場合に使用できます。ただし、回線をいったん削除してから再作成する必要があります。トラフィックを中断することなくノードを追加する場合は、次の手順を実行します。
6. [NTP-A323 ウィザードによるリニア ADM へのノードの追加](#) (p.14-18) — 2 つのリニア ADM ノード間にノードを追加する場合は、必要に応じてこの手順を実行します。
7. [NTP-A313 リニア ADM からの稼働中のノードの削除](#) (p.14-21) — トラフィックを中断することなくリニア ADM からノードを削除する場合は、必要に応じてこの手順を実行します。

## NTP-A212 BLSR ノードの追加

目的	この手順では、ノードを追加して BLSR を拡張します。
工具 / 機器	新規ノードを接続するためのファイバ
事前準備手順	BLSR へ追加するノードにカードを取り付けて、ノードの起動手順を完了しておく必要があります。第2章「カードおよび光ファイバケーブルの取り付け」と第4章「ノードの起動」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
セキュリティ レベル	プロビジョニング以上のレベル

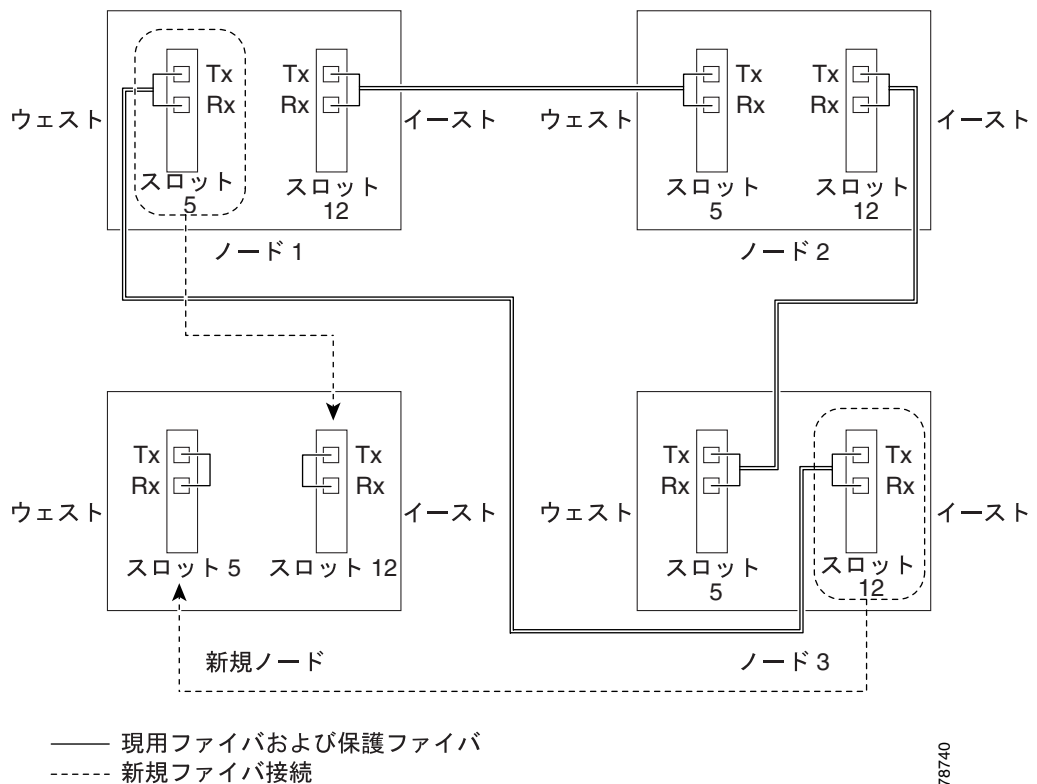


**注意**

BLSR ノードの追加はサービスに影響する可能性があるため、保守時間中に作業を行ってください。

- ステップ 1** ノードを追加する BLSR の図を描きます。この図で、新しいノードに接続する東と西の BLSR OC-N トランク (スパン) カードが分かるようにしておきます。この情報は、この手順を間違えないで実行するために重要です。図 14-1 に、3 ノードから構成される 2 ファイバの BLSR を示します。各ノードで、BLSR トランク カードにスロット 5 と 12 を使用しています。点線の矢印は、4 番めのノードを BLSR に追加するために作成する新しいファイバ接続を示しています。

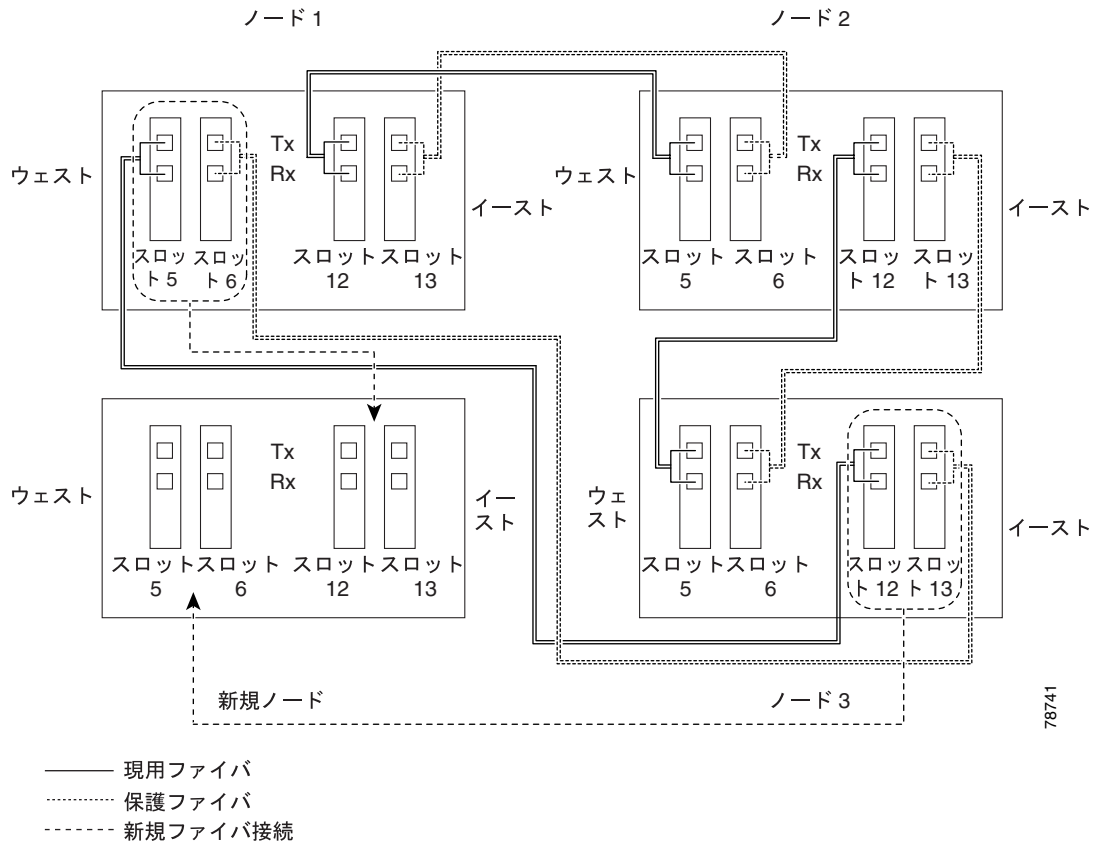
図 14-1 4 番めのノードを追加する前の 3 ノード、2 ファイバの BLSR



78740

図 14-2 に、3 ノードから構成される 4 ファイバ BLSR の例を示します。点線の矢印は、4 番めのノードを追加するために作成する新しいファイバ接続を示しています。4 ファイバ BLSR の場合は、現用ファイバと保護ファイバの 2 つのファイバセットを再接続します。

図 14-2 4 番めのノードを追加する前の 3 ノード、4 ファイバの BLSR



**ステップ 2** 現地の状況に合わせて、リング内のすべてのノードについて「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 3** 「[NTP-A323 カードの取り付けの確認](#)」(p.4-2) で、新しいノードにカードが取り付けられていることを確認します。BLSR トランク カードとなる OC-N カードの光伝送速度が BLSR の光伝送速度と同じであることを確認します。たとえば、BLSR が OC-48 の場合は、新しいノードに OC-48 カードが取り付けられている必要があります。OC-N カードが取り付けられていないか、光伝送速度が BLSR と同じでない場合は、「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行します。

**ステップ 4** 新しいノードを既存のノードに接続するためのファイバがあることを確認します。[ステップ 1](#) の図を参照してください。

**ステップ 5** 「[NTP-A35 ノードの起動の確認](#)」(p.5-3) を実行します。追加した新しいノードを CTC で表示させるには、そのノードの権限があること、およびそのノードに IP 接続できることが必要です。

**ステップ 6** 次の条件が満たされている場合は、新しいノードに関するスタティック ルートを作成します。この状態になっていない場合は、[ステップ 7](#) へ進みます。

- 新しいノードの IP アドレスがネットワークの他のノードと同じサブネットにある。

- 新しいノードの Provisioning > Network > General サブタブで、Gateway Settings の Craft Access Only がオフになっている。
- CTC コンピュータが新しいノードに直接接続されている。
- CTC コンピュータが同じサブネット内の他のノードに直接接続されている。

上記の条件が満たされている場合は、次の設定を使用して、BLSR に追加するノードに関するスタティックルートを追加します。

- 宛先 IP アドレス：IP-address-of-the-CTC-computer-connected-to-the-new-node
- ネットマスク：255.255.255.255
- ネクスト ホップ：IP-address-of-the-Cisco-ONS-15454
- コスト：1

「DLP-A65 スタティック ルートの作成」(p.17-78) を参照してください。ゲートウェイの設定を表示する場合は、「DLP-A249 IP 設定のプロビジョニング」(p.19-35) を参照してください。

**ステップ 7** BLSR 上のノードで「DLP-A60 CTC へのログイン」(p.17-71) を行います。

**ステップ 8** 「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を行って、BLSR に Major アラームや問題がないことを確認します。問題がある場合 (Major アラームが存在する場合など) は、問題を解決してから次へ進みます。第 8 章「アラームの管理」を参照してください。また、必要に応じて『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 9** View メニューから、Go to Network View を選択し、Provisioning > BLSR タブをクリックします。

**ステップ 10** リング名、リングタイプ、回線レート、リングの復元時間、およびスパンの復元時間 (4 ファイバ) を紙に記録します。

**ステップ 11** Node カラムに表示されている BLSR のノード ID を記録します。ノード ID は、ノード名の隣にあるカッコ内の数字です。

**ステップ 12** 次のようにして、新しいノードにログインします。

- ノードが LAN に接続されていて、ネットワーク マップに表示されている場合は、View メニューから Go to Other Node を選択し、続いて新しいノードに入ります。
- 新しいノードがネットワークに接続されていない場合は、「DLP-A60 CTC へのログイン」(p.17-71) の手順に従ってノードにログインします。

**ステップ 13** 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-A227 アラーム フィルタリングのディセーブル化」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 14** ステップ 10 と 11 で記録した情報とステップ 1 で作成した図を使用して、新しいノードに BLSR を作成します。「DLP-A242 単一ノードでの BLSR の作成」(p.19-28) を参照してください。

**ステップ 15** (任意) BLSR トランク カードを経由するテスト回線を作成し、テストトラフィックをノードに流して、カードが適切に機能することを確認します。詳細は、「NTP-A344 手動ルーティングによる光回線の作成」(p.6-54) と「NTP-A62 光回線のテスト」(p.6-63) を参照してください。

**ステップ 16** 新しいノードに Data Communication Channel (DCC; データ通信チャネル) の終端を作成します。「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を参照してください。



**(注)** DCC の終端を作成すると、SDCC Termination Failure と Loss of Signal (LOS; 信号損失) のアラームが表示されます。これらのアラームは、ノードを BLSR に接続するまでクリアされません。



**(注)** K3 バイトを別のバイト (E2 など) にマップする場合は、新しいノードのいずれかの側のラインカードを同じバイトにマップし直す必要があります。「[DLP-A89 K3 バイトの再マップ](#)」(p.17-94) を参照してください。

**ステップ 17** 新しいノードに接続する BLSR ノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。

**ステップ 18** [ステップ 1](#) で作成した図を参照して、新しいノードのウェストライン (ポート) に接続するノード上で「[DLP-A303 BLSR 強制リング切り替えの開始](#)」(p.20-3) を行います。[図 14-2](#) の例では、ノード 1 のウェストライン (スロット 5 と 6) で BLSR の強制リング切り替えが発生します。

**ステップ 19** [ステップ 1](#) で作成した図を参照して、新しいノードのイーストライン (ポート) に接続するノード上で「[DLP-A303 BLSR 強制リング切り替えの開始](#)」(p.20-3) を行います。[図 14-2](#) の例では、ノード 3 のイーストライン (スロット 12 と 13) で BLSR の強制リング切り替えが発生します。

**ステップ 20** Alarms タブをクリックします。

- 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-A227 アラームフィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 21** [ステップ 1](#) で作成した図に従って、新しいノードに接続する 2 つのノードからファイバ接続を取り外します。

- 新しいノードのイーストポートに接続するノードから、ウェスト側のファイバを取り外します。[図 14-1](#) の例では、ノード 1 のスロット 5 がこれに該当します。また [図 14-2](#) では、ノード 1 のスロット 5 と 6 がこれに該当します。
- 新しいノードのウェストポートに接続するノードから、イースト側のファイバを取り外します。[図 14-1](#) の例では、ノード 3 のスロット 12 がこれに該当します。また [図 14-2](#) では、ノード 3 のスロット 12 と 13 がこれに該当します。

**ステップ 22** [ステップ 1](#) で作成した図に従って、隣接ノードから新しいノードへファイバを接続します。ウェストポートをイーストポートに接続し、イーストポートをウェストポートに接続します。4 ファイバ BLSR の場合は、保護ファイバを接続します。

**ステップ 23** 新しく追加したノードがネットワークビューに表示されたら、そのノードをダブルクリックしてノードビューに表示します。

**ステップ 24** Provisioning > BLSR タブをクリックします。

**ステップ 25** Ring Map をクリックします。新しいノードが他の BLSR ノードとともにリング マップに表示されることを確認して、OK をクリックします。

**ステップ 26** View メニューから Go to Network View を選択して、次の確認を行います。

- a. Provisioning > BLSR タブをクリックします。新しいノードが Node カラムに表示されていることを確認します。
- b. Alarms タブをクリックします。RING MISMATCH、E-W MISMATCH、PRC-DUPID (重複ノード ID)、APSCDFLTK (デフォルト K) などの BLSR アラームが表示されていないことを確認します。

新しいノードが Node カラムに表示されていないか、または BLSR アラームが表示されている場合は、新しいノードにログインして、BLSR がステップ 10 と 11 の情報で正しくプロビジョニングされていることを確認します。それでもノードが表示されないか、またはアラームが消えない場合は、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 27** Circuits タブをクリックします。すべての回線が検出されるのを待ちます。新しいノードを経由する回線が不完全な形で表示されます。



**(注)** 1分経っても回線が表示されない場合は、いったん CTC からログアウトしたあと、再度ログインします。

**ステップ 28** ネットワーク ビューで新しいノードを右クリックし、ショートカットメニューから Update Circuits With The New Node を選択します。ダイアログボックスに更新された回線が表示されるので、その数が正しいことを確認します。

**ステップ 29** それでも不完全な回線が表示される場合は、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 30** History タブをクリックします。BLSR 内のすべてのノードについて、BLSR\_RESYNC 状態が表示されていることを確認します。

**ステップ 31** 「DLP-A194 BLSR 強制リング切り替えのクリア」(p.18-65)を行い、BLSR のイーストラインとウェストラインからリング切り替えを削除します。

**ステップ 32** 現地の状況に合わせて、「NTP-A175 2 ファイバ BLSR の受け入れテスト」(p.5-17)または「NTP-A176 4 ファイバ BLSR の受け入れテスト」(p.5-20)を実行します。

**終了:** この手順は、これで完了です。

## NTP-A240 BLSR ノードの削除

目的	この手順では、ノードから BLSR リングを 1 つまたは複数削除します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A126 BLSR の作成 (p.5-16)</a>
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

次の手順では、ノードを削除しているときのトラフィックの停止を最小限に抑えることができます。削除するノードに起点または終点のある回線をすべて削除します。さらに、ノードをパスする回線が別の STS または VT (またはその両方) に入出力していないことを確認します。該当する回線がある場合は、その回線を削除して再作成することになり、その間のトラフィックが損失します。

- ステップ 1** 現地の状況に合わせて、リング内のすべてのノードについて「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 2** BLSR から削除するノードで、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。
- ステップ 3** 「[DLP-A195 縮小されたリングで使用されているタイミングの確認](#)」(p.18-66) を実行します。



**(注)** リングで使用されている唯一の Building Integrated Timing Supply (BITS) であるノードを削除すると、そのリングのすべてのノードに対して唯一の同期ソースを失うことになります。リングの回線の中に、Stratum 1 クロックに同期している他のネットワークと接続している回線があると、高いレベルでポイント調整が行われるため、トラフィックのパフォーマンスに悪影響を与える可能性があります。

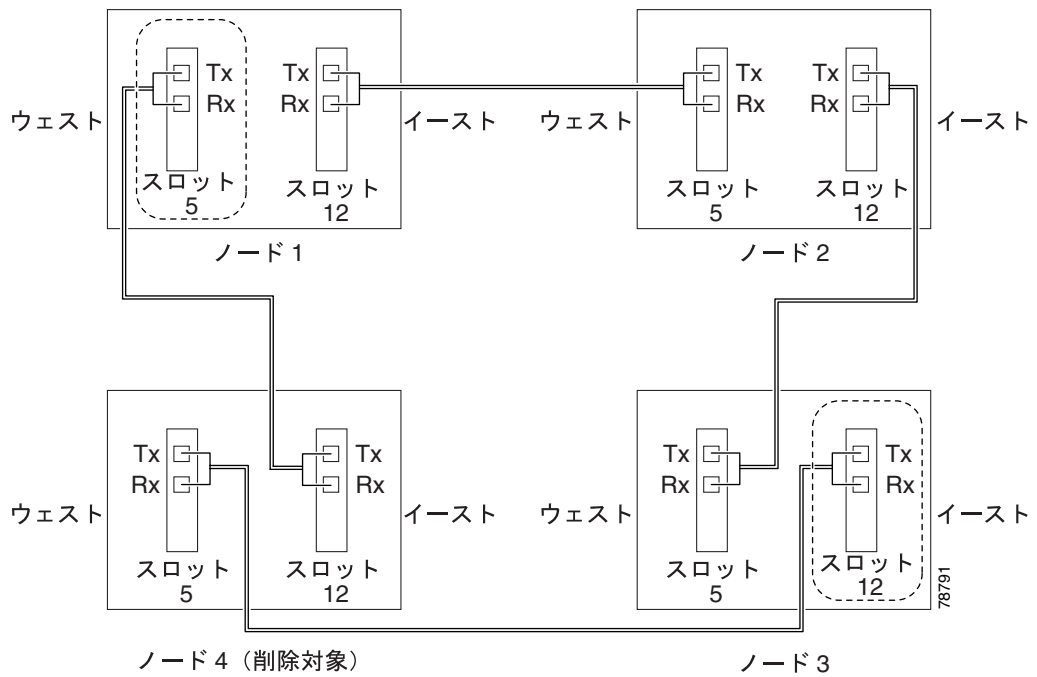
- ステップ 4** ノードを削除する BLSR の図を作成します。手で BLSR を描くこともできますが、次の手順で CTC から印刷することもできます。
- View メニューから **Go to Network View** を選択します。
  - Provisioning > BLSR** タブをクリックします。
  - 必要な BLSR を選択して、**Edit** をクリックします。
  - BLSR ウィンドウにポートの情報がすべて表示されていることを確認します。表示されない部分があれば、**Ctrl** を押してノード アイコンを別の場所にドラッグし、情報が表示されるようにします。
  - 「[DLP-A531 CTC データの印刷](#)」(p.22-34) を実行します。
  - File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。
- ステップ 5** BLSR の図を参照して、次のノードを識別します。

- ウェストポート経由で対象 (削除する) ノードに接続されているノード。たとえば、[図 14-3](#) のノード 4 を削除した場合、ウェストポート経由でノード 4 に接続されているのはノード 1 です。

- イーストポート経由で対象（削除する）ノードに接続されているノード。図 14-3 の場合、イーストポート経由でノード 4 に接続されているのはノード 3 です。

ノード内の BLSR リングのロットとポートを記録します。

図 14-3 ノードを削除する前の 4 ノード、2 ファイバの BLSR



- ステップ 6** 「DLP-A298 ネットワーク上のアラームおよび状態のチェック」(p.19-71) を行って、BLSR にアラームがないことを確認します。問題がある場合（Major アラームが存在する場合など）は、問題を解決してから次へ進みます。第 8 章「アラームの管理」を参照してください。また、必要に応じて『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- ステップ 7** View メニューから **Go to Other Node** を選択します。削除するノードを選択して、**OK** をクリックします。
- ステップ 8** **Circuits** タブをクリックします。Scope 設定が Network になっている場合は、Scope ドロップダウンリストから **Node** を選択します。すべての回線が表示されるように Filter ボタンがオフになっている（インデントされていない）ことを確認します。
- ステップ 9** ノードに起点または終点のあるすべての回線を削除します。「DLP-A333 回線の削除」(p.20-23) を参照してください。
- ステップ 10** 「DLP-A442 パススルー回線の確認」(p.21-24) を実行して、対象ノードをパススルーする回線が同じ STS または VT（またはその両方）上のノードに出入りしていることを確認します。K3 拡張バイトマッピングは、すべての ONS 15600 OC-48 トラフィックカードと OC-192 トラフィックカード、および ONS 15454 OC-48 AS カードでサポートされています。
- ステップ 11** View メニューから **Go to Network View** を選択します。



**ステップ 12** ステップ 4 で作成した図を参照して、対象(削除する)ノードに接続している各ノードで「DLP-A303 BLSR 強制リング切り替えの開始」(p.20-3)を行い、トラフィックがそのノードを通らないようにします。強制切り替えは、対象ノードに接続されている各ポートで実行する必要があります。たとえば、図 14-3 では、ノード 3 のイーストポートとノード 1 のウェストポートで強制切り替えを実行します。

**ステップ 13** 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-A227 アラームフィルタリングのディセーブル化」(p.19-21)を参照してください。
- b. 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 14** 削除するノードと 2 つの近接ノードを接続しているすべてのファイバを取り外します。

**ステップ 15** BLSR ノードを削除したあとに接続する 2 つのノードに OC-48 AS トランク(スパン)カードがあって、その K3 バイトが再マップされている場合は、「DLP-A422 BLSR の拡張バイトマッピングの確認」(p.21-7)を行います。それ以外の場合は、ステップ 16 へ進みます。

**ステップ 16** 2 つの近接ノードを結ぶファイバを、ウェストポートからイーストポートに直接再接続します。たとえば、図 14-3 では、ノード 3 (スロット 12) のイーストポートをノード 1 (スロット 5) のウェストポートに接続します。

**ステップ 17** 次の手順を実行します。

- a. View メニューから **Go to Other Node** を選択します。新しく接続したノードの 1 つを選択し、**OK** をクリックします。
- b. **Provisioning > BLSR** タブをクリックします。
- c. 削除したノードが含まれていた BLSR を選択し、**Ring Map** をクリックします。
- d. 削除したノードがリストに表示されなくなるまで、待ちます。
- e. 新規接続された BLSR 内のその他のノードで、ステップ a ~ d を繰り返します。

**ステップ 18** 「DLP-A196 単一ノードからの BLSR の削除」(p.18-67)を実行します。

**ステップ 19** History タブをクリックします。BLSR 内のすべてのノードについて、BLSR\_RESYNC 状態が表示されていることを確認します。

**ステップ 20** 「DLP-A194 BLSR 強制リング切り替えのクリア」(p.18-65)を行って、強制保護切り替えを削除します。

**ステップ 21** 現地の状況に合わせて、「NTP-A175 2 ファイバ BLSR の受け入れテスト」(p.5-17)を実行します。

**ステップ 22** 「DLP-A371 パススルー接続の削除」(p.20-61)を実行します。

**ステップ 23** 縮小したリングのノードに再度ログインします。CTC の Login ダイアログボックスで **Disable Network Discovery** チェックボックスをオフにします。



**(注)** 削除したノードは、すべての SDCC 終端が削除されるまでネットワーク ビューに表示され続けます。SDCC の終端を削除するには、「[DLP-A156 SDCC 終端の削除](#)」(p.18-25)を行います。

**ステップ 24** Circuits タブをクリックして、不完全な回線が存在しないことを確認します。不完全な回線が表示される場合は、ステップ 22 ~ 23 を繰り返します。

**ステップ 25** ログイン ノード グループにあったノードを削除すると、CTC のネットワーク ビューでそのノードの回線が正しく表示されなくなります。削除されたノードはすでにリングから外されていますが、ログイン ノード グループから削除されるまでは CTC に表示され続けます。必要な場合は、「[DLP-A372 指定したログイン ノード グループからのノードの削除](#)」(p.20-62)を行います。

**ステップ 26** BLSR から別のノードを削除するには、そのノードに対してこの手順を繰り返します。

**ステップ 27** 現地の状況に合わせて、「[NTP-A175 2 ファイバ BLSR の受け入れテスト](#)」(p.5-17)または「[NTP-A176 4 ファイバ BLSR の受け入れテスト](#)」(p.5-20)を実行します。

**終了：**この手順は、これで完了です。

## NTP-A105 UPSR ノードの追加

目的	この手順では、UPSR にノードを追加します。
工具 / 機器	なし
事前準備手順	UPSR へ追加するノードにカードを取り付けて、ノードの起動手順を完了しておく必要があります。第 2 章「カードおよび光ファイバケーブルの取り付け」と第 4 章「ノードの起動」を参照してください。  NTP-A44 UPSR ノードのプロビジョニング (p.5-27)
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** 現地の状況に合わせて、リング内のすべてのノードについて「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 2** ノードを追加する UPSR の既存ノードにログインします。手順については、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を参照してください。追加した新しいノードを CTC で表示させるには、そのノードの権限があること、およびそのノードに IP 接続できることが必要です。
- ステップ 3** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を行って、UPSR に Major アラームや問題がないことを確認します。問題がある場合 (Major アラームが存在する場合など) は、問題を解決してから次へ進みます。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 4** 新しいノードにカードが取り付けられていることを確認します。「[NTP-A323 カードの取り付けの確認](#)」(p.4-2) を参照してください。UPSR トランク (スパン) カードとなる OC-N カードの光伝送速度が、新しいノードの接続先であるトランク カードの UPSR 光伝送速度と同じであることを確認します。たとえば、隣接ノードに OC-48 トランク カードがある場合は、新しいノードに OC-48 カードが取り付けられている必要があります。OC-N カードが取り付けられていないか、光伝送速度が隣接ノードのトランク カードの光伝送速度と同じでない場合は、「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行してカードを取り付けます。
- ステップ 5** 新しいノードを既存のノードに接続するためのファイバがあることを確認します。
- ステップ 6** 「[NTP-A35 ノードの起動の確認](#)」(p.5-3) を実行します。
- ステップ 7** 次の状態になっているかどうかを調べます。
- 新しいノードの IP アドレスがネットワークの他のノードと同じサブネットにある。
  - 新しいノードの Provisioning > Network > General サブタブで、Gateway Settings の Craft Access Only がオフになっている。
  - CTC コンピュータが新しいノードに直接接続されている。
  - CTC コンピュータが同じサブネット内の他のノードに直接接続されている。
- この状態になっていない場合は、[ステップ 8](#) へ進みます。この状態になっている場合は、UPSR に追加するノードで「[DLP-A65 スタティック ルートの作成](#)」(p.17-78) を行います。次のように設定します。
- 宛先 IP アドレス : *IP-address-of-the-CTC-computer-connected-to-the-new-node*
  - ネット マスク : 255.255.255.255

- ネクスト ホップ : *IP-address-of-the-Cisco-ONS-15454*
- コスト : 1

ゲートウェイの設定を表示する場合は、「[DLP-A249 IP 設定のプロビジョニング](#)」(p.19-35) を参照してください。

**ステップ 8** 次のようにして、新しいノードにログインします。

- ノードが LAN に接続されていて、ネットワーク マップに表示されている場合は、View メニューから **Go to Other Node** を選択し、続いて新しいノードに入ります。
- 新しいノードがネットワークに接続されていない場合は、「[DLP-A60 CTC へのログイン](#)」(p.17-71) の手順に従ってノードにログインします。

**ステップ 9** Alarms タブをクリックします。Critical アラームまたは Major アラーム、あるいは LOS、LOF、AIS-L、SF、SD などのファシリティ アラームが存在していないことを確認します。問題がある場合 (Major アラームが存在する場合など) は、問題を解決してから次へ進みます。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 10** (任意) UPSR トランク カードを経由するテスト回線を作成し、テストトラフィックをノードに流して、カードが適切に機能することを確認します。詳細は、「[NTP-A344 手動ルーティングによる光回線の作成](#)」(p.6-54) と「[NTP-A62 光回線のテスト](#)」(p.6-63) を参照してください。

**ステップ 11** 新しいノードに DCC の終端を作成します。「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を参照してください。

**ステップ 12** View メニューから **Go to Network View** を選択します。

**ステップ 13** 「[DLP-A197 UPSR 強制切り替えの開始](#)」(p.18-68) を行って、トラフィックが切断するスパンを通らずに新しいノードへ流れるように切り替えます。

**ステップ 14** 2つのノードを新しいノードに直接接続することになるので、これら2つのノードを接続しているファイバを次のようにして切断します。

- a. 新しいノードのウェストポートに接続するノードから、イースト側のファイバを切断します。
- b. 新しいノードのイーストポートに接続するノードから、ウェスト側のファイバを切断します。

**ステップ 15** 切断したファイバを、新しいノードに接続しているファイバに置き換えます。

**ステップ 16** CTC からログアウトして、ネットワークのノードにログインしなおします。

**ステップ 17** View メニューから **Go to Network View** を選択して、UPSR ノードを表示します。ネットワークマップに新しいノードが表示されます。すべてのノードが表示されるまで数分待ちます。

**ステップ 18** Circuits タブをクリックし、スパンも含めてすべての回線が表示されるのを待ちます。不完全な回線の数数を数えます。



(注) ネットワーク内のノードに UNEQ-P アラームが表示されることがあります。これは通常の状態であり、回線が更新されると、アラームはクリアされます。

**ステップ 19** ネットワーク ビューで新しいノードを右クリックし、ショートカットメニューから **Update Circuits With New Node** を選択します。確認のダイアログボックスが表示されるのを待ちます。ダイアログボックスに更新された回線が表示されるので、その数が正しいことを確認します。

**ステップ 20** Circuits タブをクリックして、不完全な回線が存在しないことを確認します。



**(注)** 1 分経っても回線が表示されない場合は、いったん CTC からログアウトしたあと、再度ログインします。

**ステップ 21** 「[DLP-A198 UPSR 強制切り替えのクリア](#)」(p.18-69) を行って、保護切り替えをクリアします。

**ステップ 22** 現地の状況に合わせて、「[NTP-A177 UPSR の受け入れテスト](#)」(p.5-29) を実行します。

**終了：**この手順は、これで完了です。

---

## NTP-A294 UPSR ノードの削除

目的	この手順では、ノードから UPSR を 1 つまたは複数削除します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a>
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

次の手順では、ノードを削除しているときのトラフィックの停止を最小限に抑えることができます。



### 注意

リングで使用されている唯一の BITS タイミングソースであるノードを削除すると、そのリング内のすべてのノードに対して唯一の同期ソースを失うこととなります。リングの回線の中に、Stratum 1 クロックに同期している他のネットワークと接続している回線があると、高いレベルでポイント調整が行われるため、カスタマー サービスに悪影響を与える可能性があります。

- ステップ 1** ノードを削除する UPSR の図を作成します。その図で次のノードを特定します。
  - ウェストポート経由で削除対象ノードに接続されているノード。
  - イーストポート経由で削除対象ノードに接続されているノード。
- ステップ 2** UPSR ノードを削除するネットワーク内のノードで、「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 3** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71)を行って、UPSR にアラームがないことを確認します。問題がある場合 (Major アラームが存在する場合など) は、問題を解決してから次へ進みます。第 8 章「[アラームの管理](#)」を参照してください。また、必要に応じて『[Cisco ONS 15454 Troubleshooting Guide](#)』を参照してください。
- ステップ 4** 削除するノードに起点または終点がある回線について、「[DLP-A333 回線の削除](#)」(p.20-23)を実行します (回線に複数の分岐がある場合は、削除するノードで終了する分岐だけを削除します)。
- ステップ 5** 「[DLP-A442 パススルー回線の確認](#)」(p.21-24)を行って、対象ノードをパススルーする回線が、同じ STS のノードに出入りしていることを確認します。
- ステップ 6** 削除するノードに接続されているすべてのスパンについて、「[DLP-A197 UPSR 強制切り替えの開始](#)」(p.18-68)を行います。
- ステップ 7** 削除するノードと 2 つの隣接ノードを接続しているすべてのファイバを取り外します。
- ステップ 8** 2 つの隣接ノードを結ぶファイバを、ウェストポートからイーストポートに直接再接続します。
- ステップ 9** CTC を終了してログインしなおします。詳細については、「[DLP-A60 CTC へのログイン](#)」(p.17-71)を参照してください。

- ステップ 10** 新しく接続した各ノードにログインして、Alarms タブをクリックします。スパン カードにアラームが発生していないことを確認します。すべてのアラームを解決してから次に進みます。『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- ステップ 11** 「DLP-A195 縮小されたリングで使用されているタイミングの確認」(p.18-66) を実行します。
- ステップ 12** 「DLP-A198 UPSR 強制切り替えのクリア」(p.18-69) を行って、保護切り替えをクリアします。
- ステップ 13** 「NTP-A177 UPSR の受け入れテスト」(p.5-29) を実行します。
- ステップ 14** 「DLP-A371 パススルー接続の削除」(p.20-61) を実行します。
- ステップ 15** 縮小したリングのノードに再度ログインします。CTC の Login ダイアログボックスで Disable Network Discovery チェックボックスをオフにします。



**(注)** 削除したノードは、すべての SDCC 終端が削除されるまでネットワーク ビューに表示され続けます。SDCC の終端を削除するには、「DLP-A156 SDCC 終端の削除」(p.18-25) を行います。

- ステップ 16** Circuits タブをクリックして、不完全な回線が存在しないことを確認します。不完全な回線が表示される場合は、ステップ 14 ~ 15 を繰り返します。
- ステップ 17** ログイン ノード グループにあったノードを削除すると、CTC のネットワーク ビューでそのノードの回線が正しく表示されなくなります。削除されたノードはすでにリングから外されていますが、ログイン ノード グループから削除されるまでは CTC に表示され続けます。必要な場合は、「DLP-A372 指定したログイン ノード グループからのノードの削除」(p.20-62) を行います。
- ステップ 18** UPSR から別のノードを削除するには、そのノードに対してこの手順を繰り返します。

**終了：**この手順は、これで完了です。

## NTP-A262 リニア ADM へのノードの追加

目的	この手順では、ONS 15454 リニア ADM ネットワークの終端に、ONS 15454 ノードを 1 つ追加します。リニア ADM にトラフィックが流れている場合は、回線を削除して再作成しないかぎり、この手順を使用して 2 つのリニア ADM ノード間にノードを追加することはできません。回線の削除と再作成を行わないようにするには、「 <a href="#">NTP-A323 ウィザードによるリニア ADM へのノードの追加</a> 」(p.14-18) を使用して、2 つのリニア ADM ノード間にノードを追加します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A38 リニア ADM ネットワークのプロビジョニング</a> (p.5-9)
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)

[表 2-4 \(p.2-20\)](#) にある各カードの仕様に示されているように、光の送受信レベルが許容範囲内にある必要があります。



(注)

リニア ADM 構成では、1+1 保護の 2 つの OC-N カードが、2 番めのノードにある 1+1 保護の 2 つの OC-N カードに接続されます。2 番めのノードでは、さらに 2 つの OC-N カードが 3 番めのノードに接続されます。リニア ADM の数によっては、3 番めのノードがさらに 4 番めのノードに接続される、というように続きます。ノード間の接続に一貫性があれば、スロット 1 ~ 4 と 14 ~ 17、またはスロット 5 ~ 6 と 12 ~ 13 を使用できます。たとえば、現用パス用には最初のリニア ADM ノードのスロット 5 を 2 番めのリニア ADM ノードのスロット 5 に接続し、保護パス用にはスロット 6 をスロット 6 に接続します。現用の OC-N ポートには DCC の終端があり、OC-N カードは 1+1 保護グループにあります。

- ステップ 1** 現地の状況に合わせて、リング内のすべてのノードについて「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 2** 新しいノードで、次のいずれかの手順を実行します。
- ノードが起動していない場合は、[第 4 章「ノードの起動」](#)に記載されているすべての手順を実行します。
  - ノードが起動している場合は、「[NTP-A35 ノードの起動の確認](#)」(p.5-3) を実行します。
- ステップ 3** リニア ADM と同じ速度の 2 つの OC-N カードが新しいノードに取り付けられていることを確認します。OC-N カードが取り付けられていない場合は、「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行します。
- ステップ 4** リニア ADM ノードに接続する 2 つの OC-N カードについて、「[DLP-A73 1+1 保護グループの作成](#)」(p.17-87) を行います。



**ステップ 5** 新しいノードの現用 OC-N カードについて、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74)を行います。Create SDCC Termination ダイアログボックスのポート サービス状態が IS に設定されていることを確認してください (保護カードに DCC の終端を作成しないようにしてください)。



(注) [ステップ 12](#) でリニア ADM ノードに DCC の終端を作成してファイバを接続するまで、DCC 障害アラームが表示されます。

**ステップ 6** 新しいノードに接続するリニア ADM 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 7](#) へ進みます。

**ステップ 7** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を実行します。

**ステップ 8** 新しいノードに接続する OC-N カードを取り付けます。「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を参照してください。カードがすでに取り付けられている場合は、[ステップ 9](#) へ進みます。

**ステップ 9** 既存のリニア ADM ノードに取り付けられている現用カードを、新しいノードの現用カードに接続します。「[DLP-A428 1+1 構成での光ファイバケーブルの取り付け](#)」(p.21-8) を参照してください。

**ステップ 10** 既存のリニア ADM ノードに取り付けられている保護カードを、新しいノードの保護カードに接続します。

**ステップ 11** 新しいノードに接続する 2 つの OC-N カードについて、「[DLP-A73 1+1 保護グループの作成](#)」(p.17-87) を行います。

**ステップ 12** 新しいノードの現用カードに接続する現用 OC-N カードについて、「[DLP-A377 SDCC 終端のプロビジョニング](#)」(p.20-74) を行います。Create SDCC Termination ダイアログボックスのポート サービス状態が IS に設定されていることを確認してください (保護カードに DCC の終端を作成しないようにしてください)。

**ステップ 13** View メニューで、Go to Network View を選択します。新しく作成したりニア ADM の構成が正しいことを確認します。各リニア ノード間には、グリーンのスパン ラインが 2 本表示されています。

**ステップ 14** 「[DLP-A298 ネットワーク上のアラームおよび状態のチェック](#)」(p.19-71) を行って、想定外のアラームまたは状態が表示されていないことを確認します。

終了：この手順は、これで完了です。

## NTP-A323 ウィザードによるリニア ADM へのノードの追加

目的	この手順では、1+1 保護グループ内の 2 つのノード間に、トラフィックを損失することなくノードを追加します。
工具 / 機器	アップグレードに必要な互換ハードウェア
事前準備手順	アプリケーションによっては、減衰器が必要となる場合があります。稼働中のトポロジー アップグレード手順では、追加するノードに到達できる (CTC と IP 接続されている) 必要があります。CTC の動作している PC と ONS 15454 が別々の場所にある場合は、2 人の技術者をそれぞれの場所に配置して、アップグレード中にお互いに連絡を取り合えるようにし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
セキュリティ レベル	プロビジョニング以上のレベル



(注) 表 2-4 (p.2-20) にある各カードの仕様で示されているように、OC-N の送受信レベルが許容範囲内にある必要があります。



(注) ネットワークにオーバーヘッド回線が存在している場合は、稼働中のトポロジー アップグレードを実行するとサービスに影響が出ます。この場合、オーバーヘッド回線でトラフィックが廃棄され、アップグレードが完了したときにステータスが PARTIAL になります。

- ステップ 1** 新しいノードに接続するリニア ADM 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** ネットワーク ビューで、新しいノードを追加する 2 つのノード間のスパンを右クリックします。ダイアログボックスが表示されます。
- ステップ 3** Upgrade Protection を選択します。ドロップダウン リストが表示されます。
- ステップ 4** Terminal to Linear を選択すると、Upgrade Protection: Terminal to Linear ダイアログ ボックスの最初のページが表示されます。
- ステップ 5** ダイアログボックスに、新しいノードを追加するために必要な次の条件が表示されます。
- 終端ノードに Critical アラームも Major アラームもない。
  - 追加するノードに Critical アラームも Major アラームもない。
  - そのノードと終端ノードのソフトウェア バージョンに互換性がある。
  - 1+1 保護の速度に合った未使用の光ポートがノードに 4 つ存在し、それら 4 つのポートに DCC がプロビジョニングされていない。
  - 追加するノードを終端ノードに接続するためのファイバがある。
- これらの条件がすべて満たされていて、この手順を続ける場合は、Next をクリックします。

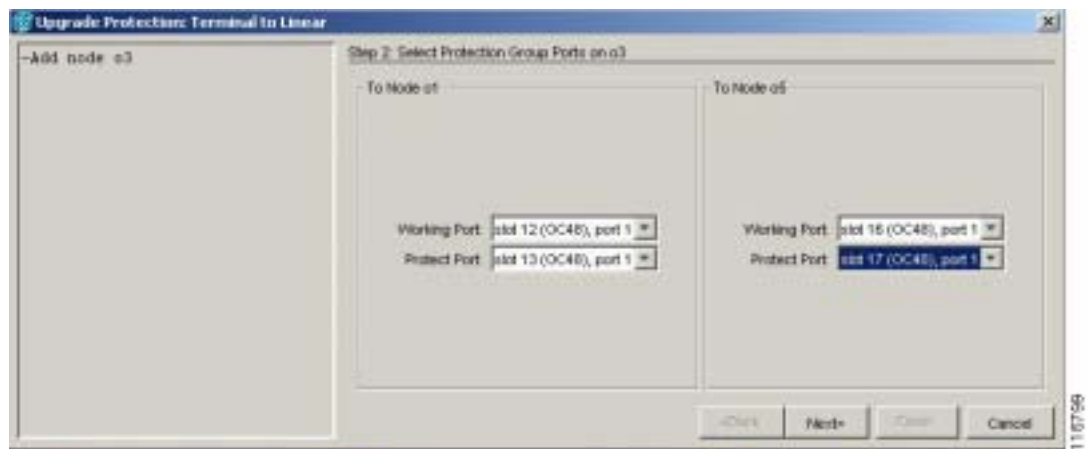


(注) 到達不能なノードを追加する場合は、まず、別の CTC セッションを使用してその到達不能なノードにログインし、そのノードを設定します。次に「DLP-A155 保護グループの削除」(p.18-25) に説明されている方法で、既存の保護グループをすべて削除します。「DLP-A156 SDCC 終端の削除」(p.18-25) および「DLP-A359 LDCC 終端の削除」(p.20-50) に説明されている方法で、既存の DCC 終端をすべて削除します。

**ステップ 6** ノードのホスト名または IP アドレスを入力するか、ドロップダウン リストで新しいノードの名前を選択します。名前を入力する場合は、実際のノード名を正しく入力してください。ノード名は、大文字と小文字を区別して指定します。

**ステップ 7** Next をクリックします。Select Protection Group Ports ページが表示されます ( 図 14-4 )。

図 14-4 保護グループ ポートの選択



**ステップ 8** 各終端ノードに接続する新しいノードの現用ポートと保護ポートを、ドロップダウン リストから選択します。

**ステップ 9** Next をクリックします。Re-fiber the Protected Path ダイアログボックスが表示されます ( 図 14-5 )。

図 14-5 保護パスのファイバ再接続



**ステップ 10** ダイアログボックスの指示に従って、ノード間をファイバで接続します。

**ステップ 11** ファイバを正しく接続したら、**Next** をクリックします。Update Circuit(s) on *Node-Name* ダイアログボックスが表示されます。



**(注)** ウィザードでは、Back ボタンを使用できません。保護のアップグレード手順をキャンセルする場合は、ここで **Cancel** ボタンをクリックし、**Yes** ボタンをクリックします。光ファイバケーブルを物理的に移動したあとで手順が失敗した場合は、ケーブルを元の位置に戻し、ノードの現用パスにトラフィックが流れていることを CTC 経由で確認してから、手順を再開します。トラフィックのステータスを確認するには、ノードビューへ進んで、**Maintenance > Protection** タブをクリックします。Protection Groups 領域で、1+1 保護グループをクリックします。Selected Group 領域でトラフィックのステータスを確認できます。

**ステップ 12** Update Circuit(s) on *Node-Name* ページで **Next** をクリックし、次へ進みます。

**ステップ 13** Force Traffic to Protect Path ページに、終端ノードでトラフィックを現用パスから保護パスへ強制的に切り替えようとしていることが表示されます。次へ進む準備ができたなら、**Next** をクリックします。

**ステップ 14** ウィザードの説明に従ってノード間の現用パスをファイバで再接続したあと、トラフィックを現用パスへ強制的に戻すための各手順を実行します。

**ステップ 15** Force Traffic to Working Path ページに、終端ノードでトラフィックを保護パスから現用パスへ強制的に切り替えようとしていることが表示されます。次へ進む準備ができたなら、**Next** をクリックします。

**ステップ 16** Completed ページが表示されます。このページは、この手順の最後のページです。**Finish** をクリックします。

**終了**：この手順は、これで完了です。

## NTP-A313 リニア ADM からの稼働中のノードの削除

目的	この手順では、トラフィックを損失することなく、リニア ADM からノードを削除します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A38 リニア ADM ネットワークのプロビジョニング (p.5-9)</a>
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)

1+1 保護グループでリニア ADM からノードを削除するには、1+1 保護グループが単方向になっている必要があります。1+1 保護グループが双方向になっている場合は、「[DLP-A154 1+1 保護グループの変更](#)」(p.18-24) を行って、単方向に変更する必要があります。この場合、リニア グループからノードを削除したあとで、保護設定を双方向に戻します。

- ステップ 1** ノードを削除するネットワーク内のノードで、「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 2** View メニューから **Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックします。
- 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-A227 アラームフィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 4** Conditions タブをクリックします。説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 5** ネットワーク マップで、グループから削除するノード (対象ノード) に隣接している 1+1 保護グループのノードをダブルクリックします。
- ステップ 6** ノード ビューで、**Maintenance > Protection** タブをクリックします。
- ステップ 7** 次のようにして、現用ポートで強制切り替えを開始します。
- Protection Groups 領域で、1+1 保護グループをクリックします。
  - Selected Group 領域で、現用ポートをクリックします。
  - Switch Commands の隣にある **Force** をクリックします。
  - Confirm Force Operation ダイアログボックスで、**Yes** をクリックします。
  - Selected Group 領域で、次のように表示されることを確認します。
    - 保護ポート : Protect/Active [FORCE\_SWITCH\_TO\_PROTECT], [PORT STATE]
    - 現用ポート : Working/Standby [FORCE\_SWITCH\_TO\_PROTECT], [PORT STATE]

**ステップ 8** 対象ノードに直接接続しているもう一方の側のノードについて、[ステップ 5 ~ 7](#)を繰り返します。

**ステップ 9** 対象ノードの現用ポートからファイバを取り外します。

**ステップ 10** 対象ノードの両側に直接接続されていた 2 つのノードの現用ポートをファイバで接続します。

**ステップ 11** [ステップ 8](#)の強制切り替えを開始したノードで、次のようにして切り替えをクリアします。

- a. Switch Commands の隣にある Clear をクリックします。
- b. Confirm Clear Operation ダイアログボックスで、Yes をクリックします。

**ステップ 12** 保護ポートで強制切り替えを開始します。

- a. Selected Group 領域で、保護ポートをクリックします。Switch Commands の隣にある Force をクリックします。
- b. Confirm Force Operation ダイアログボックスで、Yes をクリックします。
- c. Selected Group 領域で、次のように表示されることを確認します。
  - 保護ポート：Protect/Standby [FORCE\_SWITCH\_TO\_WORKING], [PORT STATE]
  - 現用ポート：Working/Active [FORCE\_SWITCH\_TO\_WORKING], [PORT STATE]

**ステップ 13** View メニューから、Go to Network View を選択します。

**ステップ 14** ネットワーク マップで、強制切り替えを開始したもう一方のノードをダブルクリックします。

**ステップ 15** ノード ビューで、Maintenance > Protection タブをクリックします。

**ステップ 16** 現用ポートで強制切り替えをクリアします。

- a. Protection Groups 領域で、1+1 保護グループをクリックします。
- b. Selected Group 領域で、現用ポートをクリックします。
- a. Switch Commands の隣にある Clear をクリックします。
- b. Confirm Clear Operation ダイアログボックスで、Yes をクリックします。

**ステップ 17** [ステップ 12](#)を実行し、保護ポートで強制切り替えを開始します。

**ステップ 18** 対象ノードの保護ポートからファイバを取り外します。

**ステップ 19** 対象ノードの両側にある 2 つのノードの保護ポートをファイバで接続します。

**ステップ 20** 次の手順を実行して、強制切り替えをクリアします。

- c. Switch Commands の隣にある Clear をクリックします。
- d. Confirm Clear Operation ダイアログボックスで、Yes をクリックします。
- e. Selected Group 領域で、次の状態を確認します。
  - 保護ポート：Protect/Standby
  - 現用ポート：Working/Active

**ステップ 21** [ステップ 13 ~ 16](#)を繰り返して、もう一方のノードの切り替えをクリアします。

**ステップ 22** CTC を終了します。

**ステップ 23** 対象ノードに隣接していたいずれかのノードで CTC を再起動します。ノードで回線のステータスを確認すると、DISCOVERED と表示されます。

**終了：**この手順は、これで完了です。

---







# ノードのメンテナンス

この章では、Cisco ONS 15454 のメンテナンス手順について説明します。

## 準備作業

次の手順を実行する前に、すべてのアラームを調べて、問題をすべて解決しておいてください。一般的なトラブルシューティング情報およびアラームやエラーの説明については、必要に応じて『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

この章では次の NTP (手順) について説明します。適用する作業 (DLP) については、各手順を参照してください。

1. [NTP-A107 エアー フィルタの検査、清掃、および交換 \(p.15-3\)](#)— 必要に応じて、この手順を実行します。
2. [NTP-A108 データベースのバックアップ \(p.15-6\)](#)— 必要に応じて、この手順を実行します。
3. [NTP-A109 データベースの復元 \(p.15-7\)](#)— 必要に応じて、この手順を実行します。
4. [NTP-A320 OSI 情報の表示および管理 \(p.15-11\)](#)— 必要に応じて、この手順を実行します。
5. [NTP-A163 ノードの出荷時の設定への復元 \(p.15-12\)](#)— データベースを削除してブランクのデータベースと最新のソフトウェアをアップロードする場合は、必要に応じてこの手順を実行します。
6. [NTP-A300 監査証跡レコードの表示 \(p.15-14\)](#)— 必要に応じて、この手順を実行します。
7. [NTP-A214 監査証跡レコードのオフロード \(p.15-16\)](#)— 必要に応じて、この手順を実行します。
8. [NTP-A306 診断ファイルのオフロード \(p.15-17\)](#)— 必要に応じて、この手順を実行します。
9. [NTP-A302 外部切り替えコマンドの開始またはクリア \(p.15-18\)](#)— 強制切り替え、手動切り替え、ロックオン、またはロックアウトを開始する場合は、必要に応じてこの手順を実行します。
10. [NTP-A112 ファイバ コネクタの清掃 \(p.15-20\)](#)— 必要に応じて、この手順を実行します。
11. [NTP-A332 CTC でのカードのリセット \(p.15-21\)](#)— 必要に応じて、この手順を実行します。
12. [NTP-A215 G シリーズ イーサネットのメンテナンス情報表示 \(p.15-22\)](#)— 必要に応じて、この手順を実行します。
13. [NTP-A239 E シリーズ イーサネットのメンテナンス情報表示 \(p.15-23\)](#)— 必要に応じて、この手順を実行します。
14. [NTP-A218 ノードのタイミング基準の変更 \(p.15-24\)](#)— 必要に応じて、この手順を実行します。
15. [NTP-A223 ONS 15454 のタイミング レポート表示 \(p.15-25\)](#)— 必要に応じて、この手順を実行します。

16. [NTP-A287 稼働中のクロスコネクタカードの交換 \(p.15-28\)](#)— 必要に応じて、この手順を実行します。
17. [NTP-A288 FTA の交換 \(p.15-30\)](#)— 必要に応じて、この手順を実行します。
18. [NTP-A290 AIP の交換 \(p.15-33\)](#)— 必要に応じて、この手順を実行します。
19. [NTP-A291 プラスチック製の下部バックプレーンカバーの取り付け \(p.15-39\)](#)— 必要に応じて、この手順を実行します。
20. [NTP-A162 UBIC-V EIA の交換 \(p.15-41\)](#)— 必要に応じて、この手順を実行します。
21. [NTP-A336 NE のデフォルト値の編集 \(p.15-44\)](#)— Cisco ONS 15454 の Network Element (NE; ネットワーク要素) に関する出荷時の (デフォルト) 設定を編集する場合は、必要に応じてこの手順を実行します。
22. [NTP-A337 NE のデフォルト値のインポート \(p.15-46\)](#)— Cisco ONS 15454 の NE に関する出荷時の (デフォルト) 設定をインポートする場合は、必要に応じてこの手順を実行します。
23. [NTP-A338 NE のデフォルト値のエクスポート \(p.15-48\)](#)— Cisco ONS 15454 の NE に関する出荷時の (デフォルト) 設定をエクスポートする場合は、必要に応じてこの手順を実行します。

## NTP-A107 エアー フィルタの検査、清掃、および交換

目的	この手順ではエアー フィルタからほこりと汚れを除去します。この作業によって空気の流れを最適化し、ほこりと汚れがシェルフに付着するのを防止します。
工具 / 機器	掃除機または洗剤、水栓、予備のフィルタ、ピン付き六角キー レンチ
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
セキュリティ レベル	なし



### 警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



### 注意

エアー フィルタを毎月検査して、3 ~ 6 カ月ごとにフィルタを清掃することを推奨します。また、2 ~ 3 年ごとにエアーフィルタを交換してください。エアー フィルタを清掃するときは、強い薬剤や溶剤を使用しないでください。



### (注)

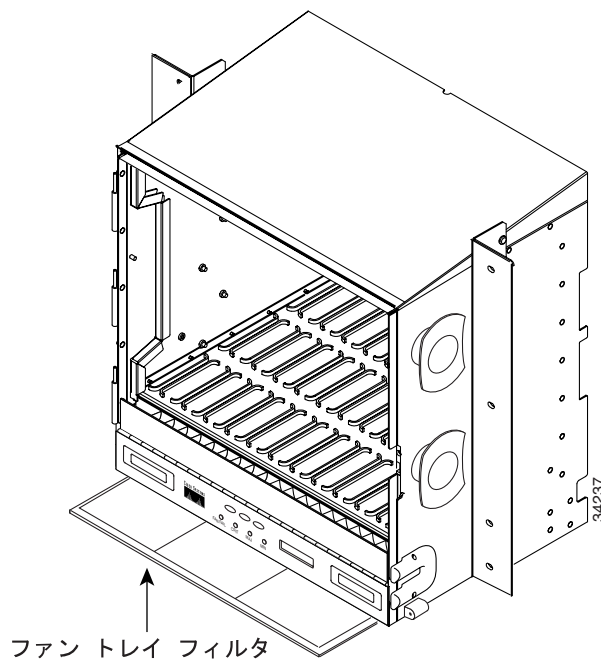
フィルタはどちらの側を正面にして取り付けても機能しますが、フィルタの表面を保護するために、押え金具を正面にしてフィルタを取り付けることを推奨します。

- ステップ 1** 交換する再使用可能なエアー フィルタを確認します。再使用可能なエアー フィルタはグレーの気泡開放型ポリウレタン フォームでできており、耐火性と抗菌性を高めるために特別なコーティングが施されています。NEBS 3E 以降のバージョンの ONS 15454 では、再使用可能なエアー フィルタを使用しています。
- ステップ 2** エアー フィルタが外部フィルタ ブラケットに取り付けられている場合は、フィルタに付着しているほこりを落とさないように注意して、フィルタをブラケットから引き出し、[ステップ 9](#)へ進みます。[図 15-1](#) に、外部フィルタのブラケットに取り付けられている再使用可能なファン トレイの図を示します。
- ステップ 3** フィルタが外部フィルタ ブラケットではなく、ファン トレイの下側に取り付けられている場合は、次のサブステップを実行してシェルフ アセンブリの前面扉を開きます。前面扉がすでに開いている場合は、[ステップ 4](#)へ進みます。
- 前面扉のロックを解除します。
 

ONS 15454 には、前面扉の鍵を開閉するためのピン付き六角キーが付属しています。キーを左回りに回転させると扉がロック解除され、右回りに回転させるとロックされます。
  - 扉のボタンを押して、ラッチをリリースします。
  - 扉を開きます。

- ステップ 4** (任意) 前面扉を取り外します。扉を外さない場合、またはすでに取り外されている場合は、[ステップ 5](#)へ進みます。
- ケプナットの1つを取り外して、扉またはシャーシからアース用ストラップを取り外します。
  - 誤って取り付けないようにアース用ストラップを取り外したあとに、ケプナットをスタッドに再度取り付けます。
  - アース用ストラップのたるんだ端を扉またはシャーシにテープで固定します。

**図 15-1** 外部フィルタのブラケットに取り付けられている再利用可能なファン トレイ エアー フィルタ (前面扉を取り外した状態)



- ステップ 5** ファン トレイ アセンブリのハンドルを外側を押して、ハンドルを引き出します。
- ステップ 6** ハンドルを引いてファン トレイ アセンブリを1インチ(25.4 mm)シェルフ アセンブリから引き出し、ファンが停止するのを待ちます。
- ステップ 7** ファンが停止したら、ファン トレイ アセンブリをシェルフ アセンブリから完全に引き出します。
- ステップ 8** エアー フィルタをシェルフ アセンブリからゆっくりと取り外します。フィルタに付着しているほこりを落とさないように注意してください。
- ステップ 9** エアー フィルタを見て、ほこりや汚れが付いていないかどうか確かめます。
- ステップ 10** 再利用可能なエアー フィルタに大量のほこりや汚れが付いている場合は、汚れたエアー フィルタを新しいエアー フィルタに交換して(予備のフィルタをストックしておいてください)、再びファン トレイ アセンブリを挿入してください。汚れたエアー フィルタは掃除機をかけるか、または、少量の洗剤を使って水を流しながら洗浄します。

**注意**

ファントレイは、シャーシの外に長時間放置しないでください。温度が上がって ONS 15454 カードが故障する場合があります。

**(注)**

清掃は、機器の付近でほこりや汚れを落とさないように、機器が作動していない場所で行ってください。

**ステップ 11** フィルタを水で洗浄した場合は、最低でも 8 時間は自然乾燥してください。

**注意**

湿ったフィルタを ONS 15454 に取り付けしないでください。

**ステップ 12** 新しいフィルタと交換します。

- a. エアー フィルタが外部フィルタ ブラケットに取り付けられている場合は、乾いたエアー フィルタをブラケットの奥まで完全に挿入して、この手順を終了します。
- b. フィルタがファントレイ アセンブリの下に取り付けられている場合は、ファントレイ アセンブリを取り外し、乾いたエアー フィルタまたは新しいエアー フィルタをシェルフ アセンブリ 底部の奥まったコンパートメントに取り付けます。エアー フィルタの前端とコンパートメントの前端が揃うように取り付けます。ファントレイをシェルフ アセンブリに戻します。

**注意**

ファントレイをシェルフ アセンブリの奥まで完全に挿入できない場合は、ファントレイを引き出し、再使用可能なフィルタの位置を調整してファントレイを正しく取り付けます。

**(注)**

ONS 15454 に電源が供給されている場合は、ファントレイ アセンブリを正しく挿入すれば、ファンがただちに回転し始めます。

**ステップ 13** ファントレイ アセンブリの前面にある LCD にノード情報が表示されているかどうかをチェックして、トレイがバックプレーンに接続されていることを確認します。

**ステップ 14** 引き込み式のハンドルを回して、コンパートメントに戻します。

**ステップ 15** 扉を取り付ける場合は、アース用ストラップも再度取り付けます。

**ステップ 16** 扉を閉じて施錠します。

**ステップ 17** 元の NTP (手順) に戻ります。

**終了** : この手順は、これで完了です。

## NTP-A108 データベースのバックアップ

目的	この手順では、Cisco Transport Controller (CTC) の動作しているワークステーションまたはネットワーク サーバで TCC2/TCC2P の (ソフトウェア) データベースをバックアップします。
工具 / 機器	なし
事前準備手順	なし
必須 / 適宜	必須。データベースのバックアップは、毎週および設定変更の前後に実行することを推奨します。
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



(注) 回線全体をメンテナンスするために、回線パス上にあるすべてのノードでデータベースをバックアップおよび復元してください。



(注) ノード名、および Internet Inter-ORB Protocol (IOP) ポート パラメータは、バックアップおよび復元されません。ノード名を変更したあとで、それより前にバックアップしておいたノード名の異なるデータベースを復元すると、回線は新しいノード名にマップされます。古いノード名と新しいノード名を記録しておくことを推奨します。

- ステップ 1** バックアップを実行するノードで、「[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** Maintenance > Database タブをクリックします。
- ステップ 3** Backup をクリックします。
- ステップ 4** ワークステーションのハード ドライブまたはネットワーク ストレージにデータベースを保存します。ファイル拡張子「.db」が付いた適切なファイル名を指定してください。たとえば、database.db のように指定します。
- ステップ 5** Save をクリックします。
- ステップ 6** 確認用のダイアログボックスで OK ボタンをクリックします。

終了：この手順は、これで完了です。

## NTP-A109 データベースの復元

目的	この手順では、TCC2/TCC2P のソフトウェア データベースを復元します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a>
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



### 注意

ONS 15454 のデータベースを復元すると、E1000-2 カードで約 90 秒間、トラフィックが損失します。トラフィックが損失するのは、スパニング ツリーが再収束する間です。この間に、CARLOSS アラームが表示されてクリアされます。



### 注意

複数のノードでデータベースを復元する場合は、あるノードで TCC2/TCC2P のリポートが完了してから次のノードへ進むまでに、約 1 分間待ってください。



### 注意

TCC2P カードは、単一 IP アドレス (リピータ) または二重 IP アドレス (セキュア) モードで使用できます。セキュア モードは、データベースの復元に関する高度な機能です。セキュアなノードからセキュアでないリピータ ノードにデータベースをロードすることはできません。セキュアでないリピータ ノード データベースをセキュアなノードにロードすることはできますが、その場合、ロードしたデータベースにそのノードの特性が適用されます (セキュアになります)。セキュア データベースは、TCC2 にロードできません。TCC2P カードのみがセキュア モードをサポートしています。二重 IP アドレス セキュア モードの詳細については、「[NTP-A169 CTC ネットワーク アクセスの設定](#)」(p.4-9) を参照してください。また、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章も参照してください。



### 注意

データベースの復元後にノード IP およびセキュア IP が同じドメインに設定されないようにするために、ドメイン内で、データベースに格納されたノード IP とリピータ モード ノードのノード IP が異なることを確認してください。また、データベースの復元後に、ドメイン内のノード IP とセキュア IP が異なることを確認してください。



### (注)

ノード名、および HOP ポートの各パラメータは、バックアップおよび復元されません。ノード名を変更したあとで、バックアップしておいたノード名の異なるデータベースを復元すると、回線はその新しい名前のノードにマップされます。古いノード名と新しいノード名を記録しておくことを推奨します。



(注) ML シリーズ イーサネット カードは、データベースを復元したあとにリセットする必要があります。これらのカードの復元方法については、『*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。



(注) 以前に使用していたソフトウェアに戻す場合は、プラットフォーム固有のアップグレード マニュアルで手順を確認してください。

**ステップ 1** データベースを復元するノードで、「[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** BLSR 切り替えイベント（イーストまたはウェストのリング切り替えなど）が存在しないことを確認します。ネットワーク ビューで **Conditions** タブをクリックし、**Retrieve** をクリックして状態の一覧を表示します。

**ステップ 3** 切り替えイベントをクリアする場合は、ノード ビューで **Maintenance > BLSR** タブをクリックして、**West Switch** および **East Switch** のカラムを表示します。

- a. (ライン障害以外の原因で発生した) 切り替えイベントが存在する場合は、ドロップダウン リストの **CLEAR** を選択して、**Apply** をクリックします。
- b. **Wait to Restore (WTR)** 状態が原因で発生した切り替えイベントが存在する場合は、ドロップダウン リストの **CLEAR** を選択して、**Apply** をクリックします。

切り替えイベントをクリアすると、カラムに **NO COMMAND** が表示されて、切り替えイベントが無効になったことが示されます。

**ステップ 4** ノード ビューで、**Maintenance > Database** タブをクリックします。図 15-2 に、TCC2 カードのタブを示します (TCC2P タブも同様です)。



図 15-2 TCC2 データベースの復元



**ステップ 5** Restore をクリックします。

**ステップ 6** ワークステーションのハード ドライブまたはネットワーク ストレージに保存されているデータベース ファイルを検索します。



(注) すべての既存プロビジョニングをクリアする場合は、最新の ONS 15454 ソフトウェア CD にあるデータベースを検索して、アップロードしてください。

**ステップ 7** データベース ファイルをクリックして、強調表示します。

**ステップ 8** Open をクリックします。DB Restore ダイアログボックスが表示されます。



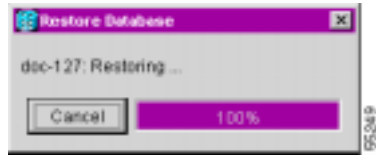
#### 注意

別のノードや以前のバックアップから復元ファイルを開くと、ログイン ノードのトラフィックに影響することがあります。

**ステップ 9** Restore をクリックします。

Restore Database ダイアログボックスで、ファイル転送をモニタします。(図 15-3)

**図 15-3** データベースの復元 — 進行表示



**ステップ 10** ファイルが TCC2/TCC2P カードへ完全に転送されるのを待ちます。

**ステップ 11** [Lost connection to node, changing to Network View] ダイアログボックスが表示されたら、OK をクリックします。ノードが再接続されるまで待ちます。

**ステップ 12** ステップ 3 で切り替えをクリアにした場合は、必要に応じて再度切り替えを適用します。

**終了** : この手順は、これで完了です。

---

## NTP-A320 OSI 情報の表示および管理

目的	この手順では、ES-IS や IS-IS のルーティング情報テーブル、TARP データ キャッシュやマニュアル エリア テーブルなど、OSI を表示および管理します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a> <a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a> <a href="#">NTP-A318 OSI のプロビジョニング (p.4-17)</a>
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 に実装されている OSI 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 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 必要に応じて次の作業を行います。

- [DLP-A549 IS-IS RIB の表示](#) (p.22-58)
- [DLP-A550 ES-IS RIB の表示](#) (p.22-59)
- [DLP-A551 TDC の管理](#) (p.22-60)

終了：この手順は、これで完了です。

## NTP-A163 ノードの出荷時の設定への復元

目的	この手順では、CTC 再初期化ツールを使用して、ONS 15454 を再初期化します。初期化しなすと、新しいソフトウェア パッケージが TCC2/TCC2P カードにアップロードされ、ノードのデータベースがクリアされて、出荷時のデフォルトパラメータが復元されます。
工具 / 機器	ONS 15454 SONET System Software CD、Version 7.2  再初期化の完了後にノードにログインするには、そのコンピュータに JRE 1.4.2 または JRE 5.0 がインストールされている必要があります。再初期化ツールは、JRE 1.3.1_02、JRE 1.4.2、または JRE 5.0 で実行できます。
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a>  <a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>  次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• <a href="#">NTP-A234 ONS 15454 ヘローカルにクラフト接続するための CTC コンピュータのセットアップ (p.3-4)</a> または</li> <li>• <a href="#">NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ (p.3-6)</a></li> </ul>
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	スーパーユーザ



注意

ノード データベースが複数ある場合は、フォルダを分けて個別に保存することを推奨します。これは、Package フィールドと Database フィールドの代わりに Search Path フィールドを使用すると、再初期化ツールで、指定したディレクトリにある最初の製品固有ソフトウェア パッケージが選択されるからです。そのため、指定したディレクトリに複数のデータベースが保管されていると、間違っただータベースをコピーしてしまう恐れがあります。



注意

ノードを出荷時の設定に復元すると、ノードのクロスコネクトはすべて削除されます。



注意

ノードの復元にソフトウェア CD で提供されるデータベースを使用しない場合は、ノード データベースを安全な場所に保存することを推奨します。



(注)

データベースを削除し、出荷時の設定を復元するとき、ノード名、IP アドレス、サブネット マスクとゲートウェイ、および IOP ポートの各パラメータは、バックアップおよび復元されません。ノード名を変更したあとで、バックアップしておいたノード名の異なるデータベースを復元すると、回線はその新しい名前のノードにマップされます。古いノード名と新しいノード名を記録しておくことを推奨します。

- 
- ステップ 1** TCC2/TCC2P カードを 1 枚以上取り付けるか交換する場合は、「[DLP-A36 TCC2/TCC2P カードの取り付け](#)」(p.17-44) を参照してください。
- ステップ 2** Microsoft Windows を使用している場合は、「[DLP-A244 再初期化ツールの使用によるデータベースのクリアおよびソフトウェアのアップロード \( Windows \)](#)」( p.19-29 ) を行います。
- ステップ 3** UNIX を使用している場合は、「[DLP-A245 再初期化ツールの使用によるデータベースのクリアおよびソフトウェアのアップロード \( UNIX \)](#)」( p.19-31 ) を行います。

**終了：**この手順は、これで完了です。

---

## NTP-A300 監査証跡レコードの表示

<p><b>目的</b></p> <p><b>工具 / 機器</b></p> <p><b>事前準備手順</b></p> <p><b>必須 / 適宜</b></p> <p><b>オンサイト / リモート</b></p> <p><b>セキュリティ レベル</b></p>	<p>この手順では、監査証跡レコードの表示方法について説明します。監査証跡レコードは、セキュリティの維持、失われたトランザクションの回復、およびアカウントビリティの実施を行う際に便利です。アカウントビリティとは、ユーザ アクティビティの追跡、つまり、プロセスまたはアクションを特定のユーザと関連付けることを意味します。</p> <p>なし</p> <p>なし</p> <p>適宜</p> <p>オンサイトまたはリモート</p> <p>プロビジョニング以上のレベル</p>
---	---

**ステップ 1** 監査証跡ログを表示するノードで「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、Maintenance > Audit タブをクリックします。

**ステップ 3** Retrieve をクリックします。

図 15-4 のように、最新の監査証跡レコードを含むウィンドウが表示されます。

図 15-4 監査証跡レコードの表示

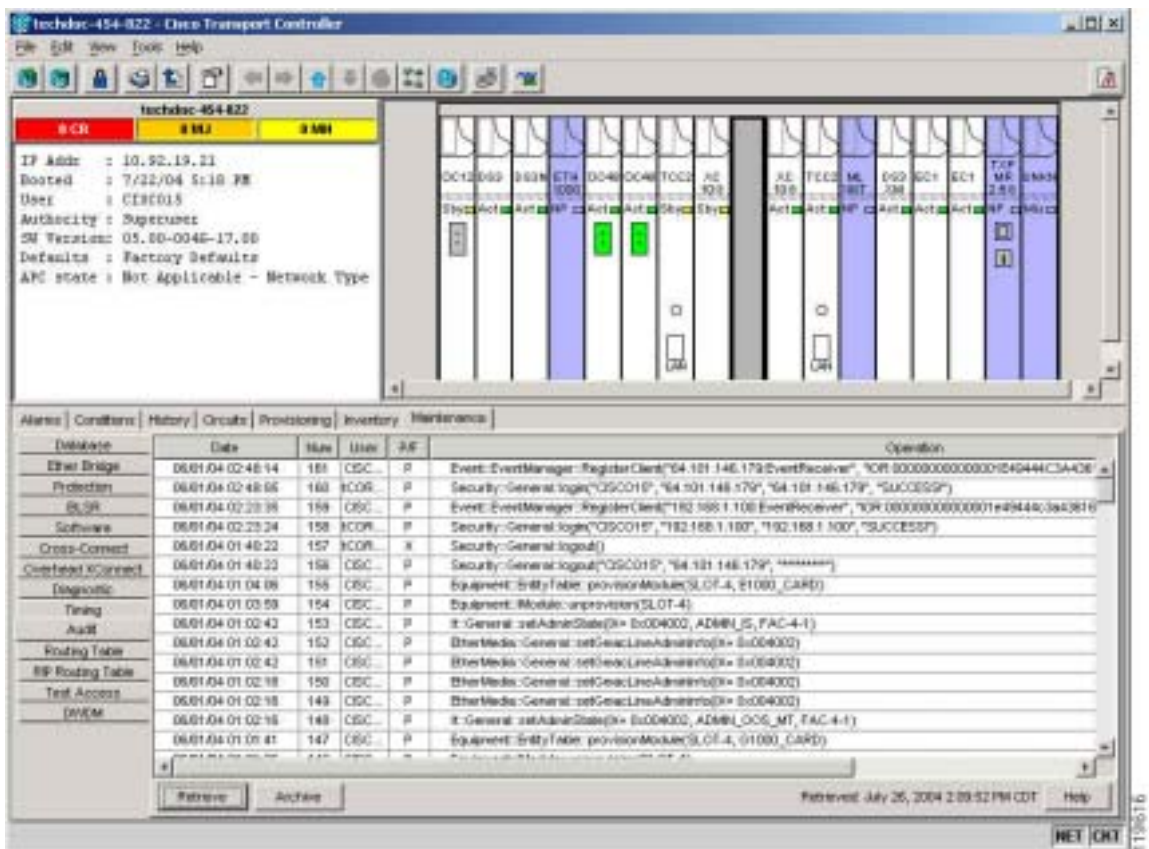


表 15-1 に、監査証跡ログの各カラムの定義を示します。

表 15-1 監査証跡カラムの定義

カラム	定義
Date	アクションが行われた日時 (MM/dd/yy HH:mm:ss 形式)
Num	アクションの増加カウント
User	アクションを開始したユーザの ID
P/F	成功 / 失敗 (そのアクションが実行されたかどうか)
Operation	実行されたアクション

**ステップ 4** リストの表示を昇順から降順に変えたり、逆に降順から昇順に変えたりする場合は、カラムの見出しを右クリックします。

**ステップ 5** 次のオプションを表示する場合は、カラムの見出しを左クリックします。

- Reset Sorting — カラムをデフォルト設定にリセットします。
- Hide Column — ビューでカラムを表示しないようにします。
- Reset Columns Order/Visibility — 非表示のカラムをすべて表示します。
- Row Count — ログ エントリ数を表示します。

**ステップ 6** リストを差分ソートする場合は、Shift キーを押しながらカラムの見出しをクリックします。

**終了 :** この手順は、これで完了です。

## NTP-A214 監査証跡レコードのオフロード

目的	この手順では、ローカルドライブまたはネットワークドライブのファイルに最大 640 個の監査証跡ログ エントリをオフロードして、ノードに対して実行されたアクションの記録を保存します。監査証跡ログをオフロードしないと、ログが最大容量に到達した時点で最も古いエントリから上書きされていきます。
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** 監査証跡ログのオフロードを実行するノードで、「[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、Maintenance > Audit タブをクリックします。

**ステップ 3** Retrieve をクリックします。

**ステップ 4** Archive をクリックします。

**ステップ 5** Archive Audit Trail ダイアログボックスで、ファイルを保存するディレクトリ(ローカルまたはネットワーク)に移動します。

**ステップ 6** File Name フィールドに名前を入力します。

アーカイブ ファイルは、特定の拡張子を付ける必要がありません。WordPad、Microsoft Word(ファイルをインポート)など、テキスト ファイルをサポートしているアプリケーションで、ファイルを読むことができます。

**ステップ 7** Save をクリックします。

640 個のエントリがこのファイルに保存されます。後続のエントリは、始めからではなく、次の番号から番号が付けられていきます。



**(注)** アーカイブを作成しても、CTC 監査証跡ログのエントリがすぐに削除されることはありません。ただし、ログが最大数に到達すると、それらのエントリは上書きされます。エントリをアーカイブに保存するとログ ファイルを CTC に再インポートすることができなくなるため、それらのログは別のアプリケーションで確認する必要があります。

終了：この手順は、これで完了です。



## NTP-A306 診断ファイルのオフロード

目的	この作業では、診断ファイルのオフロード方法を示します。診断ファイルには、ノードで実行された一連のデバッグ コマンドとその実行結果が格納されています。このファイルは、Cisco Technical Support (TAC) でノード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	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	メンテナンス以上のレベル

**ステップ 1** 診断ファイルをオフロードするノードで「[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、Maintenance > Diagnostic タブをクリックします。

**ステップ 3** Retrieve Tech Support Log をクリックします。

**ステップ 4** Saving Diagnostic File ダイアログボックスで、ファイルを保存するディレクトリ (ローカルまたはネットワーク) に移動します。

**ステップ 5** File Name フィールドに名前を入力します。

アーカイブ ファイルは、特定の拡張子を付ける必要がありません。アーカイブ ファイルは、シスコのテクニカル サポート担当者が解凍して参照する圧縮ファイル (.gzip) です。

**ステップ 6** Save をクリックします。

Get Diagnostics ステータス ウィンドウの進行バーに、ファイルの保存進行状況がパーセント (%) で表示され、保存が完了すると、[Get Diagnostics Complete] が表示されます。

**ステップ 7** OK をクリックします。

**終了 :** この手順は、これで完了です。

## NTP-A302 外部切り替えコマンドの開始またはクリア

目的	この手順では、外部切り替えコマンド(手動切り替え、強制切り替え、ロックオン、ロックアウトなど)を光カードまたは電気回路カードに適用する方法を示します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A324 保護グループの作成 (p.4-12)</a>
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	スーパーユーザ

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。

**ステップ 2** 必要に応じて、「[DLP-A365 光保護切り替えの開始](#)」(p.20-55) を行います。

**ステップ 3** 必要に応じて、「[DLP-A366 電気保護切り替えの開始](#)」(p.20-56) を行います。

**ステップ 4** 現用カードまたは保護カードのトラフィックがペアのカードへ切り替わるのを防止する場合は、「[DLP-A201 ロックオンの適用](#)」(p.19-1) を行います。

**ステップ 5** トラフィックが保護カードに切り替わるのを防止するには、「[DLP-A202 ロックアウトの適用](#)」(p.19-2) を実行します。



**(注)** 1:1 保護と 1:N 保護はロックオンやロックアウトと組み合わせることができます。たとえば、現用カードのロックオンと保護カードのロックアウトが可能です。

**ステップ 6** ロックオンまたはロックアウトを解除して保護グループを通常の切り替え方式に戻す場合は、「[DLP-A203 ロックオンまたはロックアウトのクリア](#)」(p.19-3) を行います。



**(注)** カードがロックオン状態またはロックアウト状態になると、アラームを伴わないイベント (INHSW) が発生します。

**ステップ 7** BLSR のスパンをロックアウトして、トラフィックがロックアウトされたスパンに切り替わるのを防止するには、「[DLP-A299 BLSR スパン ロックアウトの開始](#)」(p.19-72) を実行します。

**ステップ 8** 必要に応じて、「[DLP-A300 BLSR スパン ロックアウトのクリア](#)」(p.20-1) を行います。

**ステップ 9** 必要に応じて、「[DLP-A301 BLSR 手動リング切り替えの開始](#)」(p.20-2) を行います。

**ステップ 10** 必要に応じて、「[DLP-A241 BLSR 手動リング切り替えのクリア](#)」(p.19-27) を行います。

**ステップ 11** 必要に応じて、「[DLP-A303 BLSR 強制リング切り替えの開始](#)」(p.20-3) を行います。

**ステップ 12** 必要に応じて、「[DLP-A194 BLSR 強制リング切り替えのクリア](#)」(p.18-65) を行います。

**ステップ 13** 必要に応じて、「[DLP-A197 UPSR 強制切り替えの開始](#)」(p.18-68)を行います。

**ステップ 14** 必要に応じて、「[DLP-A198 UPSR 強制切り替えのクリア](#)」(p.18-69)を行います。

**終了：**この手順は、これで完了です。

---

## NTP-A112 ファイバ コネクタの清掃

目的	この手順では、ファイバ コネクタを清掃します。
工具 / 機器	検査用の顕微鏡 圧縮空気 / ダスター タイプ A 光ファイバ コネクタ用クリーナー (CLETOP リール式) 濃度 70% 以上のイソプロピル アルコール 光ファイバ用綿棒 光レーザー クリーニング スティック
事前準備手順	なし
必須 / 適宜	必須
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



### 警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器 (ルーペ、拡大鏡、顕微鏡など) で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。

**ステップ 1** 検査用の顕微鏡を使用して、各ファイバ コネクタの汚れ、ひび、傷を検査します。

**ステップ 2** 損傷のあるファイバ コネクタはすべて交換します。



**(注)** 機器を 30 分以上使用しない場合は、ダスト キャップをすべて閉めてください。

**ステップ 3** 必要に応じて、「[DLP-A204 アルコールと乾いた布によるファイバ コネクタとアダプタの検査および清掃](#)」(p.19-4) を行います。

**ステップ 4** 必要に応じて、「[DLP-A205 CLETOP によるファイバ コネクタの清掃](#)」(p.19-5) を行います。

**ステップ 5** 必要に応じて、「[DLP-A206 ファイバ アダプタの清掃](#)」(p.19-5) を行います。



### 注意

光ファイバ用の綿棒は再使用しないでください。未使用の綿棒は作業場のそばに置かないでください。

終了：この手順は、これで完了です。

## NTP-A332 CTC でのカードのリセット

目的	この手順では、CTC でカードをリセットします。
工具 / 機器	なし
事前準備手順	DLP-A36 TCC2/TCC2P カードの取り付け (p.17-44) NTP-A16 光カードおよびコネクタの取り付け (p.2-8) NTP-A17 電気回路カードの取り付け (p.2-11) NTP-A246 イーサネット カードおよびコネクタの取り付け (p.2-13) NTP-A274 FC_MR-4 カードの取り付け (p.2-15)
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** 「DLP-A60 CTC へのログイン」(p.17-71) を実行します。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** 必要に応じて、「DLP-A364 CTC による TCC2/TCC2P カードのリセット」(p.20-54) を行います。
- ステップ 3** 光カード、電気回路カード、E シリーズ イーサネット カード、G シリーズ イーサネット カード、ML シリーズ イーサネット カード、CE-1000-4 イーサネット、または Storage Access Networking (SAN) カードをリセットするには、「DLP-A460 CTC でのトラフィック カードのリセット」(p.21-46) を行います。
- ステップ 4** 必要に応じて、「DLP-A54 CTC を使用した CE-100T-8 カードのハードリセット」(p.17-68) を行います。
- ステップ 5** 必要に応じて、「DLP-A224 CTC を使用した CE-100T-8 カードのソフトリセット」(p.19-19) を行います。

終了：この手順は、これで完了です。

---

## NTP-A215 G シリーズ イーサネットのメンテナンス情報表示

目的	この手順では、G シリーズ イーサネット カードのループバック、帯域幅、および J1 パストレース情報を表示します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A246 イーサネット カードおよびコネクタの取り付け (p.2-13)</a>
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** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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、G 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 3** ループバックのステータスを表示する場合は、**Maintenance > Loopback** タブをクリックします。

Port および Service State カラムで、各ポートのポート番号および現在のサービス状態 ( In-Service and Normal [IS-NR]、 Out-of-Service and Management, Disabled [OOS-MA,DSBLD]、または Out-of-Service and Management, Maintenance [OOS-MA,MT] ) を識別します。Loopback Type カラムで、カードの各ポートに適用されているループバックのタイプ ( None、 Terminal [Inward]、または Facility [Line] ) を識別します。

**ステップ 4** イーサネットの帯域幅の使用状況を表示する場合は、**Maintenance > Bandwidth** タブをクリックします。

**ステップ 5** **Retrieve Bandwidth Usage** をクリックします。

現在の STS 帯域幅の使用情報が表示されます。

**ステップ 6** J1 パストレース情報を表示する場合は、**Maintenance > Path Trace** タブをクリックして、**Retrieve** をクリックします。

**終了** : この手順は、これで完了です。

## NTP-A239 E シリーズイーサネットのメンテナンス情報表示

目的	この作業では、E シリーズイーサネット カードのメンテナンス情報を表示します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A246 イーサネット カードおよびコネクタの取り付け (p.2-13)</a>
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)

E-Series Maintenance タブは、このリリースには実装されていません。

**ステップ 1** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。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** 必要に応じて次の作業を行います。

- [DLP-A430 スパニングツリー情報の表示](#) (p.21-9)
- [DLP-A309 イーサネット MAC アドレス テーブルの表示](#) (p.20-4)
- [DLP-A310 イーサネット トランクの使用率の表示](#) (p.20-5)

終了：この手順は、これで完了です。

## NTP-A218 ノードのタイミング基準の変更

目的	この手順では、タイミング基準の自動切り替えをイネーブルにしたり、ノード タイミングを通常動作に戻したりします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A28 タイミングの設定 (p.4-11)</a>
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** タイミング切り替えをイネーブルにするノードで「[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** 必要に応じて、「[DLP-A322 ノードで使用するタイミング基準の手動または強制切り替え](#)」(p.20-14)を行います。
- ステップ 3** 必要に応じて、「[DLP-A323 ノードで使用するタイミング基準の手動または強制切り替えのクリア](#)」(p.20-14)を行います。

終了：この手順は、これで完了です。

---



## NTP-A223 ONS 15454 のタイミング レポート表示

目的	この手順では、ONS 15454 のタイミング基準について、現在のステータスを表示します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A28 タイミングの設定 (p.4-11)</a>
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 タイミング ステータスを表示するノードで「[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** Maintenance > Timing > Report タブをクリックします。
- ステップ 3** Timing Report 領域で、ノードのタイミング情報を表示します。レポートの日付と時間がレポートの上部に表示されます。タイム スタンプはアラームのタイム スタンプと同じで、「[DLP-A112 時間帯に合わせたアラームおよび状態の表示](#)」(p.18-3)を行って設定することができます。表 15-2 に、レポートのフィールドとエントリを示します。
- ステップ 4** レポートを更新するには、Refresh をクリックします。

表 15-2 ONS 15454 のタイミング レポート

項目	内容	オプション	オプションの説明
Clock	タイミング クロックの種類を示します。あとに続くレポート セクションは、ここに示されているタイミング クロックに関する情報です。	NE	ノード タイミング クロック
		BITS -1 Out	BITS-1 Out タイミング クロック
		BITS -2 Out	BITS-2 Out タイミング クロック

表 15-2 ONS 15454 のタイミングレポート (続き)

項目	内容	オプション	オプションの説明
Status	タイミングクロックのステータスです。	INIT_STATE	タイミング基準がプロビジョニングされていません。基準が NE の場合は、TCC2/TCC2P のブートで、最初のプロビジョニングメッセージが表示される直前にこのステータスが表示されます。タイミングはノードの内部クロックにプロビジョニングされます。
		HOLDOVER_STATE	クロックが、障害が発生してから 140 秒以上の間、有効なタイミング基準にロックされています。Holdover (ホールドオーバー) 状態になっているときのタイミングは、ノードの内部クロックと正常状態時のタイミングに基づいて計算されます。ノードでは、有効な基準が復元されるまで、この周期が使用されます。このステータスは、基準が NE の場合にだけ表示されます。
		FREERUN_STATE	ノードが内部クロック以外で実行されています。タイミングが 0 PPM になるように値が調整された以外は何も修正されていません。Freerun(フリーラン)状態が発生する可能性があるのは、内部クロックへ強制的に切り替わるとき、ホールドオーバーデータが 140 秒間ないためにすべての基準が失敗したとき、または、定義されているタイミング基準が内部タイミングだけのときです。このステータスは、基準が NE の場合にだけ表示されます。
		NO_SYNC_STATE	同期タイミング基準が定義されていません。OC-N カードの基準を Provisioning > Timing タブで定義しないかぎり、BITS-1 Out または BITS-2 Out のデフォルト値はこのステータスに設定されます。このステータスは、基準が外部の場合にだけ表示されます。
		NE_SYNCH_STATE	BITS-1 Out と BITS-2 Out で、NE と同じタイミングソースが使用されています。このステータスは、Provisioning > Timing タブの BITS-1 Out and BITS-2 Out Reference List で NE Reference を選択すると表示されます。
		NORMAL_STATE	タイミング基準が、プロビジョニングされている基準の 1 つにロックされています。基準が Internal または No Sync 状態になることはありません。
		FAST_START_STATE	ノードの基準は切り替わりましたが、許容時間内に通常の基準になることができないような基準値です。Fast Start (高速起動) は、ノードで迅速に基準を取得する高速獲得モードです。基準を取得すると、ノードは通常の状態になります。
		FAST_START_FAILED_STATE	タイミング基準が離れすぎていて、通常の状態ではその基準に到達できません。Fast Start (高速起動) 状態でも、許容時間内に十分なタイミング情報を取得できませんでした。
Status Changed At	最後にステータスを変更した日時です。	—	—

表 15-2 ONS 15454 のタイミング レポート (続き)

項目	内容	オプション	オプションの説明
Switch Type	切り替えのタイプです。	AUTOMATIC	タイミングの切り替えが、システムによって行われました。
		Manual	タイミングの切り替えが、ユーザによって手動で行われました。
		Force	タイミングの切り替えが、ユーザによって強制的に行われました。
Reference	タイミング基準です。	Provisioning > Timing タブで 3 つのタイミング基準 (Ref-1、Ref-2、および Ref-3) が利用できます。	これらのオプションは、システムで使用するタイミング基準と、それらの基準を呼び出す順序を表しています (たとえば、Ref-1 が使用可能になると、Ref-2 が呼び出されます)。
Selected	基準が選択されているかどうかを示します。	選択されている基準には、X が付きます。	—
Facility	Provisioning > Timing タブの基準に対してプロビジョニングされているタイミング ファシリティです。	BITS-1	ノードの BITS -1 のピンに接続された BITS クロックがタイミング ファシリティになっています。
		BITS-2	ノードの BITS-2 ピンに接続された BITS クロックがタイミング ファシリティになっています。
		ポート番号が示された OC-N カード	ノードがライン タイミングに設定されている場合に、タイミング基準としてプロビジョニングされた OC-N カードとポートです。
		Internal clock	ノードは内部クロックを使用しています。
State	タイミング基準の状態です。	IS	タイミング基準稼働中です。
		OOS	タイミング基準は、停止状態です。
Condition	タイミング基準の状態です。	OKAY	基準は有効で、タイミング基準として使用できます。
		OOB	有効な範囲から外れています。基準が有効でないため、タイミング基準としては使用できません (BITS クロックが接続されていないなど)。
Condition Changed	最後にステータスが変更された日時を MM/DD/YY HH:MM:SS の形式で示します。	—	—
SSM	タイミング基準の SSM が有効かどうかを示します。	Enabled	SSM はイネーブルです。
		Disabled	SSM はディセーブルです。
SSM Quality	SSM のタイミング品質です。	8 ~ 10 の SSM 品質メッセージが表示される場合もあります。	SSM のメッセージセットの一覧については、『Cisco ONS 15454 Reference Manual』を参照してください。
SSM Changed	最後に SSM ステータスが変更された日時を MM/DD/YY HH:MM:SS の形式で示します。	—	—

終了：この手順は、これで完了です。

## NTP-A287 稼働中のクロスコネク ト カードの交換

目的	この手順では、稼働中のクロスコネク ト カードを交換します。
工具 / 機器	なし
事前準備手順	DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け (p.17-47)
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



### 警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



### 注意

ONS 15454 からアクティブ カードを取り外すと、トラフィックが中断します。カードの交換は注意して行い、交換するカードがスタンバイになっていることを確認してください。

- ステップ 1** カードを交換するノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71)を行います。
- ステップ 2** View メニューで、**Go to Network View** を選択します。
- ステップ 3** Alarms タブをクリックして、次のサブステップを実行します。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21)を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 4** アクティブなクロスコネク ト カード(XCVT/XC10G/XC-VXC-10G)を判別します。アクティブ カードの ACT/STBY LED はグリーンに点灯しています。スタンバイ カードの ACT/STBY LED はオレンジに点灯しています。



(注) カードの図にカーソルを置いてポップアップを表示し、カードがアクティブであるかスタンバイであるかを識別することもできます。

- ステップ 5** アクティブなクロスコネク ト カードを交換する場合は、まず、次のサブステップを実行してスタンバイに切り替えます。スタンバイ カードを交換する場合は、このステップを省略して**ステップ 6**へ進みます。
- ノード ビューで、**Maintenance > Cross-Connect** タブをクリックします。
  - Cross Connect Cards 領域で、**Switch** をクリックします。
  - Confirm Switch ダイアログボックスで **Yes** をクリックします。



(注) アクティブな XCVT/XC10G/XC-VXC-10G がスタンバイになると、元のスタンバイ スロットがアクティブになります。その結果、以前スタンバイであったカードの ACT/STBY LED がグリーンに変わります。

**ステップ 6** ONS 15454 からスタンバイ クロスコネクタカード (XCVT/XC10G/XC-VXC-10G) を物理的に取り外します。



(注) CTC からカードを削除することなくカードを取り外して再び取り付けると、取り外しが不適切であることを知らせるアラーム (IMPROPRMVL) が発生します。このアラームは、カードの交換が完了するとクリアされます。

**ステップ 7** 交換用のクロスコネクタカード (XCVT/XC10G/XC-VXC-10G) を空のスロットに差し込みます。

交換したカードがブートし、約 1 分後には作動可能な状態になります。

**終了 :** この手順は、これで完了です。

## NTP-A288 FTA の交換

目的	この手順では、ファントレイ アセンブリを交換します。
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
セキュリティ レベル	なし



### 注意

15454-FTA3 および 15454-FTA3-T ファントレイ アセンブリを取り付けることができるのは、ONS 15454 R3.1 以降のシェルフ アセンブリ (15454-SA-ANSI [ 部品番号 : 800-19857-xx ], 15454-SA-HD [ 部品番号 : 800-24848-xx ]) のみです。ファントレイ アセンブリにはピンが付いているため、ONS 15454 R3.1 より前にリリースされた ONS 15454 シェルフ アセンブリ (15454-SA-NEBS3E、15454-SA-NEBS3、および 15454-SA-R1 [ 部品番号 : 800-07149 ]) に取り付けることはできません。15454-FTA3-T または 15454-FTA3 を互換性のないシェルフ アセンブリに取り付けようとすると、機器が損傷することがあります。



### 注意

ファントレイ アセンブリを無理に押し込まないでください。ファントレイのコネクタまたはバックプレーンのコネクタ (あるいはその両方) が破損することがあります。



### (注)

ONS 15454 XC-10G、OC-192、および OC-48 Any Slot (AS) カードには、15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリ、および 15454-FTA-3 または 15454-FTA3 FTA が必要です。



### (注)

ファントレイ アセンブリを交換する場合に、ケーブル マネジメント ファシリティを移動する必要はありません。

**ステップ 1** ファントレイ アセンブリを交換する際は、表 15-3 を参照してコンポーネントに互換性があることを確認し、互換性がない場合に発生するアラームに注意します。



### (注)

ノードに取り付けられているハードウェアを確認する場合は、ノード ビューで Inventory タブをクリックします。

表 15-3 非互換性アラーム

シェルフアセンブリ <sup>1</sup>	ファントレイ <sup>2</sup>	AIP <sup>3</sup>	10Gカード <sup>4</sup>	イーサネットカード <sup>5</sup>	アラーム
—	—	ヒューズなし	—	—	Alarm Interface Panel ( AIP ) に関する Mismatch of Equipment Attributes ( MEA )
NEBS3E または NEBS3	2A	2A	×	—	なし
NEBS3E または NEBS3	2A	2A		—	10G カードに関する MEA
NEBS3E または NEBS3	2A	5A	×	—	なし
NEBS3E または NEBS3	2A	5A		—	10G カードに関する MEA
ANSI または HD	2A	2A	×	—	なし
ANSI または HD	2A	2A		2.5G と互換	ファントレイ、AIP、またはイーサネットに関する MEA
ANSI または HD	2A	2A		10G と互換	ファントレイ および AIP に関する MEA
ANSI または HD	2A	5A	×	いずれか	なし
ANSI または HD	2A	5A		2.5G と互換	ファントレイおよびイーサネットに関する MEA
ANSI または HD	2A	5A		10G と互換	ファントレイに関する MEA
ANSI または HD	5A	2A	×	いずれか	AIP に関する MEA
ANSI または HD	5A	2A		2.5G と互換	AIP およびイーサネットに関する MEA
ANSI または HD	5A	2A		10G と互換	AIP に関する MEA
ANSI または HD	5A	5A	×	いずれか	なし
ANSI または HD	5A	5A		いずれか	なし

- 15454-SA-NEBS3E ( 部品番号 : 800-07149-xx ) または 15454-SA-NEBS3 ( 部品番号 : 800-06741-xx ) = ONS 15454 Release 3.1 より前にリリースされたシェルフアセンブリ  
15454-SA-ANSI ( 部品番号 : 800-19857-xx ) = ONS 15454 Release 3.1 以降のシェルフアセンブリ  
15454-SA-HD ( 部品番号 : 800-24848-xx ) = ONS 15454 Release 3.1 以降のシェルフアセンブリ
- 5A ファントレイ = 15454-FTA3 ( 部品番号 : 800-19858-xx ) または 15454-FTA3-T ( 部品番号 : 800-21448-xx )  
2A ファントレイ = 15454-FTA2 ( 部品番号 : 800-07145-xx, 800-07385-xx, 800-19591-xx, 800-19590-xx )
- 5A AIP ( 部品番号 : 73-7665-xx ), 2A AIP ( 部品番号 : 73-5262-xx )
- 10G カードには、XC-10G、OC-192、および OC-48 AS があります。
- 2.5G は、XC および XCVT クロスコネクタカードと互換性のあるカード ( E100T-12、E1000-2、E100T-G、E1000-2-G、G1K-4、ML100T-12、ML1000-2 ) を示します。10G は、XC10G クロスコネクタカードと互換性のあるカード ( E100T-G、E1000-2-G、G1000-4、G1K-4、ML100T-12、ML1000-2 ) を示します。

**ステップ 2** シェルフアセンブリの前面扉を開きます。シェルフアセンブリに前面扉がない場合は、[ステップ 4](#)に進んでください。

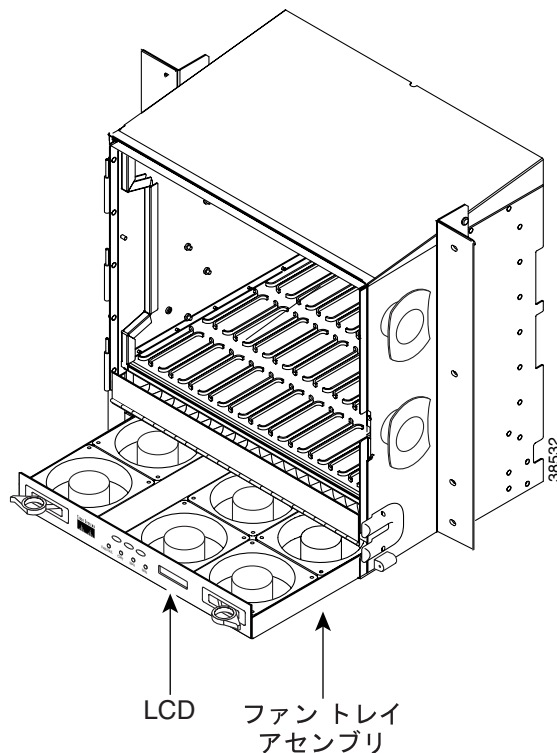
- a. 前面扉のロックを解除します。

ONS 15454 には、前面扉の鍵を開閉するためのピン付き六角キーが付属しています。キーを左回りに回転させると扉がロック解除され、右回りに回転させるとロックされます。

- b. 扉のボタンを押して、ラッチをリリースします。  
c. 扉を開きます。

- ステップ3** (任意) 前面扉を取り外します。扉を外さない場合には、[ステップ4](#)へ進みます。
- ケブナットの1つを取り外して、扉またはシャーシからアース用ストラップを取り外します。
  - 誤って取り付けないようにアース用ストラップを取り外したあとに、ケブナットをスタッドに再度取り付けます。
  - アース用ストラップのたるんだ端を扉またはシャーシにテープで固定します。
- ステップ4** ファントレイアセンブリのハンドルを外側を押して、ハンドルを引き出します。
- ステップ5** ファントレイの外側にある引き込み式ハンドルを出します。
- ステップ6** ハンドルを引いてファントレイアセンブリを1インチ(25.4 mm)シェルフアセンブリから引き出し、ファンが停止するのを待ちます。
- ステップ7** ファンが停止したら、ファントレイアセンブリをシェルフアセンブリから完全に引き出します。ファントレイの位置は[図15-5](#)のとおりです。

図15-5 ファントレイアセンブリの取り外しまたは交換(前面扉を取り外した状態)



- ステップ8** ファントレイアセンブリの下に取り付けられているファントレイエアークフィルタを交換する場合は、ファントレイアセンブリを交換する前に、既存のエアークフィルタをシェルフアセンブリの外へスライドさせて交換します。

外付けの下部ブラケットに取り付けられているファントレイエアークフィルタを交換する場合は、既存のエアークフィルタをブラケットの外へスライドさせて、いつでも交換することができます。ファントレイのエアークフィルタについては、「[NTP-A107 エアークフィルタの検査、清掃、および交換](#)」(p.15-3)を参照してください。



**ステップ 9** 新しいファン トレイをシェルフ アセンブリ内にスライドさせて、トレイの背面にある電気プラグがバックプレーンの対応するコンセントに差し込まれるようにします。

**ステップ 10** ファン トレイの前面にある LCD がアクティブになっていれば、トレイがバックプレーンに正しく差し込まれています。

**ステップ 11** 扉を取り付ける場合は、アース用ストラップを再度取り付けます。

終了：この手順は、これで完了です。

## NTP-A290 AIP の交換

目的	この手順では、トラフィックに影響を与えることなく、稼働中のノードの AIP を新しい AIP に交換します。ただし、交換手順が完了したら、共有パケットリングを削除し、再構築する必要があります。R4.0 より前のソフトウェア リリースがインストールされたノードを経由するイーサネット回線は、影響を受けます。
工具 / 機器	#2 プラス ドライバ
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



### 警告

カバーは製品の安全設計に必要な部品です。カバーを外した状態で装置を稼働させないでください。



### 注意

2A AIP と 5A ファン トレイ アセンブリを併用しないでください。AIP のヒューズが飛びます。



### 注意

イーサネット回線内のどのノードもソフトウェア R4.0 以降を使用していない場合は、イーサネットトラフィックが中断する危険性があります。手順の指示に従って、Cisco Technical Support に問い合わせてください。



### 注意

ONS 15454 に電力が供給されている状態で作業する場合は、必ず付属の静電気防止用リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンドケーブルを接続してください。

**注意**

トラフィックが実際に流れているノードでは、この手順を実行しないでください。AIP をホットスワップすると、トラフィックに影響が及び、データが損失することがあります。AIP の交換手順については、Cisco Technical Support に問い合わせてください。「[テクニカル サポート](#)」(p.xxix) を参照してください。

**(注)**

この手順は、保守時間中に実行してください。アクティブ TCC2/TCC2P カードをリセットすると、OC-N または DS-N トラフィックに 50 ミリ秒未満のサービス中断が発生する可能性があります。イーサネット回線のどのノードもソフトウェア R4.0 以降を使用していない場合に、アクティブ TCC2/TCC2P カードをリセットすると、スパンニングツリーが再収束して、すべてのイーサネットトラフィックに 3 ~ 5 分間のサービス中断が発生する可能性があります。

**ステップ 1** ファントレイ アセンブリを交換する際は、[表 15-3](#) を参照してコンポーネントに互換性があることを確認し、互換性がない場合に発生するアラームに注意します。

**ステップ 2** AIP を交換して回線を修復する前に、次のサブステップを実行して、影響を受けるネットワーク内のすべてのノードで同じソフトウェアバージョンが稼働していることを確認します。

- a. まだノードにログインしていない場合は、「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行して、ログインします。
- b. ネットワーク ビューで、**Maintenance > Software** タブをクリックします。Working Version カラムに、各ノードの現用ソフトウェアバージョンが表示されます。
- c. ノードのソフトウェアをアップグレードする場合は、リリース固有のソフトウェア アップグレード マニュアルを参照して、ソフトウェア アップグレード手順を確認してください。ソフトウェア アップグレードが完了するまでは、ハードウェアの変更や回線修復を実行しないで下さい。ソフトウェアをアップグレードする必要がない場合や、ソフトウェア アップグレードをすでに完了した場合は、[ステップ 3](#) へ進みます。

**ステップ 3** 古い AIP の MAC (メディア アクセス制御) アドレスを記録します。

- a. 単一 IP アドレスの「リピータ」設定を使用している場合は、**Provisioning > Network > General** タブをクリックします。
- b. General タブに表示されている MAC アドレスを記録します ([図 15-6](#))。

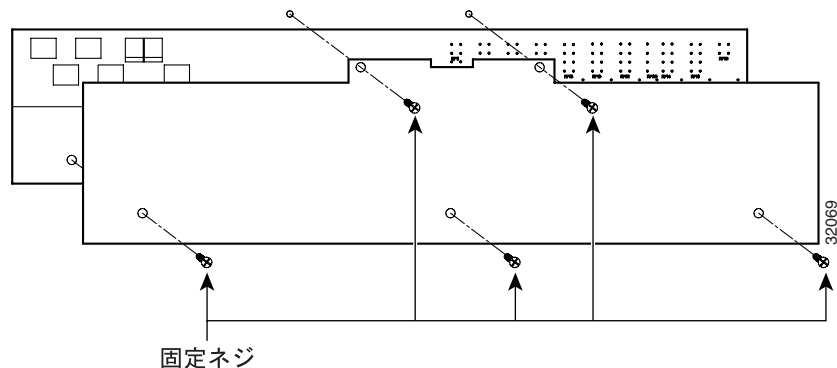
図 15-6 単一 IP アドレス設定における MAC アドレスの検出



(セキュアな二重 IP モード設定を使用している場合は、MAC アドレスは Provisioning > Security > Data Comm タブに表示されます)

- ステップ 4** AIP 交換、および元の MAC アドレスの維持については、Cisco Technical Support に問い合わせてください。「テクニカル サポート」(p.xxix) を参照してください。
- ステップ 5** 下部バックプレーンカバーを所定位置に固定している 5 本のネジを外します (図 15-7)。

図 15-7 下部バックプレーンカバー



**ステップ 6** 下部バックプレーン カバーをつかんで、バックプレーンからまっすぐ静かに引き抜きます。

**ステップ 7** AIP カバーを所定位置に固定している 2 本のネジを外します。

**ステップ 8** カバーをつかんで、バックプレーンから静かに引き抜きます。



**(注)** 15454-SA-HD (部品番号: 800-24848)、15454-SA-NEBS3E、15454-SA-NEBS3、および 15454-SA-R1 (部品番号: 800-07149) シェルフの AIP カバーは、クリアプラスチック製です。15454-SA-ANSI シェルフ (部品番号: 800-19857) の AIP カバーは、金属製です。

**ステップ 9** AIPをつかんで、バックプレーンから静かに引き抜きます。

**ステップ 10** AIP からファントレイアセンブリの電源コードを取り外します。

**ステップ 11** 古い AIP はシスコへ返却するために取っておきます。



**注意**

AIP が取り付けられているシェルフタイプによって、故障した AIP と交換する AIP のバージョンを判別します。15454-SA-ANSI シェルフ (部品番号: 800-19857) および 15454-SA-HD (部品番号: 800-24848) は現在、5A AIP (部品番号: 73-7665-01) を使用しています。15454-SA-NEBS3E、15454-SA-NEBS3、および 15454-SA-R1 (部品番号: 800-07149) 以前のシェルフは、2A AIP (部品番号: 73-5262-01) を使用しています。



**注意**

2A AIP (部品番号: 73-5262-01) を 15454-SA-ANSI シェルフ (部品番号: 800-19857) または 15454-SA-HD (部品番号: 800-24848) に取り付けないでください。AIP のヒューズが飛びます。

**ステップ 12** 新しい AIP にファントレイアセンブリの電源コードを取り付けます。

**ステップ 13** DIN コネクタを使用してパネルをバックプレーンに装着して、新しい AIP をバックプレーンに取り付けます。

**ステップ 14** AIP カバーを AIP に取り付けて、2 本のネジでカバーを固定します。

**ステップ 15** 下部バックプレーン カバーを取り付けて、5 本のネジでカバーを固定します。



**注意**

サービスが中断することがないように、TCC2/TCC2P カードのリセットは保守時間内に実行することを推奨します。

**ステップ 16** スタンバイ TCC2/TCC2P カードをリセットします。

- a. スタンバイ TCC2/TCC2P カードを右クリックし、**Reset Card** を選択します。
- b. Resetting Card ダイアログボックスで **Yes** をクリックします。カードをリセットすると、CTC のカードにロード中 (Ldg) の表示が現れます。



(注) リセットには約 5 分かかります。リセットが完了するまで、その他のステップは実行しないでください。

**ステップ 17** アクティブ TCC2/TCC2P カードをリセットするには、「DLP-A364 CTC による TCC2/TCC2P カードのリセット」(p.20-54) を実行します。

**ステップ 18** File メニューから Exit を選択して、CTC セッションを終了します。

**ステップ 19** ノードにログインし直します。Login ダイアログボックスの Additional Nodes ドロップダウン リストから、(None) を選択します。

**ステップ 20** 新しい MAC アドレスを記録します。

- a. ノード ビューで、Provisioning > Network タブをクリックします。
- b. General タブに表示されている MAC アドレスを記録します。



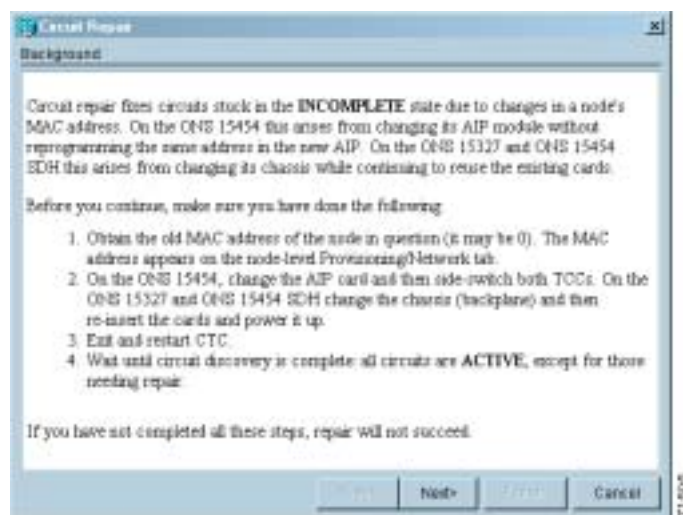
(注) ここでの説明は、単一 IP の「リピータ」設定の場合です。セキュアな二重 IP ノードの場合、IP は Provisioning > Security > Data Comm タブに表示されます。

**ステップ 21** ノード ビューで、Circuits タブをクリックします。表示されているすべての回線のステータスが PARTIAL であることを確認します。

**ステップ 22** ノード ビューで、Tools メニューから Circuits > Repair Circuits を選択します。Circuit Repair ダイアログボックスが表示されます。

**ステップ 23** Circuit Repair ダイアログボックスの手順を参照します (図 15-8)。ダイアログボックス内のすべてのステップを完了したら、Next をクリックします。古い MAC アドレスと新しい MAC アドレスが記録されていることを確認します。

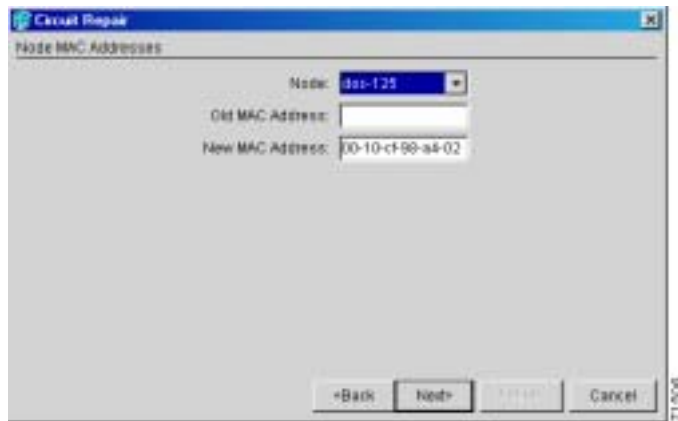
図 15-8 回線の修復



**ステップ 24** Node MAC Addresses ダイアログボックスが表示されます (図 15-9)。

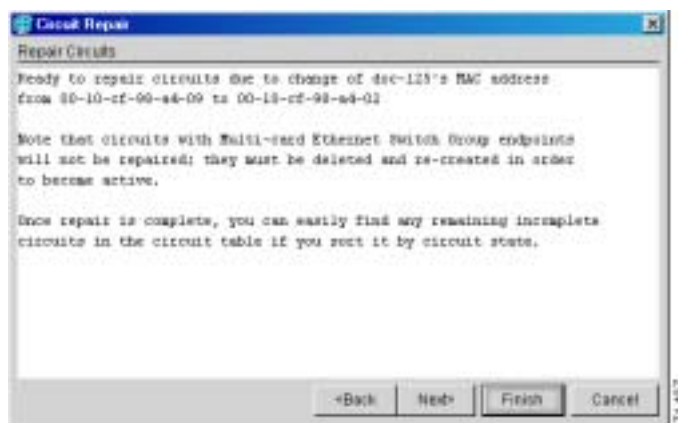
- a. Node ドロップダウン リストから、AIP を交換したノードの名前を選択します。
- b. Old MAC Address フィールドに、ステップ 3 で記録した古い MAC アドレスを入力します。
- c. Next をクリックします。

図 15-9 AIP 交換前の古い MAC アドレスの記録



**ステップ 25** Repair Circuits ダイアログボックスが表示されます (図 15-10)。ダイアログボックス内の情報を確認し、Finish をクリックします。

図 15-10 回線の修復情報



(注) すべての回線を修復するまで、CTC セッションはフリーズします。プロビジョニングされた回線数によっては、回線修復に 5 分以上かかることがあります。

回線修復が完了すると、Circuits Repaired ダイアログボックスが表示されます。

**ステップ 26** OK をクリックします。

**ステップ 27** 新しいノードのノードビューで、**Circuits** タブをクリックします。表示されているすべての回線のステータスが DISCOVERED であることを確認します。表示されているすべての回線のステータスが DISCOVERED でない場合は、Cisco Technical Support に問い合わせ、Return Material Authorization (RMA) を利用します。「[テクニカル サポート](#)」(p.xxix) を参照してください。

終了：この手順は、これで完了です。

---

## NTP-A291 プラスチック製の下部バックプレーン カバーの取り付け

目的	この手順では、ONS 15454 の背面下部にあるプラスチック製カバーを取り付けます。
工具 / 機器	プラス ドライバ
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
セキュリティ レベル	なし


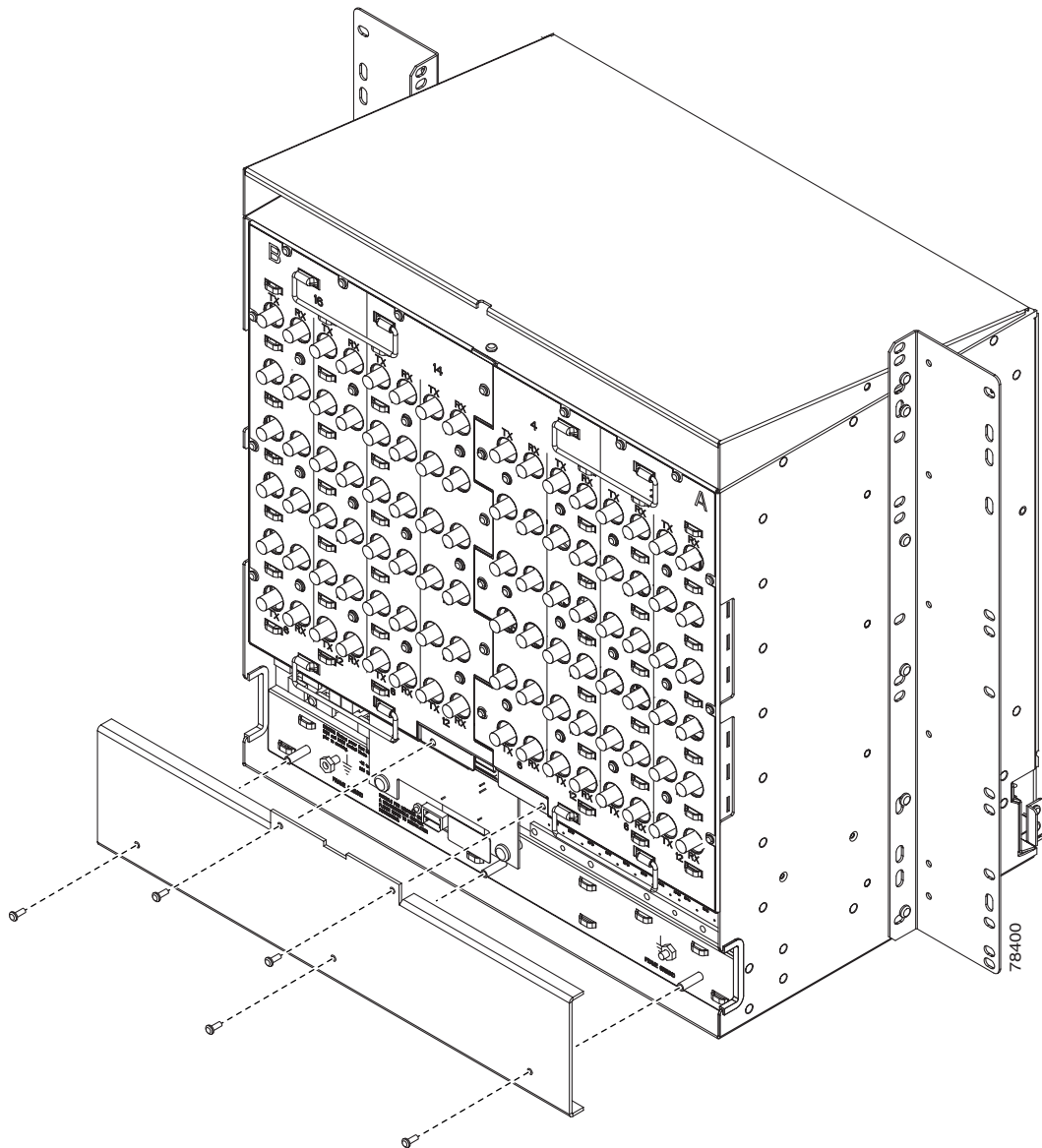
- 
- ステップ 1** プラス ドライバを使用して、プラスチック製カバーを所定位置に固定している 5 本の固定ネジを外します。
- ステップ 2** 金属製カバーの両側を持ちます。
- ステップ 3** プラスチック製カバーをバックプレーンから静かに引き抜きます。
- ステップ 4** プラスチック カバーをシェルフ アセンブリに取り付けて、カバーとシェルフ アセンブリのネジ穴を合わせます (  15-11 )。

図 15-11 プラスチック製の下部バックプレーン カバーの取り付け



**ステップ 5** 5本の固定ネジを締めて、プラスチック製カバーを所定位置に固定します。

**終了：**この手順は、これで完了です。

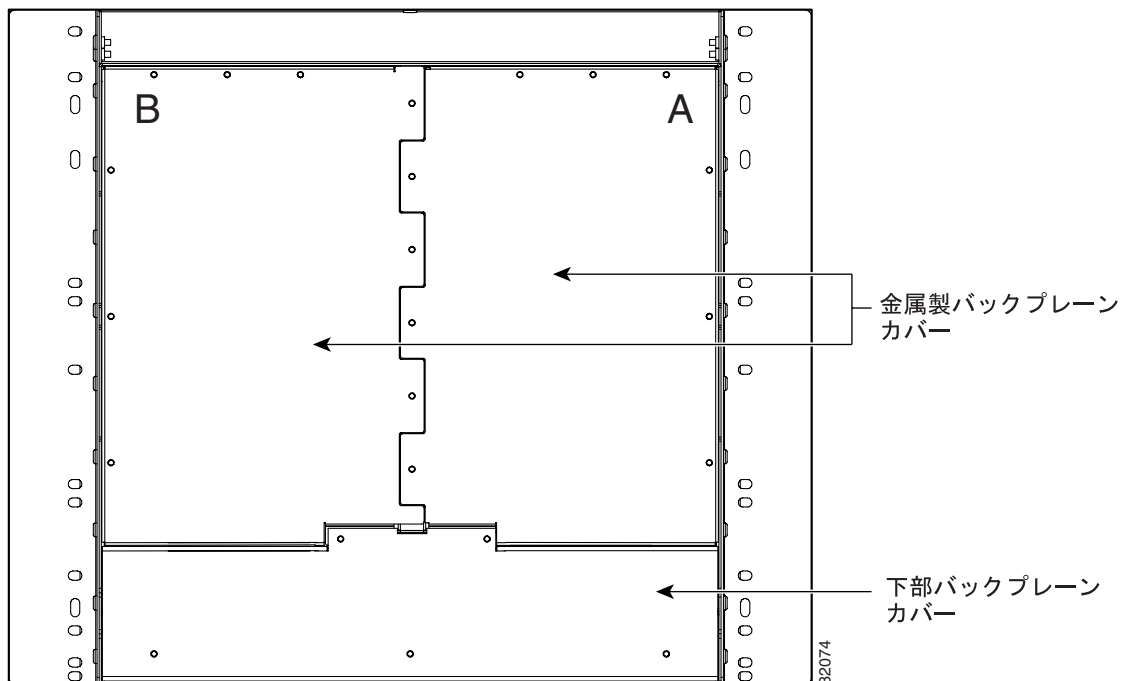


## NTP-A162 UBIC-V EIA の交換

目的	この手順では、UBIC-V EIA を交換します。
工具 / 機器	#2 プラス ドライバ 小型スロット ヘッド ネジ用ドライバ 交換用の UBIC-V EIA および付属ネジ
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
セキュリティ レベル	なし

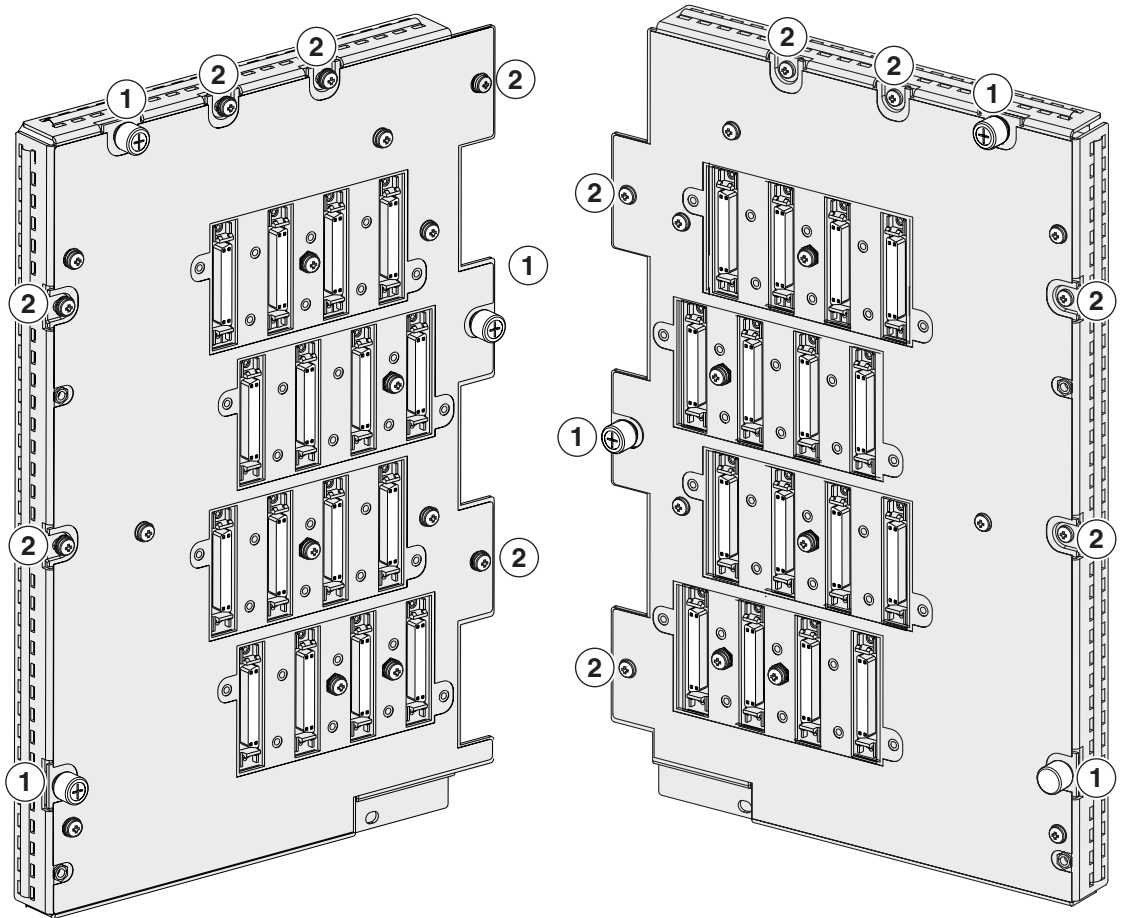
- ステップ 1** 下部バックプレーン カバーを取り外すには、ONS 15454 にカバーを固定している 5 本のネジを緩めて取り外し、シェルフ アセンブリから下部バックプレーン カバーを引き出します ( 図 15-12 )。

図 15-12 ONS 15454 の背面図 (金属製カバーが取り付けられた状態)



**ステップ2** 金属製カバーおよび UBIC-V を所定位置に固定している 6 本の周辺ネジを緩めて、取り外します (図 15-13)。

図 15-13 UBIC-V EIA ネジの位置



- ① ジャックネジ (3)
- ② 周辺ネジ、6-32 x 0.375 インチ プラス ネジ (6)

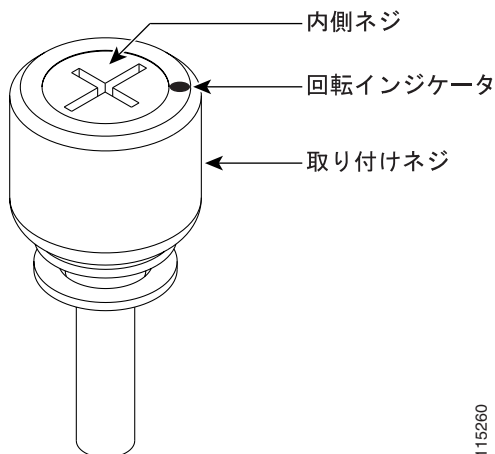
115140

**ステップ 3** プラス ドライバを使用して、ジャック ネジをそれぞれ最大 2 回転させて緩めます。各ジャック ネジを（回転インジケータを基準として）一度に 2 回転ずつさせながら、すべてのジャックネジを完全に外します（[図 15-14](#)）。

**注意**

ジャックネジを均等に緩めないで、UBIC-V コネクタが破損することがあります。

**図 15-14 UBIC-V EIA ジャック ネジ**



**ステップ 4** 2 本のジャック ネジを持ち、UBIC-V をシェルフから慎重に引き抜きます。



**(注)** EIA を取り付けない場合は、必ず金属製バックプレーン カバーを取り付けます。

**ステップ 5** 新しい UBIC-V EIA を取り付ける場合は、「[DLP-A190 UBIC-V EIA の取り付け](#)」(p.18-60) を実行します。

**終了：**この手順は、これで完了です。

## NTP-A336 NE のデフォルト値の編集

目的	この手順では、NE Defaults Editor を使用して NE のデフォルト値を編集します。新しいデフォルト値については、それらのデフォルト値を編集したノードだけに適用することも、ファイルにエクスポートして他のノードにインポートすることもできます。
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	スーパーユーザ



(注) カードとノードのデフォルト設定のリストについては、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。カードの設定を（デフォルト値を変更せずに）個別に変更する場合は、第 10 章「カードの設定変更」を参照してください。ノードの設定を変更する場合は、第 11 章「ノード設定の変更」を参照してください。

- ステップ 1** NE のデフォルト値を編集するノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。
- ステップ 2** Provisioning > Defaults タブをクリックします。
- ステップ 3** Defaults Selector の下で、カード タイプ(カード レベルのデフォルト値を編集する場合)、CTC(CTC のデフォルト値を編集する場合)、または NODE (ノード レベルのデフォルト値を編集する場合) を選択します。ノード名 (Defaults Selector カラムの最上部) をクリックすると、その NE で使用可能なすべてのデフォルト値が Default Name カラムにリストされます。指定したカード タイプ、ノード レベル、または CTC レベルのデフォルト値だけを選択的に表示する場合は、Defaults Selector メニュー構造をドリルダウンします。
- ステップ 4** 変更するデフォルト値を Default Name の下で検索します。
- ステップ 5** Default Value カラム内をクリックして変更するデフォルト プロパティを選択し、ドロップダウンメニュー（表示される場合）から値を選択するか、または新しい値を入力します。



(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 6** Apply をクリックします (Apply ボタンが使用できない場合は、Default Name カラム内をクリックして、このボタンを有効にします)。変更を適用する前に、複数のデフォルト値を修正できます。
- デフォルト値のファイルを編集したことによって変更されることになる各デフォルト値の隣には、鉛筆型のアイコンが表示されます。
- ステップ 7** ノード レベルのデフォルト値を変更すると、ダイアログボックスが開き、ノード レベル アトリビュートにデフォルト値を適用すると現在のプロビジョニングが上書きされることを示すメッセージが表示され、処理を継続するかどうかを確認されます。Yes をクリックします。

IOP Listener Port の設定を変更する場合は、ノードがリブートされることを警告するダイアログボックスが表示され、処理を継続するかどうかを確認されます。Yes をクリックします。



(注) 通常は、ノードのデフォルト値を変更して Apply をクリックすると、ノードが再プロビジョニングされます。Defaults Editor を使用してカードの設定に変更を加えても、取り付けられているカードの設定やカードに事前にプロビジョニングされているスロットの設定が変更されることはありません。変更が適用されるのは、変更後に取り付けられたカードまたは事前プロビジョニングされたカードのみです。取り付けられているカードや事前プロビジョニングされているスロットの設定を変更する場合は、第 10 章「カードの設定変更」を参照してください。



(注) NE のデフォルト値を変更すると、CTC が切断されたり、デフォルト値を有効にするためにノードがリブートされることがあります。デフォルト値を変更する前に、Defaults Editor の Side Effects カラムを表示して (カラム ヘッダーを右クリックして Show Column > Side Effects を選択) デフォルト値を変更した場合に生じる副作用に対応します。

終了 : この手順は、これで完了です。

## NTP-A337 NE のデフォルト値のインポート

目的	この手順では、NE Defaults Editor を使用して NE のデフォルト値をインポートします。デフォルト値は、CTC のソフトウェア CD (出荷時の設定) からインポートすることも、ノードからエクスポートされて保存されているカスタマイズ済みのファイルからインポートすることもできます。
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	スーパーユーザ



(注) カードとノードのデフォルト設定のリストについては、『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** NE のデフォルト値をインポートするノードで「[DLP-A60 CTC へのログイン \(p.17-71\)](#)」を行います。
- ステップ 2** Provisioning > Defaults タブをクリックします。
- ステップ 3** Import をクリックします。
- ステップ 4** インポートするファイルの名前と場所が Import Defaults from File ダイアログボックスに正しく表示されない場合は、Browse をクリックして、インポートするファイルを参照します。
- ステップ 5** ダイアログボックスにファイル名と場所が正しく表示されたら、OK をクリックします (出荷時の設定をインポートする場合は、15454-defaults.txt が正しいファイル名です)。
- デフォルト値のファイルをインポートすることで変更される各デフォルト値の隣には、鉛筆型のアイコンが表示されます。
- ステップ 6** Apply をクリックします。
- ステップ 7** ファイルからインポートする編集内容に正しくないものがある場合は、そうした問題のあるデフォルト値の中で最初に検出されたデフォルト値が問題フィールドに表示されるので、それを修正する必要があります。問題のあるデフォルト値を変更して、Apply をクリックします。編集されたすべての値がファイルから正しくインポートされるまで、このステップを繰り返します。
- ステップ 8** ノード レベルのデフォルト値を変更すると、ダイアログボックスが開き、ノード レベル アトリビュートにデフォルト値を適用すると現在のプロビジョニングが上書きされることを示すメッセージが表示され、処理を継続するかどうかを確認されます。Yes をクリックします。

IIOP Listener Port の設定を変更する場合は、ノードがリポートされることを警告するダイアログボックスが表示され、処理を継続するかどうかを確認されます。Yes をクリックします。



(注) 通常は、ノードのデフォルト値を変更して Apply をクリックすると、ノードが再プロビジョニングされます。Defaults Editor を使用してカードの設定に変更を加えても、取り付けられているカードの設定やカードに事前にプロビジョニングされているスロットの設定が変更されることはありません。変更が適用されるのは、変更後に取り付けられたカードまたは事前プロビジョニングされたカードのみです。取り付けられているカードや事前プロビジョニングされているスロットの設定を変更する場合は、第 10 章「カードの設定変更」を参照してください。



(注) NE のデフォルト値を変更すると、CTC が切断されたり、デフォルト値を有効にするためにノードがリブートされることがあります。デフォルト値を変更する前に、Defaults Editor の Side Effects カラムを表示して (カラム ヘッダーを右クリックして Show Column > Side Effects を選択) デフォルト値を変更した場合に生じる副作用に対応します。

終了 : この手順は、これで完了です。

## NTP-A338 NE のデフォルト値のエクスポート

目的	この手順では、NE Defaults Editor を使用して NE のデフォルト値をエクスポートします。エクスポートしたデフォルト値は、他のノードにインポートできます。
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	スーパーユーザ



(注) 現在表示されているデフォルト値は、現在のノードに適用されているかどうかに関係なく、エクスポートされます。



(注) NE のデフォルト値も File > Export メニューからエクスポートできます。エクスポートされたこれらのデフォルト値は、参照専用なので、インポートできません。

- 
- ステップ 1** NE のデフォルト値をエクスポートするノードで「[DLP-A60 CTC へのログイン](#)」(p.17-71) を行います。
- ステップ 2** Provisioning > Defaults タブをクリックします。
- ステップ 3** Export をクリックします。
- ステップ 4** Export Defaults to File ダイアログボックスにエクスポート先のファイルが表示されない (または存在しない) 場合は、Browse をクリックして、データのエクスポート先となるディレクトリを参照してから、エクスポート先のファイルを選択するか、または入力 (作成) します (デフォルトでは等号 [=] 区切りのテキスト ファイルとしてエクスポートされます)。
- ステップ 5** OK をクリックします。

終了 : この手順は、これで完了です。

---





## ノードの電源切断

この章では、ノードの電源を切断して Cisco ONS 15454 で行われているノード アクティビティをすべて停止する方法について説明します。

### NTP-A114 ノードの電源切断

目的	この手順では、ノードのアクティビティをすべて停止します。
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
セキュリティ レベル	ソフトウェアに関する手順については、プロビジョニング以上のレベルが必要です。ハードウェアに関する手順については、どのレベルでも実行できます。



#### 警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



#### 注意

次の手順は、ノードの電源を切断してもトラフィックの停止が最小限に抑えられるように考えられています。ただし、動作中のノードをパススルーする回線を削除して再作成する場合は、トラフィックが失われます。



#### (注)

ONS 15454 の作業を行う場合は、必ず付属の静電気防止用リストバンドを使用してください。リストバンド ケーブルはファントレイ アセンブリにある ESD ジャックに接続するか、または NEBS 3 シェルフ アセンブリのシェルフの右下外側の端にある ESD ジャックに接続してください。NEBS 3 シェルフ アセンブリの ESD プラグを使用する場合は、ONS 15454 の前面扉を開きます。前面扉は感電防止のためにアースされています。

- ステップ 1** 電源を切断するノードを特定します。カードが取り付けられていない場合は、ステップ 14 へ進みます。カードが取り付けられている場合は、ノードにログインします。手順については、「DLP-A60 CTC へのログイン」(p.17-71) を参照してください。
- ステップ 2** 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 3** ノードがネットワークに接続されていないことを確認します。
- ノードの属しているネットワークが動作中である場合は、そのノードからログアウトして、「NTP-A313 リニア ADM からの稼働中のノードの削除」(p.14-21)、 「NTP-A240 BLSR ノードの削除」(p.14-7)、または「NTP-A294 UPSR ノードの削除」(p.14-14) を実行します。ノードが Dense Wavelength Division Multiplexing (DWDM; 高密度波長分割多重) 設定の一部である場合は、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。ステップ 4 へ進んでください。
  - ノードの接続されているネットワークが動作していなくて、現在の設定も必要でなくなった場合は、ステップ 4 へ進みます。



(注) ステップ 4 ~ 14 を省略すると、現在の設定が保存されます。

- ステップ 4** ノード ビューで Circuits タブをクリックして回線が表示されていないことを確認し、ステップ 5 へ進みます。回線が表示されている場合は、そのノードに起点または終点があるすべての回線を、次のようにして削除します。



(注) ノードから回線を削除する場合は、どのネットワークにもノードが接続されていないことを確認してください。

- 削除の必要がある回線をクリックし、Delete をクリックします。
- Yes をクリックします。

回線が表示されなくなるまで繰り返します。

- ステップ 5** ノード ビューで Provisioning > Protection タブをクリックし、次のようにしてすべての保護グループを削除します。

- 削除する必要がある保護グループをクリックし、Delete をクリックします。
- Yes をクリックします。

保護グループが表示されなくなるまで繰り返します。

- ステップ 6** ノード ビューで Provisioning > Comm Channels タブをクリックし、通信チャネルの終端をすべて削除します。

- 削除する必要がある Section DCC (SDCC)、Line DCC (LDCC)、Generic Communications Channel (GCC) または OSC 終端を、該当するサブタブ (SDCC、LDCC、GCC、または OSC) からクリックし、Delete をクリックします。
- Yes をクリックします。

SDCC、LDCC、GCC、または OSC の終端が表示されなくなるまで、この手順を繰り返します。



(注) OSC の終端を削除する前に、リング ID が削除されていることを確認してください。  
Provisioning > Comm Channels > OSC タブをクリックします。リング ID を選択して Delete をクリックします。

**ステップ 7** 取り付けられている OC-N または DS-N カードごとに、すべてのポートを Out-of-Service and Management, Disabled (OOS-MA,DSBLD) サービス状態にします。

- a. カード ビューで、Provisioning > Line タブをクリックします。
- b. すべてのポートについて、Status カラムの下をクリックして OOS,DSBLD が選択されていることを確認します。



(注) DWDM カードの詳細については、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。

**ステップ 8** カードに接続されているファイバをすべて取り外します。

**ステップ 9** ノード ビューで、取り付けられているカードを右クリックし、Delete をクリックします。

**ステップ 10** Yes をクリックします。

**ステップ 11** カードを削除したら、そのカードのイジェクタを開いてノードから取り外します。

**ステップ 12** 取り付けられているカードごとに、[ステップ 7 ~ 11](#) を繰り返します。



(注) Cisco Transport Controller (CTC) の TCC2 または TCC2P カードは削除できません。他のすべてのカードを削除して取り外したあとで、物理的に取り外してください。

**ステップ 13** 取り外したすべてのカードを保管し、現場の規則に従ってインベントリ レコードを更新します。

**ステップ 14** ノードに電力を供給している電源装置の電源を切断します。

**ステップ 15** ノードをその外部ヒューズ ソースから切り離します。

**終了 :** この手順は、これで完了です。





## DLP A1 ~ A99

---

### DLP-A1 シェルフ アセンブリの開梱と確認

目的	この作業では、パッケージからシェルフ アセンブリを取り出します。
工具 / 機器	なし
事前準備手順	なし
必須 / 適宜	必須
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** 設置場所で ONS 15454 システム機器を受け取ったら、箱の上部を開きます。Cisco Systems のロゴがある側が箱の上部です。
- ステップ 2** 箱から発砲スチロールを取り出します。箱には、ONS 15454 シェルフ（ビニールで包装されています）と、設置に必要な部品を含む小さい箱が入っています。
- ステップ 3** シェルフを取り出します。その際、シェルフ取り出しストラップの両方のリングを持って、シェルフを箱の外にゆっくりと持ち上げます。
- ステップ 4** 設置用の部品が入った小さな箱を開き、「[シスコが提供する部品](#)」(p.1-3) に示されている品目がすべて揃っていることを確認します。



---

**(注)** ファントレイ アセンブリは、同梱されていません。

---

- ステップ 5** 元の NTP（手順）に戻ります。
-

## DLP-A2 シェルフ アセンブリの検査

目的	この作業では、シェルフ アセンブリのすべての部品が適切な状態であることを確認します。
工具 / 機器	前面扉用ピン付き六角（アレン）キー
事前準備手順	DLP-A1 シェルフ アセンブリの開梱と確認（p.17-1）
必須 / 適宜	必須
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** ピン付き六角キーを使用してシェルフを開きます。詳細については、「DLP-A8 前面扉のオープン」（p.17-8）を参照してください。
- ステップ 2** 次の点を確認します。
- ピンが曲がっていたり、壊れていたたりしない。
  - フレームが曲がっていない。
- ステップ 3** ピンが曲がっているか壊れている場合やフレームが曲がっている場合は、シスコの販売担当者に連絡して交換してください。
- ステップ 4** 設置する前に、前面扉を閉じます。
- ステップ 5** 元の NTP（手順）に戻ります。
- 

## DLP-A3 19 インチ（482.6 mm）ラックに適合させるためのマウント ブラケットの反転

目的	この作業では、マウント ブラケットを取り付けて、23 インチ（584.2 mm）ラックを 19 インチ（482.6 mm）ラックに変換します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
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
セキュリティ レベル	なし

**注意**

圧着部品は ONS 15454 の付属品のみを使用し、ハードウェアおよび結合部の緩み、劣化、電気機械的な腐食がないよう注意してください。

---

**注意**

ONS 15454 を不導体コーティング (塗料、ラッカー、またはエナメルなど) を施したフレームに取り付ける場合は、ONS 15454 梱包キットに付属の溝付きネジを使用するか、または溝からコーティングを除去して、電気的導通性を確保します。

**ステップ 1** シェルフ アセンブリの片側から、マウント ブラケットの取り付けネジを取り外します。

**ステップ 2** 取り外したマウント ブラケットを上下逆さまにします。

マウント ブラケットに刻まれた文字も逆さまになります。

**ステップ 3** マウント ブラケットの幅広の面がシェルフ アセンブリと接するように合わせます (図 17-1 を参照)。

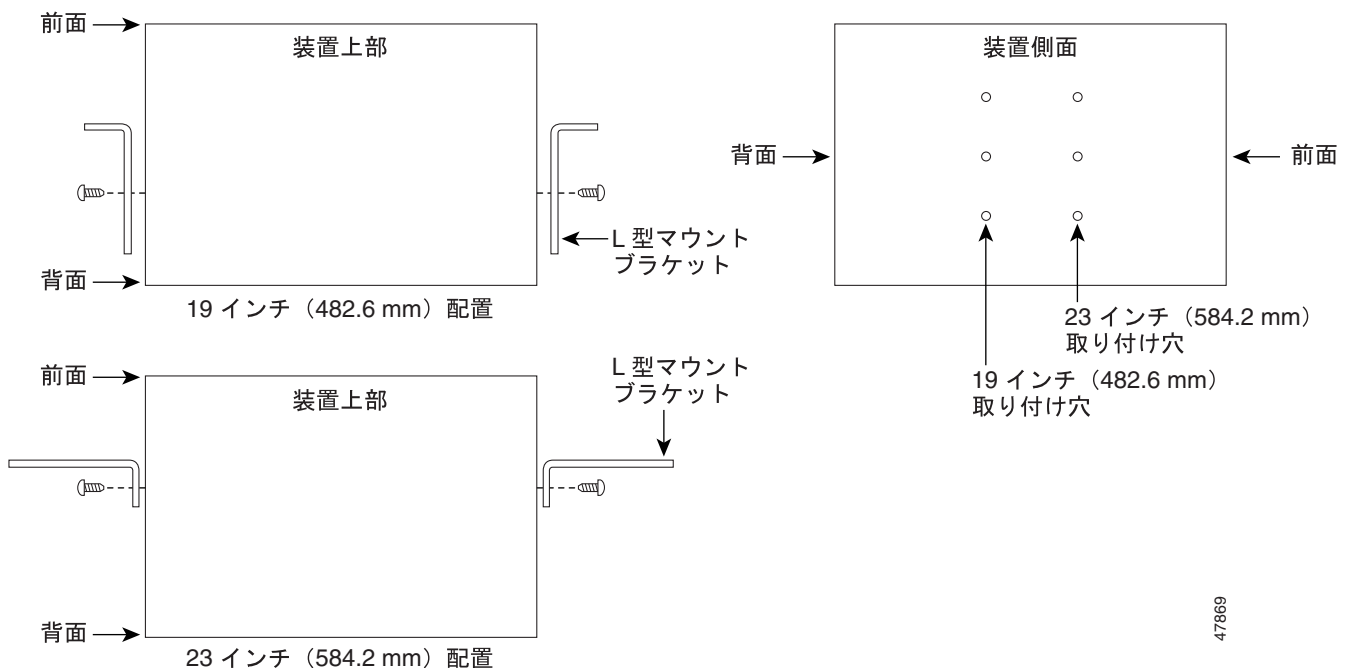
マウント ブラケットの幅が狭い面が、シェルフ アセンブリの前面を向くようにします。マウント ブラケットに刻まれた文字が逆さまに見える位置になります。

**ステップ 4** マウント ブラケットのネジ穴をシェルフ アセンブリのネジ穴に合わせます。

**ステップ 5** ステップ 1 で取り外したネジを差し込んで、締めます。

**ステップ 6** 反対側のマウント ブラケットにもこの作業を繰り返します。

図 17-1 マウント ブラケットの反転 (23 インチ [584.2 mm] 配置から 19 インチ [482.6 mm] 配置へ)



**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A4 外部ブラケットおよびエアー フィルタの取り付け

目的	この作業では、ファントレイ アセンブリの下でなくシェルフの底部に、外部ブラケットおよびエアー フィルタを取り付けます。シェルフの底部に外部ブラケットおよびエアー フィルタを取り付けると、エアー フィルタを扱うときに、ファントレイ アセンブリを取り外す必要がなくなります。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	DLP-A3 19 インチ (482.6 mm) ラックに適合させるためのマウント ブラケットの反転 (p.17-2) (必要に応じて)
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)

ブラケットを取り付けない場合は、エアー フィルタをシェルフ アセンブリの底部にあるコンパートメントにスライドさせて、取り付けます。これ以降は、エアー フィルタを取り外して取り付け直すたびに、まずファントレイ アセンブリを取り外す必要があります。シェルフ アセンブリのいずれのフィルタ位置にも、エアー フィルタを取り付けないでください。

**ステップ 1** ファントレイ アセンブリを取り外した状態のまま、ONS 15454 を水平な場所に逆さまに置きます。



(注)

フィルタはどちらの側を正面にして取り付けても機能しますが、フィルタの表面を保護するために、押え金具を表向きにしてフィルタを取り付けることを推奨します。

**ステップ 2** シェルフ アセンブリ底部の左右両側に並んでいる 3 つのネジ穴を確認します。

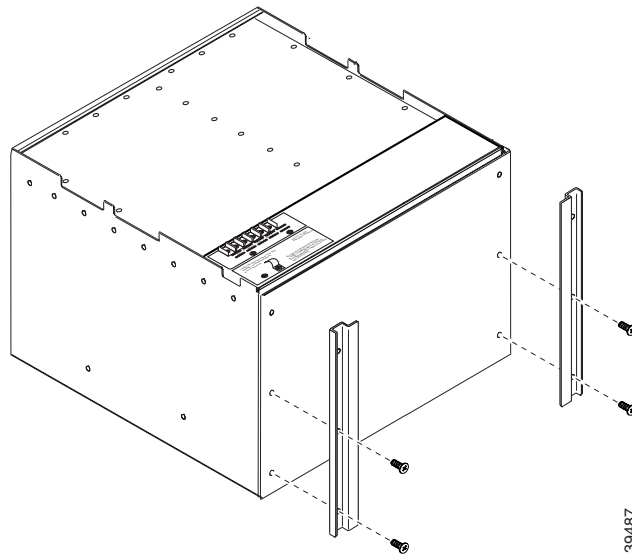
**ステップ 3** バックプレーン スタンドオフ キット (53-0795-XX) に付属のネジ (48-0003) を使用して、シェルフ アセンブリの底部に各ブラケットを固定します。

各ブラケットの一端には、フィルタ ストッパとフランジがあります。ストッパとフランジがシェルフ アセンブリの背面 (取り付け時に ONS 15454 を逆さまにした場合は、上部) を向くようにブラケットを取り付けます

図 17-2 に、底部ブラケットの取り付け方法を示します。これ以降、ブラケットを使用しない場合は、ファントレイ アセンブリを取り外してから、エアー フィルタを取り外す必要があります。ブラケットを使用すると、ファントレイ アセンブリを取り外さなくても、エアー フィルタを清掃したり、交換することができます。



図 17-2 外部ブラケットの取り付け



**ステップ 4** エアー フィルタをシェルフ アセンブリにスライドします。

**ステップ 5** 元の NTP (手順) に戻ります。

## 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)

<b>目的</b>	この作業では、シェルフ アセンブリを 1 人でラックに取り付けます。
<b>工具 / 機器</b>	ピン付き六角レンチ 固定ネジ (48-1003-XX) (2) 取り付け用プラスなベネジ (48-1004-XX、48-1007-XX) (8) #2 プラス ドライバ
<b>事前準備手順</b>	<a href="#">DLP-A3 19 インチ (482.6 mm) ラックに適合させるためのマウント ブラケットの反転 (p.17-2)</a> (必要に応じて) <a href="#">DLP-A4 外部ブラケットおよびエアー フィルタの取り付け (p.17-4)</a> (必要に応じて)
<b>必須 / 適宜</b>	適宜
<b>オンサイト / リモート</b>	オンサイト
<b>セキュリティ レベル</b>	なし

**ステップ 1** 上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。

- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル (シェルフごとに最低 30 A のヒューズ) が必要。
- 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル (シェルフごとに最低 20 A のヒューズ) が必要。

## ■ 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)

- ステップ 2** シェルフ アセンブリが、適切なラック サイズに合わせてあることを確認します (23 インチ [584.2 mm] または 19 インチ [482.6 mm])。
- ステップ 3** アセンブリに付属している六角レンチを使用して、シェルフの取り付けに使用しないネジ穴に 2 本の固定ネジを取り付けます。ネジをしっかりと差し込んで、マウント ブラケットを固定します。
- ステップ 4** シェルフ アセンブリを目的のラック位置まで持ち上げて、固定ネジの上に置きます。
- ステップ 5** マウント ブラケットのネジ穴をラックの取り付け穴の位置に合わせます。
- ステップ 6** プラス ドライバを使用して、アセンブリの両側にそれぞれ取り付けネジを 1 本取り付けます。
- ステップ 7** シェルフ アセンブリをラックに固定したら、残りの取り付けネジを取り付けます。



(注) 1 組以上の水平ネジ穴を使用して、ONS 15454 が滑らないようにします。

- ステップ 8** 六角レンチを使用して、仮留め用のネジを取り外します。
- ステップ 9** 元の NTP (手順) に戻ります。

## 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)

<b>目的</b>	この作業では、シェルフ アセンブリを 2 人でラックに取り付けます。
<b>工具 / 機器</b>	ピン付き六角レンチ 固定ネジ (48-1003-XX) (2) 取り付け用プラスなベネジ (48-1004-XX、48-1007-XX) (8) #2 プラス ドライバ
<b>事前準備手順</b>	<a href="#">DLP-A3 19 インチ (482.6 mm) ラックに適合させるためのマウント ブラケットの反転 (p.17-2)</a> (必要に応じて) <a href="#">DLP-A4 外部ブラケットおよびエア フィルタの取り付け (p.17-4)</a> (必要に応じて)
<b>必須 / 適宜</b>	必須
<b>オンサイト / リモート</b>	オンサイト
<b>セキュリティ レベル</b>	なし

- ステップ 1** 上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。
- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル (シェルフごとに最低 30 A のヒューズ) が必要。
  - 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル (シェルフごとに最低 20 A のヒューズ) が必要。

- ステップ 2** シェルフ アセンブリが、適切なラック サイズに合わせてあることを確認します (23 インチ [584.2 mm] または 19 インチ [482.6 mm])。
- ステップ 3** シェルフ アセンブリに付属している六角レンチを使用して、シェルフの取り付けに使用しないネジ穴に 2 本の固定ネジ (48-1003-XX) を取り付けます。固定ネジを差し込んで、マウント ブラケットをしっかりと固定します。
- ステップ 4** シェルフ アセンブリを目的のラック位置まで持ち上げます。
- ステップ 5** マウント ブラケットのネジ穴をラックの取り付け穴の位置に合わせます。
- ステップ 6** 1 人がシェルフ アセンブリを適切な位置に保持している間に、もう 1 人がプラス ドライバを使用して、アセンブリの両側へ取り付けネジを 1 本ずつ取り付けます。
- ステップ 7** シェルフ アセンブリをラックに固定したら、残りの取り付けネジを取り付けます。



**(注)** 1 組以上の水平ネジ穴を使用して、ONS 15454 が滑らないようにします。

- ステップ 8** 六角レンチを使用して、仮留め用のネジを取り外します。
- ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A7 ラックへの複数のシェルフ アセンブリの取り付け

目的	この作業では、複数のシェルフをラックに取り付けます。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	DLP-A3 19 インチ (482.6 mm) ラックに適合させるためのマウント ブラケットの反転 (p.17-2) (必要に応じて) DLP-A4 外部ブラケットおよびエア フィルタの取り付け (p.17-4) (必要に応じて)
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)** ONS 15454 のファン吸気口にエアフローを取り入れるには、設置されたシェルフ アセンブリの下に 1 インチ (25.4 mm) の隙間が必要です。シェルフ アセンブリの下に別の ONS 15454 を設置する場合は、下部シェルフ アセンブリの上にあるエア ランプによって必要なスペースが確保されます。ただし、サードパーティ製の機器の上に ONS 15454 を取り付けた場合は、サードパーティ製シェルフ アセンブリと ONS 15454 の底部との間に、1 インチ (25.4 mm) 以上の隙間を確保する必要があります。サードパーティ製の機器から ONS 15454 に熱気が排出されないようにしてください。

- ステップ 1** 上部取り付けスペースに、適切なヒューズ アラーム パネルが取り付けられていることを確認します。ヒューズ アラーム パネルが取り付けられていない場合は、メーカーの指示に従って取り付けます。
- 15454-SA-ANSI または 15454-SA-HD シェルフ アセンブリを取り付ける場合は、100 A ヒューズ パネル（シェルフごとに最低 30 A のヒューズ）が必要。
  - 15454-SA-NEBS3 シェルフ アセンブリを取り付ける場合は、標準の 80 A ヒューズ パネル（シェルフごとに最低 20 A のヒューズ）が必要。
- ステップ 2** 最初の ONS 15454 を、ヒューズ アラーム パネルの下に直接取り付けます。「[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) または「[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) に従ってください。
- ステップ 3** 残りのシェルフにこの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-A8 前面扉のオープン

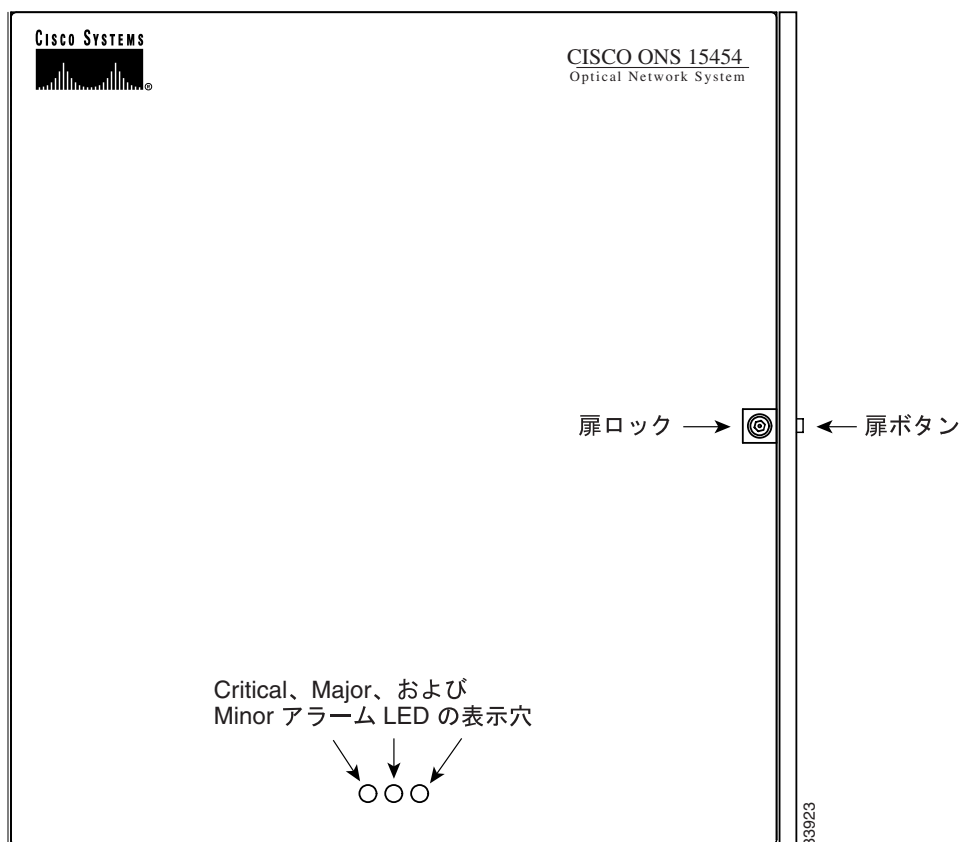
目的	この作業では、キャビネット コンパートメントの前面扉を開く方法を示します。
工具 / 機器	ピン付き六角キー
事前準備手順	なし
必須 / 適宜	必須
オンサイト / リモート	オンサイト
セキュリティ レベル	なし



- (注)** ONS 15454 には静電気防止用リスト ストラップが付属していて、その差し込み口があります。リスト ストラップのプラグ差し込み口は、シェルフ アセンブリの右下外側の端にあります。上部および下部に [ESD] というラベルが付いています。ONS 15454 で作業をする際は、必ず静電気防止用リスト ストラップを着用し、ストラップを ESD プラグに接続してください。

- ステップ 1** 前面扉のロックを解除します（[図 17-3](#)）。
- ONS 15454 には、前面扉の鍵を開閉するためのピン付き六角キーが付属しています。キーを左回りに回転させると扉がロック解除され、右回りに回転させるとロックされます。
- ステップ 2** 扉のボタンを押して、ラッチをリリースします。
- ステップ 3** 扉を開きます。

図 17-3 Cisco ONS 15454 の前面扉



**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A9 前面扉の取り外し

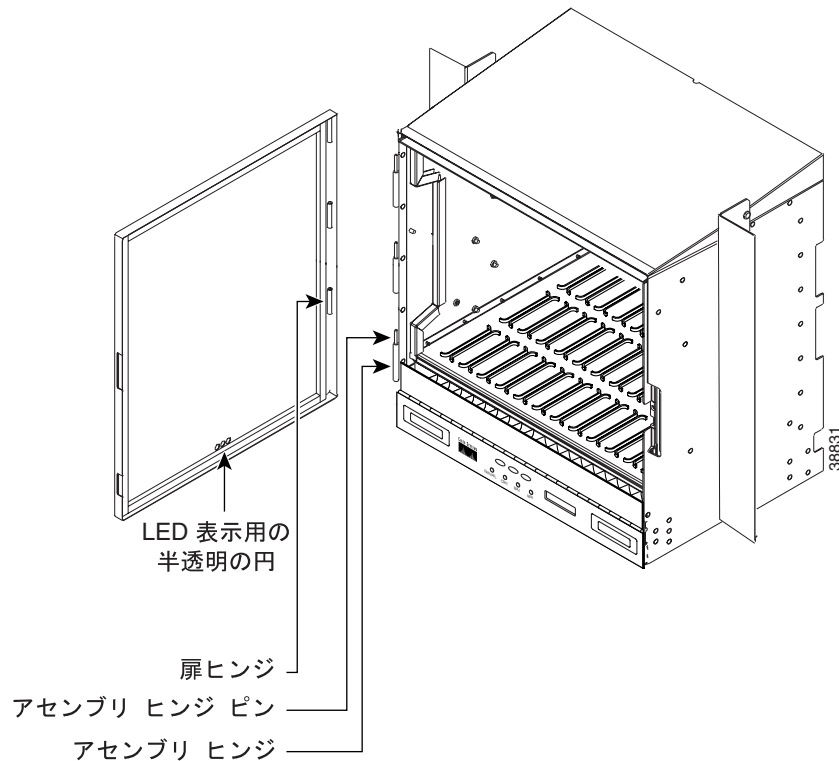
目的	この作業では、キャビネット コンパートメントの前面扉を取り外します。
工具 / 機器	オープンエンド レンチ
事前準備手順	<a href="#">DLP-A8 前面扉のオープン (p.17-8)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

**ステップ 1** 扉のアース ストラップ (Release 3.3 以降で使用可能) を取り外す手順は、次のとおりです。

- 前面扉からアース ストラップを取り外すには、オープンエンド レンチを使用して #6 ケブナット (49-0600-01) を緩めます。扉内のオス スタッドから、アース ストラップ 圧着端子 (72-3622-01) の一端を取り外します。
- ファイバ ガイドの長い方のネジからアース ストラップの反対側を取り外すには、オープンエンド レンチを使用して、圧着端子の #4 ケブナット (49-0337-01) を緩めます。圧着端子およびロック ワッシャを取り外します。

**ステップ2** 扉の左上隅にあるヒンジから扉を持ち上げます (図 17-4)。

図 17-4 ONS 15454 前面扉の取り外し



**ステップ3** 元の NTP (手順) に戻ります。

## DLP-A10 下部バックプレーン カバーの取り外し

目的	この作業では、下部バックプレーン カバーを取り外します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	なし
必須 / 適宜	必須
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** カバーを所定位置に固定している 5 本の固定ネジを外します。

**ステップ2** カバーの両側を持ちます。

**ステップ3** カバーをバックプレーンから静かに引き抜きます。

**ステップ 4** 元の NTP (手順) に戻ります。

---

## DLP-A11 金属製バックプレーン カバーの取り外し

目的	この作業では、EIA が取り付けられていない場合に、バックプレーンに取り付けられた金属製バックプレーン カバーを取り外します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ
事前準備手順	<a href="#">DLP-A10 下部バックプレーン カバーの取り外し (p.17-10)</a>
必須 / 適宜	必須
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** バックプレーンの金属製カバーを取り外すには、ONS 15454 を固定している 5 本のネジを緩めて、シェルフ アセンブリから引き出します。

**ステップ 2** 金属製バックプレーン カバーを所定位置に固定している 9 本の周辺ネジを緩めます。

**ステップ 3** パネルを底部から持ち上げて、シェルフ アセンブリから取り外します。

**ステップ 4** あとで使用できるようにパネルを保管しておきます。EIA を取り付けない場合は、必ずバックプレーン カバーを取り付けます。

**ステップ 5** 元の NTP (手順) に戻ります。

---

## DLP-A12 BNC または高密度 BNC EIA の取り付け

目的	この作業では、BNC または高密度 BNC EIA を取り付けます。DS3-12、DS3XM-6、または EC-1 カードを使用していて、SMB インターフェイスよりも BNC インターフェイスが必要な場合は、この作業を実行します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺に取り付けるネジ (9) 内側に取り付けるネジ (12) バックプレーン カバー ネジ (5) BNC または 高密度 BNC カード
事前準備手順	<a href="#">NTP-A4 バックプレーン カバーの取り外し (p.1-8)</a>
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** パッケージから BNC または高密度 BNC カードを取り出します。カードのコネクタをバックプレーンの対応するコネクタに合わせます。カードを静かに押し込んで、両方のコネクタ セットをしっかりと噛み合わせます。
- ステップ 2** 金属製 EIA パネルをカードに合わせます。
- ステップ 3** 9 本の周辺ネジ (部品番号 48-0358) を差し込んで締め (8 ~ 10 lb [3.6 ~ 4.5 kg])、カバー パネルをバックプレーンに固定します。
- ステップ 4** 12 本 (BNC) または 9 本 (高密度 BNC) の内側ネジ (部品番号 48-0004) を差し込んで締め (8 ~ 10 lb [3.6 ~ 4.5 kg])、カバー パネルをカードおよびバックプレーンに固定します。

 [17-5](#) に、BNC EIA の取り付け方法を示します。



図 17-5 BNC EIA の取り付け

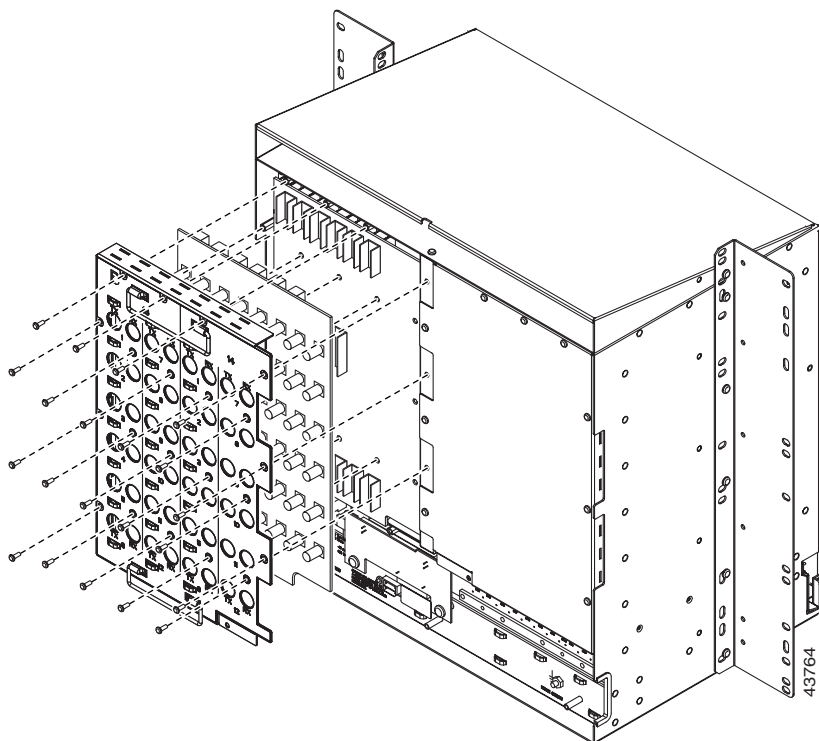
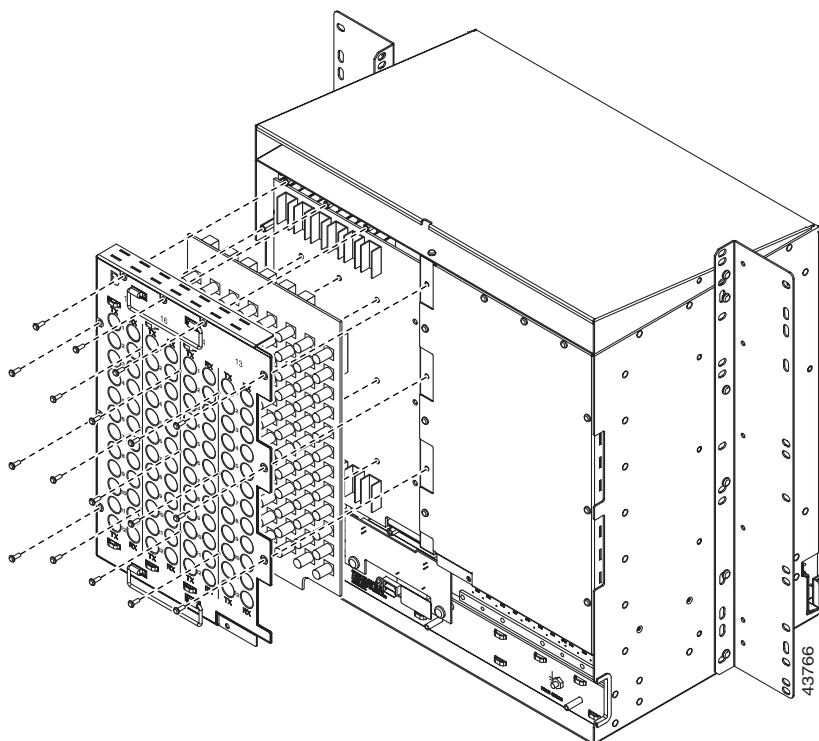


図 17-6 に、高密度 BNC EIA の取り付け方法を示します。

図 17-6 高密度 BNC EIA の取り付け



**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A13 SMB EIA の取り付け

<b>目的</b>	この作業では、SMB EIA を取り付けます。DS1-14 カードを使用して、AMP インターフェイスよりも SMB インターフェイスが必要な場合、または DS3-12、DS3XM-6、または EC-1 カードを使用している、BNC インターフェイスよりも SMB インターフェイスが必要な場合は、SMB EIA を使用します。
<b>工具 / 機器</b>	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺ネジ (9) 内側に取り付けるネジ (12) バックプレーン カバー ネジ (5) SMB カード フォイル EMI ガスケット (SMB EIA アセンブリによってはすでに取り付けられていることがある) 金属製 SMB カバー パネル
<b>事前準備手順</b>	なし
<b>必須 / 適宜</b>	適宜
<b>オンサイト / リモート</b>	オンサイト
<b>セキュリティ レベル</b>	なし

**ステップ 1** パッケージから SMB カードを取り出します。カードのコネクタをバックプレーンの対応するコネクタに合わせます。カードを静かに押し込んで、両方のコネクタ セットをしっかりと噛み合わせます。

**ステップ 2** フォイル EMI ガスケットを SMB カードに合わせて、フォイル EMI ガスケットの穴を SMB コネクタの穴に合わせます。



### 注意

SMB EIA アセンブリが取り付けられた状態でフォイル EMI ガスケットが出荷される場合があります。そうでない場合は、フォイル EMI ガスケットを取り付けて、EMI (電磁波干渉) に関する注意事項に適合させる必要があります。

**ステップ 3** 金属製 SMB カバー パネルをカードに合わせます。

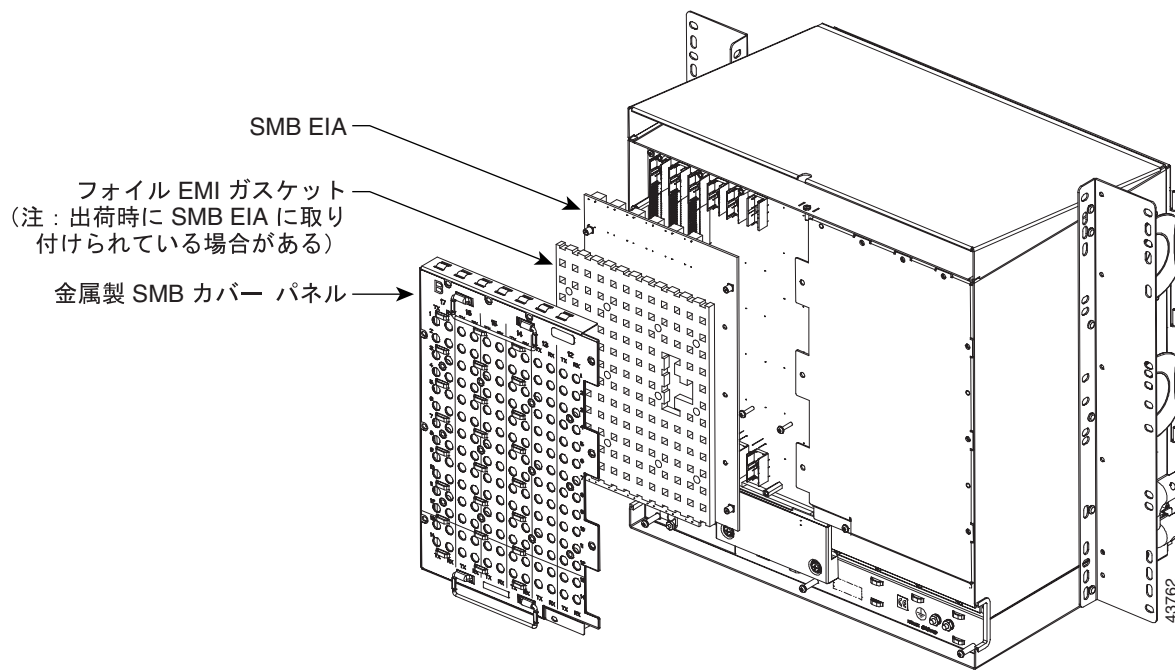
**ステップ 4** 12 本の内側ネジ (部品番号 48-0004) を差し込んで締め (8 ~ 10 lb [3.6 ~ 4.5 kg])、カバー パネルをカードおよびバックプレーンに固定します。

**ステップ 5** 9 本の周辺ネジ (部品番号 48-0358) を差し込んで締め (8 ~ 10 lb [3.6 ~ 4.5 kg])、カバー パネルをバックプレーンに固定します。

SMB EIA を使用して DS-1 接続を行っている場合は、DS-1 電気インターフェイス アダプタが必要です。このアダプタは通常、バラン (部品番号 15454-WW-14=) といいます。

図 17-7 に、SMB EIA の取り付け方法を示します。

図 17-7 SMB EIA の取り付け (DS-1 接続にバランを使用)



**ステップ 6** 元の NTP (手順) に戻ります。

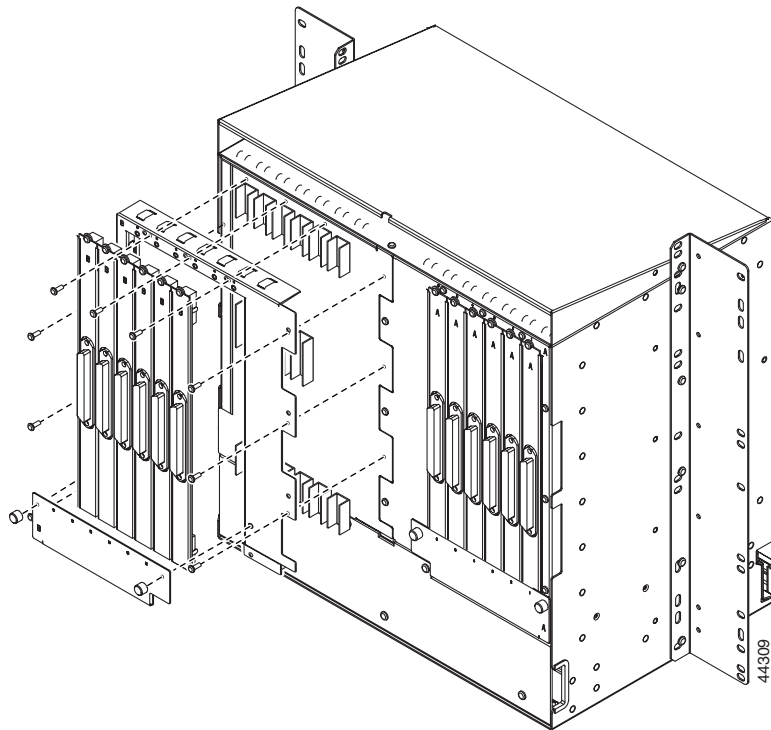
## DLP-A14 AMP Champ EIA の取り付け

目的	この作業では、AMP Champ EIA を取り付けます。DS1-14 カードを使用していて、SMB インターフェイスより AMP インターフェイスが必要な場合は、AMP Champ EIA を使用します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ 周辺ネジ (9) 内側に取り付けるネジ (12) バックプレーン カバー ネジ (5) AMP Champ カード (6) EIA パネル
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
セキュリティ レベル	なし

- 
- ステップ 1** AMP Champ パネルをバックプレーンに合わせ、9 本の周辺ネジ (部品番号 48-0358) を差し込んで締めます (8 ~ 10 lb [3.6 ~ 4.5 kg])。
- ステップ 2** AMP Champ カードをバックプレーン コネクタに合わせて、押し込み、しっかり装着します。6 つの AMP Champ カードをすべて取り付けるまで、この手順を繰り返します。
- ステップ 3** 各 AMP Champ カードをカバー パネルに固定するには、各カードの上部にネジ (部品番号 48-003) を差し込んで締めます (8 ~ 10 lb [3.6 ~ 4.5 kg])。
- ステップ 4** AMP Champ 固定プレートをカバー パネルの底部に合わせて、2 本の取り付けネジを手で締めます。

[図 17-8](#) に、AMP Champ EIA の取り付け方法を示します。

図 17-8 AMP Champ EIA の取り付け



**ステップ 5** 元の NTP (手順) に戻ります。

---

## DLP-A16 ONS 15454 へのオフィス アースの接続

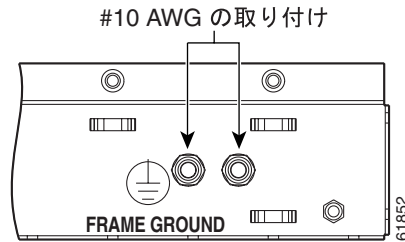
目的	この作業では、ONS 15454 シェルフにアースを接続します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ ネジ 電源コード (ヒューズ アラーム パネルからアセンブリまで)、#10 AWG、銅コンダクタ、90°C (194°F) ストランド アース ケーブル (機器フレームからオフィス アースまで)、#6 AWG リストされている圧着端子コネクタ (通常はデュアル端子タイプ)。コネクタは、スタッド サイズおよび間隔が装置ラックの仕様に基づく #6 AWG 銅コンダクタに適したものを使用する必要があります。オフィス アース接続には、通常、現地の規約に従って H-TAP 圧着コネクタを使用します。 ワイヤ カッター ワイヤ ストリッパ 圧着工具
事前準備手順	DLP-A10 下部バックプレーン カバーの取り外し (p.17-10)
必須 / 適宜	必須
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** オフィス アース ケーブル (#6 AWG ストランド) が、現地の規約に従って、ベイ上部およびオフィス アースに接続されていることを確認します。
- ステップ 2** 指定された 2 穴圧着端子コネクタを使用して、シェルフ アース ケーブル (#10 AWG) の一端をシェルフのフレーム アース支柱に取り付けます。バックプレーンのアース場所については、[図 17-9](#) を参照してください。



**(注)** フレーム アースを終端する場合は、ONS 15454 に付属のケブナットを使用して、31 インチ / ポンドの指定トルクで締めます。ケブナットを使用すると、フレーム アース接続が可能になり、取り付け時およびメンテナンス作業中の回転による緩みを最小限に抑えることができます。ケブナットがフレーム アース接続で実現する防止タイプは、本来、バッテリー接続およびバッテリー リターン接続の端子ブロックで提供されます。

図 17-9 バックプレーンのアース場所



**ステップ 3** 装置ベイ フレーム仕様に従って、2 穴コネクタ圧着端子を使用し、シェルフ アース ケーブルの反対側を装置ベイ フレームに接続します。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A17 ONS 15454 シェルフへのオフィス電源の接続

目的	この作業では、ONS 15454 シェルフに電源を接続します。
工具 / 機器	#2 プラス ドライバ 中型スロット ヘッド ネジ用ドライバ 小型スロット ヘッド ネジ用ドライバ ワイヤ カッター ワイヤ ストリッパ 圧着工具 ヒューズ パネル 電源コード (ヒューズ アラーム パネルとアセンブリを接続)、#10 AWG、銅コンダクタ、90°C (194°F) スtrand アース ケーブル #6 AWG
事前準備手順	<a href="#">DLP-A16 ONS 15454 へのオフィス アースの接続 (p.17-18)</a>
必須 / 適宜	必須
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



**警告**

装置の取り付けまたは交換を行う場合は、必ずアース線を最初に接続し、最後に取り外す必要があります。



**(注)**

バッテリー リターン接続は、Telcordia GR-1089-CORE Issue 3 の定義に従って、DC-I として処理されます。



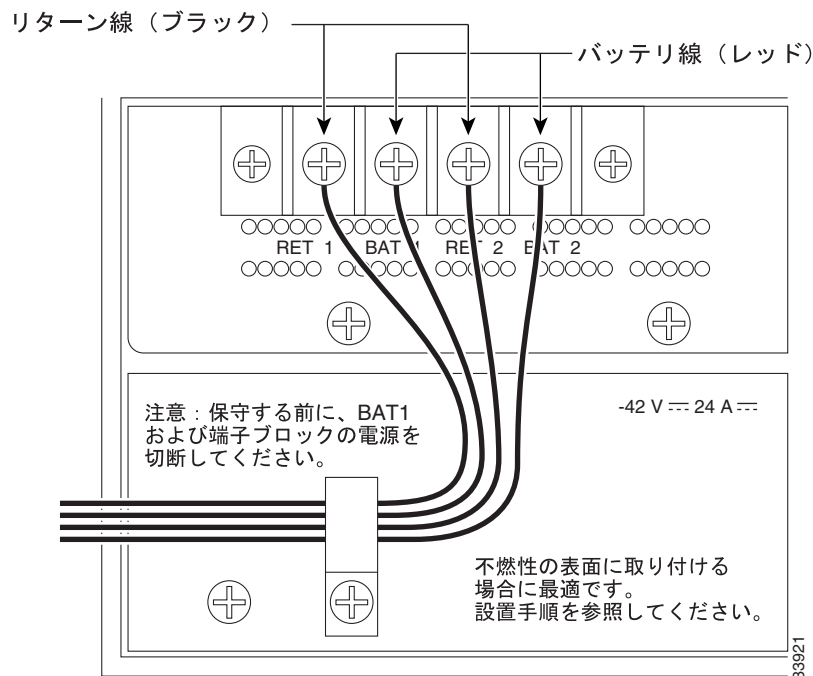
(注) Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) サーバから時刻を取得するようにプロビジョニングされていないシステムで、電源が切断されるか、または TCC2/TCC2P の両方のカードがリセットされた場合は、ONS 15454 クロックをリセットする必要があります。電源の切断後、日付はデフォルトの 1970 年 1 月 1 日 00:04:15 になります。クロックのリセットについては、「NTP-A25 名前、日付、時刻、連絡先情報の設定」(p.4-6) を参照してください。TCC2/TCC2P カードを使用している場合、システム クロックは最長 3 時間まで稼働し続けます。この場合、対応は不要です。



(注) 電源装置に問題が発生した場合は、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

- ステップ 1** ヒューズ パネルのエンジニアリング仕様に従って、オフィス電源を接続します。
- ステップ 2** ヒューズ パネルから ONS 15454 まで到達するようにケーブルを測定し、必要に応じて切断します。[図 17-10](#) に、ONS 15454 の電源端子を示します。
- ステップ 3** 現地の規約に従って、電源コードに印を付けます。

**図 17-10 Cisco ONS 15454 の電源端子**



- ステップ 4** ONS 15454 の #8 電源端子ネジを取り外すか、または緩めます。混乱を避けるために、BAT1/RET1 (A) 電源端子に接続されたケーブルに 1 のラベルを付け、BAT2/RET2 (B) 電源端子に接続されたケーブルに 2 のラベルを付けます。





(注) バッテリー、バッテリーリターン、およびフレームアースコンダクタを終端する場合は、リング、フォーク、デュアル端子タイプなどの圧着端子コネクタのみを使用します。

**注意**

圧着接続を行う場合は、むき出しのすべての導体（バッテリー、バッテリーリターン、およびフレームアース）を、適切な酸化防止剤でコーティングします。めっきしていないすべてのコネクタ、ブレードストラップ、およびバスバーを接続する前に、光沢仕上げを施し、酸化防止剤でコーティングします。コネクタにスズめっき、はんだめっき、または銀めっきを施したり、接続面にその他のめっき処理を施す必要はありません。ただし、これらを常に清潔な状態に保ち、汚れが付着しないようにしてください。

**注意**

電源、リターン、フレームアースを終端する場合は、はんだ付け端子、ネジなし（押し込み）コネクタ、クイック接続コネクタ、または他の摩擦式コネクタを使用しないでください。

**ステップ 5** 使用するすべての電源コードから、絶縁被膜を 1/2 インチ（12.7 mm）はぎ取ります。

**ステップ 6** すべての電源コードの両端に圧着端子を圧着します。



(注) バッテリー接続およびバッテリーリターン接続を終端する場合は（[図 17-10](#) を参照）、10 インチ / ポンドのトルク仕様に従います。

**ステップ 7** リターン 1 導線を RET1 バックプレーン端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

**ステップ 8** マイナス 1 導線をマイナス BAT1 バックプレーン電源端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

**ステップ 9** 冗長電源コードを使用している場合は、リターン 2 導線を ONS 15454 のプラス RET2 端子に終端します。マイナス 2 導線を ONS 15454 のマイナス BAT2 端子に終端します。酸化防止用グリースを使用して、接続の腐食を防止します。

**ステップ 10** プラスチックのケーブルクランプを使用して、電源端子の下にケーブルを配線します（[図 17-10](#) を参照）。

**ステップ 11** 元の NTP（手順）に戻ります。

## DLP-A18 オフィス電源の投入と検証

目的	この作業では、電力を測定して正しい電源およびリターンであることを確認します。
工具 / 機器	電圧計
事前準備手順	DLP-A16 ONS 15454 へのオフィスアースの接続 (p.17-18) DLP-A17 ONS 15454 シェルフへのオフィス電源の接続 (p.17-19)
必須 / 適宜	必須
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** 電圧計を使用して、ヒューズ アラーム パネルの次のポイントでオフィス バッテリとアースを検証します。

- a. 電源を検証するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を A 側接続に接続し、 $-40.5$  VDC から  $-57$  VDC の間であることを確認します。レッドのテスト線を B 側接続に接続し、 $-40.5$  VDC から  $-57$  VDC の間であることを確認します。



**(注)**  $-40.5$  VDC と  $-57$  VDC という電圧は、それぞれシャーシに電力を供給するために必要な最小および最大電圧です。

- b. アースを確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を A 側リターン アースに接続し、電圧が存在しないことを確認します。レッドのテスト線を B 側リターン アースに接続し、電圧が存在しないことを確認します。

**ステップ 2** 次のいずれかの手順を実行して、ノードに電力を供給します。

- 80 A のヒューズ パネルを使用している場合は、現地の規約に従ってヒューズ位置に 20 A ヒューズを挿入します。
- 100 A のヒューズ パネルを使用している場合は、現地の規約に従ってヒューズ位置に 30 A ヒューズを挿入します。

**ステップ 3** 電圧計を使用して、シェルフで  $-48$  VDC バッテリとアースを確認します。

- a. シェルフの A 側を確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を BAT1 (A 側バッテリー接続) のレッド ケーブルに接続します。 $-40.5$  VDC から  $-57$  VDC の間になることを確認します。その後、電圧計のレッドのテスト線を RET1 (A 側リターン アース) ブラック ケーブルに接続し、電圧が存在しないことを確認します。



**(注)**  $-40.5$  VDC と  $-57$  VDC という電圧は、それぞれシャーシに電力を供給するために必要な最小および最大電圧です。


- b. シェルフの B 側を確認するには、電圧計のブラックのテスト線をフレーム アースに接続します。レッドのテスト線を BAT2 (B 側バッテリー接続) のレッド ケーブルに接続します。 $-40.5$  VDC から  $-57$  VDC の間になることを確認します。その後、電圧計のレッドのテスト線を RET2 (B 側リターン アース) ブラック ケーブルに接続し、電圧が存在しないことを確認します。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A19 バックプレーンへのアラーム ケーブルの取り付け

目的	この作業では、バックプレーンにアラーム ケーブルを取り付けることにより、Alarm Interface Controller-International (AIC-I) カードを使用して外部 (環境) のアラームおよび制御をプロビジョニングできるようにします。Alarm Extension Panel (AEP) を使用している場合は、この作業を実行しないでください。
工具 / 機器	ワイヤラッパー  #22 または #24 AWG (0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) ケーブル  100 シールド付き Building Integrated Timing Supply (BITS) クロック ケーブル ペア #22 または #24 AWG(0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) ツイストペア T1 タイプ
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
セキュリティ レベル	なし

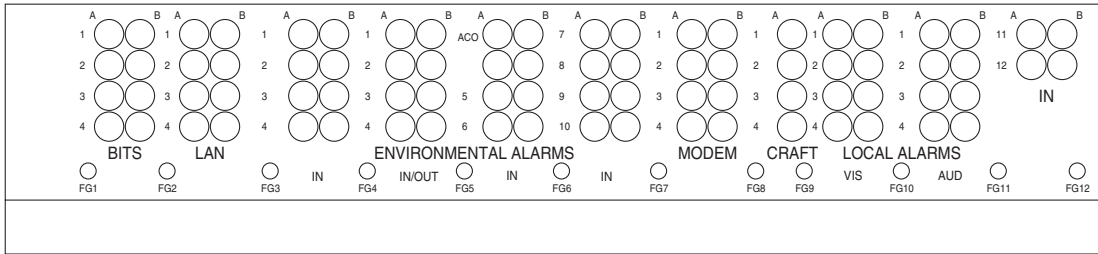
**ステップ 1** 100 シールド付き BITS クロック ケーブル ペア #22 または #24 AWG(0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup>) ツイストペア T1 タイプ ケーブルを使用して、現地の規約に従って、適切なワイヤラップ ピンにアラーム ケーブルをラップします。BITS 側で、BITS 入力ケーブルのシールドをアースします。BITS 出力の場合は、BITS ケーブルのアース シールドを、BITS ピンの列の下にあるフレーム アース ピン (FG1) にラップします。

 [図 17-11](#) に、Release 3.4 以上の ONS 15454 バックプレーンの AIC-I に対応するアラーム ピン割り当てを示します。



**(注)** AIC-I を使用する場合は、シェルフ アセンブリで 3.4.0 以降のソフトウェア リリースが稼働している必要があります。ANSI シェルフのバックプレーンには、[図 17-11](#) のレイアウトに従ってピンが割り当てられたワイヤラップ フィールドがあります。シェルフ アセンブリの既存のシェルフが、R3.4 以降にアップグレードされている場合には、バックプレーン ピンのラベルが[図 17-13](#) のようになりますが、[図 17-11](#) に示された AIC-I のピン割り当てを使用する必要があります。

図 17-11 Cisco ONS 15454 バックプレーンのピン割り当て (Release 3.4 以降)



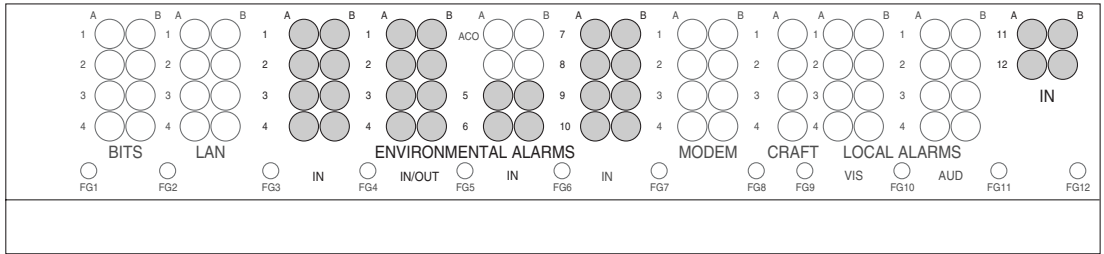
フィールド	ピン	説明	フィールド	ピン	説明	
BITS	A1	BITS 出力 2 マイナス (-)	ENVIR ALARMS IN/OUT	A1/A13	通常開いている出力ペア番号 1	
	B1	BITS 出力 2 プラス (+)		B1/B13		
	A2	BITS 入力 2 マイナス (-)		A2/A14	通常開いている出力ペア番号 2	
	B2	BITS 入力 2 プラス (+)		B2/B14		
	A3	BITS 出力 1 マイナス (-)		A3/A15	通常開いている出力ペア番号 3	
	B3	BITS 出力 1 プラス (+)		B3/B15		
	A4	BITS 入力 1 マイナス (-)		A4/A16	通常開いている出力ペア番号 4	
	B4	BITS 入力 1 プラス (+)		B4/B16		
LAN	ハブまたはスイッチに接続		ACO	A1	通常開いている ACO ペア	
	A1	RJ-45 ピン 6 RX-		B1		
	B1	RJ-45 ピン 3 RX+		CRAFT	A1	受信 (PC ピン #2)
	A2	RJ-45 ピン 2 TX-			A2	送信 (PC ピン #3)
	B2	RJ-45 ピン 1 TX+	A3		アース (PC ピン #5)	
	PC/ワークステーションまたはルータに接続		A4		DTR (PC ピン #4)	
	A1	RJ-45 ピン 2 RX-	LOCAL ALARMS AUD (Audible)	A1	アラーム出力ペア番号 1 : リモート音声アラーム	
	B1	RJ-45 ピン 1 RX+		B1		
A2	RJ-45 ピン 6 TX-	A2		アラーム出力ペア番号 2 : Critical 音声アラーム		
B2	RJ-45 ピン 3 TX+	B2				
ENVIR ALARMS IN	A1	アラーム入力ペア番号 1 : 接続ケーブルが閉じているかどうかをレポート	N/O	A3	アラーム出力ペア番号 3 : Major 音声アラーム	
	B1	アラーム入力ペア番号 2 : 接続ケーブルが閉じているかどうかをレポート		B3		
	A2	アラーム入力ペア番号 2 : 接続ケーブルが閉じているかどうかをレポート		A4	アラーム出力ペア番号 4 : Minor 音声アラーム	
	B2	アラーム入力ペア番号 2 : 接続ケーブルが閉じているかどうかをレポート		B4		
	A3	アラーム入力ペア番号 3 : 接続ケーブルが閉じているかどうかをレポート	LOCAL ALARMS VIS (Visual)	A1	アラーム出力ペア番号 1 : リモート ビジュアル アラーム	
	B3	アラーム入力ペア番号 3 : 接続ケーブルが閉じているかどうかをレポート		B1		
	A4	アラーム入力ペア番号 4 : 接続ケーブルが閉じているかどうかをレポート		A2	アラーム出力ペア番号 2 : Critical ビジュアル アラーム	
	B4	アラーム入力ペア番号 4 : 接続ケーブルが閉じているかどうかをレポート		B2		
	A5	アラーム入力ペア番号 5 : 接続ケーブルが閉じているかどうかをレポート	N/O	A3	アラーム出力ペア番号 3 : Major ビジュアル アラーム	
	B5	アラーム入力ペア番号 5 : 接続ケーブルが閉じているかどうかをレポート		B3		
	A6	アラーム入力ペア番号 6 : 接続ケーブルが閉じているかどうかをレポート		A4	アラーム出力ペア番号 4 : Minor ビジュアル アラーム	
	B6	アラーム入力ペア番号 6 : 接続ケーブルが閉じているかどうかをレポート		B4		
A7	アラーム入力ペア番号 7 : 接続ケーブルが閉じているかどうかをレポート					
A8	アラーム入力ペア番号 8 : 接続ケーブルが閉じているかどうかをレポート					
A9	アラーム入力ペア番号 9 : 接続ケーブルが閉じているかどうかをレポート					
A10	アラーム入力ペア番号 10 : 接続ケーブルが閉じているかどうかをレポート					
A11	アラーム入力ペア番号 11 : 接続ケーブルが閉じているかどうかをレポート					
A12	アラーム入力ペア番号 12 : 接続ケーブルが閉じているかどうかをレポート					

AIC-I カードを使用している場合は、ピン 1~4 が OUT としてプロビジョニングされています。また、ピン 13~16 が IN としてプロビジョニングされています。

83020

図 17-12 に、Release 3.4 以降のバックプレーンの環境アラーム ピン割り当てを示します。

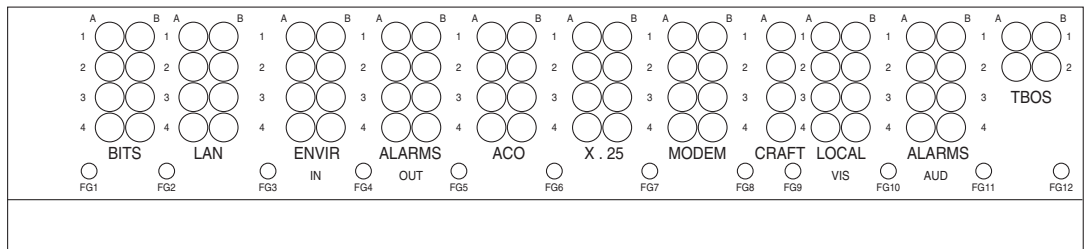
図 17-12 環境アラーム (強調表示)



83020

図 17-13 に、Release 3.3 以前のシェルフのアラーム ピン割り当てを示します。AIC-I は Release 3.3 以前のシェルフと互換性がありません。

図 17-13 Cisco ONS 15454 バックプレーンのピン割り当て (Release 3.3 以前)



フィールド	ピン	説明	フィールド	ピン	説明
BITS	A1	BITS 出力 2 マイナス (-)	ENVIR ALARMS OUT	A1	通常開いている出力ペア番号 1
	B1	BITS 出力 2 プラス (+)		B1	
	A2	BITS 入力 2 プラス (+)		A2	通常開いている出力ペア番号 2
	B2	BITS 入力 2 プラス (+)		B2	
	A3	BITS 出力 1 マイナス (-)	N/O	A3	通常開いている出力ペア番号 3
	B3	BITS 出力 1 プラス (+)		B3	
LAN	A4	BITS 入力 1 マイナス (-)	ACO	A1	通常開いている ACO ペア
	B4	BITS 入力 1 プラス (+)		B1	
	ハブまたはスイッチに接続		CRAFT	A1	受信 (PC ピン #2)
	A1	RJ-45 ピン 6 RX-		A2	送信 (PC ピン #3)
	B1	RJ-45 ピン 3 RX+		A3	アース (PC ピン #5)
	A2	RJ-45 ピン 2 TX-		A4	DTR (PC ピン #4)
	PC/ワークステーションまたはルータに接続		LOCAL ALARMS AUD (Audible)	A1	アラーム出力ペア番号 1 : リモート音声アラーム
	A1	RJ-45 ピン 2 RX-		B1	
B1	RJ-45 ピン 1 RX+	A2		アラーム出力ペア番号 2 : Critical 音声アラーム	
A2	RJ-45 ピン 6 TX-	B2			
ENVIR ALARMS IN	B2	RJ-45 ピン 3 TX+	N/O	A3	アラーム出力ペア番号 3 : Major 音声アラーム
	A1	アラーム入力ペア番号 1 : 接続ケーブルが閉じているかどうかをレポート		B3	
	B1	アラーム入力ペア番号 2 : 接続ケーブルが閉じているかどうかをレポート		A4	アラーム出力ペア番号 4 : Minor 音声アラーム
	A2	アラーム入力ペア番号 3 : 接続ケーブルが閉じているかどうかをレポート		B4	
	A3	アラーム入力ペア番号 4 : 接続ケーブルが閉じているかどうかをレポート	LOCAL ALARMS VIS (Visual)	A1	アラーム出力ペア番号 1 : リモート ビジュアル アラーム
	A4	アラーム入力ペア番号 4 : 接続ケーブルが閉じているかどうかをレポート		B1	
B3		A2		アラーム出力ペア番号 2 : Critical ビジュアル アラーム	
B4		B2			
		N/O	A3	アラーム出力ペア番号 3 : Major ビジュアル アラーム	
			B3		
			A4	アラーム出力ペア番号 4 : Minor ビジュアル アラーム	
			B4		

38533

## ■ DLP-A20 バックプレーンへのタイミングケーブルの取り付け



(注) X.25、Modem、および TBOS ピン フィールドは無効です。

**ステップ 2** 元の NTP (手順) に戻ります。

## DLP-A20 バックプレーンへのタイミングケーブルの取り付け

目的	この作業では、バックプレーンに BITS タイミングケーブルを取り付けます。
工具 / 機器	ワイヤラッパー 100 シールド付き BITS クロック ケーブル ペア #22 または #24 AWG (0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) ツイストペア T1 タイプ
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
セキュリティレベル	なし

**ステップ 1** 100 シールド付き BITS クロック ケーブル ペア #22 または #24 AWG(0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup>) ツイストペア T1 タイプ ケーブルを使用して、現地の規約に従って、適切なワイヤラップ ピンにクロック線をラップします

BITS 側で、BITS 入力ケーブルのシールドをアースします。BITS 出力の場合は、BITS ケーブルのアース シールドを、BITS ピンの列の下にあるフレーム アース ピン (FG1) にラップします。表 17-1 に、BITS タイミング ピン フィールドのピン割り当てを示します。

表 17-1 BITS の外部タイミング ピン割り当て

BITS ピン	Tip/Ring	CTC/TL1 名	説明
A4	Ring	BITS-1	BITS デバイス 1 からの入力
B4	Tip	BITS-1	BITS デバイス 1 からの入力
A3	Ring	BITS-1	外部デバイス 1 への出力
B3	Tip	BITS-1	外部デバイス 1 への出力
A2	Ring	BITS-2	BITS デバイス 2 からの入力
B2	Tip	BITS-2	BITS デバイス 2 からの入力
A1	Ring	BITS-2	外部デバイス 2 への出力
B1	Tip	BITS-2	外部デバイス 2 への出力



(注) タイミングの詳細については、『Cisco ONS 15454 Reference Manual』にある「Timing」の章を参照してください。システム タイミングの設定については、「NTP-A28 タイミングの設定」(p.4-11)を参照してください。

**ステップ 2** 元の NTP (手順) に戻ります。

## DLP-A21 バックプレーンへの LAN ケーブルの取り付け

目的	この作業では、バックプレーンに LAN ケーブルを取り付けます。
工具 / 機器	ワイヤラッパー  #22 または #24 AWG (0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) ケーブル (CAT-5 UTP を推奨)
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
セキュリティ レベル	なし



(注)

必要であれば、LAN ケーブルを使用しないで、TCC2/TCC2P の LAN 接続ポートを使用することもできます。バックプレーン接続または TCC2/TCC2P 前面接続を使用します。LAN バックプレーンピンと TCC2/TCC2P の LAN 接続ポートを同時に使用することはできません。ただし、TCC2/TCC2P に直接接続しているコンピュータが同じ LAN に接続していない場合に限って、LAN バックプレーンピンが使用されているときに、コンピュータから TCC2/TCC2P の LAN 接続ポートに直接接続することができます。

- ステップ 1** #22 または #24 AWG (0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup>) ケーブルまたは CAT-5 UTP イーサネット ケーブルを使用し、現地の規約に従って、適切なワイヤラップピンにケーブルをラップします。



注意

受信 (Rx) および送信 (Tx) ピンが CAT-5 ケーブルの同じツイストペア線に接続されている場合は、漏話が発生することがあります。2 つの Tx ピンと 2 つの Rx ピンをそれぞれ異なるツイストペアに接続する必要があります。

フレームアースピンは各ピンフィールドの下にあります (LAN ピンフィールドの場合は FG2)。LAN インターフェイスケーブルのアースシールドを、フレームアースピンにラップします。表 17-2 に、LAN ピン割り当てを示します。

表 17-2 LAN ピン割り当て

ピンフィールド	バックプレーンピン	RJ-45 ピン	機能 / 色
LAN 1 Data Circuit-terminating Equipment (DCE*; データ回線終端装置) (ハブまたはスイッチ)、ONS 15454 は DCE。	B2	1	TX+ ホワイト / グリーン
	A2	2	TX- グリーン
	B1	3	RX+ ホワイト / オレンジ
	A1	6	RX- オレンジ
LAN 1 Data Terminal Equipment (DTE; データ端末装置) に接続 (PC/ ワークステーションまたはルータ)	B1	1	RX+ ホワイト / グリーン
	A1	2	RX- グリーン
	B2	3	TX+ ホワイト / オレンジ
	A2	6	TX- オレンジ



(注) TCC2/TCC2P はイーサネット極性検出をサポートしません。イーサネット接続の極性が正しくない場合は(ケーブルの受信線ペアがフリップしている場合のみ発生することがある) [Lan Connection Polarity Reversed] 状態が生じます。この状態は通常、アップグレード中または最初のノード配置中に発生します。この状況を改善するには、イーサネットケーブルにワイヤラップピンが正しく対応付けられているか確認します。

**ステップ 2** 元の NTP (手順) に戻ります。

## DLP-A22 TL1 クラフト インターフェイスの取り付け

目的	この作業では、クラフトバックプレーンピンを使用して、TL1 クラフト インターフェイスを取り付けます。TCC2/TCC2P カードの EIA/TIA-232 ポートに接続された LAN ケーブルを使用して、TL1 クラフト インターフェイスにアクセスすることもできます。
工具 / 機器	ワイヤラッパー
事前準備手順	#22 または #24 AWG (0.51 mm <sup>2</sup> または 0.64 mm <sup>2</sup> ) アラーム線 <a href="#">NTP-A4 バックプレーン カバーの取り外し (p.1-8)</a>
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) クラフトピンを使用しないで、TCC2/TCC2P カードの EIA/TIA-232 ポートに接続された LAN ケーブルを使用して、TL1 クラフト インターフェイスにアクセスすることもできます。

**ステップ 1** #22 または #24 AWG (0.51 mm<sup>2</sup> または 0.64 mm<sup>2</sup>) ケーブルを使用し、現地の規約に従って、適切なワイヤラップピンにクラフト インターフェイス ケーブルをラップします。

**ステップ 2** クラフト インターフェイス ケーブルのアース シールドを、フレーム アース ピンにラップします。

コンピュータ ケーブルのアース線をクラフト ピン フィールドのピン A3 にラップします。[表 17-3](#) に CRAFT ピン フィールドのピン割り当てを示します。



(注) クラフトバックプレーンピンと TCC2/TCC2P カードの EIA/TIA-232 ポートを同時に使用することはできません。同時に使用すると、ノードにアクセスできなくなったり、接続が切断されたりします。



表 17-3 クラフト インターフェイス ピンの割り当て

ピン フィールド	ピン	説明
Craft	A1	受信
	A2	送信
	A3	アース
	A4	DTR

**ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A23 電気インターフェイス アダプタ (バラン) を使用した DS-1 ケーブルの取り付け

目的	この作業では、電気インターフェイス アダプタを使用して、SMB EIA に DS-1 ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー ツイストペア ケーブル
事前準備手順	<a href="#">DLP-A13 SMB EIA の取り付け (p.17-14)</a>
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)

ONS 15454 DS-1 ポートに接続されたすべての DS-1 ケーブルは、ツイストペア ケーブルを使用して終端し、DS-1 電気インターフェイス アダプタに接続する必要があります。DS-1 電気インターフェイス アダプタは、SMB EIA よりも 1.72 インチ (43.7 mm) 突き出しています。詳細については、『Cisco ONS 15454 Reference Manual』の「Shelf and Backplane Hardware」の章を参照してください。

**ステップ 1** バックプレーンのポート送信ペアの SMB コネクタに、アダプタの SMB コネクタを接続します。

**ステップ 2** バックプレーンのポート受信ペアの SMB コネクタに、アダプタの SMB コネクタを接続します。

**ステップ 3** ポートの DS-1 送受信ケーブルをアダプタのワイヤラップ ポートに終端します。

- ワイヤラップ工具を使用して、受信ケーブルを、目的のポートに対応したバックプレーン コネクタの受信アダプタ ピンに接続します。
- 送信ケーブルを、目的のポートに対応したバックプレーン コネクタの送信アダプタ ピンに接続します。
- 現地の規約に従って、DS-1 ケーブルのシールド アース ケーブルをアースに終端します。

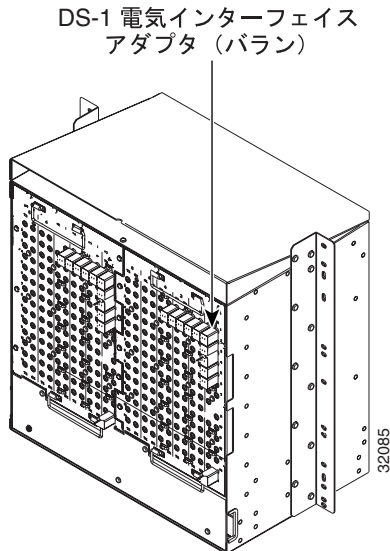


(注)

DS1N-14 カードをスロット 3 および 15 に装着して 1:N 保護グループを形成する場合は、DS-1 電気インターフェイス アダプタのスロット 3 および 15 をラップしないでください。

図 17-14 に、SMB EIA が取り付けられた ONS 15454 バックプレーンを示します。シェルフ アセンブリの両側に DS-1 電気インターフェイス アダプタ (バラン) が取り付けられていて、DS-1 ツイストペア終端ポイントを形成しています。

図 17-14 DS-1 ケーブルに対応する SMB EIA が取り付けられたバックプレーン



**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A24 AMP Champ EIA への DS-1 AMP Champ ケーブルの取り付け

目的	この作業では、AMP Champ EIA に DS-1 AMP Champ ケーブルを取り付けます。
工具 / 機器	ワイヤ ラッパー ツイストペア ケーブル
事前準備手順	<a href="#">DLP-A14 AMP Champ EIA の取り付け (p.17-16)</a>
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** シェルフ アセンブリに取り付ける DS1-14/DS1N-14 カードごとに、56 線ケーブルを 1 本準備します。

**ステップ 2** ケーブルのオス AMP Champ コネクタを、ONS 15454 バックプレーンのメス AMP Champ コネクタに接続します。

**ステップ 3** オス AMP Champ コネクタのクリップを使用して、接続を固定します。

メス コネクタの外側エッジには、クリップを所定位置に合わせるための溝があります。

表 17-4 に、ONS 15454 AMP Champ EIA の AMP Champ コネクタのピン割り当てを示します。



(注) 表 17-4 の影のついた領域は、ホワイト / オレンジ バインダ グループに対応します。バインダ グループは、業界標準の色分け方式によって色分けされた 25 のケーブル ペアで構成されています。

表 17-4 AMP Champ コネクタのピン割り当て

信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 1 ホワイト / ブルー	1	33	Tx Ring 1 ブルー / ホワイト	Rx Tip 1 イエロー / オレンジ	17	49	Rx Ring 1 オレンジ / イエロー
Tx Tip 2 ホワイト / オレンジ	2	34	Tx Ring 2 オレンジ / ホワイト	Rx Tip 2 イエロー / グリーン	18	50	Rx Ring 2 グリーン / イエロー
Tx Tip 3 ホワイト / グリーン	3	35	Tx Ring 3 グリーン / ホワイト	Rx Tip 3 イエロー / ブラウン	19	51	Rx Ring 3 ブラウン / イエロー
Tx Tip 4 ホワイト / ブラウン	4	36	Tx Ring 4 ブラウン / ホワイト	Rx Tip 4 イエロー / ブルーグレー	20	52	Rx Ring 4 ブルーグレー / イエロー
Tx Tip 5 ホワイト / ブルーグレー	5	37	Tx Ring 5 ブルーグレー / ホワイト	Rx Tip 5 バイオレット / ブルー	21	53	Rx Ring 5 ブルー / バイオレット
Tx Tip 6 レッド / ブルー	6	38	Tx Ring 6 ブルー / レッド	Rx Tip 6 バイオレット / オレンジ	22	54	Rx Ring 6 オレンジ / バイオレット
Tx Tip 7 レッド / オレンジ	7	39	Tx Ring 7 オレンジ / レッド	Rx Tip 7 バイオレット / グリーン	23	55	Rx Ring 7 グリーン / バイオレット
Tx Tip 8 レッド / グリーン	8	40	Tx Ring 8 グリーン / レッド	Rx Tip 8 バイオレット / ブラウン	24	56	Rx Ring 8 ブラウン / バイオレット
Tx Tip 9 レッド / ブラウン	9	41	Tx Ring 9 ブラウン / レッド	Rx Tip 9 バイオレット / ブルーグレー	25	57	Rx Ring 9 ブルーグレー / バイオレット
Tx Tip 10 レッド / ブルーグレー	10	42	Tx Ring 10 ブルーグレー / レッド	Rx Tip 10 <sup>1</sup> ホワイト / ブルー	26	58	Rx Ring 10 ブルー / ホワイト
Tx Tip 11 ブラック / ブルー	11	43	Tx Ring 11 ブルー / ブラック	Rx Tip 11 ホワイト / オレンジ	27	59	Rx Ring 11 オレンジ / ホワイト
Tx Tip 12 ブラック / オレンジ	12	44	Tx Ring 12 オレンジ / ブラック	Rx Tip 12 ホワイト / グリーン	28	60	Rx Ring 12 グリーン / ホワイト
Tx Tip 13 ブラック / グリーン	13	45	Tx Ring 13 グリーン / ブラック	Rx Tip 13 ホワイト / ブラウン	29	61	Rx Ring 13 ブラウン / ホワイト

表 17-4 AMP Champ コネクタのピン割り当て (続き)

信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 14 ブラック / ブラウン	14	46	Tx Ring 14 ブラウン / ブラック	Rx Tip 14 ホワイト / ブルー グレー	30	62	Rx Ring 14 ブルーグレー / ホ ワイト
Tx Spare0+ 使用しない	15	47	Tx Spare0- 使用しない	Rx Spare0+ 使用しない	31	63	Rx Spare0- 使用しない
Tx Spare1+ 使用しない	16	48	Tx Spare1- 使用しない	Rx Spare1+ 使用しない	32	64	Rx Spare1- 使用しない

1. ピン 26、27、28、29、30、58、59、60、61、および 62 は、ホワイト / オレンジ バインダグループに対応します。バインダグループは、業界標準の色分け方式によって色分けされた 25 のケーブル ペアで構成されています。

表 17-5 に、シールド付き DS-1 ケーブルに対応する、ONS 15454 AMP Champ EIA の AMP Champ コネクタのピン割り当てを示します。

表 17-5 AMP Champ コネクタのピン割り当て (シールド付き DS-1 ケーブル)

64 ピン ブルー バンドル				64 ピン オレンジ バンドル			
信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 1 ホワイト / ブルー	1	33	Tx Ring 1 ブルー / ホワイト	Rx Tip 1 ホワイト / ブルー	17	49	Rx Ring 1 ブルー / ホワイト
Tx Tip 2 ホワイト / オレンジ	2	34	Tx Ring 2 オレンジ / ホワイト	Rx Tip 2 ホワイト / オレンジ	18	50	Rx Ring 2 オレンジ / ホワイト
Tx Tip 3 ホワイト / グリーン	3	35	Tx Ring 3 グリーン / ホワイト	Rx Tip 3 ホワイト / グリーン	19	51	Rx Ring 3 グリーン / ホワイト
Tx Tip 4 ホワイト / ブラウン	4	36	Tx Ring 4 ブラウン / ホワイト	Rx Tip 4 ホワイト / ブラウン	20	52	Rx Ring 4 ブラウン / ホワイト
Tx Tip 5 ホワイト / ブルー グレー	5	37	Tx Ring 5 ブルーグレー / ホ ワイト	Rx Tip 5 ホワイト / ブルー グレー	21	53	Rx Ring 5 ブルーグレー / ホ ワイト
Tx Tip 6 レッド / ブルー	6	38	Tx Ring 6 ブルー / レッド	Rx Tip 6 レッド / ブルー	22	54	Rx Ring 6 ブルー / レッド
Tx Tip 7 レッド / オレンジ	7	39	Tx Ring 7 オレンジ / レッド	Rx Tip 7 レッド / オレンジ	23	55	Rx Ring 7 オレンジ / レッド
Tx Tip 8 レッド / グリーン	8	40	Tx Ring 8 グリーン / レッド	Rx Tip 8 レッド / グリーン	24	56	Rx Ring 8 グリーン / レッド
Tx Tip 9 レッド / ブラウン	9	41	Tx Ring 9 ブラウン / レッド	Rx Tip 9 レッド / ブラウン	25	57	Rx Ring 9 ブラウン / レッド
Tx Tip 10 レッド / ブルー グレー	10	42	Tx Ring 10 ブルーグレー / レッド	Rx Tip 10 レッド / ブルー グレー	26	58	Rx Ring 10 ブルーグレー / レッド
Tx Tip 11 ブラック / ブルー	11	43	Tx Ring 11 ブルー / ブラック	Rx Tip 11 ブラック / ブルー	27	59	Rx Ring 11 ブルー / ブラック

表 17-5 AMP Champ コネクタのピン割り当て (シールド付き DS-1 ケーブル)(続き)

64 ピン ブルー バンドル				64 ピン オレンジ バンドル			
信号 / 線	ピン	ピン	信号 / 線	信号 / 線	ピン	ピン	信号 / 線
Tx Tip 12 ブラック/オレンジ	12	44	Tx Ring 12 オレンジ/ブラック	Rx Tip 12 ブラック/オレンジ	28	60	Rx Ring 12 オレンジ/ブラック
Tx Tip 13 ブラック/グリーン	13	45	Tx Ring 13 グリーン/ブラック	Rx Tip 13 ブラック/グリーン	29	61	Rx Ring 13 グリーン/ブラック
Tx Tip 14 ブラック/ブラウン	14	46	Tx Ring 14 ブラウン/ブラック	Rx Tip 14 ブラック/ブラウン	30	62	Rx Ring 14 ブラウン/ブラック
Tx Tip 15 ブラック/ブルーグレー	15	47	Tx Tip 15 ブルーグレー/ブラック	Rx Tip 15 ブラック/ブルーグレー	31	63	Rx Tip 15 ブルーグレー/ブラック
Tx Tip 16 イエロー/ブルー	16	48	Tx Tip 16 ブルー/イエロー	Rx Tip 16 イエロー/ブルー	32	64	Rx Tip 16 ブルー/イエロー

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け

目的	この作業では、BNC コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A12 BNC または高密度 BNC EIA の取り付け (p.17-12)</a>
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



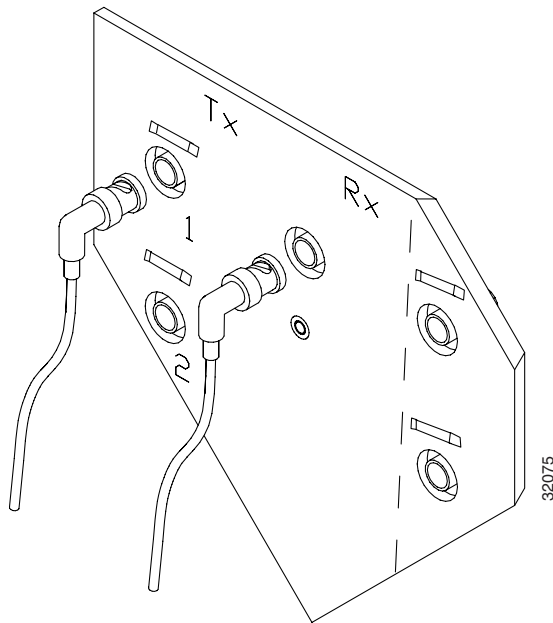
### 警告

外部プラント回線 (T1/E1/T3/E3 など) に接続するための金属製インターフェイスは、CSU/DSU (チャンネル サービス ユニット / データ サービス ユニット) や NT1 (ネットワーク終端 1) などの登録済みデバイスや承認済みデバイスを介して接続する必要があります。

**ステップ 1** バックプレーンの目的の接続ポイントに BNC ケーブル コネクタを合わせます。

[図 17-15](#) に、直角 BNC ケーブル コネクタを使用して BNC EIA に同軸ケーブルを接続する方法を示します。

図 17-15 直角 BNC コネクタを使用した 同軸ケーブルの取り付け



- ステップ 2** ケーブル コネクタの slots がバックプレーン接続ポイントの対応するノッチの上になるように、コネクタを合わせます。
- ステップ 3** コネクタを静かに押し下げて、バックプレーン コネクタのノッチをケーブル コネクタの slots にスライドさせます。
- ステップ 4** ケーブル コネクタを右に回して、所定の位置にロックします。
- ステップ 5** Telcordia 標準 (GR-1275-CORE) または現地の規約に従って、ケーブルを EIA にタイラップするか、または燃り合わせます。
- ステップ 6** 現地の規約に従って、ケーブルをシェルフアセンブリの最も近い側面の穴に通して、この側面に配線します。側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。
- ステップ 7** 接続の両側ですべてのケーブルにラベルを付け、外見の似たケーブルが混同しないようにします。
- ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け

目的	この作業では、高密度 BNC コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	BNC 取り付け工具
事前準備手順	<a href="#">DLP-A12 BNC または高密度 BNC EIA の取り付け (p.17-12)</a>
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** バックプレーンの目的の接続ポイントにケーブル コネクタを合わせます。
- ステップ 2** BNC 取り付け工具を使用して、ケーブル コネクタのスロットがバックプレーン接続ポイントの対応するノッチの上になるように、コネクタを合わせます。
- ステップ 3** コネクタを静かに押し下げて、バックプレーン コネクタのノッチをケーブル コネクタのスロットにスライドさせます。
- ステップ 4** ケーブル コネクタを右に回して、所定の位置にロックします。
- ステップ 5** Telcordia 標準 (GR-1275-CORE) または現地の規約に従って、ケーブルを EIA にタイラップするか、または撚り合わせます。
- ステップ 6** 現地の規約に従って、ケーブルをシェルフアセンブリの最も近い側面の穴に通して、この側面に配線します。
- 側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。
- ステップ 7** 元の NTP (手順) に戻ります。
- 

## DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け

目的	この作業では、SMB コネクタを使用して同軸ケーブルを取り付けます。
工具 / 機器	SMB ケーブル コネクタ
事前準備手順	<a href="#">DLP-A13 SMB EIA の取り付け (p.17-14)</a>
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

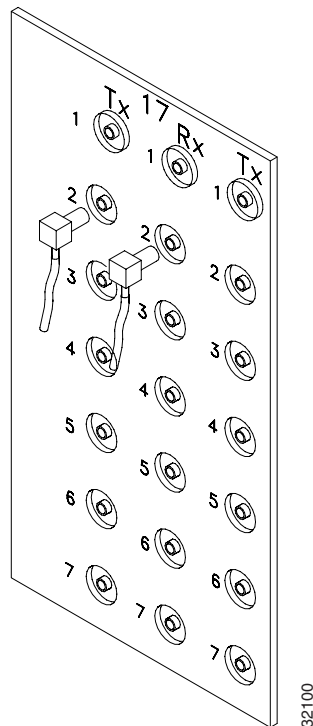


**警告**

外部プラント回線 (T1/E1/T3/E3 など) に接続するための金属製インターフェイスは、CSU/DSU や NT1 などの登録済みデバイスや承認済みデバイスを介して接続する必要があります。

**ステップ 1** バックプレーンの目的の接続ポイントに SMB ケーブル コネクタを合わせます (図 17-16)。

図 17-16 SMB コネクタを使用した同軸ケーブルの取り付け



**ステップ 2** カチッという音がするまでコネクタを静かに押して、コネクタを固定します。

**ステップ 3** Telcordia 標準 (GR-1275-CORE) または現地の規約に従って、ケーブルを EIA にタイラップするか、または燃り合わせます。

**ステップ 4** 現地の規約に従って、ケーブルをシェルフアセンブリの最も近い側面に這わせて、ラックに配線します。

**ステップ 5** 接続の両側で終端ケーブル、受信ケーブル、現用ケーブル、および保護ケーブルにラベルを付け、外見の似たケーブルと混同しないようにします。

**ステップ 6** 元の NTP (手順) に戻ります。



## DLP-A28 同軸ケーブルの配線

目的	この作業では、同軸ケーブルを配線します。
工具 / 機器	RG179、RG59 (735A) #26 AWG ケーブル、または RG59 (734A) #20 AWG ケーブル
事前準備手順	必要に応じて次の作業を 1 つまたは複数実行します。 <ul style="list-style-type: none"> <li>• DLP-A25 BNC コネクタを使用した同軸ケーブルの取り付け (p.17-33)</li> <li>• DLP-A26 高密度 BNC コネクタを使用した同軸ケーブルの取り付け (p.17-35)</li> <li>• DLP-A27 SMB コネクタを使用した同軸ケーブルの取り付け (p.17-35)</li> </ul>
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** 現地の規約に従って同軸ケーブルをタイラップするか撚り合わせて、ONS 15454 のいずれかの側面の穴を通してケーブルを配線します。側面開口部のゴムで覆われたエッジが、ケーブルの摩擦を防ぎます。

**ステップ 2** 短いピグテール RG179 を使用して、シェルフアセンブリを終端します。

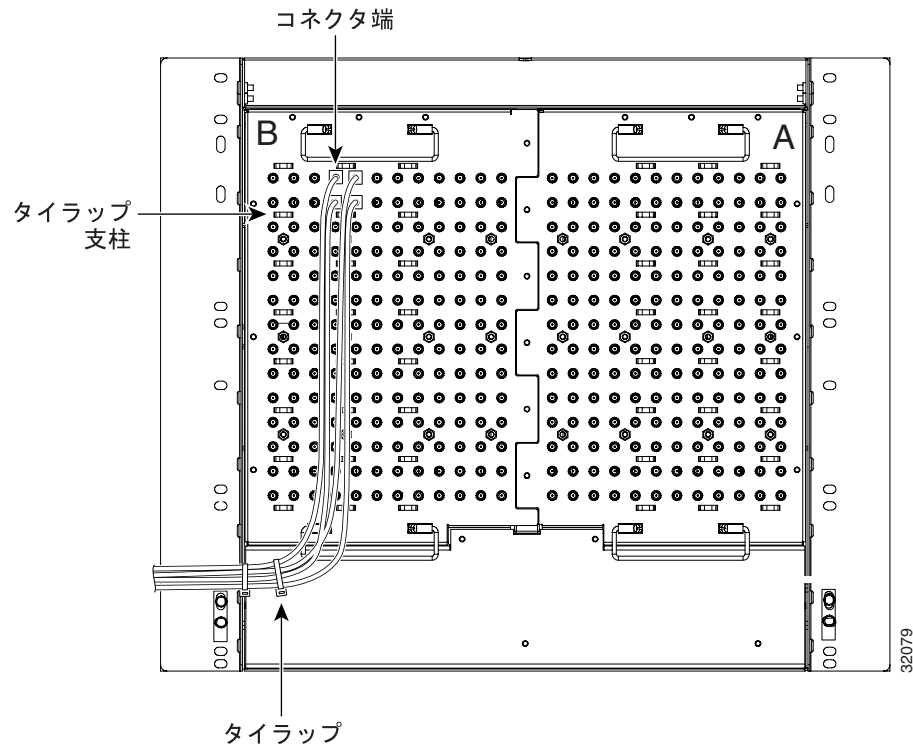
**ステップ 3** RG179 に接続された標準 RG59 (735A) ケーブルを使用して、残りのケーブルを配線します。10 フィート (3.05 m) の RG179 を使用した場合は、最大 437 フィート (133 m) の RG59 (735A) を接続できます。30 フィート (9.1 m) の RG179 を使用した場合は、最大 311 フィート (94.8 m) の RG59 (735A) を接続できます。

RG179 ケーブルを使用した場合の最大距離 (122 フィート、37.2 m) は、標準 RG59 (735A) ケーブルの最大距離 (306 フィート、93.3 m) よりも短くなります。RG59 (734A) ケーブルを使用した場合の最大距離は、450 フィート (137.2 m) です。RG179 の最大距離が短くなるのは、ケーブルが細いために減衰率が大きくなるからです。減衰率の計算には、DS-3 信号を使用します。

- RG179 の減衰率は、22 MHz で 59 dB/kft (dB/キロフィート) です。
- RG59 (735A) の減衰率は、22 MHz で 23 dB/kft です。

計算するときは、ケーブル全体の損失に 5.0 を使用します。図 17-17 に、適切な同軸ケーブル配線例を示します。

図 17-17 同軸ケーブルの配線 (SMB EIA バックプレーン)



**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A29 DS-1 ツイストペア ケーブルの配線

目的	この作業では、DS-1 ツイストペア ケーブルを配線します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A23 電気インターフェイス アダプタ (バラン) を使用した DS-1 ケーブルの取り付け (p.17-29)</a>
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** 次の点を確認します。

- DS-1 ポートのすべての送受信コネクタに、DS-1 電気インターフェイス アダプタが取り付けられている。
- DS-1 電気インターフェイス アダプタのワイヤラップ支柱が、終端された着信ケーブルの接続に使用されている。

**ステップ 2** 現地の規約に従ってツイストペア ケーブルをタイラップするか撚り合わせて、ONS 15454 のいずれかの側面の穴を通してケーブルを配線します。



(注) SMB EIA には、ケーブルをカバー パネルにタイラップしたり、燃り合わせるためのケーブル マネジメント アイレットがあります。

**ステップ 3** 元の NTP (手順) に戻ります。

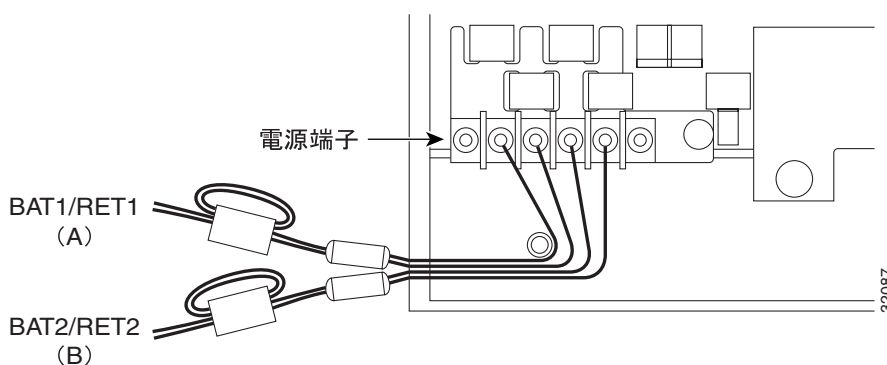
## DLP-A30 電源コードへのフェライトの取り付け

目的	この作業では、電源コードにフェライトを取り付けます。ケーブルペア (BAT1/RET1 [A] および BAT2/RET2 [B]) ごとに、クランプ型フェライト (TDK ZCAT2035-0930) とブロック フェライト (Fair Rite 0443164151) を 1 つずつ使用します。
工具 / 機器	クランプ型フェライトおよびブロック フェライト
事前準備手順	なし
必須 / 適宜	必須
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** ケーブルをブロック フェライトの周りに 1 回巻いてブロック フェライトに通してから、クランプ型フェライトにまっすぐ通します。

**ステップ 2** ONS 15454 とブロック フェライトの間の、電源端子にできるだけ近い位置に、クランプ型フェライトを配置します (図 17-18 を参照)。ブロック フェライトは電源端子の 5 ~ 6 インチ (127 ~ 152 mm) 以内になければなりません。

図 17-18 ブロック フェライトとクランプ型フェライトおよび電源コードの接続



**ステップ 3** 元の NTP (手順) に戻ります。

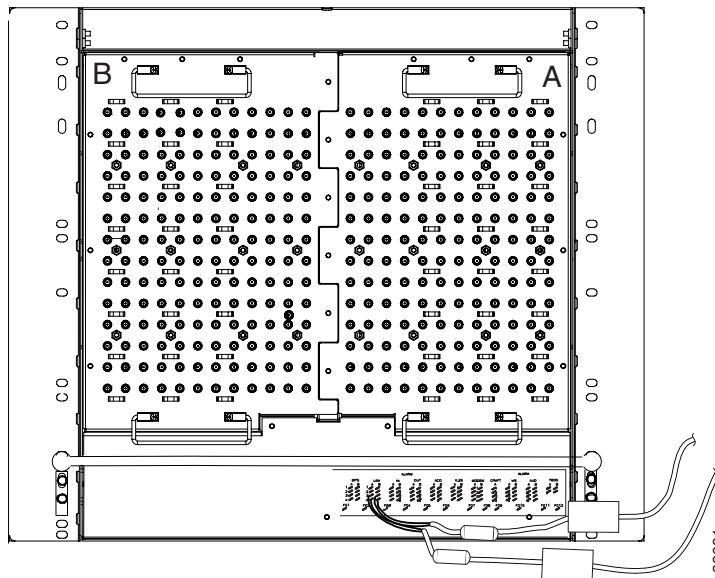
## DLP-A31 ワイヤラップ ピン フィールドへのフェライトの接続

目的	この作業では、ワイヤラップ ピン フィールドにフェライトを接続します。ケーブルペアごとに、クランプ型フェライト (TDK ZCAT1730-0730) とブロック フェライト (Fair Rite 0443164151) を1つずつ使用します。
工具 / 機器	クランプ型フェライトおよびブロック フェライト
事前準備手順	NTP-A8 アラーム、タイミング、LAN、およびクラフト ピン接続のための配線 (p.1-18)
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** ケーブルをブロック フェライトの周りに 1 回巻いてブロック フェライトに通してから、クランプ型フェライトにまっすぐ通します。

**ステップ 2** ONS 15454 とブロック フェライトの間の、ワイヤラップ ピン フィールドにできるだけ近い位置に、クランプ型フェライトを配置します (図 17-19 を参照)。ブロック フェライトはワイヤラップ ピン フィールドの 5 ~ 6 インチ (127 ~ 152 mm) 以内になければなりません。

図 17-19 ワイヤラップ ピン フィールドへのフェライトの接続



**ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A32 シェルフの取り付けおよび接続の検査

目的	この作業では、シェルフの取り付けおよび接続を検査し、すべてが正しく取り付けられ、接続されていることを確認します。
工具 / 機器	なし
事前準備手順	表 1-5 (p.1-32) を行います。
必須 / 適宜	必須
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** 各ワイヤおよびケーブル接続を調べ、すべてのケーブルがしっかりと固定されていることを確認します。ワイヤまたはケーブルが緩んでいる場合は、該当する取り付け手順に戻って直します。
- ステップ 2** バックプレーンが正しく装着されているか調べるには、ネジ穴とバックプレーン インターフェイスカードの穴が正しく合っていること、および A コネクタと B コネクタがかみ合っていることを確認します。
- ステップ 3** 元の NTP (手順) に戻ります。
- 

## DLP-A33 電圧の測定

目的	この作業では、電力を測定して正しい電源およびリターンであることを確認します。
工具 / 機器	電圧計
事前準備手順	表 1-5 (p.1-32) の作業を行います。
必須 / 適宜	必須
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** 電圧計を使用して、オフィス アースおよび電源を確認します。図 17-10 に電源端子を示します。
- ブラックの線 (プラス) を、ベイのフレーム アースに接続します。ステップ b が完了するまでそのままにします。
  - レッドの線 (マイナス) を、ヒューズ電源ポイントおよびアラームパネルに接続し、 $-40.5 \sim -57$  VDC (電源) または 0 (リターン アース) となることを確認します。
- ステップ 2** 電圧計を使用して、シェルフ アースおよび電源の配線を確認します。
- ブラックの線 (プラス) を RET1 に、レッドの線を BAT1 ポイントに接続します。 $-40.5 \sim -57$  VDC になることを確認します。電圧が存在しない場合は、次の点を調べ、必要に応じて修正します。
    - バッテリーおよびアースがシェルフに逆方向に流れていないか。
    - バッテリーが開いていたり、なくなっていたりしないか。
    - リターンが開いていたり、なくなっていたりしないか。

- b. B 電源装置が装備されている場合は、RET2 および BAT2 について、[ステップ 2](#) を繰り返します。

**ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A34 最適化 1+1 保護グループの作成

目的	この作業では、OC3-4 および OC3-8 カードの最適化 1+1 保護グループを作成します。
工具 / 機器	取り付けられた OC3-4 カード、OC3-8 カード、または事前にプロビジョニングされたスロット
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜。この機能を使用する前に、ネットワーク管理者に問い合わせてください。
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** [表 4-1 \(p.4-12\)](#) に示す、最適化 1+1 の要件に応じたカードが取り付けられていることを確認します。

**ステップ 2** 最適化 1+1 保護グループをプロビジョニングする OC3-4 または OC3-8 カードの該当するポートごとに、ポート タイプを SONET から SDH に変更します。

- ノード ビューで、該当するカードをダブルクリックします。
- Provisioning > Line タブをクリックします。
- ポートの横にある Type カラムのドロップダウン リストから SDH を選択して、Apply をクリックします。

**ステップ 3** ノード ビューで、Provisioning > Protection タブをクリックします。

**ステップ 4** Protection Groups 領域で、Create をクリックします。

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

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字 (a ~ z、A ~ Z、0 ~ 9) を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符 (?)、バックスラッシュ (\)、二重引用符 (") は使用しないでください。
- Type — ドロップダウン リストから 1+1 Optimized を選択します。
- Protect Card — ドロップダウン リストから保護ポートを選択します。ドロップダウン リストには、使用可能な OC3-4 または OC3-8 ポートが表示されます。OC3-4 または OC3-8 カードが取り付けられていないと、ドロップダウン リストにポートは表示されません。

保護カードを選択すると、保護に使用できるカードのリストが Available Ports リストに表示されます ([図 17-33](#) を参照)。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「[DLP-A330 カード スロットの事前プロビジョニング \(p.20-22\)](#)」を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

**ステップ 6** Available Ports リストから、Protect Port フィールドで選択したポートで保護するポートを選択します。上にある矢印ボタンをクリックして、各ポートを Working Ports リストに移動します。

**ステップ 7** 残りのフィールドを次のように設定します。

- Reversion time — Revertive をオンにした場合に、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。復元時間は、プライマリ チャネルがセカンダリに、セカンダリ チャネルがプライマリに自動変更されるまでの経過時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。
- Verification guard time — ドロップダウン リストから検証ガード時間を選択します。指定できる範囲は 500 ミリ秒 ~ 1 秒です。検証ガード タイマーは、遠端ノードからの強制切り替えコマンドを受け入れるように設定する場合に使用します。強制コマンドの着信時に、ロックアウトが存在しない場合、またはセカンダリ セクションに障害が発生していない場合は、発信 K1 バイトが強制を示すように変更され、検証ガード タイマーが開始します。検証ガード タイマーの有効期限内に、遠端側で強制切り替えコマンドが受け入れられない場合は、強制コマンドがクリアされます。
- Recovery guard time — ドロップダウン リストから回復ガード時間を選択します。指定できる範囲は 0 ~ 10 秒です。デフォルトは 1 秒です。回復ガード タイマーは、Signal Degrade (SD; 信号劣化) または Signal Failure (SF; 信号障害) が原因で発生する短時間での切り替えを防止する場合に使用します。回線の SD/SF 障害がクリアされると、回復ガード タイマーが開始します。回復ガード時間は、SD/SF 障害が検出されてから、状態がクリアされたとシステムが宣言するまでの経過時間です。
- Detection guard time — ドロップダウン リストから検出ガード時間を選択します。指定できる範囲は 0 ~ 5 秒です。デフォルトは 1 秒です。検出ガード タイマーは、SD、SF、Loss of Signal (LOS; 信号損失)、Loss of Frame (LOF; フレーム損失)、Alarm Indication Signal - Line (AIS-L) 障害が検出されると開始します。検出ガード時間は、アクティブカードで SD、SF、LOS、LOF、AIS-L 障害が検出されてから、スタンバイカードにトラフィックが切り替わるまでの経過時間です。

**ステップ 8** OK をクリックします。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A35 最適化 1+1 保護グループの変更

目的	この作業では、OC3-4 および OC3-8 カードの最適化 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-A34 最適化 1+1 保護グループの作成 (p.17-42) 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 > Protection タブをクリックします。

**ステップ 2** Protection Groups 領域で、変更する最適化 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、ここに新しい名前を入力します。保護グループの名前は、32 文字までの英数字で指定できます。

- Reversion time — Revertive をオンにした場合に、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。復元時間は、プライマリ チャンネルがセカンダリに、セカンダリ チャンネルがプライマリに自動変更されるまでの経過時間です。
- Verification guard time — ドロップダウン リストから検証ガード時間を選択します。指定できる範囲は 500 ミリ秒 ~ 1 秒です。検証ガード タイマーは、遠端ノードからの強制切り替えコマンドを受け入れるように設定する場合に使用します。強制コマンドの着信時に、ロックアウトが存在しない場合、またはセカンダリ セクションに障害が発生していない場合は、発信 K1 バイトが強制を示すように変更され、検証ガード タイマーが開始します。検証ガード タイマーの有効期限内に、遠端側で強制ユーザ コマンドが受け入れられない場合は、強制コマンドがクリアされます。
- Recovery guard time — ドロップダウン リストから回復ガード時間を選択します。指定できる範囲は 0 ~ 10 秒です。デフォルトは 1 秒です。回復ガード タイマーは、SD または SF 障害が原因で発生する短時間での切り替えを防止する場合に使用します。回線の SD/SF 障害がクリアされると、回復ガード タイマーが開始します。回復ガード時間は、SD/SF 障害が検出されてから、状態がクリアされたとシステムが宣言するまでの経過時間です。
- Detection guard time — ドロップダウン リストから検出ガード時間を選択します。指定できる範囲は 0 ~ 5 秒です。デフォルト値は 1 秒です。検出ガード タイマーは、SD、SF、LOS、LOF、または AIS-L 障害が検出されると開始します。検出ガード時間は、アクティブ カードで SD、SF、LOS、LOF、AIS-L 障害が検出されてから、スタンバイ カードにトラフィックが切り替わるまでの経過時間です。

**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。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A36 TCC2/TCC2P カードの取り付け

目的	この作業では、冗長 TCC2/TCC2P カードを取り付けます。ONS 15454 に取り付ける最初のカードは、TCC2/TCC2P カードでなければなりません。他のクロスコネク トカードやトラフィック カードを取り付ける前に、この TCC2/TCC2P カードを初期化しておく必要があります。
工具 / 機器	TCC2/TCC2P カード (2)
事前準備手順	なし
必須 / 適宜	必須
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)** カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

**ステップ 1** 取り付ける TCC2/TCC2P カードのラッチまたはイジェクタを開きます。

**ステップ 2** ラッチまたはイジェクタを使用して、ガイドレールに沿ってカードをスライドさせ、スロット (スロット 7 または 11) の後ろのレセプタクルにカードを確実に取り付けます。

**ステップ 3** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。





(注) カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクトが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

**ステップ 4** TCC2 カードの場合は、ステップ a を実行して LED の動作を確認します。TCC2P カードの場合は、ステップ b を実行します。

**a. TCC2 カードの場合**

- すべての LED が短時間点灯します。レッドの FAIL LED とイエローの ACT/STBY LED が約 15 秒間点灯します。
- レッドの FAIL LED とグリーン of ACT/STBY LED が約 40 秒間点灯します。
- レッドの FAIL LED が約 15 秒間点滅します。
- レッドの FAIL LED が約 15 秒間点灯します。すべての LED が約 3 秒間点灯してから、3 秒間消灯します。
- グリーンの 2 つの PWR LED がともに 10 秒間点灯します。その後、その PWR LED は 2 ~ 3 分間レッドに変わってから、グリーンになります。
- PWR LED が 2 ~ 3 分間レッドになっているあいだ、ACT/STBY、MJ、および MN LED が点灯し、その後 SNYC LED が点灯します。
- PWR LED がグリーンになり、ACT/STBY が点灯したままになると、ブート処理が完了です (最初の TCC2 カードを取り付ける場合、ACT/STBY LED はグリーンで、2 枚目の TCC2 カードを取り付ける場合はオレンジに点灯します)。



(注) A 電源アラームと B 電源アラームがクリアされるまでに、最大 4 分かかる場合があります。



(注) アラーム LED が点灯することがありますが、Cisco Transport Controller (CTC) にログインしてアラームタブを表示できるようになるまでは、アラーム LED を無視してください。



(注) CTC にログインしている場合は、TCC2 カードの初期化中に SFTWDOWN アラームが 2 回表示されます。このアラームは、カードのブートが完了するとクリアされます。



(注) FAIL LED が連続して点灯する場合は、TCC2 カードの自動アップロードと関係している可能性があります。ステップ 8 のヒントを参照してください。

**b. TCC2P カードの場合**

- すべての LED が短時間点灯します。レッドの FAIL LED、イエローの ACT/STBY LED、グリーン of SYNC LED、およびグリーン of ACO LED が約 15 秒間点灯します。
- レッドの FAIL LED とグリーン of ACT/STBY LED が約 30 秒間点灯します。

- レッドの FAIL LED が約 3 秒間点滅します。
- レッドの FAIL LED が約 15 秒間点灯します。
- レッドの FAIL LED が約 10 秒間点滅してから点灯します。
- すべての LED (CRIT、MAJ、MIN、REM、SYNC、および ACO LED を含む) が一度点滅してから、約 5 秒間消灯します。
- グリーンの 2 つの PWR LED がともに 10 秒間点灯します。その後、その PWR LED は 2 ~ 3 分間レッドに変わってから、グリーンになります。この間、ACT/STBY、MJ、および MN LED が点灯し、その後 SNYC LED が短時間点灯する場合があります。
- PWR LED がグリーンになり、イエローの ACT/STBY が点灯したままになると、ブート処理が完了です (最初の TCC2P カードを取り付ける場合、ACT/STBY LED はグリーンで、2 枚目の TCC2P カードを取り付ける場合はイエローに点灯します)。



(注) A 電源アラームと B 電源アラームがクリアされるまでに、最大 3 分かかる場合があります。



(注) アラーム LED が点灯することがありますが、CTC にログインしてアラーム タブを表示できるようにするまでは、アラーム LED を無視してください。



(注) CTC にログインしている場合は、TCC2P カードの初期化中に SFTWDOWN アラームが 2 回表示されます。このアラームは、カードのブートが完了するとクリアされます。



(注) FAIL LED が連続して点灯する場合は、TCC2P カードの自動アップロードと関係している可能性があります。ステップ 8 のヒントを参照してください。

**ステップ 5** TCC2/TCC2P カードの ACT/STBY LED を見て、そのカードが最初に電源を入れたカードであれば、LED の色がグリーン (アクティブ) になっていることを確認します。また、そのカードが 2 番めに電源を入れたカードであれば、LED の色がイエロー (スタンバイ) になっていることを確認します。IP アドレス、ノードの温度、および日時が LCD に表示されます。デフォルトの日付と時刻は、1970 年 1 月 1 日 12:00 AM です。

**ステップ 6** LCD に、IP アドレス (デフォルトは 192.1.0.2)、ノード名、およびソフトウェアバージョンが順番に繰り返されて表示されます。正しいソフトウェアバージョンが LCD に表示されていることを確認します。ソフトウェアの文字列は、ノードタイプ (SDH または SONET) およびソフトウェアリリースを示しています (たとえば、SDH 07.00-05L-20.10 は、SDH ソフトウェア ロード、Release 7.00 であることを示しています。リリース番号の後ろの数字には、特に意味はありません)。

**ステップ 7** LCD に正しいソフトウェアバージョンが表示されている場合は、ステップ 8 へ進みます。LCD に正しいソフトウェアバージョンが表示されていない場合は、ソフトウェアをアップグレードするか、または TCC2/TCC2P カードを取り外して交換用カードを取り付けてください。

ソフトウェアを交換する場合は、そのリリース専用のソフトウェア アップグレード マニュアルを参照してください。TCC2/TCC2P カードを交換するには、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 8** 冗長 TCC2/TCC2P カードに対してステップ 1 ~ 7 を繰り返します。



**ヒント**

アクティブ カードとソフトウェア バージョンの異なるスタンバイ TCC2/TCC2P カードを取り付けると、新たに取り付けたそのスタンバイ TCC2/TCC2P カードにアクティブ TCC2/TCC2P カードのソフトウェア バージョンが自動的にコピーされます。この場合、特に作業を行う必要はありませんが、TCC2/TCC2P カードをロードしても通常の方法ではブートされません。スタンバイ カードを最初に挿入したとき、LED は**ステップ 4** に示す順序にほぼ従って動作します。ただし、レッドの FAIL LED が約 5 秒間点灯したあと、新しいソフトウェアをアクティブ TCC2/TCC2P カード上でロードしている間、FAIL LED と ACT/STBY LED が最大 30 分間交互に点滅を始めます。新しいソフトウェアをロードしたあと、アップグレードされた TCC2/TCC2P カードの LED が **ステップ 4** の順序を繰り返し、オレンジの ACT/STBY LED が点灯します。



**(注)**

別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。



**(注)**

アラーム LED が点灯することがありますが、CTC にログインしてアラーム タブを表示できるようにするまでは、アラーム LED を無視してください。

**ステップ 9** ACT/STBY LED がスタンバイを示すオレンジになっていることを確認します。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け

目的	この作業では、クロスコネク (XCVT/XC10G/XC-VXC-10G) カードを取り付けます。
工具 / 機器	XCVT/XC10G/XC-VXC-10G (クロスコネク) カード
事前準備手順	<a href="#">DLP-A36 TCC2/TCC2P カードの取り付け (p.17-44)</a>
必須 / 適宜	必須
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)**

クロスコネク カードをアップグレードする場合は、この手順を使用しないでください。XCVT カードを XC10G カードに、または XC10G カードを XC-VXC-10G カードにアップグレードする場合は、[第 12 章「カードとスパンのアップグレード」](#)を参照してください。



**(注)**

カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

- ステップ 1** 取り付ける 1 つめの XCVT、XC10G、または XC-VXC-10G カードのラッチまたはイジェクタを開きます。
- ステップ 2** ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをスライドさせ、スロット (スロット 8 または 10) の後ろのレセプタクルにカードを確実に取り付けます。
- ステップ 3** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



(注) カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

**ステップ 4** LED の動作を確認します。

- レッドの FAIL LED が 20 ~ 30 秒間点灯します。
- レッドの FAIL LED が 35 ~ 45 秒間点滅します。
- レッドの FAIL LED が 5 ~ 10 秒間点灯します。
- すべての LED が一度点滅してから点灯します。
- ACT/STBY LED が点灯します。



(注) 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。



(注) レッドの FAIL LED が点灯しない場合は、電源を調べてください。



(注) レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 1 ~ 4 を繰り返してください。

**ステップ 5** ACT/STBY LED がアクティブを示すグリーンになっていることを確認します。

**ステップ 6** ラッチまたはイジェクタを使用して、ガイド レールに沿って 2 つめのクロスコネクタ カードをスライドさせ、スロット (スロット 8 または 10) の後ろのレセプタクルにカードを確実に取り付けます。

**ステップ 7** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



(注) カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

**ステップ 8** LED の動作を確認します。

- レッドの FAIL LED が 20 ~ 30 秒間点灯します。
- レッドの FAIL LED が 35 ~ 45 秒間点滅します。
- レッドの FAIL LED が 5 ~ 10 秒間点灯します。
- すべての LED が一度点滅してから点灯します。
- ACT/STBY LED が点灯します。



(注) 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。



(注) レッドの FAIL LED が点灯しない場合は、電源を調べてください。



(注) レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 6 ~ 8 をやり直してください。

**ステップ 9** ACT/STBY LED がスタンバイを示すオレンジになっていることを確認します。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A39 イーサネットカードの取り付け

目的	この作業では、イーサネットカード (E100T-12、E100T-G、E1000-2、E1000-2-G、G1K-4、ML100T-12、ML1000-2、ML100X-8、CE-100T-8、および CE-1000-4) を取り付けます。
工具 / 機器	イーサネットカード
事前準備手順	<a href="#">NTP-A15 共通コントロールカードの取り付け (p.2-2)</a>
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** カードのラッチまたはイジェクタを開きます。

**ステップ 2** ラッチまたはイジェクタを使用して、ガイド レールに沿ってカードをしっかりとスライドさせ、スロットの後方のレセプタクルにカードを取り付けます。

**ステップ 3** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



(注) カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが開まる場合があります。カードをそれ以上挿入できないことを確かめてください。

**ステップ 4** LED の動作を確認します。

- レッドの FAIL LED が 20 ~ 30 秒間点灯します。
- レッドの FAIL LED が 35 ~ 45 秒間点滅します。
- すべての LED が一度点滅してから、1 ~ 5 秒間消灯します。
- ACT または ACT/STBY LED が点灯します。SF LED は、すべてのカードポートがそれぞれの遠端の相手先に接続されて、信号が発生するまで点灯し続けます。



(注) レッドの FAIL LED が点灯しない場合は、電源を調べてください。



(注) 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A41 AIC-I カードの取り付け

目的	この作業では、AIC-I カードを取り付けます。AIC-I カードは、外部アラームおよび制御 (環境アラーム) の接続に使用します。
工具 / 機器	AIC-I カード
事前準備手順	<a href="#">DLP-A36 TCC2/TCC2P カードの取り付け (p.17-44)</a> <a href="#">DLP-A37 XCVT、XCI0G、または XC-VXC-10G カードの取り付け (p.17-47)</a>
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) カードを取り付ける場合は、各カードのブートが完了してから、次のカードを取り付けてください。

**ステップ 1** カードのラッチまたはイジェクタを開きます。

**ステップ 2** ラッチまたはイジェクタを使用して、ガイドレールに沿ってカードをスライドさせ、スロット (スロット 9) の後ろのレセプタクルにカードを確実に取り付けます。

**ステップ 3** カードが正しく挿入されていることを確認して、カードのラッチまたはイジェクタを閉めます。



**(注)** カードがバックプレーンに完全に取り付けられていない状態でも、ラッチまたはイジェクタが閉まる場合があります。カードをそれ以上挿入できないことを確かめてください。

**ステップ 4** 次の点を確認します。

- レッドの FAIL LED が 1 秒間点灯したあと、1 ~ 5 秒間点滅します。
- PWR A LED と PWR B LED がレッドになり、2 つの INPUT/OUTPUT LED が約 3 秒間グリーンになります。
- PWR A LED がグリーンになってから、INPUT/OUTPUT LED が消灯し、次に ACT LED が点灯します。レッドの FAIL LED が点灯しない場合は、電源を調べてください。



**(注)** PWR A LED と PWR B LED が更新されるまでに、最大 3 分かかる場合があります。



**(注)** 別のカード用にプロビジョニングされたスロットにカードを挿入すると、すべての LED が消灯します。



**(注)** レッドの FAIL LED が連続して点灯する場合や、LED の動作が異常な場合は、カードが正しく取り付けられていません。カードを取り外して、ステップ 1 ~ 4 を繰り返してください。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A43 UPSR 構成での光ファイバケーブルの取り付け

目的	この作業では、各ノードのイーストおよびウエスト Unidirectional Path Switched Ring (UPSR; 単方向バススイッチ型リング) ポートに光ファイバケーブルを接続します。UPSR 構成のプロビジョニングとテストについては、 <a href="#">第 5 章「ネットワークの起動」</a> を参照してください。
工具 / 機器	光ファイバケーブル
事前準備手順	<a href="#">NTP-A112 ファイバコネクタの清掃 (p.15-20)</a>
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)

間違いを防止するために、右端のポートをイーストポートとし、左端のポートをウェストポートとして、光ファイバケーブルを接続します。あるノードのイーストポートに接続されたファイバは、隣接ノードのウェストポートに接続する必要があります。



注意

UPSR のイーストポートとウェストポートは、同じ OC-N カードにプロビジョニングしないでください。

- ステップ 1** ファイバ接続計画を立てます。すべての UPSR ノードに対して同じ計画を使用します。
- ステップ 2** ファイバをあるノードの OC-N カードの送信 (Tx) コネクタに接続し、もう一方の端を隣接ノードの OC-N カードの受信 (Rx) コネクタに接続します。送信用のファイバと受信用のファイバが一致していない (1 本のファイバが、あるカードの受信ポートと他のカードの受信ポートを接続している、あるいは送信ポートで同様の状況になっている) と、カードの SF LED が点灯します。
- ステップ 3** リングの構成が完了するまで、**ステップ 2** を繰り返します。

図 17-20 に、スロット 5 (ウェスト) とスロット 12 (イースト) にトランク (スパン) カードを備えた、4 ノード UPSR のファイバ接続を示します。

図 17-20 4 ノード UPSR へのファイバ接続

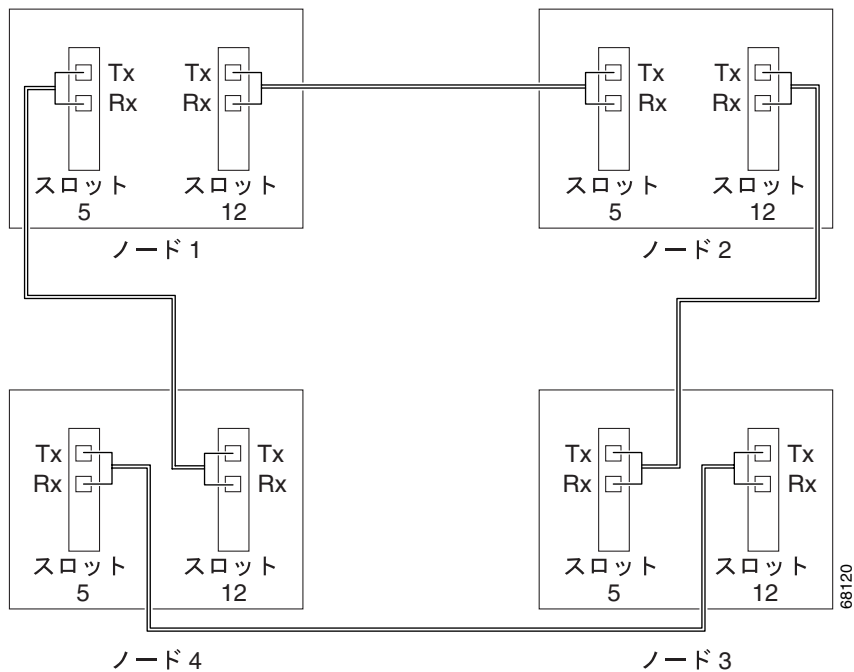
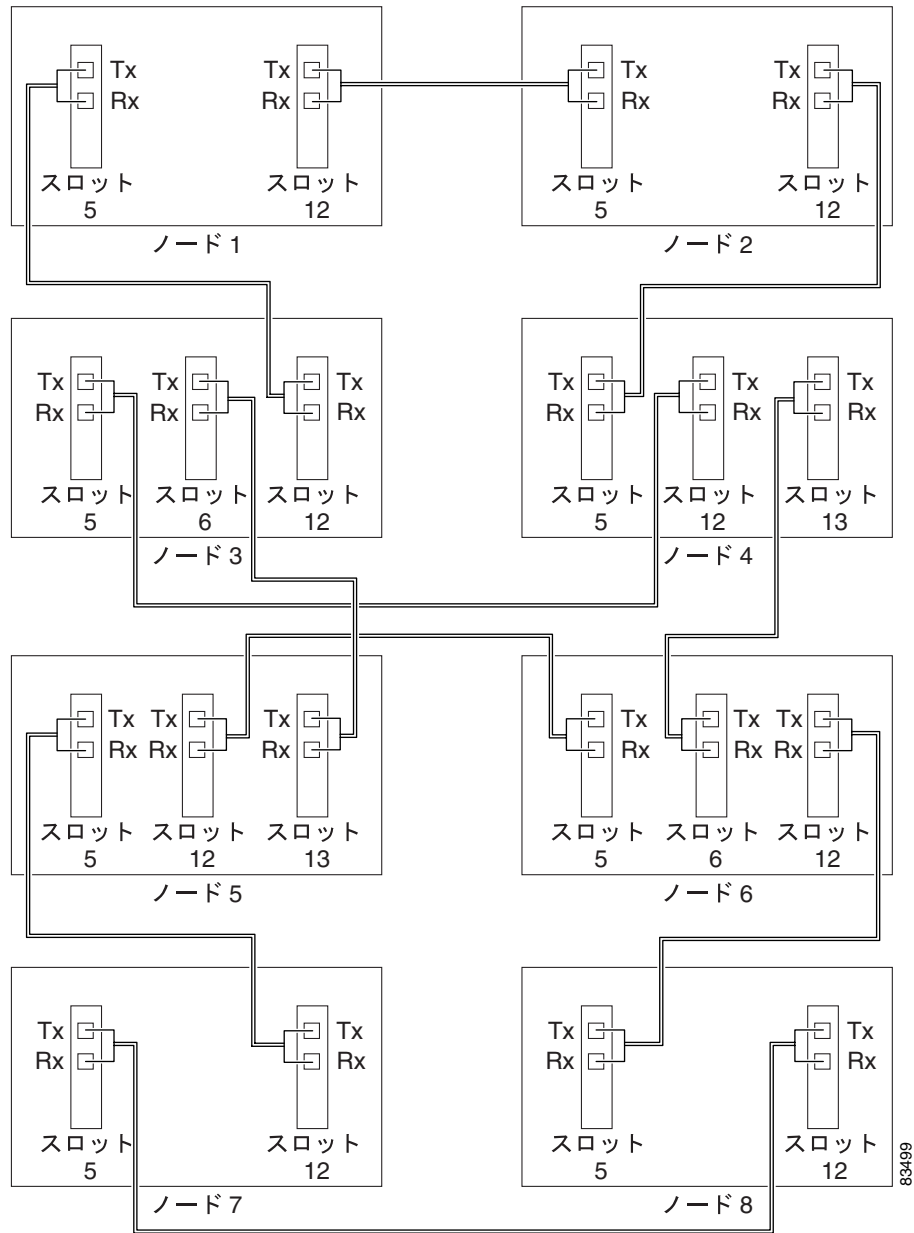




図 17-21 に、従来型 UPSR Dual-Ring Interconnect (DRI; デュアルリング相互接続) の例を示します。

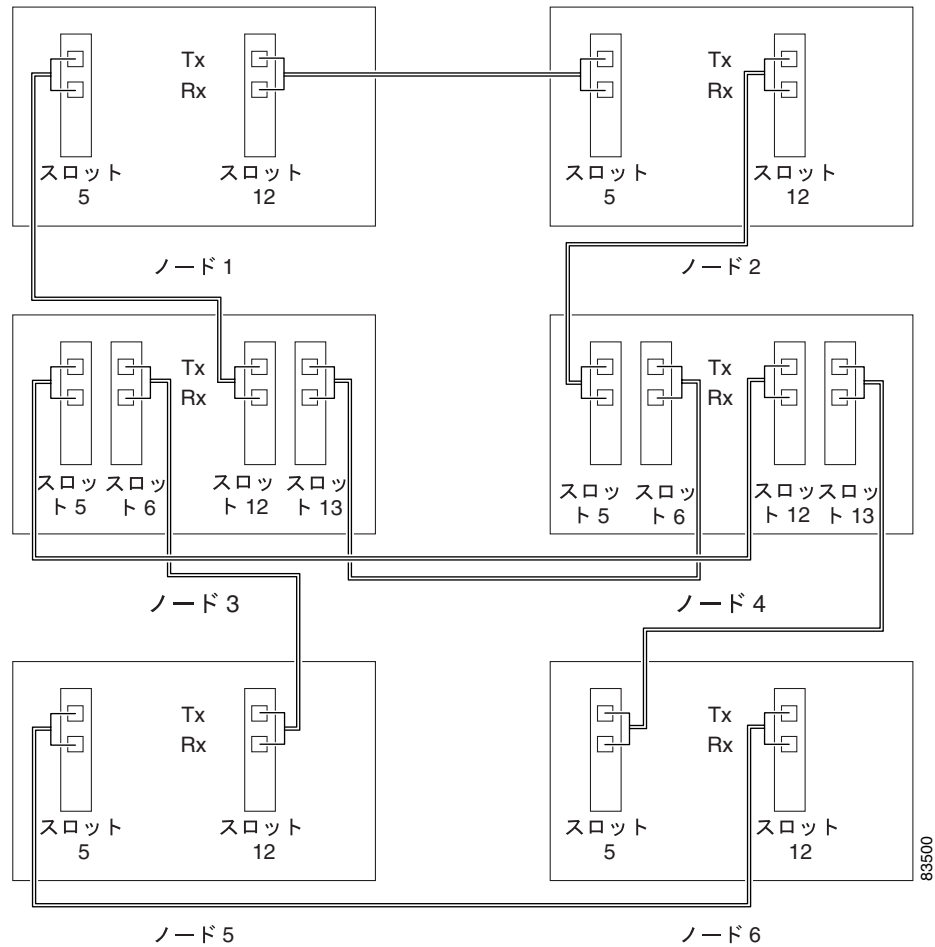
図 17-21 8 ノードの従来型 UPSR DRI へのファイバ接続



83499

図 17-22 に、統合 DRI の例を示します。

図 17-22 6 ノードの統合 UPSR DRI へのファイバ接続



**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A44 BLSR 構成での光ファイバケーブルの取り付け

目的	この作業では、各ノードのイーストおよびウェスト Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) ポートに光ファイバケーブルを接続します。BLSR 構成のプロビジョニングとテストについては、 <a href="#">第 5 章「ネットワークの起動」</a> を参照してください。
工具 / 機器	光ファイバケーブル
事前準備手順	<a href="#">NTP-A112 ファイバ コネクタの清掃 (p.15-20)</a>
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)

間違いを防止するために、右端のスロットをイーストポートとし、左端のスロットをウェストポートとして、光ファイバケーブルを接続します。あるノードのイーストポートに接続されたファイバは、隣接ノードのウェストポートに接続する必要があります。



注意

BLSR のイーストポートとウェストポートは、同じ OC-N カードにプロビジョニングしないでください。

**ステップ 1** ファイバ接続計画を立てます。すべての BLSR ノードに対して同じ計画を使用します。

**ステップ 2** ファイバをあるノードの OC-N カードの送信 (Tx) コネクタに接続し、もう一方の端を隣接ノードの OC-N カードの受信 (Rx) コネクタに接続します。送信用のファイバと受信用のファイバが一致していないと、カードの SF LED が点灯します。



(注)

4 ファイバ BLSR を接続する場合は、現用カードと保護カードの接続を混在させないでください。現用カードと保護カードが相互接続されていると、BLSR は機能しません。4 ファイバ BLSR の正しいケーブル接続の例については、[図 17-24](#)を参照してください。

**ステップ 3** リングの構成が完了するまで、[ステップ 2](#)を繰り返します。

[図 17-23](#)に、スロット 5 (ウェスト) とスロット 12 (イースト) にトランク (スパン) カードを備えた、2 ファイバ BLSR のファイバ接続を示します。

図 17-23 4 ノード、2 ファイバ BLSR でのファイバ接続

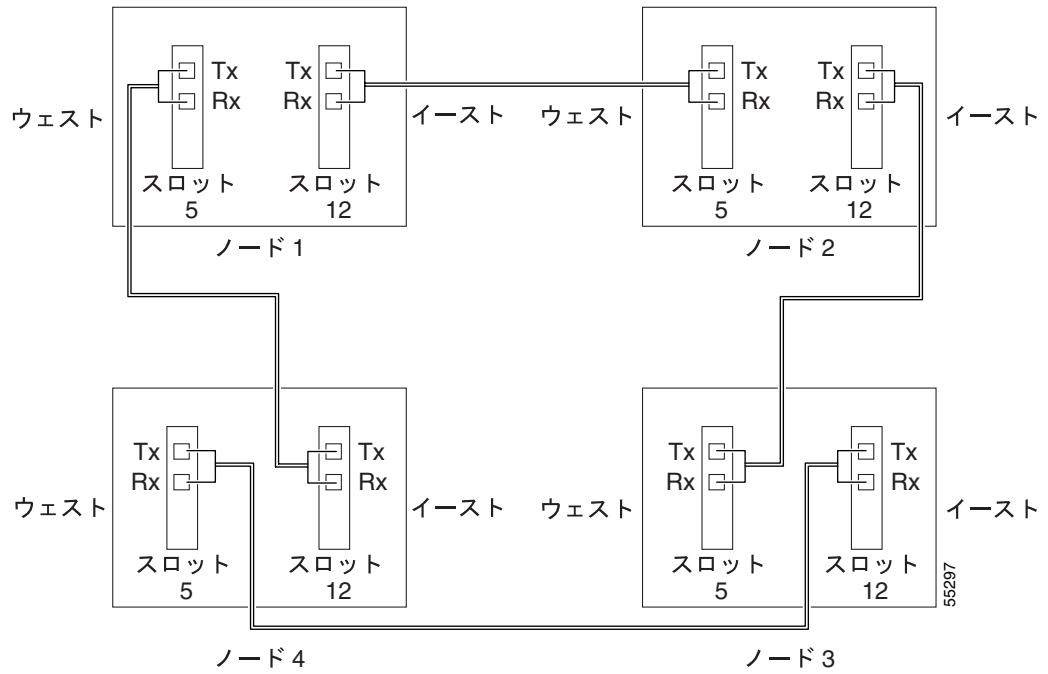
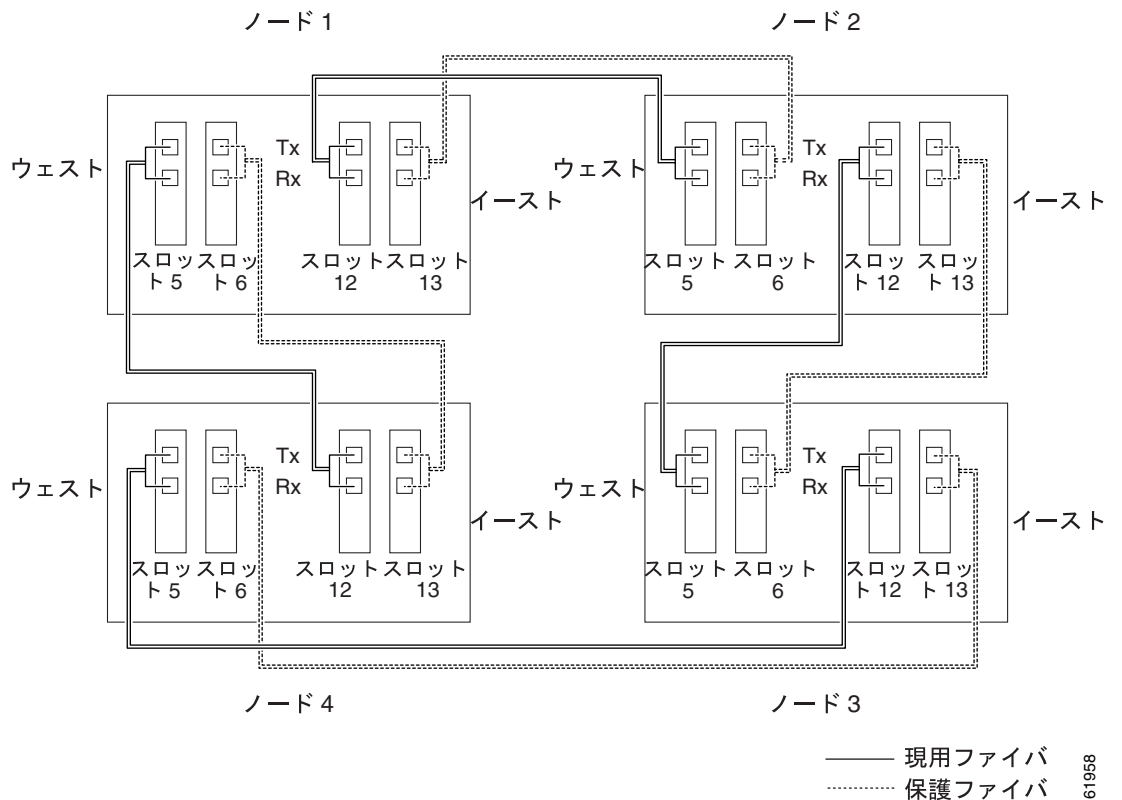


図 17-24 に、4 ファイバ BLSR のファイバ接続を示します。スロット 5 (ウェスト) とスロット 12 (イースト) は現用トラフィックを伝送します。スロット 6 (ウェスト) とスロット 13 (イースト) は保護トラフィックを伝送します。

図 17-24 4 ノード、4 ファイバ BLSR でのファイバ接続



**ステップ 4** 元の NTP（手順）に戻ります。

## DLP-A45 ファイバブーツの取り付け

目的	この作業では、ファイバが屈曲し過ぎないように保護するファイバブーツを取り付けます。OC-192、OC192-XFP、および OC-48 AS カードでは、角度の付いた SC コネクタを使用しているためブーツは必要ありませんが、これらを除くすべての OC-N カードに、ファイバブーツが必要です。
工具 / 機器	ファイバブーツ
事前準備手順	<a href="#">NTP-A16 光カードおよびコネクタの取り付け (p.2-8)</a>
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)** 光ファイバケーブルを OC-N カードに取り付ける前、または取り付けたあとに、光ファイバケーブルにファイバブーツを取り付けることができます。

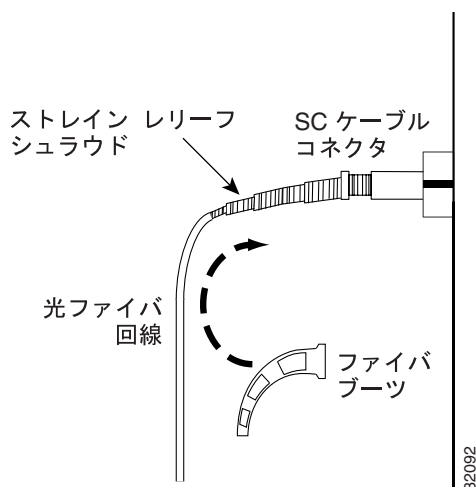


**(注)** OC3IR/STM1SH 1310-8 カードを取り付ける場合は、ポート 8 の Rx ファイバ コネクタに、ファイバブーツの代わりにファイバクリップを使用する必要があります。

**ステップ 1** 光ファイバケーブルの下にファイバブーツの開いたスロットを位置合わせします。

**ステップ 2** 光ファイバケーブルをファイバブーツに押し込みます。図 17-25 にファイバブーツの取り付けを示します。

図 17-25 ファイバブーツの取り付け



32092

- ステップ 3** ファイバブーツをひねって、光ファイバケーブルをファイバブーツの末端に固定します。
- ステップ 4** 光ファイバケーブルに沿ってファイバブーツを前方にスライドさせて、SC ケーブル コネクタの端にファイバブーツをぴったりとはめ込みます。
- ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A50 スタティック IP アドレスを使用して同一サブネット上の ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、次のような場合に ONS 15454 にローカル クラフト接続するようにコンピュータを設定します。
	<ul style="list-style-type: none"> <li>• Software Release 3.3 より前のソフトウェア リリースが稼働するノードにアクセスする。</li> <li>• 1 つの ONS 15454 に接続する。複数の ONS 15454 に接続する場合は、ONS 15454 へ接続するたびにコンピュータの IP を設定しなければならぬことがあります。</li> <li>• ONS 15454 には備わっていないアプリケーション (ping や tracert [トレースルート] など) を使用する必要がある。</li> </ul>
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
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** コンピュータにインストールされている OS (オペレーティング システム) を確認してください。
- Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
  - [ コントロール パネル ] ウィンドウ内の [ システム ] アイコンをダブルクリックします。
  - [ システム設定 ] ウィンドウの [ 全般 ] タブで、Windows OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。
- ステップ 2** コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。
- Windows 98 の場合は、[ステップ 3](#) を実行します。
  - Windows NT 4.0 の場合は、[ステップ 4](#) を実行します。
  - Windows 2000 の場合は、[ステップ 5](#) を実行します。
  - Windows XP の場合は、[ステップ 6](#) を実行します。
- ステップ 3** PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。
- Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
  - [ コントロール パネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。

- c. [ ネットワーク ] ダイアログボックスで、使用している NIC カード用の TCP/IP を選択し、[ プロパティ ] をクリックします。
- d. [ TCP/IP のプロパティ ] ダイアログボックスで、[ DNS 設定 ] タブをクリックし、[ DNS を使わない ] を選択します。
- e. [ WINS 設定 ] タブをクリックし、[ WINS の解決をしない ] を選択します。
- f. [ IP アドレス ] タブをクリックします。
- g. [ IP アドレス ] ウィンドウ内の [ IP アドレスを指定 ] をクリックします。
- h. [ IP アドレス ] フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ~ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。
- i. [ サブネット マスク ] フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは 255.255.255.0 (24 ビット) です。
- j. [ OK ] をクリックします。
- k. [TCP/IP] ダイアログボックス内で [ ゲートウェイ ] タブをクリックします。
- l. [ 新しいゲートウェイ ] フィールドに ONS 15454 の IP アドレスを入力します。[ 追加 ] をクリックします。
- m. その IP アドレスが [ インストールされているゲートウェイ ] フィールドに表示されていることを確認してから [ OK ] をクリックします。
- n. PC を再起動するよう求めるプロンプトが表示されたら、[ はい ] をクリックします。

**ステップ 4** PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
- b. [ コントロール パネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。
- c. [ ネットワーク ] ダイアログボックスで、[ プロトコル ] タブをクリックし、[ TCP/IP のプロトコル ] を選択してから [ プロパティ ] をクリックします。
- d. [ IP アドレス ] タブをクリックします。
- e. [ IP アドレス ] ウィンドウ内の [ IP アドレスを指定 ] をクリックします。
- f. [ IP アドレス ] フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ~ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。
- g. [ サブネット マスク ] フィールドに 255.255.255.0 と入力します。
- h. [ 詳細 ] をクリックします。
- i. [ ゲートウェイ ] で [ 追加 ] をクリックします。[ TCP/IP ゲートウェイ アドレス ] ダイアログボックスが表示されます。
- j. [ ゲートウェイ アドレス ] フィールドに ONS 15454 の IP アドレスを入力します。
- k. [ 追加 ] をクリックします。
- l. [ OK ] をクリックします。
- m. [ 適用 ] をクリックします。
- n. Windows NT 4.0 では、PC をリブートするよう求めるプロンプトが表示される場合があります。このプロンプトが表示されたら、[ はい ] をクリックします。

**ステップ 5** PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ ネットワークとダイヤルアップ接続 ] > [ ローカル エリア接続 ] の順に選択します。
- b. [ ローカル エリア接続の状態 ] ダイアログボックス内の [ プロパティ ] をクリックします。
- c. [ 全般 ] タブで、[ インターネット プロトコル (TCP/IP) ] を選択し、[ プロパティ ] をクリックします。
- d. [ 次の IP アドレスを使う ] をクリックします。
- e. [ IP アドレス ] フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ~ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。
- f. [ サブネット マスク ] フィールドに 255.255.255.0 と入力します。
- g. [ デフォルト ゲートウェイ ] フィールドに ONS 15454 の IP アドレスを入力します。
- h. [ OK ] をクリックします。
- i. [ ローカル エリア接続のプロパティ ] ダイアログボックス内で [ OK ] をクリックします。
- j. [ ローカル エリア接続の状態 ] ダイアログボックス内で [ 閉じる ] をクリックします。

**ステップ 6** PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ コントロール パネル ] > [ ネットワーク接続 ] の順に選択します。



**(注)** [ ネットワーク接続 ] メニューが有効になっていない場合は、[ クラシック表示に切り替える ] をクリックします。

- b. [ ネットワーク接続 ] ダイアログボックス内の [ ローカル エリア接続 ] アイコンをクリックします。
- c. [ ローカル エリア接続のプロパティ ] ダイアログボックスで、[ インターネット プロトコル (TCP/IP) ] を選択し、[ プロパティ ] をクリックします。
- d. [ IP アドレス ] フィールドに、最後のオクテットを除いて ONS 15454 の IP アドレスと同じ IP アドレスを入力します。最後のオクテットは、1 または 3 ~ 254 の値にする必要があります。ノードをプロビジョニングしているときに LCD の表示を無効にしていなければ、その LCD にこの IP アドレスが表示されます。
- e. [ サブネット マスク ] フィールドに 255.255.255.0 と入力します。
- f. [ デフォルト ゲートウェイ ] フィールドに ONS 15454 の IP アドレスを入力します。
- g. [ OK ] をクリックします。
- h. [ ローカル エリア接続のプロパティ ] ダイアログボックス内で [ OK ] をクリックします。
- i. [ ローカル エリア接続の状態 ] ダイアログボックス内で [ 閉じる ] をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。



## DLP-A51 DHCP を使用して ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、Dynamic Host Configuration Protocol (DHCP) を使用して ONS 15454 へクラフト接続するようにコンピュータを設定します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a> <a href="#">NTP-A169 CTC ネットワーク アクセスの設定 (p.4-9)</a>
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)

最初のノードを立ち上げるときには、この作業を使用しないでください。この作業は、ONS 15454 で DHCP フォワーディングがイネーブルになっている場合にだけ使用してください。デフォルトでは、DHCP がディセーブルになっています。イネーブルにする場合は、「[NTP-A169 CTC ネットワーク アクセスの設定](#)」(p.4-9) を参照してください。



(注)

ONS 15454 からは IP アドレスが提供されません。DHCP フォワーディングをイネーブルにすると、ONS 15454 は DHCP の要求を外部 DHCP サーバに送ります。

- ステップ 1** コンピュータにインストールされている OS を確認してください。
- Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
  - [ コントロール パネル ] ウィンドウ内の [ システム ] アイコンをダブルクリックします。
  - [ システム設定 ] ウィンドウの [ 全般 ] タブで、Windows OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。
- ステップ 2** コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。
- Windows 98 の場合は、[ステップ 3](#) を実行します。
  - Windows NT 4.0 の場合は、[ステップ 4](#) を実行します。
  - Windows 2000 の場合は、[ステップ 5](#) を実行します。
  - Windows XP の場合は、[ステップ 6](#) を実行します。
- ステップ 3** PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。
- Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
  - [ コントロール パネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。
  - [ ネットワーク ] ダイアログボックスで、使用している NIC 用の TCP/IP を選択し、[ プロパティ ] をクリックします。
  - [ TCP/IP のプロパティ ] ダイアログボックスで、[ DNS 設定 ] タブをクリックし、[ DNS を使わない ] を選択します。

- e. [ WINS 設定 ] タブをクリックし、[ WINS の解決をしない ] を選択します。
- f. [ IP アドレス ] タブをクリックします。
- g. [ IP アドレス ] ウィンドウ内の [ IP アドレスを自動的に取得 ] をクリックします。
- h. [ OK ] をクリックします。
- i. PC を再起動するよう求めるプロンプトが表示されたら、[ はい ] をクリックします。

**ステップ 4** PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロールパネル ] の順に選択します。
- b. [ コントロールパネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。
- c. [ ネットワーク ] ダイアログボックスで、[ プロトコル ] タブをクリックし、[ TCP/IP のプロトコル ] を選択してから [ プロパティ ] をクリックします。
- d. [ IP アドレス ] タブをクリックします。
- e. [ IP アドレス ] ウィンドウ内の [ DHCP サーバから IP アドレスを取得する ] をクリックします。
- f. [ OK ] をクリックします。
- g. [ 適用 ] をクリックします。
- h. Windows により PC を再起動するよう求めるプロンプトが表示されたら、[ はい ] をクリックします。

**ステップ 5** PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ ネットワークとダイヤルアップ接続 ] > [ ローカル エリア接続 ] の順に選択します。
- b. [ ローカル エリア接続の状態 ] ダイアログボックス内の [ プロパティ ] をクリックします。
- c. [ 全般 ] タブで、[ インターネット プロトコル (TCP/IP) ] を選択し、[ プロパティ ] をクリックします。
- d. [ DHCP サーバから IP アドレスを取得する ] をクリックします。
- e. [ OK ] をクリックします。
- f. [ ローカル エリア接続のプロパティ ] ダイアログボックス内で [ OK ] をクリックします。
- g. [ ローカル エリア接続の状態 ] ダイアログボックス内で [ 閉じる ] をクリックします。

**ステップ 6** PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ コントロールパネル ] > [ ネットワーク接続 ] の順に選択します。



(注) [ ネットワーク接続 ] メニューが有効になっていない場合は、[ クラシック表示に切り替える ] をクリックします。

- b. [ ネットワーク接続 ] ダイアログボックス内の [ ローカル エリア接続 ] をクリックします。
- c. [ ローカル エリア接続の状態 ] ダイアログボックス内の [ プロパティ ] をクリックします。

- d. [全般] タブで、[インターネット プロトコル (TCP/IP)] を選択し、[プロパティ] をクリックします。
- e. [DHCP サーバから IP アドレスを取得する] をクリックします。
- f. [OK] をクリックします。
- g. [ローカル エリア接続のプロパティ] ダイアログボックス内で [OK] をクリックします。
- h. [ローカル エリア接続の状態] ダイアログボックス内で [閉じる] をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A52 自動ホスト検出を使用して ONS 15454 にクラフト接続するための Windows PC の設定

目的	この作業では、次のような場合に ONS 15454 にローカル クラフト接続するようにコンピュータを設定します。 <ul style="list-style-type: none"> <li>• ONS 15454 イーサネット ポートまたは バックプレーン ピンに直接接続するか、ハブを介して接続する。</li> <li>• アクセスするすべてのノードで、Software Release 3.3 以降が実行されている。</li> <li>• 複数の ONS 15454 に接続し、接続のたびに毎回 IP アドレスを再設定しなくてもよいようにしたい。</li> <li>• ONS 15454 には備わっていないアプリケーション (ping や tracert [トレースルート] など) へアクセスする必要がない。</li> </ul>
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
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** コンピュータにインストールされている OS を確認してください。

- a. Windows の [スタート] メニューから、[設定] > [コントロール パネル] の順に選択します。



**(注)** Windows XP の場合は、[スタート] メニューから直接 [コントロール パネル] を選択できます。クラシック表示になっていることを確認した上で、この手順を実行してください。

- b. [コントロール パネル] ウィンドウ内の [システム] アイコンをダブルクリックします。
- c. [システム設定] ウィンドウの [全般] タブで、Windows OS が Windows 98、Windows NT 4.0、Windows 2000、または Windows XP のいずれかであることを確認します。

**ステップ 2** コンピュータにインストールされている Windows の OS に応じて、次のステップのいずれかを実行してください。

- Windows 98 の場合は、[ステップ 3](#) を実行します。

- Windows NT 4.0 の場合は、**ステップ 4** を実行します。
- Windows 2000 の場合は、**ステップ 5** を実行します。
- Windows XP の場合は、**ステップ 6** を実行します。

**ステップ 3** PC に Windows 98 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
- b. [ コントロール パネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。
- c. [ ネットワーク ] ダイアログボックスで、使用している NIC 用の TCP/IP を選択し、[ プロパティ ] をクリックします。
- d. [ TCP/IP のプロパティ ] ダイアログボックスで、[ DNS 設定 ] タブをクリックし、[ DNS を使わない ] を選択します。
- e. [ WINS 設定 ] タブをクリックし、[ WINS の解決をしない ] を選択します。
- f. [ IP アドレス ] タブをクリックします。
- g. [ IP アドレス ] ウィンドウ内の [ IP アドレスを指定 ] をクリックします。
- h. [ IP アドレス ] フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。
- i. [ サブネット マスク ] フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは 255.255.255.0 (24 ビット) です。
- j. [ OK ] をクリックします。
- k. [ TCP/IP ] ダイアログボックス内で [ ゲートウェイ ] タブをクリックします。
- l. [ 新しいゲートウェイ ] フィールドに、ステップ h で指定したアドレスを入力します。[ 追加 ] をクリックします。
- m. その IP アドレスが [ インストールされているゲートウェイ ] フィールドに表示されていることを確認してから [ OK ] をクリックします。
- n. PC を再起動するよう求めるプロンプトが表示されたら、[ はい ] をクリックします。

**ステップ 4** PC に Windows NT 4.0 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。
- b. [ コントロール パネル ] ダイアログボックス内で [ ネットワーク ] アイコンをクリックします。
- c. [ ネットワーク ] ダイアログボックスで、[ プロトコル ] タブをクリックし、[ TCP/IP のプロトコル ] を選択してから [ プロパティ ] をクリックします。
- d. [ IP アドレス ] タブをクリックします。
- e. [ IP アドレス ] ウィンドウ内の [ IP アドレスを指定 ] をクリックします。
- f. [ IP アドレス ] フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。
- g. [ サブネット マスク ] フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは 255.255.255.0 (24 ビット) です。
- h. [ 詳細 ] をクリックします。
- i. [ ゲートウェイ ] で [ 追加 ] をクリックします。[ TCP/IP ゲートウェイ アドレス ] ダイアログボックスが表示されます。
- j. ステップ f で指定した IP アドレスを [ ゲートウェイ アドレス ] フィールドに入力します。
- k. [ 追加 ] をクリックします。
- l. [ OK ] をクリックします。

- m. [適用] をクリックします。
- n. PC をリブートします。

**ステップ 5** PC に Windows 2000 がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [スタート] メニューから、[設定] > [ネットワークとダイヤルアップ接続] > [ローカル エリア接続] の順に選択します。
- b. [ローカル エリア接続の状態] ダイアログボックス内の [プロパティ] をクリックします。
- c. [全般] タブで、[インターネット プロトコル (TCP/IP)] を選択し、[プロパティ] をクリックします。
- d. [次の IP アドレスを使う] をクリックします。
- e. [IP アドレス] フィールドに、ノード IP アドレスとは別の正規の IP アドレスを入力します。
- f. [サブネット マスク] フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは 255.255.255.0 (24 ビット) です。
- g. ステップ e で指定した IP アドレスを [ゲートウェイ アドレス] フィールドに入力します。
- h. [OK] をクリックします。
- i. [ローカル エリア接続のプロパティ] ダイアログボックス内で [OK] をクリックします。
- j. [ローカル エリア接続の状態] ダイアログボックス内で [閉じる] をクリックします。

**ステップ 6** PC に Windows XP がインストールされている場合は、次のステップを実行して TCP/IP の設定を変更してください。

- a. Windows の [スタート] メニューから、[コントロール パネル] > [ネットワーク接続] の順に選択します。



(注) [ネットワーク接続] メニューが有効になっていない場合は、[クラシック表示に切り替える] をクリックします。

- b. [ネットワーク接続] ダイアログボックス内の [ローカル エリア接続] アイコンをクリックして選択します。右クリックして [プロパティ] を選択します。
- c. [ローカル エリア接続のプロパティ] ダイアログボックスで、[インターネット プロトコル (TCP/IP)] をクリックして選択し、[プロパティ] をクリックします。
- d. [IP アドレス] フィールドに、ONS 15454 の LCD で示されているように、ノード IP アドレスとは別の正規の IP アドレスを入力します。デフォルトの IP アドレスは 192.1.0.2 です。
- e. [サブネット マスク] フィールドに、ONS 15454 と同じサブネット マスクを入力します。デフォルトは 255.255.255.0 (24 ビット) です。
- f. ステップ d で指定した IP アドレスを [ゲートウェイ アドレス] フィールドに入力します。
- g. [OK] をクリックします。
- h. [ローカル エリア接続のプロパティ] ダイアログボックス内で [OK] をクリックします。
- i. [ローカル エリア接続の状態] ダイアログボックス内で [閉じる] をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A53 ONS 15454 にクラフト接続するための Solaris ワークステーションの設定

目的	この作業では、ONS 15454 ヘクラフト接続するように Solaris ワークステーションを設定します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
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** root ユーザとしてワークステーションにログインします。

**ステップ 2** 次のように入力して、インターフェイスがプログラミングされていることを確認します。

```
# ifconfig device
```

たとえば、次のようになります。

```
# ifconfig hme1
```

インターフェイスがプログラミングされている場合は、次のようなメッセージが表示されます。

```
hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0
netmask 0
```

このようなメッセージが表示されたら、[ステップ 4](#) へ進みます。

インターフェイスがプログラミングされていない場合は、次のようなメッセージが表示されます。

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

このようなメッセージが表示されたら、[ステップ 3](#) へ進みます。

**ステップ 3** 次のように入力して、インターフェイスをプログラミングします。

```
# ifconfig device plumb
```

たとえば、次のようになります。

```
# ifconfig hme1 plumb
```

**ステップ 4** 次のように入力して、インターフェイス上に IP アドレスを設定します。

```
# ifconfig interface ip-address netmask netmask up
```

たとえば、次のように入力します。

```
# ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up
```



**(注)** ONS 15454 の IP アドレスと同じ IP アドレスを入力します(ただし、最後のオクテットを除く)。最後のオクテットは必ず 1 または 3 ~ 254 でなければなりません。

**ステップ 5** Subnet Mask フィールドに **255.255.255.0** と入力します。Provisioning > Network > General > Gateway Settings タブを順にクリックして Craft Access Only をオンにした場合は、このステップを省略してください。

**ステップ 6** 接続をテストします。

- a. Netscape Navigator を起動します。
- b. Web アドレス (URL) のフィールドに ONS 15454 の IP アドレスを入力します。接続が確立されると、Java Console ウィンドウ、CTC キャッシング メッセージ、および Cisco Transport Controller Login ダイアログボックスが表示されます。このあと、「[DLP-A60 CTC へのログイン](#)」(p.17-71)のステップ 2 へ進んでログインを実行します。Login ダイアログボックスが表示されない場合は、ステップ c と d を実行してください。
- c. プロンプトが表示されたら、次のように入力します。

```
ping ONS-15454-IP-address
```

たとえば、デフォルト IP アドレスの 192.1.0.2 を使用した ONS 15454 に接続する場合は、次のように入力します。

```
ping 192.1.0.2
```

ワークステーションが ONS 15454 に接続されている場合は、次のようなメッセージが表示されます。

```
IP-address is alive
```



**(注)** Provisioning > Network > General > Gateway Settings タブを順にクリックして Craft Access Only チェックボックスをオンにした場合は、このステップを省略してください。

- d. CTC からの応答がない場合は、[Request timed out] (Windows の場合) メッセージまたは [no answer from x.x.x.x] (UNIX の場合) メッセージが表示されます。IP とサブネット マスクに関する情報を確認します。ワークステーションと ONS 15454 との間を接続しているケーブルが確実に取り付けられていることを確認します。次のように入力して、リンクの状態を確認します。

```
# ndd -set/dev/device instance 0
```

```
# ndd -get/dev/device link_status
```

たとえば、次のようになります。

```
# ndd -set/dev/hme instance 0
```

```
# ndd -get/dev/hme link_status
```

結果が「1」の場合は、このリンクがアップしています。結果が「0」の場合は、このリンクがダウンしています。



**(注)** ndd については、マニュアル ページを確認してください。たとえば、次のように入力します。# `man ndd`.

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A54 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、物理的に取り外すことなく 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



注意

---

ハードリセットを行うと、トラフィックが中断します。

---



(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 OOS-MA,MT 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 メニューをクリックして、**OOS-MT,MA** 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。CTC 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、ポップアップ 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-A56 Internet Explorer によるプロキシ サービスのディセーブル化 (Windows)

目的	この作業では、Internet Explorer を実行している PC に対してプロキシ サービスをディセーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
必須 / 適宜	コンピュータがネットワーク コンピュータのプロキシ サーバに接続されており、かつブラウザが Internet Explorer である場合は必須
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

**ステップ 1** Windows の [ スタート ] メニューから、[ 設定 ] > [ コントロール パネル ] の順に選択します。



**(注)** コンピュータが Windows XP を実行している場合は、[ スタート ] メニューから直接コントロール パネルを選択できます。クラシック表示になっていることを確認した上で、この手順を実行してください。

**ステップ 2** [ コントロール パネル ] ウィンドウから、[ インターネット オプション ] を選択します。

**ステップ 3** [ インターネットのプロパティ ] ダイアログボックスで、[ 接続 ] > [ LAN の設定 ] の順にクリックします。

**ステップ 4** [ ローカル エリア ネットワーク (LAN) の設定 ] ダイアログボックスで、次のいずれかを実行します。

- [ LAN にプロキシ サーバを使用する ] をオフにして、このサービスをディセーブルにします。
- [ LAN にプロキシ サーバを使用する ] をオンのままにして、[ 詳細設定 ] をクリックします。[ プロキシの設定 ] ダイアログボックスの [ 例外 ] の下に、アクセスする ONS 15454 ノードの IP アドレスを入力します。アドレスの間はセミコロンで区切ります。ホスト番号にアスタリスク (\*) を入れると、ネットワーク上のすべての ONS 15454 ノードを含めることができます。[ OK ] をクリックして、開いた状態の各ダイアログボックスを閉じます。



**(注)** TCC2P カードが取り付けられた ONS 15454 ノードで、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。ノードがセキュア モードで、コンフィギュレーションがロックされている場合、Cisco Technical Support によりロックがディセーブル化されない限り、IP アドレスを変更できません。セキュア モードの詳細については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A57 Netscape によるプロキシ サービスのディセーブル化 (Windows および UNIX)

目的	この作業では、Netscape を実行している PC と UNIX ワークステーションに対してプロキシ サービスをディセーブルにします。コンピュータがネットワーク コンピュータのプロキシ サーバに接続されており、かつブラウザが Netscape である場合は、この作業を実行する必要があります。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A260 CTC 用コンピュータのセットアップ (p.3-2)</a>
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

**ステップ 1** Netscape を開きます。

**ステップ 2** [編集] メニューから [設定] を選択します。

**ステップ 3** [設定] ダイアログボックスのカテゴリの中で、[詳細] > [プロキシ] の順に選択します。

**ステップ 4** [設定] ダイアログボックスの右側の、[プロキシ] の下で、次のいずれかを実行します。

- [インターネットに直接接続する] を選択して、プロキシ サーバをバイパスします。
- [手動でプロキシを設定する] を選択し、プロキシ サーバに例外を追加してから [表示] をクリックします。[手動でプロキシを設定] ダイアログボックスの [例外] の下に、アクセスする ONS 15454 ノードの IP アドレスを入力します。アドレスの間はカンマで区切ります。[OK] をクリックして、開いた状態の各ダイアログボックスを閉じます。



**(注)** TCC2P カードが取り付けられた ONS 15454 ノードで、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。ノードがセキュア モードで、コンフィギュレーションがロックされている場合、Cisco Technical Support によりロックがディセーブル化されない限り、IP アドレスを変更できません。セキュア モードの詳細については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A60 CTC へのログイン

目的	この作業では、ユーザーが CTC にログインします。
工具 / 機器	なし
事前準備手順	NTP-A260 CTC 用コンピュータのセットアップ (p.3-2) 次の手順のいずれか <ul style="list-style-type: none"> <li>• NTP-A234 ONS 15454 へローカルにクラフト接続するための CTC コンピュータのセットアップ (p.3-4)</li> <li>• NTP-A235 ONS 15454 に社内 LAN で接続するための CTC コンピュータのセットアップ (p.3-6)</li> <li>• NTP-A236 ONS 15454 へのリモート アクセス接続のセットアップ (p.3-7)</li> </ul>
必須 / 適宜	必須
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)

CTC のビューとナビゲーションについては、付録 A「CTC の情報およびショートカット」を参照してください。

**ステップ 1** ONS 15454 に接続されているコンピュータから Netscape (PC または UNIX の場合) または Internet Explorer (PC の場合のみ) を起動します。

- PC を使用している場合は、Windows の [ スタート ] メニューまたはショートカット アイコンから Netscape または Internet Explorer を起動します。
- UNIX を使用している場合は、コマンドラインに次のように入力して Netscape を起動します。
  - Netscape を使用するための Netscape の色をインストールするには、次のように入力します。

```
# netscape -install
```
  - Netscape の色を 32 色に制限して、希望の色が利用できない場合に Netscape に最も近い色を選択させるには、次のように入力します。

```
netscape -ncols 32
```



(注)

CTC が正常に動作するには、24 色フルカラー パレットが必要です。UNIX 版の Netscape のように色の種類が重要なアプリケーションでは、CTC を使用するには色が足りない可能性があります。-install または -ncols 32 のコマンドライン オプションにより、Netscape が使用する色の数を制限できます。

**ステップ 2** Netscape または Internet Explorer の Web アドレス (URL) フィールドに、ONS 15454 の IP アドレスを入力します。初期設定の場合、デフォルトの IP アドレスは 192.1.0.2 です。この IP アドレスは LCD に表示されます。CTC を使用すれば LCD の IP アドレスを非表示にできます。詳細については、「DLP-A266 IP 設定の変更」(p.19-57) を参照してください。Enter キーを押します。



(注) ログインしようとしている ONS 15454 ノードの CTC ソフトウェアにリリースの異なるものがある場合は、最新のリリースを実行しているノードにログインしてください。以前のリリースを実行しているノードにログインすると、新しいリリースを実行している各ノードで INCOMPATIBLE-SW アラームが発生し、CTC でそれらのノードを管理できなくなります。ノードのソフトウェアバージョンを確認するには、CTC Help メニューから About CTC を選択します。このようにすれば、ネットワークビューに表示されている各ノードで ONS 15454 のソフトウェアバージョンが表示されます。表示されていないノードについては、LCD ディスプレイの表示で調べられます。アラームの解決については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

Java Plug-in Security Warning ダイアログボックスが表示されたら、「[DLP-A418 公開鍵セキュリティ証明書のインストール](#)」(p.21-5)を実行して、Software Release 4.1 以降で必要となる公開鍵のセキュリティ証明書をインストールしてください。

セキュリティ証明書ダイアログボックスでの操作が終了すると(または証明書がすでにインストールされている場合は) Java Console ウィンドウに CTC ファイルのダウンロード ステータスが表示されます。Web ブラウザには、使用している Java の環境とシステムの環境に関する情報が表示されます。今回のログインが初めての場合は、コンピュータへ CTC のファイルがダウンロードされているときに CTC のキャッシング メッセージが表示されます。ONS 15454 に初めて接続する場合は、この処理に数分かかることがあります。ダウンロードが終了すると、CTC Login ダイアログボックス(図 17-26)が表示されます。

図 17-26 CTC へのログイン



**ステップ 3** Login ダイアログボックスにユーザ名とパスワード(いずれも大文字と小文字を区別する)を入力します。初めて設定する場合は、ユーザ名として CISCO15 を入力し、パスワードとして otbu+1 を入力してください。



(注) すべての ONS 15454 に ユーザ CISCO15 が設定されています。ユーザ CISCO15 にはスーパーユーザの権限があるので、他のユーザを作成できます。ユーザ CISCO15 を削除する場合は、その前に別のスーパーユーザを作成する必要があります。ユーザ CISCO15 には otbu+1 というパスワードが付与されています。ユーザ CISCO15 のパスワードを変更する場合は、ログインしたあとに Provisioning > Security タブを順にクリックしてから、パスワードを変更します。ONS 15454 のユーザを設定してセキュリティを割り当てる場合は、「[NTP-A30 ユーザの作成とセキュリティの割り当て](#)」(p.4-5)へ進みます。セキュリティの詳細については、『Cisco ONS 15454 Reference Manual』にある「Security」の章を参照してください。

**ステップ 4** ONS 15454 にログインするたびに、次のようなログイン オプションを選択できます。

- Node Name — Web ブラウザに入力した IP アドレスとともに、以前に入力した ONS 15454 の IP アドレスがドロップダウン リスト形式で表示されます。リストにあるいずれかの ONS 15454 をログイン用に選択するか、または新しくログインするノードの IP アドレス（またはノード名）を入力できます。
- Additional Nodes — 現在のログイン ノードグループをリストで表示します。ログイン ノードグループの作成方法と新規グループの追加方法については、「[DLP-A61 ログイン ノードグループの作成](#)」(p.17-74)を参照してください。
- Disable Network Discovery — このボックスをオンにすると、Node Name フィールドに入力した ONS 15454（および、存在する場合は、ログイン ノードグループ メンバー）だけが表示されます。DCC を介してこのノードにリンクされているノードは検出されないため、CTC のネットワーク ビューに表示されません。このオプションを使用すると、ネットワークに DCC で接続されているノードが多数ある場合の CTC の起動時間を短縮できます。
- Disable Circuit Management — このボックスをオンにすると、既存回線の検出が行われなくなります。このオプションを使用すると、ネットワークに回線が多数存在する場合の CTC の起動時間を短縮して、メモリの消費を削減できます。このオプションによって新規回線の作成と管理が妨害されることはありません。

**ステップ 5** Disable Network Discovery をオフにしておく、CTC はネットワーク検出時につけた最新バージョンの JAR ファイルをダウンロードして、CTC ソフトウェアのアップグレードを試みます。CTC が最新の JAR ファイルをダウンロードすることを許可する場合は Yes、CTC による JAR ファイルのダウンロードを許可しない場合は No をクリックします。



(注) CTC ソフトウェアのアップグレードを行うと、既存のソフトウェアは上書きされます。アップグレードが完了したら、CTC を再起動する必要があります。

**ステップ 6** Login をクリックします。

ログインに成功すると、CTC のウィンドウが表示されます。このウィンドウから、他の CTC ビューに移動して、ONS 15454 のプロビジョニングと管理を行うことができます。初めてシェルフを起動する必要がある場合は、[第 4 章「ノードの起動」](#)を参照してください。また、ログインで問題が発生した場合は、『Cisco ONS 15454 Troubleshooting Guide』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-A61 ログイン ノード グループの作成

目的	この作業では、ログイン ノード グループを作成して、ログイン ノードに DCC ではなく IP で接続している ONS 15454 を表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 Edit メニューから **Preferences** を選択します。
- ステップ 2** **Login Node Group** と **Create Group** をクリックします。
- ステップ 3** Create Login Group Name ダイアログボックスにグループの名前を入力します。OK をクリックします。
- ステップ 4** Members 領域に、このグループに追加するノードの IP アドレス (またはノード名) を入力します。Add をクリックします。グループに追加するノードごとに、このステップを繰り返します。

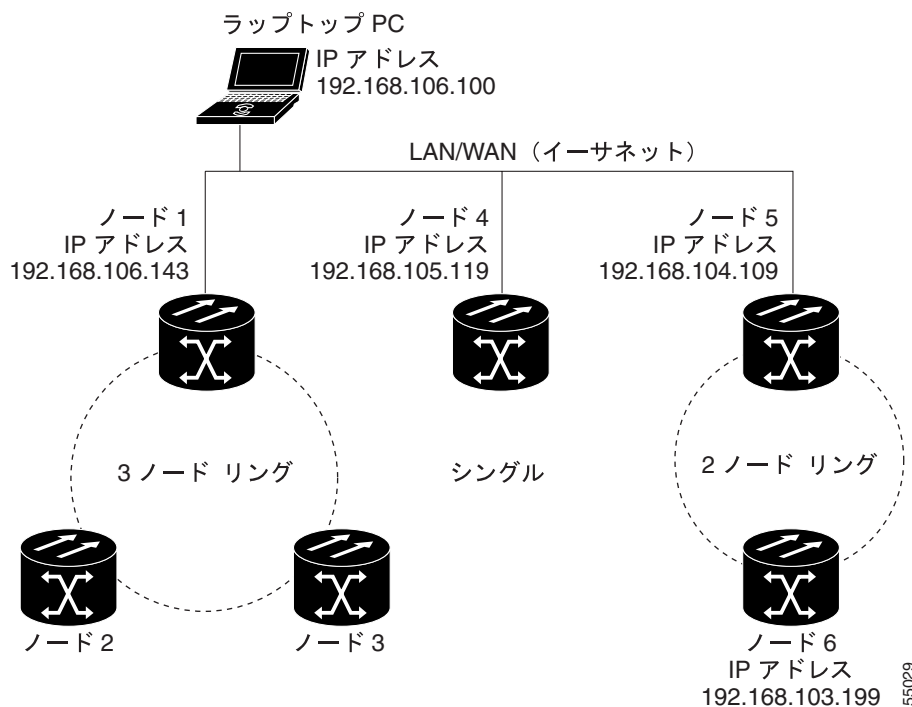


**(注)** ログイン ノード グループに追加する ONS 15454 に TCC2P カードが取り付けられていて、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。ノードがセキュア モードで、コンフィギュレーションがロックされている場合、Cisco Technical Support によりロックがディセーブル化されない限り、IP アドレスを変更できません。セキュア モードの詳細については、『*Cisco ONS 15454 Reference Manual*』の「Management Network Connectivity」の章を参照してください。

- ステップ 5** OK をクリックします。

ONS 15454 へ次回ログインするときに、このログイン ノード グループが Login ダイアログボックスの Additional Nodes リストで利用可能となります。たとえば、[図 17-27](#) では、ノード 1、4、および 5 の IP アドレスを含むログイン ノード グループが作成されます。ログイン時に Additional Nodes リストからこのグループを選択して、Disable Network Discovery を選択しないと、図の中のすべてのノードが表示されます。ログイン グループと Disable Network Discovery を両方とも選択すると、ノード 1、4、および 5 が表示されます。ログイン グループは必要な数だけ作成できます。これらのグループは、CTC のプリファレンス ファイルに保存され、他のユーザに対しては表示されません。

図 17-27 ログイン ノード グループ



**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A62 現在のセッションまたはログイン グループへのノードの追加

目的	この作業では、現在の CTC セッションまたはログイン ノード グループへノードを追加します。
工具	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** CTC File メニューから **Add Node** をクリックします。

**ステップ 2** Add Node ダイアログボックスにノード名 (または IP アドレス) を入力します。

追加する ONS 15454 に TCC2P カードが取り付けられていて、TCC2P のセキュア モード オプションがイネーブルになっている場合は、バックプレーン LAN ポートの IP アドレスを入力します。



(注) ノードがセキュア モードの場合は、バックプレーンの IP アドレス表示がディセーブルになることがあります。スーパーユーザは IP アドレスの表示を再度イネーブルにできます。ノードがセキュア モードで、コンフィギュレーションがロックされている場合、Cisco Technical Support によりロックがディセーブル化されない限り、IP アドレスを変更できません。セキュア モードの詳細については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

**ステップ 3** 現在のログイン グループにノードを追加する場合は、**Add node to current login group** をオンにします。それ以外の場合は、このチェックボックスをオフのままにします。このチェックボックスは、CTC へのログイン時にログイン グループを選択した場合にだけ、アクティブとなります。

**ステップ 4** OK をクリックします。

数秒が経過すると、新規ノードがネットワーク ビュー マップに表示されます。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A64 LCD による IP アドレス、デフォルト ルータ、ネットワーク マスクの設定

目的	この作業では、ファントレイ アセンブリの LCD を使って ONS 15454 の IP アドレス、デフォルト ルータ、およびネットワーク マスクを変更します。この作業は、CTC へログインできない場合に使用します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A36 TCC2/TCC2P カードの取り付け (p.17-44)</a>
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) ノード ビューの Provisioning > Network タブで LCD IP Display が Display Only または Suppress Display に設定されている場合は、この作業を行えません。LCD IP Display フィールドの表示方法と変更方法については、「[DLP-A249 IP 設定のプロビジョニング](#)」(p.19-35)を参照してください。ノードがセキュア モードにロックされ、LCD の表示がディセーブルになっている場合、Cisco Technical Support によりロックがディセーブル化されない限り、このプロビジョニングを変更できません。セキュア モードの詳細については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。



(注) 5 秒間ボタン操作がないと、LCD は通常の表示モードに戻ります。

**ステップ 1** ONS 15454 の前面パネルで、LCD に Node の文字が表示されるまで Slot ボタンを繰り返し押します。

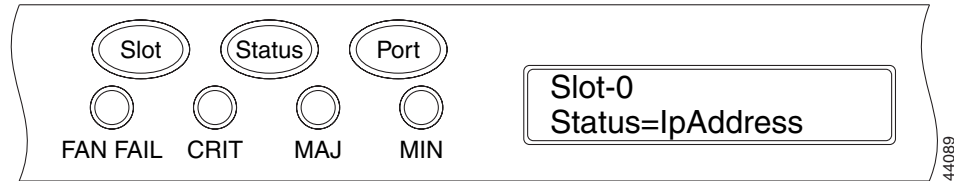
**ステップ 2** 次の表示が現れるまで、Port ボタンを繰り返し押します。

- ノードの IP アドレスを変更する場合は、Status=IpAddress ( [図 17-28](#) )



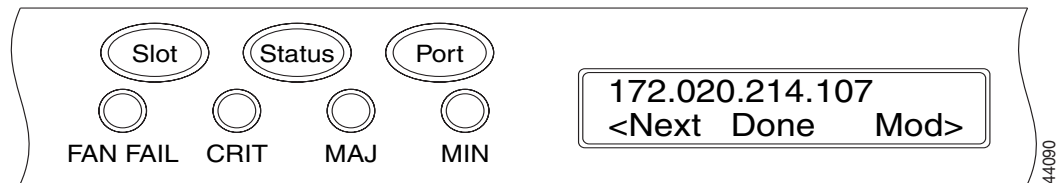
- ノードのネットワークマスクを変更する場合は、Status=Net Mask
- デフォルトルータの IP アドレスを変更する場合は、Status=Default Rtr

図 17-28 IP アドレス オプションの選択



- ステップ 3** Status ボタンを押して、ノードの IP アドレス (図 17-29)、ノードのサブネットマスク長、またはデフォルトルータの IP アドレスを表示します。

図 17-29 IP アドレスの変更



- ステップ 4** Slot ボタンを押して、変更が必要な IP アドレスまたはサブネットマスクの桁に移動します。選択した桁が点滅します。



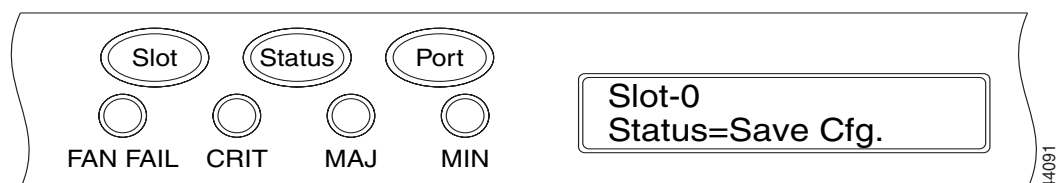
**ヒント** Slot、Status、および Port の各ボタンの位置は、LCD のコマンドの位置に対応しています。たとえば、図 17-29 では、Slot ボタンを押して Next コマンドを呼び出し、Port ボタンを押して Done コマンドを呼び出します。

- ステップ 5** Port ボタンを押して IP アドレスまたはサブネットマスクの該当する桁へ進みます。

- ステップ 6** 変更が完了したら、Status ボタンを押して Node メニューに戻ります。

- ステップ 7** Save Configuration オプションが表示されるまで、Port ボタンを繰り返し押します (図 17-30)。

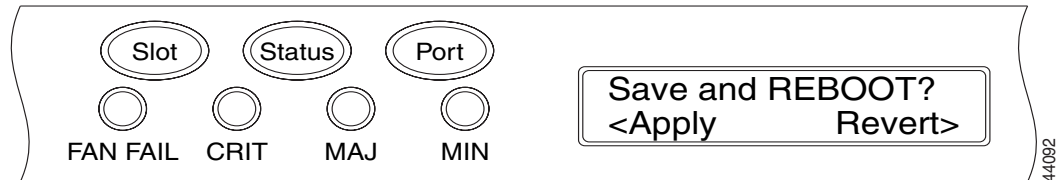
図 17-30 Save Configuration オプションの選択



**ステップ 8** Status ボタンを押して、Save Configuration オプションを選択します。

[Save and REBOOT] というメッセージが表示されます ( 図 17-31 )。

図 17-31 TCC2/TCC2P の保存とリブート



**ステップ 9** Slot ボタンを押して新しい IP アドレス設定を適用するか、Port を押して設定をキャンセルします。

新しい設定を保存すると、TCC2/TCC2P カードがリブートされます。リブート中に、[Saving Changes - TCC Reset] というメッセージが LCD に表示されます。TCC2/TCC2P のリブートが完了すると、LCD は通常の交差表示に戻ります。



**(注)** IP アドレスとデフォルト ルータは、同じサブネット上に設定する必要があります。サブネットが異なる場合は、設定を適用できません。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A65 スタティック ルートの作成

目的	この作業では、別のネットワークにあるコンピュータとの間で CTC 接続を確立するために、スタティック ルートを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	次のいずれかの条件に該当する場合は必須です。 <ul style="list-style-type: none"> <li>• あるサブネット内の CTC コンピュータを、ルータを介して別のサブネット内の ONS 15454 に接続されている ONS 15454 と接続する必要があります。また OSPF がディセーブルで、しかも、ENE のゲートウェイ設定がイネーブルになっていない。</li> <li>• 同じサブネット内の ONS 15454 間で複数の CTC セッションをイネーブルにする必要がある。また、ENE のゲートウェイ設定がイネーブルになっていない。</li> </ul>
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。Create をクリックします。

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

- Destination — CTC が稼働しているコンピュータの IP アドレスを入力します。アクセス先を 1 つのコンピュータに制限する場合は、完全な IP アドレスとサブネット マスク 255.255.255.255 を入力します。192.168.1.0 サブネット上のすべてのコンピュータへアクセスできるようにするには、192.168.1.0 とサブネット マスク 255.255.255.0 を入力します。宛先として 0.0.0.0 を入力すると、ルータに接続しているすべての CTC コンピュータへアクセスできるようになります。
- Mask — サブネット マスクを入力します。宛先がホストルート(つまり、1 つの CTC コンピュータ)の場合は、32 ビットのサブネット マスク (255.255.255.255) を入力します。宛先がサブネットの場合は、255.255.255.0 のようにサブネット マスクを調整します。宛先が 0.0.0.0 の場合は CTC によって自動的にサブネット マスク 0.0.0.0 が入力され、すべての CTC コンピュータへアクセスできるようになります。この値は変更できません。
- Next Hop — CTC コンピュータがノードに直接接続されている場合は、ルータ ポートまたはノードの IP アドレスを入力します。
- Cost — ONS 15454 とコンピュータの間のホップ数を入力します。

**ステップ 4** OK をクリックします。Static Route ウィンドウにスタティック ルートが表示されることを確認します。



(注) スタティック ルート ネットワークの例については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A67 ONS 15454 での IOP リスナー ポートのプロビジョニング

目的	この作業では、ONS 15454 上で Internet Inter-ORB Protocol (IOP) リスナー ポートを設定し、ファイアウォールの背後にある ONS 15454 ノードにアクセスできるようにします。
工具 / 機器	LAN 管理者またはファイアウォール管理者が指定する IOP リスナー ポート番号
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) ポート 1080 の Enable SOCKS Proxy Server チェックボックスがオンになっている場合、CTC ではポート 1080 が使用され、ここで設定した IOP ポート設定は無視されます。あとで Enable SOCKS Proxy Server チェックボックスをオフにした場合は、ここで設定した IOP リスナー ポートが使用されます。

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

**ステップ 2** TCC CORBA (IIOP) 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) — ONS 15454 が CTC コンピュータと同じファイアウォール側にある場合、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、このオプションを選択します。このオプションは、ONS 15454 リスナー ポートをポート 57790 に設定します。ポート 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 — ONS 15454 リスナー ポートとしてポート 683 (CORBA のデフォルトポート番号) を使用する場合は、このオプションを選択します。
- Other Constant — ポート 683 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 ポートを入力します。

**ステップ 3** Apply をクリックします。

**ステップ 4** [Change Network Configuration] というメッセージが表示されたら、Yes をクリックします。

両方の ONS 15454 TCC2/TCC2P カードは、一度に 1 つずつリブートします。リブートには約 15 分かかります。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A68 CTC コンピュータにおける IIOP リスナー ポートのプロビジョニング

目的	この作業では、CTC 上で IIOP リスナー ポートの選択を行います。CTC を実行しているコンピュータがファイアウォールの背後にある場合は、この作業を実行する必要があります。
工具 / 機器	LAN 管理者またはファイアウォール管理者が指定する IIOP リスナー ポート番号
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

**ステップ 2** Preferences ダイアログボックスで Firewall タブをクリックします。

**ステップ 3** CTC CORBA (IIOP) Listener Port 領域で、リスナー ポート オプションを選択します。

- Variable (デフォルト) — ONS 15454 が CTC コンピュータと同じファイアウォール側にある場合、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、このオプションを選択します。このオプションは、CTC リスナー ポートをポート 57790 に設定します。ポート 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 — CTC コンピュータのリスナー ポートとしてポート 683 (CORBA のデフォルトポート番号) を使用する場合は、このオプションを選択します。

- Other Constant — ポート 683 を使用しない場合は、管理者が定義した IOP ポートを入力します。

- ステップ 4** Apply をクリックします。ポートの変更は次回の CTC ログイン時に適用される旨の警告メッセージが表示されます。
- ステップ 5** OK をクリックします。
- ステップ 6** Preferences ダイアログボックスで OK をクリックします。
- ステップ 7** IOP ポートを使用して ONS 15454 にアクセスする場合は、CTC からログアウトしてから、ログインしなおします（ログアウトするには、File メニューから Exit を選択します）。
- ステップ 8** 元の NTP（手順）に戻ります。

## DLP-A69 外部タイミングまたはライン タイミングの設定

目的	この作業では、ONS 15454 の SONET タイミング ソース（外部またはライン）を定義します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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** General Timing 領域で、次の情報を入力します。

- Timing Mode — ONS 15454 がタイミングをバックプレーン ピンに接続された BITS ソースから得る場合は External を選択し、タイミング ノードに光接続された OC-N カードから得る場合は Line を選択します。3 番目のオプション Mixed を選択すると、ユーザは外部タイミング基準とライン タイミング基準を設定できます



**(注)** Mixed タイミングではタイミング ループが発生することがあるので、使用しないことを推奨します。このモードを使用するときは注意してください。

- SSM Message Set — Synchronization Status Messaging (SSM; 同期ステータス メッセージング) メッセージ セットを選択します。すべての ONS 15454 は Generation 2 メッセージ セットを変換できるため、ONS 15454 がほかの ONS 15454 に接続されている場合は、Generation 2 を選択します。Generation 1 を選択するのは、Generation 2 をサポートしない機器に ONS 15454 が接続されている場合に限定してください。SSM メッセージが Generation 1 に設定されているノードが Generation 2 メッセージを受信すると、メッセージは次に使用可能な Generation 1 メッセージにマッピングされます。Transit Node Clock (TNC) および ST3E (Stratum 3E) は、ST3 (Stratum 3) クロックになります。

- Quality of RES — タイミング ソースが予約済みの S1 バイトをサポートしている場合は、タイミング品質をここで設定します（ほとんどのタイミングソースは RES を使用しません）。品質は降順で、範囲として表示されます。たとえば、ST3<RES<ST2 は、タイミング基準が Stratum 3 より大きく、Stratum 2 より小さいことを示します。SONET タイミング レベルの定義など、SSM の詳細については、『Cisco ONS 15454 Reference Manual』の「Timing」の章を参照してください。
- Revertive — セカンダリ タイミング基準へ切り替わる要因となった状態が修正されたあとで、ONS 15454 をプライマリ基準ソースに戻す場合は、このチェック ボックスをオンにします。
- Revertive Time — Revertive がオンになっている場合に、プライマリ タイミング ソースに戻るまでに ONS 15454 が待つ時間を選択します。デフォルトは 5 分です。

### ステップ 3 Reference List 領域で、次の情報を入力します。



**(注)** 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、バックプレーンにあるノードの BITS Out ピンに接続可能な機器で使用されるタイミング基準を定義します。機器を BITS Out ピンに接続する場合は、特別なことがないかぎり、ライン モードでノードに接続します。機器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直接つなぐことができるからです。

- NE Reference — 3 つのタイミング基準 (Ref 1、Ref 2、Ref 3) を定義できます。その基準で障害が発生しないかぎり、ノードは Reference 1 を使用します。障害が発生した場合は、Reference 2 を使用します。Reference 2 が失敗すると、ノードは、通常内部クロックに設定されている Reference 3 を使用します。内部クロックは、TCC2/TCC2P に提供される Stratum 3 クロックです。表示されるオプションは、Timing Mode の設定により異なります。
- Timing Mode が External に設定されている場合に選択できるオプションは、BITS1、BITS2、および Internal Clock です。
- Timing Mode が Line に設定されている場合に選択できるオプションは、ノードの現用 OC-N カードおよび Internal Clock です。BITS ソース、すなわちノードのトランク (スパン) カードに配線されたノードに直接または間接的に接続されたカードやポートを選択します。Reference 1 は BITS ソースに一番近いトランク カードに設定されています。たとえば、スロット 5 が BITS ソースに配線されたノードに接続されている場合、スロット 5 を Reference 1 として選択します。
- Timing Mode が Mixed に設定されている場合は、BITS カードと OC-N カードの両方を使用できます。これにより、外部 BITS カードと OC-N トランク (スパン) カードを組み合わせたものをタイミング基準として設定できます。
- BITS-1 Out/BITS-2 Out — バックプレーンの BITS Out ピンに接続された機器のタイミング基準を定義します。BITS-1 Out および BITS-2 Out は、BITS-1 および BITS-2 ファシリティが移動中の場合にイネーブルになります。Timing Mode が External に設定されている場合は、タイミング設定に使用する OC-N カードを選択します。Timing Mode が Line に設定されている場合は、OC-N カードを選択できます。または、NE Reference を選択して、BITS-1 Out または BITS-2 Out (またはその両方) が NE と同じタイミング基準に従うように設定することもできます。

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

BITS Facilities セクションには、BITS1 タイミング基準と BITS2 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。機器のタイミングを BITS Out から取得していれば、その機器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。

**ステップ 5** BITS In 領域で、次の情報を入力します。

- Facility Type — (TCC2P カードのみ) BITS クロックでサポートされている BITS 信号タイプを選択します (DS1 または 64Khz+8Khz.)
- BITS In State — Timing Mode を External または Mixed に設定した場合は、MIC 上の BITS 入力ピンペアが外部タイミングソースに 1 つだけ接続されているか、または両方とも接続されているかによって、BITS-1 または BITS-2 (またはその両方) の BITS In State を IS (移動中) に設定します。Timing Mode を Line に設定した場合は、BITS In State を OOS(停止)に設定します。

**ステップ 6** BITS In State を OOS に設定した場合は、[ステップ 7](#) に進みます。BITS In State を IS に設定した場合は、次の情報を入力します。

- Coding — BITS 基準で使用される符号化として、Binary 8-Zero Substitution (B8ZS; バイナリ 8 ゼロ置換) または Alternate Mark Inversion (AMI; 交互マーク反転) を選択します。
- Framing — ご使用の BITS 基準で使用されるフレーミングを、Extended Super Frame (ESF; 拡張スーパーフレーム) または Super Frame (SF) (D4) から選択します。
- Sync Messaging — SSM をイネーブルにする場合は、このチェックボックスをオンにします。Framing が Super Frame に設定されている場合は、SSM を使用できません。
- Admin SSM — Sync Messaging チェックボックスがオフになっていれば、ドロップダウン リストから SSM Generation 2 タイプを選択できます。

**ステップ 7** BITS Out 領域で、次の情報を入力します。

- Facility Type — BITS Out 信号タイプとして、DS1 または 64 KHz を選択します。
- BITS Out State — 機器がバックプレーンにあるノードの BITS 出力ピンに接続されていて、ノード基準から機器のタイミングを取るようになっていない場合は、外部機器に使用されている BITS Out ピンに応じて、BITS-1 と BITS-2 のいずれかまたは両方の BITS Out State を IS に設定します。機器が BITS 出力ピンに接続されていない場合は、BITS Out State を OOS に設定します。

**ステップ 8** BITS Out State を OOS に設定した場合は、[ステップ 9](#) へ進みます。BITS Out State を IS に設定した場合は、次の情報を入力します。

- Coding — BITS 基準で使用される符号化として、B8ZS または AMI を選択します。
- Framing — ご使用の BITS 基準で使用されるフレーミングを、ESF または SF (D4) から選択します。
- AIS Threshold — SSM がディセーブルの場合、または SF が使用されている場合は、ノードが BITS1 Out や BITS2 Out バックプレーン ピンから Alarm Indication Signal (AIS; アラーム表示信号) を送信するときの品質レベルを設定します。BITS 基準の光ソースがこのフィールドで定義された SSM 品質レベル以下に低下すると、AIS アラームが発生します。
- LBO — BITS Out ピンに接続された外部デバイスのタイミングを取る場合は、デバイスと ONS 15454 の間の距離を選択します。選択できるオプションは、0 ~ 133 フィート (デフォルト)、124 ~ 266 フィート、267 ~ 399 フィート、400 ~ 533 フィート、および 534 ~ 655 フィートです。Line Build Out (LBO) は BITS ケーブル長に関係します。

**ステップ 9** Apply をクリックします。

(注) タイミング関連のアラームについては、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

ステップ 10 元の NTP (手順) に戻ります。

## DLP-A70 内部タイミングの設定

目的	この作業では、ONS 15454 の内部タイミング (Stratum 3) を設定します。BITS ソースを使用できない場合のみ、実行してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

内部タイミングは Stratum 3 なので、一時的にしか使用しません。ONS 15454 ノードのタイミングは、すべて Stratum 2 以上のプライマリ基準ソースに合わせる必要があります。

**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 領域で、次の情報を入力します。

- Timing Mode — **External** を選択します。
- SSM Message Set — **Generation 1** に設定します。
- Quality of RES — 内部タイミングには適用されません。
- Revertive — 内部タイミングには適用されません。
- Revertive Time — 内部タイミングには適用されません。

**ステップ 3** Reference Lists 領域で、次の情報を入力します。

- NE Reference
  - Ref 1 — **Internal Clock** に設定します。
  - Ref 2 — **Internal Clock** に設定します。
  - Ref 3 — **Internal Clock** に設定します。
- BITS-1 Out/BITS-2 Out — **None** に設定します。

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

**ステップ 5** BITS Facilities 領域で、BITS In State および BITS Out State を **OOS** に変更します。その他の BITS Facilities 設定は無視してください。内部タイミングには関係しません。

**ステップ 6** **Apply** をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。



## DLP-A71 1:1 保護グループの作成

目的	この作業では、1:1 電気回路カード保護グループを作成します。
工具 / 機器	冗長的な DS-1、DS-3、EC-1、または DS3XM カードをシェルフに取り付けるか、またはこれらのカードのうちの 2 枚に対して ONS 15454 スロットをプロビジョニングする必要があります。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** [表 4-1 \(p.4-12\)](#) に示す、1:1 保護の要件に応じたカードが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。

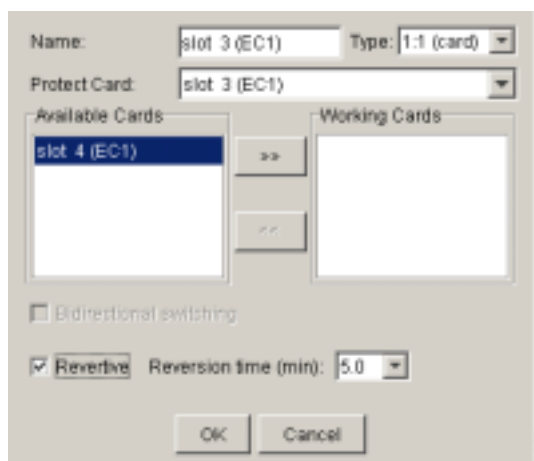
**ステップ 3** **Create** をクリックします。

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

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字 (a ~ z、A ~ Z、0 ~ 9) を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符 (?)、バックスラッシュ (\)、二重引用符 (") は使用しないでください。
- Type — ドロップダウン リストから 1:1 を選択します。
- Protect Card — ドロップダウン リストから保護カードを選択します。ドロップダウン リストには、1:1 保護で使用可能なカードが表示されます。使用可能なカードがないと、リストにカードは表示されません。

保護カードを選択すると、保護に使用できるカードが Available Cards リストに表示されます ([図 17-32](#) を参照)。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「[DLP-A330 カード スロットの事前プロビジョニング \(p.20-22\)](#)」を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

図 17-32 1:1 保護グループの作成



**ステップ 5** Available Cards リストから、Protect Card ドロップダウン リストで選択したカードで保護するカードを選択します。上にある矢印ボタンをクリックして、各カードを Working Cards リストに移動します。


**ステップ 6** 残りのフィールドを次のように設定します。

- Bidirectional switching — 1:1 保護では使用できません。
- Revertive — 障害状態が修正されたあと、正常な状態が Reversion Time フィールドに入力された時間だけ続いた場合に、トラフィックを現用カードに復帰させるには、このボックスをオンにします。
- Reversion time — Revertive をオンにした場合に、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。これは、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

**ステップ 7** OK をクリックし、確認用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-A72 1:N 保護グループの作成

目的	この作業では、DS-1、DS-3、または SVC-RAN の 1:N 保護グループを作成します。
工具 / 機器	DS1N-14、DS3N-12、DS3N-12E、DS3/EC1-48、または DS1/E1-56 (保護カード); DS1-14、DS3-12、または DS3-12E (現用カード)
	 <p><b>(注)</b> DS1N-14、DS3N-12、DS3N-12E、DS3/EC1-48、または DS1/E1-56 保護カードは、スロット 3 またはスロット 15 に取り付けられ、保護するカード (DS1-14、DS3-12、DS3-12E) はシェルフの同じ側にある必要があります。</p>
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** [表 4-1 \(p.4-12\)](#) に示す、1:N の要件に応じたカードが取り付けられていることを確認します。

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

**ステップ 3** Protection Groups 領域で、Create をクリックします。

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

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字 (a ~ z、A ~ Z、0 ~ 9) を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符 (?)、バックスラッシュ (\)、二重引用符 (") は使用しないでください。
- Type — ドロップダウン リストから 1:N を選択します。
- Protect Card — ドロップダウン リストから保護カードを選択します。リストには、DS1N-14、DS3N-12、DS3/EC1-48、DS3N-12E、または DS1/E1-56 カード (スロット 3 または 15 に取り付け済み) が表示されます。これらのカードが取り付けられていないと、ドロップダウン リストにカードは表示されません。

保護カードを選択すると、保護に使用できるカードのリストが Available Cards リストに表示されます。使用可能なカードがないと、カードは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カードスロットの事前プロビジョニング」(p.20-22) を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

**ステップ 5** Available Cards リストから、Protect Card ドロップダウン リストで選択したカードで保護するカードを選択します。上にある矢印ボタンをクリックして、各カードを Working Cards リストに移動します。

**ステップ 6** 残りのフィールドを次のように設定します。

- Bidirectional switching — 1:N 保護では使用できません。
- Revertive — 1:N 保護グループの場合は必ずイネーブルになります。
- Reversion time — **Reversion time** をクリックし、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。これは、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

**ステップ 7** OK をクリックし、確認用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-A73 1+1 保護グループの作成

目的	この作業では、任意の OC-N カードまたはポート (OC-3、OC3-8、OC-12、OC12-4、OC-48、OC-48 AS、OC-192、MRC-12、OC192SR1/STM64IO Short Reach、および OC192/STM64 Any Reach カード) の 1+1 保護グループを作成します。
工具 / 機器	取り付け済みの OC-N カードまたは事前にプロビジョニングされたスロット
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** [表 4-1 \(p.4-12\)](#) に示す、1+1 の要件に応じたカードが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、**Create** をクリックします。

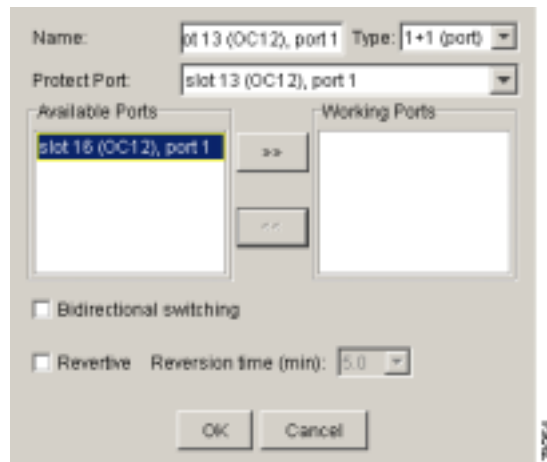
**ステップ 4** Create Protection Group ダイアログボックスで次の情報を入力します。

- Name — 保護グループの名前を入力します。保護グループ名には、32 文字までの英数字 (a ~ z、A ~ Z、0 ~ 9) を使用します。特殊文字も使用できますが、TL1 と互換性を持たせるために、疑問符 (?)、バックスラッシュ (\)、二重引用符 (") は使用しないでください。
- Type — ドロップダウン リストから 1+1 を選択します。

- Protect Card — ドロップダウン リストから保護ポートを選択します。ドロップダウン リストには、使用可能な OC-N ポートが表示されます (図 17-33 を参照)。OC-N カードが取り付けられていないと、ドロップダウン リストにポートは表示されません。

保護ポートを選択すると、保護に使用できるポートのリストが Available Ports リストに表示されます (図 17-33 を参照)。使用可能なカードがないと、ポートは表示されません。その場合は、この作業を行う前に、物理カードを取り付けるか、「DLP-A330 カード スロットの事前プロビジョニング」(p.20-22) を行って ONS 15454 スロットを事前にプロビジョニングする必要があります。

図 17-33 1+1 保護グループの作成



**ステップ 5** Available Ports リストから、Protect Port フィールドで選択したポートで保護するポートを選択します。上にある矢印ボタンをクリックして、各ポートを Working Ports リストに移動します。

**ステップ 6** 残りのフィールドを次のように設定します。

- Bidirectional switching — いずれかの信号に障害が発生した際に Tx と Rx の信号を両方とも保護ポートに切り替える場合は、このボックスをオンにします。障害が発生した信号だけを保護ポートに切り替える場合は、オフにします。
- Revertive — 障害状態が修正されたあと、正常な状態が Reversion Time フィールドに入力された時間だけ続いた場合に、トラフィックを現用カードに復帰させるには、このボックスをオンにします。
- Reversion time — Revertive をオンにした場合に、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。復元時間は、切り替えの原因になった状態が解消されたあと、トラフィックが現用カードに復帰するまでに経過する時間です。切り替えの原因になった状態が解消されると、復元タイマーが動き始めます。

**ステップ 7** OK をクリックします。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A74 新規ユーザの作成：単一ノード

目的	この作業では、単一の ONS 15454 ノードに対して新しいユーザを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Users** タブをクリックします。

**ステップ 2** Users ウィンドウで、**Create** をクリックします。

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

- Name — ユーザ名を入力します。ユーザ名は、6 ~ 20 文字以内の英数字 (a ~ z、A ~ Z、0 ~ 9) で指定します。TL1 との互換性を保つには、ユーザ名を 6 ~ 10 文字にする必要があります。
- Password — ユーザのパスワードを入力します。パスワードは、6 ~ 20 文字以内の英数字 (a ~ z、A ~ Z、0 ~ 9) および特殊文字 (+、#、%) で指定します。少なくとも 2 文字は英字以外の文字、少なくとも 1 文字は特殊文字を使用する必要があります。TL1 との互換性を保つには、パスワードを 6 ~ 10 文字にする必要があります。パスワードには、ユーザ名を含めないでください。
- Confirm Password — 確認のためにパスワードをもう一度入力します。
- Security Level — ユーザのセキュリティ レベルを、RETRIEVE、MAINTENANCE、PROVISIONING、または SUPERUSER の中から選択します。各レベルで提供される機能については、『Cisco ONS 15454 Reference Manual』の「Security」の章を参照してください。



**(注)** 各セキュリティ レベルには、それぞれ異なるアイドル時間があります。アイドル時間とは、CTC がアイドル状態になってからパスワードが再入力されるまでの時間です。デフォルトのアイドル時間は、検索ユーザは無制限、メンテナンス ユーザは 60 分、プロビジョニングユーザは 30 分、スーパーユーザは 15 分です。アイドル時間の変更方法については、『[NTP-A205 ユーザの変更とセキュリティの変更](#)」(p.11-9) を参照してください。

**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-A75 新規ユーザの作成：複数ノード

目的	この作業では、複数の ONS 15454 ノードに対して新しいユーザを作成します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) ユーザを追加するすべてのノードに、ネットワーク ビューでアクセスできるように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。

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

**ステップ 3** Users ウィンドウで、**Create** をクリックします。

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

- Name — ユーザ名を入力します。ユーザ名は、6 ~ 20 文字以内の英数字 (a ~ z、A ~ Z、0 ~ 9) で指定します。TL1 との互換性を保つには、ユーザ名を 6 ~ 10 文字にする必要があります。
- Password — ユーザのパスワードを入力します。パスワードは、6 ~ 20 文字以内の英数字 (a ~ z、A ~ Z、0 ~ 9) および特殊文字 (+、#、%) で指定します。少なくとも 2 文字は英字以外の文字、少なくとも 1 文字は特殊文字を使用する必要があります。TL1 との互換性を保つには、パスワードを 6 ~ 10 文字にする必要があります。パスワードには、ユーザ名を含めないでください。
- Confirm Password — 確認のためにパスワードをもう一度入力します。
- Security Level — ユーザのセキュリティ レベルを、RETRIEVE、MAINTENANCE、PROVISIONING、または SUPERUSER の中から選択します。各レベルで提供される機能については、『Cisco ONS 15454 Reference Manual』の「Security」の章を参照してください。



(注) 各セキュリティ レベルには、それぞれ異なるアイドル時間があります。アイドル時間とは、CTC がアイドル状態になってからロックアップしてパスワードが再入力されるまでの時間です。デフォルトのアイドル時間は、検索ユーザは無制限、メンテナンス ユーザは 60 分、プロビジョニング ユーザは 30 分、スーパーユーザは 15 分です。アイドル時間の変更方法については、『[NTP-A205 ユーザの変更とセキュリティの変更 \(p.11-9\)](#)』を参照してください。

**ステップ 5** [Select applicable nodes] で、ユーザを追加しないノードの選択を解除します (デフォルトでは、すべてのネットワーク ノードが選択されます)。

**ステップ 6** OK をクリックします。

- ステップ 7** User Creation Results ダイアログボックスで、**ステップ 5** で選択したすべてのノードにユーザが追加されたことを確認します。ユーザが追加されていない場合は、**OK** をクリックして**ステップ 2 ~ 6** を繰り返します。すべてのノードにユーザが追加されていたら、**OK** をクリックして次のステップへ進みます。
- ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A83 オーダーワイヤのプロビジョニング

目的	この作業では、AIC-I カードのオーダーワイヤをプロビジョニングします。
工具 / 機器	AIC-I カードがスロット 9 に取り付けられている必要があります。
事前準備手順	OC-N カードが取り付けられている必要があります。 <a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 ビューで、**Provisioning > Overhead Circuits** 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** Overhead Circuit Creation ダイアログボックスの Circuit Attributes 領域で次のフィールドを指定します。
- Name — 回線に名前を付けます。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。
  - Circuit Type — 作成するオーダーワイヤパスに応じて、**Local Orderwire** または **Express Orderwire** を選択します。ONS 15454 ノード間でリジェネレータが使用されていない場合は、ローカル オーダーワイヤ チャネルまたはエクスプレス オーダーワイヤ チャネルを使用します。リジェネレータが存在する場合は、エクスプレス オーダーワイヤ チャネルを使用します。オーダーワイヤパスごとに 4 つまでの ONS 15454 OC-N ポートをプロビジョニングできます。
  - PCM — Pulse Code Modulation (PCM; パルス符号変調) 音声符号化およびコンパandingの標準として、Mu\_Law (北米、日本) または A\_Law (ヨーロッパ) のいずれかを選択します。プロビジョニングの手順は、どちらの種類 of オーダーワイヤでも同じです。



### 注意

リングにある ONS 15454 ノードのオーダーワイヤをプロビジョニングする場合は、オーダーワイヤ ループ全体をプロビジョニングしないでください。たとえば、4 ノードのリングでは、通常、4 つのノードすべてにイーストポートとウェストポートがプロビジョニングされていますが、オーダーワイヤループを防止するために、1 つのリング ノードを除いて、他のノードに 2 つのオーダーワイヤポート (イーストとウェスト) をプロビジョニングしてください。

- ステップ 4** **Next** をクリックします。

**ステップ 5** Circuit Source 領域で次の項目を指定します。

- Node — 送信元ノードを選択します。
- Slot — 送信元スロットを選択します。
- Port — 表示された場合は、送信元ポートを選択します。

**ステップ 6** Next をクリックします。

**ステップ 7** Circuit Destination 領域で、次の項目を指定します。

- Node — 宛先ノードを選択します。
- Slot — 宛先スロットを選択します。
- Port — 表示された場合は、宛先ポートを選択します。

**ステップ 8** Finish をクリックします。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A88 1+1 光保護のテスト

目的	この作業では、1+1 保護グループでトラフィックが正しく切り替えられることを確認します。1+1 保護グループを作成した場合は、この手順を実行する必要があります。
工具 / 機器	受け入れテストの手順で指定したテスト セット
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> トポロジーの受け入れテストで作成したテスト回線
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** View メニューから **Go to Network View** を選択します。

**ステップ 2** Alarms タブをクリックします。

- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 3** Conditions タブをクリックします。説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 4** ネットワーク マップ上でテスト対象の 1+1 保護グループがあるノードをダブルクリックし、ノードビューで開きます。



**ステップ 5** Maintenance > Protection タブをクリックします。

**ステップ 6** 次のようにして、現用ポートで強制切り替えを開始します。

- a. Protection Groups 領域で、1+1 保護グループをクリックします。
- b. 現用ポートをクリックします。Switch Commands の隣にある Force をクリックします。
- c. Confirm Force Operation ダイアログボックスで、Yes をクリックします。
- d. Selected Group 領域で、次のように表示されることを確認します。
  - Protect port: Protect/Active [FORCE\_SWITCH\_TO\_PROTECT], [PORT STATE]
  - Working port: Working/Standby [FORCE\_SWITCH\_TO\_PROTECT], [PORT STATE]

**ステップ 7** ノードに接続されたテスト セットのトラフィックが動作していることを確認します。ビット エラーはあってもかまいませんが、トラフィック フローが中断する場合は問題があります。トラフィックの中断が発生する場合は、[ステップ 8](#) を実行して、上位レベルのサポートに連絡します。トラフィックの中断が発生しない場合は、[ステップ 8 ~ 12](#) を実行します。

**ステップ 8** 現用ポートで切り替えをクリアします。

- a. Switch Commands の隣にある Clear をクリックします。
- b. Confirm Clear Operation ダイアログボックスで、Yes をクリックします。

**ステップ 9** 保護ポートで強制切り替えを開始します。

- a. Selected Group 領域で、保護ポートをクリックします。Switch Commands の隣にある Force をクリックします。
- b. Confirm Force Operation ダイアログボックスで、Yes をクリックします。
- c. Selected Group 領域で、次のように表示されることを確認します。
  - Protect port: Protect/Active [FORCE\_SWITCH\_TO\_WORKING], [PORT STATE]
  - Working port: Working/Standby [FORCE\_SWITCH\_TO\_WORKING], [PORT STATE]

**ステップ 10** ノードに接続されたテスト セットのトラフィックが動作していることを確認します。トラフィックの中断が発生する場合は、[ステップ 11](#) を実行し、上位レベルのサポートに連絡します。トラフィックの中断が発生しない場合は、[ステップ 11](#) および [12](#) を実行します。

**ステップ 11** 保護ポートで切り替えをクリアします。

- a. Switch Commands の隣にある Clear をクリックします。
- b. Confirm Clear Operation ダイアログボックスで、Yes をクリックします。
- c. Selected Group 領域で、次の状態を確認します。
  - 保護ポート：Protect/Standby
  - 現用ポート：Working/Active

**ステップ 12** 元の手順 (NTP) に戻ります。

## DLP-A89 K3 バイトの再マップ

目的	この作業では、K3 バイトをプロビジョニングします。ONS 15454 の BLSR をサードパーティ製機器経由で運用する必要がない場合は、K3 バイトを再マップしないでください。特別なユーザでないかぎり、この作業は不要です。
工具 / 機器	再マップする BLSR スパンに OC48 AS カードが取り付けられている必要があります。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

K3 バイトを再マップする場合は、スパンの両端で同じ拡張バイト (Z2、E2、または F1) に再マップします。

- 
- ステップ 1** ノードビューで、サードパーティ製機器に接続する OC48 AS 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** BLSR Ext Byte をクリックして、Z2、E2、または F1 から代替バイトを選択します。
- ステップ 4** Apply をクリックします。
- ステップ 5** (4 ファイバ BLSR のみ) 保護カードごとにステップ 2 ~ 4 を繰り返します。
- ステップ 6** BLSR スパンの他端にあるノードとカードで、この作業を繰り返します。



(注) [ステップ 3](#) で選択した拡張バイトは、スパンの両端で一致している必要があります。

- ステップ 7** 元の NTP (手順) に戻ります。
- 

## DLP-A91 BLSR 切り替えテスト

目的	この作業では、BLSR で保護切り替えが正しく実行されることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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 メニューで、**Go to Network View** を選択します。

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

**ステップ 3** 切り替える BLSR の行をクリックし、**Edit** をクリックします。

**ステップ 4** ウェスト ポートで強制リング切り替えを開始します。

- a. 任意の BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。図 19-2 (p.19-12) に例を示します (グラフィック アイコンを移動するには、そのアイコンをクリックし、**Ctrl** キーを押しながら新しい場所にドラッグアンドドロップします)。



**(注)** 2 ファイバの BLSR の場合、ノード アイコンの四角形は、BLSR の現用チャンネルと保護チャンネルを表します。いずれかのチャンネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。現用ポートまたは保護ポートを右クリックします。

- 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 **FORCE RING** を選択します。
- c. **OK** をクリックします。
- d. 表示された 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制リング切り替えを呼び出した BLSR チャンネルに F が表示されます。強制リング切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。

**ステップ 5** 次の状態を確認します。

- a. **Conditions** タブをクリックします。
- b. **Retrieve** をクリックします。
- c. ウェスト ポートで強制リング切り替えを呼び出したノードで、次の状態が報告されることを確認します。
  - **FORCED-REQ-RING** — ノードのウェスト側にあるスパンの現用スロットに対して、Force Switch Request On Ring 状態が報告されます。
  - **RING-SW-EAST** — ノードのイースト側にある現用スパンに対して、イースト側で Ring Switch Active 状態が報告されます。



**(注)** ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

- d. 切り替えを実行したノードのウェスト ラインに接続されたノードで、次の状態が報告されることを確認します。
  - **FE-FRCDWKSWPR-RING** — ノードのイースト側にある現用スパンに対して、Far-End Working Facility Forced to Switch to Protection 状態が報告されます。
  - **RING-SW-WEST** — ノードのウェスト側にある現用スパンに対して、ウェスト側で Ring Switch Active 状態が報告されます。

**ステップ 6** (任意) ONS 15454 の BLSR をサードパーティ製機器経由で運用するために K3 バイトを再マップしている場合は、次の状態が報告されていることを確認します。強制リング切り替えを実行したノードのウェスト側に接続されていない他のノードで、FULLPASSTHR-BI 状態が報告されていることを確認します。

**ステップ 7** 各ノードで BLSR のライン ステータスを確認します。

- a. View メニューから、Go to Node View を選択します。
- b. Maintenance > BLSR タブをクリックします。
- c. 次の点を確認します。
  - 強制リング切り替えを呼び出したノードのライン ステータスが、ウェスト側では Stby/Stby、イースト側では Act/Act と表示されること。
  - 強制リング切り替えを呼び出したノードのウェスト ラインに接続されたノードのライン ステータスが、イースト側では Stby/Stby、ウェスト側では Act/Act と表示されること。
  - リング内の残りのノードのライン ステータスが、イースト側とウェスト側の両方で Act/Act と表示されること。

**ステップ 8** View メニューから Go to Network View を選択します。

**ステップ 9** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 10** 強制リング切り替えを呼び出した BLSR ウィンドウを表示します(このウィンドウは、CTC ウィンドウの下に隠れていることがあります)。

**ステップ 11** ウェスト ポートで切り替えをクリアします。

- a. 強制リング切り替えを実行した BLSR ノードのウェスト ポートを右クリックし、Set West Protection Operation を選択します。
- 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。
- c. OK をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで Yes をクリックします。

ネットワーク ビューの図では、強制リング切り替えが削除され、切り替えを表す F も表示されなくなっています。BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 12** ネットワーク ビューで、Conditions タブをクリックします。この手順を実行して表示されたすべての状態がネットワークからクリアされていることを確認します。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。

**ステップ 13** 各ノードで BLSR のライン ステータスを確認します。

- a. View メニューから、**Go to Node View** を選択します。
- a. **Maintenance > BLSR** タブをクリックします。
- b. リング内にある各ノードのライン ステータスが、イースト側とウェスト側の両方で Act/Stby と表示されることを確認します。

**ステップ 14** イースト ポートで強制リング切り替えを開始します。

- a. BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。
- 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 **FORCE RING** を選択します。
- c. **OK** をクリックします。
- d. 表示された 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制リング切り替えを呼び出した現用 BLSR チャンネルに F が表示されます。強制リング切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 15** 次の状態を確認します。

- a. **Conditions** タブをクリックします。
- b. **Retrieve** をクリックします。
- c. イースト ポートで切り替えを呼び出したノードで、次の状態が報告されることを確認します。
  - **FORCED-REQ-RING** — ノードのイースト側にあるスパンの現用スロットに対して、Force Switch Request On Ring 状態が報告されます。
  - **RING-SW-WEST** — ノードのイースト側にある現用スパンに対して、ウェスト側で Ring Switch Active 状態が報告されます。



**(注)** ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

- d. 切り替えを実行したノードのイースト ラインに接続されたノードで、次の状態が報告されることを確認します。
  - **FE-FRCDWKSWPR-RING** — ノードのウェスト側にある現用スパンに対して、Far-End Working Facility Forced to Switch to Protection 状態が報告されます。
  - **RING-SW-EAST** — ノードのウェスト側にある現用スパンに対して、イースト側で Ring Switch Active 状態が報告されます。

**ステップ 16** (任意) K3 バイトを再マップして ONS 15454 の BLSR をサード パーティ製機器経由で運用している場合は、強制リング切り替えを実行したノードのウェスト側に接続されていない他のノードで、FULLPASSTHR-BI 状態が報告されていることを確認します。

**ステップ 17** 各ノードで BLSR のライン ステータスを確認します。

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

- b. Maintenance > BLSR タブをクリックします。
  - 次の点を確認します。
  - 強制リング切り替えを呼び出したノードのライン ステータスが、イースト側では Stby/Stby、ウェスト側では Act/Act と表示されること。
  - 強制リング切り替えを呼び出したノードのイースト ラインに接続されたノードのライン ステータスが、ウェスト側では Stby/Stby、イースト側では Act/Act と表示されること。
  - リング内の残りのノードのライン ステータスが、イースト側とウェスト側の両方で Act/Act と表示されること。

**ステップ 18** View メニューから **Go to Network View** を選択します。

**ステップ 19** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 20** 強制リング切り替えを呼び出した BLSR ウィンドウを表示します(このウィンドウは、CTC ウィンドウの下に隠れていることがあります)。

**ステップ 21** イースト ポートで切り替えをクリアします。

- a. 強制リング切り替えを呼び出した BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。
- 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。
- c. **OK** をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制リング切り替えが削除され、切り替えを表す F も表示されなくなっています。BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 22** ネットワーク ビューで、**Conditions** タブをクリックします。この手順を実行して表示されたすべての状態がネットワークからクリアされていることを確認します。説明のつかない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。

**ステップ 23** 各ノードで BLSR のライン ステータスを確認します。

- a. View メニューから、**Go to Node View** を選択します。
- b. Maintenance > BLSR タブをクリックします。
- c. リング内にある各ノードのライン ステータスが、イースト側とウェスト側の両方で Act/Stby と表示されることを確認します。

**ステップ 24** File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

**ステップ 25** 元の NTP (手順) に戻ります。

## DLP-A92 4 ファイバ BLSR のスパン負荷テスト

目的	この作業では、4 ファイバ BLSR のスパンに対して負荷テストを実行します。リング試験状態 (K バイトのパススルーなど) が報告され、10 ~ 15 秒以内にクリアされます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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** View メニューから **Go to Network View** を選択します。

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

**ステップ 3** 負荷テストをする BLSR をクリックして、**Edit** をクリックします。

**ステップ 4** ウェスト スパンの負荷テストを実行します。

- a. 負荷テストを行う 4 ファイバ BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します (グラフィック アイコンを移動するには、Ctrl キーを押しながら、アイコンを新しい場所にドラッグ アンド ドロップします)。



**(注)** ネットワーク マップ上の四角形は、ポートを表します。現用ポートを右クリックします。

- 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 **EXERCISE SPAN** を選択します。
- c. **OK** をクリックします。**Confirm BLSR Operation** ダイアログボックスで、**Yes** をクリックします。ネットワーク ビューの図で、試験を呼び出す BLSR チャンネルに E が表示されます。E は、10 ~ 15 秒間表示されてから消えます。

**ステップ 5** 次の状態を確認します。

- a. **Conditions** タブをクリックしてから、**Retrieve** をクリックします。
- b. 次の状態を確認します。
  - EXERCISING-SPAN — スパンの負荷テストを実行したノードで Exercise Ring Successful 状態が報告されます。
  - FE-EX-SPAN — スパンの負荷テストを実行したノードのウェスト側に接続されたノードのイースト スパンに対して Far-End Exercise Span Request 状態が報告されます。
  - KB-PASSTHR — 該当する場合に K Byte Pass Through Active 状態が報告されます。



**(注)** ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

**ステップ 6** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 7** イースト スパンの負荷テストを実行します。

- a. 負荷テストを行う 4 ファイバ BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します
- 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 **EXERCISE SPAN** を選択します。
- c. **OK** をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。  
ネットワーク ビューの図で、試験を呼び出す BLSR チャネルに E が表示されます。E は、10 ~ 15 秒間表示されてから消えます。

**ステップ 8** File メニューから、**Close** を選択します。

**ステップ 9** 次の状態を確認します。

- a. **Conditions** タブをクリックしてから、**Retrieve** をクリックします。
- b. 次の状態を確認します。
  - EXERCISING-SPAN — スパンの負荷テストを実行したノードで Exercise Ring Successful 状態が報告されます。
  - FE-EX-SPAN — スパンの負荷テストを実行したノードのウェスト側に接続されたノードのイースト スパンに対して Far-End Exercise Span Request 状態が報告されます。
  - KB-PASSTHR — 該当する場合に K Byte Pass Though Active 状態が報告されます。



**(注)** ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、Node カラムをクリックします。

**ステップ 10** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 11** File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

**ステップ 12** 元の NTP (手順) に戻ります。



## DLP-A93 4 ファイバ BLSR のスパン切り替えテスト

目的	この作業では、4 ファイバ BLSR のスパンでトラフィックが現用ファイバから保護ファイバに切り替わることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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** View メニューから **Go to Network View** を選択します。

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

**ステップ 3** **Edit** をクリックします。BLSR ウィンドウが開き、BLSR の図が表示されます。



**(注)** BLSR の図にノードアイコンが重なって表示されている場合は、Ctrl キーを押しながら各アイコンを新しい場所にドラッグアンドドロップし、BLSR ポートの情報を見やすくできます。

**ステップ 4** ウェスト スパンを切り替えます。

- a. テストする 4 ファイバ BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。[図 19-2 \(p.19-12\)](#) に例を示します。



**(注)** ネットワーク マップ上の四角形は、ポートを表します。現用ポートを右クリックします。

- 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 **FORCE SPAN** を選択します。
- c. **OK** をクリックします。
- d. 表示された 2 つの **Confirm BLSR Operation** ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、保護切り替えを呼び出した BLSR チャネルに F が表示されます。強制スパン切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。

**ステップ 5** 次の状態を確認します。

- a. **Conditions** タブをクリックします。
- b. **Retrieve** をクリックします。
- c. 強制スパン切り替えを呼び出したノードで **SPAN-SW-WEST** (Span Switch West) 状態が報告され、切り替えを実行したノードのウェスト ラインに接続されたノードで **SPAN-SW-EAST** (Span Switch East) 状態が報告されることを確認します。ウィンドウの右下にある **Filter** ボタンがオフになっていることを確認します。ノードをキーにして状態をソートする場合は、**Node** カラムをクリックします。

**ステップ 6** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**ステップ 7** 強制スパン切り替えを呼び出した BLSR ウィンドウを表示します(このウィンドウは、CTC ウィンドウの下に隠れていることがあります)。**ステップ 8** ウェスト切り替えをクリアします。

- a. 強制スパン切り替えを呼び出した BLSR ノードのウェスト ポートを右クリックし、**Set West Protection Operation** を選択します。
- 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。
- c. **OK** をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制スパン切り替えが削除され、F が表示されなくなり、BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 9** イースト スパンを切り替えます。

- a. BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。
- 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 **FORCE SPAN** を選択します。
- c. **OK** をクリックします。
- d. 表示された 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

ネットワーク ビューの図で、強制スパン切り替えを呼び出した BLSR チャネルに F が表示されます。強制スパン切り替えが呼び出された BLSR スパン ラインがパープルに変わり、他の BLSR ノード間のスパン ラインはすべてグリーンに変わります。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 10** 次の状態を確認します。

- a. **Conditions** タブをクリックします。
- b. **Retrieve** をクリックします。
- c. 強制スパン切り替えを呼び出したノードで SPAN-SW-EAST (Span Switch East) 状態が報告され、切り替えを実行したノードのウェスト ラインに接続されたノードで SPAN-SW-WEST (Span Switch West) 状態が報告されることを確認します。ウィンドウの右下にある Filter ボタンがオフになっていることを確認します。

**ステップ 11** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。

- b. 説明のつかないアラーム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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 12** 強制スパン切り替えを呼び出した BLSR ウィンドウを表示します (このウィンドウは、CTC ウィンドウの下に隠れていることがあります)。

**ステップ 13** イースト切り替えをクリアします。

- a. 強制スパン切り替えを呼び出した BLSR ノードのイースト ポートを右クリックし、**Set East Protection Operation** を選択します。
- 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。
- c. **OK** をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで **Yes** をクリックします。

ネットワーク ビューの図では、強制スパン切り替えが削除され、F が表示されなくなり、BLSR ノード間のスパン ラインはパープルとグリーンで表示されます。スパン ラインの色が変わるまでには、数秒かかることがあります。

**ステップ 14** File メニューから **Close** を選択して、BLSR ウィンドウを閉じます。

**ステップ 15** 元の NTP (手順) に戻ります。

## DLP-A94 UPSR の保護切り替えテスト

目的	この作業では、UPSR スパンが正しく切り替わることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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)

60 ミリ秒未満のサービスの中断が発生することがありますが、テスト回線は、切り替えの実行前、実行中、実行後に関係なく動作し続ける必要があります。回線が停止した場合は、作業を中断し、次のレベルのサポートに問い合わせます。

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

**ステップ 2** ネットワークのスパンを右クリックして、**Circuits** を選択します。

Circuits on Span ダイアログボックスが開き、UPSR 回線 (回線名、場所、スパンでアクティブな回線の色分けなど) が表示されます。

**ステップ 3** 次のようにして、スパンのすべての回線で強制切り替えを開始します。

- a. Perform UPSR span switching フィールドをクリックします。
- b. ドロップダウン リストから FORCE SWITCH AWAY を選択します。
- c. Apply をクリックします。
- d. Confirm UPSR Switch ダイアログボックスで、Yes をクリックします。
- e. 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 ダイアログボックスにあるすべての回線の Switch State 値が FORCE になります。保護されていない回線は、切り替わりません。

**ステップ 4** 次の手順を実行して、強制切り替えをクリアします。

- a. Perform UPSR span switching フィールドをクリックします。
- b. ドロップダウン リストから CLEAR を選択します。
- c. Apply をクリックします。
- d. Confirm UPSR Switch ダイアログボックスで、Yes をクリックします。
- e. 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 UPSR 回線の Switch State が CLEAR になります。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A95 DS-1 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-1 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、送信元の起点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、回線の送信元となる DS1-14、DS1N-14、DS1/E1-56、DS3XM-6、または DS3XM-12 カードが存在するスロットを選択します。



(注) VT 回線の送信元および宛先は、ポートレス集約回線の STS グルーミング エンドポイント上に設定できます。

- ステップ 3** カードとして DS3XM-6 または DS3XM-12 を選択した場合は、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** DS-1 ドロップダウン リストから送信元 DS-1 を選択します。
- ステップ 5** セカンダリ送信元を作成する場合は (マルチベンダー UPSR における UPSR ブリッジまたはセレクト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 ~ 4 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 6](#) へ進みます。
- ステップ 6** **Next** をクリックします。
- ステップ 7** 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 8** Slot ドロップダウン リストから、宛先カードが存在するスロットを選択します。宛先は、通常、DS-1 カードです。OC-N 転送の場合は、OC-N カードを選択して DS-1 を VT1.5 にマップすることもできます。
- ステップ 9** [ステップ 8](#) 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、宛先カードに応じて宛先ポート、STS、VT、または DS1 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。ほかの回線で使用されているポート、STS、VT、または DS1 は、CTC に表示されません。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 DS1 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 10** 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ト回線の出口ポイントなど) **Use Secondary Destination** をクリックし、ステップ 7 ~ 9 を繰り返してセカンダリ宛先を定義します。
- ステップ 11** **Next** をクリックします。
- ステップ 12** 元の NTP (手順) に戻ります。

## DLP-A96 DS-1 または DS-3 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した DS-1 または DS-3 回線の回線ルートを実行します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71) 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/Edit 領域で送信元ノードのアイコンがまだ選択されていない場合は、そのアイコンをクリックして選択します。
- ステップ 2** 送信元ノードにあるスパンから開始して、回線を通させるスパンの矢印をクリックしていきま。矢印がイエローになります。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。送信元 STS および VT (DS-1 回線のみ) が表示されます。
- ステップ 3** 送信元 STS を変更する場合は、Source STS 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** DS-1 回線の送信元 VT を変更する場合は、Source VT 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。



(注) DS-3 回線の VT はグレー (使用不可) です。

- 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** Circuit Routing Preferences パネルで Fully Protect Path チェックボックスがオンになっている場合は、次の作業を行います。
- 送信元から宛先までの回線ルートにあるすべての UPSR 部分または保護されていない部分に対しては、2 つのスパンを追加します。
  - 送信元から宛先までのルートにあるすべての BLSR 部分または 1+1 部分に対しては、1 つのスパンを追加します。
  - UPSR DRI トポロジーの中でルーティングされる回線については、DRI ノード間のスパンと同様に、現用パスと保護パスを実行します。
- ステップ 7** 中継ノードも含めて回線が送信元から宛先まですべて実行されるまで、[ステップ 2 ~ 6](#)を繰り返します。
- ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A97 OC-N 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、OC-N 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、回線の送信元と宛先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、回線の始点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、回線の始点になる OC-N カードが取り付けられているスロットを選択します。(伝送容量を使い切っているカードは、リストに表示されません)
- ステップ 3** 回線の送信元カードに応じて、Port リストと STS リストから送信元ポートまたは STS またはその両方を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS は、別の回線によってすでに使用されている場合は、表示されません。



(注)

表示される STS は、カード、回線のサイズ、および保護方式によって異なります。たとえば、UPSR の OC-12 カードに STS-3c 回線を作成する場合は、4 つの STS しか使用できません。また、BLSR の OC-12 カードに STS-3c 回線を作成する場合は、BLSR の保護特性のため、2 つの STS しか使用できません。

- 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 UPSR における UPSR ブリッジまたはセレクト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。
- 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、回線の宛先となる OC-N カード(宛先カード)が存在するスロットを選択します(伝送容量を使い切っているカードは、リストに表示されません)。
- ステップ 8** ステップ 2 で選択したカードに合わせて、Port ドロップダウン リストと STS ドロップダウン リストから、宛先ポートまたは STS またはその両方を選択します。Port ドロップダウン リストは、カードに複数のポートがある場合にだけ使用できます。表示される STS は、カード、回線のサイズ、および保護方式によって異なります。
- 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ト回線の入口ポイントなど) **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-A99 使用可能な VLAN の判別

目的	この作業では、E シリーズ回線の作成に必要な新しい VLAN (仮想 LAN) に対して、ネットワークに十分な伝送容量があることを確認します。この手順は、ポートマップ モードの E シリーズ カードには適用できません。
工具 / 機器	E シリーズ イーサネット カード (E100T-12/E100T-G、E1000-2/E1000-2-G) がイーサネット回線の両端に取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A127 ネットワークの起動の確認 (p.6-5)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** CTC のいずれかのビューで、**Circuits** タブをクリックします。

**ステップ 2** 既存のイーサネット回線をクリックします。

**ステップ 3** **Edit** をクリックしてから、**VLANs** タブをクリックします。

Edit Circuit ダイアログボックスに、回線で使用されている VLAN の数と使用可能な VLAN の合計数が表示されます。

**ステップ 4** 表示された使用可能な VLAN の数が、作成する E シリーズ イーサネット回線の数だけ十分にあるかどうかを判別します。



### 注意

スパニングツリーがイネーブルになっている複数の E シリーズ イーサネット回線が、同じ E シリーズ イーサネット カードを通過していて、しかも同じ VLAN を使用していると、それらの回線は互いにブロックしあいます。

**ステップ 5** 元の NTP (手順) に戻ります。





## DLP A100 ~ A199

---

### DLP-A111 アラーム履歴のセッション エントリ最大数の変更

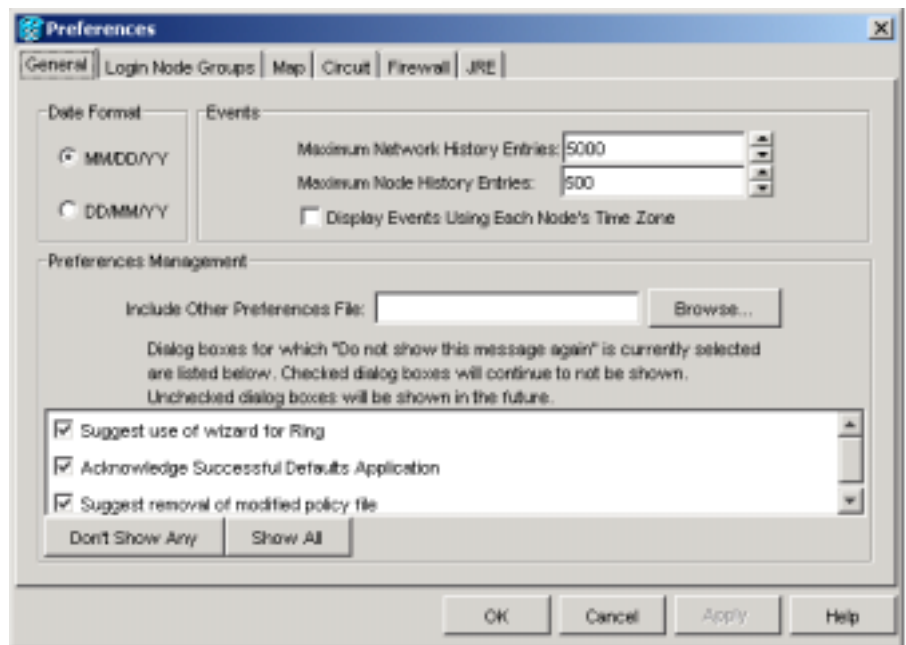
目的	この作業では、アラーム履歴に記録できるセッション エントリの最大数を変更します。履歴リストには、将来の参照やトラブルシューティングで使用する情報が保存されます。この作業は、その履歴リストを拡張するときに使用します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル

---

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


Cisco Transport Controller (CTC) の Preferences ダイアログボックスが表示されます ( [図 18-1](#) )。


図 18-1 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る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-A112 時間帯に合わせたアラームおよび状態の表示

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 18-1)。

**ステップ 2** **Display Events Using Each Node's Time Zone** 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-A113 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のレベルで発生した ONS 15454 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、アラームおよび状態の変化 (発生またはクリア) を調べる时候にも使用します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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-A114 状態の表示

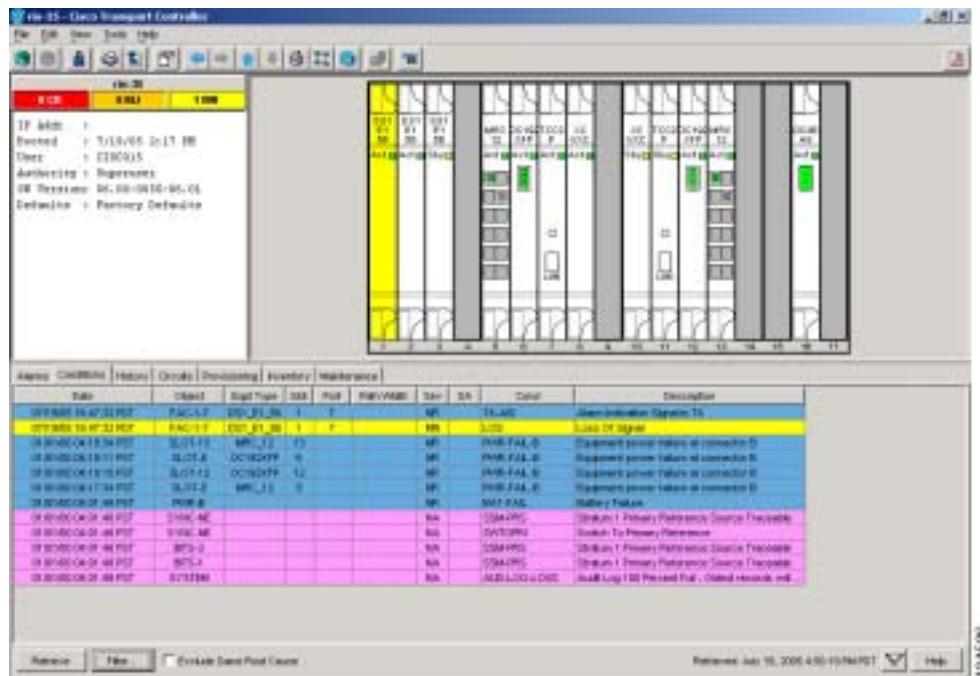
目的	この作業は、カード、ノード、またはネットワークのレベルで状態 (重大度が Not Reported [NR] のイベント) を表示するときに使用します。Conditions ウィンドウからは、アラームに至らなかった変化やイベントの記録が詳細に得られます。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71)
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

**ステップ 1** 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 18-2)。

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、ウィンドウは更新されません。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 18-2 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-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。

重大度が Major (MJ)、Minor (MN)、または Critical (CR) で報告されるイベントはアラームです。Not Alarmed (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 Not Reported (NR) のマークが付きます。

重大度が Critical (CR)、Major (MJ)、Minor (MN)、または Not Alarmed (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。



(注) アラーム抑制の詳細については、「[DLP-A522 アラーム レポートの抑制](#)」(p.22-21) を参照してください。

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-A71 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.8-8) を参照してください。



(注) ポートのサービス状態が Out-of-Service and Management, Maintenance (OOS-MA,MT) になると、Alarms Suppressed for Maintenance (AS-MT) 状態が発生します。アラームおよび状態のトラブルシューティングについては、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。

**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、AIS 状態、および SF 状態が発生しますが、**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。Telcordia に従って、除外規則は「ノードからのすべての状態」の照会に適用されます。

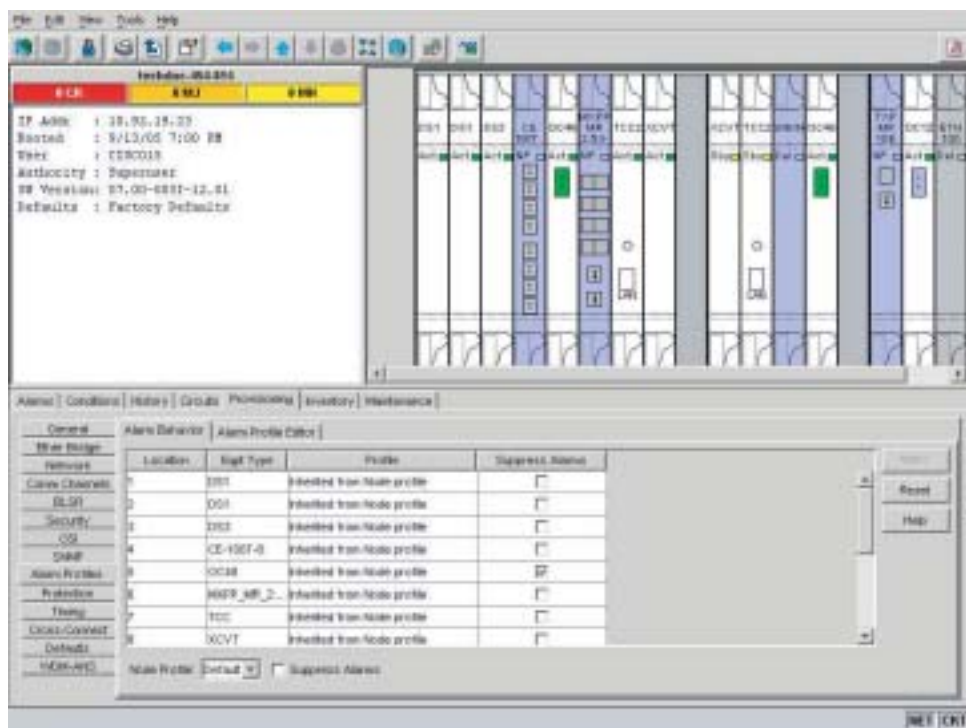
**ステップ 4** 元の NTP (手順) に戻ります。

## 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

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-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、Provisioning > Alarm Profiles > Alarm Behavior タブをクリックします( 図 18-3 )。

図 18-3 ノード ビューの Alarm Behavior ウィンドウ



**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 カラムで選択する項目をクリックします。
- 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 18-3 )。

- 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** 元の手順 (NTP) に戻ります。

## DLP-A121 ポインタ位置調整カウンタの PM のイネーブル化またはディセーブル化

<b>目的</b>	この作業では、ポインタ位置調整カウンタをイネーブルまたはディセーブルにして、Synchronous Transport Signal ( STS; 同期転送信号 ) 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モニタしたりできるようにします。ポインタ位置調整カウンタの状態が大きい値のまま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。
<b>工具 / 機器</b>	なし
<b>事前準備手順</b>	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
<b>必須 / 適宜</b>	適宜
<b>オンサイト / リモート</b>	オンサイトまたはリモート
<b>セキュリティ レベル</b>	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、モニタ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。

Line Terminating Equipment ( LTE; 回線終端装置 ) カードのリストについては、[表 18-1](#) を参照してください。

**表 18-1 回線を終端するための OC-N カード (LTE)**

LTE
EC1-12
OC3 IR 4/STM1 SH 1310
OC3 IR4/STM1 SH 1310-8
OC12 LR/STM4 LH 1310
OC12 IR/STM4 SH 1310
OC12 IR/STM4 SH 1310-4
OC12 LR/STM4 LH 1550
OC48 LR 1550
OC48 IR 1310
OC48 LR/STM16 LH AS 1550
OC48 IR/STM16 SH AS 1310
OC48 ELR 200 GHz
OC48 ELR/STM16 EH 100 GHz
OC192 SR/STM64 IO 1310

表 18-1 回線を終端するための OC-N カード (LTE)(続き)

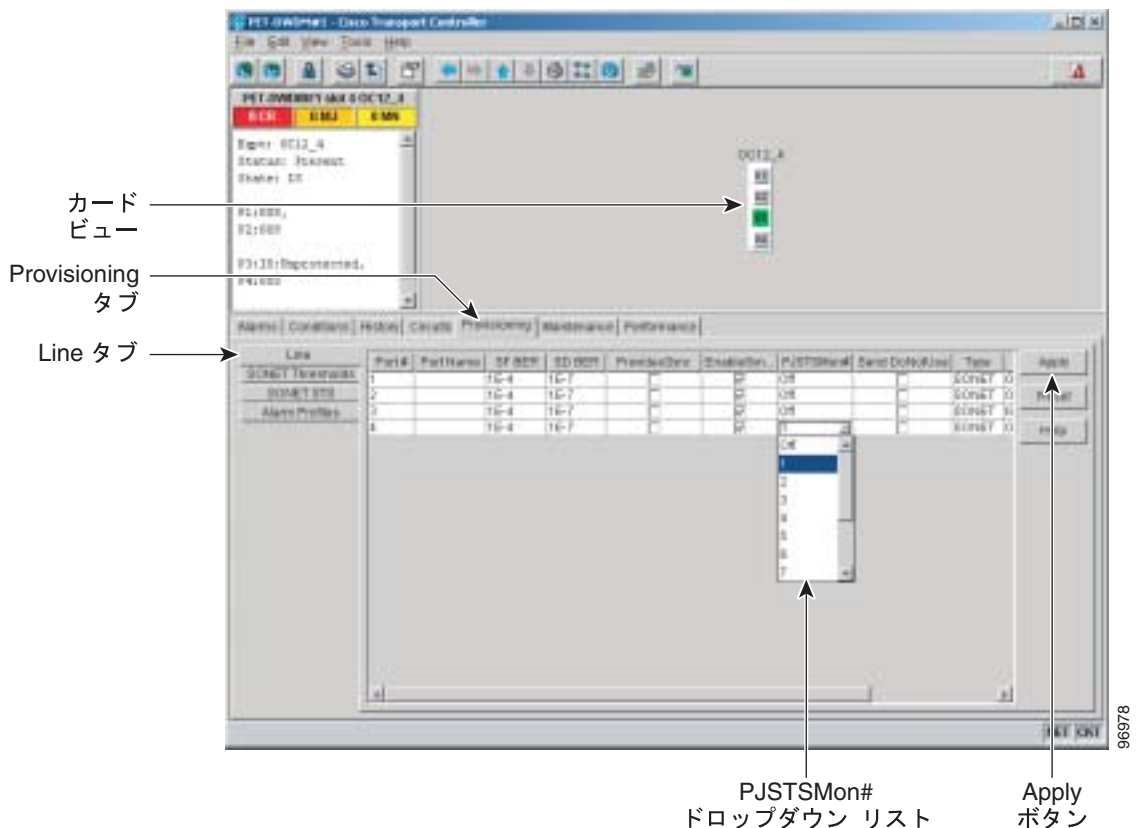
LTE
OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550
OC192 ELR/STM64 LH ITU 15xx.xx

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

**ステップ 3** PJSTSMon# ドロップダウン リストから、次の規則に基づいて選択します (図 18-4)。

- 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 STS の番号です。PJSTSMon# カード ドロップダウン リストを使用して、ポートごとに STS を 1 つイネーブルにできます。

図 18-4 ポインタ位置調整カウンタ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 4** Service State フィールドで、ポートのサービス状態が In-Service and Normal (IS-NR) になっていることを確認します。

**ステップ 5** ポートの状態が IS-NR になっている場合は、Apply をクリックします。ポートが Out-of-Service and Management, Disabled (OOS-MA,DSBLD)、Out-of-Service and Management, Maintenance (OOS-MA,MT)、または Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) サービス状態の場合、Admin State ドロップダウン リストから IS を選択して、Apply をクリックします。



**ステップ 6** Performance タブをクリックして、Performance Monitoring (PM; パフォーマンス モニタリング) パラメータを表示します。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。



(注) ポインタ位置調整カウンターの PM がイネーブルになっていないと、PPJC と NPJC PM パラメータのカウンターフィールドは白黒で表示されます。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A122 IPPM のイネーブル化またはディセーブル化

目的	この作業では、Intermediate Path Performance Monitoring (IPPM; 中間パス パフォーマンス モニタリング) をイネーブルまたはディセーブルにします。IPPM をイネーブルにすることによって、中継ノードに流れる大量の STS トラフィックをモニタできるようになります。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 でモニタできるパラメータは、STS CV-P、STS ES-P、STS SES-P、STS UAS-P、および STS FC-P です。遠端側のパス モニタリングは、OC3-4 と EC-1 カードで実行できます。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。



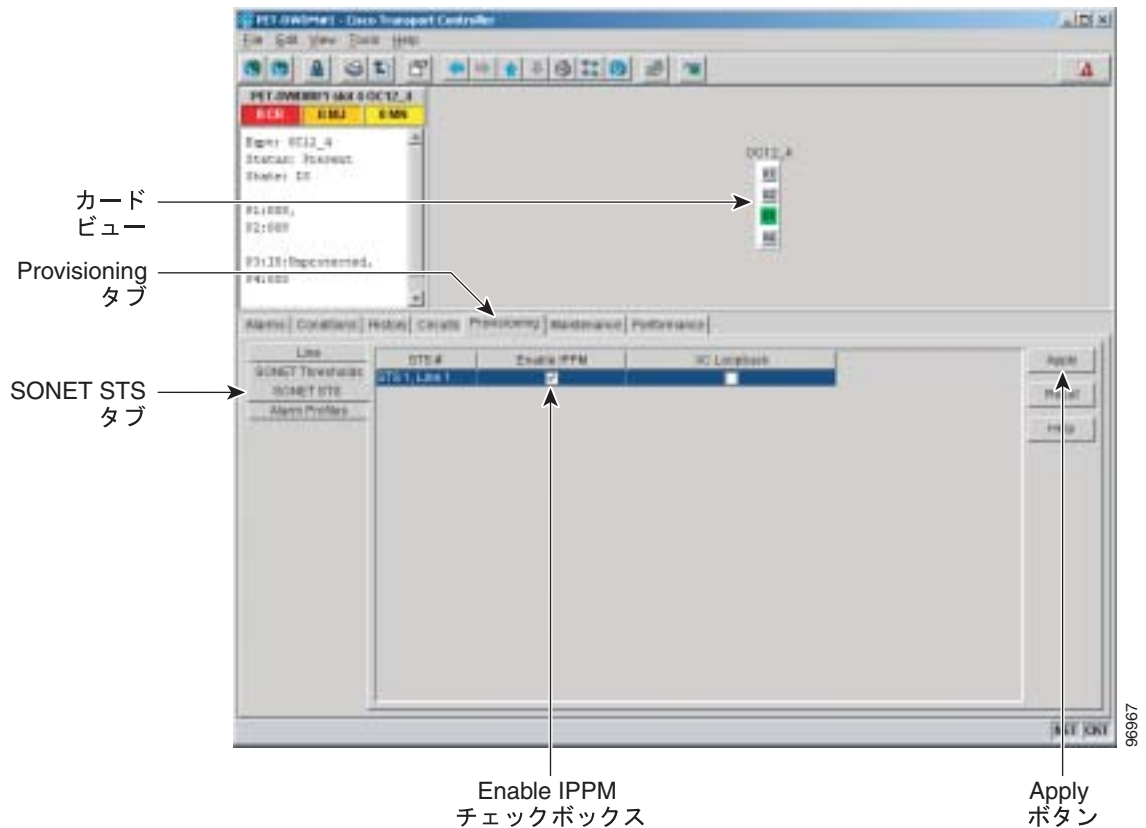
(注) 保護切り替え中、BLSR で使用されている OC-48 IR カードは IPPM をサポートしません。

**ステップ 1** ノード ビューで、モニタする 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。

OC-N LTE カードのリストについては、[表 18-1](#) を参照してください。

**ステップ 2** Provisioning > SONET STS タブをクリックします (図 18-5)。

図 18-5 IPPM をイネーブルまたはディセーブルにするための SONET STS 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 STS の IPPM をディセーブルにします (デフォルト)。
- チェックボックスがオン — その STS の IPPM をイネーブルにします。

**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 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-A124 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

モニタ対象のパフォーマンスパラメータには、現在のインターバルに対するスレッシュホールド値がそれぞれあります。カウンタの値が個々のインターバル（選択したインターバル）のスレッシュホールド値を超えると、スレッシュホールド超過アラート（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ト値を表しています。

- ステップ 6** Prev-*n* カラムを表示し、15 分間隔で表示される以前の 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、ポートのサービス状態が変更された、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、次のインターバル（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-A125 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 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。

モニタ対象のパフォーマンスパラメータには、現在のインターバルに対するスレッシュホールド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スレッシュホールド値を超えると、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ト値を表しています。

**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、ポートのサービス状態が変更された、といったような原因が考えられます。問題を解決すると、次のインターバル(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-A126 近端側の PM カウントの表示

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。選択したカードに対して着信信号で発生したすべての 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 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、現在のインターバルの 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、以前のインターバルの 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-A127 遠端側の PM カウントの表示

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 パラメータを表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

## ■ DLP-A129 現在の PM カウントのリセット

- 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信号で記録された 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 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、現在のインターバルの 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、以前のインターバルの 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-A129 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。



**(注)** Baseline ボタンをクリックすると、現在のインターバルで表示されている 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。現在のインターバルが終了した場合やウィンドウ表示を変更した場合は、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 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、現在のインターバルの PM カウントが変化の様子を観察します。
- ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A131 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 回線を検索します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Go to Network View** をクリックします。
- 特定のノードを送信元または着信先とする回線、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 > Go to Other Node** をクリックして検索するノードを選択し、**OK** をクリックします。
- 特定のカードを送信元または着信先とする回線、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、画面の右下にある **Scope** ドロップダウン リストで、検索の範囲を選択します (**Node** または **Network (All)**)

**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った場合に次の回線を検索するには、**Find Next** をもう一度クリックします。

**ステップ 7** ステップ 5 と 6 を繰り返します。検索を終了するには **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-A137 OC-N ポートでの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 OC-N ポートにおけるパストレースをモニタします。
工具 / 機器	モニタ対象の OC-N ポートは、パストレースを受信できる OC-N カードに存在する必要があります。表 19-3 (p.19-52) を参照してください。
事前準備手順	DLP-A264 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.19-51)  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** 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上で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 STS 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、ウィンドウ下部にある **Show Detailed Map** チェックボックスをクリックします。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 OC-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)** OC-N ポートは、表 19-3 (p.19-52) 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。OC-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。
- ステップ 7** Path Trace Mode フィールドを Manual に設定した場合は、OC-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、詳細な回線マップ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、回線の送信元または宛先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-A140 ノード名、日付、時刻、および連絡先情報の変更

目的	この手順では、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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 Savings Time
- AIS-V Insertion On STS-1 Signal Degrade - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degrade - Path: SD-P BER

フィールドの詳細については、「[NTP-A25 名前、日付、時刻、連絡先情報の設定](#)」(p.4-6) 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-A142 スタティック ルートの変更

目的	この作業では、ONS 15454 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A65 スタティック ルートの作成 (p.17-78)</a>
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-A65 スタティック ルートの作成](#)」(p.17-78) 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-A143 スタティック ルートの削除

目的	この作業では、ONS 15454 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A65 スタティック ルートの作成 (p.17-78)</a>
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-A144 OSPF のディセーブル化

目的	この作業では、ONS 15454 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	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a> <a href="#">DLP-A250 OSPF プロトコルの設定または変更 ( p.19-39 )</a>
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 > 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-A145 ネットワーク ビューの背景色の変更

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	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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-A148 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 のアイコンをグループ化するためのアイコンです。デフォルトでは、ネットワークにログインしているすべての CTC セッションに対してドメインが表示されます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) 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に表示されます。

---



(注) あらゆるセキュリティ レベルのユーザがローカルドメイン、つまりホーム CTC セッションのみに表示されるドメインを作成できるようにするためには、スーパーユーザが CTC.network.LocalDomainCreationAndViewing NE デフォルト値を TRUE に設定します。値が TRUE ということは、あらゆるユーザが自分のユーザ設定ファイルにドメイン情報を保持でき、ドメインを変更しても他の CTC セッションには影響を与えないことを意味します (デフォルト値は FALSE で、ドメイン情報がすべての CTC セッションに影響を与え、スーパーユーザだけがドメインを作成したり、ノードをドメインに追加したりできることを意味します)。NE デフォルト値の変更については、「[NTP-A336 NE のデフォルト値の編集 \(p.15-44\)](#)」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** 元の NTP (手順) に戻ります。

## DLP-A149 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 アイコンを管理します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A148 ドメイン アイコンの作成 (p.18-20)</a>
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)** ノードの追加や削除といったすべてのドメインの変更は、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)** あらゆるセキュリティ レベルのユーザがローカル ドメイン、つまりホーム CTC セッションのみに表示されるドメインを作成できるようにするためには、スーパーユーザが CTC.network.LocalDomainCreationAndViewing NE デフォルト値を TRUE に設定します。値が TRUE ということは、あらゆるユーザが自分のユーザ設定ファイルにドメイン情報を保持でき、ドメインを変更しても他の CTC セッションには影響を与えないことを意味します (デフォルト値は FALSE で、ドメイン情報がすべての CTC セッションに影響を与え、スーパーユーザだけがドメインを作成したり、ノードをドメインに追加したりできることを意味します)。NE デフォルト値の変更については、「[NTP-A336 NE のデフォルト値の編集 \(p.15-44\)](#)」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 18-2](#) 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 18-2 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	Ctrl キーを押しながら、ドメイン アイコンを新しい場所にドラッグ 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 <b>Rename Domain</b> 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。

表 18-2 ドメインの管理操作 (続き)

ドメインの操作	手順
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。 <b>Move Node Back to Parent View</b> を選択します。
ドメインを開く	<ul style="list-style-type: none"> <li>ドメイン アイコンをダブルクリックします。</li> <li>ドメインを右クリックし、<b>Open Domain</b> を選択します。</li> </ul>
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 <b>Go to Parent View</b> 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、 <b>Show Domain Overview</b> を選択します。ドメイン アイコンではドメイン内の各ノードが小さなプレビューとなって表示されます。ドメインの一覧表示を変更する場合は、その表示を右クリックして、 <b>Show Domain Overview</b> 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、 <b>Remove Domain</b> を選択します。ドメインのノードは、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-A150 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 (DS-1、DS-3、EC-1、および DS3XM) 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	<a href="#">DLP-A71 1:1 保護グループの作成 (p.17-85)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 — 必要に応じて、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 文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場合に、トラフィックを現用カードに戻すには、このチェックボックスをオンにします。トラフィックを現用カードに戻さないようには、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 リストから復帰時間を選択します。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。



(注) 電気保護グループを変換する場合は、「NTP-A91 DS-1 および DS-3 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-A152 1:N 保護グループの変更

目的	この作業では、DS-1 カードと DS-3 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-A72 1:N 保護グループの作成 (p.17-86) 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** DS-1 または DS-3 カードが、「DLP-A72 1:N 保護グループの作成」(p.17-86) 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、ここに新しい名前を入力します。保護グループの名前は、32 文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-A72 1:N 保護グループの作成」(p.17-86) を参照してください。

**ステップ 5** Apply をクリックします。



(注) 電気保護グループを変換する場合は、「NTP-A91 DS-1 および DS-3 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-A154 1+1 保護グループの変更

目的	この作業では、光ポート (OC-3、OC-12、OC-12 IR、OC-48、OC-48AS、および OC-192) 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-A73 1+1 保護グループの作成 (p.17-87) 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 > 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、ここに新しい名前を入力します。保護グループの名前は、32 文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場合に、トラフィックを現用カードに戻すには、このチェックボックスをオンにします。トラフィックを現用カード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 リストから復帰時間を選択します。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-A73 1+1 保護グループの作成](#)」(p.17-87)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。



## DLP-A155 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 字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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** をクリックします。
- ステップ 5** 元の NTP (手順) に戻ります。
- 

## DLP-A156 SDCC 終端の削除

目的	この作業では、ONS 15454 にある SONET Section DCC (SDCC) 終端を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Comm Channel > SDCC タブをクリックします。
- ステップ 2** 削除する SDCC の終端をクリックして、Delete をクリックします。Delete SDCC Termination ダイアログボックスが表示されます。
- ステップ 3** 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** 元の NTP (手順) に戻ります。
-

## DLP-A157 ノードのタイミングソースの変更

目的	この作業では、ONS 15454 の SONET 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

**ステップ 1** ノード ビューで、**Provisioning > Timing** 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。

- SSM Message Set
- Quality of RES
- Revertive
- Revertive Time

フィールドの説明については、「[DLP-A69 外部タイミングまたはライン タイミングの設定 \(p.17-81\)](#)」を参照してください。

**ステップ 3** BITS Facilities セクションで、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、BITS1 タイミング基準と BITS2 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。機器のタイミングを BITS Out から取得していれば、その機器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。

- BITS In State
- BITS Out State
- State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- LBO

**ステップ 4** 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、バックプレーンにあるノードの BITS Out ピンに接続可能な機器で使用されるタイミング基準を定義します。機器を BITS Out ピンに接続する場合は、特別なことがないかぎり、ライン モードでノードに接続します。機器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 5** 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-A158 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

目的	この作業では、既存ユーザの設定を 1 つのノードで変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > 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てから、Change をクリックします。

**ステップ 3** Change User ダイアログボックスで、次の作業を行います。

- ユーザパスワードの変更
- ユーザのセキュリティ レベルの変更
- ユーザのロックアウト

フィールドの説明については、「[NTP-A30 ユーザの作成とセキュリティの割り当て](#)」(p.4-5)を参照してください。

**ステップ 4** 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 5** 元の NTP（手順）に戻ります。

## DLP-A159 ユーザの削除：単一ノード

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)** 現在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-A315 ユーザのログアウト：単一ノード](#)」(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、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、CISCO15 ユーザは、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したい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。

**ステップ 6** 元の NTP（手順）に戻ります。

## DLP-A160 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

目的	この作業では、既存ユーザの設定を複数のノードで変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

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、次の作業を行います。
  - ユーザパスワードの変更
  - ユーザのセキュリティ レベルの変更
  - ユーザのロックアウトフィールドの説明については、「[DLP-A75 新規ユーザの作成：複数ノード](#)」(p.17-90)を参照してください。
- ステップ 5** Select Applicable Nodes 領域で、ユーザの設定を変更しないノードのチェックをオフにします（デフォルトでは、すべてのネットワーク 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-A161 ユーザの削除：複数ノード

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) 現在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-A316 ユーザのログアウト：複数ノード](#)」(p.20-10)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、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、CISCO15 ユーザは、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** 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** Select Applicable Nodes 領域で、このユーザを削除したくないノードをオフにします。
- ステップ 5** **OK** をクリックします。User Deletion Results 確認用のダイアログボックスが表示されます。
- ステップ 6** **OK** をクリックして、変更を許可します。
- ステップ 7** 元の NTP (手順) に戻ります。
- 

## DLP-A163 SNMP トラップ宛先の削除

目的	この作業では、ONS 15454 の SNMP (簡易ネットワーク管理プロトコル) トラップ宛先を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。
- ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A165 DS1-14 または DS1N-14 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、DS1-14 または DS1N-14 カードの回線および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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 DS1-14 または DS1N-14 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 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 18-3 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 18-4 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 18-5 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 18-6 を参照してください。

表 18-3 に、Provisioning > Line タブの値を示します。

**表 18-3 DS1-14 と DS1N-14 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 ~ 14
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。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビットエラー レートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• D4</li> <li>• ESF - Extended Super Frame (拡張スーパーフレーム)</li> <li>• Unframed</li> </ul>
Line Coding	DS-1 伝送符号化タイプを定義します。	<ul style="list-style-type: none"> <li>• AMI - Alternate Mark Inversion(交互マーク反転) (デフォルト)</li> <li>• B8ZS - Bipolar 8 Zero Substitution</li> </ul>
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)を定義します。	<ul style="list-style-type: none"> <li>• 0 ~ 131</li> <li>• 132 ~ 262</li> <li>• 263 ~ 393</li> <li>• 394 ~ 524</li> <li>• 525 ~ 655</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>



表 18-3 DS1-14 と DS1N-14 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
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>

表 18-4 に、Provisioning > Line Thresholds タブの値を示します。

表 18-4 DS1-14 と DS1N-14 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 ~ 14)
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
LOSS	1 つまたは複数の Loss of Signal (LOS; 信号損失) 障害が発生した 1 秒間の間隔です。
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 18-5 に、Provisioning > Elect Path Thresholds タブの値を示します。

**表 18-5 DS1-14 と DS1N-14 カードの電気回路バス 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 ~ 14)
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
SAS	重大エラー フレーム / アラーム表示信号
AISS	アラーム表示信号秒数
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。

表 18-6 に、DS-1 カードに対する Provisioning > SONET Thresholds タブの値を示します。

**表 18-6 DS1-14 と DS1N-14 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) STS に対して分割されている DS-1 ポート Line 1, STS 1、Line 2, STS 1 Line 3, STS 1、Line 4, STS 1
CV	符号化違反数
ES	エラー秒数
FC	障害カウント
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値は、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-A166 DS3-12 または DS3N-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、DS3-12 または DS3N-12 カードの回線および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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 回線またはスレッシュホールドの設定変更を行う DS3-12 または DS3N-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 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 18-7 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 18-8 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 18-9 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 18-10 を参照してください。

表 18-7 に、Provisioning > Line タブの値を示します。

**表 18-7 DS3-12 または DS3N-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	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビットエラーレートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 0 ~ 225 (デフォルト)</li> <li>• 226 ~ 450</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

表 18-7 DS3-12 または DS3N-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
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
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 (0 ~ 48 時間、15 分刻み)。この時間が経過すると、カードが自動的にイン サービス状態 (IS) へ変わります。

表 18-8 に、Provisioning > Line Thresholds タブの値を示します。

表 18-8 DS3-12 または DS3N-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	LOS 秒数。1 つまたは複数の LOS 障害が発生した 1 秒間の間隔です。
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 18-9 に、Provisioning > Elect Path Thresholds タブの値を示します。

表 18-9 DS3-12 または DS3N-12 カードの電気回路バス 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)
EB	エラー ブロック数
BBE	バックグラウンド ブロック エラー数
ES	エラー秒数
SES	重大エラー秒数
UAS	使用不可秒数
AISS	アラーム表示信号秒数
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。

表 18-10 に、Provisioning > SONET Thresholds タブの値を示します。

表 18-10 DS3-12 または DS3N-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) STS に対して分割されている DS-3 ポート Line 1, STS 1、Line 2, STS 1 Line 3, STS 1、Line 4, STS 1
CV	(近端および遠端、STS 終端のみ) 符号化違反数
ES	(近端および遠端、STS 終端のみ) エラー秒数
FC	(近端および遠端、STS 終端のみ) 障害カウント
SES	(近端および遠端、STS 終端のみ) 重大エラー秒数
UAS	(近端および遠端、STS 終端のみ) 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値は、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-A167 DS3E-12 または DS3N-12E 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、DS3E-12 または DS3N-12E (DS3E) カードの回線および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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。



(注) DS-3 カード用にプロビジョニングされている ONS 15454 スロットに DS-3E が取り付けられている場合、DS3E 拡張 PM パラメータは使用できません。この場合、ONS 15454 から DS3E を取り外し、『[DLP-A191 カードの削除](#)」(p.18-65) を使用して CTC の DS-3 カードを削除し、『[DLP-A330 カードスロットの事前プロビジョニング](#)」(p.20-22) を使用して DS3E 用にスロットをプロビジョニングします。

- ステップ 1** 回線またはスレッシュホールドの設定変更を行う DS3E-12 または DS3N-12E 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 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 18-11 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 18-12 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 18-13 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 18-14 を参照してください。

表 18-11 に、Provisioning > Line タブの値を示します。

**表 18-11 DS3-12E と DS3N-12E 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	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビットエラーレートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• M13</li> <li>• C Bit</li> <li>• Auto Provisioned</li> </ul>
Detected Line Type	(表示専用) 検出された回線のタイプを表示します。	<ul style="list-style-type: none"> <li>• M13</li> <li>• C Bit</li> <li>• Unframed</li> <li>• Unknown</li> </ul>
Line Coding	DS3E 伝送符号化タイプを指定します。	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。	<ul style="list-style-type: none"> <li>• 0 ~ 225 (デフォルト)</li> <li>• 226 ~ 450</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>



表 18-11 DS3-12E と DS3N-12E 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
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>OOS-MA,MT — (Out-of-Service and Management, Maintenance) ポートはメンテナンスのためにア停止しています。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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>

表 18-12 に、Provisioning > Line Thresholds タブの値を示します。

表 18-12 DS3-12E と DS3N-12E 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	LOS 秒数。1 つまたは複数の LOS 障害が発生した 1 秒間の間隔です。
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 18-13 に、Provisioning > Elect Path Thresholds タブの値を示します。

表 18-13 DS3-12E と DS3N-12E カードの電気回路バス オプション

パラメータ	内容
Port	(表示専用) ポート番号 (1 ~ 12)
CV	符号化違反数。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、近端および遠端。
ES	エラー秒数。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、近端および遠端。
SES	重大エラー秒数。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、近端および遠端。
SAS	重大エラー フレーム / アラーム表示信号。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、近端および遠端。
AIS	アラーム表示信号秒数。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、近端および遠端。
UAS	使用不可秒数。DS3 Pbit で利用可能、近端専用 ; および DS3 Cpbit、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 18-14 に、Provisioning > SONET Thresholds タブの値を示します。

表 18-14 DS3-12E と DS3N-12E 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) STS に対して分割されている DS-3 ポート Line 1, STS 1、Line 2, STS 1 Line 3, STS 1、Line 4, STS 1
CV	符号化違反数。近端および遠端で利用可能、STS 終端専用。
ES	エラー秒数。近端および遠端で利用可能、STS 終端専用。
FC	障害カウント。近端および遠端で利用可能、STS 終端専用。
SES	重大エラー秒数。近端および遠端で利用可能、STS 終端専用。
UAS	使用不可秒数。近端および遠端で利用可能、STS 終端専用。
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値は、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-A168 DS3XM-6 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、DS3XM-6 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) DS3XM-6 ( Transmux ) カードは、最大 6 つのチャネライズド DS-3 信号を受け入れ、各信号を 28 の VT1.5 信号に変換します。反対に、カードは 28 の T-1 をチャネライズド C ビットまたは M13 フレームド DS-3 に多重化できます。



(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 DS3XM-6 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 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 18-15 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 18-16 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 18-17 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 18-18 を参照してください。

表 18-15 に、DS3XM-6 カードに対する Provisioning > Line タブの値を示します。

**表 18-15 DS3XM-6 パラメータの回線オプション**

パラメータ	内容	オプション
Port	(表示専用)ポート番号を設定します	1 ~ 6
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	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビット エラーレートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• M13 (デフォルト)</li> <li>• C BIT</li> </ul>
Line Coding	使用される DS-1 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。	<ul style="list-style-type: none"> <li>• 0 ~ 225 (デフォルト)</li> <li>• 226 ~ 450</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

表 18-15 DS3XM-6 パラメータの回線オプション (続き)

パラメータ	内容	オプション
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>

表 18-16 に、DS3XM-6 カードに対する Provisioning > Line Thresholds タブの値を示します。

表 18-16 DS3XM-6 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 ~ 6)
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
LOSS	LOS 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。

表 18-17 に、DS3XM-6 カードに対する Provisioning > Elect Path Thresholds タブの値を示します。

表 18-17 DS3XM-6 カードの電気回路バス 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 ~ 6。
CV	符号化違反数。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
ES	エラー秒数。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
SES	重大エラー秒数。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
SAS	重大エラー フレーム / アラーム表示信号。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
AISS	アラーム表示信号秒数。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
UAS	使用不可秒数。DS3 で利用可能、Pbit は近端のみ、DS3 Cpbit、近端および遠端 ; DS1 はポートで VT 回線が廃棄される場合のみ。
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 18-18 に、DS3XM-6 カードに対する Provisioning > SONET Thresholds タブの値を示します。

表 18-18 DS3XM-6 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
CV	符号化違反数
ES	エラー秒数
FC	障害カウント
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値は、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-A169 EC1-12 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、EC1-12 (EC-1) 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 EC-1 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 または SONET Thresholds 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) STS サブタブは、IPPM をプロビジョニングするのに使用します。IPPM をプロビジョニングするには、回線が EC1-12 カードでプロビジョニングされている必要があります。回線の作成手順については[第 6 章「回線と VT トンネルの作成」](#)を、また、IPPM のプロビジョニングについては「[DLP-A121 ポインタ位置調整カウンターの PM のイネーブル化またはディセーブル化](#)」(p.18-7) をそれぞれ参照してください。



(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。

表 18-19 に、EC1-12 カードの Line タブの値を示します。SONET スレッシュホールドの設定の定義については、表 18-20 を参照してください。

**表 18-19 EC1-12 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	(任意) ポートの名前を設定します。	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。デフォルトは空白です。  「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	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビット エラー レートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
PJStsMon#	ポインタの位置調整に使用される STS を設定します。ゼロに設定すると、STS が使用されません。	<ul style="list-style-type: none"> <li>• 0 (デフォルト)</li> <li>• 1</li> </ul>
Line Buildout	バックプレーンから次の終端地点までの距離 (フィート単位) を定義します。	<ul style="list-style-type: none"> <li>• 0 ~ 225 (デフォルト)</li> <li>• 226 ~ 450</li> </ul>
Rx Equalization	EC1-12 カードの旧バージョンでは、回線の長さが短い場合や極寒地域の場合、イコライゼーションをオフにすることができます。Rx Equalization は通常 On に設定します。	<ul style="list-style-type: none"> <li>• On (オン、デフォルト)</li> <li>• Off (オフ)</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>



表 18-19 EC1-12 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
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>

表 18-20 に、EC1-12 カードの SONET Thresholds タブの値を示します。

表 18-20 EC1-12 カードの SONET スレッシュホールド オプション

SONET レイヤ	パラメータ	内容
すべて	Port #	(表示専用) EC-1 カードのポート番号 ( 1 ~ 12 )
Line ( L )	CV	符号化違反数
	ES	エラー秒数
Line ( L )	SES	重大エラー秒数
	FC	障害カウント
	UAS	使用不可秒数
Section ( S )	CV	符号化違反数 ( 近端のみ )
	ES	エラー秒数
	SES	重大エラー秒数
	SEFS	重大エラー フレーム秒数

表 18-20 EC1-12 カードの SONET スレッシュホールド オプション (続き)

SONET レイヤ	パラメータ	内容
Path ( P )	CV	符号化違反数 ( 近端および遠端 )
	ES	エラー秒数
	FC	障害カウント
	SES	重大エラー秒数
	UAS	使用不可秒数

**ステップ 7** 元の NTP ( 手順 ) に戻ります。

## DLP-A171 OC-N カードのスレッシュホールドの設定変更

目的	この作業では、OC-N カードの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	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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、スレッシュホールドの設定を変更する OC-N カードをダブルクリックします。

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









**(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 3** 変更したいフィールドをクリックして希望の値を入力し、[表 18-21](#) にある設定を変更します。

**ステップ 4** Apply をクリックします。

表 18-21 OC-N スレッシュホールド オプション

パラメータ	内容
Port	ポート番号 <ul style="list-style-type: none"> <li>• 1 (OC-3、OC-12、OC-48、OC-192)</li> <li>• 1 ~ 4 (OC12-4)</li> <li>• 1 ~ 12 : PPM 1 (MRC_12)</li> </ul>
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
SEFS	重大エラー フレーム秒数
FC	障害カウント
UAS	使用不可秒数
PSC	保護切り替えカウント (回線)
PSD	保護切り替え持続時間 (回線)
PSC-W	保護切り替えカウント — 現用回線   <b>(注)</b> OC-3 カードでは Bidirectional Line Switch Ring (BLSR; 双方向ラインスイッチ型リング) がサポートされていません。このため、PSC-W、PSD-S、および PSC-R PM は増分されません。
PSD-W	保護切り替え持続時間 — 現用回線   <b>(注)</b> OC-3 カードでは BLSR がサポートされていません。このため、PSD-W、PSD-S、および PSD-R PM は増分されません。
PSC-S	保護切り替え持続カウント — スパン   <b>(注)</b> OC-3 カードでは BLSR がサポートされていません。このため、PSC-W、PSC-S、および PSC-R PM は増分されません。
PSD-S	保護切り替え持続時間 — スパン   <b>(注)</b> OC-3 カードでは BLSR がサポートされていません。このため、PSD-W、PSD-S、および PSD-R PM は増分されません。
PSC-R	保護切り替えカウント — リング   <b>(注)</b> OC-3 カードでは BLSR がサポートされていません。このため、PSC-W、PSC-S、および PSC-R PM は増分されません。
PSD-R	保護切り替え持続時間 — リング   <b>(注)</b> OC-3 カードでは BLSR がサポートされていません。このため、PSD-W、PSD-S、および PSD-R PM は増分されません。

**ステップ 5** 元の NTP（手順）に戻ります。

## DLP-A172 SDH への光ポートの変更

目的	この作業では、OC-N カードのポートを SDH 用にプロビジョニングします。ポートを SDH 用に変更する前に、ポートを OOS,MT 管理サービス状態にする必要があります。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A214 ポートのサービス状態の変更 (p.19-10)</a>
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、ポートを SDH 用にプロビジョニングする OC-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** 対象ポートの Type フィールドで、**SDH** を選択します。



**(注)** ポート タイプを SDH に変更する前に、EnableSyncMsg と SendDoNotUse フィールドがオフになっていること、カードが BLSR または 1+1 保護グループの一部になっていないこと、カードがオーダーワイヤ チャネルの一部になっていないこと、カードが SONET Data Communication Channel/Generic Communication Channel (DCC/GCC) 終端地点になっていないことを確認します。

**ステップ 4** Apply をクリックします。

**ステップ 5** カードがマルチポート OC-N カード（たとえば、4 ポート OC-3、8 ポート OC-3、4 ポート OC-12、または MRC-12）の場合、そのカードの他のポートについて **ステップ 3** および **4** を繰り返すことができます。

**ステップ 6** 元の NTP（手順）に戻ります。

## DLP-A176 DS1-14 カードの 1:1 保護から 1:N 保護への変換

目的	この作業では、1:1 保護スキームの DS1-14 カードを 1:N 保護に変換します。1:N 保護グループでは、最大で 5 つの現用カードを保護できません。
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
セキュリティ レベル	プロビジョニング以上のレベル



(注)

この作業では、DS1-14 カードがスロット 1 ~ 6 およびスロット 12 ~ 17 (またはいずれか一方) に取り付けられていることを想定しています。保護スロットであるスロット 3 および 15 にある DS1-14 カードは、DS1N-14 カードに置き換えられます。

- 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** (DS1N-14 カードの取り付け先となる)スロット 3 または 15 を含む保護グループをクリックします。
- ステップ 3** アップグレードするスロットに現用トラフィックが流れていないことを確認します。Selected Group リストにある保護スロットのステータスは、Protect/Active ではなく、Protect/Standby になっている必要があります。保護スロットのステータスが Protect/Active になっている場合は、トラフィックを現用カードに切り替えます。
- Selected Group で、保護カードをクリックします。
  - Switch Commands の隣にある、Switch をクリックします。  
現用スロットのステータスが Working/Active に変わり、保護スロットのステータスが Protect/Standby に変わります。変わらない場合は、作業を続けしないでください。現用のカードとスロットにある問題を調べ、カードに現用トラフィックが流れない原因を突き止めてください。
- ステップ 4** 変換が必要な保護グループごとに、ステップ 1 ~ 3 を繰り返します。
- ステップ 5** Alarms タブをクリックして、変換しているどの DS1-14 カードにも未解決のアラームがないことを確認します。アラームが解除できない場合は、上位レベルのサポートに連絡してください。
- ステップ 6** Provisioning > Protection タブをクリックします。
- ステップ 7** 新しい保護グループへ移動するカードが含まれている 1:1 保護グループをクリックします。
- ステップ 8** Delete をクリックします。
- ステップ 9** 確認用のダイアログボックスが表示されたら、Yes をクリックします。



(注) 1:1 保護グループを削除しても、サービスは中断されません。ただし、1:N 保護の手順が完了するまでは、現用回線を保護するための帯域幅がありません。したがって、この手順はできるだけ早く完了させてください。

**ステップ 10** 必要に応じて、1:N グループに含める他の DS-1 1:1 保護グループに対してステップ 7 ~ 9 を繰り返します。

**ステップ 11** DS1-14 カードをスロット 3 またはスロット 15 から物理的に取り外します。これにより、不適切な取り外しのアラーム状態 (IMPROPRMVL) が発生します。

**ステップ 12** ノード ビューで、取り外されたカードが取り付けられていたスロットを右クリックして、ショートカット メニューから **Delete** を選択します。ノード ビューからカードが表示されなくなるまで待ちます。

**ステップ 13** DS1N-14 カードを同じスロットへ物理的に挿入します。

**ステップ 14** カードが正常にブートすることを確認します。

**ステップ 15** **Inventory** タブをクリックして、新しいカードが DS1N-14 カードとして表示されていることを確認します。

**ステップ 16** **Provisioning > Protection** タブをクリックします。

**ステップ 17** **Create** をクリックします。

**ステップ 18** **Name** フィールドに、保護グループの名前を入力します (任意)。

**ステップ 19** **Type** ドロップダウン リストから **1:N (card)** を選択します。

**ステップ 20** **Protect Card** ドロップダウン リストから、DS1N-14 カードを選択します。**Protect Card** フィールドに適切な DS1N-14 カードが表示されていることを確認します。

**ステップ 21** **Available Cards** リストで、保護グループに入れるカードを強調表示します。矢印(>>)タブをクリックして、カードを **Working Cards** リストへ移動します。

**ステップ 22** **Reversion time** ドロップダウン リストで、必要に応じて新しい復元時間を設定します。



(注) 1:N 保護グループは常にリバーティブです。

**ステップ 23** **OK** をクリックします。**Protection** サブタブの **Protection Groups** リストに、保護グループが表示されます。

**ステップ 24** 元の手順 (NTP) に戻ります。

## DLP-A177 DS3-12 カードの 1:1 保護から 1:N 保護への変換

目的	この作業では、DS3-12 カードを 1:1 保護から 1:N 保護に変換します。1:N 保護グループでは、最大で 5 つの現用カードを保護できます。
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
セキュリティ レベル	プロビジョニング以上のレベル



(注)

この手順では、DS3-12 カードがスロット 1 ~ 6 およびスロット 12 ~ 17 (またはいずれか一方) に取り付けられていることを想定しています。保護スロットであるスロット 3 または 15 にある DS3-12 カードは、DS3N-12 カードに置き換えられます。ONS 15454 では、Release 2.0 以降の CTC が実行されている必要があります。また、この手順には 1 つ以上の DS3N-12 カードと、DS3-12 カードを使用する保護グループが必要です。

- 
- 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** (DS3N-12 カードの取り付け先となる)スロット 3 または 15 を含む保護グループをクリックします。
- ステップ 3** アップグレードするスロットに現用トラフィックが流れていないことを確認します。Selected Group リストにある保護スロットのステータスは、Protect/Active ではなく、Protect/Standby になっている必要があります。保護スロットのステータスが Protect/Active になっている場合は、トラフィックを現用カードに切り替えます。
- Selected Group で、保護カードをクリックします。
  - Switch Commands の隣にある、Switch をクリックします。
- 現用スロットのステータスが Working/Active に変わり、保護スロットのステータスが Protect/Standby に変わります。変わらない場合は、作業を続けしないでください。現用のカードとスロットにある問題を調べ、カードに現用トラフィックが流れない原因を突き止めてください。
- ステップ 4** 変換の必要な保護グループごとに、ステップ 2 と 3 を繰り返します。
- ステップ 5** Alarms タブをクリックして、変換しているどの DS3-12 カードにも未解決のアラームがないことを確認します。アラームが解除できない場合は、上位レベルのサポートに連絡してください。
- ステップ 6** Provisioning > Protection タブをクリックします。
- ステップ 7** 新しい保護グループへ移動するカードが含まれている 1:1 保護グループをクリックします。
- ステップ 8** Delete をクリックします。
- ステップ 9** 確認用のダイアログボックスが表示されたら、Yes をクリックします。



(注) 1:1 保護グループを削除しても、サービスは中断されません。ただし、1:N 保護の手順が完了するまでは、現用回線を保護するための帯域幅が存在しません。したがって、この手順はできるだけ早く完了させてください。

**ステップ 10** 複数の DS-3 1:1 保護グループを削除する場合は、1:N グループに含める各グループに対してステップ 7 ~ 9 を繰り返します。

**ステップ 11** 保護 DS3-12 カードをスロット 3 またはスロット 15 から物理的に取り外します。これにより、不適切な取り外しのアラーム状態 (IMPROPRMVL) が発生します。

**ステップ 12** ノード ビューで、取り外されたカードが取り付けられていたスロットを右クリックして、ショートカット メニューから **Delete** を選択します。ノード ビューからカードが表示されなくなるまで待ちます。

**ステップ 13** DS3N-12 カードを同じスロットへ物理的に挿入します。

**ステップ 14** カードが正常にブートすることを確認します。

**ステップ 15** **Inventory** タブをクリックして、新しいカードが DS3N-12 カードとして表示されていることを確認します。

**ステップ 16** **Provisioning > Protection** タブをクリックします。

**ステップ 17** **Create** をクリックします。

**ステップ 18** **Name** フィールドに、保護グループの名前を入力します (任意)。

**ステップ 19** **Type** をクリックして、ドロップダウン リストから **1:N (card)** を選択します。

**ステップ 20** **Protect Card** フィールドに DS3N-12 カードが表示されていることを確認します。

**ステップ 21** **Available Cards** リストで、保護グループに入れるカードを強調表示します。矢印 (>>) タブをクリックして、カードを **Working Cards** リストへ移動します。

**ステップ 22** **OK** をクリックします。

Protection サブタブの **Protection Groups** リストに保護グループが表示されます。

**ステップ 23** 元の NTP (手順) に戻ります。



## DLP-A178 DS3-12E カードの 1:1 保護から 1:N 保護への変換

目的	この作業では、DS3-12E カードを 1:1 保護から 1:N 保護に変換します。1:N 保護グループでは、最大で 5 つの現用カードを保護できます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

この作業では、DS3-12E カードがスロット 1 ~ 6 およびスロット 12 ~ 17 (またはいずれか一方) に取り付けられていることを想定しています。保護スロットであるスロット 3 または 15 にある DS3-12E カードは、DS3N-12E カードに置き換えられます。この手順には 1 つ以上の DS3N-12E カードと、DS3-12E カードを使用する保護グループが必要です。

- 
- 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** (DS3N-12E カードの取り付け先となる) スロット 3 または 15 を含む保護グループをクリックします。
- ステップ 3** アップグレードするスロットに現用トラフィックが流れていないことを確認します。Selected Group リストにある保護スロットのステータスは、Protect/Active ではなく、Protect/Standby になっている必要があります。保護スロットのステータスが Protect/Active になっている場合は、トラフィックを現用カードに切り替えます。
- Selected Group で、保護カードをクリックします。
  - Switch Commands の隣にある、**Switch** をクリックします。
- 現用スロットのステータスが Working/Active に変わり、保護スロットのステータスが Protect/Standby に変わります。変わらない場合は、作業を続けしないでください。現用のカードとスロットにある問題を調べ、カードに現用トラフィックが流れない原因を突き止めてください。
- ステップ 4** 変換の必要な保護グループごとに、ステップ 2 と 3 を繰り返します。
- ステップ 5** Alarms タブをクリックして、変換しているどの DS3-12E カードにも未解決のアラームがないことを確認します。アラームが解除できない場合は、上位レベルのサポートに連絡してください。
- ステップ 6** Provisioning > Protection タブをクリックします。
- ステップ 7** 新しい保護グループへ移動するカードが含まれている 1:1 保護グループをクリックします。
- ステップ 8** Delete をクリックします。
- ステップ 9** 確認用のダイアログボックスが表示されたら、Yes をクリックします。



(注) 1:1 保護グループを削除しても、サービスは中断されません。ただし、1:N 保護の手順が完了するまでは、現用回線を保護するための帯域幅が存在しません。この手順はできるだけ早く完了させてください。

**ステップ 10** 複数の DS-3 1:1 保護グループを削除する場合は、1:N グループに含める各グループに対してステップ 7 ~ 9 を繰り返します。

**ステップ 11** 保護 DS3-12E カードをスロット 3 またはスロット 15 から物理的に取り外します。これにより、不適切な取り外しのアラーム状態 (IMPROPRMVL) が発生します。

**ステップ 12** ノード ビューで、取り外されたカードが取り付けられていたスロットを右クリックして、ショートカット メニューから **Delete** を選択します。ノード ビューからカードが表示されなくなるまで待ちます。

**ステップ 13** DS3N-12E カードを同じスロットへ物理的に挿入します。

**ステップ 14** カードが正常にブートすることを確認します。

**ステップ 15** **Inventory** タブをクリックして、新しいカードが DS3N-12E として表示されていることを確認します。

**ステップ 16** **Provisioning > Protection** タブをクリックします。

**ステップ 17** **Create** をクリックします。

**ステップ 18** **Name** フィールドに、保護グループの名前を入力します (任意)。

**ステップ 19** **Type** をクリックして、ドロップダウン リストから **1:N (card)** を選択します。

**ステップ 20** **Protect Card** フィールドに DS3N-12E カードが表示されていることを確認します。

**ステップ 21** **Available Cards** リストで、保護グループに入れるカードを強調表示します。矢印 (>>) タブをクリックして、カードを **Working Cards** リストへ移動します。


**ステップ 22** **OK** をクリックします。

Protection サブタブの **Protection Groups** リストに保護グループが表示されます。

**ステップ 23** 元の NTP (手順) に戻ります。

## DLP-A189 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であること）を確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 領域で、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。
- Selected Group 領域で、ステータスが Protect/Active になっているスロットを選択します。
  - Switch Commands フィールドで、**Manual** を選択します。
  - 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。アラームの説明と手順については、『Cisco ONS 15454 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。
- Switch Commands フィールドで、**Clear** を選択します。
  - 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 に戻っていないことを確認します。戻っている場合は、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-A190 UBIC-V EIA の取り付け

目的	この作業では、Universal Backplane Interface Connector — Vertical (UBIC-V) EIA を取り付けます。
工具 / 機器	#2 プラス ドライバ 小型スロット ヘッド ネジ用ドライバ 6本の周辺ネジ(6-32 × 0.375 インチのプラス ネジ)(P/N 48-0422-01) A 側 UBIC-V (15454-EIA-UBICV-A) EIA パネルおよび B 側 UBIC-V (15454-EIA-UBICV-B) EIA パネル (またはどちらか一方)
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
セキュリティ レベル	なし

**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず静電気防止用 (ESD) リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンド ケーブルを接続してください。

**(注)**

UBIC-V EIA を取り付けられるのは、15454-SA-HD シェルフ アセンブリだけです。15454-SA-HD シェルフ アセンブリは、ブルーの六角形の印で他のシェルフ アセンブリと区別されています。この印は、利用可能な高密度スロット (スロット 1 ~ 3 と 15 ~ 17) の下についています。

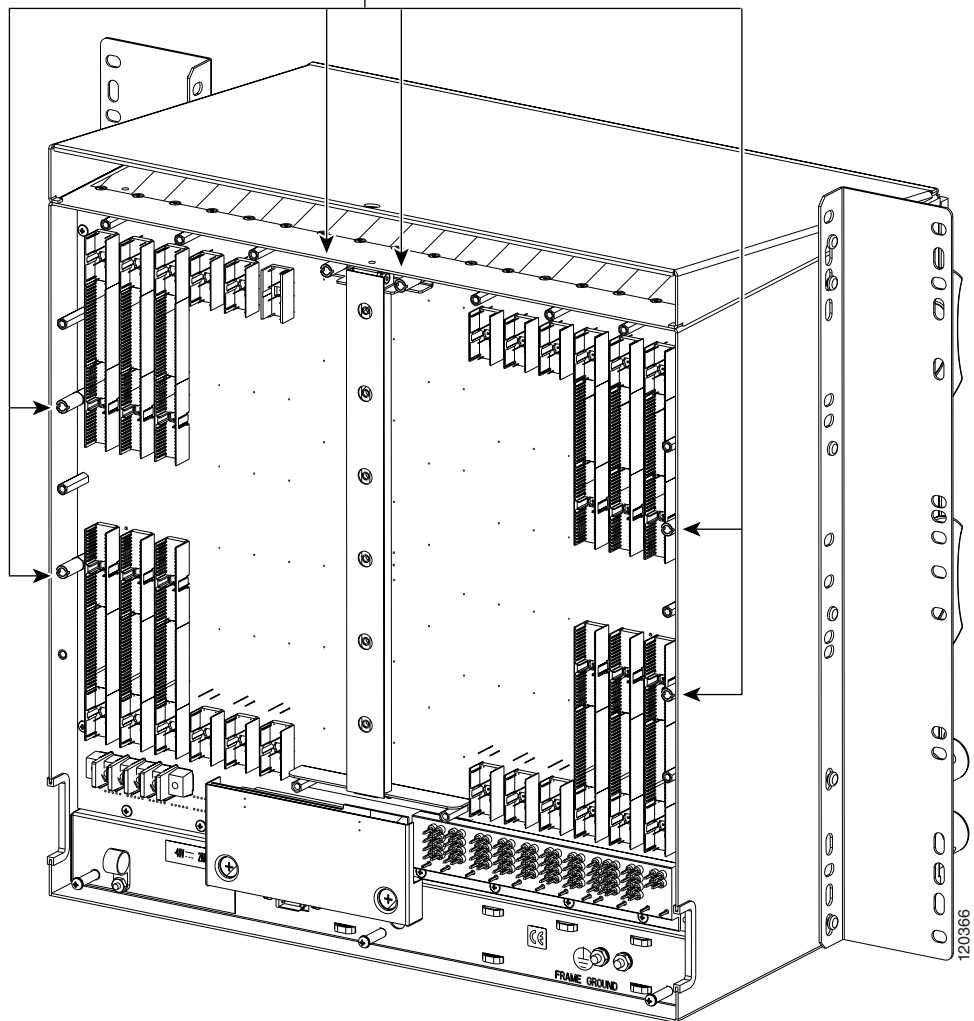
**(注)**

高密度の電気回路カード (48 ポートの DS-3 および 12 ポートの DS3XM) を使用する場合に、UBIC-V または UBIC-H EIA が必要になります。

- ステップ 1** 取り付けおよび取り外しを行う側に合った UBIC-V EIA を探し、パッケージから取り出します。
- ステップ 2** UBIC EIA のすべてのピンが曲がっていないことを確認します。
- ステップ 3** 曲がっているピンがある場合は、イエローのコネクタ プロテクタを取り外します。
- ステップ 4** ガイド スタンドオフの穴にネジが付いている場合は、プラス ドライバを使用して取り外します。
- ステップ 5** フラットヘッド ドライバまたは 5/16 インチのソケット レンチを使用して、スタンドオフを 8 ~ 10 pound-force-inch (lbf-in) (9.2 ~ 11.5 kilogram-force-centimeter [kgf-cm]) の力で締めます。図 18-6 では、シェルフに取り付けられたガイド スタンドオフを示しています。

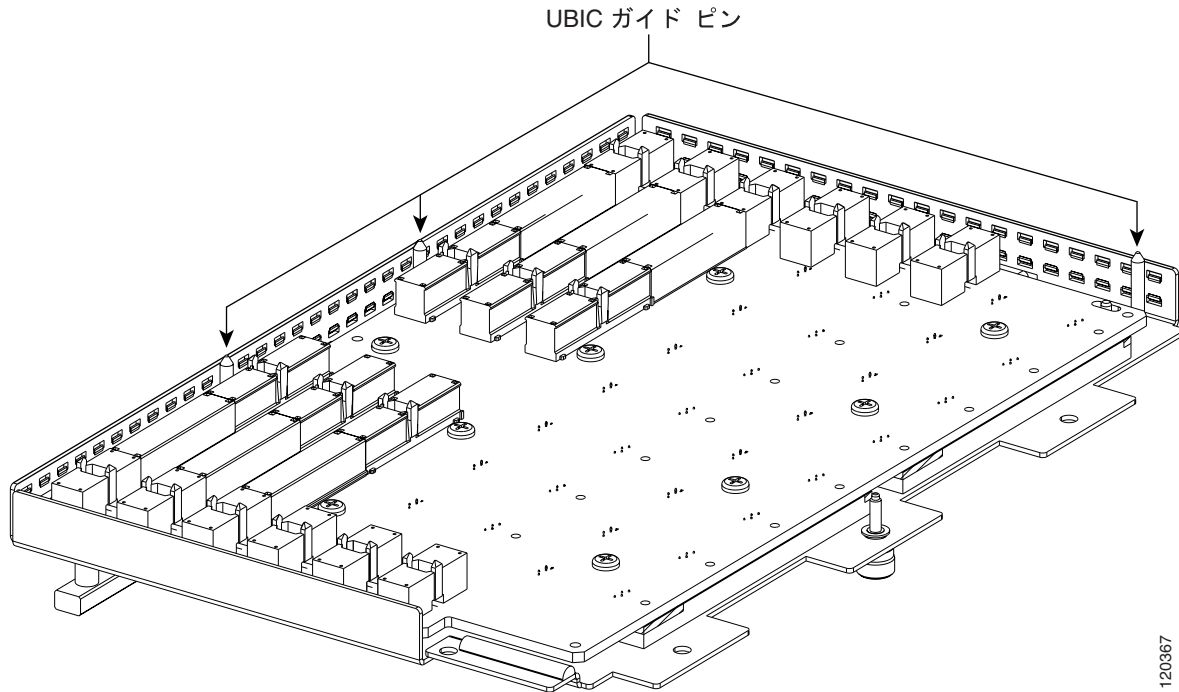
図 18-6 ガイド スタンドオフの取り付け

取り付けたガイド スタンドオフ



**ステップ 6** UBIC EIA のガイド ピンをシェルフのガイド スタンドオフの位置に合わせて、ピンとスタンドオフがしっかりと噛み合うまで UBIC EIA を一定の圧力で押し込みます (図 18-7)。

図 18-7 UBIC-V のガイド ピン



**注意**

強い抵抗感がある場合には、UBIC-V EIA を無理にシェルフに押し込まないでください。

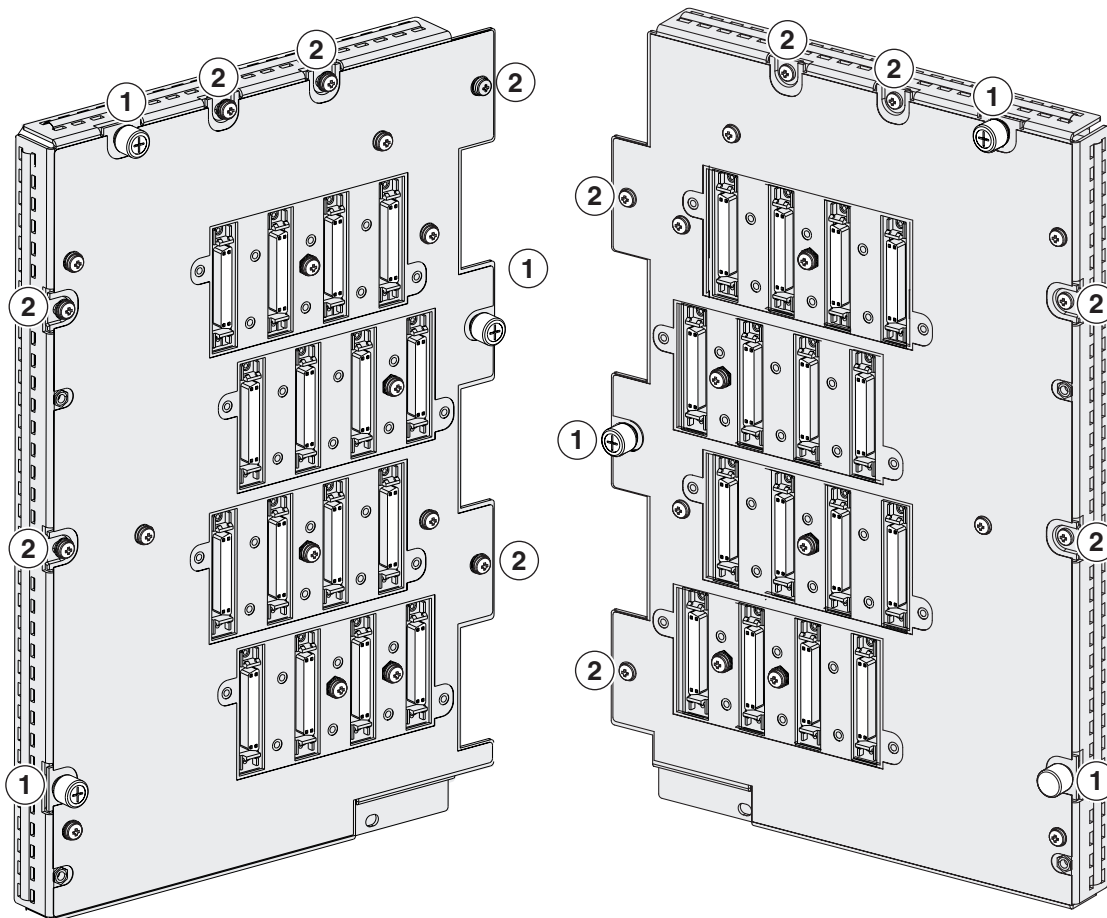
**ステップ 7** UBIC-V の 3 本のジャックネジを探します (図 18-8)。任意のジャックネジから始め、取り付けネジを数回まわして締めたら、次のネジに移ります。3 本のネジがすべて固く締まるまで、各取り付けネジを一度に数回ずつ順番にまわします (図 18-9)。



**注意**

均等にジャックネジを締めないと、UBIC-V コネクタが破損することがあります。

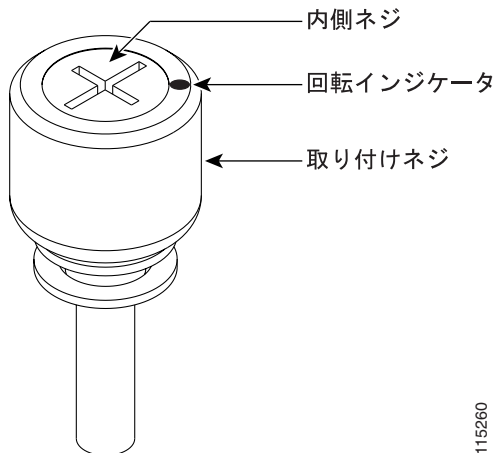
図 18-8 UBIC-V EIA ネジの位置



- ① ジャックネジ (3)
- ② 周辺ネジ、6-32 x 0.375 インチ プラス ネジ (6)

115140

図 18-9 UBIC-V EIA ジャックネジ

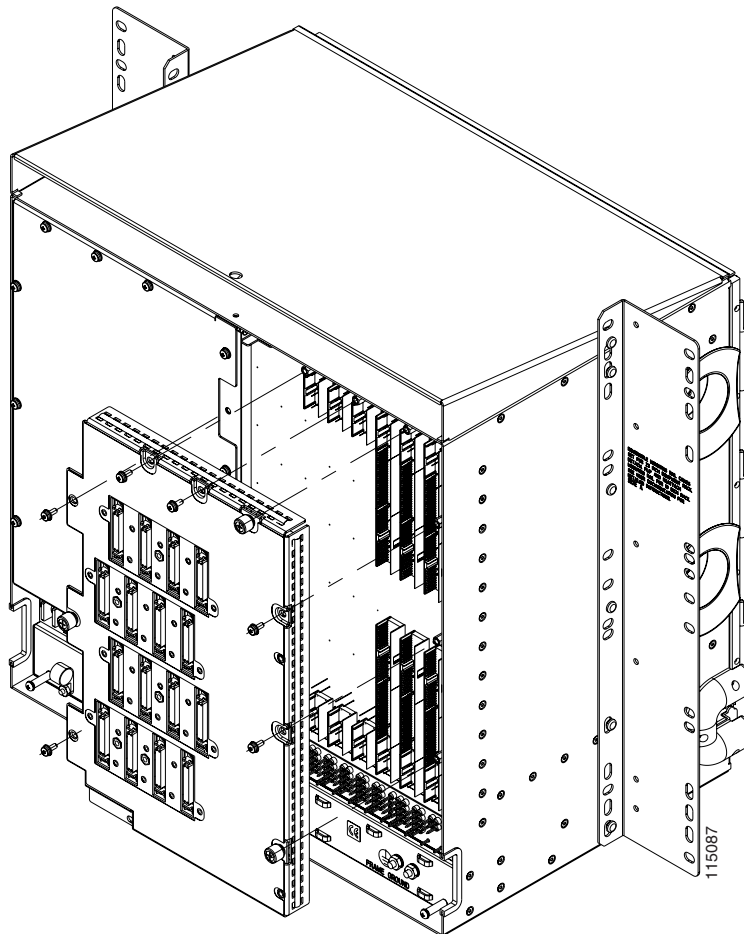


115260

**ステップ 8** プラス ドライバを使用して、6 本の周辺ネジとブラケット ネジ (P/N 48-0422-01) を 8 ~ 10 lbf-inch (9.2 ~ 11.5 kgf-cm) で取り付け、カバー パネルをバックプレーンに固定します (図 18-8)。アラームおよびタイミングパネルのカバーを取り付けてから、最後の周辺ネジを差し込んで、締めます。

図 18-10 に、UBIC-V EIA の取り付けを示します。

図 18-10 UBIC-V EIA の取り付け



**ステップ 9** 元の NTP (手順) に戻ります。



## DLP-A191 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** CTC のシェルフ図で取り外すカードを右クリックし、**Delete Card** を選択します。

次のいずれかの条件に該当している場合は、カードを削除できません。

- 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 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-A155 保護グループの削除](#)」(p.18-25) を参照してください。
- カードに回線がある。「[NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除](#)」(p.7-6) および「[DLP-A333 回線の削除](#)」(p.20-23) を参照してください。
- カードが BLSR の一部になっている。「[NTP-A240 BLSR ノードの削除](#)」(p.14-7) 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-A157 ノードのタイミングソースの変更](#)」(p.18-26) を参照してください。
- カードに DCC/GCC の終端がある。「[NTP-A292 通信チャネルの終端とプロビジョニング可能なパッチコードの変更または削除](#)」(p.11-7) 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、カードがリポートして再び CTC に表示されます。

**ステップ 2** 元の NTP (手順) に戻ります。

## DLP-A194 BLSR 強制リング切り替えのクリア

目的	この作業では、BLSR 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** View メニューから **Go to Network View** を選択します。

**ステップ 2** Provisioning > BLSR 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** ウェスト 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 BLSR のウェスト 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、プルダウン メニューから **CLEAR** を選択します。OK をクリックします。
- c. Confirm BLSR 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 BLSR 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、プルダウン メニューから **CLEAR** を選択します。OK をクリックします。
- c. Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

BLSR 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が、保護操作が起動されていないときの BLSR 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-A195 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイト / 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** 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 Lists 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** 削除したノードが唯一の BITS 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、同期に関する担当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すべて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-A157 ノードのタイミング ソースの変更](#)」(p.18-26) 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 and BITS-2 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。これにより、最初のノードを強制的に他のノードのプライマリ タイミング ソースにします（「[DLP-A157 ノードのタイミング ソースの変更](#)」[p.18-26] を参照）。



**(注)** この種類のタイミングは Stratum 3 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** 削除したノードが唯一の BITS タイミング ソースではない場合は、外部 BITS タイミング を使用するノードまで追跡可能なタイミング ソースとして、隣接ノードを SONET リンク（イーストとウェスト）を使用したライン タイミングにプロビジョニングします。「[NTP-A28 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-A196 単一ノードからの BLSR の削除

目的	この作業は、BLSR からノードを削除したあとに、ノードから BLSR を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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、BLSR 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** Provisioning > BLSR 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-A197 UPSR 強制切り替えの開始

目的	この作業では、UPSR スパンにある回線をすべて別のスパンに切り替えます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。



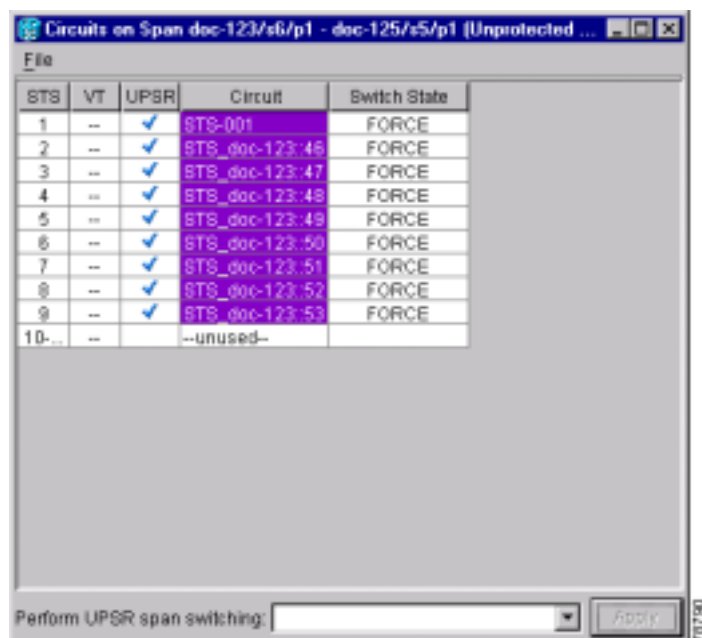
### 注意

強制保護の切り替え中は、トラフィックは保護されません。

- 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** UPSR 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 UPSR 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、すべての回線の Switch State が **FORCE** になります。[図 18-11](#) に、その例を示します。

図 18-11 強制切り替えが有効になった Circuits on Span ダイアログボックス



(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にすると、この状態もクリアされます。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A198 UPSR 強制切り替えのクリア

目的	この作業では、UPSR 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

## ■ DLP-A198 UPSR 強制切り替えのクリア

**ステップ 4** Confirm UPSR 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 UPSR 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。

---



## DLP A200 ~ A299

### DLP-A201 ロックオンの適用

目的	この作業では、トラフィックが1つのカードまたはポートから別のカードまたはポートに切り替わるのを回避します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



(注)

1:1 または 1:N 保護グループの保護カードにロックオンを適用するには、保護カードをアクティブにする必要があります。保護カードがスタンバイ状態にある場合、Lock On ボタンは無効になります。保護カードをアクティブにするには、トラフィックを現用カードから保護カードへ切り替える必要があります ([ステップ 4](#))。保護カードがアクティブになれば、ロックオンを適用できます。

**ステップ 1** 次のルールを使用して、ロックオンを適用できるかどうかを判断します。

- 1:1 電気回路保護グループでは、現用または保護カードにロックオンを適用できます。
- 1:N 電気回路保護グループでは、現用または保護カードにロックオンを適用できます。
- 1+1 光保護グループでは、現用ポートにのみロックオンを適用できます。

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

**ステップ 3** Protection Groups リストで、ロックオンを適用する保護グループをクリックします。

**ステップ 4** 保護カードがスタンバイ モードにあり、保護カードにロックオンを適用する場合は、保護カードをアクティブにします。

- a. Selected Group リストで、保護カードをクリックします。
- b. Switch Commands 領域で、**Force** をクリックします。

**ステップ 5** Selected Group リストで、トラフィックをロックするアクティブカードをクリックします。

**ステップ 6** Inhibit Switching 領域で、**Lock On** をクリックします。

**ステップ 7** 確認用のダイアログボックスで **Yes** をクリックします。

ロックオンが適用されて、トラフィックは現用カードに切り替えることができなくなります。ロックオンをクリアするには、「[DLP-A203 ロックオンまたはロックアウトのクリア](#)」(p.19-3)を参照してください。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A202 ロックアウトの適用

目的	この作業では、他の外部切り替えコマンド (Force、Manual、および Exercise) より優先される切り替えメカニズムであるロックアウトを使用して、トラフィックを 1 つのカードから別のカードへ切り替えま
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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	メンテナンス以上のレベル



(注) 同じ保護グループでの複数のロックアウトは許可されていません。

**ステップ 1** 次のルールを使用して、対象のカードをロックアウト状態にできるかどうかを判断します。

- 1:1 電気回路保護グループでは、現用または保護カードにロックアウトを適用できます。
- 1:N 電気回路保護グループでは、現用または保護カードにロックアウトを適用できます。
- 1:1 光保護グループでは、保護ポートにロックアウトを適用できます。

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

**ステップ 3** Protection Groups リストで、ロックアウトするカードを含む保護グループをクリックします。

**ステップ 4** Selected Group リストで、トラフィックをロックアウトするカードをクリックします。

**ステップ 5** Inhibit Switching 領域で、**Lock Out** をクリックします。

**ステップ 6** 確認用のダイアログボックスで **Yes** をクリックします。

ロックアウトが適用されて、トラフィックは反対のカードに切り替わります。ロックアウトをクリアするには、「[DLP-A203 ロックオンまたはロックアウトのクリア](#)」(p.19-3)を参照してください。





(注) ロックアウトをプロビジョニングすると、Cisco Transport Controller (CTC) で LOCKOUT-REQ 状態が発生します。スパンに適用された場合、FE-LOCKOUTOFPR-SPAN 状態も発生します。ロックアウト切り替え要求をクリアすると、これらの状態もクリアされます。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A203 ロックオンまたはロックアウトのクリア

目的	この作業では、ロックオンまたはロックアウトをクリアします。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71) DLP-A201 ロックオンの適用 (p.19-1) または DLP-A202 ロックアウトの適用 (p.19-2)
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	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** Protection Groups リストで、クリアするカードを含む保護グループをクリックします。

**ステップ 3** Selected Group リストで、クリアするカードをクリックします。

**ステップ 4** Inhibit Switching 領域で、Unlock をクリックします。

**ステップ 5** 確認用のダイアログボックスで Yes をクリックします。

ロックオンまたはロックアウトがクリアされます。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A204 アルコールと乾いた布によるファイバ コネクタとアダプタの検査および清掃

目的	この作業では、アルコールと乾いた布でファイバ コネクタとアダプタを清掃します。
工具 / 機器	圧縮空気 / ダスター 濃度 70% 以上のイソプロピル アルコール 光ファイバ用綿棒 光レシーバクリーニング スティック
事前準備手順	なし
必須 / 適宜	必須
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



## 警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器（ルーペ、拡大鏡、顕微鏡など）で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。

- 
- ステップ 1** ファイバ コネクタからダストキャップを外します。
- ステップ 2** あらかじめアルコールで湿らせた布でコネクタの先端を拭きます。
- ステップ 3** フィルタにかけた空気を吹き付けて乾かします。
- ステップ 4** 検査用のマイクروسコープを使用して、各ファイバ コネクタの汚れ、ひび、傷を検査します。コネクタが汚れている場合は、ステップ 1 ~ 3 を繰り返します。
- ステップ 5** ファイバ コネクタを該当するアダプタに差し込むか、ファイバ コネクタにダスト キャップを取り付けます。



**(注)** コネクタのダスト キャップを交換する必要がある場合は、まず、ダスト キャップが汚れていないことを確認してください。ダスト キャップを清掃するには、乾いた柔らかい布でキャップの外側を拭き、CLETOP 綿棒（14100400）でダスト キャップの内側を拭きます。

- ステップ 6** 元の NTP（手順）に戻ります。
-

## DLP-A205 CLETOP によるファイバ コネクタの清掃

目的	この作業では、CLETOP を使用してファイバ コネクタを清掃します。
工具 / 機器	タイプ A 光ファイバ コネクタ用クリーナー (CLETOP リール式) 光レシーバクリーニング スティック
事前準備手順	なし
必須 / 適宜	必須
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** ファイバ コネクタからダストキャップを外します。
- ステップ 2** レバーを下方向に押し、シャッター扉を開きます。レバーを押すたびに清潔な拭き取り面が現れます。
- ステップ 3** コネクタを CLETOP クリーニング カセット スロットに挿入し、90 度回して、ゆっくりと下方向に通します。
- ステップ 4** 検査用の顕微鏡を使用して、各ファイバ コネクタの汚れ、ひび、傷を検査します。コネクタが汚れている場合は、ステップ 1 ~ 3 を繰り返します。
- ステップ 5** ファイバ コネクタを該当するアダプタに差し込むか、ファイバ コネクタにダスト キャップを取り付けます。



**(注)** コネクタのダスト キャップを交換する必要がある場合は、まず、ダスト キャップが汚れていないことを確認してください。ダスト キャップを清掃するには、乾いた柔らかい布でキャップの外側を拭き、CLETOP 綿棒 (14100400) でダスト キャップの内側を拭きます。

- ステップ 6** 元の NTP (手順) に戻ります。
- 

## DLP-A206 ファイバ アダプタの清掃

目的	この作業では、ファイバ アダプタを清掃します。
工具 / 機器	CLETOP 綿棒
事前準備手順	なし
必須 / 適宜	必須
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** ファイバ アダプタからダスト プラグを外します。
- ステップ 2** CLETOP 綿棒 (14100400) をアダプタの開口部に挿入して、回転させます。

**ステップ 3** 使用しない場合には、ファイバアダプタにダスト プラグを取り付けます。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A207 LGX インターフェイスへの光ファイバケーブルの取り付け

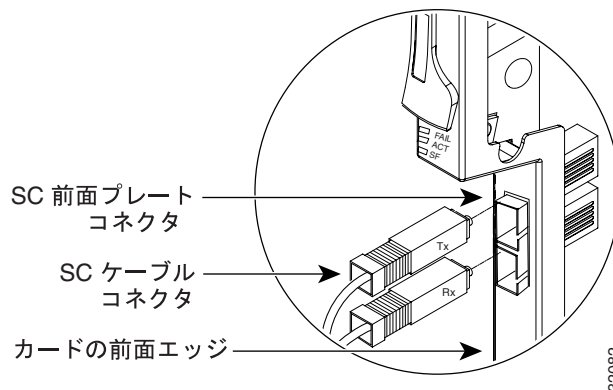
目的	この作業では、セントラル オフィスの Lightguide Cross Connect (LGX) インターフェイスに光ファイバケーブルを取り付けます。
工具 / 機器	光ファイバケーブル
事前準備手順	<a href="#">NTP-A112 ファイバ コネクタの清掃 (p.15-20)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし

**ステップ 1** ケーブル コネクタのキー付きの突起を、LGX 前面プレートの接続箇所にある受信 SC コネクタに合わせます。それぞれのモジュールには、光搬送ポートを作成するための送信コネクタと受信コネクタが少なくとも 1 つずつあります。

**ステップ 2** ケーブル コネクタを前面プレートの接続箇所に合わせてゆっくり挿入し、確実に取り付けます。

**ステップ 3** OC-N カードに光ファイバケーブルを接続します。図 19-1 に、ケーブルの接続位置を示します。

図 19-1 光ファイバケーブルの取り付け



**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A208 AIC-I カードを使用した外部アラームの変更

目的	この作業では、Alarm Interface Controller-International (AIC-I) カードの外部アラームの設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

Alarm Expansion Panel (AEP) を使用している場合、手順は同じですが、これに応じて画面に表示される接点数が変わります。

- 
- ステップ 1** 外部デバイスのリレーが ENVIR ALARMS IN バックプレーン ピンに配線されていることを確認します。詳細については、「[DLP-A19 バックプレーンへのアラーム ケーブルの取り付け](#)」(p.17-23) を参照してください。
- ステップ 2** AIC-I カードをダブルクリックして、カード ビューで表示させます。
- ステップ 3** Provisioning > External Alarms タブをクリックします。
- ステップ 4** ONS 15454 のバックプレーンに接続されているすべての外部デバイスについて、次の任意のフィールドを変更します。これらのフィールドの定義については、「[NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング](#)」(p.8-11) を参照してください。
- Enabled
  - Alarm Type
  - Severity
  - Virtual Wire
  - Raised When
  - Description
- ステップ 5** プロビジョニングするデバイスがほかにもある場合には、それらのデバイスに対して **ステップ 4** を実行します。
- ステップ 6** Apply をクリックします。
- ステップ 7** 元の NTP (手順) に戻ります。
-

## DLP-A209 AIC-I カードを使用した外部制御の変更

目的	この作業では、AIC-I カードの外部制御の設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

AEP を使用している場合、手順は同じですが、これに応じて画面に表示される接点数が変わります。

- 
- ステップ 1** ENVIR ALARMS OUT バックプレーン ピンへの外部制御のリレーを確認します。詳細については、「[DLP-A19 バックプレーンへのアラーム ケーブルの取り付け](#)」(p.17-23) を参照してください。
- ステップ 2** ノード ビューで AIC-I カードをダブルクリックし、カード ビューで表示させます。
- ステップ 3** External Controls サブタブで、ONS 15454 バックプレーンに接続された各外部制御について、次の任意のフィールドを変更します。これらのフィールドの定義については、「[NTP-A258 AIC-I カードへの外部アラームおよび制御のプロビジョニング](#)」(p.8-11) を参照してください。
- Enabled
  - Trigger Type
  - Control Type
  - Description
- ステップ 4** プロビジョニングする制御がほかにもある場合には、それらの制御に対して**ステップ 3** を実行します。
- ステップ 5** 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-A210 AIC-I カード オーダーワイヤ設定の変更

目的	この作業では、AIC-I カードのオーダーワイヤ設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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**

リングにある ONS 15454 のオーダーワイヤをプロビジョニングする場合は、オーダーワイヤ ループ全体をプロビジョニングしないでください。たとえば、4 ノードのリングでは、通常、4 つのノードすべてにイーストポートとウェストポートがプロビジョニングされていますが、オーダーワイヤループを防止するために、1 つのリングノードを除いて、他のノードに 2 つのオーダーワイヤポート（イーストとウェスト）をプロビジョニングしてください。

**ヒント**

プロビジョニングを開始する前に、オーダーワイヤ通信に必要な ONS 15454 のスロットおよびポートのリストを作成してください。

- 
- ステップ 1** ノードビューで AIC-I カードをダブルクリックし、カードビューに表示します。
- ステップ 2** 作成するオーダーワイヤパスに応じて、**Provisioning > Local Orderwire** タブ、または **Provisioning > Express Orderwire** タブをクリックします。プロビジョニングの手順は、どちらのタイプのオーダーワイヤでも同じです。
- ステップ 3** 必要に応じて、使用するヘッドセットのタイプ（4 線式または 2 線式）に合わせて、スライダを右または左に移動し、送信（Tx）dBm および受信（Rx）dBm を調整します。通常は、dBm を調整する必要はありません。
- ステップ 4** オーダーワイヤの音声アラート（ブザー）を有効にする場合は、**Buzzer On** チェックボックスをオンにします。
- ステップ 5** **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-A212 UDC 回線の作成

目的	この作業では、ONS 15454 ノードに User Data Channel（UDC）回線を作成します。UDC 回線により、ノード間に専用のデータチャンネルを作成できます。
工具 / 機器	OC-N カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A323 カードの取り付けの確認（p.4-2）</a> <a href="#">DLP-A60 CTC へのログイン（p.17-71）</a>
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で、**Provisioning > Overhead Circuits** タブをクリックします。
- ステップ 2** **Create** をクリックします。

## ■ DLP-A214 ポートのサービス状態の変更

- ステップ 3** Overhead Circuit Creation ダイアログボックスの Circuit Attributes 領域で次のフィールドを指定します。
- Name — 回線に名前を付けます。名前には、48 文字（スペースを含む）以下の英数字を指定します。
  - Type — ドロップダウン リストから **User Data-F1** または **User Data D-4-D-12** を選択します。（ONS 15454 が Dense Wavelength Division Multiplexing [ DWDM; 高密度波長分割多重 ] 用にプロビジョニングされている場合、User Data D-4-D-12 は選択できません。）
- ステップ 4** Next をクリックします。
- ステップ 5** Circuit Source 領域で次の項目を指定します。
- Node — 送信元ノードを選択します。
  - Slot — 送信元スロットを選択します。
  - Port — 表示された場合は、送信元ポートを選択します。
- ステップ 6** Next をクリックします。
- ステップ 7** Circuit Destination 領域で、次の項目を指定します。
- Node — 宛先ノードを選択します。
  - Slot — 宛先スロットを選択します。
  - Port — 表示された場合は、宛先ポートを選択します。
- ステップ 8** Finish をクリックします。
- ステップ 9** 元の NTP（手順）に戻ります。

## DLP-A214 ポートのサービス状態の変更

目的	この作業では、ポートのサービス状態を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)** E シリーズ イーサネット ポートのプロビジョニングについては、「[DLP-A220 E シリーズ イーサネットポートのプロビジョニング](#)」(p.19-15) を参照してください。

- ステップ 1** ノード ビューのシェルフ図で、稼働させるポートまたは停止するポートがあ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** G シリーズ以外のすべてのカードでは、**Provisioning > Line** タブをクリックします。G シリーズカードでは、**Provisioning > Port** タブを選択します。

**ステップ 3** ターゲット ポートの Admin State カラムで、ドロップダウン リストから次のいずれか 1 つを選択します。

- IS — ポートのサービス状態を In-Service and Normal ( IS-NR ) にします。
- OOS, DSBLD — ポートのサービス状態を Out-of-Service and Management, Disabled ( OOS-MA,DSBLD ) にします。このサービス状態では、サービス状態が IS-NR、Out-of-Service and Management, Maintenance ( OOS-MA,MT )、または Out-of-Service and Autonomous, Automatic In-Service ( OOS-AU,AINS ) に変わるまで、トラフィックはポートを通過できません。
- OOS, MT — ポートのサービス状態を OOS-MA,MT にします。このサービス状態では、トラフィック フローは中断されず、ループバックは許可されますが、アラーム報告は抑制されます。アラームが報告されているかどうかに関係なく、発生した障害状態は、CTC の Conditions タブまたは TL1 RTRV-COND コマンドを使用して検索できます。アラームを一時的にテストしたり、抑制したりする場合は、この OOS-MA,MT サービス状態を使用します。ループバックを行う前には、ポートが OOS-MA,MT サービス状態になっている必要があります。テストが完了したら、IS-NR または OOS-AU,AINS サービス状態に変更します。
- IS, AINS — ポートのサービス状態を OOS-AU,AINS にします。このサービス状態では、アラーム報告は抑制されますが、トラフィックは伝送され、ループバックは許可されます。ソーク期間が終了すると、ポートは IS-NR に変わります。アラームが報告されているかどうかに関係なく、発生した障害状態は、CTC の Conditions タブまたは TL1 RTRV-COND コマンドを使用して検索できます。

サービス状態の詳細については、『Cisco ONS 15454 Reference Manual』の付録「Administrative and Service States」を参照してください。

**ステップ 4** ポートがループバック ( OOS-MA,LPBK & MT ) になっている場合、Admin State を IS に設定しようとすると、確認ウィンドウに、ループバックが解除され、それによりサービスに影響が出ることが示されます。操作を続けるには Yes をクリックします。

**ステップ 5** Admin State を IS,AINS に設定した場合は、ソーク期間を AINS Soak フィールドに設定します。これは、信号が連続的に受信されたあと、ポートが OOS-AU,AINS サービス状態に留まっている期間です。ソーク期間が経過すると、ポートのサービス状態は IS-NR に変わります。

**ステップ 6** Apply をクリックします。新しいポートのサービス状態が、Service State カラムに表示されます。

**ステップ 7** 必要に応じて、各ポートについてこの作業を繰り返します。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A217 BLSR の試験リングテスト

目的	この作業では、トラフィックを切り替えずに、Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) の機能をテストします。リング試験状態 (K バイトのパススルーなど) が報告され、10 ~ 15 秒以内にクリアされます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > BLSR タブをクリックします。

**ステップ 3** 試験する BLSR の行をクリックし、**Edit** をクリックします。

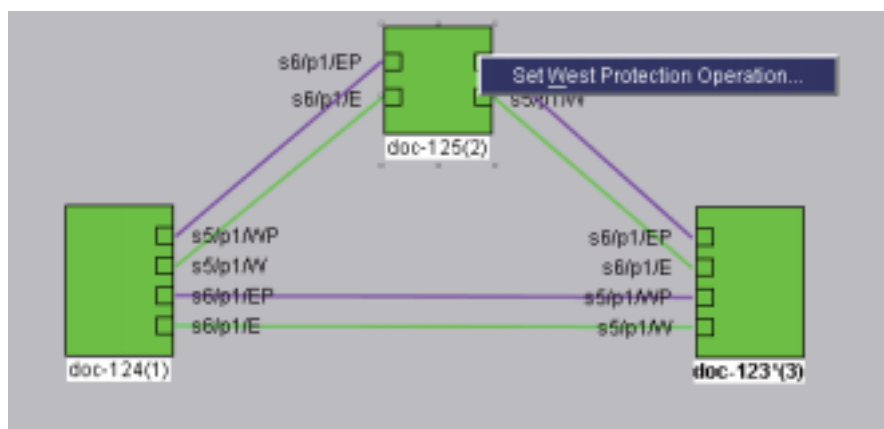
**ステップ 4** ウェストポートを試験します。

- a. 任意の BLSR ノードのウェストポートを右クリックし、**Set West Protection Operation** を選択します。図 19-2 に例を示します (グラフィックアイコンを移動するには、Ctrl キーを押しながら、アイコンを新しい場所にドラッグアンドドロップします)。



**(注)** 2 ファイバの BLSR の場合、ノードアイコンの四角形は、BLSR の現用チャンネルと保護チャンネルを表します。いずれかのチャンネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。現用ポートまたは保護ポートを右クリックします。

図 19-2 3 ノードの BLSR の保護操作



- 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 **EXERCISE RING** を選択します。
- c. **OK** をクリックします。

- d. Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。

ネットワーク ビューの図で、保護切り替えを呼び出した現用 BLSR チャンセルに E が表示され  
ます。E は、10 ~ 15 秒間表示されてから消えます。

#### ステップ 5 イースト ポートを試験します。

- a. 任意の BLSR ノードのイースト ポートを右クリックし、Set East Protection Operation を選択し  
ます。



**(注)** 2 ファイバの BLSR の場合、ノード アイコンの四角形は、BLSR の現用チャンネルと保護  
チャンネルを表します。いずれかのチャンネルを右クリックします。4 ファイバ BLSR の場  
合、四角形はポートを表します。現用ポートまたは保護ポートを右クリックします。

- 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 EXERCISE  
RING を選択します。
- c. OK をクリックします。
- d. Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。

ネットワーク ビューの図で、試験を呼び出した BLSR チャンセルに E が表示されます。E は、10  
~ 15 秒間表示されてから消えます。

#### ステップ 6 Cisco Transport Controller ウィンドウで、History タブをクリックします。

BLSR の試験状態がまったく表示されない場合は、Filter ボタンをクリックし、フィルタリングが  
オンになっていないことを確認します。また、ノードまたは BLSR ドロップ カードについて、ア  
ラームおよび状態が抑制されていないことを確認します。詳細については、「[NTP-A72 アラーム抑  
制の開始と中止](#)」(p.8-10) を参照してください。

#### ステップ 7 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-A227 アラーム  
フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
- b. 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454  
Troubleshooting Guide*』を参照してください。

#### ステップ 8 File メニューから Close を選択して、BLSR ウィンドウを閉じます。

#### ステップ 9 元の NTP (手順) に戻ります。

## DLP-A218 UPSR セレクタのプロビジョニング

目的	この作業では、回線作成時またはトポロジー アップグレード変換時に Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) セレク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-A60 CTC へのログイン (p.17-71)
	Circuit Creation ウィザードの Circuit Attributes 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 Creation ウィザードの Circuit Attributes ページで信号劣化パス (SD-P) または信号障害パス (SF-P) スレッシュホールドをプロビジョニングする場合、UPSR 保護スパンに対してだけ値が設定されます。回線の送信元および宛先では、非保護回線および UPSR 回線の送信元とドロップに関して、SD-P に対しては 10E-4、SF-P に対しては 10E-6 というノードのデフォルト値を使用します。

**ステップ 1** Circuit Creation ウィザードの Circuit Attributes ページの UPSR 領域で、UPSR パス セレクタを設定します。

- Provision working go and return on primary path — 1 つのファイバ ペアで現用パスをルーティングし、別のファイバ ペアで保護パスをルーティングする場合は、このボックスをオンにします。この機能は、双方向の UPSR 回線にだけ適用されます。
- Revertive — トラフィックを保護パスに変更した状態がクリアされたときにトラフィックを現用パスに復帰させる場合は、このボックスをオンにします。Revertive を選択しないと、トラフィックは切り替え後も保護パスに残ります。
- Reversion time — Revertive がオンになっている場合は、Reversion time フィールドをクリックして、ドロップダウン メニュー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。これは、トラフィックが現用パスに復帰するまでに経過する時間です。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。
- SF threshold — UPSR パスレベルの Signal Failure (SF; 信号障害) BER (ビット エラー レート) スレッシュホールドを設定します。
- SD threshold — UPSR パスレベルの Signal Degrade (SD; 信号劣化) BER スレッシュホールドを設定します。
- Switch on PDI-P — Synchronous Transport Signal (STS; 同期転送信号) 回線の場合、STS Payload Defect Indicator (PDI; ペイロード障害インジケータ) を受信したときにトラフィックを切り替えるには、このボックスをオンにします。Virtual Tributary (VT) 回線では使用できません。

**ステップ 2** 元の NTP (手順) に戻ります。

## DLP-A219 VT トンネル 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 VT トンネルのルートを実行します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
	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 ページで、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)。矢印は、送信元ノードからトンネルをルーティングできるスパンを表しています。
- ステップ 2** VT トンネルを通過させるスパンの矢印をクリックします。矢印がイエローになります。Selected Span 領域の From および To フィールドに、トンネルが伝送されるスロットとポートが表示されず、送信元 STS が表示されます。
- ステップ 3** 送信元 STS を変更する場合は、Source STS フィールドを変更します。変更しない場合は次のステップへ進みます。
- ステップ 4** 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 5** トンネルがすべての中継ノードを通過して送信元ノードから宛先ノードまで設定されるまで、ステップ 3 と 4 を繰り返します。
- ステップ 6** 元の NTP (手順) に戻ります。
- 

## DLP-A220 E シリーズ 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 E100T-12、E100T-G、E1000-2、および E1000-2-G イーサネット ポートをイネーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	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、プロビジョニングするイーサネット カードをダブルクリックします。
- ステップ 2** Provisioning > Port タブをクリックします。

**ステップ 3** 各イーサネット ポートについて、次のパラメータを設定します。

- 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。
- Mode — イーサネット ポートに適したモードを選択します。
  - E100T-12 および E100T-G カードで選択できるのは、Auto、10 Half、10 Full、100 Half、および 100 Full です。
  - E1000-2 および E1000-2-G カードで選択できるのは、1000 Full および Auto です。



**(注)** 1000 Full モードおよび Auto モードでは、E1000-2 ポートは 1000 Mbps の全二重動作モードに設定されます。ただし、1000 Full を選択した場合にはフロー制御は無効になります。Auto モードを選択すると、E1000-2 カードでフロー制御を自動ネゴシエートできます。フロー制御とは、送信デバイスが受信デバイスにデータを過剰に送信しないようにすることによって、ネットワークで輻輳が発生するのを防ぐメカニズムです。E1000-2 ポートは、接続されているネットワーク デバイスとハンドシェイクすることによって、そのデバイスがフロー制御をサポートしているかどうかを判別します。

- Enabled — このチェックボックスをオンにすると、対象のイーサネット ポートが有効になります。
- Priority — ポートのキューイング プライオリティを選択します。範囲は 0 (低) ~ 7 (高) です。プライオリティ キューイング (IEEE 802.1Q) では、イーサネット トラフィックをさまざまなプライオリティ レベルにマップすることによって、ネットワーク輻輳の影響が抑えられます。プライオリティ キューイングについては、『Cisco ONS 15454 Reference Manual』を参照してください。このパラメータは、ポートマップモードでは E シリーズカードに適用されません。
- Stp Enabled — このチェックボックスをオンにすると、ポートで Spanning-Tree Protocol (STP; スパニングツリー プロトコル) がイネーブルになります。このパラメータは、ポートマップモードでは E シリーズカードに適用されません。スパニングツリーについては、『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** VLAN (仮想 LAN) 内のその他のカードについて、ステップ 1 ~ 4 を繰り返します。E シリーズカードがポート マップ モードになっている場合は、ポイントツーポイント回線のその他のカードについて、ステップ 1 ~ 4 を繰り返します。イーサネット ポートがプロビジョニングされ、VLAN メンバーシップ用に設定する準備ができました。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A221 VLAN メンバーシップ用の E シリーズイーサネット ポートのプロビジョニング

目的	この作業では、VLAN メンバーシップ用に E シリーズのポートをプロビジョニングします。この手順は、ポートマップモードの E シリーズカードには適用できません。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、E シリーズ 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 > VLAN タブをクリックします。

**ステップ 3** 次の手順で VLAN にポートを設定します。

- a. ポートをクリックし、Tagged または Untag のどちらかを選択します。
- b. ポートのメンバーが 1 つの VLAN だけの場合は、VLAN の行の Port カラムから Untag を選択します。その Port カラムで他のすべての VLAN 行について -- を選択します。



**(注)** Untag を選択した VLAN はポートに接続できますが、その他の VLAN はそのポートにアクセスできません。

- c. トランク接続が必要なすべての VLAN 行では、Tagged を選択します。デフォルトの VLAN など、トランク接続する必要がない VLAN 行では、Untag を選択します。



**(注)** 各イーサネット ポートは、接続する VLAN のうち少なくとも 1 つを Untag に設定する必要があります。トランク ポートでは、トランキングをサポートしている、スイッチなどの外部デバイスに複数の VLAN が接続されます。トランク ポートでは、外部デバイスに接続するすべての VLAN に対してタグ機能 (IEEE 802.1Q) がイネーブルでなければなりません。

**ステップ 4** 各ポートが適切な VLAN に配置されたら、Apply をクリックします。表 19-1 に VLAN の設定を示します。

表 19-1 VLAN の設定

設定	内容
--	この記号が付いているポートは、VLAN には属していません。
Untag	ONS 15454 で、入力フレームにタグが付けられ、出力フレームからタグが外されます。
Tagged	ONS 15454 で、VLAN ID に従って入力フレームが処理されます。出力フレームのタグは削除されません。



(注) Tagged を選択した場合、接続されている外部のイーサネット デバイスは IEEE 802.1Q VLAN を認識する必要があります。



(注) E1000-2 または E1000-2-G カード上の両ポートは、同じ VLAN のメンバーにすることはできません。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A222 G シリーズ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 G シリーズ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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) カードのポートをプロビジョニングする前またはあとに、G シリーズの回線をプロビジョニングできます。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-A344 手動ルーティングによる光回線の作成 \(p.6-54\)](#)」を参照してください。

**ステップ 1** ノードビューで、G シリーズ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 > Port タブをクリックします。

**ステップ 3** 各 G シリーズポートについて、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。
- 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。
- 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。カスタムフロー制御の水準点の設定については、「[DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング \(p.21-6\)](#)」を参照してください。
- Max Size — 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には、Jumbo を選択します (デフォルト)。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。





(注) 最大フレーム サイズを 1548 バイトにすることによって、ISL (スイッチ間リンク) などのプロトコルを使用する有効なイーサネット フレームをポートで受け入れることができます。ISL によって 30 バイトのオーバーヘッドが追加され、フレーム サイズが従来の上限である 1518 バイトを超える可能性があります。

- Payload Type — G シリーズ カードの LEX カプセル化を設定するには、Payload Type フィールドをクリックして Cyclic Redundancy Check (CRC; 巡回冗長検査) のサイズを選択します。
  - LEX-FCS-16 は 16 ビット (2 バイト) CRC です。
  - LEX-FCS-32 は 32 ビット (4 バイト) CRC です。

**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 > Statistics タブをクリックします。
- b. Refresh をクリックします。



(注) G シリーズ 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-A224 CTC を使用した CE-100T-8 カードのソフト リセット

目的	この手順では、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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) ソフト リセットは、ほとんどの場合エラーが発生することはありません。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、カードを右クリックして、ポップアップ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-A225 アラーム フィルタリングのイネーブル化

目的	この作業では、すべてのネットワーク ノードのアラーム、状態、またはイベント履歴のアラーム フィルタリングをイネーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

**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** タブをクリックします。

**ステップ 2** 下部のツールバーの右下にある **Filter** をクリックします。

このツールが選択されている場合はアラーム フィルタリングがイネーブルで、選択されていない場合はディセーブルです。

アラーム フィルタリングは、そのノードのカード ビュー、ノード ビュー、およびネットワーク ビューの **Alarms** タブでイネーブルになるほか、ネットワーク内のその他すべてのノードでもイネーブルになります。たとえば、Alarm Filter ツールが、あるノードのノード ビューの **Alarms** タブでイネーブルになっている場合、そのノードのネットワーク ビューとカード ビューの **Alarms** タブでもツールはイネーブルになっており、ネットワーク内の他のノードでもすべて、ツールはイネーブルになっています。

カード ビューでアラームをフィルタリングすると、そのアラームはノード ビューでは表示されたままになります。このビューでは、カードは最も高いレベルのアラームの色を表示します。アラームは、そのノードのネットワークビューにも表示されます。

**ステップ 3** 状態を表示するときにアラーム フィルタリングをイネーブルにする場合は、**Conditions** ウィンドウで **ステップ 1** と **2** を繰り返します。

**ステップ 4** アラーム履歴を表示するときにアラーム フィルタリングをイネーブルにする場合は、**History** ウィンドウで **ステップ 1** と **2** を繰り返します。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A227 アラーム フィルタリングのディセーブル化

目的	この作業では、すべての重大度が CTC でレポートされるように、すべてのネットワーク ノードで特定のアラーム フィルタリングをディセーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A225 アラーム フィルタリングのイネーブル化 (p.19-20)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

**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** タブをクリックします。

**ステップ 2** 下部のツールバーの右下にある **Filter** をクリックします。

このツールがインデント表示されている場合はアラーム フィルタリングがイネーブルで、表示(選択)されていない場合はディセーブルです。

**ステップ 3** 状態を表示するときにアラーム フィルタリングをディセーブルにする場合は、**Conditions** タブをクリックして、**Filter** をクリックします。

**ステップ 4** アラーム履歴を表示するときにアラーム フィルタリングをディセーブルにする場合は、**History** タブをクリックして、**Filter** ツールをクリックします。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A229 スパンにおける回線の表示

目的	この作業では、スパンにある未使用の STS および VT と同様に、ONS 15454 スパン上の回線を表示します。
工具 / 機器	なし
事前準備手順	スパン上に回線を作成する必要があります。回線の作成手順については、 <a href="#">第 6 章「回線と VT トンネルの作成」</a> を参照してください。 <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 メニューで、**View > Go to Network View** を選択します。すでにネットワーク ビューにいる場合は、[ステップ 2](#) へ進みます。

**ステップ 2** 表示する回線を含むグリーン色の線を右クリックし、次のいずれかを選択します。

- Circuits — スパン上の BLSR、UPSR、1+1、Virtual Concatenated (VCAT; 仮想連結)、DWDM Optical Channel Network Connection (OCHNC; 光チャネルネットワーク接続) または非保護回線を表示する場合。
- PCA Circuits — BLSR 保護チャンネル上でルーティングされた回線を表示する場合(このオプションは、右クリックしたスパンが BLSR スパンではない場合は表示されません)。

Circuits on Span ダイアログボックスでは、このスパンについて次の情報を参照できます。表示される情報は、回線のタイプによって異なります。

- STS — STS を表示します。
- VT — VT を表示します。
- UPSR — (UPSR スパンのみ) オンにすると、UPSR 回線がスパン上に表示されます。
- Circuit — 回線名が表示されます。回線が STS または VT を使用していない場合、このコラムには [unused] が表示されます。
- Switch State — (UPSR スパンのみ) 回線の切り替え状態(どのスパン切り替えがアクティブであるか)を表示します。UPSR スパンの場合、切り替えのタイプには、CLEAR (切り替え済みのスパンは存在しない)、MANUAL (手動切り替えがアクティブ)、FORCE (強制切り替えがアクティブ)、または LOCKOUT OF PROTECTION (スパン ロックアウトがアクティブ)があります。



**(注)** Circuits on Span ダイアログボックスから、別の手順を実行できます。スパンが UPSR の場合、スパントラフィックを切り替えることができます。手順については、「[DLP-A197 UPSR 強制切り替えの開始](#)」(p.18-68)を参照してください。スパン上の回線を編集するには、回線をダブルクリックします。手順については、「[DLP-A231 回線名の編集](#)」(p.19-24)または「[DLP-A233 UPSR 回線パス セレクタの編集](#)」(p.19-26)を参照してください。

**ステップ 3** 元の NTP (手順)に戻ります。

## DLP-A230 回線のサービス状態の変更

目的	この作業では、回線のサービス状態を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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** View メニューから **Go to Network View** を選択します。

**ステップ 2** Circuits タブをクリックします。

**ステップ 3** サービス状態を変更する回線をクリックします。



(注) Release 3.4 より前の CTC ソフトウェア リリースのノードにルーティングされた回線の場合、その回線のサービス状態を編集できません。これらの回線は自動的に稼働状態 (IS) になります。

**ステップ 4** Tools メニューから、**Circuits > Set Circuit State** を選択します。

**ステップ 5** Set Circuit State ダイアログボックスの Target Circuit Admin State ドロップダウン メニューで、次の中から管理状態を選択します。

- IS — 回線のクロスコネクトのサービス状態を IS-NR にします。
- OOS,DSBLD — 回線のクロスコネクトのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
- IS,AINS — 回線のクロスコネクトのサービス状態を OOS-AU,AINS にします。接続で有効な信号を受信すると、クロスコネクトのサービス状態は自動的に IS-NR になります。
- OOS,MT — 回線のクロスコネクトのサービス状態を OOS-MA,MT にします。このサービス状態になっても、トラフィックの流れが中断されることはなく、その回線に対してループバックを実行することができますが、アラームおよび状態は抑制されます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合は、この OOS,MT 管理状態を使用します。テストが完了したら、管理状態を IS、OOS、または IS,AINS に変更します。
- OOS,OOG — (VCAT 回線のみ) メンバーのサービス状態を Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) にします。この管理状態は、メンバーの回線をグループから外し、トラフィックの送信を停止するために使用します。OOS-MA,OOG は、VCAT があるエンド ノード上のクロスコネクトだけに適用されます。中継ノードのクロスコネクトは、OOS-MA,MT サービス状態にあります。

回線および VCAT の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

**ステップ 6** このサービス状態を回線の送信元ポートと宛先ポートに適用する場合、**Apply to Drop Ports** チェックボックスをオンにします。

**ステップ 7** Apply をクリックします。

**ステップ 8** Apply to Ports Results ダイアログボックスが表示されたら、結果を見て **OK** をクリックします。

CTC は、回線の送信元ポートと宛先ポートのサービス状態を変更しない場合があります。たとえば、ポートがループバック (OOS-MA,LPBK & MT) になっている場合、CTC はポートを IS-NR に変更しません。別の例として、回線のサイズがポートより小さい場合 (STS ポート上の VT1.5 回線など)、CTC はポートのサービス状態を IS-NR から OOS-MA,DSBLD には変更しません。CTC がポートのサービス状態を変更できない場合、手動でポート状態を変更する必要があります。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。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A231 回線名の編集

目的	この作業では、回線名または VCAT メンバー名を編集します。
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** View メニューから **Go to Network View** を選択します。

**ステップ 2** **Circuits** タブをクリックします。

**ステップ 3** 名前を変更する回線を選択し、**Edit** をクリックします。

**ステップ 4** VCAT 回線のメンバー名を編集する場合は、**Edit Circuit** ウィンドウで次のステップを実行します。編集しない場合は、**ステップ 5** へ進みます。

- a. **Members** タブをクリックします。
- b. 編集する VCAT メンバーをクリックしてから、**Edit Member** をクリックします。Edit Member ウィンドウが表示されます。

**ステップ 5** **General** タブで、**Name** フィールドをクリックし、回線の編集または回線名の変更を行います。



**(注)** 名前には 48 文字以下の英数字または特殊文字を使用できます。ただし、この回線上にモニタ回線を確実に作成するためには、44 文字を超える文字数の名前は付けしないでください。モニタ回線では、回線名に [MON] (4 文字) を追加します。

**ステップ 6** **Apply** をクリックします。

**ステップ 7** **File** メニューから **Close** を選択します。

**ステップ 8** VCAT 回線のメンバー名を変更した場合は、**Edit Circuit** ウィンドウに対して**ステップ 7** を繰り返します。

**ステップ 9** **Circuits** ウィンドウで、回線の名前変更が正しく行われたかどうかを確認します。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A232 アクティブ スパンおよびスタンバイ スパンの色の変更

目的	この作業では、Edit Circuits ウィンドウの詳細回線マップに表示される、アクティブ（現用）およびスタンバイ（保護）の回線スパンの色を変更します。デフォルトでは、現用スパンはグリーン、保護スパンはパープルです。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 任意のビューの Edit メニューから、**Preferences** を選択します。

**ステップ 2** Preferences ダイアログボックスで、**Circuit** タブをクリックします。

**ステップ 3** 必要に応じて、次の手順を 1 つまたは複数実行します。

- アクティブ（現用）スパンの色を変更する場合は、[ステップ 4](#) へ進みます。
- スタンバイ（保護）スパンの色を変更する場合は、[ステップ 5](#) へ進みます。
- アクティブおよびスタンバイ スパンをデフォルトの色に戻す場合は、[ステップ 6](#) へ進みます。

**ステップ 4** 必要に応じて、次の手順でアクティブ スパンの色を変更します。

- a. Span Colors 領域で、Active という語の右にある色の付いた四角をクリックします。
- b. Pick a Color ダイアログボックスで、アクティブ スパン用の色をクリックします。また、直前に適用（保存）した色でアクティブ スパンを表示する場合は、**Reset** ボタンをクリックします。
- c. **OK** をクリックして、Pick a Color ダイアログボックスを閉じます。スタンバイ スパンの色を変更するには、[ステップ 5](#) へ進みます。スタンバイ スパンの色を変更しない場合は、**OK** をクリックして、変更を保存し Preferences ダイアログボックスを閉じるか、**Apply** をクリックして、変更を保存し Preferences ダイアログボックスを開いたままにしておきます。

**ステップ 5** 必要に応じて、次の手順でスタンバイ スパンの色を変更します。

- a. Span Colors 領域で、Standby という語の右にある色の付いた四角をクリックします。
- b. Pick a Color ダイアログボックスで、スタンバイ スパン用の色をクリックします。また、直前に適用（保存）した色でスタンバイ スパンを表示する場合は、**Reset** ボタンをクリックします。
- c. **OK** をクリックして、変更を保存し Preferences ダイアログボックスを閉じるか、または **Apply** をクリックして、変更を保存し Preferences ダイアログボックスを開いたままにしておきます。

**ステップ 6** 必要に応じて、次の手順でアクティブ スパンおよびスタンバイ スパンをデフォルトの色に戻します。

- a. **Reset to Defaults** をクリックします。
- b. **OK** をクリックして、変更を保存し Preferences ダイアログボックスを閉じるか、または **Apply** をクリックして、変更を保存し Preferences ダイアログボックスを開いたままにしておきます。

**ステップ 7** 元の NTP（手順）に戻ります。

## DLP-A233 UPSR 回線バス セレクタの編集

目的	この作業では、1 つまたは複数の UPSR 回線に対する UPSR の SF と SD のスレッショールド、復帰設定、復元時間、および ペイロード障害表示パス (PDI-P) 設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** **Circuits** タブをクリックします。

**ステップ 3** **Circuits** タブで、編集する UPSR 回線 (複数可) をクリックします。複数回線の設定を変更するには、**Shift** キー (隣接している回線を選択する場合) または **Ctrl** キー (隣接していない回線を選択する場合) を押して、変更する各回線をクリックします。

**ステップ 4** **Tools** メニューから、**Circuits > Set Path Selector Attributes** を選択します。

**ステップ 5** **Path Selectors Attributes** ダイアログボックスで、必要に応じて次の UPSR セレクタを編集します。

- **Revertive** — オンにしておく、トラフィックを保護パスに変更した状態がクリアされたときに、トラフィックが現用パスに復帰します。チェックボックスをオフにすると、トラフィックは現用パスに復帰しません。
- **Reversion Time (Min)** — **Revertive** をオンにした場合、この値は、トラフィックが現用パスに復帰するまでの時間を設定します。範囲は 0.5 ~ 12 分で、0.5 分単位で指定します。
- **STS Circuits Only** 領域で、次のスレッショールドを設定します。
  - **SF threshold** — UPSR の SF BER スレッショールドを設定します。
  - **SD threshold** — UPSR の SD BER スレッショールドを設定します。
  - **Switch on PDI-P** — オンにしておく、STS ペイロード障害表示を受信したときにトラフィックが切り替わります。
- **VT Circuits Only** 領域で、次のスレッショールドを設定します。
  - **SF threshold** — UPSR の SF BER スレッショールドを設定します。
  - **SD threshold** — UPSR の SD BER スレッショールドを設定します。

**ステップ 6** **OK** をクリックし、**Circuits** ウィンドウで変更した値が正しいことを確認します。

**ステップ 7** 元の NTP (手順) に戻ります。



## DLP-A241 BLSR 手動リング切り替えのクリア

目的	この作業では、手動リング切り替えをクリアします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 メニューで、**Go to Network View** を選択します。

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

**ステップ 3** BLSR を選択して、**Edit** をクリックします。



---

**ヒント** たとえば BLSR チャンネル (ポート) の情報を見やすくするために、アイコンを新しい場所へ移動する場合は、Edit BLSR のネットワーク図でアイコンをクリックし、Ctrl キーを押したままアイコンを新しい場所にドラッグします。

---

**ステップ 4** 手動リング切り替えが適用されている BLSR ノード チャンネル (ポート) を右クリックし、そのチャンネルに応じて、**Set West Protection Operation** または **Set East Protection Operation** を選択します。

**ステップ 5** ダイアログボックス内で、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。

**ステップ 6** Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。チャンネル (ポート) から [M] の文字が消え、ネットワーク ビュー マップのスパンがグリーンに変わります。

**ステップ 7** File メニューから、**Close** を選択します。

**ステップ 8** 元の NTP (手順) に戻ります。

---

## DLP-A242 単一ノードでの BLSR の作成

目的	この作業では、単一ノードに BLSR を作成します。既存の BLSR にノードを追加する場合、または単一ノードで一時的に BLSR を削除して再度作成する場合に、使用します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > BLSR** タブをクリックします。

**ステップ 2** Suggestion ダイアログボックスで **OK** をクリックします。

**ステップ 3** Create BLSR ダイアログボックスで、次の BLSR 情報を入力します。

- Ring Type — BLSR のリング タイプ (2 ファイバまたは 4 ファイバ) を入力します。
- Ring Name — BLSR のリング名を入力します。BLSR にノードを追加する場合は、BLSR のリング名を使用します。
- Node ID — ノード ID を入力します。BLSR にノードを追加する場合は、他の BLSR ノードが使用していない ID を使用します。
- Ring Reversion — 既存の BLSR のリング復元時間を入力します。
- West Line — ノードのウェスト ライン (ポート) を経由して既存の BLSR に接続するノードの スロットを入力します。
- East Line — ノードのイースト ライン (ポート) を経由して既存の BLSR に接続するノードの スロットを入力します。

4 ファイバの BLSR にノードを追加する場合は、ファイバの 2 番めのセットについて次の項目を入力します。

- Span Reversion — 既存の BLSR のスパン復元時間を入力します。
- West Line — ノードのウェスト ラインを經由して既存の BLSR に接続するノードの スロットを入力します。
- East Line — ノードのイースト ラインを經由して既存の BLSR に接続するノードの スロットを入力します。

**ステップ 4** **OK** をクリックします。



**(注)** BLSR は不完全なため、ノードを他の BLSR ノードに接続するまで、アラームが表示されません。

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A244 再初期化ツールの使用によるデータベースのクリアおよびソフトウェアのアップロード (Windows)

<b>目的</b>	この作業では、Windows コンピュータで CTC 再初期化ツールを使用して、ONS15454 を再初期化します。初期化しなすと、新しいソフトウェア パッケージが TCC2/TCC2P カードにアップロードされ、ノードのデータベースがクリアされて、出荷時のデフォルト パラメータが復元されます。
<b>工具 / 機器</b>	ONS 15454 SONET System Software CD、Version 7.2  再初期化が完了したときにノードにログインするには、そのコンピュータに JRE 1.4.2 または JRE 5.0 がインストールされている必要があります。再初期化ツールは、JRE 1.3.1_02、JRE 1.4.2、または JRE 5.0 で実行できます。
<b>事前準備手順</b>	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
<b>必須 / 適宜</b>	適宜
<b>オンサイト / リモート</b>	オンサイトまたはリモート
<b>セキュリティ レベル</b>	スーパーユーザ



### 注意

ノードを出荷時の設定に復元すると、ノードのクロスコネクトはすべて削除されます。

- ステップ 1** システム ソフトウェア CD をコンピュータの CD-ROM ドライブに挿入します。CTC インストール ウィザードが開いたら、**Cancel** をクリックします。
- ステップ 2** Windows の [ スタート ] メニューから、[ **ファイル名を指定して実行** ] を選択します。[ **ファイル名を指定して実行** ] ダイアログボックスで、[ **参照** ] をクリックし、ソフトウェア CD の CISCO15454 フォルダに移動します。
- ステップ 3** [ **ファイルの参照** ] ダイアログボックスの [ **ファイルの種類** ] フィールドで、[ **すべてのファイル** ] を選択します。
- ステップ 4** RE-INIT.jar ファイルを選択して、[ **開く** ] をクリックします。NE Re-Initialization ウィンドウが表示されます ( [図 19-3](#) )。

図 19-3 再初期化ツール

**ステップ 5** 次のフィールドを設定します。

- GNE IP — 再初期化するノードに、Gateway Network Element ( GNE; ゲートウェイ ネットワーク エlement ) として設定されている別のノードを通してアクセスする場合、GNE IP アドレスを入力します。ノードに直接アクセスする場合は、このフィールドを空白にしておきます。
- Node IP — 再初期化するノードのノード名または IP アドレスを入力します。
- User ID — ノードのアクセスに必要なユーザ ID を入力します。
- Password — ユーザ ID のパスワードを入力します。
- Upload Package — このボックスをオンにすると、ソフトウェア パッケージ ファイルがノードに送られます。オフにしておくと、ノードに保存されているソフトウェアは編集されません。
- Force Upload — このボックスをオンにすると、同じバージョンのソフトウェア パッケージ ファイルをノードが実行していても、そのソフトウェア パッケージがノードに送られます。オフにしておくと、同じバージョンのソフトウェア パッケージがノードですでに実行されている場合、再初期化ではそのソフトウェア パッケージは送られません。
- Activate/Revert — このボックスをオンにすると、ソフトウェア ファイルがアップロードされるとただちに、アップロードされたソフトウェアを起動 ( ソフトウェアのバージョンがインストールされているものよりも新しい場合 ) またはアップロードされたソフトウェアに復帰 ( ソフトウェアのバージョンがインストールされているものよりも古い場合 ) します。オフにしておくと、ソフトウェアはアップロード後に起動も復帰もされないのので、あとでノードビューの Maintenance > Software タブからその機能を起動できます。
- Re-init Database — このボックスをオンにすると、新しいデータベースがノードに送られます ( これは、CTC データベースの復元操作と同じです )。オフにしておくと、ノードのデータベースは編集されません。
- Confirm — 操作を行う前に警告メッセージを表示させるには、このボックスをオンにします。オフにしておくと、再初期化では警告メッセージは表示されません。
- Search Path — CD ドライブ上の CISCO15454 フォルダのパスを入力します。

**ステップ 6** Go をクリックします。**注意**

次のステップへ進む前に、アップロードするデータベースが正しいかどうか確認します。Yes をクリックしたあとに、アップロード処理を無効にすることはできません。

**ステップ 7** Confirm NE Re-Initialization ダイアログボックスの情報を調べてから、Yes をクリックして再初期化を開始します。

再初期化が始まります。ソフトウェアがダウンロードされて起動し、データベースが TCC2/TCC2P カードにアップロードされると、ステータス バーに [Complete] と表示され、TCC2/TCC2P カードがリポートします。リポートの完了には 2、3 分かかります。

**ステップ 8** リポートが完了したら、「[DLP-A60 CTC へのログイン](#)」(p.17-71) に従ってノードにログインします。**ステップ 9** 「[NTP-A25 名前、日付、時刻、連絡先情報の設定](#)」(p.4-6) および「[NTP-A169 CTC ネットワーク アクセスの設定](#)」(p.4-9) を実行します。**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A245 再初期化ツールの使用によるデータベースのクリアおよびソフトウェアのアップロード (UNIX)

目的	この作業では、UNIX コンピュータで CTC 再初期化ツールを使用して、ONS15454 を再初期化します。初期化しなすと、新しいソフトウェア パッケージが TCC2/TCC2P カードにアップロードされ、ノードのデータベースがクリアされて、出荷時のデフォルト パラメータが復元されます。
工具 / 機器	ONS 15454 SONET System Software CD、Version 7.2  再初期化が完了したときにノードにログインするには、そのコンピュータに JRE 1.4.2 または JRE 5.0 がインストールされている必要があります。再初期化ツールは、JRE 1.3.1_02、JRE 1.4.2、または JRE 5.0 で実行できます。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



### 注意

ノードを出荷時の設定に復元すると、ノードのクロスコネクトはすべて削除されます。

- ステップ 1** 再初期化ツール、ソフトウェア、およびデフォルト値のデータベースが格納されているシステム ソフトウェア CD を、コンピュータの CD-ROM ドライブに挿入してください。CTC インストール ウィザードが開いたら、**Cancel** をクリックします。
- ステップ 2** 復旧ツールのファイルを検出するには、CD の CISCO15454 ディレクトリ (通常 /cdrom/cdrom0/CISCO15454) に移動します。
- ステップ 3** ファイル エクスプローラを使用している場合は、**RE-INIT.jar** ファイルをダブルクリックします。コマンド ラインを使用している場合は、**java -jar RE-INIT.jar** を実行します。NE Re-Initialization ウィンドウが開きます ( [図 19-3](#) )。
- ステップ 4** 次のフィールドを設定します。
- GNE IP — 再初期化するノードに、GNE として設定されている別のノードを通してアクセスする場合、GNE IP アドレスを入力します。ノードに直接アクセスする場合は、このフィールドを空白にしておきます。
  - Node IP — 再初期化するノードのノード名または IP アドレスを入力します。
  - User ID — ノードのアクセスに必要なユーザ ID を入力します。
  - Password — ユーザ ID のパスワードを入力します。
  - Upload Package — このボックスをオンにすると、ソフトウェア パッケージ ファイルがノードに送られます。オフにしておくと、ノードに保存されているソフトウェアは編集されません。
  - Force Upload — このボックスをオンにすると、同じバージョンのソフトウェア パッケージ ファイルをノードが実行していても、そのソフトウェア パッケージがノードに送られます。オフにしておくと、同じバージョンのソフトウェア パッケージがノードですでに実行されている場合、再初期化ではそのソフトウェア パッケージは送られません。

- Activate/Revert — このボックスをオンにすると、ソフトウェア ファイルがアップロードされると同時に、アップロードされたソフトウェアを起動（ソフトウェアのバージョンがインストールされているものよりも新しい場合）またはアップロードされたソフトウェアに復帰（ソフトウェアのバージョンがインストールされているものよりも古い場合）します。オフにしておくと、ソフトウェアはアップロード後に起動も復帰もされないため、あとでノード ビューの Maintenance > Software タブからその機能を起動できます。
- Re-init Database — このボックスをオンにすると、新しいデータベースがノードに送られます（これは、CTC データベースの復元操作と同じです）。オフにしておくと、ノードのデータベースは編集されません。
- Confirm — 操作を行う前に警告メッセージを表示させるには、このボックスをオンにします。オフにしておくと、再初期化では警告メッセージは表示されません。
- Search Path — CD ドライブ上の CISCO15454 フォルダのパスを入力します。

**ステップ 5** Go をクリックします。



**注意**

次のステップへ進む前に、アップロードするデータベースが正しいかどうか確認します。Yes をクリックしたあとに、アップロード処理を無効にすることはできません。

**ステップ 6** Confirm NE Re-Initialization ダイアログボックスの情報を確認してから、Yes をクリックして再初期化を開始します。

再初期化が始まります。ソフトウェアがダウンロードされて起動し、データベースが TCC2/TCC2P カードにアップロードされると、ステータス バーに [Complete] と表示され、TCC2/TCC2P カードがリポートします。リポートの完了には 2、3 分かかります。

**ステップ 7** リポートが完了したら、「[DLP-A60 CTC へのログイン \(p.17-71\)](#)」に従ってノードにログインします。

**ステップ 8** 「[NTP-A25 名前、日付、時刻、連絡先情報の設定 \(p.4-6\)](#)」および「[NTP-A169 CTC ネットワーク アクセスの設定 \(p.4-9\)](#)」を実行します。

**ステップ 9** 元の NTP（手順）に戻ります。

## DLP-A246 E シリーズイーサネット カードのモードのプロビジョニング

目的	この作業では、E シリーズイーサネット カードに、マルチカード EtherSwitch グループ、シングルカード EtherSwitch、ポートマップのいずれかのモードをプロビジョニングします。
工具 / 機器	E シリーズイーサネット カード (E100T-12/E100T-G、E1000-2/E1000-2-G) が取り付けられている必要があります。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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**

イーサネット カードに回線が接続されている間は、モードを変更できません。カードのモードを変更する場合は、まず接続されている回線を削除します。「[NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除](#)」(p.7-6)を参照してください。

- ステップ 1** ネットワーク ビューで、プロビジョニングする E シリーズイーサネットカードを取り付けたノードをダブルクリックしてから、その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** Provisioning > Card タブをクリックします。
- ステップ 3** Card Mode 領域で、次のいずれかを選択します。
- マルチカード EtherSwitch 回線グループの場合は、**Multicard EtherSwitch Group** を選択します。
  - シングルカード EtherSwitch 回線の場合は、**Single-card EtherSwitch** を選択します。
  - ポートマップ回線の場合は、**Port-mapped** を選択します。
- ステップ 4** Apply をクリックします。
- ステップ 5** マルチカード EtherSwitch 回線を使用する場合は、それらの回線を伝送する、ノードのその他すべてのイーサネットカードに対してステップ 2 ~ 4 を繰り返します。
- ステップ 6** 必要に応じて、他のノードに対してステップ 1 ~ 5 を繰り返します。
- ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A247 OC-N カードの変更

目的	この作業では、Data Communication Channel (DCC; データ通信チャネル)、回線、保護、タイミング、およびリングを含む既存のプロビジョニングを維持しながら、OC-N カードを交換します。この作業は、タイプや回線レートが同一のカードと交換する場合や、スロットが事前にプロビジョニングされていて、カードの光伝送速度を変更したい場合、または自動スパン アップグレードから復帰した場合に使用することを目的としています。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (p.17-71)
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**

OC-N カードを物理的に取り外すと、現用トラフィックまたは保護切り替えが失われる可能性があります。トラフィックをより速い速度にアップグレードする情報については、[第 12 章「カードとスパンのアップグレード」](#)を参照してください。

**(注)**

マルチポート カードをポート数が少ないカードと交換できるのは、新しいカードの回線レートがマルチポートと同じである場合のみです (MRC-12 カードはシングルポート OC-12 カードまたはシングルポート OC-48 カードと交換できます)。

- 
- ステップ 1** カードが 1+1 保護グループのアクティブカードの場合は、トラフィックをそのカードから切り替えてください。
- ネットワーク上のノードにログインします。すでにログインしている場合は、ステップ **b** へ進みます。
  - CTC ノード (ログイン) ビューを表示します。
  - Maintenance > Protection タブをクリックします。
  - 該当カードを含む保護グループをダブルクリックします。
  - 選択したグループのアクティブカードをクリックします。
  - Switch をクリックし、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 2** CTC で、取り外したいカードを右クリックし、Change Card を選択します。
- ステップ 3** Change Card のドロップダウン リストで、適切なカード タイプを選択し、OK をクリックします。カードを交換するまで、Mismatched Equipment Alarm (MEA) アラームが表示されます。
- ステップ 4** 物理的にカードを取り外します。
- カードの前面に接続されているファイバを取り外します。
  - カードのラッチまたはイジェクタを開きます。
  - ラッチまたはイジェクタを使用してカードを前に引き出し、シェルフから取り出します。
- ステップ 5** 「NTP-A16 光カードおよびコネクタの取り付け」(p.2-8) を実行します。
- ステップ 6** 元の NTP (手順) に戻ります。
-



## DLP-A249 IP 設定のプロビジョニング

目的	この作業では、ONS 15454 ノードの IP アドレス、デフォルト ルータ、Dynamic Host Configuration Protocol( DHCP)アクセス、ファイアウォール アクセス、および SOCKS プロキシ サーバの設定などの IP 設定をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



### 注意

ONS 15454 IP アドレスとネットワーク パラメータはすべて、ネットワーク (または LAN) 管理者の確認が必要です。



### 注意

ノードに割り当てられている IP アドレスが同一サブネット上の別の ONS 15454 に割り当てられているアドレスと重複していないことを確認します。同一サブネット上の ONS 15454 に同じアドレスが割り当てられると、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 > Network > General** タブをクリックします。

**ステップ 2** 表示されたフィールドに次の情報を入力します。

- IP Address — ONS 15454 ノードに割り当てられた IP アドレスを入力します。



**(注)** TCC2P カードが取り付けられている場合、セキュア モード経由のデュアル IP アドレスリングを使用できます。セキュア モードがオフの場合 (リピータ モードと呼ばれることもある)、IP Address フィールドに入力された IP アドレスはバックプレーンの LAN ポートと TCC2P TCP/IP (LAN) ポートに適用されます。セキュア モードがオンの場合、IP Address フィールドには TCC2P TCP/IP (LAN) ポートに割り当てられたアドレスが表示され、スーパーユーザはバックプレーン IP アドレスの表示をイネーブルまたはディセーブルにできます。必要に応じて、「[DLP-A433 ノードのセキュア モードのイネーブル化](#)」(p.21-10) を参照してください。セキュア モードの詳細については、『*Cisco ONS 15454 Reference Manual*』の「Management Network Connectivity」の章を参照してください。

- Net/Subnet Mask Length — サブネット マスク長 (ビットでサブネット マスク長を表す 10 進数) を入力するか、または矢印をクリックしてサブネット マスク長を調整します。サブネット マスク長は、同一サブネットの ONS 15454 ではすべて同じになります。
- MAC Address — (表示専用) ONS 15454 の IEEE 802 MAC (メディア アクセス制御) アドレスを表示します。



(注) セキュア モードでは、フロントおよびバック TCP/IP (LAN) ポートには異なる MAC アドレスが割り当てられていて、スーパーユーザはバックプレーン情報を非表示にしたり、表示したりできます。

- Default Router — ONS 15454 が LAN に接続されている場合は、デフォルト ルータの IP アドレスを入力します。デフォルト ルータは、ONS 15454 では直接アクセスできないネットワーク デバイスにパケットを転送します。このフィールドは、次のいずれかがあてはまる場合には無視されます。
  - ONS 15454 が LAN に接続されていない。
  - SOCKS プロキシ サーバがイネーブルになっており、ONS 15454 が End Network Element (ENE) としてプロビジョニングされている。
  - Open Shortest Path First (OSPF) が、ONS 15454 とその ONS 15454 が接続されている LAN の両方でイネーブルになっている。
- LCD IP Setting — 次のいずれかを選択します。
  - **Allow Configuration** — LCD にノード の IP アドレスが表示され、LCD を使用して IP 設定を変更できます。このオプションを設定すると、「[DLP-A64 LCD による IP アドレス、デフォルト ルータ、ネットワーク マスクの設定](#)」(p.17-76) が行えるようになります。
  - **Display Only** — LCD にノード の IP アドレスが表示されますが、LCD を使用して IP アドレスを変更することはできません。
  - **Suppress Display** — LCD でノードの IP アドレスを非表示にします。
- Suppress CTC IP Display — セキュリティ レベルがプロビジョニング、メンテナンス、または検索のユーザの CTC (情報領域の IP Address フィールド) でノード IP アドレスを非表示にする場合、このチェックボックスをオンにします。IP アドレスが非表示になっていない場合は IP Address フィールドに表示されます。



(注) IP アドレスの非表示はセキュリティ レベルがスーパーユーザのユーザには適用されません。ただし、セキュア モードでは、バックプレーン IP アドレスの表示を、ルーティング テーブルを表示しているローカル接続のスーパーユーザに限定することができます。この場合、バックプレーン IP アドレスは、ルーティング テーブル上または自律メッセージ (TL1 REPT^DBCHG コマンド、アラーム、および PM レポート) 内の他の NE のユーザに対しては表示されません。

- Forward DHCP Request To — DHCP 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て、Request To フィールドに DHCP サーバの IP アドレスを入力します。このチェックボックスは、デフォルトではオフになっています。任意のゲートウェイ設定をイネーブルにして ONS 15454 SOCKS プロキシ サーバ機能を実装する場合は、このフィールドをブランクのままにします。



(注) DHCP をイネーブルにした場合、ONS 15454 ノードに接続されたコンピュータは一時的な IP アドレスを外部 DHCP サーバから取得します。ONS 15454 は DHCP 要求を転送するだけで、DHCP サーバとしては機能しません。

- Gateway Settings — ONS 15454 SOCKS プロキシ サーバ機能をプロビジョニングします(SOCKS は、IP ベースのアプリケーションの標準プロキシ プロトコルです)。これらのオプションの変更は、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章で SOCKS プロキシ サーバのシナリオを調べたあとに行ってください。SOCKS プロキシ サーバ ネットワークでは、ONS 15454 は、ENE、GNE、またはプロキシ専用サーバのいずれかになります。プロビジョニングは NE タイプごとに一貫している必要があります。
- Enable SOCKS proxy server on port — このボックスをオンにすると、ONS 15454 は、CTC クライアントとプロキシ ONS 15454 に DCC 接続された ONS 15454 との接続のプロキシとして機能します。CTC クライアントは、プロキシ ノードを介して DCC 接続 ノードへの接続を確立します。CTC クライアントには、DCC 接続 ノードへの IP 接続は必要なく、プロキシ ONS 15454 への接続のみが必要です。ポート上の イネーブル SOCKS プロキシ サーバが切断されている場合、ノードはいずれの CTC クライアントに対してもプロキシを行いません。このボックスをオンにすると、ノードを ENE または GNE として設定できます。
  - External Network Element (ENE) — ONS 15454 が LAN には接続されておらず、他の ONS ノードに DCC 接続されている場合、このオプションを選択します。TCC2/TCC2P クラフトポートを通して ENE に接続されている CTC コンピュータは、ENE に DCC 接続されているノードを管理できます。ただし、CTC コンピュータは、これらのノードまたはこれらのノードが接続される可能性のある LAN/WAN には、直接 IP 接続することはできません。
  - Gateway Network Element (GNE) — ONS 15454 が LAN に接続されており、他の ONS ノードに DCC 接続されている場合、このオプションを選択します。LAN に接続されている CTC コンピュータは、GNE に DCC 接続されているすべてのノードを管理できますが、これらに直接 IP 接続することはできません。GNE オプションでは、LAN は DCC ネットワークから切り離されるので、DCC 接続されたノードおよびそれらに接続された CTC コンピュータから発信される IP トラフィックは、LAN には到達しません。
  - SOCKS Proxy-Only — ONS 15454 が LAN に接続されており、LAN がファイアウォールでノードから分離されている場合、このオプションを選択します。SOCKS Proxy Only は、GNE オプションと同じですが、SOCKS Proxy Only では DCC ネットワークを LAN から分離しません。



**(注)** ノードがセキュア モードでプロビジョニングされる場合、SOCKS プロキシがイネーブルになった GNE として自動的にプロビジョニングされます。ただし、このプロビジョニングは上書き可能で、セキュア ノードを ENE に変更することができます。セキュア モードでは、SOCKS をディセーブルにはできません。GNE または ENE のステータスをはじめとしたプロビジョニング手順については、「[DLP-A433 ノードのセキュア モードのイネーブル化](#)」(p.21-10) を参照してください。

**ステップ 3** Apply をクリックします。

**ステップ 4** 確認用のダイアログボックスで Yes をクリックします。

両方の TCC2/TCC2P カードは、一度に 1 つずつリブートします。この間 (約 5 分間)、アクティブ およびスタンバイ状態の TCC2/TCC2P カードの LED は表 19-2 に示すサイクルで変化します。最後に、[Lost node connection, switching to network view] というメッセージが表示されます。

表 19-2 TCC2/TCC2P リポート中の LED 動作

リポート アクティビティ	アクティブ TCC2/TCC2P LED	スタンバイ TCC2/TCC2P LED
<p>スタンバイ TCC2/TCC2P カードを新規ネットワーク情報で更新</p> <p>メモリテスト (1 ~ 2 分)</p> <p>AIC-I カードが取り付けられている場合、AIC の更新時に AIC FAIL とアラーム LED が短時間点灯します。</p> <p>スタンバイ TCC2/TCC2P はアクティブ TCC2/TCC2P になります。</p>	<p>ACT/STBY : グリーンで点滅</p>	<ol style="list-style-type: none"> <li>1. ACT/STBY : イエローで点滅</li> <li>2. FAIL LED : レッドで点灯</li> <li>3. ACT/STBY 以外のすべての LED がオン</li> <li>4. CRIT がオフ</li> <li>5. MAJ および MIN がオフ</li> <li>6. REM、SYNC、および ACO がオフ</li> <li>7. A&amp;B PWR 以外のすべての LED がオフ (1 ~ 2 分)</li> <li>8. ACT/STBY : イエローで点灯</li> <li>9. ALARM LED : 一度点滅</li> <li>10. ACT/STBY : グリーンで点灯</li> </ol>
<p>メモリテスト (1 ~ 2 分)</p> <p>TCC2/TCC2P を新規ネットワーク情報で更新</p> <p>アクティブ TCC2/TCC2P はスタンバイ TCC2/TCC2P になります。</p>	<ol style="list-style-type: none"> <li>1. すべての LED : オフ (1 ~ 2 分)。CTC に [Lost node connection, switching to network view] というメッセージが表示されます。</li> <li>2. FAIL LED : レッドで点灯</li> <li>3. FAIL LED : レッドで点滅</li> <li>4. ACT/STBY 以外のすべての LED がオン</li> <li>5. CRIT がオフ</li> <li>6. MAJ および MIN がオフ</li> <li>7. REM、SYNC、および ACO がオフ、すべての LED がオフ</li> <li>8. ACT/STBY : イエローで点灯</li> <li>9. ACT/STBY : イエローで点滅</li> <li>10. ACT/STBY : イエローで点灯</li> </ol>	<p>ACT/STBY : グリーンで点灯</p>

**ステップ 5** OK をクリックします。ネットワーク ビューが表示されます。ノードにアクセスできない間は、ノードのアイコンがグレーで表示されます。

**ステップ 6** グリーンに変わったらノードのアイコンをダブルクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A250 OSPF プロトコルの設定または変更

目的	この作業では、ONS 15454 にある OSPF ルーティング プロトコルをイネーブルにします。ONS 15454 を OSPF 対応のネットワークに組み込みたい場合、この作業を実行します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > OSPF** タブをクリックします。

**ステップ 2** OSPF ペインの左上で次の項目を設定します。

- DCC/GCC OSPF Area ID Table — ドット付き 10 進表記で、ONS 15454 を一意の OSPF エリア ID として識別する番号を入力します。Area ID は、000.000.000.000 ~ 255.255.255.255 の任意の数字でかまいませんが、LAN OSPF エリアで一意となっている必要があります。
- SDCC Metric — この値は、通常は変更しません。Section DCC (SDCC) を介したパケット送信コストを設定する値であり、OSPF ルータが最短パスを計算するために使用します。この値は、常に LAN メトリックより大きな値にする必要があります。デフォルトの SDCC のメトリックは 100 です。
- LDCC Metric — Line DCC (LDCC) を介したパケット送信コストを設定します。この値は、常に SDCC メトリックより小さな値にする必要があります。デフォルトの LDCC メトリックは 33 です。通常は変更しません。

**ステップ 3** OSPF on LAN 領域で次の項目を設定します。

- OSPF active on LAN — オンにすると、ONS 15454 の OSPF トポロジを LAN 上の OSPF ルータにアダプタイズできます。このフィールドは、OSPF ルータに直接接続されている ONS 15454 でオンにします。
- LAN Port Area ID — ONS 15454 が接続されているルータ ポートの OSPF エリア ID (ドット付き 10 進表記) を入力します (この数値は、DCC/Generic Communication Channel [GCC] OSPF Area ID とは異なります)。

**ステップ 4** デフォルトでは、OSPF は No Authentication に設定されています。OSPF ルータが認証を必要とする場合は、次のステップを実行します。それ以外の場合は、[ステップ 5](#) へ進みます。

- a. **No Authentication** ボタンをクリックします。
- b. Edit Authentication Key ダイアログボックスで次の項目を指定します。
  - Type — **Simple Password** を選択します。
  - Enter Authentication Key — パスワードを入力します。
  - Confirm Authentication Key — 確認のために同じパスワードを入力します。
- c. **OK** をクリックします。

認証ボタンのラベルが Simple Password に変わります。

**ステップ 5** OSPF のプライオリティとインターバルの設定をプロビジョニングします。

OSPF のプライオリティとインターバルのデフォルト値は、OSPF ルータで最もよく使用される値です。これらのデフォルト値が、ONS 15454 の接続先 OSPF ルータで使用される値と一致していることを確認します。

- Router Priority — サブネットの指定ルータを選択します。
- Hello Interval (sec) — OSPF ルータが送信する OSPF hello パケットのアドバタイズ間隔の秒数を設定します。デフォルトは 10 秒です。
- Dead Interval — OSPF ルータのパケットが表示されなくなってから近接ルータがそのルータのダウンを宣言するまでの秒数を設定します。デフォルトは 40 秒です。
- Transit Delay (sec) — サービス速度を指示します。デフォルトは 1 秒です。
- Retransmit Interval (sec) — パケットを再送するまでの経過時間を設定します。デフォルトは 5 秒です。
- LAN Metric — LAN を介したパケット送信コストを設定します。この値は、常に DCC メトリックよりも小さな値にする必要があります。デフォルトは 10 です。

**ステップ 6** エリア範囲テーブルが必要な場合は、OSPF Area Range Table 領域で作成します。

**(注)** エリア範囲テーブルは、OSPF エリア境界外にある情報を統合するテーブルです。ONS 15454 の OSPF エリアにある ONS 15454 の 1 つは、OSPF ルータに接続されています。このノードにあるエリア範囲テーブルは、ONS 15454 の OSPF エリア内に存在する他のノードをルータに示します。

- a. OSPF Area Range Table 領域で、**Create** をクリックします。
- b. Create Area Range ダイアログボックスで次の項目を指定します。
  - Range Address — OSPF エリア内にある ONS 15454 のエリア IP アドレスを入力します。たとえば、ONS 15454 の OSPF エリア内に IP アドレスが 10.10.20.100、10.10.30.150、10.10.40.200、および 10.10.50.250 のノードがある場合、範囲アドレスは 10.10.0.0 となります。
  - Range Area ID — ONS 15454 の OSPF エリア ID を入力します。これは、DCC OSPF Area ID フィールドの ID または Area ID for LAN Port フィールドの ID のいずれかになります。
  - Mask Length — サブネット マスク長を入力します。上記の範囲アドレスの例では、この値は 16 になります。
  - Advertise — OSPF 範囲テーブルをアドバタイズする場合は、このボックスをオンにします。
- c. **OK** をクリックします。

**ステップ 7** すべての OSPF エリアはエリア 0 に接続されている必要があります。ONS 15454 の OSPF エリアが物理的にエリア 0 に接続されていない場合は、次のステップに従って仮想リンク テーブルを作成し、接続されていないエリアにエリア 0 への論理パスを提供します。

- a. OSPF Virtual Link Table 領域で、**Create** をクリックします。
- b. Create Virtual Link ダイアログボックスで、次のフィールドを設定します。OSPF の設定は、ONS 15454 の OSPF エリアの設定と一致する必要があります。
  - Neighbor — エリア 0 ルータのルータ ID。
  - Transit Delay (sec) — サービスの速度。デフォルトは 1 秒です。

- Hello Int (sec) — OSPF ルータが送信する OSPF hello パケットのアドバタイズ間隔の秒数。デフォルトは 10 秒です。
- Auth Type — ONS 15454 の接続先ルータが認証を使用する場合は、**Simple Password** を選択します。それ以外の場合は、**No Authentication** を選択します。
- Retransmit Int (sec) — パケットを再送するまでの経過時間を設定します。デフォルトは 5 秒です。
- Dead Int (sec) — OSPF ルータのパケットが表示されなくなってから近接ルータがそのルータのダウンを宣言するまでの秒数を設定します。デフォルトは 40 秒です。

c. **OK** をクリックします。

**ステップ 8** ONS 15454 の OSPF エリア データを入力したら、**Apply** をクリックします。

エリア ID を変更した場合は、一度に 1 つずつ TCC2/TCC2P カードがリセットされます。リセットには約 10 ~ 15 分かかります。表 19-2 に、TCC2/TCC2P リセット中の LED の動作を示しています。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A251 RIP の設定または変更

目的	この作業では、ONS 15454 にある Routing Information Protocol (RIP) をイネーブルにします。ONS 15454 を RIP イネーブルのネットワークに組み込みたい場合、この作業を実行します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > RIP** タブをクリックします。

**ステップ 2** RIP を有効にする場合は、**RIP Active** チェックボックスをオンにします。

**ステップ 3** ネットワークでサポートされているバージョンに応じて、ドロップダウン リストから RIP Version 1 または RIP Version 2 を選択します。

**ステップ 4** RIP メトリックを設定します。RIP メトリックは 1 ~ 15 までの数値に設定できます。これは、ホップ数を表します。

**ステップ 5** デフォルトでは、RIP は No Authentication に設定されています。ONS 15454 の接続先ルータが認証を必要とする場合は、次のステップを実行します。それ以外の場合は、**ステップ 6** へ進みます。

a. **No Authentication** ボタンをクリックします。

- b. Edit Authentication Key ダイアログボックスで次の項目を指定します。
  - Type — **Simple Password** を選択します。
  - Enter Authentication Key — パスワードを入力します。
  - Confirm Authentication Key — 確認のために同じパスワードを入力します。
- c. **OK** をクリックします。

認証ボタンのラベルが Simple Password に変わります。

**ステップ 6** アドレス サマリーを入力する場合は、次のステップを実行します。それ以外の場合は、[ステップ 7](#) へ進みます。アドレス サマリーは、ONS 15454 が GNE である場合だけ入力します。GNE では、異なるサブネットで複数の外部 ONS 15454 の NE が IP アドレスによって接続されています。

- a. RIP Address Summary エリアで、**Create** をクリックします。
- b. Create Address Summary ダイアログボックスで次の情報を入力します。
  - Summary Address — サマリー IP アドレスを入力します。
  - Mask Length — 上矢印と下矢印を使用してサブネット マスク長を入力します。
  - Hops — ホップ数を入力します。ホップ数が少ないほど、プライオリティが高くなります。
- c. **OK** をクリックします。

**ステップ 7** 元の手順 (NTP) に戻ります。

## DLP-A255 クロスコネク ト カードのサイド切り替えテスト

目的	この作業では、XCVT、XC10G、および XC-VXC-10G カードでサービスがアクティブとスタンバイの間で効果的に切り替えられることを確認します。
工具 / 機器	受け入れテストの手順で指定した、接続および設定済みのテスト セット
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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

クロスコネク ト カード (サイド) 切り替えには、常に 60 秒かかります。

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

**ステップ 2** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。



- b. 説明のつかないアラーム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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 3** **Conditions** タブをクリックします。説明のつかない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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 4** ネットワーク マップ上で、テスト対象のクロスコネク ト カードを取り付けたノードをダブルクリックして、ノード ビューで開きます。

**ステップ 5** **Maintenance > Cross-Connect** タブをクリックします。

**ステップ 6** **Cross-Connect Cards** エリアで、アクティブ スロットとスタンバイ スロットを記録します。

**ステップ 7** シェルフ図で、アクティブなクロスコネク ト カードに緑色の ACT LED が表示され、スタンバイのクロスコネク ト カードにオレンジ色の SBY LED が表示されていることを確認します。LED の状態が異なる場合は、「[DLP-A37 XCVT、XC10G、または XC-VXC-10G カードの取り付け](#)」(p.17-47)を参照するか、次のレベルのサポートに問い合わせます。

**ステップ 8** **Switch** をクリックします。

**ステップ 9** **Confirm Switch** ダイアログボックスで、**Yes** をクリックします。



(注) XC-VXC-10G カードおよび TCC2/TCC2P カードを使用して実行されたクロスコネク ト のサイド切り替えでは、エラーは発生しません。

**ステップ 10** ステップ 6 で記録したアクティブ スロットがスタンバイ スロットに変わり、スタンバイ スロットがアクティブ スロットに変わったことを確認します。通常は、1 ~ 2 秒で切り替わります。

**ステップ 11** ノードに接続されたテスト セットのトラフィックが動作していることを確認します。ビット エラーはあってもかまいませんが、トラフィック フローが中断する場合は問題があります。トラフィックが中断する場合は、作業を中断し、次のレベルのサポートに問い合わせます。

**ステップ 12** 60 秒待ってから、ステップ 7 ~ 9 を繰り返して、アクティブ / スタンバイ スロットをこの手順を開始したときの設定に戻します。

**ステップ 13** ステップ 6 で記録したとおりにクロスコネク ト カードが表示されることを確認します。

**ステップ 14** 元の NTP (手順) に戻ります。

## DLP-A256 イーサネット PM パラメータの表示：統計情報

目的	この作業では、イーサネットカードとポートについて現在の PM カウントの統計を表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 E シリーズまたは G 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 > Statistics タブをクリックします。
- 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 カラムに PM パラメータの名前が表示されるのを確認します。Port # カラムには PM パラメータの現在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 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-A253 PM カウントの表示変更](#)」(p.9-2)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-A257 イーサネット PM パラメータの表示：使用率

目的	この作業では、イーサネットカードとポートについて回線使用率の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 E シリーズまたは G 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 > Utilization タブをクリックします。
- 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使用率の値が表示されます。

**ステップ 4** モニタするポートを見つける場合は、Port # カラムを表示します。

**ステップ 5** これまでのインターバルでの送信 (Tx) および受信 (Rx) の帯域使用率の値が Prev-*n* 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。



(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-A253 PM カウントの表示変更」(p.9-2) 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-A258 イーサネット PM パラメータの表示：履歴

目的	この作業では、イーサネットカードおよびポートについて、選択したインターバルで統計をとった PM カウントの履歴を表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 E シリーズまたは G 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 > History タブをクリックします。

**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。Prev-*n* 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 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-A253 PM カウントの表示変更」(p.9-2) 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-A259 イーサネット PM カウントのリフレッシュ間隔の変更

目的	この作業では、指定した PM カウントが、選択したオプションに基づくインターバルで表示されるようにウィンドウの表示を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 タブをクリックします。



**(注)** CE シリーズおよび ML シリーズ カードについては、Performance > Ether Ports または Performance > POS Ports タブをクリックします。

**ステップ 3** Utilization タブまたは History タブをクリックします。

**ステップ 4** Interval ドロップダウン リストで、次の 4 つのオプションからいずれかを選択します。

- 1 min — 指定した PM カウントが 1 分間隔で表示されます。
- 15 min — 指定した PM カウントが 15 分間隔で表示されます。
- 1 hour — 指定した PM カウントが 1 時間間隔で表示されます。
- 1 day — 指定した PM カウントが 1 日 (24 時間) 間隔で表示されます。

**ステップ 5** Refresh をクリックします。選択したインターバルに基づいた値で PM カウントがリフレッシュされます。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A260 PM カウントの自動リフレッシュ間隔の設定

目的	この作業では、表示されている PM カウントを更新する、ウィンドウの自動リフレッシュ間隔を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Auto-refresh ドロップダウン リストから、次の 6 つのオプションのいずれかを選択します。
- **None** — 自動リフレッシュ機能をディセーブルにします。
  - **15 Seconds** — ウィンドウの自動リフレッシュ間隔を 15 秒に設定します。
  - **30 Seconds** — ウィンドウの自動リフレッシュ間隔を 30 秒に設定します。
  - **1 Minute** — ウィンドウの自動リフレッシュ間隔を 1 分に設定します。
  - **3 Minutes** — ウィンドウの自動リフレッシュ間隔を 3 分に設定します。
  - **5 Minutes** — ウィンドウの自動リフレッシュ間隔を 5 分に設定します。
- ステップ 4** Refresh をクリックします。新たに選択した自動リフレッシュ間隔で PM カウントが表示されます。
- 選択した自動リフレッシュ間隔に基づいて、リフレッシュ時間が経過するたびに表示の PM カウントが自動的に更新されます。自動リフレッシュ間隔を None に設定した場合は、Refresh をクリックしないかぎり PM カウントは更新されません。
- ステップ 5** 元の NTP (手順) に戻ります。
- 

## DLP-A261 別ポートの PM カウントのリフレッシュ

目的	マルチポート カードで別のポートの PM カウントを表示するようにウィンドウの表示を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Port ドロップダウン リストで、ポートを選択します。
- ステップ 4** Refresh をクリックします。新たに選択したポートの PM カウントが表示されます。
- ステップ 5** 元の NTP (手順) に戻ります。
-

## DLP-A262 回線表示のフィルタリング

目的	この作業は、Circuits ウィンドウで回線の表示をフィルタリングします。回線の名前、サイズ、タイプ、方向、およびその他の属性に基づいて、ネットワーク ビュー、ノード ビュー、またはカード ビューで回線のフィルタリングができます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- ネットワーク回線をフィルタリングする場合は、View メニューで **Go to Network View** を選択します。
- 特定のノードを、送信元または宛先とするかパススルーする回線をフィルタリングする場合は、View メニューで **Go to Other Node** を選択してから、検索するノードを選択して **OK** をクリックします。
- 特定のカードを、送信元または宛先とするかパススルーする回線をフィルタリングする場合は、シェルフ図でカードをダブルクリックして、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 回線表示をフィルタリングする属性を設定します。

- Filter** ボタンをクリックします。
- Circuit Filter ダイアログボックスの General タブで、必要に応じて次のフィルタ属性を設定します。
  - Name — 回線名で回線をフィルタリングする場合は、回線名または回線名の一部を入力します。それ以外の場合は空白にします。
  - Direction — **Any** (回線のフィルタリングに方向を使用しない) **1-way** (単方向の回線だけを表示) または **2-way** (双方向の回線だけを表示) のいずれかを選択します。
  - OCHNC Dir — (DWDM OCHNC のみ) **East to West** (イーストからウェストの回線だけを表示) **West to East** (ウェストからイーストの回線だけを表示) のいずれかを選択します。詳細については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。
  - OCHNC Wlen — (DWDM OCHNC のみ) 回線をフィルタリングする OCHNC 波長を選択します。たとえば、1530.33 は、1530.33 nm 波長でプロビジョニングされたチャネルを表示します。詳細については、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。
  - Status — 回線をフィルタリングするための回線ステータスを選択します。回線ステータスの詳細については、[表 21-2 \(p.21-3\)](#) を参照してください。
  - State — **OOS** (停止中の回線だけを表示) **IS** (稼働中の回線だけを表示、OCHNC の場合は IS のみ) または **OOS-PARTIAL** (複数のサービス状態のクロスコネクトを持つ回線だけを表示) のいずれかを選択します。
  - Protection — 回線をフィルタリングするための保護タイプを選択します。保護タイプの詳細については、[表 21-1 \(p.21-3\)](#) を参照してください。
  - Slot — 送信元スロットまたは宛先スロットに基づいて回線をフィルタリングする場合はスロット番号を入力します。それ以外の場合は空白のままにします。

- Port — 送信元ポートまたは宛先ポートに基づいて回線をフィルタリングする場合はポート番号を入力します。それ以外の場合は空白のままにします。
- Type — Any (回線のフィルタ処理にタイプを使用しない)、STS (STS 回線だけを表示)、VT (VT 回線だけを表示)、VT Tunnel (VT トンネルだけを表示)、STS-V (STS VCAT 回線だけを表示)、VT-V (VT VCAT 回線だけを表示)、VT Aggregation Point (VT 集約ポイントだけを表示) または OCHNC (OCHNC だけを表示、<sup>『Cisco ONS 15454 DWDM Procedure Guide』</sup>を参照) のいずれかを選択します。
- Size — サイズに基づいて回線をフィルタリングする場合は、VT1.5、VT2、STS-1、STS3c、STS-6c、STS-9c、STS-12c、STS-18c、STS-24c、STS-36c、STS-48c、STS-192c、Multi-rate、Equipment non specific、2.5 Gbps FEC、2.5 Gbps No FEC、10 Gbps FEC、または 10 Gbps No FEC の中から該当するチェックボックスをクリックします。

表示されるチェックボックスは、Type フィールドの選択により異なります。Any を選択するとすべてのサイズの回線が表示されます。VT を選択すると、VT1.5 または VT2 が表示されます。VT-V を選択すると、VT1.5 だけが表示されます。STS を選択すると、STS のサイズだけが表示されます。VT Tunnel または VT Aggregation Point を選択すると、STS-1 だけが表示されます。回線タイプに OCHNC を選択すると、Multi-rate、Equipped not specific、2.5 Gbps FEC、2.5 Gbps No FEC、10 Gbps FEC、および 10 Gbps No FEC が表示されます (DWDM のみ、<sup>『Cisco ONS 15454 DWDM Procedure Guide』</sup>を参照)。STS-V を選択すると、STS-1、STS3c、および STS-12c だけが表示されます。

**ステップ 4** リング、ノード、リンク、および送信元とドロップのタイプのフィルタを設定するには、Advanced タブをクリックして、次のサブステップを実行します。詳細フィルタを選択しない場合は、[ステップ 5](#) へ進みます。

- General タブで選択を行ったら、確認用ボックスで Yes をクリックして設定を適用します。
- Circuit Filter ダイアログボックスの Advanced タブで、必要に応じて次のフィルタ属性を設定します。
  - Ring — ドロップダウン リストからリングを選択します。
  - Node — ネットワークの各ノードでチェックボックスをクリックし、ノードに基づいて回線をフィルタリングします。
  - Link — ネットワークの対象リンクを選択します。
  - Source/Drop — 送信元とドロップが 1 つか複数かに基づいて回線をフィルタリングするため、One Source and One Drop Only または Multiple Sources or Multiple Drops のいずれかを選択します。

**ステップ 5** OK をクリックします。Filter Circuits ダイアログボックスの属性と一致する回線が Circuits ウィンドウに表示されます。

**ステップ 6** フィルタリングをオフにする場合は、Circuits ウィンドウの右下隅にある、Filter アイコンをクリックします。フィルタリングをオンにする場合はこのアイコンをもう一度クリックし、フィルタリングの属性を変更する場合は Filter ボタンをクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A263 UPSR DRI 回線ホールドオフ タイマーの編集

目的	この作業では、UPSR Dual-Ring Interconnect (DRI; デュアル リング相互接続) トポロジー上でルーティングした回線について、パス セクタ スイッチが遅延する時間を変更します。スイッチの Hold-Off Time (HOT; ホールド オフ時間) の設定により、回線が複数の UPSR セクタを介してルーティングされる場合に、不要な交互の切り替えを避けられます。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A44 UPSR ノードのプロビジョニング (p.5-27)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

DRI ポートの HOT 値をゼロに設定し、回線パス セクタの HOT 値をゼロ以上の数値に設定することを推奨します。

- 
- 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** **Circuits** タブをクリックします。
- ステップ 3** 編集する UPSR 回線をクリックし、**Edit** をクリックします。
- ステップ 4** Edit Circuit ウィンドウで、**UPSR Selectors** タブをクリックします。
- ステップ 5** 回線の送信元ポートと宛先ポートの HOT を作成します。
- a. Hold-Off Timer 領域で、回線の送信元ポート (上の行) のセルをダブルクリックしてから、新しい HOT を入力します。範囲は 0 ~ 10,000 ミリ秒で、100 ミリ秒単位で指定します。
  - b. Hold-Off Timer 領域で、回線の宛先ポート (下の行) のセルをダブルクリックしてから、ステップ a で入力した HOT を入力します。
- ステップ 6** **Apply** をクリックしてから、File メニューで **Close** を選択して Edit Circuit ウィンドウを閉じます。
- ステップ 7** 元の NTP (手順) に戻ります。
-



## DLP-A264 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

目的	この作業では、STS 回線の送信元ポートおよび宛先ポート、または VCAT 回線メンバー上に、パストレースを作成します。
工具 / 機器	回線の送信元ポートと宛先ポートには、パストレースを送受信できる ONS 15454 カードが取り付けられている必要があります。カードのリストは <a href="#">表 19-3</a> を参照してください。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) この作業では、双方向回線上にパストレースを設定することと、回線の送信元および宛先に送信文字列を設定することを前提としています。

- 
- 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** Circuits タブをクリックします。
  - ステップ 3** モニタする STS 回線で、送信元ポートと宛先ポートの存在するカードでパストレースの文字列を送受信できることを確認します。カードのリストは [表 19-3](#) を参照してください。

表 19-3 パス トレース対応の ONS 15454 カード

J1 の機能	カード
送受信	CE-1000-4
	CE-100T-8
	DS1-14 <sup>1</sup>
	DS1N-14
	DS1/E1-56
	DS3-12E
	DS3i-N-12
	DS3/EC1-48
	DS3N-12E
	DS3XM-6
	DS3XM-12
	G シリーズ
	ML シリーズ
	受信専用
OC3 IR 4/STM1 SH 1310	
OC3 IR 4/STM1 SH 1310-8	
OC12/STM4-4	
OC48 IR/STM16 SH AS 1310	
OC48 LR/STM16 LH AS 1550	
OC192 SR/STM64 IO 1310	
OC192 LR/STM64 LH 1550	
OC192 IR/STM SH 1550	
ML シリーズ	
FC_MR-4	

1. J1 パス トレースは、VT 回線で使用されている DS-1 ではサポートされていません。



**(注)** FC\_MR-4 カードの場合、パス トレースの文字列は VCAT 回線のすべてのメンバーで同一である必要があります。VCAT グループのメンバー間でパス トレースの文字列を混合させることはできません。FC\_MR-4 card view Maintenance > Path Trace サブタブでパス トレースの文字列を検索するとき、パス トレースの文字列が割り当てられたメンバーのみがパス トレース情報に表示されます。



(注) どちらのポートも送受信カード上に存在しない場合、この手順を完了することはできません。片方のポートが送受信カード上にあり、もう片方が受信専用カード上にある場合、送信文字列を送受信ポートで、受信文字列を受信専用ポートでそれぞれ設定できます。ただし、双方向に送信することはできません。

**ステップ 4** トレースする STS 回線を選択し、**Edit** をクリックします。

**ステップ 5** VCAT 回線を選択した場合、次の作業を行います。それ以外の場合は、**ステップ 6** へ進みます。

a. Edit Circuit ウィンドウで、**Members** タブをクリックします。

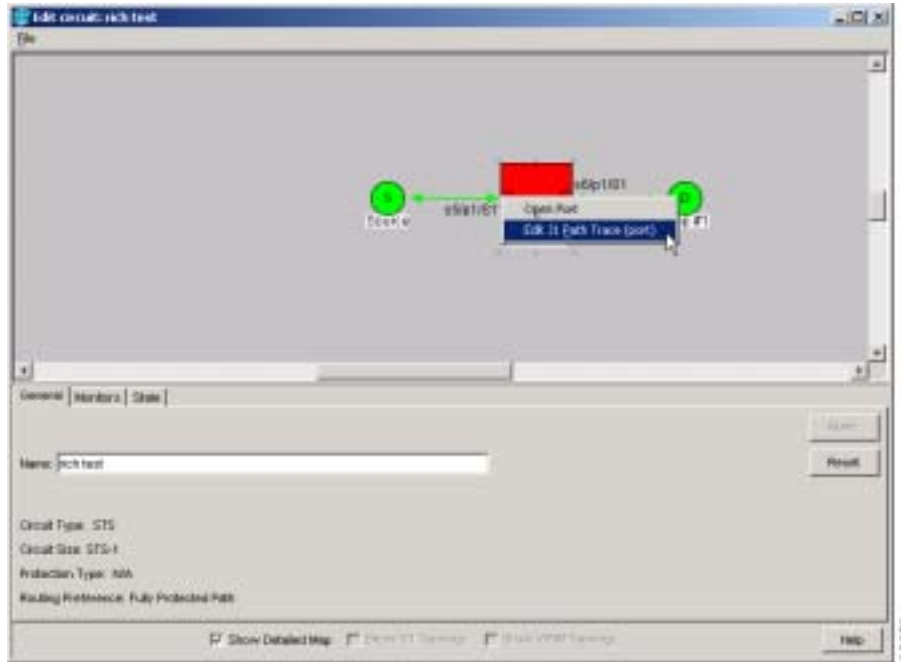
b. **Edit Member** をクリックし、**ステップ 6** へ進みます。

**ステップ 6** Edit Circuit ウィンドウで、ウィンドウ下部にある **Show Detailed Map** チェックボックスをクリックします。送信元ポートと宛先ポートの詳細マップが表示されます。

**ステップ 7** 回線の送信元が送信する文字列を、次の手順でプロビジョニングします。

a. 詳細回線マップで、回線の送信元ポート（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 J1 Path Trace (port)** を選択します。図 19-4 に例を示します。

図 19-4 Edit Path Trace オプションの選択



b. New Transmit String フィールドで、回線の送信元が送信する文字列を入力します。入力する文字列は、ノードの IP アドレス、ノード名、回線名、その他の文字列など、送信元のポートが容易に識別できるものにします。New Transmit String フィールドを空白のままにすると、J1 はヌル文字列を送信します。

c. **Apply** をクリックしてから **Close** をクリックします。

**ステップ 8** 回線の宛先が送信する文字列を、次の手順でプロビジョニングします。

- a. 詳細回線マップで回線の宛先ポートを右クリックし、ショートカットメニューから **Edit Path Trace** を選択します (図 19-4)。
- b. New Transmit String フィールドで、回線の宛先から送信する文字列を入力します。入力する文字列は、ノードの IP アドレス、ノード名、回線名、その他の文字列など、宛先ポートが容易に識別できるものにします。New Transmit String フィールドを空白のままにすると、J1 はヌル文字列を送信します。
- c. **Apply** をクリックします。

**ステップ 9** 回線の宛先で受信する予測文字列を、次の手順でプロビジョニングします。

- a. 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 — 送信元ポートから受信された最初の文字列が、現在の予測文字列として自動的にプロビジョニングされます。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。
  - Manual — Current Expected String フィールドに入力された文字列がベースラインになります。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。
- b. Path Trace Mode フィールドを Manual に設定した場合、回線の宛先が回線の送信元から受信する文字列を New Expected String フィールドに入力します。Path Trace Mode 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。
- c. STS Path Trace Identifier Mismatch Path (TIM-P) アラームが検出された場合に、Alarm Indication Signal (AIS; アラーム表示信号) および Remote Defect Indication (RDI; リモート障害表示) を抑制する場合は、**Disable AIS and RDI if TIM-P is detected** チェックボックスをクリックします。アラームおよび状態の説明については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- d. (チェックボックスの表示はカードの選択により異なります) C2 の不一致が発生したときに AIS を抑制する場合は、**Disable AIS on C2 Mis-Match** チェックボックスをクリックします。
- e. **Apply** をクリックしてから **Close** をクリックします。



**(注)** 回線の宛先で受信する予測文字列に関しては、形式 (16 バイトまたは 64 バイト) を設定する必要はありません。パストレースの処理で自動的に形式が判別されるからです。

**ステップ 10** 回線の送信元で受信する予測文字列を、次の手順でプロビジョニングします。

- a. Edit Circuit ウィンドウで (Show Detailed Map を選択、図 19-4 を参照) 回線の送信元ポートを右クリックし、ショートカットメニューから **Edit Path Trace** を選択します。
- b. 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 — ベースライン文字列として、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。
  - 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。
- c. Path Trace Mode フィールドを Manual に設定した場合は、回線の送信元が回線の宛先から受信する文字列を New Expected String フィールドに入力します。Path Trace Mode 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。

- d. TIM-P アラームが表示されたときに AIS および RDI を抑制する場合は、**Disable AIS and RDI if TIM-P is detected** チェックボックスをオンにします。アラームおよび状態の説明については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。
- e. (チェックボックスの表示はカードの選択により異なります) C2 の不一致が発生したときに AIS を抑制する場合は、**Disable AIS on C2 Mis-Match** チェックボックスをクリックします。
- f. **Apply** をクリックします。



(注) 回線の送信元で受信する予測文字列に関しては、形式(16バイトまたは64バイト)を設定する必要はありません。パストレースの処理で自動的に形式が判別されるからです。

**ステップ 11** パストレースを設定すると、パストレース設定ウィンドウの Received フィールドに受信した文字列が表示されます。次のオプションを指定します。

- パストレースを 16 進表記で表示する場合は、**Hex Mode** ボタンをクリックします。ボタンの名前が ASCII Mode に変わります。パストレースを ASCII 表記に戻す場合は、このボタンをクリックします。
- ポートから値を再度読み取る場合は、**Reset** ボタンをクリックします。
- パストレースのデフォルト設定に戻す場合は、**Default** をクリックします (Path Trace Mode は Off に、New Transmit String と New Expected String はヌルに設定されます)。

**注意**

相手ポートに異なる文字列がプロビジョニングされている場合に **Default** をクリックすると、アラームが発生します。

Path Trace Mode フィールドを Auto または Manual に設定した場合、予測文字列と受信文字列は数秒ごとに更新されます。

**ステップ 12** **Close** をクリックします。

詳細な回線マップでは、回線の送信元ポートと宛先ポートにパストレースが M (手動パストレース) または A (自動パストレース) という文字で表示されます。

**ステップ 13** 元の NTP (手順) に戻ります。

## DLP-A265 ログイン時の法的免責事項の説明の変更

目的	この作業は、CTC ログイン ダイアログボックスに表示される法的免責事項の説明を変更して、ユーザがネットワークにログインする際にユーザ仕様の情報を表示するようにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Legal Disclaimer > HTML** タブをクリックします。

**ステップ 2** 現在の文章はデフォルトです。ユーザ仕様の免責事項ではありません。この文章は、ユーザ側で会社の方針に合わせて変更できます。必要に応じて、次の HTML コマンドを使用してテキストの書式設定をします。

- `<b>` 太字の開始
- `</b>` 太字の終了
- `<center>` ウィンドウの中央に表示
- `</center>` 中央配置の終了
- `<font=n, n = ポイント サイズ>` フォント サイズの変更
- `</font>` フォント サイズ コマンドの終了
- `<p>` 改行
- `<sub>` 下付き文字の開始
- `</sub>` 下付き文字の終了
- `<sup>` 上付き文字の開始
- `</sup>` 上付き文字の終了
- `<u>` 下線の開始
- `</u>` 下線の終了

**ステップ 3** 変更した文章とその書式を確認する場合は、**Preview** サブタブをクリックします。

**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-A266 IP 設定の変更

目的	この作業では、IP アドレス、サブネット マスク、デフォルト ルータ、DHCP アクセス、ファイアウォール Internet Inter-ORB Protocol ( IOP ) リスナー ポート、LCD IP 表示、および SOCKS プロキシ サーバ設定を変更します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン ( p.17-71 )  DLP-A249 IP 設定のプロビジョニング ( p.19-35 )
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



### 注意

ノードの IP アドレスやサブネット マスク、あるいは IOP リスナー ポートを変更すると、TCC2/TCC2P はリポートされます。STP を使用しているイーサネット回線が、ノードに取り付けられた E シリーズイーサネット カード上で発信または終端する場合、回線トラフィックはスパンニング ツリーが再収束するまでの数分間中断されます。他の回線は TCC2/TCC2P のリポートによる影響を受けません。



### (注)

ノードに TCC2P カードが組み込まれ、デフォルト (リピータ) モードである場合、ノード IP アドレスは、バックプレーン LAN ポートと同様に、TCC2P フロントアクセス TCP/IP (LAN) ポートも参照します。ノードがセキュア モードである場合、この作業により、フロントアクセス ポート IP アドレスのみを変更します。ノードがセキュア モードでロックされている場合、Cisco Technical Support がロックを削除しない限り、IP アドレスは変更できません。

**ステップ 1** ノード ビューで、**Provisioning > Network > 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。

- IP Address
- Suppress CTC IP Display
- LCD IP Setting
- Default Router
- Forward DHCP Request To
- Net/Subnet Mask Length
- TCC CORBA (IOP) Listener Port
- Gateway Settings

フィールドの詳細については、「[DLP-A249 IP 設定のプロビジョニング](#)」(p.19-35) を参照してください。セキュア モードの詳細については、『[Cisco ONS 15454 Reference Manual](#)』にある「Management Network Connectivity」の章を参照してください。

**ステップ 3** Apply をクリックします。

IP アドレス、サブネット マスク、または TCC Common Object Request Broker Architecture (CORBA) Listener Port などの、ノードのリポートを伴うネットワーク フィールドの変更を行った場合、Change Network Configuration 確認ダイアログボックスが表示されます。ゲートウェイ設定を変更すると、ゲートウェイ フィールドの変更に関する確認ダイアログボックスが表示されます。

**ステップ 4** 確認のダイアログボックスが表示されたら、Yes をクリックします。

IP アドレス、サブネット マスク長、または TCC CORBA (IOP) Listener Port を変更すると、両方の ONS 15454 TCC2/TCC2P カードが一度に 1 つずつリポートします。TCC2/TCC2P カードがリポートされている間は、一時的にノードへ接続できなくなりますが、トラフィックには影響しません。TCC2/TCC2P のリポート動作については、表 19-2 を参照してください。

**ステップ 5** Provisioning > Network > General タブに、変更内容が表示されることを確認します。変更内容が表示されない場合は、作業を繰り返します。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』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-A268 ネットワーク ビューへのカスタム背景マップの適用

目的	この作業では、CTC ネットワーク ビューの背景イメージまたはマップを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)** ネットワーク ビューの背景イメージは、ローカルまたはネットワーク ドライブ上でアクセス可能な JPEG または GIF イメージに置き換えることができます。カスタム背景イメージを使用する場合、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フにします。**ステップ 2** View メニューから Go to Network View を選択します。**ステップ 3** ネットワークまたはドメイン マップを右クリックして、Set Background Image を選択します。**ステップ 4** Browse をクリックします。背景に使用するグラフィック ファイルを参照します。**ステップ 5** ファイルを選択します。Open をクリックします。



- ステップ 6** Apply をクリックして、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、これを繰り返します。
- 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-A269 ダイアログボックス非表示オプションのイネーブル化

目的	この作業では、ユーザが選択した非表示ダイアログボックスを以降のセッションに対してイネーブルにするか、非表示ダイアログボックスをディセーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

ある操作 (たとえば、回線の作成など) を実行する権限を持つユーザが、ダイアログボックスの [Do not show this dialog again] チェックボックスを選択すると、そのコマンドが以後の作業で上書きされないかぎり、同一のコンピュータからそのネットワーク上で同じ操作を実行する他のユーザに対しても、ダイアログボックスは表示されません (設定は、ノードのデータベースではなく、コンピュータに保存されます)。

- ステップ 1** Edit メニューから **Preferences** を選択します。
- ステップ 2** Preferences ダイアログボックスで、**General** タブをクリックします。
- Preferences Management area フィールドには、[Do not show this dialog again] がイネーブルになっているすべてのダイアログボックスが一覧表示されます。
- ステップ 3** 次のオプションのいずれかを選択するか、または表示したい個々のダイアログボックスをオフにします。
- **Don't Show Any** — 非表示のチェックボックスをすべて非表示にします。
  - **Show All** — 非表示チェックボックスの選択を無視して、すべてのダイアログボックスを表示します。
- 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-A271 セキュリティ ポリシーの変更：単一ノード

目的	この作業では、アイドル ユーザのタイムアウト、ユーザ ロックアウト、パスワード変更、同時ログイン ポリシーなど、単一ノードのセキュリティ ポリシーを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Policy** タブをクリックします。

**ステップ 2** アイドル ユーザのタイムアウト時間を変更するには、設定したいセキュリティ レベル（検索、メンテナンス、プロビジョニング、スーパーユーザ）の Idle User Timeout 領域にある hour (H) と minute (M) の矢印をクリックします。アイドル時間の範囲は、0 ~ 16 時間および 0 ~ 59 分です。ユーザは、アイドルユーザのタイムアウト時間に到達すると、ログアウトされます。

**ステップ 3** User Lockout 領域では、次の情報を修正します。

- Failed Logins Allowed Before Lockout — ユーザがノードにロックアウトされるまでの最大ログイン 試行回数を入力します。0 ~ 10 の範囲で値を選択します。
- Manual Unlock by Superuser — オンになっている場合、「スーパーユーザ」の権限を持つユーザは、ノードからロックアウトされたユーザを手動でロック解除できます。
- Lockout Duration — ユーザがログインに失敗したあと、ロックアウトされている時間を設定します。0 ~ 10 分および 0 ~ 55 秒（5 秒単位）の値を選択します。

**ステップ 4** Password Change 領域で、次の情報を修正します。

- Prevent Reusing Last [ ] Passwords — ユーザが同じパスワードを再度利用できるようになるまで、別のパスワードをいくつ作成しなければならないかという数を、1 ~ 10 の間で選択します。
- New Password must Differ from the Old Password by [ ] Characters — 古いパスワードと新しいパスワードで異ならなければならない文字数を選択します。デフォルトは 1 です。
- Cannot Change New Password for [ ] days — オンにすると、ユーザは指定した期間パスワードを変更できなくなります。範囲は 20 ~ 95 日です。
- Require Password Change on First Login to New Account — オンにすると、ユーザが初めて自分のアカウントにログインした際にパスワードの変更を要求します。

**ステップ 5** ユーザに定期的にパスワードの変更を要求するには、Password Aging 領域の Enforce Password Aging チェックボックスをオンにします。オンにしたら、次のパラメータを設定します。

- Aging Period — セキュリティ レベル（検索、メンテナンス、プロビジョニング、スーパーユーザ）ごとに、ユーザがパスワードを変更しなければなくなるまでの日数を設定します。範囲は 20 ~ 95 日です。
- Warning — セキュリティ レベルごとに、ユーザがパスワードの変更を警告されるまでの日数を設定します。範囲は 2 ~ 20 日です。

**ステップ 6** Other 領域で、次の情報を設定します。

- Single Session Per User — チェックを付けると、ユーザが一度にログインできるセッションを 1 つに制限します。
- Disable Inactive User — チェックを付けると、Inactive Duration ボックスで指定した日数ノードにログインしなかったユーザを無効にします。Inactive Duration の範囲は 0 ~ 99 日です。



**(注)** Inactive Duration ボックスのスレッシュホールドの日付を超えてノードの日付を進めると、ユーザ アカウントが無効になります。ノードの日付を戻して訂正しても、アカウントがすでに無効になっている場合、ユーザ アカウントは再度有効になりません。

**ステップ 7** Apply をクリックします。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A272 セキュリティ ポリシーの変更：複数ノード

目的	この作業では、アイドル ユーザのタイムアウト、ユーザ ロックアウト、パスワード変更、同時ログイン ポリシーなど、複数ノードのセキュリティ ポリシーを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** View メニューから **Go to Network View** を選択します。

**ステップ 2** **Provisioning > Security > Policy** タブをクリックします。読み取り専用のテーブルに、ノードの一覧とそのポリシーが表示されます。

**ステップ 3** 変更するテーブルのノードをクリックしてから、**Change** をクリックします。

**ステップ 4** アイドル ユーザのタイムアウト時間を変更するには、設定したいセキュリティ レベル (検索、メンテナンス、プロビジョニング、スーパーユーザ) の Idle User Timeout 領域にある hour (H) と minute (M) の矢印をクリックします。アイドル時間の範囲は、0 ~ 16 時間および 0 ~ 59 分です。ユーザは、アイドル ユーザのタイムアウト時間に到達すると、ログアウトされます。

**ステップ 5** User Lockout 領域では、次の情報を修正します。

- Failed Logins Allowed Before Lockout — ユーザがノードにロックアウトされるまでの最大ログイン試行回数を入力します。0 ~ 10 の範囲で値を選択します。
- Manual Unlock by Superuser — 「スーパーユーザ」の権限を持つユーザは、ノードからロックアウトされたユーザを手動でロック解除できます。
- Lockout Duration — ユーザがログインに失敗したあと、ロックアウトされている時間を設定します。0 ~ 10 分および 0 ~ 55 秒 (5 秒単位) の値を選択します。

**ステップ 6** Password Change 領域で、次の情報を修正します。

- Prevent Reusing Last [ ] Passwords — ユーザが同じパスワードを再度利用できるようになるまで、別のパスワードをいくつ作成しなければならないかという数を、1 ~ 10 の間で選択します。
- New Password must Differ from the Old Password by [ ] Characters — 古いパスワードと新しいパスワードで異ならなければならない文字数を選択します。デフォルトは 1 です。
- Cannot Change New Password for [ ] days — オンにすると、ユーザは指定した期間パスワードを変更できなくなります。範囲は 20 ~ 95 日です。
- Require Password Change on First Login to New Account — オンにすると、ユーザが初めて自分のアカウントにログインした際にパスワードの変更を要求します。

**ステップ 7** ユーザに定期的にパスワードの変更を要求するには、Password Aging 領域の Enforce Password Aging チェックボックスをオンにします。オンにしたら、次のパラメータを設定します。

- Aging Period — セキュリティ レベル（検索、メンテナンス、プロビジョニング、スーパーユーザ）ごとに、ユーザがパスワードを変更しなければなくなるまでの日数を設定します。範囲は 20 ~ 95 日です。
- Warning — セキュリティ レベルごとに、ユーザがパスワードの変更を警告されるまでの日数を設定します。範囲は 2 ~ 20 日です。

**ステップ 8** Other 領域で、次の情報を設定します。

- Single Session Per User — オンにすると、ユーザが一度にログインできるセッションを 1 つに制限します。
- Disable Inactive User — オンにすると、Inactive Duration ボックスで指定した日数ノードにログインしなかったユーザを無効にします。Inactive Duration の範囲は 0 ~ 99 日です。



**(注)** Inactive Duration ボックスのスレッシュホールドの日付を超えてノードの日付を進めると、ユーザ アカウントが無効になります。ノードの日付を戻して訂正しても、アカウントがすでに無効になっている場合、ユーザ アカウントは再度有効になりません。

**ステップ 9** Select Applicable Nodes 領域で、変更したくないノードをオフにします。

**ステップ 10** OK をクリックします。

**ステップ 11** Security Policy Change Results ダイアログボックスで、変更内容が正しいことを確認して OK をクリックします。

**ステップ 12** 元の NTP（手順）に戻ります。

## DLP-A273 SNMP トラップ宛先の修正

目的	この作業では、コミュニティ名、デフォルトの UDP ポート、SNMP (簡易ネットワーク管理プロトコル) トラップバージョン、1 秒間あたりの最大トラップ数など、ONS 15454 の SNMP トラップ宛先を修正します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 領域からトラップを選択します。

SNMP トラップの詳細については、『*Cisco ONS 15454 Reference Manual*』の「SNMP」の章を参照してください。

**ステップ 3** **Community** カラムの下の **Destination row** フィールドのエントリを選択して、別の有効なコミュニティ名にエントリを変更します。



**(注)** コミュニティ名は、認証とアクセス制御を組み合わせた形式で指定します。ONS 15454 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、ネットワーク管理システムのコミュニティ名と一致する必要があります。



**(注)** SNMP のデフォルトの UDP ポートは 162 です。

**ステップ 4** **Trap Version** フィールドを、SNMPv1 または SNMPv2 のいずれかに設定します。

SNMPv1 と 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 5** 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。このボックスがオフになっていると、SET 要求は拒否されます。

**ステップ 6** 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 レポート、およびパフォーマンス統計の取得ができるように、SNMP のプロキシ機能を設定する場合は、SNMP タブにある **Allow SNMP Proxy** チェックボックスをオンにします。

**ステップ 7** 汎用 SNMP MIB (管理情報ベース) の使用をイネーブルにする場合は、**Use Generic MIBs** チェックボックスをオンにします。

**ステップ 8** **Apply** をクリックします。

## DLP-A293 2 ファイバ BLSR での手動スパン アップグレード

**ステップ 9** SNMP の設定が変更されました。各ノードの SNMP 情報を表示する場合は、Trap Destinations 画面の Trap Destinations 領域でノードの IP アドレスを選択します。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A293 2 ファイバ BLSR での手動スパン アップグレード

目的	この作業では、2 ファイバの BLSR スパンを上位の OC-N の速度にアップグレードします。スパンをダウングレードする場合にもこの作業を繰り返しますが、その場合は <b>ステップ 5</b> で低速のカードを選択します。
工具 / 機器	高速のカード アップグレードに必要な互換ハードウェア
事前準備手順	アプリケーションによっては、減衰器が必要となる場合があります。 <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

**警告**

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。

**注意**

スパン アップグレード中に、これ以外の保守操作を実行したり回線を追加したりしないでください。

**(注)**

帯域幅が使用可能になる前に、BLSR のノードに接続されているすべてのスパンをアップグレードする必要があります。

**(注)**

BLSR Protection Channel Access (PCA) 回線が存在していた場合、それらの回線は既存の STS 内にそのまま残されます。そのため、これらの回線はアップグレード スパンの現用パスに配置され、BLSR の完全な保護を受けます。PCA 回線を アップグレード スパン内の保護チャンネルにルーティングする場合は、スパンをアップグレードしたあとにこれらの回線を削除して、再作成します。たとえば、OC-48 スパンを OC-192 にアップグレードした場合、OC-48 BLSR 内の保護 STS (STS 25 ~ 48) の PCA 回線は、既存の STS (STS 25 ~ 48)、つまり OC-192 BLSR 内で保護されている現用 STS 内にそのまま残されます。OC-48 PCA 回線を削除して再作成すると、回線は OC-192 BLSR 内の STS 96 ~ 192 に移動します。回線の削除については、「[NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除](#)」(p.7-6)を参照してください。回線の作成については、第 6 章「[回線と VT トンネルの作成](#)」を参照してください。

- 
- ステップ 1** 最初にアップグレードするスパンの両方のエンドポイント( ノード )に強制切り替えを適用します。  
「[DLP-A303 BLSR 強制リング切り替えの開始](#)」(p.20-3) を参照してください。
- ステップ 2** 両方のエンドポイントからファイバを取り外し、トラフィックがまだ流れていることを確認します。
- ステップ 3** 両方のエンドポイントから OC-N カードを取り外します。
- ステップ 4** ノード ビューで、両方のエンドポイントから各 OC-N スロットを右クリックし、**Change Card** を選択します。
- ステップ 5** Change Card ダイアログボックスで、新しい OC-N カード タイプを選択します。
- ステップ 6** OK をクリックします。
- ステップ 7** 「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行して、両方のエンドポイントに新しい OC-N カードを取り付けます。
- ステップ 8** 送受信信号が許容範囲内にあることを確認します。OC-N カードの送受信レベルについては、[表 2-4 \(p.2-20\)](#) を参照してください。受信レベルがそのカードの許容範囲外にある場合、それに応じて減衰させます。
- ステップ 9** 「[DLP-A44 BLSR 構成での光ファイバケーブルの取り付け](#)」(p.17-55) を行って、カードにファイバを接続します。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 10** 両方のエンドポイント ノードでカードが正常にアップグレードされ、すべてのファシリティ アラーム (Loss of Signal [LOS; 信号損失]、SD、および SF) がクリアされたら、アップグレードされたスパンの両方のエンドポイントから強制切り替えを解除します。「[DLP-A194 BLSR 強制リング切り替えのクリア](#)」(p.18-65) を参照してください。
- ステップ 11** 試験リング テストを実行して、トラフィックを切り替えずに、BLSR リング機能を確認します。  
「[DLP-A217 BLSR の試験リング テスト](#)」(p.19-12) を参照してください。
- ステップ 12** BLSR の各スパンについてこの作業を繰り返します。各スパンの作業が完了すると、アップグレードは完了です。
- ステップ 13** 元の NTP (手順) に戻ります。
-

## DLP-A294 4 ファイバ BLSR での手動スパン アップグレード

目的	この作業では、4 ファイバの BLSR スパンを上位の OC-N の速度にアップグレードします。各スパンを上位の OC-N の速度にアップグレードするには、この作業を繰り返します。スパンをダウングレードする場合にもこの作業を繰り返しますが、その場合は <b>ステップ 5</b> で低速のカードを選択します。
工具 / 機器	高速のカード  アップグレードに必要な互換ハードウェア
事前準備手順	アプリケーションによっては、減衰器が必要となる場合があります。 <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



### 警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



### 注意

スパン アップグレード中に、これ以外の保守操作を実行したり回線を追加したりしないでください。



### (注)

帯域幅が使用可能になる前に、BLSR のノードに接続されているすべてのスパンをアップグレードする必要があります。



### (注)

BLSR PCA 回線が存在していた場合、それらの回線は既存の STS 内にそのまま残されます。そのため、これらの回線はアップグレード スパンの現用パスに配置され、BLSR の完全な保護を受けます。PCA 回線をアップグレード スパン内の保護チャンネルにルーティングする場合は、スパンをアップグレードしたあとにこれらの回線を削除して、再作成します。たとえば、OC-48 スパンを OC-192 にアップグレードした場合、OC-48 BLSR 内の保護 STS (STS 25 ~ 48) の PCA 回線は、既存の STS (STS 25 ~ 48) つまり OC-192 BLSR 内で保護されている現用 STS 内にそのまま残されます。OC-48 PCA 回線を削除して再作成すると、回線は OC-192 BLSR 内の STS 96 ~ 192 に移動します。回線の削除については、「[NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除](#)」(p.7-6) を参照してください。回線の作成については、[第 6 章「回線と VT トンネルの作成」](#) を参照してください。

**ステップ 1** 最初にアップグレードするスパンの両方のエンドポイント(ノード)に強制切り替えを適用します。「[DLP-A303 BLSR 強制リング切り替えの開始](#)」(p.20-3) を参照してください。

**ステップ 2** 両方のスパン エンドポイント(ノード)で現用カードと保護カードからファイバを取り外し、トラフィックがまだ流れていることを確認します。



- ステップ 3** 両方のエンドポイントから OC-N カードを取り外します。
- ステップ 4** スパンのエンドポイントの両端について、ノードビューで各 OC-N スロットを右クリックし、**Change Card** を選択します。
- ステップ 5** Change Card ダイアログボックスで、新しい OC-N カードタイプを選択します。
- ステップ 6** OK をクリックします。
- ステップ 7** 「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行して、両方のエンドポイントに新しい OC-N カードを取り付けます。
- ステップ 8** 送信信号が許容範囲内にあることを確認します。OC-N カードの送受信レベルについては、[表 2-4](#) (p.2-20) を参照してください。
- ステップ 9** 「[DLP-A44 BLSR 構成での光ファイバケーブルの取り付け](#)」(p.17-55) を行って、カードにファイバを接続します。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 10** 両方のエンドポイント ノードのカードが正常にアップグレードされ、すべてのファシリティ アラーム (LOS、SD、および SF) がクリアされたら、アップグレードされたスパンの両方のエンドポイント (ノード) から強制切り替えを解除します。「[DLP-A194 BLSR 強制リング切り替えのクリア](#)」(p.18-65) を参照してください。
- ステップ 11** 試験リング テストを実行して、トラフィックを切り替えずに、BLSR リング機能を確認します。「[DLP-A217 BLSR の試験リング テスト](#)」(p.19-12) を参照してください。
- ステップ 12** BLSR の各スパンについてこれらのステップを繰り返します。BLSR リング内のすべてのスパンがアップグレードされると、リングがアップグレードされます。
- ステップ 13** 元の NTP (手順) に戻ります。

## DLP-A295 UPSR での手動スパン アップグレード

目的	この作業では、UPSR スパンを上位の OC-N の速度にアップグレードします。リング全体を上位の OC-N の速度にアップグレードするには、各スパンに対してこの作業を繰り返します。スパンをダウングレードする場合にもこの作業を繰り返しますが、その場合は <b>ステップ 5</b> で低速のカードを選択します。
工具 / 機器	高速のカード
事前準備手順	アップグレードに必要な互換ハードウェア
必須 / 適宜	<a href="#">DLP-A60 CTC へのログイン</a> (p.17-71)
オンサイト / リモート	適宜
セキュリティ レベル	オンサイト
	プロビジョニング以上のレベル

**警告**

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。

**注意**

スパン アップグレード中に、これ以外の保守操作を実行したり回線を追加したりしないでください。

- 
- ステップ 1** 「[DLP-A197 UPSR 強制切り替えの開始](#)」(p.18-68) を行って、アップグレードするスパンに強制切り替えを適用します。
- ステップ 2** スパンの両方のエンドポイント ノードからファイバを取り外し、トラフィックがまだ流れていることを確認します。
- ステップ 3** 両方のスパンのエンドポイントから OC-N カードを取り外します。
- ステップ 4** スパンの両端について、ノード ビューで各 OC-N スロットを右クリックし、**Change Card** を選択します。
- ステップ 5** Change Card ダイアログボックスで、新しい OC-N カード タイプを選択します。
- ステップ 6** OK をクリックします。
- ステップ 7** 「[NTP-A16 光カードおよびコネクタの取り付け](#)」(p.2-8) を実行して、両方のエンドポイントに新しい OC-N カードを取り付けます。
- ステップ 8** 送信信号が許容範囲内にあることを確認します。OC-N カードの送受信レベルについては、[表 2-4 \(p.2-20\)](#) を参照してください。
- ステップ 9** 「[DLP-A43 UPSR 構成での光ファイバケーブルの取り付け](#)」(p.17-51) を行って、カードにファイバを接続します。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 10** 両方のエンドポイント ノードのカードが正常にアップグレードされ、すべてのファシリティ アラーム (LOS、SD、および SF) がクリアされたら、「[DLP-A198 UPSR 強制切り替えのクリア](#)」(p.18-69) を行います。
- ステップ 11** 元の NTP (手順) に戻ります。
-

## DLP-A296 1+1 保護グループでの手動スパン アップグレード

目的	この作業では、リニア スパンを上位の OC-N の速度にアップグレードします。スパンをダウングレードする場合にもこの作業に従いますが、その場合は <b>ステップ 6</b> で低速のカードを選択します。
工具 / 機器	高速のカード
事前準備手順	アップグレードに必要な互換ハードウェア 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
セキュリティ レベル	プロビジョニング以上のレベル



### 警告

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。



### 注意

スパン アップグレード中に、これ以外の保守操作を実行したり回線を追加したりしないでください。

- ステップ 1** 保護ポートから順に、アップグレードするポートで強制切り替えを開始します。
- ノード ビューで、**Maintenance > Protection** タブをクリックします。
  - Protection Groups 領域から保護グループを選択します。Selected Group 領域に、現用スパンおよび保護スパンが表示されます。
  - Selected Group 領域で、保護 OC-N ポートをクリックします。
  - Switch Commands で、**Force** を選択します。
  - 確認用のダイアログボックスで **Yes** をクリックします。  
強制切り替えを適用するスパンの隣に FORCE-SWITCH-TO-WORKING が表示されます。
- ステップ 2** マルチポート カードをアップグレードする場合、各ポートで**ステップ 1**を繰り返します。
- ステップ 3** スパンの両端からファイバを取り外し、トラフィックがまだ流れていることを確認します。
- ステップ 4** 両方のスパンのエンドポイントから OC-N カードを取り外します。
- ステップ 5** スパンの両端について、ノード ビューで各 OC-N スロットを右クリックし、**Change Card** を選択します。
- ステップ 6** Change Card ダイアログボックスで、新しい OC-N カード タイプを選択します。
- ステップ 7** OK をクリックします。
- ステップ 8** 「NTP-A16 光カードおよびコネクタの取り付け」(p.2-8) を実行して、両方のエンドポイントに新しい OC-N カードを取り付けます。

## ■ DLP-A297 非保護スパンでの手動スパン アップグレード

- ステップ 9** 送信信号が許容範囲内にあることを確認します。OC-N カードの送受信レベルについては、表 2-4 (p.2-20) を参照してください。
- ステップ 10** 「DLP-A428 1+1 構成での光ファイバケーブルの取り付け」(p.21-8) を行って、カードにファイバを接続します。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 11** スパンの両端のカードが正常にアップグレードされ、すべてのファシリティ アラーム (LOS、SD、および SF) がクリアされたら、次の手順で強制切り替えを解除します。
- a. ノード ビューで、Maintenance > Protection タブをクリックします。
  - b. Protection Groups 領域で、クリアするカードまたはポートを含む保護グループをクリックします。
  - c. Selected Group 領域で、クリアするカードをクリックします。
  - d. Switch Commands で、Clear を選択します。
  - e. 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 12** 1+1 リニア構成の他のスパンについてこの作業を繰り返します。
- ステップ 13** 元の NTP (手順) に戻ります。

## DLP-A297 非保護スパンでの手動スパン アップグレード

目的	この作業では、非保護スパンを上位の OC-N の速度に手動でアップグレードします。
工具 / 機器	高速のカード
事前準備手順	アップグレードに必要な互換ハードウェア
必須 / 適宜	DLP-A60 CTC へのログイン (p.17-71)
オンサイト / リモート	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

**警告**

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。

**注意**

非保護スパンをアップグレードすると、そのスパンで伝送されているすべてのトラフィックが失われます。

**注意**

スパン アップグレード中に、これ以外の保守操作を実行したり回線を追加したりしないでください。

**注意**

ファイバを取り外すと、非保護スパンのすべてのトラフィックが失われます。

- 
- ステップ 1** スパンの両方のエンドポイント ノードからファイバを取り外します。
- ステップ 2** 両方のスパンのエンドポイントから OC-N カードを取り外します。
- ステップ 3** スパンの両端について、ノード ビューで各 OC-N スロットを右クリックし、**Change Card** を選択します。
- ステップ 4** Change Card ダイアログボックスで、新しい OC-N タイプを選択します。
- ステップ 5** OK をクリックします。
- ステップ 6** 両方のノードについてステップ 2 ~ 5 が完了したら、両方のエンドポイントに新しい OC-N カードを取り付け、ファイバをカードに接続します。IMPROPRMVL アラームがクリアされ、カードがアクティブになるまで待ちます。
- ステップ 7** 元の NTP (手順) に戻ります。
- 

## DLP-A298 ネットワーク上のアラームおよび状態のチェック

目的	この作業では、ネットワーク上にアラームや状態が存在しないことを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** View メニューから **Go to Network View** を選択します。ネットワーク マップ上で、影響を受けるすべてのスパンがグリーンであることを確認します。
- ステップ 2** ネットワーク マップ上で、影響を受けるスパンにアクティブな切り替えが存在しないことを確認します。スパン リングの切り替えは、ロックアウト リングの場合は [L]、強制リングの場合は [F]、手動リングの場合は [M]、試験リングの場合は [E] という文字で表されます。
- ステップ 3** 別の方法として、Conditions タブから確認することもできます。**Retrieve Conditions** をクリックして、アクティブな切り替えが存在しないことを確認します。Filter ボタンが選択されていないことを確認します。
- ステップ 4** 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。

- b. 説明のつかないアラーム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。表示されている場合は、操作を続ける前にこれらのアラームをよく調べて解決してください。手順については、『Cisco ONS 15454 Troubleshooting Guide』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-A299 BLSR スパン ロックアウトの開始

目的	この作業では、BLSR スパンのロックアウトを実行できます。これにより、トラフィックがロックアウトされたスパンに切り替わるのを防ぎます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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**

スパンのロックアウト中、トラフィックは保護されません。

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

**ステップ 2** BLSR を選択して、Edit をクリックします。



**ヒント** BLSR チャネル (ポート) の情報を見やすくするためなど、アイコンを新しい場所へ移動する場合は、Edit BLSR のネットワーク図でアイコンをドラッグアンドドロップします。

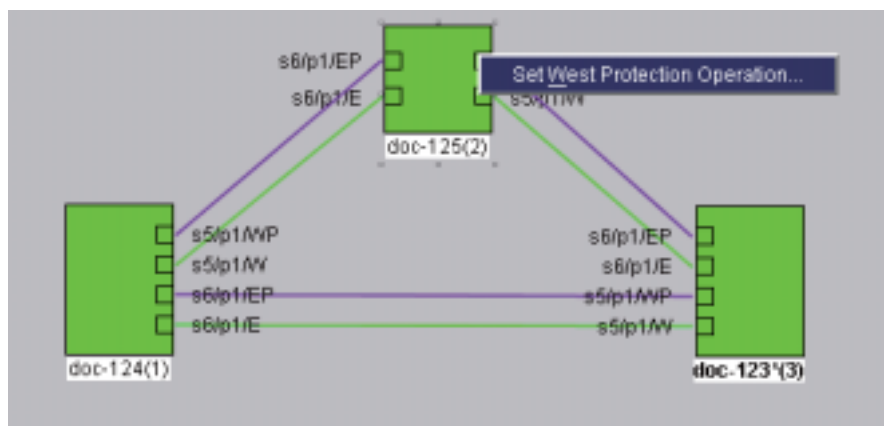
**ステップ 3** 次の手順で、ウェスト スパンをロックアウトします。

- a. BLSR ノードのウェスト チャネル (ポート) を右クリックして、**Set West Protection Operation** を選択します。図 19-5 に例を示します。



**(注)** 2 ファイバの BLSR の場合、ノード アイコンの四角形は、BLSR の現用チャネルと保護チャネルを表します。いずれかのチャネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。どちらの現用ポートも右クリックできます。

図 19-5 3 ノードの BLSR の保護操作



- 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 **LOCKOUT PROTECT SPAN** を選択します。OK をクリックします。
- c. Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。ロックアウトを作成した選択チャンネル (ポート) 上に、[L] が表示されます。

ロックアウトは、LKOUTPR-S 状態と FE-LOCKOUTOFPR-SPAN 状態を生成します。

**ステップ 4** 次の手順を実行して、イースト スパンをロックアウトします。

- a. ノードのイースト チャンネル (ポート) を右クリックして、Set East Protection Operation を選択します。
- 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 **LOCKOUT PROTECT SPAN** を選択します。OK をクリックします。
- c. Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。保護切り替えを起動した選択チャンネル (ポート) 上に、ロックアウトを示す [L] が表示されます。

ロックアウトは、LKOUTPR-S 状態と FE-LOCKOUTOFPR-SPAN 状態を生成します。

**ステップ 5** File メニューから、Close を選択します。

**ステップ 6** 元の NTP (手順) に戻ります。







## DLP A300 ~ A399

### DLP-A300 BLSR スパン ロックアウトのクリア

目的	この作業では、Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング) スパン ロックアウトをクリアします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 メニューで、**Go to Network View** を選択します。

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

**ステップ 3** BLSR を選択して、**Edit** をクリックします。



**ヒント** BLSR チャンネル (ポート) の情報を見やすくするためなど、アイコンを新しい場所へ移動する場合は、Edit BLSR のネットワーク図でアイコンをドラッグアンドドロップします。

**ステップ 4** ロックアウトを解除する BLSR ノード チャンネル (ポート) を右クリックして、**Set West Protection Operation** または **Set East Protection Operation** を選択します。

**ステップ 5** ダイアログボックス内で、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。

**ステップ 6** Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。ロックアウトを表す [L] が、ネットワーク ビュー マップに表示されなくなります。

**ステップ 7** File メニューから、**Close** を選択します。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A301 BLSR 手動リング切り替えの開始

目的	この作業では、BLSR 手動リング切り替えを実行します。手動リング切り替えでトラフィックがスパンから切り替わるのは、より高いプライオリティの切り替え（強制またはロックアウト）がなく、しかも Signal Degrade (SD; 信号劣化) 状態でも Signal Failure (SF; 信号障害) 状態でもない場合です。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 メニューで、**Go to Network View** を選択します。

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

**ステップ 3** BLSR を選択して、**Edit** をクリックします。



**ヒント** BLSR チャンネル (ポート) の情報を見やすくするためなど、アイコンを新しい場所へ移動する場合は、アイコンをクリックして新しい場所にドラッグアンドドロップします。

**ステップ 4** 任意の BLSR ノードチャンネル (ポート) を右クリックし、**Set West Protection Operation** (ウェストチャンネルを選択した場合) または **Set East Protection Operation** (イーストチャンネルを選択した場合) を選択します。



**(注)** ノード アイコン上の四角形は、BLSR の現用チャンネルと保護チャンネルを表しています。いずれかのチャンネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。いずれかの現用ポートを右クリックします。

**ステップ 5** Set West Protection Operation ダイアログボックス、または 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 **MANUAL RING** を選択します。 **OK** をクリックします。

**ステップ 6** 2 つの Confirm BLSR Operation ダイアログボックスで、**Yes** をクリックします。

**ステップ 7** チャンネル (ポート) に手動リングを表す文字 [M] が表示されていることを確認します。手動切り替えが起動されたノード間のスパン ラインがパープルに変わり、他のすべてのノード間のスパン ラインがネットワーク ビュー マップでグリーンに変わっていることも確認します。これにより、手動切り替えが実行されたことを確認できます。

**ステップ 8** File メニューから、**Close** を選択します。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A303 BLSR 強制リング切り替えの開始

目的	この作業を使用して、BLSR ポートの BLSR 強制切り替えを実行します。強制リング切り替えでトラフィックがスパンから切り替わるのは、スパンに SD、SF、またはロックアウト切り替えがない場合です。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。



### 注意

強制保護の切り替え中は、トラフィックは保護されません。

- 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** **Provisioning > BLSR** 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** 次の手順を実行して、ウェストラインに強制切り替えを適用します。
  - a. BLSR トラフィックを切り替えする BLSR のウェストポートを右クリックして、**Set West Protection Operation** を選択します。



**(注)** ノードアイコンが重なっている場合は、アイコンを別の場所にドラッグアンドドロップします。BLSR のノードアイコンはネットワークビューのノードアイコンの位置に基づいているため、ネットワークビューに戻ってネットワークノードアイコンの位置を変更することもできます。



**(注)** 2 ファイバの BLSR の場合、ノードアイコンの四角形は、BLSR の現用チャネルと保護チャネルを表します。いずれかのチャネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。いずれかの現用ポートを右クリックします。

- 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 **FORCE RING** を選択します。OK をクリックします。

- c. 表示された 2 つの Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。
- ネットワーク図では、保護切り替えを呼び出した現用 BLSR チャンネルに F が表示されます。強制されたトラフィックを反映して、スパン ラインの色が変わります。緑色のスパン ラインは新しい BLSR パスを示し、保護切り替え間のラインはパープルになります。
- 強制切り替えを行うと、FORCED-REQ-RING や WKSWPR など、いくつかの状態が生成されます。

**ステップ 5** 次の手順を実行して、イーストラインに強制切り替えを適用します。

- a. イースト BLSR ポートを右クリックして、**Set East Protection Operation** を選択します。



**(注)** ノード アイコンが重なっている場合は、アイコンを新しい場所にドラッグ アンド ドロップします。または、BLSR ノードのアイコンはネットワーク ビューのノード アイコンの位置に基づいているため、ネットワーク ビューに戻ってネットワーク ノード アイコンの位置を変更します。



**(注)** 2 ファイバの BLSR の場合、ノード アイコンの四角形は、BLSR の現用チャンネルと保護チャンネルを表します。いずれかのチャンネルを右クリックします。4 ファイバ BLSR の場合、四角形はポートを表します。いずれかの現用ポートを右クリックします。

- 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 **FORCE RING** を選択します。OK をクリックします。
- c. 表示された 2 つの Confirm BLSR Operation ダイアログボックスで、Yes をクリックします。
- ネットワーク図では、保護切り替えを呼び出した現用 BLSR チャンネルに F が表示されます。強制されたトラフィックを反映して、スパン ラインの色が変わります。緑色のスパン ラインは新しい BLSR パスを示し、保護切り替え間のラインはパープルになります。
- 強制切り替えを行うと、FORCED-REQ-RING や WKSWPR など、いくつかの状態が生成されます。

**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-A309 イーサネット MAC アドレス テーブルの表示

目的	この作業では、1 つまたは複数の E シリーズ イーサネット カードが取り付けられているすべてのノードについて、イーサネットの MAC (メディア アクセス制御) アドレス テーブルを表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、Maintenance > Ether Bridge > MAC Table タブをクリックします。

**ステップ 2** Layer 2 Domain フィールドで適切な E シリーズ イーサネット カードを選択します。

**ステップ 3** Retrieve をクリックします。

MAC アドレス テーブルの情報が表示されます。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A310 イーサネット トランクの使用率の表示

目的	この作業では、1 つまたは複数の E シリーズ イーサネット カードが取り付けられているすべてのノードについて、イーサネットのトランク帯域幅の使用率を表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、Maintenance > Ether Bridge > Trunk Utilization タブをクリックします。

**ステップ 2** Interval フィールドでインターバルを選択します。

**ステップ 3** Refresh をクリックします。

現在と前回のインターバルでのトランク使用率情報が表示されます。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A311 BLSR または 1+1 構成での半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、BLSR と 1+1 構成で半回線の送信元と宛先をプロビジョニングします。半回線を使用すると、一部のパス (回線の一端) をプロビジョニングできます。たとえば、パスの完成をあと回しにしたり、別の位置で行えるように回線をプロビジョニングできます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、回線の送信元と宛先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 リストから半回線を含む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カードが取り付けられているスロットを選択します。
- ステップ 3** Port ドロップダウン リストから回線の送信元になるポートを選択します。 **ステップ 2** で DS-1 カードが選択されている場合は、このフィールドを使用できません。
- ステップ 4** 回線が DS-1 で、送信元に DS-1 カードを選択する場合、DS-1 ドロップダウン リストからトラフィックの送信元となる DS-1 を選択します。
- 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、 **ステップ 1** で選択した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、OC-N 転送に DS-1 を VT1.5 にマップする OC-N カードを選択するか、DS-3 または OC-N の Synchronous Transport Signal ( STS; 同期転送信号 ) 回線を STS にマップする OC-N カードを選択します。
- ステップ 8** 表示されたドロップダウン リストから 宛先の STS または Virtual Tributary ( VT ) を選択します。
- ステップ 9** 元の NTP ( 手順 ) に戻ります。
- 

## DLP-A312 UPSR での半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、Unidirectional Path Switched Ring ( UPSR; 単方向パススイッチ型リング ) 構成で、半回線の送信元と宛先をプロビジョニングします。半回線を使用すると、一部のパス ( 回線の一端 ) をプロビジョニングできます。たとえば、パスの完成をあと回しにしたり、別の位置で行えるように回線をプロビジョニングできます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
必須 / 適宜	Circuit Creation ウィザードの Circuit Source ページを開いておく必要があります。
オンサイト / リモート	適宜
セキュリティ レベル	オンサイトまたはリモート プロビジョニング以上のレベル

- 
- ステップ 1** Node ドロップダウン リストから半回線を含む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カードが取り付けられているスロットを選択します。
- ステップ 3** Port ドロップダウン リストから回線の送信元になるポートを選択します。 **ステップ 2** で DS-1 カードが選択されている場合は、このフィールドを使用できません。
- ステップ 4** 回線が DS-1 で、送信元に DS-1 カードを選択する場合、DS-1 ドロップダウン リストからトラフィックの送信元となる DS-1 を選択します。
- 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、 **ステップ 1** で選択した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、OC-N 転送に DS-1 を VT1.5 にマップする OC-N カードを選択するか、DS-3 または OC-N の STS 回線を STS にマップする OC-N カードを選択します。
- ステップ 8** 表示されたドロップダウン リストから宛先の STS または VT を選択します。
- ステップ 9** Use Secondary Destination をクリックして、ステップ 6 ~ 8 を繰り返します。
- ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A313 DCC トンネルの作成

目的	この作業では、ONS 15454 ネットワークを経由してサードパーティ製の SONET 機器からトラフィックを転送する Data Communication Channel (DCC; データ通信チャンネル) トンネルを作成します。トンネルは、Section DCC (SDCC) チャンネル (D1-D3) (終端の DCC として ONS 15454 が使用しない場合) または任意の Line DCC (LDCC) チャンネル (D4-D6、D7-D9、または D10-D12) 上に作成できます。
工具 / 機器	OC-N カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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 トンネル接続の最大数は 84 にすることを推奨します。ONS 15454 が使用する終端の SDCC は、DCC トンネルのエンドポイントとしては使用できません。また、DCC トンネルのエンドポイントとして使用される SDCC は終端できません。DCC トンネル接続はすべて双方向です。

- ステップ 1** ネットワーク ビューで、Provisioning > Overhead Circuits 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** Overhead Circuit Creation ダイアログボックスの Circuit Attributes 領域で次の項目を指定します。

- Name — トンネル名を入力します。
- Circuit Type — 次のいずれかを選択します。
  - **DCC Tunnel-D1-D3** — 送信元エンドポイントまたは宛先エンドポイントとして、SDCC (D1-D3) または LDCC (D4-D6、D7-D9、または D10-D12) を選択できます。
  - **DCC Tunnel-D4-D12** — LDCC 全体をトンネルとしてプロビジョニングします。

**ステップ 4** Next をクリックします。

**ステップ 5** Circuit Source 領域で次の項目を指定します。

- Node — 送信元ノードを選択します。
- Slot — 送信元スロットを選択します。
- Port — 表示された場合は、送信元ポートを選択します。
- Channel — トンネルタイプとして DCC Tunnel-D1-D3 を選択した場合は、次のオプションが表示されます。次のいずれかを選択します。
  - **DCC1 (D1-D3)** — これは SDCC です。
  - **DCC2 (D4-D6)** — これは LDCC 1 です。
  - **DCC3 (D7-D9)** — これは LDCC 2 です。
  - **DCC4 (D10-D12)** — これは LDCC 3 です。

DCC オプションは、ONS 15454 (DCC1) またはその他のトンネルでその DCC が使用されていると、表示されません。

**ステップ 6** Next をクリックします。

**ステップ 7** Circuit Destination 領域で、次の項目を指定します。

- Node — 宛先ノードを選択します。
- Slot — 宛先スロットを選択します。
- Port — 表示された場合は、宛先ポートを選択します。
- Channel — トンネルタイプとして DCC Tunnel-D1-D3 を選択した場合は、次のオプションが表示されます。次のいずれかを選択します。
  - **DCC1 (D1-D3)** — これは SDCC です。
  - **DCC2 (D4-D6)** — これは LDCC 1 です。
  - **DCC3 (D7-D9)** — これは LDCC 2 です。
  - **DCC4 (D10-D12)** — これは LDCC 3 です。

DCC オプションは、ONS 15454 (DCC1) またはその他のトンネルでその DCC が使用されていると、表示されません。

**ステップ 8** Finish をクリックします。

**ステップ 9** DCC トンネルを提供するポートを稼働状態にします。手順については、「[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。

**ステップ 10** 元の NTP (手順) に戻ります。



## DLP-A314 ポートへの名前の割り当て

目的	この作業では、ONS 15454 カードのポートに名前を割り当てます。
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) 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** プロビジョニングするポートがある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** 名前を割り当てるポートの番号の Port Name カラムをクリックします。

**ステップ 4** ポート名を入力します。

ポートの名前を 32 文字以下の英数字または特殊文字で指定します。このフィールドは、デフォルトでは空白になっています。

**ステップ 5** 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-A315 ユーザのログアウト : 単一ノード

目的	この作業では、単一ノードからユーザをログアウトします。
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 > Active Logins タブをクリックします。

**ステップ 2** ログアウトするユーザを選択して、Logout をクリックします。

**ステップ 3** ユーザをロックアウトする場合は、Logout User ダイアログボックスで Lockout before Logout をオンにします。これにより、ログアウト後のログインが、Policy タブのユーザ ロックアウト パラメータに基づいて防止されます。スーパーユーザが手動でロックを解除するか、または Lockout Duration フィールドで指定した時間が過ぎるまでユーザはロックアウトされます。詳細については、「DLP-A271 セキュリティ ポリシーの変更 : 単一ノード」(p.19-60) を参照してください。

**ステップ 4** OK をクリックします。

## ■ DLP-A316 ユーザのログアウト：複数ノード

**ステップ 5** Yes をクリックして、ログアウトを確認します。

**ステップ 6** 元の NTP（手順）に戻ります。

## DLP-A316 ユーザのログアウト：複数ノード

目的	この作業では、複数ノードからユーザをログアウトします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** View メニューから **Go to Network View** を選択します。

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

**ステップ 3** ログアウトするユーザを選択します。

**ステップ 4** **Logout** をクリックします。

**ステップ 5** **Logout User** ダイアログボックスで、そのユーザをログアウトさせるノードをオンにします。

**ステップ 6** ログアウトの前にユーザをロックアウトする場合は、**Lockout before Logout** をオンにします。これにより、ログアウト後のログインが、**Policy** タブで設定したユーザ ロックアウト パラメータに基づいて防止されます。スーパーユーザが手動でロックを解除するか、または **Lockout Duration** フィールドで指定した時間が過ぎるまでユーザはロックアウトされます。詳細については、「[DLP-A271 セキュリティ ポリシーの変更：単一ノード](#)」(p.19-60) を参照してください。

**ステップ 7** **Select Applicable Nodes** 領域で、ユーザの設定を変更しないノードをオフにします（デフォルトでは、すべてのネットワーク ノードが選択されています）。

**ステップ 8** **OK** をクリックします。

**ステップ 9** 元の NTP（手順）に戻ります。

## DLP-A320 ML シリーズ PM パラメータの表示 : イーサネット ポート

目的	この作業では、指定したインターバルで ML シリーズ イーサネット 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

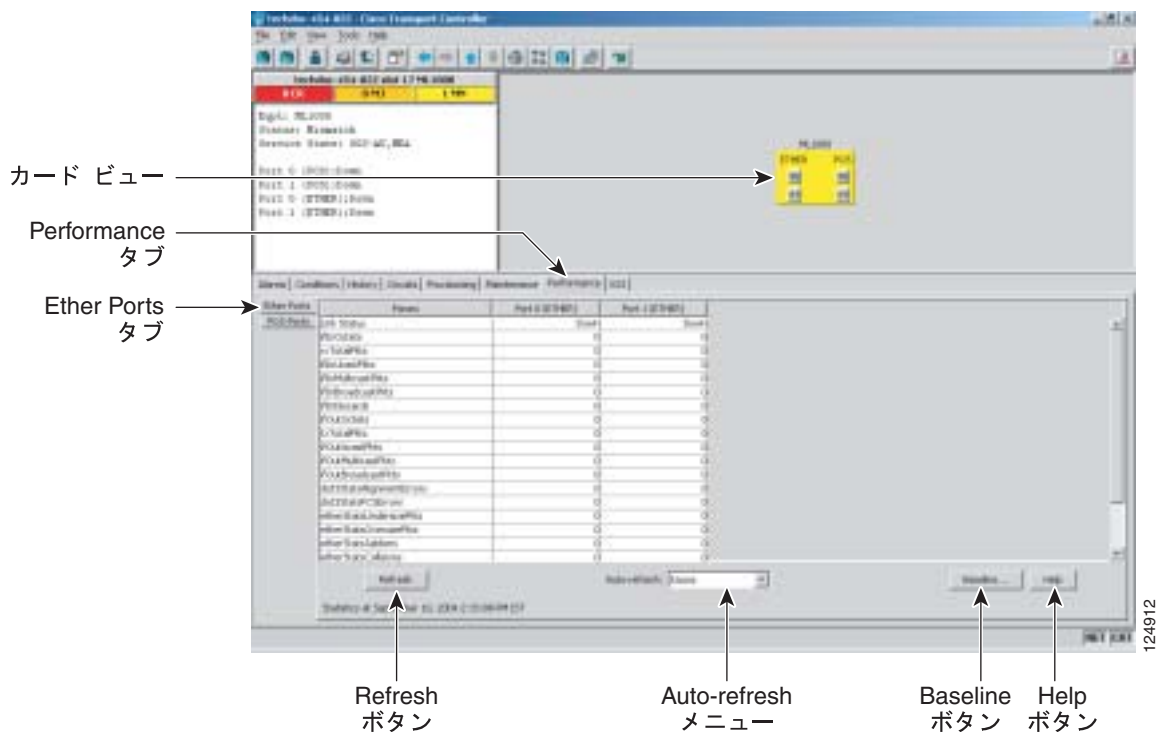


(注) ML シリーズ カードのプロビジョニングについては、『*Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*』を参照してください。

**ステップ 1** ノード ビューで、PM カウントを表示する ML 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 タブをクリックします (図 20-1)。

図 20-1 ML シリーズカード ビューの Performance ウィンドウにある Ether Ports



**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。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 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-A253 PM カウントの表示変更](#)」(p.9-2) 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-A321 ML シリーズ PM パラメータの表示 : POS ポート

目的	この作業では、ML シリーズ イーサネット カードおよびポートについて、指定したインターバルで Packet Over SONET (POS) ポートの PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン</a> (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



(注) ML シリーズ カードのプロビジョニングについては、『*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 1** ノード ビューで、PM カウントを表示する ML 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 > POS Ports タブをクリックします ( [図 20-2](#) )。



## DLP-A322 ノードで使用するタイミング基準の手動または強制切り替え

目的	この作業では、選択したタイミング基準の Synchronization Status Message (SSM; 同期ステータス メッセージ) 品質が現在のタイミング基準以上であれば、ノードを選択した基準に切り替えます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Timing > Source タブをクリックします。
- ステップ 2** 対象となる Clock の Reference ドロップダウン リストから、基準を選択します。
- ステップ 3** 対象となる Clock の Operation ドロップダウン リストから、次のオプションのいずれかを選択します。
- **Manual** — このオプションでは、選択した基準の SSM 品質が現在のタイミング基準以上であれば、そのノードを選択した基準に切り替えます。
  - **Force** — このオプションでは、SSM 品質には関係なく (基準が有効であれば)、そのノードを選択した基準に切り替えます。
- Clear オプションの詳細については、「[DLP-A323 ノードで使用するタイミング基準の手動または強制切り替えのクリア](#)」(p.20-14) を参照してください。
- ステップ 4** タイミングソースの隣にある **Apply** をクリックします。
- ステップ 5** 確認用のダイアログボックスで **Yes** をクリックします。選択したタイミング基準が許容される有効な基準であれば、そのノードは選択したタイミング基準に切り替わります。
- ステップ 6** 選択したタイミング基準が無効な場合、警告ダイアログボックスが表示されます。OK をクリックします。ノードは通常のタイミング基準に戻りません。
- ステップ 7** 元の NTP (手順) に戻ります。
- 

## DLP-A323 ノードで使用するタイミング基準の手動または強制切り替えのクリア

目的	この作業では、手動または強制で切り替えたノードのタイミング基準をクリアして、プロビジョニングされている基準に戻します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Timing > Source タブをクリックします。

- ステップ 2** Operation メニューで、現在 Manual または Force に設定されているクロック基準を見つけます。
- ステップ 3** Operation ドロップダウン リストから Clear を選択します。
- ステップ 4** Apply をクリックします。
- ステップ 5** 確認用のダイアログボックスで Yes をクリックします。通常のタイミング基準が許容される有効な基準であれば、ノードはシステムの設定で定義されている通常のタイミング基準に戻ります。
- ステップ 6** 通常のタイミング基準が無効である場合や、障害がある場合は、警告ダイアログボックスが表示されます。OK をクリックします。タイミング基準は元には戻せません。
- ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A324 VCAT 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、Virtual Concatenated (VCAT; 仮想連結) 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)  Circuit Creation ウィザードの Circuit 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

- ステップ 1** Node ドロップダウン リストから、回線の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、回線の送信元となる CE シリーズ、ML シリーズ、または FC\_MR-4 カードが取り付けられているスロットを選択します (伝送容量を使い切っているカードは、リストに表示されません)。
- ステップ 3** 回線の送信元となるカードに合わせて、Port ドロップダウン リストと STS ドロップダウン リストから、送信元ポートと STS (またはどちらか一方) および該当する場合は VT を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS と VT は、別の回線によってすでに使用されている場合は、表示されません。VT は、STS-V 回線では表示されません。
- ステップ 4** Next をクリックします。
- ステップ 5** Node ドロップダウン リストから宛先ノードを選択します。
- ステップ 6** Slot ドロップダウン リストから、回線の終端となる CE シリーズ、ML シリーズ、または FC\_MR-4 カード (宛先カード) が取り付けられているスロットを選択します (伝送容量を使い切っているカードは、リストに表示されません)。

**ステップ 7** **ステップ 2** で選択されたカードに応じて、Port ドロップダウン リストと STS ドロップダウン リストから、送信元ポートと STS (またはどちらか一方)、および該当する場合は VT を選択します。Port リストは、カードに複数のポートがある場合にだけ使用できます。STS と VT は、別の回線によってすでに使用されている場合は、表示されません。VT は、STS-V 回線では表示されません。

**ステップ 8** Next をクリックします。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A325 VCAT 回線ルートのプロビジョニング

目的	この作業では、手動ルーティング VCAT 回線の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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	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。
オンサイト / リモート	適宜
セキュリティ レベル	オンサイトまたはリモート プロビジョニング以上のレベル

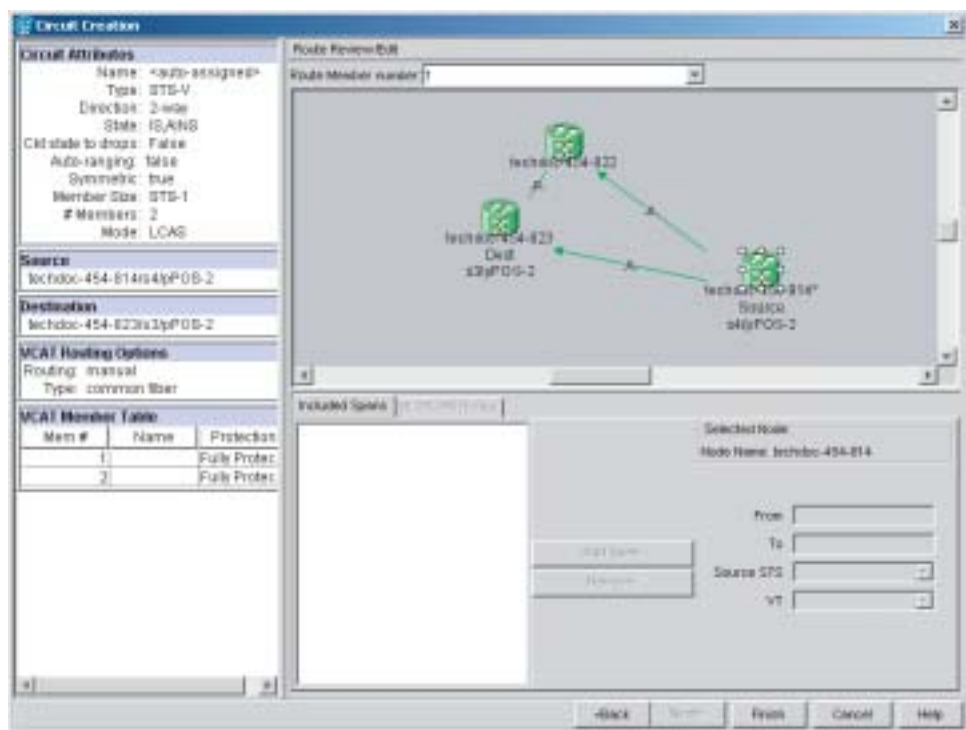
**ステップ 1** Circuit Creation ウィザードの Route Review and Edit 領域で、Route Member Number ドロップダウン リストからメンバー番号を選択します。

**ステップ 2** 送信元 ノード アイコンが選択されていない場合は、このアイコンをクリックします。

**ステップ 3** 送信元 ノードにあるスパンから開始して、回線を通過させるスパンの矢印をクリックしていきま。矢印がイエローになります。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。送信元 STS が表示されます。図 20-3 は、その一例です。



図 20-3 VCAT 回線の手動ルーティング



- ステップ 4** 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 5** すべての中継ノードを通過して回線が送信元ノードから宛先ノードへプロビジョニングされるまで、ステップ 3 と 4 を繰り返します。
- ステップ 6** 各メンバーについてステップ 1 ~ 5 を繰り返します。
- ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A326 BLSR のノード ID の変更

目的	この作業では、BLSR のノード ID を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 メニューで、Go to Network View を選択します。
- ステップ 2** ネットワーク マップ上で、変更するノード ID を持つノードをダブルクリックします。

- ステップ 3** Provisioning > BLSR タブをクリックします。
- ステップ 4** ノード ID 番号を選択します。同じ BLSR の他のノードにすでに割り当てられている番号は選択できません。
- ステップ 5** 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-A327 CTC Alerts ダイアログボックスの自動ポップアップ設定

目的	この作業では、CTC Alerts ダイアログボックスをすべてのアラートに対して開くように設定したり、回線削除エラーに対してだけ開くように設定したり、いかなる場合にも開かないように設定したりします。CTC Alerts ダイアログボックスには、ネットワーク切断、Send-PDIP の不一致、回線削除状態、条件取得エラー、およびソフトウェア ダウンロードの失敗が表示されます。
工具	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** CTC Alerts ツールバー アイコンをクリックします。
- ステップ 2** CTC Alerts ダイアログボックスで、次のいずれかを選択します。
- **All alerts** — すべての通知に対して CTC Alerts ダイアログボックスが自動的に開くように設定します。
  - **Error alerts only** — 回線削除エラーに対してだけ CTC Alerts ダイアログボックスが自動的に開くように設定します。
  - **Never** — いかなる場合にも CTC Alerts ダイアログボックスが自動的に開かないように設定します。
- ステップ 3** Close をクリックします。
- ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A328 BLSR ウィザードによる 2 ファイバ BLSR の作成

目的	この作業では、BLSR 設定の各ノードで CTC BLSR ウィザードを使用して 2 ファイバ BLSR を作成します。BLSR ウィザードで各ノードが BLSR のプロビジョニングを開始できる状態であるかどうかを確認し、すべてのノードを同時にプロビジョニングします。
工具 / 機器	なし
事前準備手順	NTP-A40 BLSR ノードのプロビジョニング (p.5-14) 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** View メニューから **Go to Network View** を選択します。

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

**ステップ 3** **Create BLSR** をクリックします。

**ステップ 4** BLSR Creation ダイアログボックスで、BLSR のプロパティを設定します。

- Ring Type — 2 ファイバを選択します。
- Speed — OC-12、OC-48、OC-192 から BLSR リングの速度を選択します。速度は BLSR トランク (スパン) カードの OC-N 速度と一致する必要があります。



**(注)** OC-12 の BLSR を作成しておいて、最終的に OC-48 または OC-192 にアップグレードする場合は、シングルポートの OC-12 カード (OC12 IR/STM4 SH 1310、OC12 IR/STM4 SH 1310、または OC12 IR/STM4 SH 1310) を使用します。OC-48 カードと OC-192 カードはシングルポートであるため、4 ポートの OC-12 (OC12/STM4-4) で BLSR をアップグレードすることはできません。

- Ring Name — リング名を割り当てます。名前に使用できる文字数は、1 ~ 6 文字です。すべての英数字を大文字と小文字を組み合わせて指定できます。文字列 [All] は、TL1 のキーワードであるため、大文字か小文字かに関係なく使用できません。すでに他の BLSR に割り当てられている名前も指定できません。
- Reversion time — リングを切り替えたあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。リングの復元を、Never に設定することもできます。

**ステップ 5** **Next** をクリックします。ネットワーク図が表示されたら、ステップ 6 へ進みます。

取り付けられている光カードの数が不足している場合や、UPSR セレクタのある回線が検出された場合などは、BLSR を作成できません。CTC でそうした状況が判明すると、[Cannot Create BLSR] というメッセージが表示されます。このメッセージが表示された場合は、次のステップを実行します。

- OK をクリックします。
- Create BLSR ウィンドウで、**Excluded Nodes** をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- 障害の内容に応じて、**Back** をクリックして始めから作業を繰り返すか、または **Cancel** をクリックして作業を取り消します。

- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。

**ステップ6** ネットワーク図で、BLSRのスパンラインを順番にダブルクリックしていきます。ダブルクリックしたスパンラインが他のBLSRカードにDCCで接続されていて完全なリングを形成していれば、それらのラインがブルーになります。ラインをダブルクリックしてもまだ完全なリングを形成できていない場合は、完全なリングが作成されるまで別のスパンラインをダブルクリックしていきます。リングがDCC接続されたら、**ステップ7**へ進みます。

**ステップ7** Finish をクリックします。BLSR ウィンドウが開き、作成したBLSRが表示されたら、**ステップ8**へ進みます。[Cannot Create BLSR] または [Error While Creating BLSR] というメッセージが表示された場合は、次の作業を行います。

- a. OK をクリックします。
- b. Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSRを作成できない理由を確認し、OK をクリックします。
- c. 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。



**(注)** BLSRの設定時には、E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、およびBLSROSYNCの各アラームのうち一部またはすべてが短時間表示されることがあります。

**ステップ8** 次の点を確認します。

- ネットワークビューの図で、すべてのBLSRノード間にグリーンのスパンラインが表示されていること。
- E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、およびBLSROSYNCの各アラームがすべてクリアされていること。アラームのトラブルシューティングについては、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。



**(注)** ノード名の後ろにあるかっこ内の数字は、CTCによって割り当てられたBLSRノードIDです。1つのBLSR内の各ONS 15454には、0～31の一意なノードIDが割り当てられています。ノードIDを変更する場合は、「DLP-A326 BLSRのノードIDの変更」(p.20-17)を行います。

**ステップ9** 元の手順(NTP)に戻ります。

## DLP-A329 2 ファイバ BLSR の手動作成

目的	この作業では、BLSR 設定の各ノードで BLSR ウィザードを使用せずに BLSR を作成します。
工具 / 機器	なし
事前準備手順	NTP-A40 BLSR ノードのプロビジョニング (p.5-14) 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 > BLSR** 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** Suggestion ダイアログボックスで **OK** をクリックします。

**ステップ 4** Create BLSR ダイアログボックスで、BLSR のプロパティを設定します。

- Ring Type — 2 ファイバを選択します。
- Ring Name — リング名を割り当てます。BLSR 内の各ノードには、同じリング名を使用する必要があります。英数字で、大文字と小文字を組み合わせで指定できます。文字列 [All] は、TL1 のキーワードであるため、大文字か小文字かに関係なく使用できません。すでに他の BLSR に割り当てられている名前も指定できません。
- Node ID — ドロップダウン リストがノード ID (0 ~ 31) を選択します。ノード ID は、BLSR でノードを識別するための ID です。同じ BLSR 内のノードの ID は一意でなければなりません。
- Reversion time — トラフィックが元の現用パスに復元するまでの時間を設定します。デフォルトは 5 分です。同じ BLSR 内のすべてのノードに同じ復元時間を設定する必要があります。
- West Line — ドロップダウン リストからノードのウェスト BLSR ポートを割り当てます。  
「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) で設定したファイバ接続と DCC 終端の設定は、イーストポートとウェストポートで一致している必要があります。
- East Line — ドロップダウン リストからノードのイースト BLSR ポートを割り当てます。

**ステップ 5** **OK** をクリックします。



**(注)** すべての BLSR ノードがプロビジョニングされるまで、E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、および BLSROSYNC の各アラームのうち一部またはすべてが表示されます。BLSR のすべてのノードが設定されると、これらのアラームはクリアされます。

**ステップ 6** View メニューから **Go to Other Node** を選択します。

**ステップ 7** Select Node ダイアログボックスで、BLSR に追加する次のノードを選択します。

**ステップ 8** BLSR に追加する各ノードで、ステップ 1 ~ 7 を繰り返します。すべてのノードを追加したら、**ステップ 9** へ進みます。

**ステップ 9** View メニューから、**Go to Network View** を選択します。10 ~ 15 秒経過したら、次の点を確認します。

- すべての BLSR ノード間に、グリーンのスパン ラインが表示されている。
- E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTk、および BLSROSYNC の各アラームがすべてクリアされていること。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A330 カード スロットの事前プロビジョニング

目的	この作業では、ONS 15454 にカードを物理的に取り付ける前に、CTC でカード スロットを事前プロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、これからカードを取り付ける空きスロットを右クリックします。

**ステップ 2** Add Card ショートカット メニューから、取り付けるカードのタイプを選択します。Add Card ショートカット メニューには、そのスロットに取り付けることができるカードだけが表示されます。

スロットを事前にプロビジョニングしておく、カードがスロットに取り付けられたときに、CTC のシェルフ図でカードがホワイトではなくパープルで表示されます。カードの図に NP (not present [存在しない]) が表示されている場合は、当該カードが物理的に取り付けられていないことを示します。

**ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A332 トンネル タイプの変更

目的	この作業は、従来の DCC トンネルを IP カプセル化トンネルに変換するか、または IP カプセル化トンネルを従来の SDCC トンネルに変換します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A313 DCC トンネルの作成 (p.20-7)</a> <a href="#">DLP-A341 IP カプセル化トンネルの作成 (p.20-36)</a>
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 > Overhead Circuits** タブをクリックします。
- ステップ 3** 変換する回線トンネルをクリックします。
- ステップ 4** **Edit** をクリックします。
- ステップ 5** Edit Circuit ウィンドウで、**Tunnel** タブをクリックします。
- ステップ 6** Attributes 領域で、次の手順を実行します。
- 従来の DCC トンネルを IP カプセル化トンネルに変換する場合は、**Change to IP Tunnel** チェックボックスをオンにし、IP トンネルで使用する SDCC 総帯域幅のパーセントを入力します（最小値は 10%）。
  - IP トンネルを従来の DCC トンネルに変換する場合は、**Change to SDCC Tunnel** チェックボックスをオンにします。
- ステップ 7** **Apply** をクリックします。
- ステップ 8** 確認用のダイアログボックスで **Yes** をクリックして、次へ進みます。
- ステップ 9** Circuit Changed ステータス ボックスで **OK** をクリックし、回線の変更が正常に行われたことを確認応答します。
- ステップ 10** 元の NTP（手順）に戻ります。
- 

## DLP-A333 回線の削除

目的	この作業では、回線を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。
- ステップ 2** 回線上でトラフィックが伝送されていないことと、回線の削除が安全に実行できることを確認します。
- ステップ 3** View メニューから **Go to Network View** を選択します。
- ステップ 4** **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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。

- b. 説明のつかないアラーム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。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。必要に応じて、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。

**ステップ 5** Circuits タブをクリックします。

**ステップ 6** 削除する回線を選択し、Delete をクリックします。

**ステップ 7** Delete Circuits 確認用のダイアログボックスで、必要に応じて次のいずれかまたは両方をオンにします。

- Change drop port admin state — ドロップポートの管理状態を選択します。
  - IS — 回線のクロスコネクタのサービス状態を In-Service and Normal (IS-NR) にします。
  - OOS,DSBLD — 回線のクロスコネクタのサービス状態を Out-of-Service and Management, Disabled (OOS-MA,DSBLD) にします。トラフィックは回線を通できません。この回線がポートと同じサイズではないか、ポートを使用している唯一の回線の場合、CTC ではポートのサービス状態を変更しません。
  - IS,AINS — 回線のクロスコネクタのサービス状態を Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) にします。接続で有効な信号を受信すると、クロスコネクタのサービス状態は自動的に IS-NR になります。
  - OOS,MT — 回線のクロスコネクタのサービス状態を Out-of-Service and Management, Maintenance (OOS-MA,MT) にします。このサービス状態になっても、トラフィックの流れが中断されることはなく、その回線に対してループバックを実行することができますが、アラームおよび状態は抑制されます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合は、この OOS,MT 管理状態を使用します。テストが完了したら、管理状態を IS、OOS、または IS,AINS に変更します。
- Notify when completed — オンにすると、すべての回線の送信元ポートまたは宛先ポートが停止状態 (OOS) になり回線が削除された時点で、CTC Alerts 確認用ダイアログボックスにそれが表示されます。この間、他の CTC 機能を実行することはできません。多くの回線を削除しようとする、確認の表示まで数分かかる場合があります。このチェックボックスのオン / オフに関係なく、回線は削除されます。



**(注)** CTC Alerts ダイアログボックスは、CTC Alerts チェックボックスで All alerts または Error alerts only をオンにした場合を除いて、自動的に開いて削除エラーを表示することはありません。詳細については、「[DLP-A327 CTC Alerts ダイアログボックスの自動ポップアップ設定](#)」(p.20-18) を参照してください。CTC Alerts ダイアログボックスが自動的に開いて通知が表示されるように設定されていない場合、CTC Alerts ツールバー アイコンの中の赤い三角表示により通知が存在することがわかります。

**ステップ 8** 次のいずれかを行います。

- Notify when completed をオンにした場合、CTC Alerts ダイアログボックスが表示されます。この情報を保存する場合は、[ステップ 9](#) へ進みます。この情報を保存しない場合は、[ステップ 10](#) へ進みます。
- Notify when completed をオフにした場合、Circuits ウィンドウが表示されます。[ステップ 11](#) へ進んでください。

**ステップ 9** CTC Alerts ダイアログボックスの情報を保存する場合は、次の手順を実行します。この情報を保存しない場合は、[ステップ 10](#) へ進みます。

- a. Save をクリックします。



- b. Browse をクリックして、ファイルの保存先となるディレクトリに移動します。
- c. ファイルの拡張子として .txt を付けたファイル名を入力し、OK をクリックします。

**ステップ 10** Close をクリックし、CTC Alerts ダイアログボックスを閉じます。

**ステップ 11** 「[NTP-A108 データベースのバックアップ](#)」(p.15-6) を実行します。

**ステップ 12** 元の NTP (手順) に戻ります。

## DLP-A334 オーバーヘッド回線の削除

目的	この作業では、オーバーヘッド回線を削除します。オーバーヘッド回線には、DCC トンネル、IP カプセル化トンネル、AIC-I カード オーダーワイヤ、および AIC-I カード User Data Channel (UDC) が含まれます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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

回線が稼働中 (IS) の場合にオーバーヘッド回線を削除すると、サービスに影響します。回線を停止 (OOS) する場合は、「[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。

**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 > Overhead Circuits** タブをクリックします。

**ステップ 3** ローカルまたはエクスプレス オーダーワイヤ、ユーザ データ、IP カプセル化トンネル、または DCC トンネルの中から、削除するオーバーヘッド回線をクリックします。

**ステップ 4** **Delete** をクリックします。

**ステップ 5** 確認用のダイアログボックスで **Yes** をクリックして、次へ進みます。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A335 VLAN の削除

目的	この作業では、ドメインから VLAN (仮想 LAN) を削除します。
工具 / 機器	なし
事前準備手順	回線の作成手順については、第 6 章「回線と VT トンネルの作成」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	プロビジョニング以上のレベル



(注) 使用中の VLAN は削除されません。

- 
- 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** Tools メニューから、**Manage VLANS** を選択します。
  - ステップ 3** All VLANs ダイアログボックスで、削除する VLAN をクリックします。
  - ステップ 4** **Delete** をクリックします。
  - ステップ 5** 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** 元の NTP (手順) に戻ります。
- 

## DLP-A336 IP トンネルの修復

目的	この作業では、ノード IP アドレスを変更した結果 OOS-PARTIAL ステータスにある回線を修復します。
工具 / 機器	なし
事前準備手順	回線の作成手順については、第 6 章「回線と VT トンネルの作成」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	プロビジョニング以上のレベル

- 
- ステップ 1** 該当するノードの元の IP アドレスを取得します。
  - ステップ 2** View メニューから **Go to Network View** を選択します。
  - ステップ 3** Tools メニューから、**Overhead Circuits > Repair IP Circuits** を選択します。
  - ステップ 4** IP Repair ウィザードのテキストを確認し、**Next** をクリックします。

**ステップ 5** Node IP address 領域で、次の手順を実行します。

- Node — OOS-PARTIAL 回線を保有するノードを選択します。
- Current IP Address — 現在の IP アドレスを入力します。
- Old IP Address — ノードの元の IP アドレスを入力します。

**ステップ 6** Next をクリックします。

**ステップ 7** Finish をクリックします。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A337 Windows での CTC インストール ウィザードの実行

目的	この作業では、Windows コンピュータに CTC のオンライン ユーザ マニュアル、Acrobat Reader 6.0.1、JRE 1.4.2、および CTC JAR ファイルをインストールします。Release 7.2 の実行には、JRE 1.4.2 または 1.5 が必要です。CTC JAR ファイルを事前にインストールしておく、初めてログインしたときに時間を節約できます。JAR ファイルがインストールされていない場合は、初めてログインしたときに TCC2/TCC2P カードからダウンロードされます。
工具 / 機器	Cisco ONS 15454 Release 7.2 のソフトウェアまたは Documentation CD
事前準備手順	なし
必須 / 適宜	この作業は、次のいずれかに該当する場合に必要となります。 <ul style="list-style-type: none"> <li>• JRE 1.4.2 または JRE 5.0 がインストールされていない場合</li> <li>• 必要な CTC オンライン ユーザ マニュアルがインストールされていない場合</li> <li>• 必要な CTC JAR ファイルがインストールされていない場合</li> </ul>
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)

Release 4.6 より前の CTC ソフトウェアを実行中のノードにログインする場合は、JRE 1.4.2 または 5.0 をアンインストールして、JRE1.3.1\_2 を再インストールしてください。ソフトウェア R7.2 を実行する場合は、JRE 1.3.1\_2 をアンインストールして、JRE 1.4.2 または 5.0 を再インストールしてください。ソフトウェア R7.2 は JRE 1.4.2 または JRE 5.0 をサポートします。JRE 1.4.2 は、ソフトウェア CD に収録されています。



(注)

JRE 1.4.2 の実行には、Netscape 7.x または Internet Explorer 6.x が必要です。

**ステップ 1** コンピュータが次の条件を満たしていることを確認します。

- プロセッサ — Pentium III、700 MHz 以上の速度

- RAM — 384 MB (推奨)、512 MB (最適)
- ハードドライブ — 20 GB のハードドライブ (推奨)、50 MB 以上の空き容量が必要
- OS (オペレーティングシステム) — Windows 98 (First Edition と Second Edition)、Windows NT 4.0 (Service Pack 6a)、Windows 2000 (Service Pack 3)、または Windows XP Home Edition

OS が Windows NT 4.0 の場合は、Service Pack 6a 以降がインストールされていることを確認します。[スタート]メニューから [プログラム] > [管理ツール] > [Windows NT 診断プログラム] の順に選択し、[Windows NT 診断プログラム] ダイアログボックスの [バージョン] タブでサービスパックを確認します。Service Pack 6a 以降がインストールされていない場合は、先へ進まないでください。現地のコンピュータ アップグレード手順に従って Service Pack 6a をインストールします。



**(注)** プロセッサ要件と RAM 要件が基準になります。より高速なプロセッサとより大容量の RAM をコンピュータに搭載すると、CTC のパフォーマンスが上がります。

**ステップ 2** コンピュータの CD ドライブに Cisco ONS 15454 Release 7.2 のソフトウェア CD または Documentation CD を挿入します。インストール プログラムが自動的に起動します。起動しない場合は、CD ディレクトリに移動し、**setup.exe** をダブルクリックします。

CTC のインストール ウィザードに、コンピュータへインストールするコンポーネントが表示されます。

- Java ランタイム環境 1.4.2
- Acrobat Reader 6.0.1
- オンライン ユーザ マニュアル
- CTC JAR ファイル

**ステップ 3** **Next** をクリックします。

**ステップ 4** 次のいずれかを実行します。

- 3 つすべてのコンポーネントをインストールする場合は、**Typical** をクリックします。コンピュータにすでに JRE 1.4.2 または 5.0 がインストールされている場合は、**Custom** を選択します。
- JRE またはオンライン ユーザ マニュアルのいずれか一方をインストールする場合は、**Custom** をクリックします。デフォルトでは、JRE と Acrobat Reader が選択されています。

**ステップ 5** **Next** をクリックします。

**ステップ 6** 状況に応じて、次の項目を実行してください。

- **ステップ 4** で **Typical** を選択した場合は、このステップを省略して **ステップ 7** へ進みます。
- **Custom** を選択した場合は、インストールする CTC コンポーネントをオンにし、**Next** をクリックします。
  - オンライン ユーザ マニュアルを選択した場合は、**ステップ 7** へ進みます。
  - オンライン ユーザ マニュアルを選択しなかった場合は、**ステップ 9** へ進みます。

**ステップ 7** インストールウィザードで CTC オンライン ユーザ マニュアルをインストールするディレクトリが表示されます。デフォルト ディレクトリは C:\Program Files\Cisco\CTC\Documentation です。

- CTC オンライン ユーザ マニュアルのディレクトリを変更する場合は、Directory Name フィールドに新しいディレクトリのパスを入力するか、または **Browse** をクリックして該当するディレクトリに移動します。
- デフォルトのディレクトリを変更しない場合は、このステップを省略します。

**ステップ 8** **Next** をクリックします。

**ステップ 9** インストールするコンポーネントを確認します。これらのコンポーネントを変更する場合は、次のいずれかを実行してください。

- **ステップ 4** で Typical を選択した場合は、**Back** を 2 回クリックして、インストールのタイプを設定するページに戻ります。Custom を選択し、ステップ 5 ~ 8 を繰り返します。
- **ステップ 4** で Custom を選択した場合は、コンポーネントの選択ページが表示されるまで **Back** を 1 回または 2 回 (選択したコンポーネントによって異なる) クリックします。ステップ 6 ~ 8 を繰り返します。

**ステップ 10** **Next** をクリックします。JRE のインストール ウィザードが表示されるまでに数分かかることがあります。**ステップ 4** で Custom を選択し、JRE をインストールする必要がある場合は、**ステップ 12** へ進みます。

**ステップ 11** JRE をインストールする場合は、次の手順を実行します。

- a. Java 2 Runtime Environment License Agreement ダイアログボックスで、使用許諾契約を確認し、次のいずれかを選択します。
  - I accept the terms of the license agreement — 使用許諾契約に同意します。ステップ b へ進んでください。
  - I do not accept the terms of the license agreement — Java 2 Runtime Environment License Agreement ダイアログボックスにある **Next** ボタンがディセーブルになります。**Cancel** をクリックして、CTC のインストール ウィザードに戻ります。CTC による JRE のインストールは実行されません。**ステップ 12** へ進んでください。



**(注)** コンピュータに JRE 1.4.2 がすでにインストールされている場合、License Agreement ページは表示されません。Next をクリックしてから、Modify を選択して JRE のインストールを変更するか、または Remove を選択して JRE をアンインストールする必要があります。Modify を選択して Next をクリックした場合は、ステップ e へ進みます。Remove を選択して Next をクリックした場合は、ステップ i へ進みます。

b. **Next** をクリックします。

c. 次のいずれかを選択します。

- JRE の機能をすべてインストールする場合は、**Typical** をクリックします。Typical を選択すると、インストールした JRE バージョンが自動的にブラウザのデフォルト JRE バージョンになります。
- インストールするコンポーネントを選択してその JRE バージョンを使用するブラウザを選択する場合は、**Custom** をクリックします。

d. **Next** をクリックします。

- e. Typical を選択した場合は、ステップ i へ進みます。Custom を選択した場合は、インストールするプログラム機能ごとにドロップダウン リストをクリックして設定を選択します。プログラム機能には、次のような機能があります。

- Java 2 Runtime Environment — (デフォルト) 欧州言語がサポートされている JRE 1.4.2 をインストールします。
- Support for Additional Languages — 欧州以外の言語のサポートを追加します。
- Additional Font and Media Support — Lucida フォント、Java サウンド、および色管理機能を追加します。

各プログラム機能のドロップダウン リスト オプションは、次のとおりです。

- This feature will be installed on the local hard drive — 選択した機能をインストールします。
- This feature and all subfeatures will be installed on the local hard drive — 選択した機能とすべての従属機能をインストールします。
- Don't install this feature now — この機能をインストールしません (Java 2 ランタイム環境では選択できません)。

JRE バージョンのインストール先のディレクトリを変更する場合は、Change をクリックし、目的のディレクトリに移動してから OK をクリックします。

- f. Next をクリックします。
- g. Browser Registration ダイアログボックスで、Java Plug-In に登録するブラウザをオンにします。この JRE バージョンが、選択したブラウザのデフォルトになります。両方のブラウザチェックボックスをオフのままにすることもできます。



(注) この JRE をこれらのブラウザのデフォルトとして設定すると、これらのブラウザで問題が発生する可能性があります。

- h. Next をクリックします。
- i. Finish をクリックします。JRE をアンインストールする場合は、Remove をクリックします。

**ステップ 12** CTC のインストール ウィザードで、Next をクリックします。オンライン ユーザ マニュアルがインストールされます。

**ステップ 13** Finish をクリックします。

**ステップ 14** 元の NTP (手順) に戻ります。

## DLP-A338 UNIX での CTC インストール ウィザードの実行

目的	この作業では、Solaris ワークステーションに CTC のオンライン ユーザ マニュアル、Acrobat Reader 6.0.1、JRE 1.4.2、および CTC JAR ファイルをインストールします。Release 7.2 の実行には、JRE 1.4.2 または JRE 1.5 が必要です。CTC JAR ファイルを事前にインストールしておく、初めてログインしたときに時間を節約できます。JAR ファイルがインストールされていない場合は、初めてログインしたときに TCC2/TCC2P カードからダウンロードされます。
工具 / 機器	Cisco ONS 15454 Release 7.2 のソフトウェアまたは Documentation CD
事前準備手順	なし
必須 / 適宜	次のいずれかに該当する場合に必要となります。 <ul style="list-style-type: none"> <li>• JRE 1.4.2 または 5.0 がインストールされていない場合</li> <li>• 必要な CTC オンライン ユーザ マニュアルがインストールされていない場合</li> <li>• 必要な CTC JAR ファイルがインストールされていない場合</li> </ul>
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)

Release 4.6 より前の CTC ソフトウェアを実行中のノードにログインする場合は、JRE 1.4.2 または 5.0 をアンインストールして、JRE1.3.1\_2 を再インストールしてください。ソフトウェア R7.2 を実行する場合は、JRE 1.3.1\_2 をアンインストールして、JRE 1.4.2 または 5.0 を再インストールしてください。ソフトウェア R7.2 は JRE 1.4.2 または JRE 5.0 をサポートします。JRE 1.4.2 は、ソフトウェア CD に収録されています。



(注)

JRE 1.4.2 の実行には、Netscape 7.x または Internet Explorer 6.x が必要です。

**ステップ 1** コンピュータが次の条件を満たしていることを確認します。

- RAM — 384 MB (推奨)、512 MB (最適)
- ハードドライブ — 20 GB のハードドライブ (推奨)、50 MB 以上の空き容量が必要
- OS — Solaris 8 または 9



(注)

これらの要件が基準になります。より高速なプロセッサとより大容量の RAM をコンピュータに搭載すると、CTC のパフォーマンスが上がります。

**ステップ 2** 次のように入力して、ディレクトリを変更します。

```
cd/cdrom/cdrom0/
```

**ステップ 3** CD の techdoc454 ディレクトリに移動して、次のように入力します。

```
./setup.bat
```

CTC のインストール ウィザードに、コンピュータへインストールするコンポーネントが表示されます。

- Java ランタイム環境 1.4.2
- Acrobat Reader 6.0.1
- オンライン ユーザ マニュアル
- CTC JAR ファイル

**ステップ 4** Next をクリックします。

**ステップ 5** 次のいずれかを実行します。

- Java ランタイム環境とオンライン ユーザ マニュアルの両方をインストールする場合は、**Typical** をクリックします。コンピュータにすでに JRE 1.4.2 または 5.0 がインストールされている場合は、**Custom** を選択します。
- JRE またはオンライン ユーザ マニュアルのいずれか一方をインストールする場合は、**Custom** をクリックします。

**ステップ 6** Next をクリックします。

**ステップ 7** 状況に応じて、次の項目を実行してください。

- **ステップ 5** で Typical を選択した場合は、**ステップ 8** へ進みます。
- Custom を選択した場合は、インストールする CTC コンポーネントをオンにし、Next をクリックします。
  - オンライン ユーザ マニュアルを選択した場合は、**ステップ 8** へ進みます。
  - オンライン ユーザ マニュアルを選択しなかった場合は、**ステップ 10** へ進みます。

**ステップ 8** インストールウィザードで CTC オンライン ユーザ マニュアルをインストールするディレクトリが表示されます。デフォルトのディレクトリは /usr/doc/ctc です。

- CTC オンライン ユーザ マニュアルのディレクトリを変更する場合は、Directory Name フィールドに新しいディレクトリのパスを入力するか、または **Browse** をクリックして該当するディレクトリに移動します。
- CTC オンライン ユーザ マニュアルのディレクトリを変更しない場合は、このステップを省略します。

**ステップ 9** Next をクリックします。

**ステップ 10** インストールするコンポーネントを確認します。

- **ステップ 5** で Typical を選択した場合は、**Back** を 2 回クリックして、インストールのタイプを設定するページに戻ります。Custom を選択し、**ステップ 6 ~ 9** を繰り返します。
- **ステップ 5** で Custom を選択した場合は、コンポーネントを選択するページが表示されるまで **Back** を 1 回または 2 回 (選択したコンポーネントによって異なる) クリックし、適切なコンポーネントをオンにします。**ステップ 7 ~ 9** を繰り返します。



**ステップ 11** Next をクリックします。JRE のインストール ウィザードが表示されるまでに数分かかることがあります。ステップ 4 で Custom を選択し、JRE をインストールする必要がある場合は、ステップ 13 へ進みます。

**ステップ 12** JRE をインストールする場合は、次の手順を実行します。

- a. Java 2 Runtime Environment License Agreement ダイアログボックスで、使用許諾契約を表示し、次のいずれかを選択します。
  - I accept the terms of the license agreement — 使用許諾契約に同意します。ステップ b へ進んでください。
  - I do not accept the terms of the license agreement — Java 2 Runtime Environment License Agreement ダイアログボックスにある Next ボタンがディセーブルになります。Cancel をクリックして、CTC のインストール ウィザードに戻ります。CTC による JRE のインストールは実行されません。ステップ 13 へ進んでください。



**(注)** コンピュータに JRE 1.4.2 がすでにインストールされている場合、License Agreement ページは表示されません。Next をクリックしてから、Modify を選択して JRE のインストールを変更するか、または Remove を選択して JRE をアンインストールする必要があります。Modify を選択して Next をクリックした場合は、ステップ e へ進みます。Remove を選択して Next をクリックした場合は、ステップ i へ進みます。

- b. Next をクリックします。
- c. 次のいずれかを選択します。
  - JRE の機能をすべてインストールする場合は、Typical をクリックします。Typical を選択すると、インストールした JRE バージョンが自動的にブラウザのデフォルト JRE バージョンになります。
  - インストールするコンポーネントを選択してその JRE バージョンを使用するブラウザを選択する場合は、Custom をクリックします。
- d. Next をクリックします。
- e. Typical を選択した場合は、ステップ i へ進みます。Custom を選択した場合は、インストールするプログラム機能ごとにドロップダウン リストをクリックして設定を選択します。プログラム機能には、次のような機能があります。
  - Java 2 Runtime Environment — (デフォルト) 欧州言語がサポートされている JRE 1.4.2 をインストールします。
  - Support for Additional Languages — 欧州以外の言語のサポートを追加します。
  - Additional Font and Media Support — Lucida フォント、Java サウンド、および色管理機能を追加します。

各プログラム機能のドロップダウン リスト オプションは、次のとおりです。

- This feature will be installed on the local hard drive — 選択した機能をインストールします。
- This feature and all subfeatures will be installed on the local hard drive — 選択した機能とすべての従属機能をインストールします。
- Don't install this feature now — この機能をインストールしません (Java 2 ランタイム環境では選択できません)。

JRE バージョンのインストール先のディレクトリを変更する場合は、Change をクリックし、目的のディレクトリに移動してから OK をクリックします。

- f. Next をクリックします。

- g. Browser Registration ダイアログボックスで、Java Plug-In に登録するブラウザをオンにします。この JRE バージョンが、選択したブラウザのデフォルトになります。両方のブラウザチェックボックスをオフのままにすることもできます。



(注) この JRE バージョンをこれらのブラウザのデフォルトとして設定すると、これらのブラウザで問題が発生する可能性があります。

- h. Next をクリックします。  
i. Finish をクリックします。JRE をアンインストールする場合は、Remove をクリックします。

**ステップ 13** CTC のインストール ウィザードで、Next をクリックします。オンライン ユーザ マニュアルがインストールされます。

**ステップ 14** Finish をクリックします。



(注) JRE とオンライン ユーザ マニュアルをインストールしたディレクトリの名前は、必ず記録しておいてください。

**ステップ 15** 元の NTP (手順) に戻ります。

## DLP-A339 現在のセッションまたはログイン グループからのノードの削除

目的	この作業では、現在の CTC セッションまたはログイン ノード グループからノードを削除します。現在のログイン ノード グループではないグループからノードを削除する方法については、「 <a href="#">DLP-A372 指定したログイン ノード グループからのノードの削除</a> 」(p.20-62) を参照してください。
工具	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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** View メニューから Go to Network View を選択します。

**ステップ 2** 削除するノードをクリックします。

**ステップ 3** CTC File メニューから Delete Selected Node をクリックします。

数秒が経過すると、このノードはネットワーク ビュー マップに表示されなくなります。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A340 LCD でのポートステータスの表示

目的	この作業では、CTC を使用しないで OC-N ポートステータスを表示します。LCD には、1+1 構成のポートと BLSR 構成のポートに対する、現用 / 保護プロビジョニングステータスとアクティブ / スタンバイ回線ステータスが表示されます。保護されていないポートと UPSR ポートに対しては、LCD に常に [Working/Active] が表示されます。
工具 / 機器	なし
事前準備手順	NTP-A16 光カードおよびコネクタの取り付け (p.2-8)
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

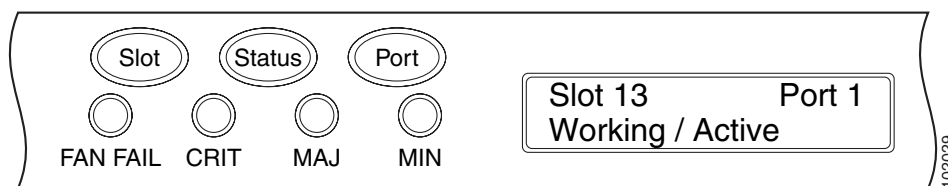
**ステップ 1** 対象となるスロットが LCD に表示されるまで、LCD パネルの Slot ボタンを押します。

**ステップ 2** 対象となるポートが LCD に表示されるまで、Port ボタンを押します(シングルポートカードの Port 1 だけが実際のポートステータスに表示されます)。

**ステップ 3** Status ボタンを押します。LCD が約 10 秒間、アラーム情報を表示し、ポートが現用または保護モードにあるか、アクティブまたはスタンバイにあるかを示します。

図 20-4 に、LCD パネルに表示されたポートステータスの図を示します。

図 20-4 LCD パネルに表示されたポートステータス



**(注)** AIP のヒューズが飛ぶと、LCD はブランクになります。この場合は、Cisco Technical Assistance (TAC) に連絡してください。詳細については、「[テクニカルサポート](#)」(p.xxix) を参照してください。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A341 IP カプセル化トンネルの作成

目的	この作業では、サードパーティ製の SONET 機器から ONS 15454 ネットワークを経由してトラフィックを転送するための、IP カプセル化トンネルを作成します。IP カプセル化トンネルは、終端の DCC として ONS 15454 が使用しなければ、SDCC チャネル (D1-D3) 上に作成されます。
工具 / 機器	OC-N カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A35 ノードの起動の確認 (p.5-3)</a>
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)** IP カプセル化トンネル接続は、各 ONS 15454 ごとに 10 個まで作成できます。ONS 15454 が使用している終端 SDCC は、トンネル エンドポイントには使用できません。また、トンネル エンドポイントとして使用している SDCC は終端できません。トンネル接続はすべて双方向です。

- ステップ 1** 作成するトンネルの送信元ノードと宛先ノードの両方で IP アドレスがプロビジョニングされていることを確認します。詳細については、「[DLP-A249 IP 設定のプロビジョニング](#)」(p.19-35) を参照してください。
- ステップ 2** ネットワーク ビューで、**Provisioning > Overhead Circuits** タブをクリックします。
- ステップ 3** **Create** をクリックします。
- ステップ 4** Overhead Circuit Creation ダイアログボックスの Circuit Attributes 領域で次の項目を指定します。
- Name — トンネル名を入力します。
  - Type — **IP Tunnel-D1-D3** を選択します。
  - Maximum Bandwidth — IP トンネルで使用する総 SDCC 帯域幅の比率 (最小比率は 10%) を指定します。
- ステップ 5** **Next** をクリックします。
- ステップ 6** Circuit Source 領域で次の項目を指定します。
- Node — 送信元ノードを選択します。
  - Slot — 送信元スロットを選択します。
  - Port — 表示された場合は、送信元ポートを選択します。
  - Channel — IPT (D1-D3) が表示されます。
- ステップ 7** **Next** をクリックします。
- ステップ 8** Circuit Destination 領域で、次の項目を指定します。
- Node — 宛先ノードを選択します。
  - Slot — 宛先スロットを選択します。

- Port — 表示された場合は、宛先ポートを選択します。
- Channel — IPT ( D1-D3 ) が表示されます。

**ステップ 9** Finish をクリックします。

**ステップ 10** IP カプセル化トンネルをホストしているポートを稼働状態にします。手順については、「[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。

**ステップ 11** 元の NTP (手順) に戻ります。

## DLP-A347 E シリーズおよび G シリーズ イーサネット カードの 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、E シリーズおよび G シリーズ イーサネット カードの PM パラメータが指定のインターバルで表示されるようにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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 > History タブをクリックします。

**ステップ 3** Interval ドロップダウン リストから、次のいずれかをクリックします。

- 1 min
- 15 min
- 1 hour
- 1 day

**ステップ 4** Refresh をクリックします。PM が、時刻と同期して、選択したインターバルで表示されます。

**ステップ 5** Prev カラムを表示して、最新のインターバル (選択したインターバル) で PM カウントが表示されていることを確認します。

モニタ対象の各パフォーマンスパラメータには、それぞれ最新のインターバルに対するスレッシュホールドがあります。カウンタの値が個々のインターバル (選択したインターバル) のスレッシュホールドを超えると、スレッシュホールド超過アラート (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* カラムを表示して、今までのインターバルで PM カウントが表示されていることを確認します。

選択したインターバルのカウントが不完全な場合は、値の背景色がイエローになります。たとえば、インターバルとして 1 日を選択した場合、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の設定が変更された、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、ポートのサービス状態が変更された、などが考えられます。問題を解決すると、次のインターバル (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-A348 選択した信号の PM カウントのモニタ

目的	この作業では、選択したカードの特定の信号 (STS $n$ )、パス (VT $n$ )、およびポート (DS $n$ ) の近端または遠端の PM カウントを表示できます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

ポートと信号タイプを選択するためのメニューは、カードと回線のタイプによって異なります。カードに基づいて、対応したタイプ (DS1、DS3、VT パス、STS パス) が表示されます。たとえば、DS3XM カードは信号タイプとして DS3、DS1、VT パス、および STS パスの PM パラメータを表示します。このため、指定された DS-3 内の DS-3 ポートと DS-1 の両方を選択できます。

**ステップ 3** 信号タイプを選択するドロップダウン リストで、対応する次のいずれかのオプションをクリックします。

- DS:  $n$  または Port:  $n$  (カードのポート番号)
- VT:  $n$  (VT パスの番号)
- STS:  $n$  (VT パス内の STS 番号)

[図 20-5](#) に、DS3XM-6 カードの Performance ウィンドウに表示されるポートと信号タイプのドロップダウン リストを示します。



## DLP-A349 選択した PM カウントのクリア

目的	この作業では、Clear ボタンを使用して特定の PM カウントをクリアします。クリアされる PM カウントは、選択したオプションによって決まります。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



### 注意

Clear ボタンは、使い方を誤ると、問題を隠してしまうことにもなります。一般にこのボタンはテスト目的で使用します。このボタンを押すと、現在のピンに無効のマークが付けられます。また UAS をカウントしている場合、このボタンをクリックしても UAS の状態はクリアされないので注意してください。したがって、UAS がカウントされなくなった場合、そのカウントは信頼性が低くなります。

- 
- 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** Clear をクリックします。
- ステップ 4** Clear Statistics ドロップダウン リストから、3 つのオプションのうち 1 つを選択します。
- **Displayed statistics** : 選択したポートの現在の統計情報の組み合わせに関連する、すべての PM カウントがカードとウィンドウから消去されます。つまり、選択したインターバル、方向、および信号タイプのカウントがカードとウィンドウから消去されます。
  - **All statistics for port  $x$**  : ポート  $x$  のすべての統計情報をクリアすると、選択したポートのすべての統計情報の組み合わせに関連する、すべての PM カウントがカードとウィンドウから消去されます。つまり、すべてのインターバル、方向、および信号タイプのカウントがカードとウィンドウから消去されます。
  - **All statistics for card** : すべてのポートのすべての PM カウントがカードとウィンドウから消去されます。
- ステップ 5** Clear Statistics ドロップダウン リストで OK を選択して、選択した統計情報をクリアします。
- ステップ 6** 選択した PM カウントがクリアされたことを確認します。
- ステップ 7** 元の NTP (手順) に戻ります。
-



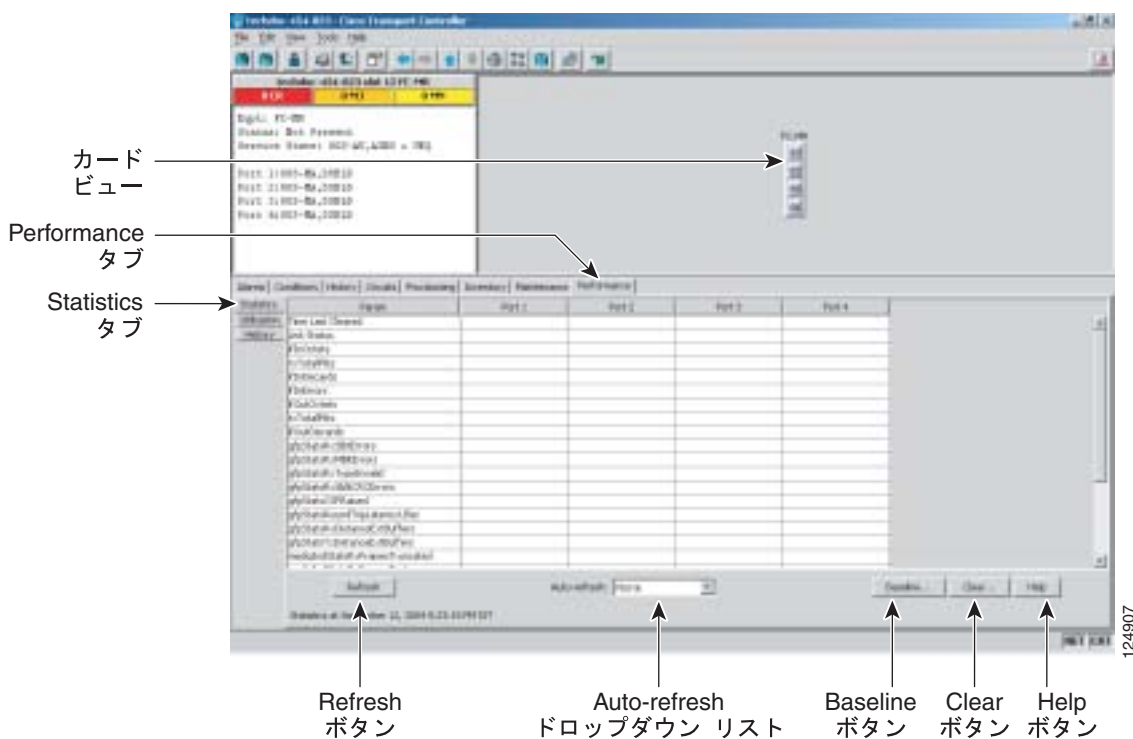
## DLP-A350 FC\_MR-4 PM パラメータの表示：統計情報

目的	この作業では、FC_MR-4 カードおよびポートについて現在の統計の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 FC\_MR-4 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 > Statistics タブをクリックします (図 20-6)。

図 20-6 カード ビューの Performance ウィンドウに表示される FC\_MR-4 統計情報



**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 カラムに PM パラメータの名前が表示されるのを確認します。Port # カラムには PM パラメータの現在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 Reference Manual』の「Performance Monitoring」の章を参照してください。

**ステップ 5** 元の NTP (手順) に戻ります。

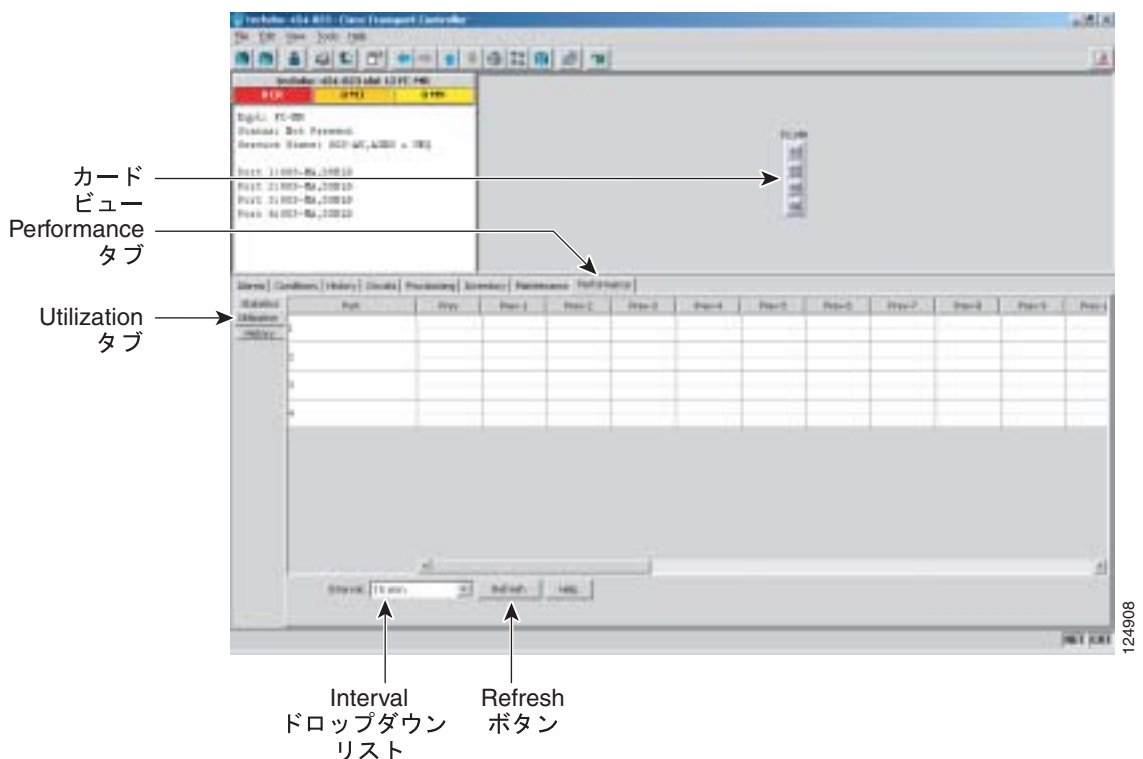
## DLP-A351 FC\_MR-4 PM パラメータの表示：使用率

目的	この作業では、FC_MR-4 カードおよびポートについて回線使用率の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 FC\_MR-4 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 > Utilization タブをクリックします ( [図 20-7](#) )。

図 20-7 カード ビューの Performance ウィンドウに表示される FC\_MR-4 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使用率の値が表示されます。

**ステップ 4** モニタするポートを見つける場合は、Port # カラムを表示します。

**ステップ 5** これまでのインターバルでの送信 (Tx) および受信 (Rx) の帯域使用率の値が Prev-n 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** 元の NTP（手順）に戻ります。

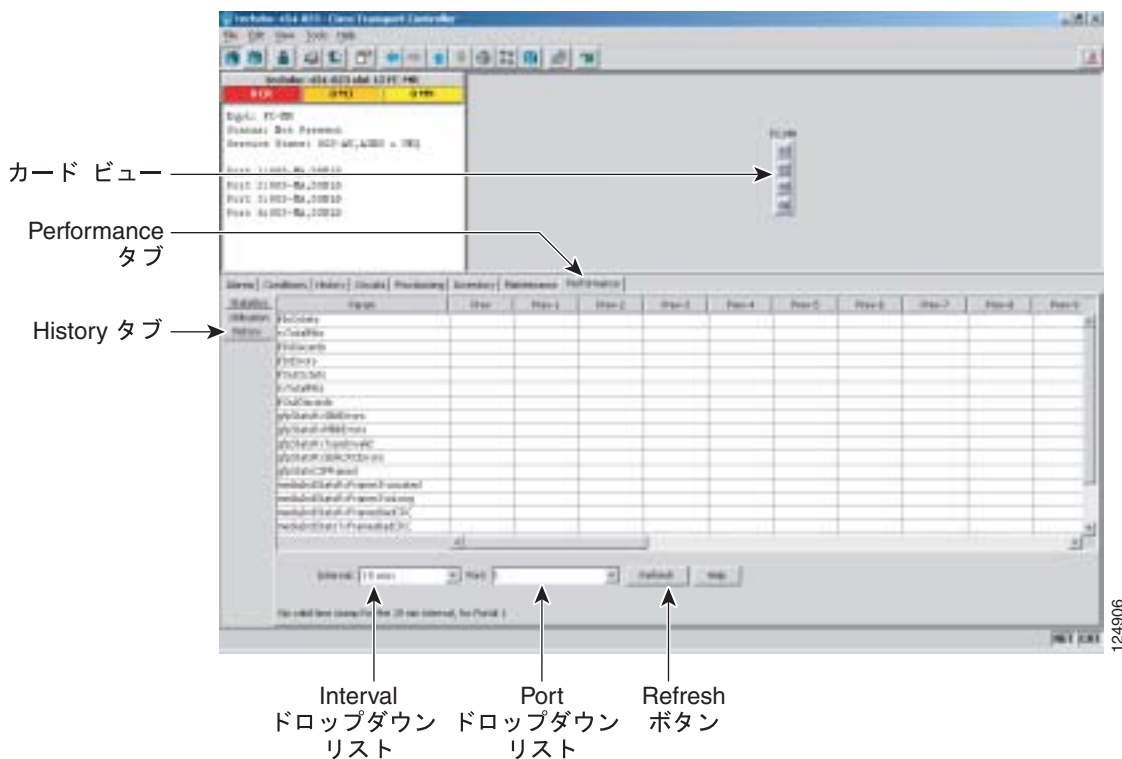
## DLP-A352 FC\_MR-4 PM パラメータの表示：履歴

目的	この作業では、FC_MR-4 カードおよびポートについて選択したインターバルでの PM カウントの履歴を表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 FC\_MR-4 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 > History タブをクリックします ( [図 20-8](#) )。

**図 20-8** カード ビューの Performance ウィンドウに表示される FC\_MR-4 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。Prev-*n* 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 Reference Manual』の「Performance Monitoring」の章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-A353 FC\_MR-4 PM カウントのリフレッシュ間隔の変更

目的	この作業では、指定した PM カウントが、選択したオプションに基づくインターバルで表示されるようにウィンドウの表示を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 FC\_MR-4 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** Utilization タブまたは History タブをクリックします。

**ステップ 4** Interval ドロップダウン リストで、次の 4 つのオプションからいずれかを選択します。

- 1 min — 指定した PM カウントが 1 分間隔で表示されます。
- 15 min — 指定した PM カウントが 15 分間隔で表示されます。
- 1 hour — 指定した PM カウントが 1 時間間隔で表示されます。
- 1 day — 指定した PM カウントが 1 日（24 時間）間隔で表示されます。

**ステップ 5** Refresh をクリックします。選択したインターバルに基づいて PM カウントの値がリフレッシュされます。

**ステップ 6** 元の NTP（手順）に戻ります。

## DLP-A356 TCC2/TCC2P カードのアクティブ/スタンバイ切り替えテスト

目的	この作業では、TCC2/TCC2P カード間の切り替えが有効に行われることを確認します。
工具 / 機器	受け入れテストの手順で指定されている接続および設定済みのテストセット
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	必須
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** View メニューから、**Go to Network View** を選択します。
- ステップ 2** Alarms タブをクリックします。
- 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-A227 アラーム フィルタリングのディセーブル化](#)」(p.19-21) を参照してください。
  - 説明のつかないアラーム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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 3** Conditions タブをクリックします。説明のつかない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。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。必要に応じて、『*Cisco ONS 15454 Troubleshooting Guide*』を参照してください。
- ステップ 4** ネットワーク マップ上で、テスト対象の TCC2/TCC2P カードを取り付けたノードをダブルクリックして、ノード ビューで開きます。
- ステップ 5** シェルフ図で LED を調べ、アクティブな TCC2/TCC2P カードとスタンバイ状態の TCC2/TCC2P カードを記録します。TCC2/TCC2P カードは、スロット 7 とスロット 11 に取り付けられています。アクティブ TCC2/TCC2P カードには、グリーン の ACT LED、スタンバイ TCC2/TCC2P カードにはオレンジの SBY LED があります。
- ステップ 6** シェルフ図でアクティブな TCC2/TCC2P カードを右クリックし、ショートカット メニューから **Reset** を選択します。
- ステップ 7** Resetting Card ダイアログボックスで **Yes** をクリックします。20 ~ 40 秒後に [lost node connection, changing to network view] というメッセージが表示されます。ネットワーク ビュー マップ上では、TCC2/TCC2P カードをリセットしたノードがグレーで表示されます。
- ステップ 8** ノード アイコンが利用可能になったら (1 ~ 2 分以内) ダブルクリックします。シェルフ図で、次の点を調べます。
- 前回スタンバイ状態だった TCC2/TCC2P カードにグリーン の ACT LED が表示されていること。
  - 前回アクティブ状態だった TCC2/TCC2P カードの LED が、NP (カードがない) Ldg (ソフトウェアのロード中) オレンジの SBY LED (TCC2/TCC2P がスタンバイ モード) の順に点灯すること。
- ステップ 9** ノードに接続されたテストセットのトラフィックが動作していることを確認します。トラフィックが中断する場合は、作業を中断し、次のレベルのサポートに問い合わせます。

## ■ DLP-A357 FC\_MR-4 RMON アラーム スレッシュホールドの作成

- ステップ 10** ステップ 2 ~ 9 を繰り返し、この手順を開始したときの TCC2/TCC2P カードのアクティブ / スタンバイ設定に戻します。
- ステップ 11** ステップ 5 で記録したとおりに TCC2/TCC2P カードが表示されることを確認します。
- ステップ 12** 元の NTP (手順) に戻ります。

## DLP-A357 FC\_MR-4 RMON アラーム スレッシュホールドの作成

目的	この作業では、Remote Monitoring (RMON) をセットアップして、ネットワーク管理システムで FC_MR-4 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> (RMON を設定するノードにおいて)
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、RMON アラームのスレッシュホールドを作成する FC\_MR-4 カードをダブルクリックします。
- ステップ 2** Provisioning > RMON Thresholds タブをクリックします。
- ステップ 3** Create をクリックします。Create Threshold ダイアログボックスが表示されます。
- ステップ 4** Slot ドロップダウン リストで、適切な FC\_MR-4 カードを選択します。
- ステップ 5** Port ドロップダウン リストで、選択した FC\_MR-4 カード上の該当す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 FC\_MR-4 のスレッシュホールド変数については、[表 20-1](#) を参照してください。

表 20-1 FC\_MR-4 のスレッシュホールド変数 — ファイバチャネル/FICON 回線速度モード (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)
ifInDiscards	エラーはないが、廃棄されて上位レイヤのプロトコルに渡されなかった着信パケット数
ifInErrors	エラーがあるために廃棄された着信パケット数

表 20-1 FC\_MR-4 のスレッシュホールド変数 — ファイバチャネル/FICON 回線速度モード (MIB) (続き)

変数	定義
ifOutOctets	送信オクテットの総数 (フレーミング パケットを含む)
ifOutDiscards	エラーはないが、廃棄されて送信されなかったパケット数
txTotalPkts	送信パケットの総数
rxTotalPkts	受信パケットの総数
fibreStatsInvalidOrderedSets	定義されているファイバ チャネル制御ワードの一部として認識できなかった受信順序付きセット数
fibreStatsEncodingDispErrors	不正なディスペリティが原因でデコードできなかった受信制御ワード数
fibreStatsRxFramesTooLong	サイズ超過の受信ファイバチャネルフレーム数 (Cyclic Redundancy Check [ CRC; 巡回冗長検査] を含めて 2148 超)
fibreStatsRxFramesBadCRC	CRC が不正な受信ファイバチャネルフレーム数
fibreStatsRxFrames	受信ファイバチャネルフレームの総数
fibreStatsRxOctets	受信ファイバチャネルデータの 1 フレームあたりのバイト数
fibreStatsTxFramesBadCRC	CRC が不正な送信ファイバチャネルフレーム数
fibreStatsTxFrames	送信ファイバチャネルフレームの総数
fibreStatsTxOctets	送信ファイバチャネルデータの 1 フレームあたりのバイト数
fibreStatsLinkResets	リンク回復のポート設定がイネーブルになっている場合に FCMR ポートによって行われたリンクのリセット回数
gfpStatsRxSBitErrors	コア ヘッダーに単一のビット エラーがあった受信 Generic Framing Protocol (GFP) フレーム数 (これらのエラーは修正可能)
gfpStatsRxMBitErrors	コア ヘッダーに複数ビット エラーがあった受信 GFP フレーム数 (これらのエラーは修正不可)
gfpStatsRxTypeInvalid	無効なタイプの受信 GFP フレーム数 (廃棄されます)。たとえば、ファイバチャネル データを受信するはずなのにイーサネット データを含む GFP フレームを受信した場合など。
gfpStatsRxSblkCRCErrors	受信透過 GFP フレームで検出されたスーパーブロックの CRC エラーの総数。透過 GFP フレームには、それぞれにファイバチャネル データを含む複数のスーパーブロックがあります。
gfpStatsCSFRaised	クライアント信号障害を表示している受信クライアント管理フレーム数
mediaIndStatsTxFramesTooLong	1548 バイト超の送信パケット数
mediaIndStatsRxFramesTruncated	5 バイト未満の受信フレームの総数

表 20-2 に、選択できる拡張モードの MIB を示します。

表 20-2 FC\_MR-4 のスレッシュホールド変数 — ファイバチャネル/FICON 拡張モード (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)
ifInDiscards	エラーはないが、廃棄されて上位レイヤのプロトコルに渡されなかった着信パケット数
ifInErrors	エラーがあるために廃棄された着信パケット数
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 20-2 FC\_MR-4 のスレッシュホールド変数 — ファイバチャネル/FICON 拡張モード(MIB)(続き)

変数	定義
ifOutDiscards	エラーはないが、廃棄されて送信されなかったパケット数
fcIngressRxDistanceExtBuffers	GFP レシーバーで使用可能な GFP バッファの最大数
fcEgressTxDistanceExtBuffers	GFP トランスミッタで送信可能な GFP バッファ数。リモート GFP レシーバーから GFP トランスミッタに送信可能なバッファ数が通知されます。
fcStatsLinkRecoveries	GFP のフレーム同期外れによりリンクのリセットが開始された回数。この値は、リンク回復がイネーブルな場合にだけ有効で、距離延長がイネーブルな場合には無効です。
fcStatsRxCredits	ファイバチャネルまたはファイバ接続 (FICON) リンクパートナーが、FCMR ファイバチャネルまたは FICON トランスミッタに送信を許可する、ファイバチャネルクレジットの最大数 (リンクパートナーが受信できるフレームの最大数)。
fcStatsTxCredits	FCMR のファイバチャネルまたは FICON トランスミッタに残っているファイバチャネルクレジットの数。すなわちファイバチャネルまたは FICON トランスミッタが送信できるフレーム数   (注) リンクパートナーからクレジットを受信すると送信クレジットは増加し、フレームが送信されると送信クレジットは減少します。
fcStatsZeroTxCredits	ファイバチャネルまたは FICON の送信クレジットがゼロ以外の値からゼロに移行すると増加するカウント。
fibreStatsInvalidOrderedSets	定義されているファイバチャネル制御ワードの一部として認識できなかった受信オーダーセット数
fibreStatsEncodingDispErrors	不正なディスパリティが原因でデコードできなかった受信制御ワード数
fibreStatsRxFramesTooLong	サイズ超過の受信ファイバチャネルフレーム数 (CRC を含めて 2148 超)
fibreStatsRxFramesBadCRC	CRC が不正な受信ファイバチャネルフレーム数
fibreStatsRxFrames	受信ファイバチャネルフレームの総数
fibreStatsRxOctets	受信ファイバチャネルデータの 1 フレームあたりのバイト数
fibreStatsTxFramesBadCRC	CRC が不正な送信ファイバチャネルフレーム数
fibreStatsTxFrames	送信ファイバチャネルフレームの総数
fibreStatsTxOctets	送信ファイバチャネルデータの 1 フレームあたりのバイト数
fibreStatsLinkResets	リンク回復のポート設定がイネーブルになっている場合に FCMR ポートによって行われたリンクのリセット回数
gfpStatsRxSBitErrors	コアヘッダーに単一のビットエラーがあった受信 GFP フレーム数 (これらのエラーは修正可能)
gfpStatsRxMBitErrors	コアヘッダーに複数ビットエラーがあった受信 GFP フレーム数 (これらのエラーは修正不可)
gfpStatsRxTypeInvalid	無効なタイプの受信 GFP フレーム数 (廃棄されます)。たとえば、ファイバチャネルデータを受信するはずなのにイーサネットデータを含む GFP フレームを受信した場合など。



表 20-2 FC\_MR-4 のスレッシュホールド変数 — ファイバチャネル/FICON 拡張モード(MIB)(続き)

変数	定義
gfpStatsRxSblkCRCErrors	受信透過 GFP フレームで検出されたスーパーブロックの CRC エラーの総数。透過 GFP フレームには、それぞれにファイバチャネルデータを含む複数のスーパーブロックがあります。
8b10bInvalidOrderedSets	ギガビット イーサネット / ファイバチャネル (GE/FC) 規格に準拠していないオーダードセットの総数
8b10bStatsEncodingDispErrors	GE/FC ディスパリティエラーに違反しているコードグループの総数。

**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、ユーザが設定する Sample Period に制限されません。Absolute を指定すると、スレッシュホールドは期間に関係なく、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 フィールドに適切な秒数を入力します。

**ステップ 10** Rising Threshold フィールド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 分あたり 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 分間に 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）がトリガーと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を初めて超えたときだけです（そうでなければ、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 をクリックします。

**ステップ 13** 元の NTP（手順）に戻ります。

## DLP-A358 FC\_MR-4 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、FC_MR-4 ポートの 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-A357 FC_MR-4 RMON アラーム スレッシュホールドの作成 (p.20-46) 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、RMON アラーム スレッシュホールドを削除する FC\_MR-4 カードをダブルクリックします。
- ステップ 2** Provisioning > 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-A359 LDCC 終端の削除

目的	この作業では、ONS 15454 にある SONET LDCC 終端を削除します。
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

DCC の終端を削除すると、他の DCC を持たないノードや、CTC コンピュータにネットワークで接続されていないノードが見えなくなることがあります。

---

- ステップ 1** Provisioning > Comm Channel > LDCC タブをクリックします。
- ステップ 2** 削除する LDCC の終端をクリックして、Delete をクリックします。Delete LDCC Termination ダイアログボックスが表示されます。

**ステップ 3** 確認用のダイアログボックスで **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 4** 元の NTP (手順) に戻ります。

## DLP-A362 BLSR ウィザードによる 4 ファイバ BLSR の作成

目的	この作業では、BLSR を設定した各ノードで CTC BLSR ウィザードを使用して 4 ファイバ BLSR を作成します。BLSR ウィザードで各ノードが BLSR のプロビジョニングを開始できる状態であるかどうかを確認し、すべてのノードを同時にプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A40 BLSR ノードのプロビジョニング (p.5-14)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > BLSR** タブをクリックします。

**ステップ 3** **Create BLSR** をクリックします。

**ステップ 4** BLSR Creation ダイアログボックスで、BLSR のプロパティを設定します。

- Ring Type — 4 ファイバを選択します。
- Speed — OC-48、または OC-192 から BLSR リングの速度を選択します。速度は BLSR トランク (スパン) カードの OC-N 速度と一致する必要があります。
- Ring Name — リング名を割り当てます。名前に使用できる文字数は、1 ~ 6 文字です。すべての英数字を大文字と小文字を組み合わせて指定することもできます。文字列 [All] は、TL1 のキーワードであるため、大文字か小文字かに関係なく使用できません。すでに他の BLSR に割り当てられている名前も指定できません。
- Reversion time — リングを切り替えたあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。リングの復元を、Never に設定することもできます。
- Span Reversion — スパンを切り替えたあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。スパンの復元を Never に設定することもできます。

**ステップ 5** **Next** をクリックします。ネットワーク図が表示されたら、ステップ 6 へ進みます。

取り付けられている光カードの数が不足している場合や、UPSR セレクタのある回線が検出された場合などは、BLSR を作成できません。CTC でそうした状況が判明すると、[Cannot Create BLSR] というメッセージが表示されます。このメッセージが表示された場合は、次のステップを実行します。

- OK をクリックします。
- Create BLSR ウィンドウで、**Excluded Nodes** をクリックします。BLSR を作成できない理由を確認し、**OK** をクリックします。

- c. 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。

**ステップ 6** ネットワーク図で、BLSR のスパン ラインを順番にダブルクリックしていきます。ダブルクリックしたスパン ラインが他の BLSR カードに DCC で接続されていて完全なリングを形成していれば、それらのラインがブルーになります。ラインをダブルクリックしてもまだ完全なリングを形成できていない場合は、完全なリングが作成されるまで別のスパン ラインをダブルクリックしていきます。リングが DCC 接続されたら、[ステップ 7](#)へ進みます。

**ステップ 7** Next をクリックします。Protect Port Selection セクションで、West Protect カラムと East Protect カラムから保護ポートを選択します。

**ステップ 8** Finish をクリックします。BLSR ウィンドウが開き、作成した BLSR が表示されたら、[ステップ 9](#)へ進みます。[Cannot Create BLSR] または [Error While Creating BLSR] というメッセージが表示された場合は、次の作業を行います。

- a. OK をクリックします。
- b. Create BLSR ウィンドウで、Excluded Nodes をクリックします。BLSR を作成できない理由を確認し、OK をクリックします。
- c. 障害の内容に応じて、Back をクリックして始めから作業を繰り返すか、または Cancel をクリックして作業を取り消します。
- d. 「NTP-A40 BLSR ノードのプロビジョニング」(p.5-14) を実行してすべてのステップが正しく完了していることを確認したあと、この手順を再度開始します。



**(注)** BLSR の設定時には、E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、および BLSROSYNC の各アラームのうち一部またはすべてが短時間表示されることがあります。

**ステップ 9** 次の点を確認します。

- ネットワーク ビューの図で、すべての BLSR ノード間にグリーンのスパン ラインが表示されていること。
- E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、および BLSROSYNC の各アラームがすべてクリアされていること。アラームのトラブルシューティングについては、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。



**(注)** ノード名の後ろにあるかっこ内の数字は、CTC によって割り当てられた BLSR ノード ID です。1 つの BLSR 内の各 ONS 15454 には、0 ~ 31 の一意なノード ID が割り当てられています。ノード ID を変更する場合は、「[DLP-A326 BLSR のノード ID の変更](#)」(p.20-17) を行います。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A363 4 ファイバ BLSR の手動作成

目的	この作業では、BLSR を設定した各ノードで BLSR ウィザードを使用せずに 4 ファイバ BLSR を作成します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > BLSR** 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** Suggestion ダイアログボックスで **OK** をクリックします。

**ステップ 4** Create BLSR ダイアログボックスで、BLSR のプロパティを設定します。

- Ring Type — 4 ファイバを選択します。
- Ring Name — リング名を割り当てます。BLSR 内の各ノードには、同じリング名を使用する必要があります。英数字で、大文字と小文字を組み合わせて指定できます。文字列 [All] は、TL1 のキーワードであるため、大文字か小文字かに関係なく使用できません。すでに他の BLSR に割り当てられている名前も指定できません。
- Node ID — ドロップダウン リストから ノード ID (0 ~ 31) を選択します。ノード ID は、BLSR でノードを識別するための ID です。同じ BLSR 内のノードの ID は一意でなければなりません。
- Reversion time — トラフィックが元の現用パスに復元するまでの時間を設定します。デフォルトは 5 分です。同じ BLSR 内のすべてのノードに同じ復元時間を設定する必要があります。
- West Line — ドロップダウン リストから ノードのウェスト BLSR ポートを割り当てます。  
「[NTP-A40 BLSR ノードのプロビジョニング](#)」(p.5-14) で設定したファイバ接続と DCC 終端の設定は、イースト ポートとウェスト ポートで一致している必要があります。
- East Line — ドロップダウン リストから ノードのイースト BLSR ポートを割り当てます。
- Span Reversion — スパンを復元したあと、トラフィックが元の現用パスに復元されるまでの時間を設定します。デフォルトは 5 分です。スパンの復元を Never に設定することもできます。復元時間を設定する場合、スパンの両端で時間が同じでなければなりません。つまり、ノード A のウェスト ファイバがノード B のイースト ポートに接続されている場合、ノード A のウェスト スパン復元時間はノード B のイースト スパン復元時間と一致していなければなりません。復元時間の不一致を回避するために、シスコでは、リング全体で同じスパン復元時間を使用することを推奨します。
- West Protect — ウェスト保護ファイバに接続するウェスト側の BLSR ポートを、ドロップダウン リストから選択します。
- East Protect — イースト保護ファイバに接続するイースト BLSR ポートを、ドロップダウン リストから割り当てます。

**ステップ 5** **OK** をクリックします。



**(注)** すべての BLSR ノードがプロビジョニングされるまで、E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、および BLSRROSYNC の各アラームのうち一部またはすべてが表示されます。BLSR のすべてのノードが設定されると、これらのアラームはクリアされます。

## ■ DLP-A364 CTC による TCC2/TCC2P カードのリセット

- ステップ 6** View メニューから **Go to Other Node** を選択します。
- ステップ 7** Select Node ダイアログボックスで、BLSR に追加する次のノードを選択します。
- ステップ 8** BLSR に追加する各ノードで、ステップ 1 ~ 7 を繰り返します。すべてのノードを追加したら、**ステップ 9** へ進みます。
- ステップ 9** View メニューから **Go to Network View** を選択します。10 ~ 15 秒経過したら、次の点を確認します。
- すべての BLSR ノード間に、グリーンのスパン ラインが表示されている。
  - E-W-MISMATCH、RING-MISMATCH、APSCIMP、APSCDFLTK、および BLSROSYNC の各アラームがすべてクリアされていること。
- ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A364 CTC による TCC2/TCC2P カードのリセット

目的	この作業では、TCC2/TCC2P カードをリセットして、ノードを冗長カードに切り替えます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A36 TCC2/TCC2P カードの取り付け (p.17-44)</a>
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

**警告**

モジュールやファンを取り付けたり取り外したりするときは、空きスロットやシャーシの内側に手を伸ばさないでください。回路の露出部に触れて、感電するおそれがあります。

**(注)**

TCC2/TCC2P をリセットする前に、データベースに加えられた変更内容が失われないように、最後に変更をプロビジョニングしてから、少なくとも 60 秒間待機する必要があります。

**(注)**

アクティブ側の TCC2/TCC2P でソフトウェア リセットを実行すると、AIC-I カードに対しても初期化処理が行われて、リセットされます。AIC-I カードのこのリセットは異常ではありません。アクティブ側の TCC2/TCC2P カードがソフトウェアによってリセットされるたびに行われます。

- ステップ 1** TCC2/TCC2P カードをリセットするノードで「[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、TCC2/TCC2P 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 3** Reset Card をクリックします。

**ステップ 4** 確認用のダイアログボックスが表示されたら、Yes をクリックします。

**ステップ 5** [Lost connection to node, changing to Network View] ダイアログボックスが表示されたら、OK をクリックします。



**(注)** TCC2/TCC2P がリブートしているときの LED の動作については、[表 19-2 \(p.19-38\)](#) を参照してください。

**ステップ 6** TCC2/TCC2P カードの LED がオレンジ (スタンバイ) になっていることを確認します。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A365 光保護切り替えの開始

目的	この手順では、光ポート上で手動切り替えまたは強制切り替えを開始します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Protection Groups 領域で、切り替える保護グループを選択します。

**ステップ 3** Selected Group 領域で、切り替えるカードとポートを選択します。

**ステップ 4** Manual (手動) または Force (強制) をクリックします。

手動切り替えを選択した場合は、パスのエラー レートが SD BER (ビット エラー レート) のスレッシュホールドよりも低いときにだけ、トラフィックが切り替えられます。強制切り替えを選択した場合は、パスが SD 状態や SF 状態にあっても、トラフィックが切り替えられます。ただし、強制切り替えは 1+1 保護チャンネル上の SF を無効にはできません。強制切り替えのプライオリティは、手動切り替えより高くなっています。

**ステップ 5** 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** 元の NTP (手順) に戻ります。

## DLP-A366 電気保護切り替えの開始

目的	この作業では、電気回路カードでトラフィックの切り替えを開始します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



(注) ユーザが開始する切り替えは、復元遅延より優先されます。つまり、ユーザが切り替えをクリアするとタイマーがクリアされ、ただちにトラフィックが復元されます。

- 
- 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** Protection Groups 領域で、切り替える保護グループを選択します。
- ステップ 3** Selected Group 領域で、切り替えるカードを選択します。
- ステップ 4** Switch をクリックします。
- ステップ 5** 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** 元の NTP (手順) に戻ります。
- 

## DLP-A367 プロビジョニング可能なパッチコードの作成

目的	この作業では、ネットワーク全般に OSPF によってアドバタイズされるユーザ プロビジョニング リンクである、プロビジョニング可能なパッチコードを作成します。プロビジョニング可能なパッチコードは、CTC ネットワーク ビューでは点線で表示されます。
工具 / 機器	パッチコードが必要となる具体的な状況については、『Cisco ONS 15454 Reference Manual』を参照してください。 OC-N、トランスポンダ / マックスポンダ、Optical Add/Drop Multiplexer (OADM; 光分岐挿入装置) およびマルチプレクサ / デマルチプレクサカード
事前準備手順	パッチコードがサポートされているカードの組み合わせについては、『Cisco ONS 15454 Reference Manual』を参照してください。 <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) 光ポートと、トランスポンダ / マックスポンダ、OADM、またはマルチプレクサ / デマルチプレクサポートとの間にプロビジョニング可能なパッチコードを設定する場合は、光ポートを SDCC/LDCC で終端するようにプロビジョニングします。ポートが 1+1 グループで保護されているときは、現用ポートを SDCC/LDCC で終端するようにプロビジョニングします。必要に応じて、「DLP-A377 SDCC 終端のプロビジョニング」(p.20-74) または 「DLP-A378 LDCC 終端のプロビジョニング」(p.20-77) を行います。



(注) リモート エンドが Y 字ケーブルで保護されている場合や、リモート エンドが OADM またはマルチプレクサ / デマルチプレクサのポートである場合は、光ポート側に 2 つのパッチコードが必要です。



(注) 光パッチコードは、OCH フィルタと OCH トランク ポートの間でプロビジョニングされる必要があります。



(注) プロビジョニング可能なパッチコードが、CTC により手動で作成された場合、TXP または MXP が最初の調整可能な波長で自動プロビジョニングするように設定されていると、TXP または MXP トランクは、OCH フィルタとして自動的に調整されます。TL1 インターフェイスでは、この機能は内部パッチコード (OPR-LINK) に限りサポートされています。

**ステップ 1** ノード ビューで、**Provisioning > Comm Channels > Provisionable Patchcords** タブをクリックします。ネットワーク ビューが表示されている場合は、**Provisioning > Provisionable Patchcords** タブをクリックします。

**ステップ 2** **Create** をクリックします。Provisionable Patchcord ダイアログボックスが表示されます。

**ステップ 3** Origination Node 領域で次の手順を実行します。

- a. ノード ビューが表示されている場合は、Origination Node にデフォルトで現在のノードが表示されています。ネットワーク ビューが表示されている場合は、ドロップダウン リストで対象となる送信元ノードをクリックします。
- b. TX/RX ID フィールドに、パッチコードの ID (0 ~ 32767) を入力します。
- c. 使用可能なスロットまたはポートのリストで、対象となる送信元スロットまたはポートをクリックします。

**ステップ 4** Termination Node 領域で、次の手順を実行します。

- a. ドロップダウン リストから対象となる終端ノードを選択します。リモート側ノードが以前に検出されていなかったにもかかわらず CTC からアクセスできる場合は、そのリモート側ノードの名前を入力します。

- b. TX/RX ID フィールドに、パッチコードの ID (0 ~ 32767) を入力します。パッチコードを同じノードの 2 つのカード間に設定する場合は、送信側と終端側の ID を別々のものにする必要があります。
- c. 使用可能なスロット / ポートのリストで、対象となる終端スロット / ポートをクリックします。送信元ポートと終端ポートは、それぞれ別のポートにする必要があります。

**ステップ 5** マルチプレクサ / デマルチプレクサカードに対して Tx と Rx を個別にプロビジョニングする必要がある場合は、**Separate Tx/Rx** チェックボックスをオンにします。それ以外の場合は、**ステップ 6** へ進みます。送信元の TX ポートと終端側の TX ポートはすでにプロビジョニングされています。次の手順を実行して、RX ポートをプロビジョニングします。

- a. Origination Node 領域の RX ID フィールドに、パッチコードの ID (0 ~ 32767) を入力します。Tx の ID と Rx の ID は、送信元と終端側でそれぞれ別の ID にする必要があります。
- b. 使用可能なスロットまたはポートのリストで、対象となる送信元スロットまたはポートをクリックします。
- c. Termination Node 領域の RX ID フィールドに、パッチコードの ID (0 ~ 32767) を入力します。Tx の ID と Rx の ID は、送信元と終端側でそれぞれ別の ID にする必要があります。
- d. 使用可能なスロット / ポートのリストで、対象となる終端スロット / ポートをクリックします。

**ステップ 6** OK をクリックします。

**ステップ 7** 1+1 保護グループにパッチコードをプロビジョニングした場合は、ダイアログボックスが表示され、ピア側にもパッチコードをプロビジョニングするかどうかを尋ねてきます。Yes をクリックします。ステップ 3 ~ 6 を繰り返します。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A368 プロビジョニング可能なパッチコードの削除

目的	この作業では、プロビジョニング可能なパッチコードを削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)

光ポートに残っている DCC の最後の終端を削除すると、そのポートにプロビジョニングされているすべてのプロビジョニング可能なパッチコードが自動的に削除されます。ポートが 1+1 保護グループである場合は、CTC によって、その保護ポート上のパッチコードリンクが自動的に削除されます。

**ステップ 1** ノード ビューで、**Provisioning > Comm Channels > Provisionable Patchcords** タブをクリックします。ネットワーク ビューが表示されている場合は、**Provisioning > Provisionable Patchcords** タブをクリックします。

- ステップ 2** 削除するプロビジョニング可能なパッチコードをクリックします。
- ステップ 3** Delete をクリックします。
- ステップ 4** 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 5** 元の NTP (手順) に戻ります。

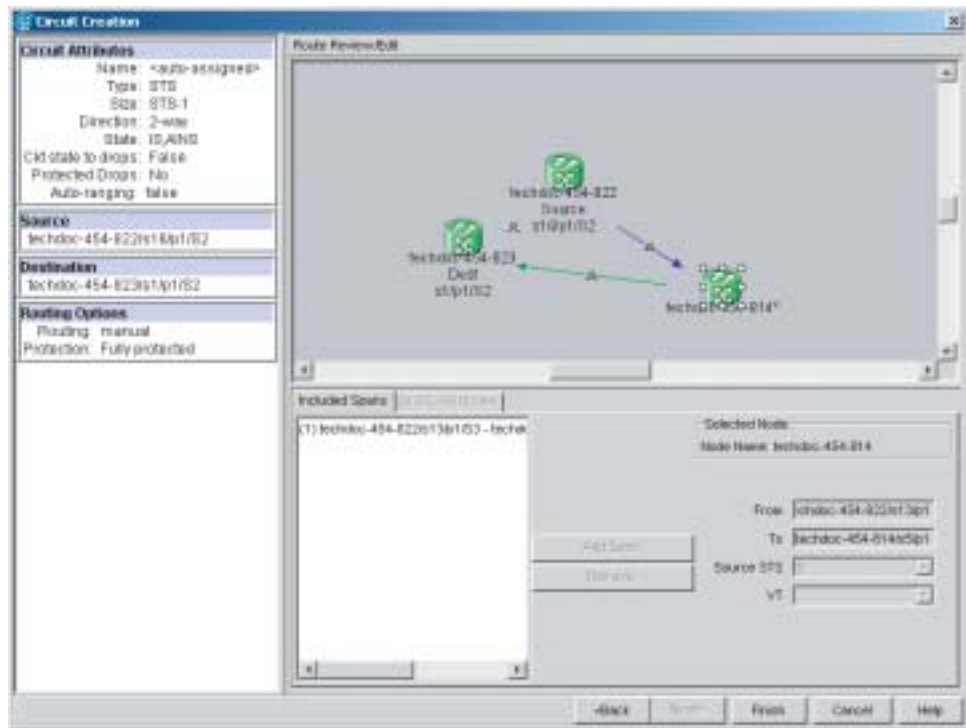
## DLP-A369 OC-N 回線ルートのプロビジョニング

目的	この作業では、手動ルーティング OC-N 回線の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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	Circuit Creation ウィザードの Route Review/Edit 領域を開いておく必要があります。
オンサイト / リモート	適宜
セキュリティ レベル	オンサイトまたはリモート 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/Edit 領域で送信元ノードのアイコンがまだ選択されていない場合は、そのアイコンをクリックします。
- ステップ 2** 送信元ノードにあるスパンから開始して、回線を通過させるスパンの矢印をクリックしていきま  
す。矢印の方向を反対にするには、矢印を 2 回クリックします。

矢印がイエローになります。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。送信元 STS が表示されます。図 20-9 に、手動でルーティングされた回線の例  
を示します。

図 20-9 手動による OC-N 回線のルーティング



**ステップ 3** 送信元の STS を変更する場合は、Source STS 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。



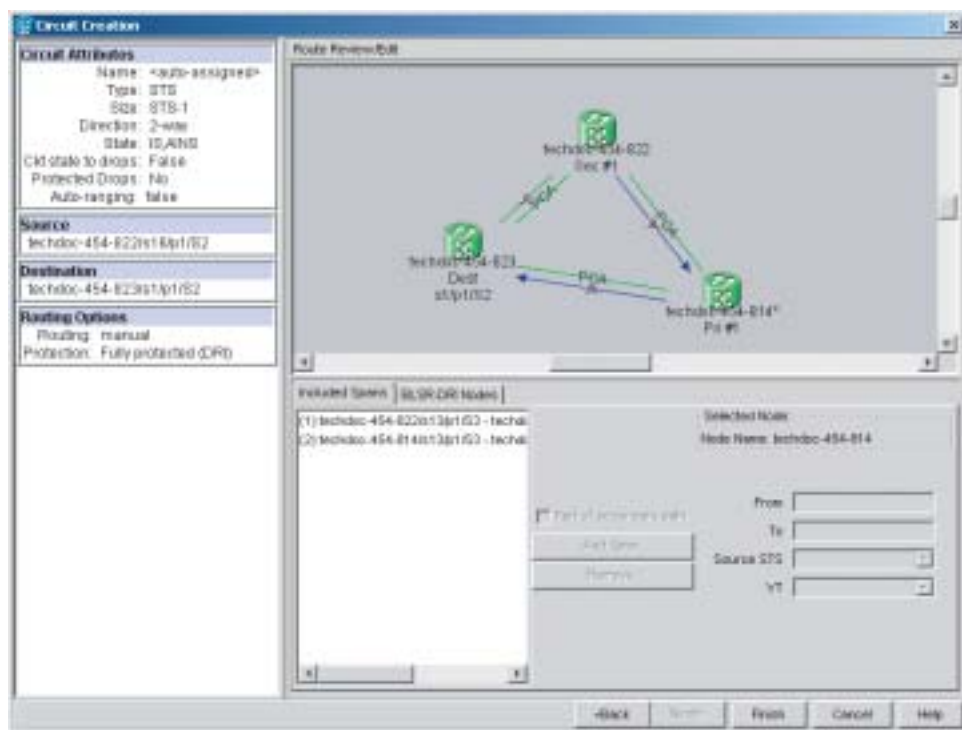
(注) OC-N 回線では VT オプションがディセーブルになっています。

**ステップ 4** 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 5** 中継ノードも含めて回線が送信元から宛先まですべてプロビジョニングされるまで、[ステップ 2 ~ 4](#)を繰り返します。Circuit Routing Preferences ページで Fully Protected Path がオンになっている場合は、次の作業を行います。

- 送信元から宛先までの回線ルートにあるすべての UPSR 部分または保護されていない部分に対しては、2 つのスパンを追加します。
- 送信元から宛先までのルートにあるすべての BLSR 部分または 1+1 部分に対しては、1 つのスパンを追加します。
- プライマリ ノードを通過して送信元から宛先に至るルートにある BLSR-DRI については、プライマリ スパンを追加します。また、セカンダリ ルートとして、セカンダリ ノード同士をつなぐスパンを追加します。[図 20-10](#)に、手動でルーティングされた BLSR DRI 回線の例を示します。PCA スパンは、セカンダリ パスの構成要素としてだけ選択できます。

図 20-10 BLSR DRI 回線ルートの手動ルーティング



**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A371 パススルー接続の削除

目的	この作業では、リングから削除したノードのパススルー接続を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 削除したノードにログインします。

**ステップ 2** CTC の Login ダイアログボックスで、**Disable Network Discovery** チェックボックスをオンにします。

**ステップ 3** Additional Nodes ドロップダウン リストから、**None** を選択します。

**ステップ 4** Login ボタンをクリックします。

**ステップ 5** Circuits タブをクリックします。ノード間にあるすべての回線が PARTIAL になっています。

## ■ DLP-A372 指定したログイン ノード グループからのノードの削除

**ステップ 6** 「NTP-A240 BLSR ノードの削除」(p.14-7) または 「NTP-A294 UPSR ノードの削除」(p.14-14) で作成したダイアグラムまたは CTC のプリントアウトを参照して、削除したノードのライン カードにある回線を見つけます。

**ステップ 7** Filter ボタンをクリックします。

**ステップ 8** 削除したノードにあるトランク カードのスロットとポートを入力します。

**ステップ 9** OK をクリックします。

**ステップ 10** Circuits タブで、フィルタにかけられた PARTIAL 回線をすべて選択し、Delete ボタンをクリックします。



**(注)** 回線を複数選択する場合は、Shift キーを押しながら、削除する回線をすべてクリックします。

**ステップ 11** もう一方のトランク カードについて、ステップ 6 ~ 10 を繰り返します。

**ステップ 12** CTC からログアウトします。

**ステップ 13** 元の NTP (手順) に戻ります。

## DLP-A372 指定したログイン ノード グループからのノードの削除

目的	この作業では、指定したログイン ノード グループからノードを削除します。現在のログイン ノード グループからノードを削除する方法については、「DLP-A339 現在のセッションまたはログイン グループからのノードの削除」(p.20-34) を参照してください。
工具	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** CTC Edit メニューから、Preferences を選択します。

**ステップ 2** Preferences ダイアログボックスで、Login Node Groups タブをクリックします。

**ステップ 3** 削除するノードが含まれているログイン ノード グループのタブをクリックします。

**ステップ 4** 削除するノードをクリックし、続いて Remove をクリックします。

**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-A373 MiniBNC EIA の取り付け

目的	この作業では、MiniBNC EIA を取り付けます。MiniBNC EIA は DS-1、DS-3、DS3XM カードで使用できます。
工具 / 機器	#2 プラス ドライバ  小型スロット ヘッド ネジ用ドライバ  6 本の周辺ネジ (6-32 × 0.375 インチのプラス ネジ) (P/N 48-0422-01)  A 側 (15454-xxxx) MiniBNC EIA パネルおよび B 側 (15454-xxx) MiniBNC EIA パネル (またはどちらか一方)
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
セキュリティ レベル	なし



**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず静電気防止用 (ESD) リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンド ケーブルを接続してください。



**(注)**

MiniBNC EIA を取り付けられるのは、15454-SA-HD シェルフ アセンブリのみです。15454-SA-HD シェルフ アセンブリは、ブルーの六角形の印で他のシェルフ アセンブリと区別されています。この印は、利用可能な高密度スロット (スロット 1 ~ 3 と 15 ~ 17) の下についています。



**(注)**

高密度の電気回路カード (48 ポートの DS-3 および DS3XM-12) を使用する場合に、MiniBNC または UBIC EIA が必要になります。

- ステップ 1** 取り付けを行う側に合った MiniBNC EIA をパッケージの中から探し、取り出します。
- ステップ 2** MiniBNC EIA のすべてのピンが曲がっていないことを確認します。
- ステップ 3** 曲がっているピンがある場合は、イエローのコネクタ プロテクタを取り外します。
- ステップ 4** カードのコネクタをバックプレーンの対応コネクタに合わせ、カードの背面にあるキーがバックプレーンと正しく合うようにします。コネクタがしっかりかみ合うまでカードを一定の圧力で押し込みます。

**注意**

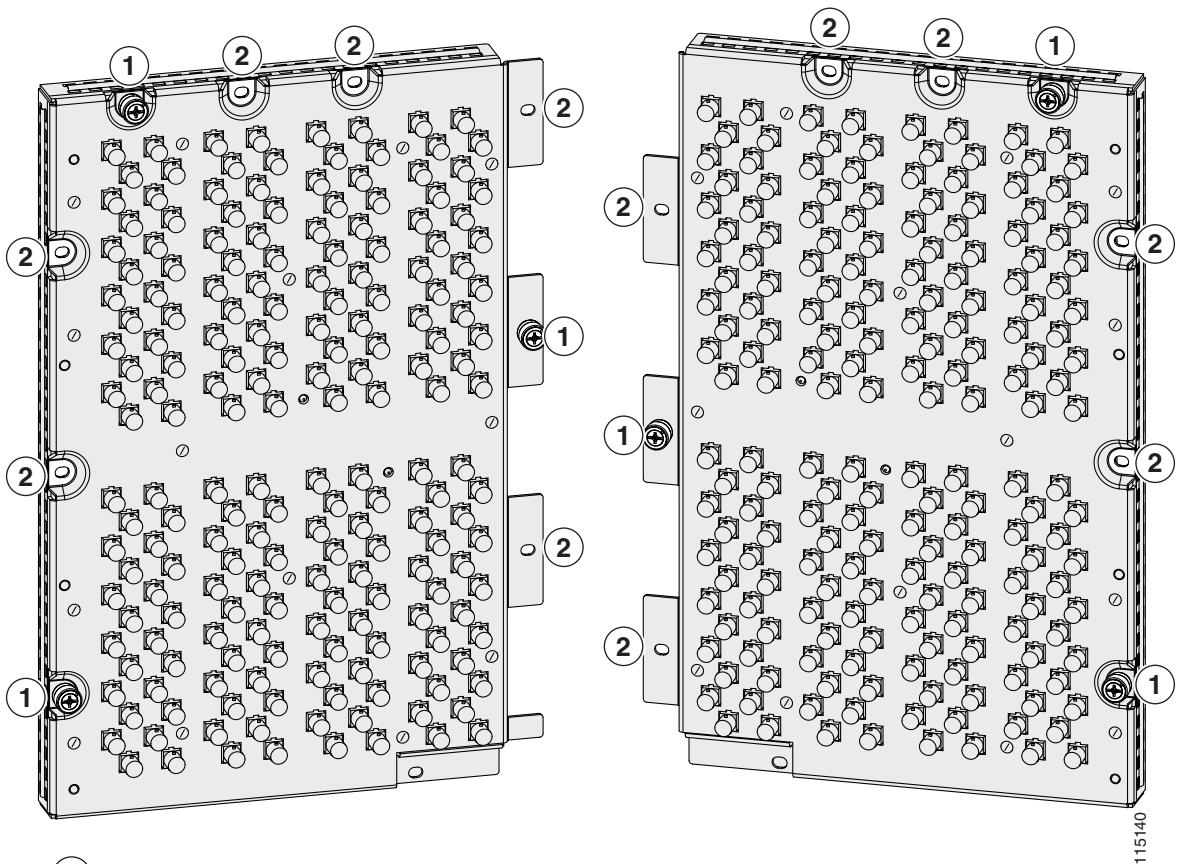
強い抵抗感がある場合には、MiniBNC EIA を無理にバックプレーンに押し込まないでください。MiniBNC EIA がバックプレーンと正しく合い、バックプレーンのピンが曲がっていないことを確認します。

**ステップ 5** MiniBNC の 3 本のジャックネジを探します (図 20-11)。任意の取り付けネジから始め、数回まわして締めたら、次のネジに移ります。3 本のネジがすべて固く締まるまで、各取り付けネジを一度に数回ずつ順番にまわします (図 20-12)。

**注意**

不均等にジャックネジを締めると、MiniBNC コネクタが損傷することがあります。

図 20-11 MiniBNC EIA ネジの位置

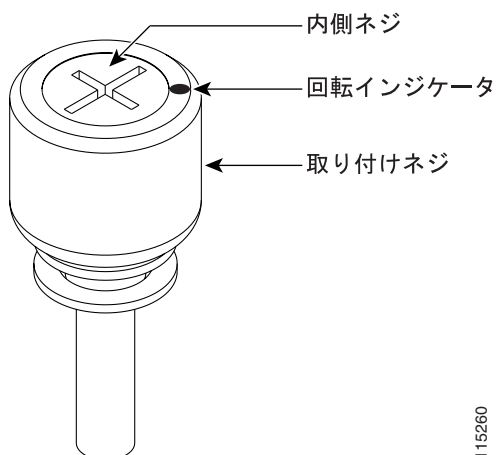


① ジャックネジ (3)

② 周辺ネジ (6-32 × 0.375 インチ プラス ネジ) (6)



図 20-12 MiniBNC EIA のジャックネジ

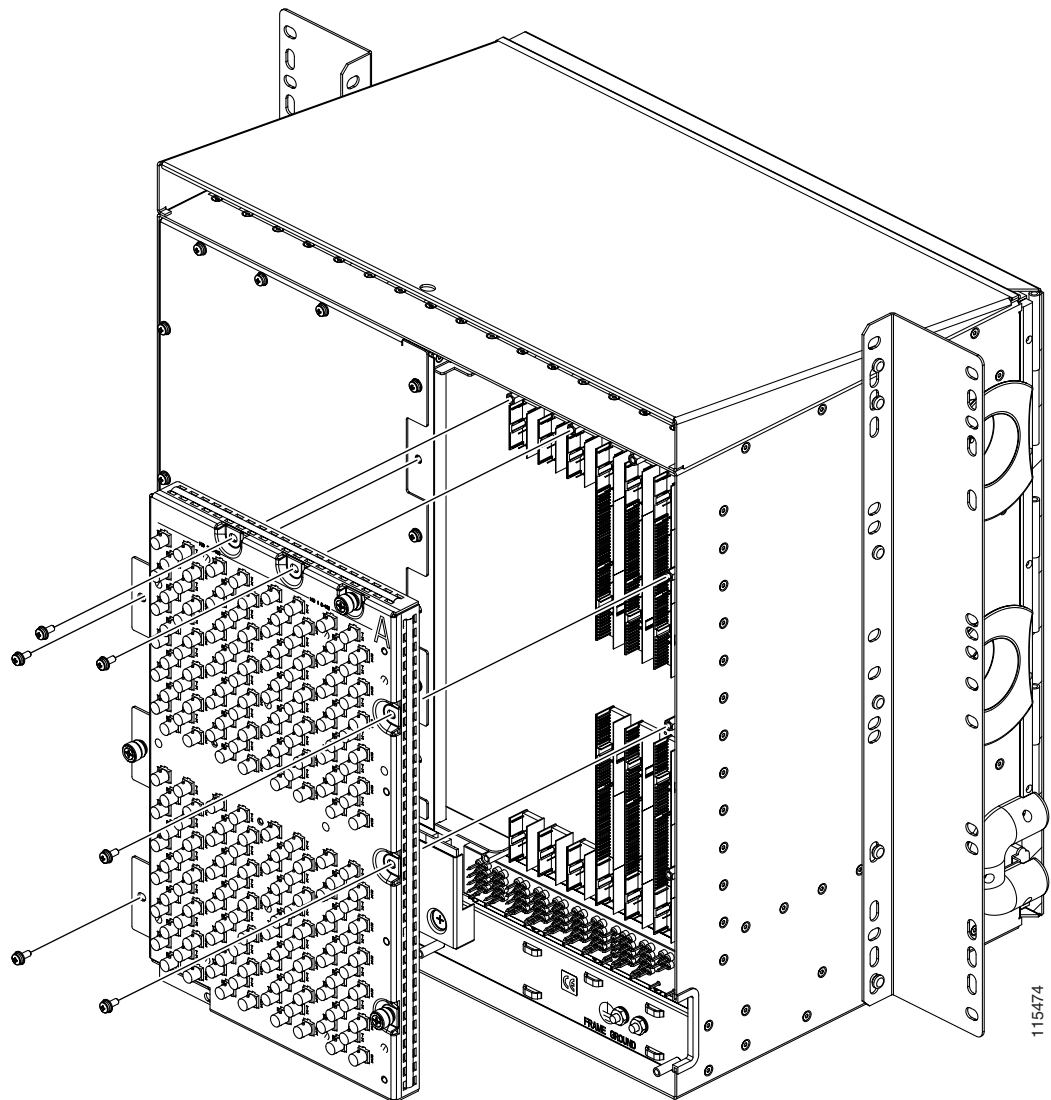


115260

**ステップ 6** プラス ドライバを使用して、6 本の周辺ネジとブラケット ネジ ( P/N 48-0422-01 ) を 8 ~ 10 lbf-inch ( 9.2 ~ 11.5 kgf-cm ) で取り付け、カバー パネルをバックプレーンに固定します ( 図 20-11 )。アラームおよびタイミングパネルのカバーを取り付け、最後の周辺ネジを差し込んで締めます。

図 20-13 に、MiniBNC EIA の取り付けを示します。

図 20-13 MiniBNC EIA の取り付け



**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A374 SDCC 終端の変更

目的	この作業では、SDCC を変更します。Open Shortest Path First (OSPF) と外部ノードの設定をイネーブルまたはディセーブルにできます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	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 > Comm Channels > SDCC の順でタブを選択します。
- ステップ 2** 変更する SDCC 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** SDCC Termination Editor ダイアログボックスで、次のように設定します。
- Disable OSPF on SDCC Link — オンにすると、そのリンクで OSPF がディセーブルになります。OSPF をディセーブルにする必要があるのは、スロットとポートの接続先が OSPF をサポートしていないサードパーティ製の装置である場合だけです。
  - Far End is Foreign — SDCC の終端が ONS ノードでない場合に、このボックスをオンにします。
  - Far End IP — Far End is Foreign チェックボックスをオンにした場合は、遠端側ノードの IP アドレスを入力するか、デフォルトの 0.0.0.0 のままにしておきます。IP アドレスが 0.0.0.0 の場合は、遠端側でどのアドレスを使用してもよいことを意味します。
- ステップ 5** OK をクリックします。
- ステップ 6** 元の手順 (NTP) に戻ります。
- 

## DLP-A375 LDCC 終端の変更

目的	この作業では、LDCC を変更します。OSPF と外部ノードの設定をイネーブルまたはディセーブルにできます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	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 > Comm Channels > LDCC の順でタブを選択します。
- ステップ 2** 変更する LDCC 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** LDCC Termination Editor ダイアログボックスで、次のように設定します。
- Disable OSPF on LDCC Link — オンにすると、そのリンクで OSPF がディセーブルになります。OSPF をディセーブルにする必要があるのは、スロットとポートの接続先が OSPF をサポートしていないサードパーティ製の装置である場合だけです。
  - Far End is Foreign — LDCC の終端が ONS ノードでない場合に、このボックスをオンにします。
  - Far end IP — Far End is Foreign チェックボックスをオンにした場合は、遠端側ノードの IP アドレスを入力するか、デフォルトの 0.0.0.0 のままにしておきます。IP アドレスが 0.0.0.0 の場合は、遠端側でどのアドレスを使用してもよいことを意味します。
- ステップ 5** OK をクリックします。

**ステップ 6** 元の手順 (NTP) に戻ります。

## DLP-A376 DS1/E1-56 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、DS1/E1-56 カードの回線および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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 回線またはスレッシュホールドの設定変更を行う DS1/E1-56 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、SONET Thresholds、または Cards 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 20-3](#) 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 20-4](#) 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 20-5](#) 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 20-6](#) を参照してください。カード設定の定義については、[表 20-7](#) を参照してください。

表 20-3 に、DS1/E1-56 カードに対する Provisioning > Line タブの値を示します。

表 20-3 DS1/E1-56 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 ~ 56
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。
Admin State	ポートの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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
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。	<ul style="list-style-type: none"> <li>IS-NR — 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。</li> <li>OOS-AU,AINS — 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。</li> <li>OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>
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。	<ul style="list-style-type: none"> <li>1E-3</li> <li>1E-4</li> <li>1E-5</li> </ul>

表 20-3 DS1/E1-56 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
SD BER	信号劣化ビット エラー レートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• Unframed ( デフォルト )</li> <li>• M13</li> <li>• C BIT</li> <li>• Auto Provision Fmt</li> </ul>
Line Coding	使用される DS-3 伝送符号化タイプを定義します。	<ul style="list-style-type: none"> <li>• B3ZS</li> <li>• AMI</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 0 ~ 131 ( デフォルト )</li> <li>• 132 ~ 262</li> <li>• 263 ~ 393</li> <li>• 394 ~ 524</li> <li>• 525 ~ 655</li> </ul>
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。有効範囲は、0 ~ 48 時間、15 分刻みです。
FDL Mode	遠端ループバックと遠端 PM のモードを設定します。	<ul style="list-style-type: none"> <li>• T1.403</li> <li>• Bidirectional Fiber Data Link ( BFDL )</li> </ul>
Send AIS-V for Ds1 AIS	回線側のトリガーが発生した場合、( バックプレーン / システム側に向かって回線側から ) DS1 AIS の代わりに、Alarm Indication Signal VT ( AIS-V ) を送信します。	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト )</li> <li>• On ( オン )</li> </ul>
Raise AIS for LOF	Loss of Frame ( LOF; フレーム損失 ) が発生した場合に、Alarm Indication Signal ( AIS; アラーム表示信号 ) を送信します。	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト )</li> <li>• On ( オン )</li> </ul>
ProvidesSync	近端のタイミング基準として、ポートがプロビジョニングされます。	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト )</li> <li>• On ( オン )</li> </ul>
SyncMsgIn	SSM ( S1 バイト ) を有効にして、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。	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト )</li> <li>• On ( オン )</li> </ul>
SendDoNotUse	Do Not Use ( DUS ) メッセージが S1 バイトで送信されます。	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト )</li> <li>• On ( オン )</li> </ul>

表 20-3 DS1/E1-56 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
Enable Retiming	<p>オンにすると、Network Element (NE; ネットワーク要素)のクロック基準に対して送信クロックの時間再調整を行い、電気回路パスに対する電気回路カードと SONET 送信タイム ドメインとの非同期関係を取り除きます。</p> <p>オフにすると、ポートが [through-timed] の状態に置かれます。つまり、送信クロックはバックプレーンから送信される SONET ペイロードの DS1/E1 データから抽出されません。</p>	<ul style="list-style-type: none"> <li>• Off ( オフ、デフォルト)</li> <li>• On ( オン)</li> </ul>
Ds1 Mapping	マッピング モードを設定します。	<ul style="list-style-type: none"> <li>• Asynchronous : DS1 transport over SONET は、VT1.5 ( VT 構造を持つ STS-1 Synchronous Payload Envelope [ SPE; 同期ペイロード エンベロープ ] 内 )への非同期マッピングを使用します。</li> <li>• Byte Synchronous : DS1 transport over SONET は、VT1.5 ( VT 構造を持つ STS-1 SPE 内 )へのバイト同期マッピングを使用します。</li> <li>• Japan Byte Synchronous : E1 transport over SONET は、VT2 ( VT 構造を持つ STS-1 SPE 内 )への非同期マッピングを使用します。</li> </ul>
Admin SSM	SSM の Synchronization Traceability Unknown ( STU; 同期追跡不能 ) の値を無効にします。ノードが SSM 信号を受信しない場合、デフォルトの STU に戻ります。	<ul style="list-style-type: none"> <li>• PRS — Primary Reference Source ( Stratum 1 )</li> <li>• ST2 — Stratum 2</li> <li>• TNC — Transit Node Clock</li> <li>• ST3E — Stratum 3E</li> <li>• ST3 — Stratum 3</li> <li>• SMC — SONET Minimum Clock</li> <li>• ST4 — Stratum 4</li> <li>• DUS — タイミング同期に対して使用しません。</li> <li>• RES — Reserved ( 予約済み )。ユーザが設定する品質レベル</li> </ul>

表 20-4 に、DS1/E1-56 カードに対する Provisioning > Line Thresholds タブの値を示します。

表 20-4 DS1/E1-56 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 ~ 56 )
CV	符号化違反数。近端のみで利用可能
ES	エラー秒数。近端のみで利用可能

表 20-4 DS1/E1-56 カードの回線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。近端のみで利用可能
LOSS	LOS 秒数。1 つまたは複数の LOS 障害が発生した 1 秒間の間隔です。近端のみで利用可能
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 20-5 に、DS1/E1-56 カードに対する Provisioning > Elect Path Thresholds タブの値を示します。

表 20-5 DS1/E1-56 カードの電気回路バス 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 ~ 56)
CV	符号化違反数。近端および遠端で利用可能
ES	エラー秒数。近端および遠端で利用可能
SES	重大エラー秒数。近端および遠端で利用可能
SAS	重大エラー フレーム / アラーム表示信号。近端のみで利用可能
AISS	AIS 秒数。近端のみで利用可能
UAS	使用不可秒数。近端および遠端で利用可能
FC	障害カウント。近端のみで利用可能
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 20-6 に、DS1/E1-56 カードに対する Provisioning > SONET Thresholds タブの値を示します。

表 20-6 DS1/E1-56 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) STS に対して分割されている DS-1 ポート Line 1, STS 1、Line 2, STS 1 Line 3, STS 1、Line 4, STS 1
CV	符号化違反数。近端および遠端で利用可能、STS 終端専用。
ES	エラー秒数。近端および遠端で利用可能、STS 終端専用。
FC	障害カウント。近端および遠端で利用可能、STS 終端専用。
SES	重大エラー秒数。近端および遠端で利用可能、STS 終端専用。
UAS	使用不可秒数。近端および遠端で利用可能、STS 終端専用。
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 20-7 に、DS1/E1-56 カードに対する Provisioning > Card タブの値を示します。

表 20-7 DS1/E1-56 カードのカード オプション


パラメータ	内容	オプション
Transport Mode	カプセル化モードを設定します。	<ul style="list-style-type: none"> <li>SONET:(DS1 のデフォルト)VT1.5 で DS1、VT2 で E1 を送信します。AU4 モードでは、1 つの STS-3c 回線だけが許可されます。</li> <li>AU4:(E1 のデフォルト)構造化された VC4 ペイロード(STS-3c)で DS1 と E1 を送信します。</li> </ul> <p> (注) ポートが回線内にある場合、稼働中の場合、または NE のタイミング基準として選択されている場合は、1 つのトランスポート モードから別のモードに切り替えることはできません。</p>
Operating Mode	ポート使用率を設定します。これらの選択項目間の切り替えは、既存の回線、稼働中のポート、および NE 基準ソースとしてのポートでは制限されています。	<ul style="list-style-type: none"> <li>All DS1:(デフォルト)56 ポートがすべて DS1 ポートとして使用されます。1 ~ 28 のポートには、タイミング再調整機能があります。56 ポートのどれでも、NE に対するタイミング基準を提供するように選択できます。</li> <li>All E1:56 ポートがすべて E1 ポートとして使用されます。1 ~ 21 のポートには、タイミング再調整機能があります。56 ポートのどれでも、NE に対するタイミング基準を提供するように選択できます。</li> </ul>
Retiming Enabled	<p>オンにすると、NE のクロック基準に対して送信クロックの時間再調整を行い、電気回路パスに対する電気回路カードと SONET 送信タイムドメインとの非同期関係を取り除きます。Operating Mode が All DS1 の場合、Retiming Enabled がオンになり、変更できません。</p> <p>E1 モードに対してオフにすると、ポートが [through-timed] の状態に置かれます。つまり、送信クロックはバックプレーンから送信される SONET ペイロードの DS1/E1 データから抽出されます。</p>	<ul style="list-style-type: none"> <li>On (オン、デフォルト)</li> <li>Off (オフ)</li> </ul>

表 20-7 DS1/E1-56 カードのカード オプション (続き)

パラメータ	内容	オプション
Port to VT Mapping	DS1 ポートが STS-1 内の VT1.5 にマップされる順序を選択します。この設定は、同じ STS-1 に関連付けられた DS1 ポートのグループに適用されます。	<ul style="list-style-type: none"> <li>GR 253 は、VT1.5 (DS1-14 と互換性がある) に DS1 ポートをインターリーブします。このマッピングでは、連続する DS1 ポートの番号が VT1.5 の 7 つの VT グループをインターリーブするようにマッピングされます。VT グループをインターリーブすることは、Telcordia GR-253 に示されているように、原則的に DS1 ポートが VT1.5 の送信順序に従うことを意味します。</li> <li>INDUSTRY は、連続する DS1 ポートの番号をマッピングして、各 VT グループを順番に埋めていきます。このマッピングでは、連続するポートが VT に圧縮され、VT グループ全体を埋めてから、次の VT グループに移動します。</li> </ul>



(注) スレッシュホールド値は、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-A377 SDCC 終端のプロビジョニング

目的	この作業では、アラーム、管理データ、信号制御情報、およびメッセージに必要な、SONET DCC の終端を作成します。この作業では、ノードが ONS 以外の遠端ノードに DCC ネットワーク経由で直接 IP アクセスできるように、ノードを設定することもできます。また、この作業では、DCC の OSI サブネットワーク接続ポイントを作成して、OSI プロトコルスタックに基づくサードパーティ製の NE とノードをネットワーク接続できるようにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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

ONS 15454 が OSI の IS Level 1 または IS Level 1/Level 2 ノードとして設定されている状態で、サードパーティ製 NE に OSI 専用 (LAP-D) SDCC をプロビジョニングする場合、ベンダー NE の最大エリアルーティングパラメータが 3 に設定されていることを確認してから、この作業を開始してください。



**(注)** SDCC をプロビジョニングすると、同じポートに LDCC 終端をプロビジョニングできますが、推奨はしません。同じポートで SDCC と LDCC を使用する必要があるのは、LDCC をサポートしていないソフトウェアバージョンをアップグレードする間だけです。SDCC と LDCC は、同じノードの別のポートにプロビジョニングできます。

**ステップ 1** ノード ビューで、**Provisioning > Comm Channels > SDCC** 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 SDCC Terminations** ダイアログボックスで、SDCC の終端を作成するポートをクリックします。複数のポートを選択する場合は、Shift キーまたは Ctrl キーを押します。



**(注)** SDCC とは、ONS 15454 の DCC 終端に使用される Section DCC です。SONET LDCC と SDCC (ONS 15454 が DCC 終端に使用していない場合) は、DCC トンネルとしてプロビジョニングできます。「[DLP-A313 DCC トンネルの作成](#)」(p.20-7) を参照してください。

**ステップ 4** Port Admin State 領域で **Set to IS** をクリックして、ポートを稼働状態にします。

**ステップ 5** **Disable OSPF on SDCC Link** がオフになっていることを確認します。

**ステップ 6** SDCC の終端に ONS 以外のノードを含める場合は、**Far End is Foreign** チェックボックスをオンにします。この操作によって、自動的に遠端ノードの IP アドレスが 0.0.0.0 に設定されます。これは、遠端でどのアドレスでも指定できることを表します。デフォルト値を特定の IP アドレスに変更する場合は、「[DLP-A374 SDCC 終端の変更](#)」(p.20-66) を参照してください。

**ステップ 7** Layer 3 ボックスで、次のいずれかを実行します。

- IP ボックスのみをオンにする — SDCC が ONS 15454 と別の ONS ノードの間にあり、ネットワーク上に ONS ノードのみがある場合。SDCC は PPP (ポイントツーポイント プロトコル) を使用します。
- IP ボックスと OSI ボックスをオンにする — SDCC が ONS 15454 と別の ONS ノードの間にあり、OSI プロトコル スタックを使用するサードパーティ製の NE が同じネットワーク上にある場合。SDCC は PPP を使用します。
- OSI ボックスのみをオンにする — SDCC が ONS ノードと、OSI プロトコル スタックを使用するサードパーティ製の NE の間にある場合。SDCC は LAP-D プロトコルを使用します。



**(注)** OSI ボックスがオンで、IP ボックスがオフ (LAP-D) の場合、ネットワーク ビューにネットワーク接続は表示されません。

**ステップ 8** OSI ボックスがオンの場合は、次のステップを実行します。IP ボックスのみをオンにした場合は、[ステップ 9](#) に進みます。

a. **Next** をクリックします。

- b. 次のフィールドをプロビジョニングします。
- Router — OSI ルータを選択します。
  - ESH — End System Hello (ESH) 伝播頻度を設定します。End System (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 (プロトコル データ ユニット) の伝播頻度を設定します。Intermediate System (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 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。
  - Metric — 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メトリック コストは 20 です。通常は、この値は変更しないでください。
- c. OSI ボックスおよび IP ボックスがオンの場合は、[ステップ 9](#)へ進みます。OSI ボックスのみがオンの場合は、Next をクリックして、次のフィールドをプロビジョニングします。
- Mode
    - AITS — (デフォルト) Acknowledged Information Transfer Service。2 つの LAP-D ユーザ間に論理接続が確立されるまで、データを交換しません。このサービスにより、信頼性の高いデータ転送、フロー制御、およびエラー制御のメカニズムが実現します。
    - UIITS — Unacknowledged Information Transfer Service。ユーザ データが格納されたフレームを、確認応答なしで転送します。このサービスでは、特定のユーザから送信されたデータが別のユーザに確実に配信される保証はなく、配信に失敗した場合にもユーザに通知されません。また、フロー制御またはエラー制御のメカニズムもありません。
  - Role — Mode が AITS に設定されている場合、LAP-D フレーム Command/Response (C/R) 値を設定します。SDCC の反対側の NE では逆のモードに設定します。
  - MTU — Maximum Transmission Unit (最大伝送ユニット) LAP-D 情報フレームの最大オクテット数を設定します。指定できる範囲は 512 ~ 1500 オクテットです。デフォルトは 512 です。通常、この値は変更しないでください。
  - T200 — Set Asynchronous Balanced Mode (SABME) フレームの再送信間隔を設定します。デフォルトは 0.2 秒です。選択できる範囲は 0.2 ~ 20 秒です。
  - T203 — フレーム交換の最大間隔、つまり、LAP-D 「キープアライブ」 Receive Ready (RR) フレームを送信するためのトリガーをプロビジョニングします。デフォルトは 10 秒です。選択できる範囲は 4 ~ 120 秒です。

**ステップ 9** Finish をクリックします。



**(注)** すべてのネットワーク DCC 終端を作成してその OC-N ポートを稼働させるまでは、EOC (DCC 終端エラー) アラームと LOS アラームが表示され続けます。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A378 LDCC 終端のプロビジョニング

目的	この作業では、アラーム、管理データ、信号制御情報、およびメッセージに必要な、LDCC の終端を作成します。LDCC のサイズは、SDCC の 3 倍です。この作業では、ノードが ONS 以外の遠端ノードに DCC ネットワーク経由で直接 IP アクセスできるように、ノードを設定することもできます。また、この作業では、DCC の OSI サブネットワーク接続ポイントを作成して、OSI プロトコルスタックに基づくサードパーティ製の NE とノードをネットワーク接続できるようにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)** LDCC をプロビジョニングすると、同じポートに SDCC 終端をプロビジョニングできますが、推奨はしません。同じポートで SDCC と LDCC を使用する必要があるのは、LDCC をサポートしていないソフトウェアバージョンをアップグレードする間だけです。SDCC と LDCC は、同じノードの別のポートにプロビジョニングできます。

- 
- ステップ 1** ノード ビューで **Provisioning > Comm Channels > LDCC** 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 LDCC Terminations** ダイアログボックスで、LDCC の終端を作成するポートをクリックします。複数のポートを選択する場合は、Shift キーまたは Ctrl キーを押します。



**(注)** LDCC とは、ONS 15454 の DCC 終端に使用される Line DCC のことです。SONET LDCC と SDCC (ONS 15454 が DCC 終端に使用していない場合) は、DCC トンネルとしてプロビジョニングできます。「[DLP-A313 DCC トンネルの作成](#)」(p.20-7) を参照してください。

- ステップ 4** Port Admin State 領域で **Set to IS** をクリックして、ポートを稼働状態にします。
- ステップ 5** Disable OSPF on DCC Link チェックボックスがオフになっていることを確認します。
- ステップ 6** SDCC の終端に ONS 以外のノードを含める場合は、**Far End is Foreign** チェックボックスをオンにします。この操作によって、自動的に遠端ノードの IP アドレスが 0.0.0.0 に設定されます。これは、遠端でどのアドレスでも指定できることを表します。デフォルト値を特定の IP アドレスに変更する場合は、「[DLP-A375 LDCC 終端の変更](#)」(p.20-67) を参照してください。
- ステップ 7** Layer 3 ボックスで、次のいずれかを実行します。
- IP ボックスのみをオンにする — LDCC が ONS 15454 と別の ONS ノードの間にあり、ネットワーク上に ONS ノードのみがある場合、LDCC は PPP を使用します。

- IP ボックスと OSI ボックスをオンにする — LDCC が ONS 15454 と別の ONS ノードの間にある、OSI プロトコル スタックを使用するサードパーティ製の NE が同じネットワーク上にある場合、LDCC は PPP を使用します。



(注) OSI 専用 (LAP-D) は、LDCC では使用できません。

**ステップ 8** OSI ボックスがオンの場合は、次のステップを実行します。IP ボックスのみをオンにした場合は、[ステップ 9](#)に進みます。

- a. Next をクリックします。
- b. 次のフィールドをプロビジョニングします。
  - Router — OSI ルータを選択します。
  - ESH — 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 — 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 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。
  - Metric — 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メトリックコストは 20 です。通常は、この値は変更しないでください。

**ステップ 9** Finish をクリックします。



(注) すべてのネットワーク DCC 終端を作成してその OC-N ポートを稼働させるまでは、EOC-L (LDCC 終端エラー) アラームと LOS アラームが表示され続けます。

**ステップ 10** 元の NTP (手順) に戻ります。

## DLP-A379 OC-N カードの回線の伝送設定の変更

目的	この作業では、OC-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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、回線の設定を変更する OC-N カードをダブルクリックします。

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



**(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 3** 変更するフィールドをクリックして、表 20-8 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。

**ステップ 4** Apply をクリックします。

表 20-8 OC-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	<ul style="list-style-type: none"> <li>• 1 (OC-12、OC-48、OC-192)</li> <li>• 1 ~ 4 (OC-3、OC12-4)</li> <li>• 1 ~ 8 (OC3-8)</li> <li>• 1 ~ 12 (MRC_12)</li> </ul>
Port Name	指定したポートに名前を割り当てます。	<p>ユーザ定義。32 文字以下の英数字または特殊文字で名前を指定します。デフォルトはブランクです。</p> <p>「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。</p>
Port Rate	(表示専用)(MRC-12 および OC192-XFP カードのみ)Pluggable Port Module (PPM) に設定されたポート レート セットを表示します。	<ul style="list-style-type: none"> <li>• OC-3</li> <li>• OC-12</li> <li>• OC-48</li> <li>• OC-192 (OC192-XFP のみ)</li> </ul>
SF BER	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビット エラー レートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
BLSR Ext. Byte	BLSR 保護切り替えを管理する情報を伝送する拡張バイトを再マップできます。サードパーティ製の機器経由で ONS BLSR を運用する必要がない場合は、K3 バイトを変更しないでください。	<ul style="list-style-type: none"> <li>• N/A</li> <li>• K3</li> </ul>

表 20-8 OC-N カードの回線設定 (続き)

パラメータ	内容	オプション
Provides Synchron	(表示専用) オンにすると、そのカードが NE のタイミング基準としてプロビジョニングされます。	—
SyncMsgIn	SSM (S1 バイト) を有効にして、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。	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Send Do Not Use	オンにすると、DUS メッセージが S1 バイトで送信されます。	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
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。	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Admin SSM In	ノードが SSM 信号を受信しない場合、デフォルトの STU に戻ります。Admin SSM In によって、STU 値を無効にすることができます。	<ul style="list-style-type: none"> <li>• PRS: Primary Reference Source( Stratum 1 )</li> <li>• ST2 : Stratum 2</li> <li>• TNC : Transit Node Clock</li> <li>• ST3E : Stratum 3E</li> <li>• ST3 : Stratum 3</li> <li>• SMC : SONET Minimum Clock</li> <li>• ST4 : Stratum 4</li> </ul>
PJSTSMon #	ポインタの位置調整に使用される STS を設定します。ゼロに設定すると、STS はモニタされません。各 OC-N ポートでモニタできる STS は 1 つだけです。	<ul style="list-style-type: none"> <li>• 0 ~ 3 ( OC-3、ポート単位 )</li> <li>• 0 ~ 12 ( OC-12 )</li> <li>• 0 ~ 48 ( OC-48 )</li> <li>• 0 ~ 192 ( OC-192 )</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>



表 20-8 OC-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) 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。	<ul style="list-style-type: none"> <li>IS-NR — 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。</li> <li>OOS-AU,AINS — 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。</li> <li>OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>
Type	ポートを SONET または SDH として定義します。ポートを SDH に設定する前に、Enable Sync Msg フィールドと Send Do Not Use フィールドをディセーブルにする必要があります。	<ul style="list-style-type: none"> <li>Sonet</li> <li>SDH</li> </ul>
ALS Mode	自動レーザー シャットダウン機能を設定します。	<ul style="list-style-type: none"> <li>Disabled</li> <li>Auto Restart</li> <li>Manual Restart</li> <li>Manual Restart for Test</li> </ul>
Reach	(一部のカードでは適用外) 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 到達範囲から自動的に到達範囲をプロビジョニングすることもできます。	<p>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。</p> <ul style="list-style-type: none"> <li>SR (短距離、最大 2 km)</li> <li>SR-1 (最大 2 km)</li> <li>IR-1 (中距離、最大 15 km)</li> <li>IR-2 (最大 40 km)</li> <li>LR-1 (長距離、最大 40 km)</li> <li>LR-2 (最大 80 km)</li> <li>LR-3 (最大 80 km)</li> </ul>

表 20-8 OC-N カードの回線設定 (続き)

パラメータ	内容	オプション
Wavelength	(一部のカードでは適用外) 波長周波数をプロビジョニングできます。	<ul style="list-style-type: none"> <li>• First Tunable Wavelength</li> <li>• 1310 nm</li> <li>• 1550 nm</li> <li>• 1470 nm</li> <li>• 1490 nm</li> <li>• 1510 nm</li> <li>• 1530 nm</li> <li>• 1570 nm</li> <li>• 1590 nm</li> <li>• 1610 nm</li> </ul>

**ステップ 5** 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-A380 プロキシ トンネルのプロビジョニング

目的	この作業では、遠端側の非 ONS ノードと通信するためにプロキシ トンネルを設定します。プロキシ トンネルが必要となるのは、プロキシ サーバがイネーブルになっていて外部に DCC の終端がある場合、あるいは、スタティック ルートが存在してリモートのネットワークまたはデバイスにアクセスするために DCC ネットワークを使用する場合だけです。プロビジョニングできるプロキシ サーバ トンネルの最大数は、12 個です。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A377 SDCC 終端のプロビジョニング (p.20-74)</a>
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) プロキシ サーバがディセーブルになっているとプロキシ トンネルは設定できません。

**ステップ 1** Provisioning > Network > Proxy サブ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 Tunnel ダイアログボックスで次の情報を入力します。

- Source Address — 送信元ノードの IP アドレス (32 ビット長) または送信元サブネットの IP アドレス (それ以外の長さ) を入力します。
- Length — 送信元サブネット マスクの長さを選択します。
- Destination Address — 宛先ノードの IP アドレス (32 ビット長) または宛先サブネットの IP アドレス (それ以外の長さ) を入力します。
- Length — 宛先サブネット マスクの長さを選択します。

**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-A381 ファイアウォール トンネルのプロビジョニング

目的	この作業では、ファイアウォールでブロックされない宛先をプロビジョニングします。ファイアウォール トンネルが必要となるのは、プロキシ サーバがイネーブルになっていて外部に DCC の終端がある場合、あるいは、スタティック ルートが存在していてリモートのネットワークまたはデバイスにアクセスするために DCC ネットワークを使用する場合だけです。プロビジョニングできるファイアウォール トンネルの最大数は、12 個です。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A377 SDCC 終端のプロビジョニング (p.20-74)</a>
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)** プロキシ サーバがプロキシ専用として設定されているかディセーブルになっていると、ファイアウォール トンネルは設定できません。

**ステップ 1** Provisioning > Network > Firewall サブ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 Tunnel ダイアログボックスで次の情報を入力します。

- Source Address — 送信元ノードの IP アドレス (32 ビット長) または送信元サブネットの IP アドレス (それ以外の長さ) を入力します。
- Length — 送信元サブネット マスクの長さを選択します。
- Destination Address — 宛先ノードの IP アドレス (32 ビット長) または宛先サブネットの IP アドレス (それ以外の長さ) を入力します。
- Length — 宛先サブネット マスクの長さを選択します。

## ■ DLP-A382 プロキシ トンネルの削除

**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-A382 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Provisioning > Network > Proxy サブ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) に戻ります。

## DLP-A383 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Provisioning > Network > Firewall サブ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-A384 VCAT 回線へのメンバーの追加

目的	<p>この作業では、次のいずれかの VCAT 回線にメンバーを追加します。</p> <ul style="list-style-type: none"> <li>FC_MR-4 (拡張モード) または CE-1000-4 カードの Software Link Capacity Adjustment Scheme (SW-LCAS) VCAT 回線</li> <li>CE-100T-8 カードの非 LCAS および LCAS 回線</li> </ul> <p>VCAT 回線にメンバーを追加すると、回線のサイズが変わります。新しく追加したメンバーでは、VCAT 回線の作成手順で指定した VCAT メンバーの送信元、宛先、およびルーティング プリファレンス (共通光ファイバまたはスプリット ルーティング) を使用します。</p>
工具 / 機器 事前準備手順	<p>FC_MR-4 カード (拡張モード) または CE シリーズ カード</p> <p><a href="#">DLP-A60 CTC へのログイン (p.17-71)</a></p> <p>ネットワークに VCAT 回線が存在している必要があります。  <a href="#">「NTP-A264 自動ルーティングによる VCAT 回線の作成」(p.6-99)</a> または <a href="#">「NTP-A265 手動ルーティングによる VCAT 回線の作成」(p.6-104)</a> を参照してください。</p>
必須 / 適宜 オンサイト / リモート セキュリティ レベル	<p>適宜</p> <p>オンサイトまたはリモート</p> <p>プロビジョニング以上のレベル</p>



**(注)** この作業では、任意で自動ルーティングを使用します。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『Cisco ONS 15454 Reference Manual』の付録「Network Element Defaults」を参照してください。



**(注)** 非 LCAS VCAT 回線にメンバーを追加すると、サービスに影響する場合があります。



**(注)** サービス状態が IS-NR、OOS-AU,AINS、または OOS-MA,MT にある SW-LCAS または LCAS VCAT 回線にメンバーを追加すると、サービスに影響することがあります。サービス状態が OOS-MA,OOG のときにメンバーを追加することを推奨します。追加したメンバーは、追加したあとで希望する状態に設定できます。



**(注)** ML シリーズ カード または FC\_MR-4 カード (回線速度モード) に送信元または宛先のある VCAT 回線には、メンバーを追加できません。

**ステップ 1** ネットワーク ビューで、Circuits タブをクリックします。

**ステップ 2** 編集する VCAT 回線をクリックして、Edit をクリックします。

**ステップ 3** Members タブをクリックします。

**ステップ 4** 非 LCAS VCAT 回線にメンバーを追加する場合、次のサブステップを実行します。SW-LCAS または LCAS VCAT 回線にメンバーを追加する場合は、このステップを省略して **ステップ 5** に進みません。

- a. In Group 状態の VCAT メンバーを選択します。In Group 状態は、メンバーのクロスコネク트가 IS-NR、OOS-MA,AINS、または OOS-MA,MT サービス状態であることを示します。
- b. **Edit Member** をクリックします。
- c. Edit Member Circuit ウィンドウで、**State** タブをクリックします。
- d. CRS Service State カラムでクロスコネク트의 サービス状態を表示します。新規のメンバーの状態を選択する場合に、この情報が必要になります。

In Group で非 LCAS のメンバーのクロスコネク트는、すべて同一のサービス状態にある必要があります。既存のすべての VCAT メンバーが Out of Group 状態の場合（非 LCAS メンバーが OOS-MA,DSBLD サービス状態）、新規のメンバーに対して任意のサービス状態を選択できます。

- e. File メニューから **Close** を選択して、Edit Circuit ウィンドウに戻ります。

**ステップ 5** **Add Member** をクリックします。Add Member ボタンは、VCAT 回線に新規メンバーのための帯域幅が十分にあるときにだけ、クリックできるようになります。

**ステップ 6** メンバーの数とメンバーのアトリビュートを指定します。

- Number of members to add — ドロップダウン リストから、追加するメンバーの数を選択します。ドロップダウン リストに数が表示されないときは、VCAT 回線に許容最大数のメンバーが設定済みで追加できるだけの余地がありません。許容メンバー数は、送信元カード、宛先カード、および既存回線のサイズによって異なります。カードに対する許容メンバー数の詳細については、『Cisco ONS 15454 Reference Manual』にある「Circuits and Tunnels」の章を参照してください。
- New Circuit Size — (表示専用) 追加されたメンバーの数に応じて、自動的に更新されます。
- Create cross-connects only( TL1-like) — 1 つまたは複数のクロスコネクートを TL1 生成済み回線に対する信号パスの一部として作成する必要がある場合は、このボックスをオンにします。このボックスがオンの場合は、回線に名前を割り当てできません。
- State — In Group の VCAT メンバーに非 LCAS メンバーを追加するには、**ステップ 4** で表示した状態を選択します。Out of Group の VCAT メンバーのみに非 LCAS メンバーを追加するには、次のいずれかの状態を選択します。SW-LCAS または LCAS メンバーを追加する場合、OOS,OOG 状態を推奨します。
  - IS — メンバーのクロスコネクートのサービス状態を IS-NR にします。
  - OOS,DSBLD — メンバーのクロスコネクートのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通してできません。
  - IS,AINS — メンバーのクロスコネクートのサービス状態を OOS-AU,AINS にして、アラームと状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。
  - OOS,MT — メンバーのクロスコネクートのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィックの流れが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。「DLP-A437 VCAT メンバーのサービス状態の変更」(p.21-16) を参照してください。
  - OOS,OOG — (LCAS および SW-LCAS VCAT 回線のみ) VCAT メンバーのクロスコネクートを Out-of-Service and Management, Out-of-Group( OOS-MA,OOG )サービス状態にします。この管理ステータスは、メンバー回線をグループから外したり、トラフィックの送信を止めたりする場合に使用します。

回線の詳細なサービス状態については、『Cisco ONS 15454 Reference Manual』の「Circuits and Tunnels」の章を参照してください。

**ステップ 7** Next をクリックします。

**ステップ 8** メンバーを自動的にルーティングする場合は、**Route Automatically** をオンにします。メンバーを手動でルーティングする場合は、Route Automatically をオフのままにします。

**ステップ 9** メンバーごとにプリファレンスを設定する場合は、Member Preferences 領域で次の項目を指定します。追加したすべてのメンバーに同じプリファレンスを設定する場合は、このステップを省略して **ステップ 10** から続けます。



**(注)** 共通ファイバまたはスプリット ルーティングは変更できません。

- Number — メンバーを識別するための数値 (1 ~ 256) をドロップダウン リストを選択します。
- Name — メンバーを識別するための一意な名前を入力します。名前には、48 文字 (スペースを含む) 以下の英数字を指定します。このフィールドを空白のままにしておくと、CTC によってデフォルトの名前が回線に割り当てられます。
- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — メンバーを BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリット ルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリット ルーティングのみ) Fully Protected が選択されている場合に、各メンバーが利用できます。

**ステップ 10** すべてのメンバーに同じプリファレンスを設定する場合は、Set Preferences for All Members 領域で次の選択を行います。

- Protection — メンバー保護タイプを選択します。
  - Fully Protected — 保護されたパスに回線をルーティングします。
  - Unprotected — 保護されていない回線を作成します。
  - PCA — メンバーを BLSR の保護チャンネルにルーティングします。
  - DRI — (スプリット ルーティングのみ) メンバーを DRI 回線にルーティングします。
- Node-Diverse Path — (スプリット ルーティングのみ) Fully Protected が選択されている場合に、利用できます。

**ステップ 11** **ステップ 8** で Route Automatically をオフのままにした場合は、Next をクリックして、次の手順を実行します。 **ステップ 8** で Route Automatically をオンにした場合は、 **ステップ 12** から続けます。

- a. Circuit Creation ウィザードの Route Review/Edit 領域にある Route Member number ドロップダウン リストから、ルーティングするメンバーを選択します。
- b. 送信元ノードアイコンが選択されていない場合は、このアイコンをクリックします。
- c. 送信元ノードにあるスパンから開始して、メンバーを通過させるスパンの矢印をクリックしていきます。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。
- d. 送信元を変更する場合は、Source STS フィールドを変更します。変更しない場合は、ステップ e へ進みます。

- e. **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。
- f. 送信元ノードから宛先ノードまで、すべての中継ノードも含めてメンバーを設定し終わるまで、ステップ c ~ e を繰り返します。Fully Protect Path を選択した場合は、次の設定を行う必要があります。
  - すべての UPSR リング、または送信元から宛先までのメンバー 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。
  - 送信元から宛先までのルートにあるすべての BLSR または 1+1 部分に対しては、1 つのスパンを追加します。
  - UPSR DRI トポロジーにルーティングするメンバーについては、DRI ノード間のスパンと同様に、現用パスと保護パスをプロビジョニングします。
- g. 各メンバーについてステップ a ~ f を繰り返します。

**ステップ 12** ステップ 8 で Route Automatically と Review Route Before Creation をオンにした場合は、次のサブステップを実行します。それ以外の場合は、ステップ 13 へ進みます。

- a. **Next** をクリックします。
- b. 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include** をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- c. プロビジョニングした回線が予定のルートと設定を反映していない場合は **Back** をクリックし、回線の情報を確認して変更します。

**ステップ 13** **Finish** をクリックします。



**(注)** VCAT 回線にメンバーを追加する処理は、ネットワークの複雑さと追加するメンバーの数によっては、数分かかることがあります。

**ステップ 14** LCAS メンバーを追加した場合、次のサブステップを実行します。

- a. Alarms タブをクリックして、VCAT Group Degraded ( VCG-DEG ) アラームが表示されるかを確認します。表示される場合は、アラームをクリアする手順について、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。表示されない場合は、ステップ b に進みます。
- b. 「DLP-A437 VCAT メンバーのサービス状態の変更」(p.21-16)を実行して、メンバーを IS サービス状態にします。

**ステップ 15** 元の NTP (手順) に戻ります。



## DLP-A385 VCAT 回線からのメンバーの削除

目的	この作業では、次のいずれかの条件で作成された VCAT 回線からメンバーを削除します。 <ul style="list-style-type: none"> <li>FC_MR-4 (拡張モード) または CE-1000-4 カードの SW-LCAS VCAT 回線</li> <li>CE-100T-8 カードの非 LCAS および LCAS 回線</li> </ul> この作業を行うと、VCAT 回線のサイズが小さくなります。
工具 / 機器 事前準備手順	FC_MR-4 カード (拡張モード) または CE シリーズ カード <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>  ネットワークに VCAT 回線が存在している必要があります。 <a href="#">「NTP-A264 自動ルーティングによる VCAT 回線の作成」(p.6-99)</a> または <a href="#">「NTP-A265 手動ルーティングによる VCAT 回線の作成」(p.6-104)</a> を参照してください。  必要に応じて <a href="#">「DLP-A437 VCAT メンバーのサービス状態の変更」(p.21-16)</a> を実行して、SW-LCAS または LCAS メンバーの状態を OOS-MA,OOG に変更します。
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) 非 LCAS 回線からメンバーを削除すると、サービスに影響する場合があります。



(注) IS-NR または OOS-AU,AINS サービス状態の SW-LCAS または LCAS メンバーを削除すると、サービスに影響する場合があります。サービスの状態を OOS-MA,OOG の状態にしてからメンバーを削除することを推奨します。非 LCAS メンバーは、OOS-MA,OOG のサービス状態をサポートしていません。



(注) ML シリーズ カード または FC\_MR-4 カード (回線速度モード) に送信元または宛先があるメンバーは削除できません。

- 
- ステップ 1** ネットワーク ビューで、Circuits タブをクリックします。
  - ステップ 2** 編集する VCAT 回線をクリックして、Edit をクリックします。
  - ステップ 3** Members タブをクリックします。
  - ステップ 4** 削除するメンバーを選択します。複数のメンバーを選択する場合は、Ctrl キーを押して、クリックします。
  - ステップ 5** Delete Member をクリックします。

## ■ DLP-A386 UBIC-V EIA での電気回路ケーブルの取り付け

**ステップ 6** 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 7** 元の NTP (手順) に戻ります。

## DLP-A386 UBIC-V EIA での電気回路ケーブルの取り付け

目的	この作業では、UBIC-V EIA に DS-1 および DS-3/EC-1 ケーブルを取り付けます。
工具 / 機器	3/16 インチ フラットヘッド ドライバ DS-1 および DS-3/EC-1 ケーブル (必要に応じて) <ul style="list-style-type: none"> <li>• DS-1 ケーブル、150 フィート : 15454-CADS1-SD</li> <li>• DS-1 ケーブル、250 フィート : 15454-CADS1-ID</li> <li>• DS-1 ケーブル、655 フィート : 15454-CADS1-LD</li> <li>• DS-3/EC-1 ケーブル、75 フィート : 15454-CADS3-SD</li> <li>• DS-3/EC-1 ケーブル、225 フィート : 15454-CADS3-ID</li> <li>• DS-3/EC-1 ケーブル、450 フィート : 15454-CADS3-LD</li> </ul>
事前準備手順	<a href="#">DLP-A190 UBIC-V EIA の取り付け (p.18-60)</a>
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



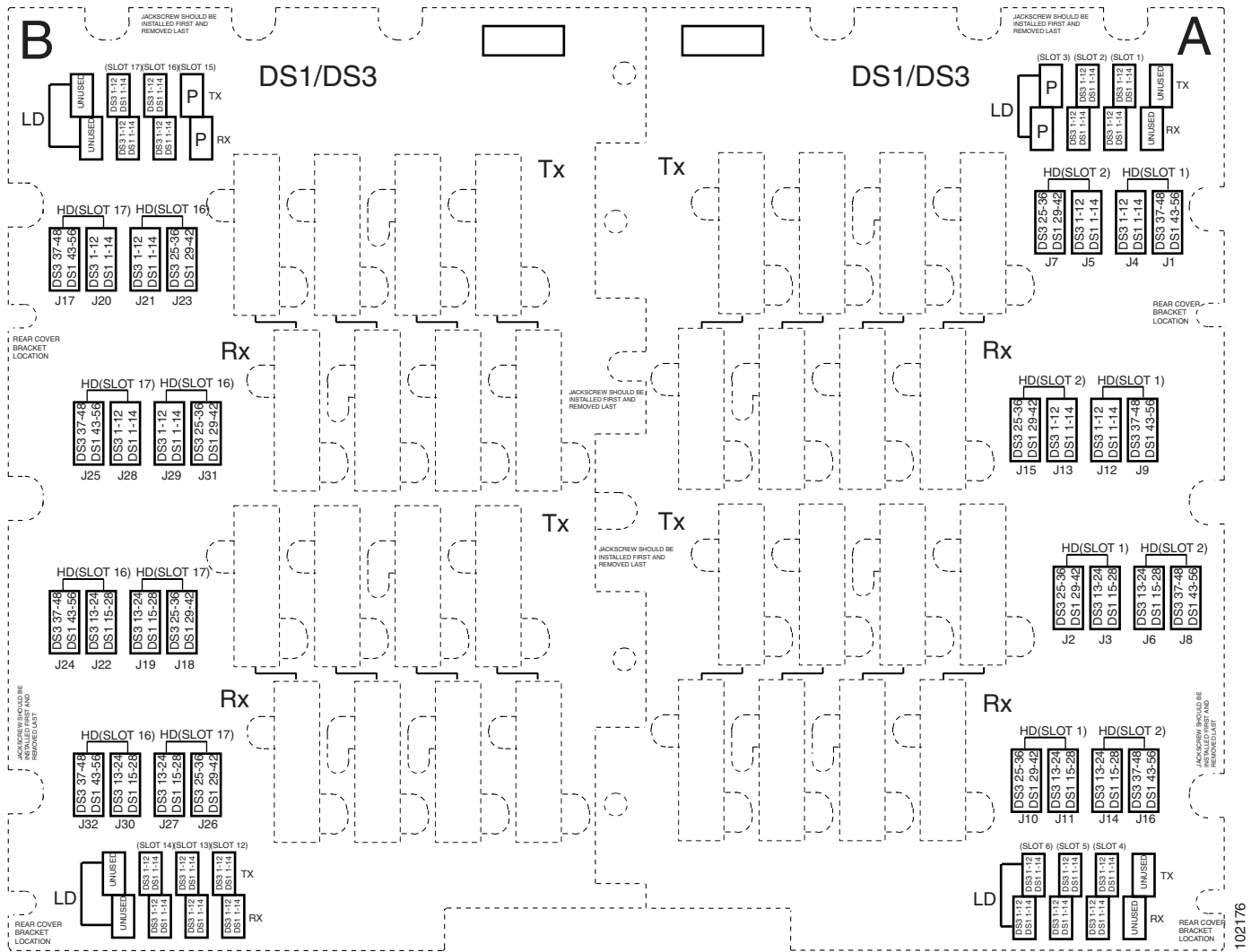
(注)

今後のスロットの使用状況を考慮して、今後使用するすべての SCSI コネクタをケーブル接続することを推奨します。

**ステップ 1** UBIC-V にケーブルを取り付ける一番下の列から開始して、UBIC-V EIA の適切な接続ポイントにケーブル コネクタを配置します。

[図 20-14](#) に、UBIC-V のスロット指定を示します。

図 20-14 UBIC-V のスロット指定



**ステップ 2** ケーブル コネクタのガイド スロットを UBIC コネクタのガイド スタンドオフに合わせた状態で、慎重にケーブルを取り付けます。

**ステップ 3** フラットヘッド ドライバを使用して、ケーブル コネクタの左上部で、8 ~ 10 lbf-inch (9.2 ~ 11.5 kgf-cm) でネジを締めます。コネクタの右下部のネジに対しても、同じことを繰り返します。両方がぴったりと固定されるまで、2 本のネジを交互に締めます。

**ステップ 4** 下の列から上の列に移動しながら、取り付ける各ケーブルに対してステップ 1 ~ 3 を繰り返します。すでに取り付けしたケーブルの近くにケーブルを取り付ける場合は、周辺のケーブルを軽く後方に押さえておいてください。各ケーブルはペア (Tx と Rx) で取り付けるようにしてください。

図 20-15 に、すべてのコネクタにケーブルが取り付けられた UBIC-V を示します。

図 20-15 すべてのケーブルが接続された UBIC-V (前面図と側面図)

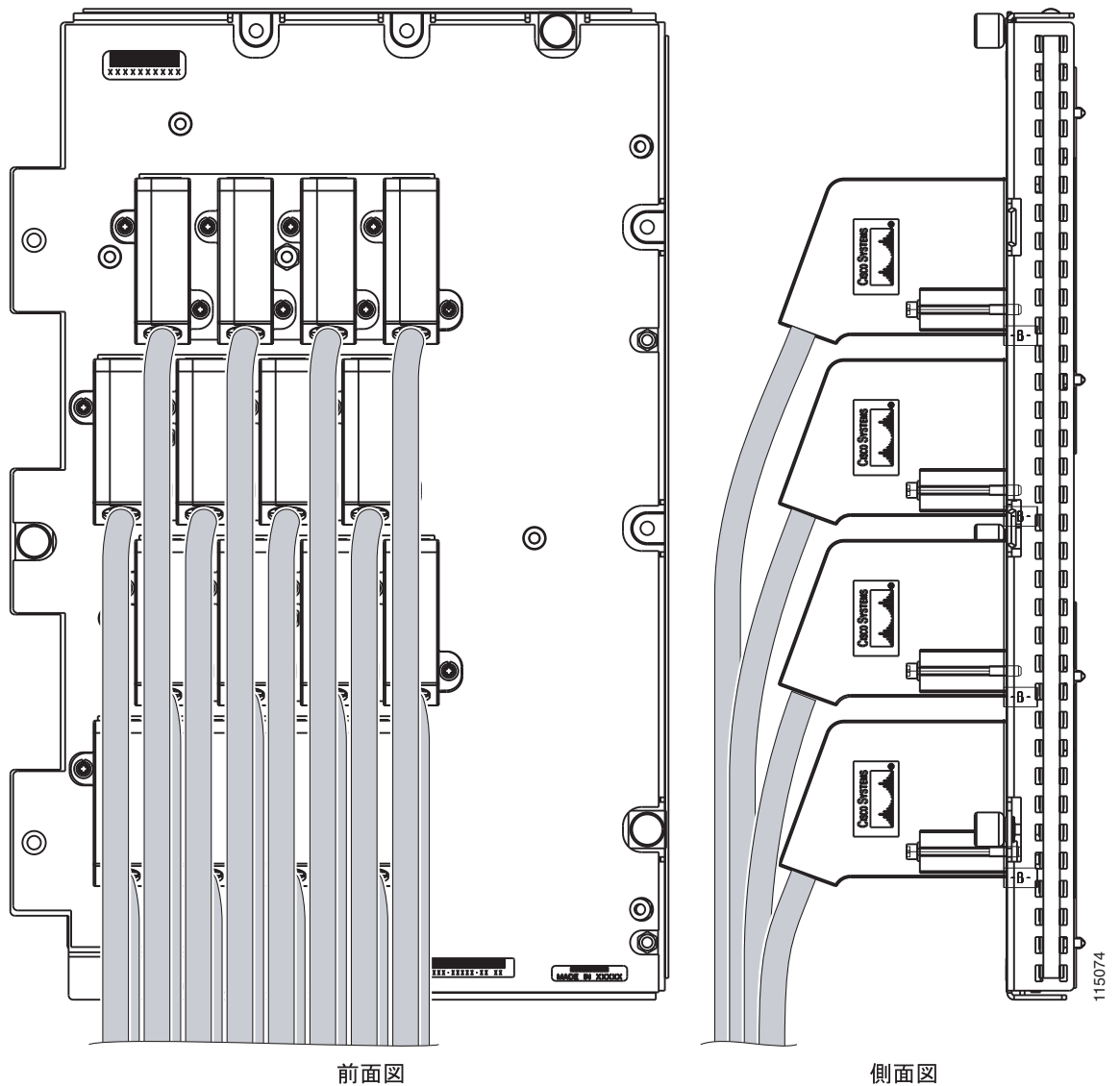
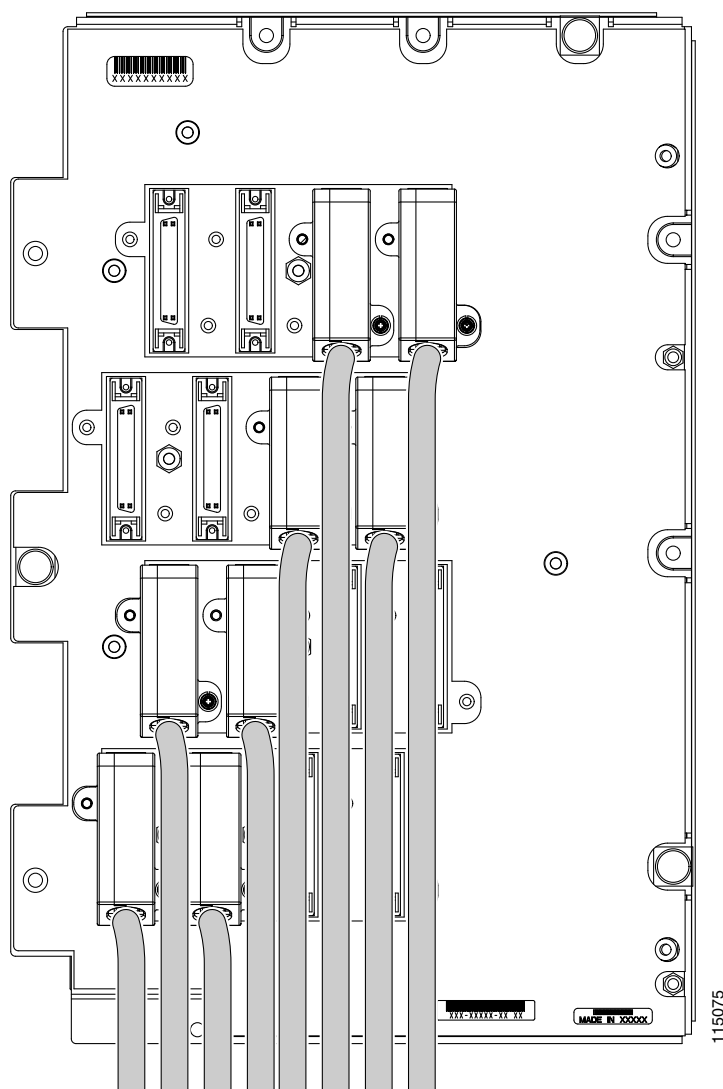


図 20-16 に、部分的に接続された UBIC-V を示します。

図 20-16 部分的にケーブル接続された UBIC-V



**ステップ 5** 可能な場合は、Telcordia 標準 (GR-1275-CORE) または現地の状況に合わせて、ケーブルを固定棒にタイラップするか撚り合わせます。



**(注)** 電気回路ケーブルを配線するには、アラームおよびタイミング パネルの前に十分なスペースを空け、メンテナンス時に手が届くようにします。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A387 DS3XM-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、DS3XM-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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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)** DS3XM-12 (トランスマックス) カードは、最大 12 のチャネライズド DS-3 信号を受け入れ、各信号を 28 の VT1.5 信号に変換できます (合計 336 の VT1.5 変換)。反対に、カードは 12 の各 DS-3 ポートについて 28 の VT1.5 をチャネライズド C ビットまたは M13 フレームド DS-3 信号に多重化できます。



**(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 DS3XM-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、DS1、Line Thresholds、Elect Path Thresholds、または SONET Thresholds 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。

**ステップ 7** 回線設定の定義については、表 20-9 を参照してください。DS1 設定の定義については、表 20-10 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 20-11 を参照してください。電気回路バス スレッシュホールドの設定の定義については、表 20-12 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 20-13 を参照してください。

表 20-9 に、DS3XM-12 カードに対する Provisioning > Line タブの値を示します。

**表 20-9 DS3XM-12 パラメータの回線オプション**

パラメータ	内容	オプション
Port #	(表示専用) ポート番号	1 ~ 36
Port Name	ポート名を表示します。	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	SFBER を設定します。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
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。	<ul style="list-style-type: none"> <li>• IS-NR — 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。</li> <li>• OOS-AU,AINS — 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。</li> <li>• OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>• OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 0 ~ 48 時間、15 分刻み</li> </ul>
SD BER	信号劣化ビット エラー レートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• M13 (デフォルト)</li> <li>• C BIT</li> </ul>

表 20-9 DS3XM-12 パラメータの回線オプション (続き)

パラメータ	内容	オプション
Line Coding	使用される DS-1 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。	<ul style="list-style-type: none"> <li>0 ~ 225 (デフォルト)</li> <li>226 ~ 450</li> </ul>
Admin State	ポートの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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>

表 20-10 に、DS3XM-12 カードに対する Provisioning > DS1 タブの値を示します。DS3XM-12 カードの「ポートレス」保護に関する詳細については、『Cisco ONS 15454 Reference Manual』を参照してください。

表 20-10 DS3XM-12 カードの DS1 オプション

パラメータ	内容	オプション
Port	(表示のみ) DS-3 および対応する DS-1 のポート番号を表示します。	DS-3 : 1 ~ 35 DS-1 : 1 ~ 28
Port Name	ポート名を表示します。	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。
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。	<ul style="list-style-type: none"> <li>IS-NR — 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。</li> <li>OOS-AU,AINS — 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。</li> <li>OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>



表 20-10 DS3XM-12 カードの DS1 オプション (続き)

パラメータ	内容	オプション
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>AUTO FRAME</li> <li>ESF - Extended Super Frame( 拡張スーパーフレーム )</li> <li>D4</li> <li>UNFRAMED</li> </ul>
FDL Mode	ポートの Fiber Data Link ( FDL ) モードを定義します。	<ul style="list-style-type: none"> <li>T1.403</li> <li>BFDL - Bidirectional FDL</li> </ul>

表 20-11 に、DS3XM-12 カードの回線スレッシュホールドのオプションを示します。

表 20-11 DS3XM-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	( 表示のみ ) DS-3 および対応する DS-1 のポート番号を表示します。 DS-3 : 1 ~ 35 DS-1 : 1 ~ 28
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
LOSS	LOS 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。

表 20-12 に、DS3XM-12 カードに対する Provisioning > Elect Path Thresholds タブの値を示します。

表 20-12 DS3XM-12 カードの電気回路バス 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 ~ 36 )
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
SAS	重大エラー フレーム / アラーム表示信号
AISS	AIS 秒数
UAS	使用不可秒数
FC	障害カウント ( STS でのみ利用可能 )
CSS	制御スリップ秒数
ESA	エラー秒数 ( タイプ A )
ESB	エラー秒数 ( タイプ B )
SEFS	重大エラー フレーム秒数
ESNE	エラー秒数 ( 近端 )
ESFE	エラー秒数 ( 遠端 )

表 20-12 DS3XM-12 カードの電気回路バス スレッシュホールド オプション (続き)

パラメータ	内容
SESNE	重大エラー秒数 (近端)
SESFE	重大エラー秒数 (遠端)
UASNE	使用不可秒数 (近端)
UASFE	使用不可秒数 (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 20-13 に、DS3XM-12 カードに対する Provisioning > SONET Thresholds タブの値を示します。

表 20-13 DS3XM-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
CV	符号化違反数
ES	エラー秒数
FC	障害カウント
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値は、回線が作成されたあとで表示されます。

**ステップ 8** 元の NTP (手順) に戻ります。

## DLP-A388 DS3/EC1-48 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、DS3/EC1-48 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 回線またはスレッシュホールドの設定変更を行う DS3/EC1-48 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 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 20-14 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 20-15 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 20-16 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 20-17 を参照してください。

表 20-14 DS3/EC1-48 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 ~ 48
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。
Admin State	ポートの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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>

表 20-14 DS3/EC1-48 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
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。	<ul style="list-style-type: none"> <li>IS-NR — 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。</li> <li>OOS-AU,AINS — 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。</li> <li>OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>
SF BER	SFBER を設定します。	<ul style="list-style-type: none"> <li>1E-3</li> <li>1E-4</li> <li>1E-5</li> </ul>
SD BER	信号劣化ビット エラー レートを設定します。	<ul style="list-style-type: none"> <li>1E-5</li> <li>1E-6</li> <li>1E-7</li> <li>1E-8</li> <li>1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>Unframed (デフォルト)</li> <li>M13</li> <li>C BIT</li> <li>Auto Provision Fmt</li> </ul>
Detected Line Type	(表示専用) 検出された回線のタイプを表示します。	<ul style="list-style-type: none"> <li>M13</li> <li>C Bit</li> <li>Unframed</li> <li>Unknown</li> </ul>
Line Coding	使用される DS-3 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。	<ul style="list-style-type: none"> <li>0 ~ 225 (デフォルト)</li> <li>226 ~ 450</li> </ul>
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。値の範囲は、0 ~ 48 時間、15 分刻みです。

表 20-15 に、DS3/EC1-48 カードに対する Provisioning > Line Thresholds タブの値を示します。

表 20-15 DS3/EC1-48 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 ~ 48)
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
LOSS	LOS 秒数。1 つまたは複数の LOS 障害が発生した 1 秒間の間隔です。
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 20-16 に、DS3/EC1-48 カードに対する Provisioning > Elect Path Thresholds タブの値を示します。

表 20-16 DS3/EC1-48 カードの電気回路バス 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 ~ 48)
CV	符号化違反数
ES	エラー秒数
SES	重大エラー秒数
SAS	重大エラー フレーム /AIS
AISS	AIS 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。

表 20-17 に、DS3/EC1-48 カードに対する Provisioning > SONET Thresholds タブの値を示します。

表 20-17 DS3/EC1-48 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) STS に対して分割されている DS-3 ポート Line 1, STS 1、Line 2, STS 1 Line 3, STS 1、Line 4, STS 1
CV	符号化違反数。近端および遠端で利用可能、STS 終端専用。
ES	エラー秒数。近端および遠端で利用可能、STS 終端専用。
FC	障害カウント。近端および遠端で利用可能、STS 終端専用。
SES	重大エラー秒数。近端および遠端で利用可能、STS 終端専用。
UAS	使用不可秒数。近端および遠端で利用可能、STS 終端専用。

表 20-17 DS3/EC1-48 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
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値は、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-A390 アラームの表示

目的	この作業では、カード、ノード、またはネットワークに存在する現在のアラームを表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** 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** タブをクリックして、そのカード、ノード、またはネットワークのアラームを表示します。

表 20-18 アラーム カラムの説明

カラム	記録情報
Num	元のアラームのシーケンス番号
Ref	元のアラームの参照番号
New	新しいアラームを示します。このステータスを変更するには、Synchronize ボタンまたは Delete Cleared Alarms ボタンをクリックします。
Date	アラームの日時
Node	アラームの発生しているノードの名前 (Dense Wavelength Division Multiplexing [DWDM; 高密度波長分割多重] 設定では、1 つのノードに複数のシェルフを含むことができます)。ネットワーク ビューに表示されます。
Object	アラームが報告されたオブジェクトの TL1 Access Identifier (AID)、STSmon または VTmon の場合、この情報はモニタ対象の STS または VT です。
Eqpt Type	カードでアラームが発生した場合に、このスロットのカード タイプを示します。
Slot	カードでアラームが発生した場合に、アラームが発生したスロットを示します (ネットワーク ビューおよびノードビューでのみ表示)。
Port	カードでアラームが発生した場合に、アラームが発生したポートを示します。STSTerm および VTTerm の場合は、このポートと組になるアップストリーム カードを意味します。

表 20-18 アラーム カラムの説明（続き）

カラム	記録情報
Path Width	アラームが報告されたパスに含まれている STS の数を表します。この情報は、アラーム オブジェクト表記の一部になっています (『Cisco ONS 15454 Troubleshooting Guide』参照)
Sev	重大度：CR (Critical) MJ (Major) MN (Minor) NA (Not Alarmed) NR (NotReported)
ST	ステータス：R (発生) C (クリア) または T (一時的)
SA	オンになっている場合は、サービスに影響するアラームがあります。
Cond	エラー メッセージ / アラーム名。これらの名前は、『Cisco ONS 15454 Troubleshooting Guide』でアルファベット順に定義されています。
Description	アラームの説明
Shelf	DWDM 設定の場合、アラーム発生オブジェクトのあるシェルフです。ネットワーク ビューに表示されます。

表 20-19 に、アラームおよび状態の重大度に関する色分けを示します。

表 20-19 アラームおよび状態の重大度に関する色分け

色	内容
レッド	Critical (CR) アラームが発生
オレンジ	Major (MJ) アラームが発生
イエロー	Minor (MN) アラームが発生
マゼンタ (ピンク)	Not Alarmed (NA) 状態が発生
ブルー	Not Reported (NR) 状態が発生
ホワイト	クリア済み (C) のアラームまたは状態

**ステップ 2** アラームが存在する場合は、『Cisco ONS 15454 Troubleshooting Guide』に記載されている説明とトラブルシューティングの手順を参照してください。

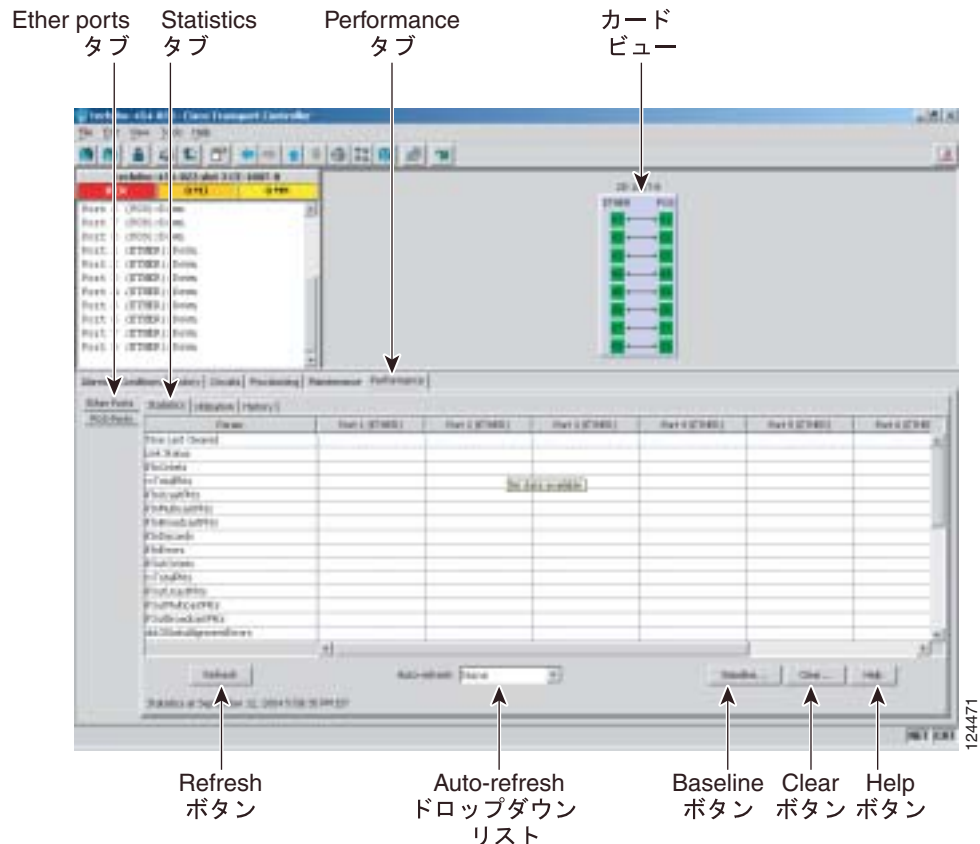
**ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A391 CE シリーズ PM パラメータの表示：イーサネット ポートおよび POS ポートの統計情報

目的	この作業では、選択したインターバルで CE シリーズ イーサネット ポート統計情報の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 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 20-17) または Performance > POS Ports > Statistics タブをクリックします。

図 20-17 CE シリーズカード ビューの Performance ウィンドウにある Ether Ports の Statistics



- 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。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 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-A253 PM カウントの表示変更](#)」(p.9-2) を参照してください。

- ステップ 5** 元の NTP (手順) に戻ります。



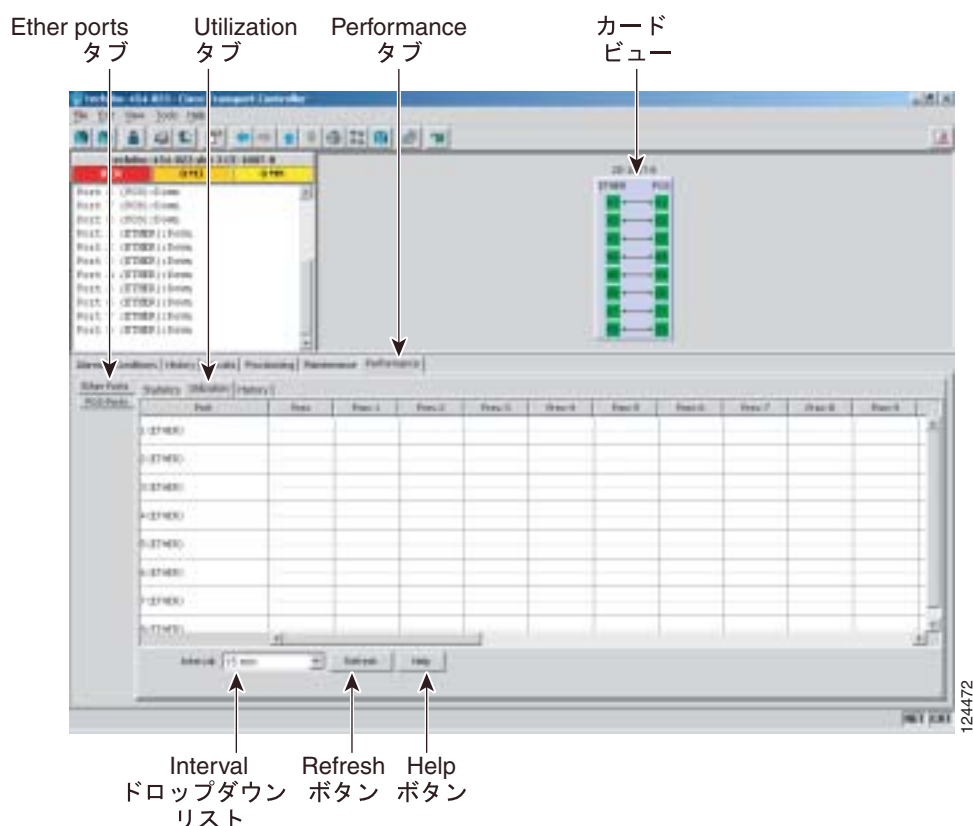
## DLP-A392 CE シリーズ PM パラメータの表示: イーサネット ポートおよび POS ポートの使用率

目的	この作業では、選択したインターバルで CE シリーズ イーサネット ポート使用率の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 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 20-18](#) ) または Performance > POS Ports > Utilization タブをクリックします。

**図 20-18** CE シリーズ カード ビューの Performance ウィンドウにある Ether Ports の Utilization



**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** モニタするポートを見つける場合は、Port # カラムを表示します。

**ステップ 5** これまでのインターバルでの送信 (Tx) および受信 (Rx) の帯域使用率の値が Prev-*n* 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。



(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-A253 PM カウントの表示変更](#)」(p.9-2)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-A393 CE シリーズ PM パラメータの表示:イーサネットポートおよび POS ポートの履歴

目的	この作業では、選択したインターバルで CE シリーズ イーサネットポート履歴の PM カウントを表示します。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	<a href="#">DLP-A60 CTC へのログイン</a> (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 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。


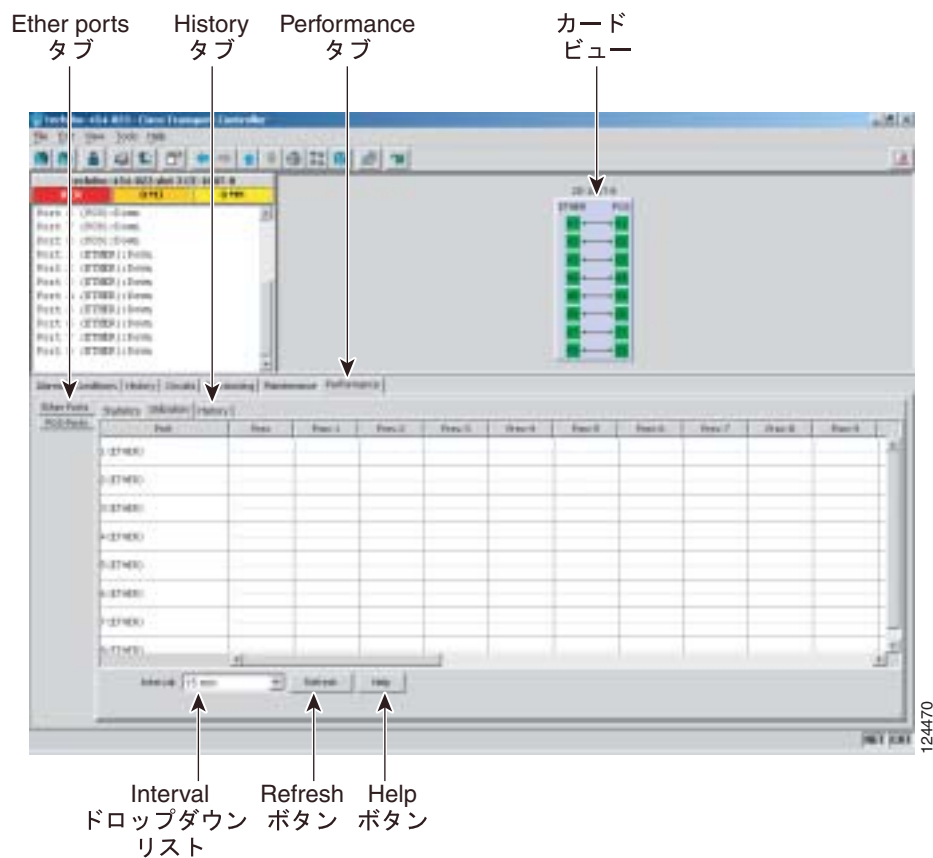
**ステップ 2** Performance > Ether Ports > History タブ (  20-19 ) または Performance > POS Ports > History タブをクリックします。

図 20-19 CE シリーズカードビューの Performance ウィンドウにある Ether Ports の History



**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。Prev-n 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 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-A253 PM カウントの表示変更](#)」(p.9-2) を参照してください。

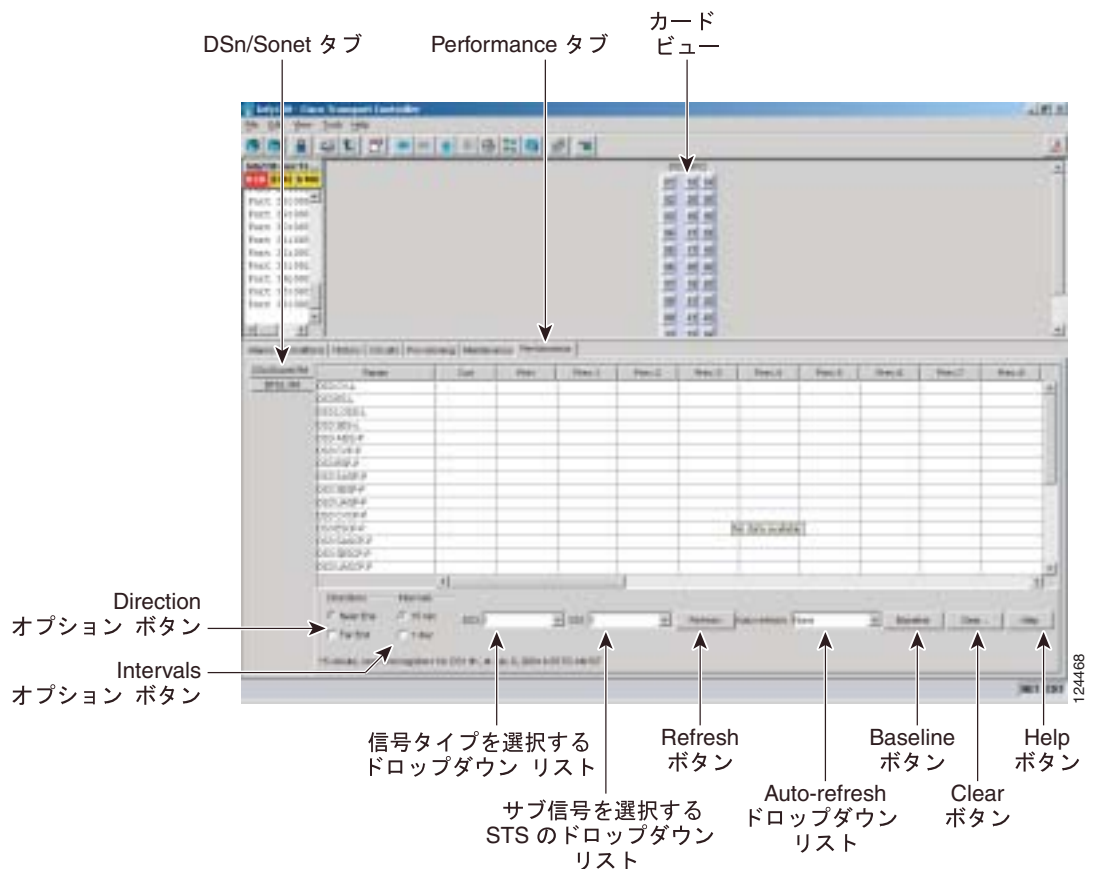
**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A394 DS3XM-12 カード PM パラメータの表示 : DS-N/SONET

目的	この作業では、DS3XM-12 電気回路カードとそのポートについて、指定したインターバルの間の近端または遠端パフォーマンスの DS-N/SONET PM パラメータを表示します。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	パフォーマンスのモニタを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、第 6 章「回線と VT トンネルの作成」と第 10 章「カードの設定変更」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	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 DS3XM-12 電気回路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 > DSn/SONET PM タブをクリックして、DS-N/SONET Performance パラメータを表示します (図 20-20)。

図 20-20 DS3XM-12 カードの DSn/SONET PM 情報の表示





(注) ポートと信号タイプを選択するためのドロップダウン リストは、カードおよび回線のタイプによって異なります。カードに基づいて、対応したタイプ (DS1、DS3、VT パス、STS パス) が表示されます。たとえば、DS3XM カードは信号タイプとして DS3、DS1、VT パス、および STS パスの PM パラメータを表示します。このため、指定された DS-3 内の DS-3 ポートと DS-1 の両方を選択できます。

**ステップ 3** 信号タイプを選択するドロップダウン リストで、指定された DS-3 内の DS-3 ポートと DS-1 ポートを選択します。

**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) カラムと Prev-*n* (過去) の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。



(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-A253 PM カウントの表示変更](#)」(p.9-2) 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-A395 DS3XM-12 カード PM パラメータの表示 : BFDL

目的	この作業では、DS3XM-12 電気回路カードとそのポートについて、指定したインターバルでモニタした近端または遠端の BFDL PM パラメータを表示します。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	パフォーマンスのモニタリングを開始する前に、適切な回線が作成されていることと、カードが仕様どおりにプロビジョニングされていることを確認してください。詳細については、 <a href="#">第 6 章「回線と VT トンネルの作成」</a> と <a href="#">第 10 章「カードの設定変更」</a> 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	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 DS3XM-12 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 > BFDL PM タブをクリックして、BFDL パフォーマンス パラメータ ([図 20-21](#)) を表示します。

図 20-21 DS3XM-12 カードの BFDL PM 情報の表示



(注) ポートと信号タイプを選択するためのドロップダウン リストは、カードおよび回線のタイプによって異なります。カードに基づいて、対応したタイプ (DS1、DS3、VT パス、STS パス) が表示されます。たとえば、DS3XM カードは信号タイプとして DS3、DS1、VT パス、および STS パスの PM パラメータを表示します。このため、指定された DS-3 内の DS-3 ポートと DS-1 の両方を選択できます。

**ステップ 3** Request ドロップダウン リストから、次のいずれかを選択します。

- Enhanced ES One Day
- Enhanced BES One day
- Enhanced SES One Day
- Enhanced UAS One Day
- Enhanced CSS/LOFC One day

**ステップ 4** 信号タイプを選択するドロップダウン リストで、指定された DS-3 内の DS-3 ポートと DS-1 ポートを選択します。

**ステップ 5** Refresh をクリックします。

**ステップ 6** 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) カラムと Prev-n (過去) の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。

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-A253 PM カウントの表示変更](#)」(p.9-2)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-A397 手動ルーティングによる UPSR 回線のトポロジー アップグレード

目的	この作業では、非保護ポイントツーポイントまたはリニア ADM (分岐挿入装置) システムから UPSR への変換中に、手動でルーティングする UPSR 回線を作成します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71) NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換 (p.13-13)
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** Unprotected to UPSR ページの Circuit Routing Preferences 領域で、**Route Automatically** をオフにします。

**ステップ 2** Next をクリックします。Route Review and Edit 領域に、回線を手動でルーティングできるようにノードアイコンが表示されます。回線の送信元ノードは選択されています。送信元ノードから他のネットワーク ノードまでを示す緑色の矢印は、回線のルーティングに使用できるスパンを表しています。

**ステップ 3** Finish をクリックします。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A398 自動ルーティングによる UPSR 回線のトポロジー アップグレード

目的	この作業では、非保護ポイントツーポイントまたはリニア ADM システムから UPSR への変換中に、自動でルーティングする UPSR 回線を作成します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71) NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換 (p.13-13)
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)

この作業には、自動ルーティングを使用する必要があります。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** Unprotected to UPSR ページの Circuit Routing Preferences 領域で、**Route Automatically** をオンにします。

**ステップ 2** 使用できるオプションは 2 つあります。設定に応じて、どちらか一方または両方を選択するか、またはどちらも選択しないようにします。

- Review Route Before Creation — 回線を作成する前にその回線を確認して編集する場合は、このチェックボックスをオンにします。
- VT-DS3 Mapped Conversion — (STS 回線のみ) DS3XM-12 カードのポートレス トランスマルチプレクシング インターフェイスによる回線を作成するには、このチェックボックスをオンにします。

**ステップ 3** 次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバース パスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 4** **ステップ 2** で VT-DS3 Mapped Conversion を選択した場合は、次のサブステップを実行します。それ以外の場合は **ステップ 5** へ進みます。

- a. Next をクリックします。
- b. Conversion Circuit Route Constraints 領域で、次の項目を指定します。
  - Node — DS3XM-12 カードが取り付けられているノードを選択します。
  - Slot — DS3XM-12 カードが取り付けられているスロットを選択します。
  - DS3 Mapped STS — 該当する場合に **Circuit Dest** を選択して、STS が回線の宛先であることを示すか、**Circuit Source** を選択して、STS が回線の送信元であることを示します。

**ステップ 5** **ステップ 2** で Review Route Before Creation を選択した場合は、次のサブステップを実行します。それ以外の場合は、**ステップ 6** へ進みます。

- a. Next をクリックします。
- b. 回線のルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢じり部分をクリックしてから、**Include** をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。



- c. プロビジョニングした回線が予定のルートと設定を反映していない場合は **Back** をクリックし、回線の情報を確認して変更します。回線を別のパスにルーティングする必要がある場合は、「[NTP-A182 手動ルーティングによる DS-1 回線の作成](#)」(p.6-13) を参照してください。

**ステップ 6** **Finish** をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

## DLP-A399 UBIC-H EIA の取り付け

目的	この作業では、Universal Backplane Interface Connector — Horizontal (UBIC-H) EIA を取り付けます。
工具 / 機器	#2 プラス ドライバ 小型スロット ヘッド ネジ用ドライバ 6本の周辺ネジ(6-32 × 0.375 インチのプラス ネジ)(P/N 48-0422-01) A 側 UBIC-H (15454-EIA-UBICH-A) EIA パネルおよび B 側 UBIC-H (15454-EIA-UBICH-B) EIA パネル (またはどちらか一方)
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
セキュリティ レベル	なし



**注意**

ONS 15454 に電力が供給されている状態で作業する場合は、必ず静電気防止用 (ESD) リストバンドを使用してください。シェルフ アセンブリの右下外側の端にある ESD ジャックにリストバンド ケーブルを接続してください。



**(注)**

UBIC EIA を取り付けられるのは、15454-SA-HD シェルフ アセンブリのみです。15454-SA-HD シェルフ アセンブリは、ブルーの六角形の印で他のシェルフ アセンブリと区別されています。この印は、利用可能な高密度スロット (スロット 1 ~ 3 と 15 ~ 17) の下についています。



**(注)**

高密度の電気回路カード(48 ポートの DS-3 および 12 ポートの DS3XM)を使用する場合に、UBIC-V または UBIC-H EIA が必要になります。

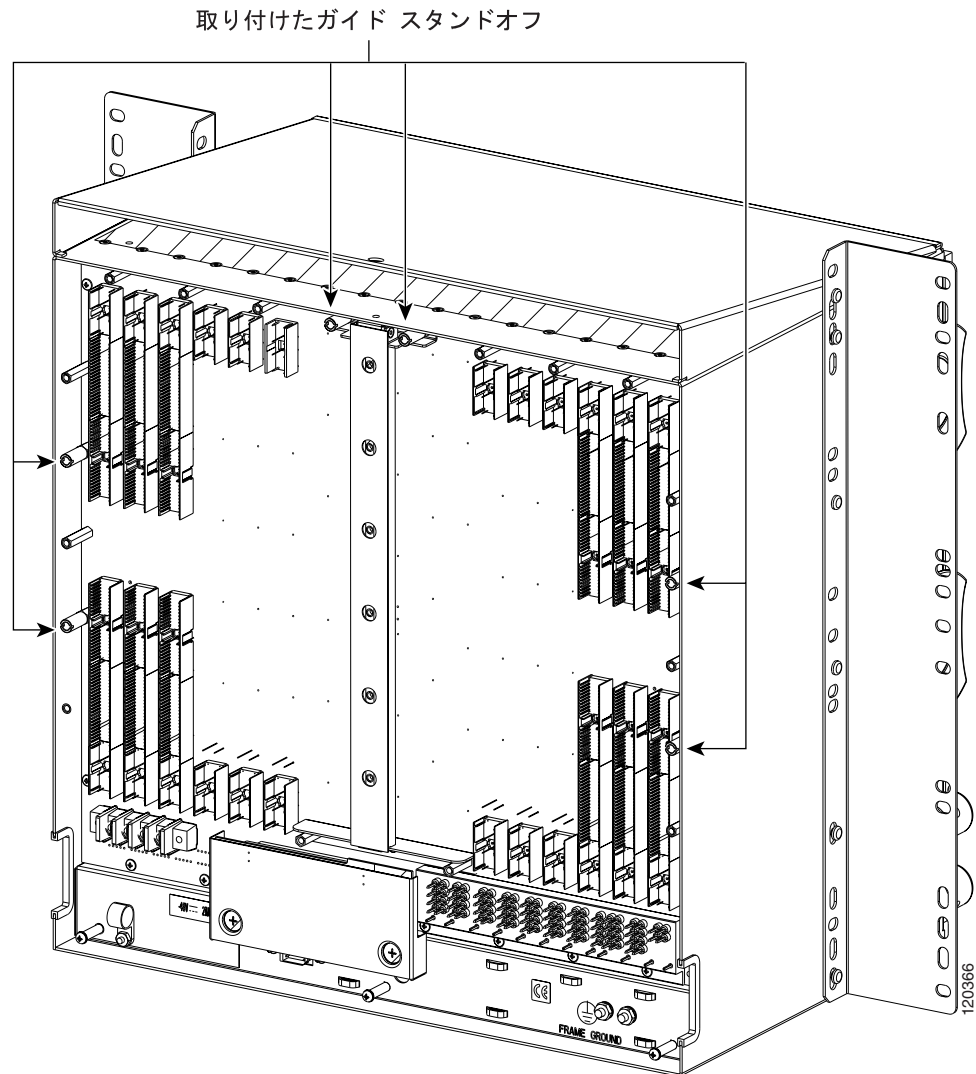
**ステップ 1** 取り付けを行う側に合った UBIC-H EIA をパッケージの中から探し、取り出します。

**ステップ 2** UBIC-H EIA のすべてのピンが曲がっていないことを確認します。

**ステップ 3** 曲がっているピンがある場合は、イエローのコネクタ プロテクタを取り外します。

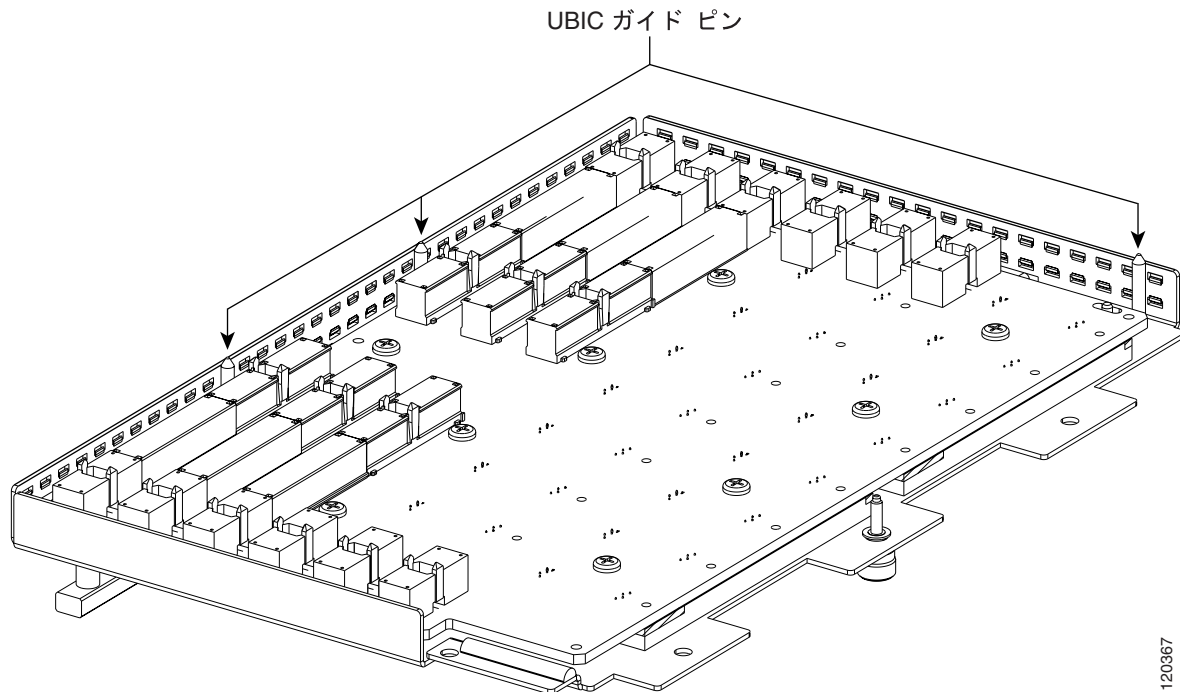
- ステップ 4** ガイド スタンドオフの穴にネジが付いている場合は、プラス ドライバを使用して取り外します。
- ステップ 5** フラットヘッド ドライバまたは 5/16 インチのソケット レンチを使用して、スタンドオフを 8 ~ 10 lbf-in (9.2 ~ 11.5 kgf-cm) で締めます。図 20-22 では、シェルフに取り付けられたガイド スタンドオフを示しています。

図 20-22 ガイド スタンドオフの取り付け



**ステップ 6** UBIC-H EIA のガイド ピンをシェルフのガイド スタンドオフの位置に合わせて、ピンとスタンドオフがしっかりと噛み合うまで UBIC-H EIA を一定の圧力で押し込みます (図 20-23)。

図 20-23 UBIC-H のガイド ピン



注意

強い抵抗感がある場合には、UBIC-H EIA を無理にシェルフに押し込まないでください。

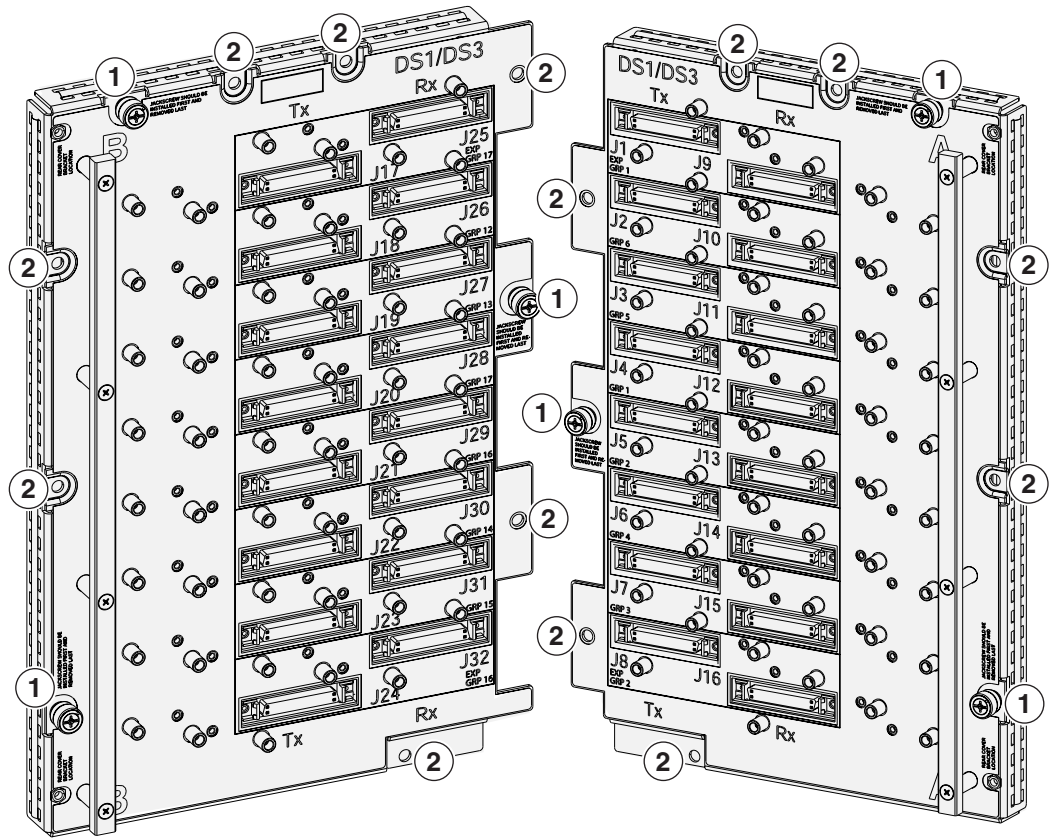
**ステップ 7** UBIC-H の 3 本のジャックネジを見つけます (図 20-24)。任意のジャックネジから始め、数回まわして締めたら、次のネジに移ります。3 本のネジがすべて固く締まるまで、各取り付けネジを一度に数回ずつ順番にまわします (図 20-25)。



注意

不均等にジャックネジを締めると、UBIC-H コネクタが損傷することがあります。

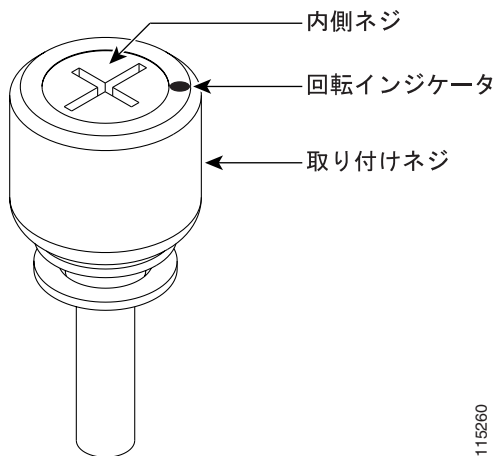
図 20-24 UBIC-H EIA ネジの位置



- ① ジャックネジ (3)
- ② 周辺ネジ (6-32 × 0.375 インチ プラス ネジ) (7)

120075

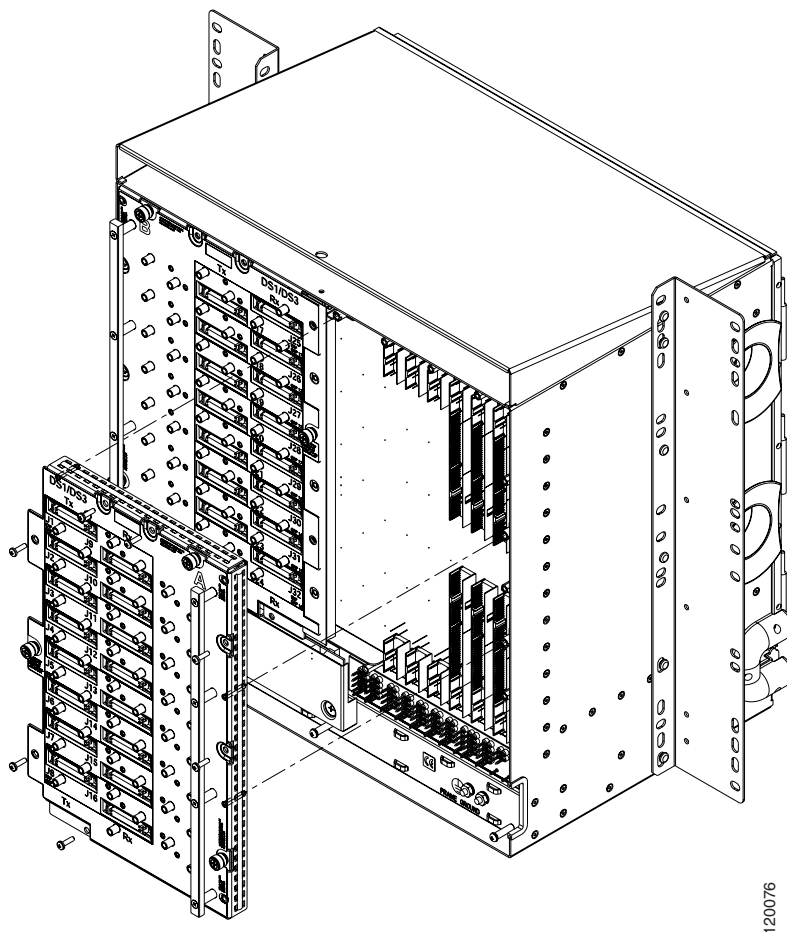
図 20-25 UBIC-H EIA のジャックネジ



115260

**ステップ 8** プラス ドライバを使用して、下の周辺ネジは取り付けないままで、6 本のうち 5 本の周辺ネジ (図 20-26) を 8 ~ 10 lbf-in (9.2 ~ 11.5 kgf-cm) のトルクで取り付け、カバー パネルをバックプレーンに固定します。

図 20-26 UBIC-H EIA の取り付け



**ステップ 9** プラス ドライバを使用して下のバックプレーン カバーを再度取り付けます。5 本のネジを取り付け、装着されるまで締めます。

**ステップ 10** 元の NTP (手順) に戻ります。





## DLP A400 ~ A499

### DLP-A412 DCU シェルフ アセンブリの取り付け

目的	分散補償モジュールを取り付ける場合、この作業に従って、Dispersion Compensation Unit (DCU) シャーシを設置します。
工具 / 機器	#2 プラス ドライバ 圧着工具
事前準備手順	#14 AWG 線およびラゲ なし
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



#### 警告

この装置にはアースを施す必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかははっきりしない場合には、電気検査機関または電気技師に確認してください。

- ステップ 1** DCU シャーシには、標準の 19 インチ (482.6 mm) または 23 インチ (584.2 mm) ラックに 1 RU のスペースが必要です。サイト計画で指定された RMU スペースを見つけます。
- ステップ 2** DCU マウント キットには、19 インチ (482.6 mm) ラック用と 23 インチ (584.2 mm) ラック用のマウント ブラケットがそれぞれ 1 組、合計 2 組含まれています。使用しているラックに合ったブラケット セットがシャーシに装着されていることを確認します。ブラケットは必要に応じて変更してください。
- ステップ 3** シャーシをラックマウントのネジ穴に合わせ、4 本のネジを 1 本ずつ差し込んで締めます。
- ステップ 4** フレーム アースを、シャーシのどちらかの側にあるアース端子に接続します。最小の #14 AWG 線を使用します。
- ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A416 回線情報の表示

目的	この作業では、名前、タイプ、サイズ、および方向などの回線に関する情報を表示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 Cisco Transport Controller (CTC) のビューに移動するには、次の手順を実行します。

- ネットワーク全体の回線を表示する場合は、View メニューで **Go to Network View** を選択します。
- 特定のノードを送信元または宛先とする回線、または特定のノードをパススルーする回線を表示する場合は、View メニューで **Go to Other Node** を選択してから、検索するノードを選択して **OK** をクリックします。
- ノード ビューで、特定のカードを送信元または宛先とする回線、または特定のカードをパススルーする回線を表示する場合は、表示する回線のあるカードをダブルクリックします。



**(注)** ノード ビューまたはカード ビューで、Circuits ウィンドウの右下隅にある Scope ドロップダウン リストから Card (カード ビュー内)、Node、または Network を選択して表示される回線の範囲を変更できます。

**ステップ 2** Circuits タブをクリックします。Circuits タブに次の情報が表示されます。

- Name — 回線の名前。回線名は手動で割り当てることも、自動的に生成することもできます。
- Type — 回線タイプ。STS ( Synchronous Transport Signal [STS] 回線 )、VT ( VT 回線 )、VTT ( VT トンネル )、VAP ( VT 集約ポイント )、OCHNC ( Dense Wavelength Division Multiplexing [ DWDM; 高密度波長分割多重 ] Optical Channel Network Connection [ OCHNC ] )、STS-v ( STS Virtual Concatenated [ VCAT; 仮想連結 ] 回線 ) および VT-v ( VT VCAT 回線 ) のいずれかになります。
- Size — 回線のサイズ。VT 回線サイズは、VT1.5 または VT2 です。STS 回線サイズは、1、3c、6c、9c、12c、18c、24c、36c、48c、および 192c です。OCHNC 回線サイズは、Equipped not specific、Multi-rate、2.5 Gbps No FEC ( 前方エラー訂正 )、2.5 Gbps FEC、10 Gbps No FEC、および 10 Gbps FEC です ( DWDM のみ、『Cisco ONS 15454 DWDM Procedure Guide』を参照 )。VCAT 回線サイズは VT1.5-nv、STS-1-nv、STS-3c-nv、および STS-12c-nv です。ここで、*n* はメンバーの数です。
- OCHNC Wlen — ( DWDM のみ ) OCHNC の場合は、プロビジョニングされた波長です。詳細については、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。
- Direction — 回線の方向 ( 双方向または単方向 )
- OCHNC Dir — ( DWDM のみ ) OCHNC の場合は OCHNC の方向。East to West ( イーストからウェスト ) または West to East ( ウェストからイースト ) のいずれかになります。詳細については、『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。
- Protection — 回線保護タイプです。保護タイプのリストは表 21-1 を参照してください。



表 21-1 回線の保護タイプ

保護タイプ	内容
1+1	回線は 1+1 保護グループで保護されます。
2F BLSR	回線は、2 ファイバ Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング) で保護されます。
4F BLSR	回線は 4 ファイバ BLSR で保護されます。
2F-PCA	回線は、2 ファイバ BLSR の Protection Channel Access (PCA) パスにルーティングされます。PCA 回線は保護されません。
4F-PCA	回線は、4 ファイバ BLSR の PCA にルーティングされます。PCA 回線は保護されません。
BLSR	回線は 2 ファイバおよび 4 ファイバの両方の BLSR で保護されます。
DRI	回線は Dual-Ring Interconnect (DRI; デュアル リング相互接続) Unidirectional Path Switched Ring [ UPSR; 単方向パス スイッチ型リング ] および BLSR の両方) で保護されます。
N/A	同じノード上に接続のある回線は保護されません。
PCA	回線は、2 ファイバ BLSR と 4 ファイバ BLSR の両方の PCA パスにルーティングされます。PCA 回線は保護されません。
Protected	回線はダイバース SONET トポロジー (BLSR と UPSR、または UPSR と 1+1) で保護されます。
Splitter	回線は、保護トランスポンダ (TXPP_MR_2.5G) のスプリッタ保護で保護されます。『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。
Unknown	回線は異なるノード上に送信元と宛先があり、ノード間の通信がダウンしています。これは、回線要素の一部が不明な場合の保護タイプです。
Unprot (black)	異なるノードに送信元と宛先がある回線は保護されません。
Unprot (red)	完全に保護する回線として作成した回線は、BLSR または 1+1 保護グループの排除などのシステムの変更が原因で保護されなくなります。
UPSR	回線は UPSR で保護されます。
Y-Cable	回線は、トランスポンダカードまたはマックスポンダカードの Y 字ケーブル保護グループで保護されます。『Cisco ONS 15454 DWDM Procedure Guide』を参照してください。

- Status — 回線のステータスです。表 21-2 に、表示される回線のステータスを示します。

表 21-2 Cisco ONS 15454 回線のステータス

ステータス	定義 / アクティビティ
CREATING	CTC は回線を作成中です。
DISCOVERED	CTC は回線を作成しました。すべてのコンポーネントが適切に配置され、回線の送信元から宛先までの完全なパスが存在します。
DELETING	CTC は回線を削除中です。

表 21-2 Cisco ONS 15454 回線のステータス (続き)

ステータス	定義 / アクティビティ
PARTIAL	<p>CTC で作成された回線でクロスコネクトまたはネットワーク スパンが見つかりません。送信元から宛先までの完全なパスが存在しないか、Alarm Interface Panel (AIP) がその回線パスのノードのいずれか 1 つで変更されているため、その回線は変更する必要があります (AIP にはノードの MAC [メディア アクセス制御] アドレスが保存されています)。</p> <p>CTC では、回線がクロスコネクトおよびネットワーク スパンを使用して表示されます。あるネットワーク スパンが回線から欠落していると、回線のステータスは PARTIAL になります。ただし、PARTIAL ステータスは、回線のトラフィックに障害が発生していることを示しているとはかぎりません。保護パス上にトラフィックが流れている場合もあります。</p> <p>ネットワーク スパンは、アップまたはダウンのいずれかのステータスとなります。CTC の回線およびネットワーク マップでは、アップしているスパンがグリーンの線で表示され、ダウンしているスパンはグレーの線で表示されます。CTC セッション中にネットワーク上のあるスパンで障害が発生した場合、そのスパンはネットワークマップに残りますが、色がグレーに変わりダウン状態を示します。障害が発生している状態で CTC セッションを再起動すると、新しい CTC セッションはそのスパンを検出できず、そのスパンに対応する線はネットワーク マップに表示されません。</p> <p>続いて、ダウンするネットワーク スパンにルーティングされている回線は、CTC の現セッションでは DISCOVERED と表示されますが、スパンに障害が発生したあとにログインしたユーザには、PARTIAL と表示されます。</p>
DISCOVERED_TL1	TL1 で作成した回線または TL1 と同様の機能の CTC で作成した回線は完全です。送信元から宛先までの完全なパスが存在します。
PARTIAL_TL1	TL1 で作成した回線または TL1 と同様の機能の CTC で作成した回線にはクロスコネクトが欠落しているため、送信元から宛先までの完全なパスは存在しません。
CONVERSION_PENDING	トポロジー アップグレード中の既存の回線は、この状態に設定されます。回線は、トポロジー アップグレードが完了すると、DISCOVERED 状態に戻ります。トポロジー アップグレードの詳細については、『Cisco ONS 15454 Reference Manual』の「SONET Topologies and Upgrades」の章を参照してください。
PENDING_MERGE	トポロジー アップグレードで、代替パスを表すために作成された新規回線はこのステータスに設定され、その回線が一時的なものであることを示します。これらの回線は、トポロジー アップグレードが失敗した場合に削除可能です。トポロジー アップグレードの詳細については、『Cisco ONS 15454 Reference Manual』の「SONET Topologies and Upgrades」の章を参照してください。
DROP_PENDING	新規回線ドロップが追加されているとき、回線はこのステータスに設定されます。
ROLL_PENDING	回線ロールは、完了またはキャンセルを待っています。

- Source — *node/slot(card type)/port "port name"/STS/VT* で表される回線の送信元（二重引用符内にポート名が表示されます）。ノードとスロットは必ず表示されます。*[port "port name"/STS/VT]* は、送信元のカード、回線タイプ、ポートに名前が割り当てられているかどうかに応じて表示の有無が変わります。ポートが MRC-12 カードの場合、ポートの形式は *[PPM-port\_number]* です。回線のサイズが連結サイズ（3c、6c、12c など）の場合、回線で使用する STS は *[S7..9]*（STS 7、8、および 9）または *[S10..12]*（STS 10、11、および 12）のように省略形で表されます。
- Destination — 回線の送信元と同じ形式（*node/slot[card type]/port "port name"/STS/VT*）で表される回線の宛先
- # of VLANS — イーサネット回線が使用する VLAN（仮想 LAN）の数
- # of Spans — 回線を構成するノード間リンクの数。カラムを右クリックすると、Span Details を選択して回線スパンの詳細を表示または非表示にできる、ショートカットメニューが表示されます。スパンの各ノードでは、スパンの詳細が *node/slot (card type)/port/STS/VT* で表されます。
- State — 回線のサービス状態（IS、OOS、または OOS-PARTIAL）です。回線のサービス状態は、クロスコネクタのサービス状態の集約です。
  - IS — すべてのクロスコネクタのサービス状態が In-Service and Normal（IS-NR）です。
  - OOS — すべてのクロスコネクタのサービス状態が Out-of-Service and Management, Disabled（OOS-MA,DSBLD）および Out-of-Service and Management, Maintenance（OOS-MA,MT）の両方またはそのいずれかにあります。
  - OOS-PARTIAL — 少なくとも 1 つのクロスコネクタが IS-NR で、それ以外が OOS-MA,DSBLD と OOS-MA,MT の両方またはそのいずれかです。

**ステップ 3** 元の NTP（手順）に戻ります。

## DLP-A418 公開鍵セキュリティ証明書のインストール

目的	この作業では、ITU 勧告 X.509 の公開鍵セキュリティ証明書をインストールします。Software Release 4.1 以降を実行するには、公開鍵証明書が必要です。
工具 / 機器	なし
事前準備手順	この作業は「 <a href="#">DLP-A60 CTC へのログイン</a> 」(p.17-71) 中に行います。CTC へログイン以外の作業中にこの作業を実行することはできません。
必須 / 適宜	必須
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** Java Plug-in Security Warning ダイアログボックスが表示されたら、次のいずれかのオプションを選択します。

- Yes (Grant This Session) — 現在のセッションに対してだけ、公開鍵証明書を PC にインストールします。証明書は、セッションが終了すると削除されます。次に ONS 15454 にログインしたときにも、このダイアログボックスは表示されます。
- No (Deny) — 証明書のインストールを拒否します。このオプションを選択すると、ONS 15454 にログインできなくなります。
- Always (Grant Always) — 公開鍵証明書をインストールし、セッションが終了したあともこの証明書が削除されないようにします。このオプションの使用を推奨します。
- More Details (View Certificate) — 公開鍵セキュリティ証明書を表示します。

**ステップ 2** Login ダイアログボックスが表示された場合は、**ステップ 3** へ進みます。Change Java Policy File ダイアログボックスが表示された場合は、このステップを実行します。Change Java Policy File ダイアログボックスは、PC の CTC で Java ポリシー ファイル (.java.policy) の変更が検出されたときに表示されます。Software Release 4.0 以前では、CTC ソフトウェア ファイルを PC へダウンロードできるように、Java ポリシー ファイルが変更されていました。この変更された Java ポリシー ファイルはソフトウェア R4.1 以降では必要ないので、R4.1 より前のソフトウェアを実行している ONS 15454 にログインしないのであれば削除できます。次のいずれかのオプションを選択します。

- Yes — 変更された Java ポリシー ファイルを PC から削除します。このオプションを選択するのは、ソフトウェア R4.1 以降のソフトウェアを実行している ONS 15454 にログインする場合だけです。
- No — 変更された Java ポリシー ファイルを PC から削除しません。このオプションを選択するのは、ソフトウェア R4.0 以前を実行している ONS 15454 にログインする場合です。No を選択した場合、ONS 15454 にログインするたびに、このダイアログボックスが表示されます。毎回表示されないようにするには、**Do not show the message again** チェックボックスをオンにします。



#### 注意

Java ポリシー ファイルを削除すると、ソフトウェア R4.0 以前のソフトウェアを実行しているノードへログインできなくなります。このファイルを削除して、以前のリリースを実行している ONS 15454 へログインする場合は、そのリリースのソフトウェア CD を PC の CD-ROM に挿入し、CTC のセットアップウィザードを実行して、Java ポリシー ファイルを再度インストールします。

**ステップ 3** 元の手順 (NTP) に戻ります。

## DLP-A421 G シリーズおよび CE-1000-4 のフロー制御水準点のプロビジョニング

目的	この作業では、G シリーズおよび CE-1000-4 イーサネット ポート上でフロー制御に使用するバッファ メモリのレベルをプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、G シリーズまたは 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 > Port タブをクリックします。

**ステップ 3** Water Marks カラムで、対象となるポートの行にあるセルをクリックします。

**ステップ 4** 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、次の手順を実行します。

- 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。

- b. Apply をクリックします。

**ステップ 5** フロー制御水準点のカスタムをプロビジョニングする場合は、次の手順を実行します。

- a. ドロップダウン リストから **Custom** を選択します。
- b. Flow Ctrl Lo カラムで、対象となるポートの行にあるセルをクリックします。
- c. セルに値を入力します。Flow Ctrl Lo の有効な値の範囲は 1 ~ 510 です。Flow Ctrl Hi の値より小さくする必要があります。  
この値は、接続されているイーサネット デバイスに対して伝送の再開を指示する信号を送るためのフロー制御のスレッシュホールドを設定します。
- d. Flow Ctrl Hi カラムで、対象となるポートの行にあるセルをクリックします。
- e. セルに値を入力します。Flow Ctrl Hi の有効な値の範囲は 2 ~ 511 です。Flow Ctrl Lo の値より大きくする必要があります。  
この値は、接続されているイーサネット デバイスに対して伝送の一時停止を指示する信号を送るためのフロー制御のスレッシュホールドを設定します。
- f. Apply をクリックします。



**(注)** 低い水準点は、STS-1 を使用する Voice Over IP (VoIP) などの低遅延サブプレート アプリケーションに最適です。高い水準点は、接続されたイーサネット デバイスに不十分なバッファリング、ベストエフォート トラフィック、または長距離のアクセス回線がある場合に最適です。

**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A422 BLSR の拡張バイト マッピングの確認

<b>目的</b>	この作業では、ノードを BLSR から削除したあとに接続する BLSR トランク (スパン) カード上で、拡張バイト マッピングが同じであることを確認します。
<b>工具 / 機器</b>	OC-48 AS カードが、接続されている BLSR スパンのどちらか一方または両端に取り付けられている必要があります。
<b>事前準備手順</b>	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
<b>必須 / 適宜</b>	適宜
<b>オンサイト / リモート</b>	オンサイトまたはリモート
<b>セキュリティ レベル</b>	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 ビューで、BLSR ノードを削除したあとに再接続する OC48 AS トランク (スパン) カード付き BLSR ノードをダブルクリックします。

**ステップ 2** 1 つの OC-48 AS BLSR トランク カードをダブルクリックします。

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

**ステップ 4** BLSR Ext Byte カラムに表示されているバイト情報を紙に記録します。

## ■ DLP-A428 1+1 構成での光ファイバケーブルの取り付け

- ステップ 5** 2 つめの OC-48 AS トランク カードについて、ステップ 2 ~ 4 を繰り返します。
- ステップ 6** 新しいスパンのもう一方の端にあるノードに OC-48 AS トランク カードがある場合は、そのノードでステップ 1 ~ 5 を繰り返します。ノードに OC-48 AS カードがないと、トランク カードは K3 拡張バイトにマップされます。ステップ 7 へ進んでください。
- ステップ 7** 新しいスパンの両端でトランク カードが同じ BLSR 拡張バイトにマップされている場合は、ステップ 8 へ進みます。同じでない場合は、どちらか一方のノードにあるトランク カードの拡張バイトをマップしなおします。「DLP-A89 K3 バイトの再マップ」(p.17-94) を参照してください。
- ステップ 8** 元の手順 (NTP) に戻ります。

## DLP-A428 1+1 構成での光ファイバケーブルの取り付け

目的	この作業では、1+1 リニア構成の光カード (OC-N) に光ファイバケーブルを取り付けます。
工具 / 機器	光ファイバケーブル
事前準備手順	NTP-A112 ファイバ コネクタの清掃 (p.15-20)
必須 / 適宜	必須
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) Cisco OC-3 IR/STM-1 SH、OC-12 IR/STM-4 SH、および OC-48 IR/STM-16 SH インターフェイス 光カードは、すべて 1310 nm で動作し、最も広く使用されていて入手先も多い SMF-28 光ファイバケーブルに最適化されています。



(注) Corning MetroCor 光ファイバケーブルは、1550 nm で送信する光インターフェイス、または DWDM ウィンドウの C および L で送信する光インターフェイス用に最適化されています。この光ファイバケーブルは、OC-3 IR/STM-1 SH、OC-12 IR/STM-4 SH、および OC-48 IR/STM-16 SH インターフェイス光カードで見られる分散許容よりも、更に高い分散許容を持つインターフェイスを対象としています。Corning MetroCor 光ファイバケーブルを使用している場合、OC-3 IR/STM-1 SH、OC-12 IR/STM-4 SH、および OC-48 IR/STM-16 SH インターフェイス光カードは、減衰限界になる前に、分散限界になります。この場合、OC-3 IR/STM-1 SH、OC-12 IR/STM-4 SH、および OC-48 IR/STM-16 SH カードの代わりに、OC-3 LR/STM-1 LH、OC-12 LR/STM-4 LH、および OC-48 LR/STM-16 LH カードを使用することを検討してください。



(注) ネットワーク計画者または技術者は、すべてのファイバ タイプについて、関連のファイバ タイプ および光カードの仕様を参照し、減衰、分散、その他の特性を確認して適切なネットワーク構成を行う必要があります。

- ステップ 1** ファイバ接続計画を立てます。すべての 1+1 ノードに対して同じ計画を使用します。
- ステップ 2** ケーブルコネクタのキー付きの突起を、あるノードの現用 OC-N カードの送信 (Tx) コネクタに合わせ、その光ファイバケーブルのもう一方の端を隣接ノードの現用 OC-N カードの受信 (Rx) コネクタに取り付けます。送信用および受信用の光ファイバケーブルが一致しない (1 本の光ファイバケーブルが、あるカードの受信ポートと他のカードの受信ポートを接続している、あるいは送信ポートで同様の状況になっている) 場合、カードの SF LED が点灯します。図 19-1 (p.19-6) にケーブルの配置を示します。
- ステップ 3** 2 つのノード上の対応する保護ポートに対して、ステップ 1 と 2 を繰り返し、1+1 構成に配置したい他のすべての現用および保護ポートのペアに対して同様に繰り返します。
- ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A430 スパニングツリー情報の表示

目的	この作業では、E シリーズイーサネット回線、および Spanning Tree Protocol (STP; スパニングツリープロトコル) で動作するイーサネットフロントポートを表示できるようにします。E シリーズのカードでは、ノードあたり最大 8 個の STP をサポートしています。STP の詳細については、『 <i>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327</i> 』を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、Maintenance > Ether Bridge > Circuits タブをクリックします。
- ステップ 2** EtherBridge Circuits ウィンドウに、次の情報が表示されます。
- Type — スパニングツリーにマップされたイーサネット回線のタイプ (EtherSwitch ポイントツーポイントなど) を示します。
  - Circuit Name/Port — スパニングツリー内の回線の回線名を示します。このカラムには、ノードに関するスパニングツリーにマップされたイーサネットのスロットとポートも表示されます。
  - STP ID — スパニングツリープロトコルの ID 番号を示します。
  - VLANs — 回線またはポートに関連する VLAN を示します。
- ステップ 3** 元の NTP (手順) に戻ります。

## DLP-A431 JRE バージョンの入れ替え

目的	この作業では、JRE のバージョンを入れ替えます。ソフトウェア CD を使用しないで旧バージョンから新しい JRE バージョンへアップグレードすることができます。この作業は、ブラウザのデフォルトバージョンには影響しません。使用する JRE バージョンを選択したら、CTC を終了してください。ノードへ次回ログインしたときに、新しい JRE バージョンが使用されます。
工具	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。
- ステップ 2** **JRE** タブをクリックします。JRE タブに、現在の JRE バージョンと推奨バージョンが表示されます。
- ステップ 3** **Browse** ボタンをクリックし、コンピュータ上の JRE ディレクトリに移動します。
- ステップ 4** JRE のバージョンを選択します。
- ステップ 5** **OK** をクリックします。
- ステップ 6** File メニューから **Exit** を選択します。
- ステップ 7** 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 8** 「[DLP-A60 CTC へのログイン](#)」(p.17-71) を実行します。
- ステップ 9** 元の NTP (手順) に戻ります。
- 

## DLP-A433 ノードのセキュア モードのイネーブル化

目的	この作業では、ONS 15454 でのセキュア モードをイネーブルにします。セキュア モードがイネーブルになっているとき、2 つの IP アドレスのうち、1 つは バックプレーン LAN ポートに割り当てられ、もう 1 つは TCC2P RJ-45 TCP/IP (LAN) ポートに割り当てられます。
工具 / 機器	TCC2P カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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



**注意**

TCC2P TCP/IP (LAN) ポートに割り当てる IP アドレスは、バックプレーン LAN ポートと ONS 15454 のデフォルト ルータとは違うサブネットに存在するものにしなければなりません。新しい TCC2P IP アドレスが要件を満たしていることと、ONS 15454 ネットワークの IP アドレスと互換性があることを確認してください。

**(注)**

この作業が完了すると、ノードはリブートします。そのため、CTC コンピュータとノードとの間の接続が一時的に切断されます。

- ステップ 1** ノード ビューで、**Provisioning > Security > Data Comm** タブをクリックします。
- ステップ 2** **Change Mode** をクリックします。
- ステップ 3** Change Secure Mode ウィザードのページに表示される情報を確認してから、**Next** をクリックします。
- ステップ 4** TCC Ethernet Port ページで、TCC2P LAN (TCP/IP) ポートの IP アドレスとサブネット マスクを入力します。IP アドレスには、バックプレーン LAN ポートや ONS 15454 のデフォルト ルータと同じサブネットの IP アドレスを指定しないでください。
- ステップ 5** **Next** をクリックします。
- ステップ 6** Backplane Ethernet Port ページで、バックプレーンの IP アドレス、サブネット マスク、およびデフォルト ルータを必要に応じて修正します (通常、ONS 15454 ネットワークを変更していない場合は、これらのフィールドを修正する必要はありません)。
- ステップ 7** **Next** をクリックします。
- ステップ 8** SOCKS Proxy Server Settings のページで、次のオプションからいずれかを選択します。
  - External Network Element (ENE) — このボックスをオンにすると、CTC コンピュータは、自分の接続されている ONS 15454 にのみ表示されるようになります。他の Data Communication Channel (DCC; データ通信チャネル) 接続ノードには、このコンピュータは表示されません。デフォルトでは、SOCKS プロキシは ENE に対してイネーブルになっています。SOCKS プロキシがディセーブルになっている場合、ファイアウォールの後ろにある他のセキュア モード NE と通信できません。
  - Gateway Network Element (GNE) — このボックスをオンにすると、CTC コンピュータは他の DCC 接続ノードで表示されるようになります。このノードでは IP トラフィックが DCC と LAN ポートとの間でルーティングされるのを防ぎます。デフォルトでは、セキュア ノードを GNE として設定しても、他のセキュア NE と通信できるように SOCKS プロキシがイネーブルになります。
- ステップ 9** **Finish** をクリックします。

30 ~ 40 秒以内に TCC2P カードがリブートします。CTC の画面がネットワーク ビューに切り替わり、CTC Alerts ダイアログボックスが表示されます。ネットワーク ビューに表示されているノードは、グレーになって DISCONNECTED 状態が発生します。

## ■ DLP-A434 ノード セキュリティのロック

**ステップ 10** CTC Alerts ダイアログボックスで **Close** をクリックします。リポートが終了するのを待ちます（数分かかります）。

**ステップ 11** DISCONNECTED 状態がクリアされたら、次のステップを実行して、バックプレーンの IP アドレスが CTC と LCD に表示されないようにします。バックプレーンの IP アドレスを非表示にしない場合は、[ステップ 12](#) へ進みます。

- a. ノード ビューでノードを表示します。
- b. **Provisioning > Security > Data Comm** タブをクリックします。
- c. LCD に IP アドレスを表示したくない場合は、LCD IP Setting フィールドで **Suppress Display** を選択します。
- d. CTC に IP アドレスが表示されないようにするには、**Suppress CTC IP Address** チェックボックスをオンにします。このオプションを選択すると、CTC の情報領域と Provisioning > Security > Data Comm タブから、IP アドレスの表示が消えます。
- e. **Apply** をクリックします。



**(注)** セキュア モードを有効にすると、TCC2P IP (LAN) ポートのアドレスは、そのノードの IP アドレスになります。バックプレーン LAN ポートは、別の IP アドレスになります。

**ステップ 12** 元の手順 (NTP) に戻ります。

## DLP-A434 ノード セキュリティのロック

目的	この作業では、ONS 15454 でのセキュア モード設定をロックします。セキュア モードがロックされると、2つの IP アドレスのうち、1つは TCC2P TCP/IP (LAN) ポートに対して、1つはバックプレーン LAN ポートに対して、ONS 15454 上で常にプロビジョニングされる必要があります。
工具 / 機器	TCC2P カードが取り付けられている必要があります。
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A433 ノードのセキュア モードのイネーブル化 (p.21-10)</a>
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



### 注意

ノードがロックされている場合、どのユーザがどんなアクションを実行してもロックを解除できません。変更できるのは、Cisco Technical Support だけです。ノードのデータベースが削除され、ロック解除された別のデータベースがロードされても、ノードはロックされたままになります。ノードに、デュアル IP アドレスをはじめとした現在のセキュア設定を永久保持したい場合以外は、作業を進めないでください。



(注) セキュア モードの詳細については、『Cisco ONS 15454 Reference Manual』の「Management Network Connectivity」の章を参照してください。

- 
- ステップ 1** Provisioning > Security > Data Comm タブをクリックします。
- ステップ 2** Lock をクリックします。
- ステップ 3** Confirm Lock Secure Mode 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-A435 セキュア モードのバックプレーン ポートの IP 設定の修正

目的	この作業では、ONS 15454 バックプレーンの IP アドレス、サブネットマスク、およびデフォルト ルータを修正します。また、CTC と ONS 15454 の LCD にバックプレーンの IP アドレスを表示するかどうかの制御設定も変更します。この作業を行う場合は、セキュア モードを設定しておく必要があります。
工具 / 機器	TCC2P カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">DLP-A433 ノードのセキュア モードのイネーブル化 (p.21-10)</a>
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



### 注意

ONS 15454 ネットワークと互換性のない IP アドレスをプロビジョニングすると、サービスに影響が出る場合があります。



### 注意

この作業は、ロックされたセキュア モード NE では実行できません。

- 
- ステップ 1** Provisioning > Security > Data Comm タブをクリックします。
- ステップ 2** 次のフィールドを必要に応じて変更します。
- IP Address
  - Subnet Mask
  - Default Router

## ■ DLP-A436 ノードのセキュリティ モードのディセーブル化

- LCD IP Setting — 次のいずれかを選択します。
  - **Allow Configuration** — LCD にバックプレーンの IP アドレスが表示され、LCD のボタンでその IP アドレスを変更できるようにします。
  - **Display only** — LCD にバックプレーンの IP アドレスが表示されますが、LCD のボタンによる IP アドレスの変更はできません。
  - **Suppress Display** — LCD に IP アドレスが表示されないようにします。
- **Suppress CTC IP Address** — このフィールドをオンにすることで、Data Comm サブタブや CTC のノード ビュー情報領域、CTC のその他の場所に IP アドレスが表示されなくなります。

**ステップ 3** Apply をクリックします。

IP アドレス、サブネット マスク、またはデフォルト ルータを変更すると、ノードがリブートします。リブートには、5 ~ 10 分かかります。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A436 ノードのセキュリティ モードのディセーブル化

目的	この作業では、ONS 15454 セキュア モードをディセーブルにします。つまり、デュアル IP アドレスがサポートされなくなります。セキュアモードがディセーブルになっている場合、1 つの IP アドレスだけが、バックプレーン LAN ポートと TCC2P TCP/IP (LAN) ポートの両方に対してプロビジョニング可能となります。ノードに対してセキュアモードがディセーブルになっている場合、そのノードは他のセキュアモードのネットワーク ノードを識別できません。
工具 / 機器	TCC2P カードが取り付けられている必要があります。
事前準備手順	<a href="#">NTP-A108 データベースのバックアップ (p.15-6)</a>  <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) この作業が完了すると、ノードはリブートします。そのため、CTC コンピュータとノードとの間の接続が一時的に切断されます。



(注) NE をセキュア モードからデフォルト (リピータ) モードの変更すると、バックプレーン IP アドレスはそのノードの IP アドレスになります。



(注) この作業は、NE のセキュリティ モード設定がロックされていると実行できません。セキュアモードがロックされている場合、Cisco Technical Support に連絡してノード設定を変更する必要があります。

- 
- ステップ 1** Provisioning > Security > Data Comm タブをクリックします。
- ステップ 2** Change Mode をクリックします。
- ステップ 3** Change Secure Mode ウィザードのページに表示される情報を確認してから、Next をクリックします。
- ステップ 4** Node IP Address のページで、ノードに割り当ててるアドレスを選択します。
- Backplane Ethernet (LAN) Port — ノードの IP アドレスとして、バックプレーンの IP アドレスを割り当てます。
  - TCC Ethernet (LAN) Port — ノードの IP アドレスとして、TCC2P ポートの IP アドレスを割り当てます。
  - New IP Address — 新しい IP アドレスを割り当てます。このオプションを選択した場合は、新しい IP アドレス、サブネット マスク、およびデフォルト ルータの IP アドレスを入力します。
- ステップ 5** Next をクリックします。
- ステップ 6** SOCKS Proxy Server Settings のページで、次のいずれかを選択します。
- **External Network Element (ENE)** — このボックスをオンにすると、SOCKS プロキシがデフォルトでディセーブルになり、CTC コンピュータは、自分の接続されている ONS 15454 にのみ表示されるようになります。他のセキュア モードの DCC 接続ノードには、このコンピュータは表示されません。ファイアウォールはイネーブルになるので、このノードでは IP トラフィックが DCC と LAN ポートとの間でルーティングされるのを防ぎます。
  - **Gateway Network Element (GNE)** — このボックスをオンにすると、CTC コンピュータは他の DCC 接続ノードで表示されるようになり、SOCKS プロキシはイネーブルのままになります。ただし、このノードは IP トラフィックが DCC と LAN ポートとの間でルーティングされるのを防ぎます。
  - **Proxy-only** — このボックスをオンにすると、ONS 15454 は CTC の要求に対して、ノードがプロキシとして機能するファイアウォール内の DCC 接続ノードのリストで応答するようになります。CTC コンピュータは、他の DCC 接続ノードで表示されるようになります。このノードでは、DCC と LAN ポート間で IP トラフィックがルーティングされるのを防ぎません。
- ステップ 7** Finish をクリックします。
- 30 ~ 40 秒以内に TCC2P カードがレポートします。CTC の画面がネットワーク ビューに切り替わり、CTC Alerts ダイアログボックスが表示されます。ネットワーク ビューに表示されているノードは、グレーになって DISCONNECTED 状態が発生します。
- ステップ 8** CTC Alerts ダイアログボックスで Close をクリックします。レポートが終了するのを待ちます (数分かかります)。
- ステップ 9** 元の NTP (手順) に戻ります。
-

## DLP-A437 VCAT メンバーのサービス状態の変更

目的	この作業では、Edit Circuit ウィンドウを表示して VCAT メンバーのサービス状態を変更します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン (p.17-71)  ネットワークに VCAT 回線が存在している必要があります。 「NTP-A264 自動ルーティングによる VCAT 回線の作成」(p.6-99) または「NTP-A265 手動ルーティングによる VCAT 回線の作成」(p.6-104) 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	プロビジョニング以上のレベル



(注)

CTC で Link Capacity Adjustment Scheme (LCAS) を使用しないメンバーの状態を変更できるのは、新しい状態が他のメンバーの In Group VCAT 状態と同じであるか、または新しい状態が Out of Group VCAT 状態である場合だけです。In Group VCAT 状態は、メンバーのクロスコネクが IS-NR、OOS-MA、AINS、または OOS-AU、MT サービス状態であることを示します。非 LCAS VCAT メンバーの場合、Out of Group VCAT 状態は、OOS-MA、DSBLD サービス状態になっています。

- 
- ステップ 1** ネットワーク ビューで、Circuits タブをクリックします。
- ステップ 2** 編集する VCAT 回線をクリックして、Edit をクリックします。
- ステップ 3** Members タブをクリックします。
- ステップ 4** 変更するメンバーを選択します。複数のメンバーを選択する場合は、Ctrl キーを押したままで、各メンバーをクリックします。
- ステップ 5** Tools メニューから Set Circuit State を選択します。



(注)

State タブを使用することでも、Edit Circuit ウィンドウに表示されているすべてのメンバーの状態を変更できます。また別の方法として、メンバーを選択してから、Edit Member ボタンをクリックして Edit Member Circuit ウィンドウを開き、State タブをクリックするという方法もあります。

- ステップ 6** Target Circuit Admin State ドロップダウン リストから、次の管理状態を選択します。
- IS — メンバーのクロスコネクのサービス状態を IS-NR にします。
  - OOS,DSBLD — メンバーのクロスコネクのサービス状態を OOS-MA,DSBLD にします。トラフィックは回線を通過できません。
  - IS,AINS — メンバーのクロスコネクのサービス状態を OOS-AU,AINS にして、アラームと状態を抑制します。接続で有効な信号を受信すると、サービス状態は自動的に IS-NR になります。

- OOS,MT — メンバーのクロスコネクトのサービス状態を OOS-MA,MT にします。メンテナンス状態になっても、トラフィック フローが中断されることはありません。アラームおよび状態が抑制され、その回線に対してループバックを実行することができます。回線をテストしたり、回線のアラームを一時的に抑制したりする場合、この OOS,MT を使用します。テストが完了したら、管理状態を IS、IS,AINS、または OOS,DSBLD に変更します。
- OOS,OOG — (LCAS および Sw-LCAS VCAT のみ) VCAT メンバーのクロスコネクトのサービス状態を Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) にします。この管理状態は、メンバー回線をグループから外したり、トラフィックの送信を停止したりする場合に使用します。

ML シリーズ カード上での 2 つの VCAT メンバーは次のように動作します(いずれも SW-LCAS および非 LCAS メンバー)

- メンバーを IS-NR から OOS-MT,MT または OOS-MA,DSBLD サービス状態に変更した場合、最初のメンバーのサービス状態を変更すると、両方のメンバーのサービス状態が自動的に変更されます。
- メンバーを OOS-MA,DSBLD から OOS-MT,MT または IS-NR サービス状態に変更した場合、2 番目の VCAT メンバーから開始する必要があります。たとえば、まず 2 番目のメンバーのサービス状態を変更し、次に最初のメンバーのサービス状態を変更します。2 番目のメンバーが別のサービス状態になっている場合、最初のメンバーのサービス状態を変更できません。

**ステップ 7** Apply をクリックします。

**ステップ 8** File メニューから Close を選択して、Edit Circuit ウィンドウを閉じます。

**ステップ 9** 元の NTP (手順) に戻ります。

## DLP-A438 FC\_MR-4 カードにある汎用ポートの設定変更

目的	この作業では、FC_MR-4 カードにある汎用ポートの設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、ポートの設定を変更する FC\_MR-4 カードをダブルクリックします。

**ステップ 2** Provisioning > Port > General 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 21-3](#) 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。

## ■ DLP-A438 FC\_MR-4 カードにある汎用ポートの設定変更

## ステップ4 Apply をクリックします。

表 21-3 FC\_MR-4 カードにある汎用ポートの設定


パラメータ	内容	オプション
Port	(表示専用) ポート番号	1 ~ 4
Port Name	指定したポートに名前を割り当てます。	<p>ユーザ定義。32 文字以下の英数字または特殊文字で名前を指定します。デフォルトはブランクです。</p> <p>「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。</p> <p> (注) このポートのファイバ チャネルまたは Fiber Connectivity( FICON )リンクが、Cisco MDS 9000 スイッチとの併用のため Cisco MDS Fabric Manager で検出される場合、ファイバ チャネル /FICON ポート名を次の文字列にプロビジョニングする必要があります。</p> <p>FC: &lt;switch&gt; &lt;interface&gt;</p> <p>ここで、&lt;switch&gt; は DNS 名または Cisco MDS 9000 スイッチの IPv4/v6 アドレス、&lt;interface&gt; は名前の割り当て先である FC_MR-4 ポートのカードスロット / ポートです。</p> <p>例 : FC:10.0.0.1 fc2/4</p>
Admin State	ポートの管理サービス状態を変更します。ネットワークの状態によっては変更できません。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>
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。	<ul style="list-style-type: none"> <li>• IS-NR — 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。</li> <li>• OOS-MA,DSBLD — ポートは停止中で、トラフィックは伝送できません。</li> <li>• OOS-MA,MT — ポートは、メンテナンスのため停止中です。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。</li> </ul>
Port Rate	ファイバ チャネル インターフェイスを選択します。	<ul style="list-style-type: none"> <li>• 1 Gbps</li> <li>• 2 Gbps</li> </ul>
Link Rate	(表示専用) ポートの実際のレートを表示します。	—



表 21-3 FC\_MR-4 カードにある汎用ポートの設定 (続き)

パラメータ	内容	オプション
Max GBIC Rate	(表示専用) GBIC (ギガビット インターフェイス コンバータ) の最大レートを表示します。シスコでは、FC_MR-4 カードに対して、2 つの GBIC をサポートしています (ONS-GX-2FC-SML および ONS-GX-2FC-MMI)。別の GBIC を使用する場合は、[Contact GBIC vendor] が表示されます。	—
Link Recovery	ローカル ポートが動作していない場合は、リンク回復をイネーブルまたはディセーブルにします。イネーブルにすると、クロスコネクタの切り替え、保護切り替え、またはアップグレードによって伝送損失が発生した場合に、リンクがリセットされます。	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Media Type	Transparent Generic Framing Protocol (GFP-T) フレームに対して適切なペイロード値を設定します。	<ul style="list-style-type: none"> <li>• Fibre Channel - 1 Gbps</li> <li>• Fibre Channel - 2 Gbps</li> <li>• FICON 1 Gbps</li> <li>• FICON 2 Gbps</li> <li>• Unknown</li> </ul>

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A439 FC\_MR-4 カードにあるポートの距離延長設定の変更

目的	この作業では、FC_MR-4 ポートの距離延長パラメータを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、ポートの設定を変更する FC\_MR-4 カードをダブルクリックします。

**ステップ 2** Provisioning > Port > Distance Extension 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 21-4 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。

ステップ 4 Apply をクリックします。

表 21-4 FC\_MR-4 カードにあるポートの距離延長設定

パラメータ	内容	オプション
Port	(表示専用) ポート番号	1 ~ 4
Enable Distance Extension	オンにすると、GFP-T ベースのフロー制御方式で距離を延長することができます。この機能によって、ノードを長距離 Storage Area Network (SAN; ストレージエリア ネットワーク) 内のリモート ノードにすることができます。オフにすると、その他のオプションは編集できなくなります。Distance Extension がイネーブルになっている場合は、接続されているファイバチャネルスイッチを、そのファイバチャネルスイッチに応じて、Interop または Open Fabric モードに設定します。FC_MR カードは、Cisco MDS ストレージ製品とデフォルトで相互動作できるようになっています。	—
Auto Detect Credits	オンにすると、ノードはリモート ノードからの伝送クレジットを検出できるようになります。クレジットは、リンクフロー制御に使用されます。また、ファイバチャネルや FICON スイッチ の E ポート間で Extended Link Protocol (ELP) のログインフレームに使用されます。	—
Credits Available	ELP ログイン フレームの設定がないか、または ELP ログイン フレームを検出できない場合に、クレジットの数を設定します。Credits Available は、Auto Detect Credits がオフになっている場合にだけ、変更できます。  <b>(注)</b> 接続されているデバイス間の距離が離れているほど、長距離リンクの遅延を補償するために必要なクレジット数が増加します。その値は、ファイバチャネルや FICON ポートでサポートされているクレジットの数と同じかそれより小さくしなければなりません。	数値。2 ~ 256 の範囲で 2 の倍数のみ。
Autoadjust GFP Buffer Threshold	オンにすると、SONET/SDH 転送に対して、帯域幅および遅延の点で最大の使用率が保証されます。	—
GFP Buffers Available	GFP バッファの深度を設定します。GFP Buffers Available は、Autoadjust GFP Buffer Threshold がオフになっている場合にだけ、変更できます。短い SONET 転送距離に対しては、遅延を少なくするために値を小さくすることを推奨します。長い SONET 転送距離に対しては、帯域幅を広くするために値を大きくすることを推奨します。	数値。16 ~ 1200 の範囲で 16 の倍数のみ。

ステップ 5 元の NTP (手順) に戻ります。

## DLP-A440 FC\_MR-4 カードにあるポートの拡張 FC/FICON 設定の変更

目的	この作業では、FC_MR-4 ポートの拡張 FC/FICON パラメータを変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、ポートの設定を変更する FC\_MR-4 カードをダブルクリックします。
- ステップ 2** Provisioning > Port > Enhanced FC/FICON 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 21-5](#) 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。
- ステップ 4** Apply をクリックします。

表 21-5 FC\_MR-4 カードにあるポートの距離延長設定

パラメータ	内容	オプション
Port	(表示専用) ポート番号	1 ~ 4
Ingress Idle Filtering	オンにすると、過剰なファイバ チャンネルコードや FICON IDLE コードを、SONET 転送から削除しないようにします。IDLE は、送信データがないときにフレーム間で送られるか、表示される 8b10b の制御ワードです。入力アイドルのフィルタリングは、フル回線速度のファイバ チャンネル転送や FICON 転送が可能な、SONET 回線の帯域幅サイズにだけ適用されます。これは、サードパーティ製の SONET 機器でリモートのファイバ チャンネルや FICON と相互運用させる場合にも使用できます。	—
Maximum Frame Size	有効なフレームの最大サイズを設定します。この設定によって、ファイバ チャンネルの最大値を超えるフレーム サイズに対して、サイズ超過の Performance Monitoring (PM; パフォーマンス モニタリング) が滞らないようにします。サイズの超過は、Cisco MDS 9000 スイッチで生成した Virtual SAN (VSAN; 仮想 SAN) タグがファイバ チャンネル フレームに追加されて発生することがあります。	数値。2148 ~ 2172。

**ステップ 5** 元の NTP（手順）に戻ります。

## DLP-A441 UBIC-H EIA での電気回路ケーブルの取り付け

目的	この作業では、UBIC-H EIA に DS-1 と DS-3/EC-1 ケーブルを取り付けます。
工具 / 機器	3/16 インチ フラットヘッド ドライバ DS-1 および DS-3/EC-1 ケーブル（必要に応じて） <ul style="list-style-type: none"> <li>• 15454-CADS1-H-25</li> <li>• 15454-CADS1-H-50</li> <li>• 15454-CADS1-H-75</li> <li>• 15454-CADS1-H-100</li> <li>• 15454-CADS1-H-150</li> <li>• 15454-CADS1-H-200</li> <li>• 15454-CADS1-H-250</li> <li>• 15454-CADS1-H-350</li> <li>• 15454-CADS1-H-450</li> <li>• 15454-CADS1-H-550</li> <li>• 15454-CADS1-H-655</li> <li>• 15454-CADS3-SD</li> <li>• 15454-CADS3-ID</li> <li>• 15454-CADS3-LD</li> </ul>
事前準備手順	<a href="#">DLP-A399 UBIC-H EIA の取り付け (p.20-113)</a>
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



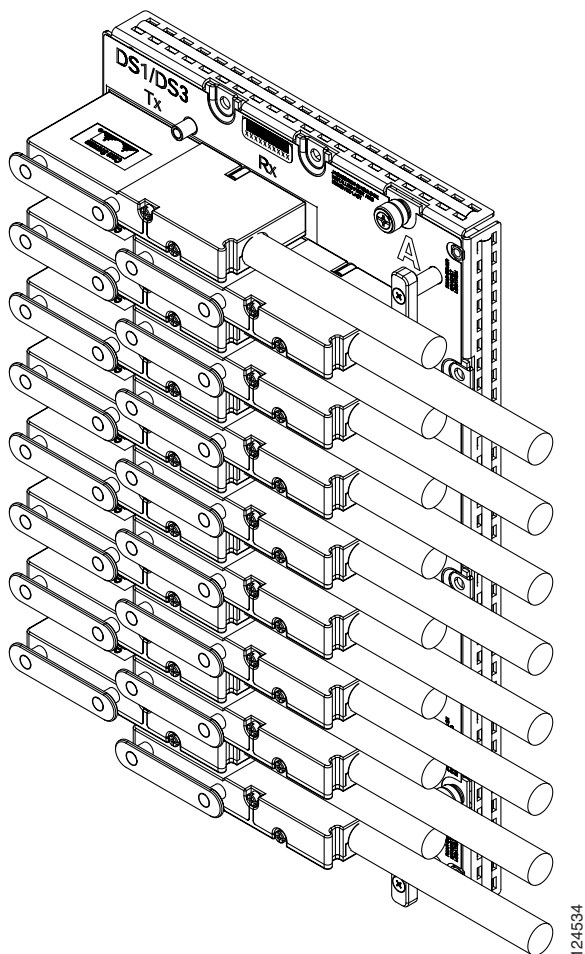
**(注)** 今後のスロットの使用状況を考慮して、今後使用するすべての SCSI コネクタにケーブルを取り付けることを推奨します。

- ステップ 1** ケーブル コネクタをバックプレーンの適切な接続箇所に配置し、ケーブルがシェルフの外側を通るようにします。
- ステップ 2** ケーブル コネクタのピンが UBIC-H のノッチにかみ合うまで、コネクタをバックプレーンに静かに押しこみます。UBIC-H のスタンドオフがケーブルのノッチに正しく合っていることを確認してください。
- ステップ 3** フラットヘッド ドライバを使用して、ネジをケーブル コネクタの端の上部および下部において、8 ~ 10 lbf-in (9.2 ~ 11.5 kgf-cm) で 2 ~ 3 回まわして、締めます。両方がぴったりと固定されるまで、2 本のネジを交互に締めます。

**ステップ 4** 取り付ける各ケーブルについて、ステップ 1 ~ 3 を繰り返します。

図 21-1 に、すべてのコネクタにケーブルが取り付けられた UBIC-H を示します。

図 21-1 すべてのケーブルが接続された UBIC-H (A 側)



**ステップ 5** 可能な場合は、Telcordia 標準 (GR-1275-CORE) または現地の状況に合わせて、ケーブルをタイラップするか撚り合わせます。



**(注)** 電気回路ケーブルを配線する際は、アラームおよびタイミングパネルの前に十分なスペースを空け、メンテナンス時に手が届くようにします。

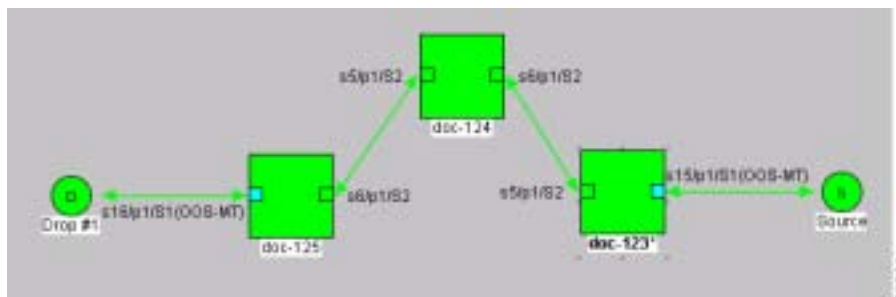
**ステップ 6** 元の NTP (手順) に戻ります。

## DLP-A442 バススルー回線の確認

目的	この作業では、ノードを経由する回線が同じ STS と VT (またはどちらか一方) でノードに出入りしていることを確認します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** CTC Circuits ウィンドウで、削除するノードを経由する回線を選択して、**Edit** をクリックします。
- ステップ 2** Edit Circuits ウィンドウで、**Show Detailed Map** をオンにします。
- ステップ 3** ノードのイーストポートとウェストポート上の STS および VT マッピングが同じであることを確認します。たとえば、回線のウェストポートのマッピングが s5/p1/S1 (スロット 5、ポート 1、STS 1) の場合、イーストポートのマッピングが STS 1 であることを確認します。回線のイーストとウェストポートで STS および VT (またはどちらか一方) が異なる場合は、その回線の名前を記録します。図 21-2 に、同じ STS (STS 2) でノード (doc-124) を経由する回線を示します。

図 21-2 バススルー STS の確認



- ステップ 4** Circuits タブの各回線について、ステップ 1 ~ 3 を繰り返します。
- ステップ 5** ステップ 3 で記録した各回線を削除して再作成します。回線を削除する際には、「[DLP-A333 回線の削除](#)」(p.20-23) を参照してください。回線を作成する際には、第 6 章「[回線と VT トンネルの作成](#)」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-A443 15454\_MRC-12 カードへのファイバクリップの取り付け

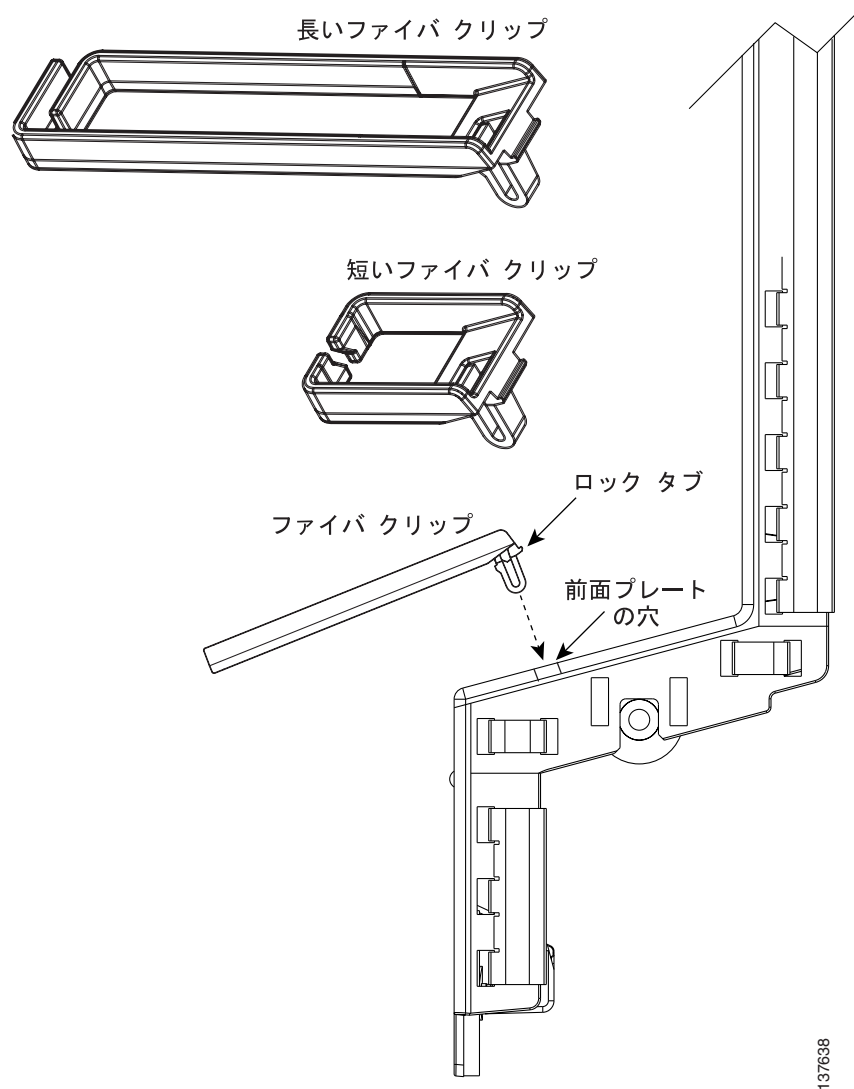
目的	この作業では、ファイバを適切に配線できるように、ファイバクリップを取り付けます。15454_MRC-12 カード (CTC では MRC-12) で必要です。
工具 / 機器	ファイバクリップ (必要に応じて長さを選択) 短いクリップ : 52-0629-01 長いクリップ : 52-0628-01
事前準備手順	<a href="#">NTP-A16 光カードおよびコネクタの取り付け (p.2-8)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイト
セキュリティ レベル	なし



(注) ファイバを 15454\_MRC-12 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 21-3](#) )。

図 21-3 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、ロック タブを押しながらクリップを前方上側に回します。

**ステップ 4** 元の NTP (手順) に戻ります。



## DLP-A444 MRC-12 カードでの PPM のプロビジョニング

目的	この作業では、MRC-12 カードでシングルレートおよびマルチレートの Pluggable Port Module ( PPM ) をプロビジョニングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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 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 ペインで、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 ペインに新規に作成されたポートが表示されます。Pluggable Port Modules ペインの行はライト 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 ペインのリストに 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-A445 MRC-12 カードでの光回線レートのプロビジョニング](#)」( p.21-28 )に進みます。
- ステップ 10** 元の NTP (手順) に戻ります。
-

## DLP-A445 MRC-12 カード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、MRC-12 PPM の光回線レートをプロビジョニングします。MRC-12 カード上の PPM がシングルレートかマルチレートかに関係なく、PPM に回線レートをプロビジョニングする必要があります。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 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 ペインで、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 番目の番号は PPM のポート番号を示します。たとえば、最初の PPM は 1-1、2 番目の PPM は 2-1 と表示されます。
  - Port Type — ドロップダウン リストで、ポートのタイプをクリックします。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。PPM タイプおよびレートに基づいて異なる可能性があります。MRC-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 21-6](#) を参照してください。

**表 21-6 PPM ポート タイプ**

カード	ポート タイプ
MRC-12	<ul style="list-style-type: none"> <li>OC-3 — 155 Mbps</li> <li>OC-12 — 622 Mbps</li> <li>OC-48 — 2.48 Gbps</li> </ul>

- 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 ペインの行はライト 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-A446 MRC-12 カード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 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 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 ペインで、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-A447 MRC-12 または OC192-XFP カードからの PPM の削除

目的	この作業では、MRC-12 または OC192-XFP カードの SFP に対する PPM 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、稼働中の場合、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-A154 1+1 保護グループの変更 \(p.18-24\)](#)
- [NTP-A85 ノードのタイミング変更 \(p.11-8\)](#)

- NTP-A292 通信チャネルの終端とプロビジョニング可能なパッチコードの変更または削除 (p.11-7)
- NTP-A151 回線の変更と削除 (p.7-5)
- NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除 (p.7-6)
- DLP-A214 ポートのサービス状態の変更 (p.19-10)

**ステップ 2** ノード ビューで、PPM 設定を削除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** 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。

- Pluggable Port Modules ペインに表示された 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。
- 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。
- Yes をクリックします。Pluggable Port Modules ペインおよび Pluggable Ports ペインから PPM プロビジョニングが削除されます。

**ステップ 5** PPM 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。
- 物理的に存在する SFP (PPM) の PPM プロビジョニングを削除した場合、CTC は削除状態に遷移して、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-A470 GBIC または SFP/XFP デバイスの取り外し」(p.21-68) 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-A448 DS3XM-6 カードまたは DS3XM-12 カードの 1:1 保護から 1:N 保護への変換

目的	この作業では、DS3XM-6 または DS3XM-12 カードを 1:1 保護から 1:N 保護に変換します。1:N 保護グループでは、最大で 5 つの現用カードを保護できます。
工具 / 機器	DS3XM-12 カード
事前準備手順	DS3XM-6 または DS3XM-12 カードの保護グループ 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
セキュリティ レベル	プロビジョニング以上のレベル



**(注)** この手順では、DS3XM-6 または DS3XM-12 のいずれかのカードがスロット 1 ~ 6 またはスロット 12 ~ 17 (またはその両方) に取り付けられていることを想定しています。保護スロットであるスロット 3 または 15 にある DS3XM-6 カードは、DS3XM-12 カードに置き換えられます。

- 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** スロット 3 または 15 を含む保護グループをクリックします。スロット 3 または 15 の 1:1 保護カードが DS3XM-6 カードの場合、**ステップ 3** に進みます。スロット 3 または 15 の 1:1 保護カードが DS3XM-12 カードの場合、**ステップ 5** に進みます。
- ステップ 3** アップグレードするスロットに現用トラフィックが流れていないことを確認します。Selected Group リストにある保護スロットのステータスは、Protect/Active ではなく、Protect/Standby になっている必要があります。保護スロットのステータスが Protect/Active になっている場合は、トラフィックを現用カードに切り替えます。
- Selected Group で、保護カードをクリックします。
  - Switch Commands の隣にある、**Switch** をクリックします。  
現用スロットのステータスが Working/Active に変わり、保護スロットのステータスが Protect/Standby に変わります。変わらない場合は、作業を続けしないでください。現用のカードとスロットにある問題を調べ、カードに現用トラフィックが流れない原因を突き止めてください。
- ステップ 4** 変換の必要な保護グループごとに、**ステップ 2** と **3** を繰り返します。
- ステップ 5** **Alarms** タブをクリックして、変換するどの DS3-12 カードにも未解決のアラームがないことを確認します。アラームが解除できない場合は、上位レベルのサポートに連絡してください。
- ステップ 6** **Provisioning > Protection** タブをクリックします。
- ステップ 7** 新しい保護グループへ移動するカードが含まれている 1:1 保護グループをクリックします。
- ステップ 8** **Delete** をクリックします。
- ステップ 9** 確認用のダイアログボックスが表示されたら、**Yes** をクリックします。



**(注)** 1:1 保護グループを削除しても、サービスは中断されません。ただし、1:N 保護の手順が完了するまでは、現用回線を保護するための帯域幅が存在しません。したがって、この手順はできるだけ早く完了させてください。

- ステップ 10** 複数の DS-3 1:1 保護グループを削除する場合は、1:N グループに含める各グループに対して**ステップ 7 ~ 9** を繰り返します。
- ステップ 11** スロット 3 または 15 の 1:1 保護カードが DS3XM-6 カードの場合、スロット 3 または 15 から保護 DS3-12 カードを物理的に取り外します。これにより、不適切な取り外し (IMPROPRMVL) のアラーム状態が発生します。スロット 3 または 15 の 1:1 保護カードが DS3XM-12 カードの場合、**ステップ 16** に進みます。
- ステップ 12** ノード ビューで、取り外されたカードが取り付けられていたスロットを右クリックして、ショートカット メニューから **Delete** を選択します。ノード ビューからカードが表示されなくなるまで待ちます。
- ステップ 13** DS3XM-12 カードを同じスロットへ物理的に挿入します。

**ステップ 14** カードが正常にブートすることを確認します。

**ステップ 15** **Inventory** タブをクリックして、新しいカードが DS3XM-12 カードとして表示されていることを確認します。

**ステップ 16** **Provisioning > Protection** タブをクリックします。

**ステップ 17** **Create** をクリックします。

**ステップ 18** **Name** フィールドに、保護グループの名前を入力します (任意)。

**ステップ 19** **Type** をクリックして、ドロップダウン リストから **1:N (card)** を選択します。

**ステップ 20** **Protect Card** フィールドに DS3XM-12 カードが表示されていることを確認します。

**ステップ 21** **Available Cards** リストで、保護グループに入れるカードを強調表示します。矢印(>>)タブをクリックして、カードを **Working Cards** リストへ移動します。

**ステップ 22** **OK** をクリックします。

Protection サブタブの **Protection Groups** リストに保護グループが表示されます。

**ステップ 23** 元の NTP (手順) に戻ります。

## DLP-A449 GNE 対応 SNMP の設定

目的	この手順では、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 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** — **Network Management System (NMS; 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 コミュニティ名を入力します(詳細については、『*Cisco ONS 15454 Reference Manual*』の「SNMP」の章を参照)。



(注) コミュニティ名は、認証とアクセス制御を組み合わせた形式で指定します。ONS 15454 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 (管理情報ベース) 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 レポート、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 を使用する場合は、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 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-A450 ENE 対応 SNMP の設定

目的	この手順では、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 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 コミュニティ名を入力します( 詳細については、『Cisco ONS 15454 Reference Manual』の「SNMP」の章を参照 )。



**(注)** コミュニティ名は、認証とアクセス制御を組み合わせた形式で指定します。ONS 15454 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 レポート、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** [Use Generic MIB] チェックボックスに関する情報を追加します。





(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 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** 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最大 3 つのリレーを設定して、SNMP トラップを NE から NMS に変換することができます。そのためには、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 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。このためには、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 の 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 のアドレスとコミュニティ名、および Relay B の NE 1 と Relay C の 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。また、次のパラメータも適用されます。

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

**ステップ 11** Apply をクリックします。

**ステップ 12** GNE と ENE 間のすべての NE に [ステップ 2 ~ 11](#) を繰り返します。

**ステップ 13** 元の NTP (手順) に戻ります。

## DLP-A451 SNMP コマンドまたは演算用の NMS コミュニティ スtringのフォーマット化および入力

目的	この手順では、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tringをフォーマットする方法を示します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 で SNMP [Get] (またはその他の演算) がイネーブルになっている場合は、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、認証とアクセス制御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 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] (またはその他の演算) がイネーブルになっている場合は、MIB ブラウザのコミュニティ名フィールドに入力する、フォーマット化されたスStringを作成します。ブラウザに対してこのスString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String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) をポート 161 から 192.168.7.4 に転送すると予測されます。発信 PDU のコミュニティ名は [net7node4] になります。このコミュニティ名は、アドレスが 192.168.7.4 の ENE で有効です。

- フォーマット化されたコミュニティ スString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 をデフォルト ポート (ポート 161) から 192.168.7.99 に転送すると予測されます。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 をポート 161 (ENE 上) から 192.168.9.6 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 で有効であり、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 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 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tring 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-A452 VLAN の作成

目的	この作業では、新規 VLAN を作成します。
工具 / 機器	なし
事前準備手順	回線の作成手順については、 <a href="#">第 6 章「回線と VT トンネルの作成」</a> 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	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** Tools メニューから、**Manage VLANS** を選択します。

**ステップ 3** All VLANs ダイアログボックスで **Create** をクリックします。

**ステップ 4** Define New VLAN ダイアログボックスで、次のように設定します。

- VLAN Name — VLAN に、簡単に識別できる名前を割り当てます。
- VLAN ID — VLAN の ID を割り当てます。VLAN に割り当てる ID は、2 ~ 4093 の範囲で既存の VLAN にはまだ割り当てられていない、次の使用可能な数値でなければなりません。1 つの ONS 15454 ネットワークがサポートする、ユーザ プロビジョニング可能な VLAN の最大数は 509 です。
- Topology Host — ドロップダウン リストからトポロジー ホストとして機能するノードを選択します。トポロジー ホストは、VLAN トポロジーの検出に使用されます。デフォルトはログイン ノードです。

**ステップ 5** **OK** をクリックします。

**ステップ 6** **Close** をクリックします。

**ステップ 7** 元の NTP (手順) に戻ります。

---

## DLP-A453 サーバ証跡の削除

目的	この作業では、サーバ証跡を削除します。
工具 / 機器	なし
事前準備手順	<a href="#">NTP-A326 サーバ証跡の作成 (p.6-111)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > Server Trails** タブをクリックします。
- ステップ 3** 削除するサーバ証跡をクリックします。
- ステップ 4** **Delete** をクリックします。
- ステップ 5** 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** 元の NTP (手順) に戻ります。
- 

## DLP-A454 BLSR STS スケルチ テーブルの表示

目的	この作業では、ONS 15454 BLSR ノードの BLSR STS スケルチ テーブルを表示できます。たとえば、ファイバ切断が発生した場合、BLSR STS スケルチ テーブルには、切り離されたそれぞれのノードに対してスケルチされる STS が表示されます。スケルチにより、適切な Alarm Indication Signal Path (AIS-P) を挿入してトラフィックが置き換えられます。これにより、トラフィックの接続ミスを防ぎます。VT アクセス チェック マーク付き STS では、100 ms 後に AIS-P が削除されます。BLSR のスケルチ機能の詳細については、Telcordia GR-1230 を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 ビューでスケルチ テーブルを開くには、次の手順を実行します。
- ノード ビューで、**Provisioning > BLSR** タブをクリックします。
  - スケルチ テーブルを表示する BLSR をクリックします。
  - Squelch Table** をクリックします。

**ステップ 2** ネットワーク ビューでスケルチ テーブルを開くには、次の手順を実行します。

- a. ネットワーク ビューで、**Provisioning > BLSR** タブをクリックします。
- b. スケルチ テーブルを表示する BLSR をクリックします。
- c. **Edit** をクリックします。
- d. **Edit** ウィンドウでノードを右クリックします。
- e. ドロップダウン リストから **Squelch Table** を選択します。

**ステップ 3** BLSR Squelch Table ウィンドウに、次の情報が表示されます。

- STS Number — BLSR STS の数を表示します。2 ファイバ BLSR の場合、STS の数は BLSR OC-N の半分です。たとえば、OC-48 BLSR のスケルチ テーブルは 24 の STS を表示します。4 ファイバ BLSR の場合、テーブルの STS 数は BLSR OC-N と同じです。
- West Source — トラフィックをノードのウェスト スパンで受信している場合に、送信元の BLSR ノード ID が表示されます (リングに存在するすべてのノードの BLSR ノード ID を表示する場合は、**Ring Map** ボタンをクリックします)。
- West VT (from the West Source) — チェックマークは、STS が受信 VT トラフィックを伝送していることを示します。トラフィックの送信元は、ウェスト側から受信されます。
- West VT (from the West Destination) — チェックマークは、STS が発信 VT トラフィックを伝送していることを示します。トラフィックは、ウェスト側でドロップされます。
- West Dest — トラフィックをノードのウェスト スパンから送信している場合に、宛先の BLSR ノード ID が表示されます。
- East Source — トラフィックをノードのイースト スパンで受信している場合に、送信元の BLSR ノード ID が表示されます。
- East VT (from the East Source) — チェックマークは、STS が受信 VT トラフィックを伝送していることを示します。トラフィックの送信元は、イースト側から受信されます。
- East VT (from the East Destination) — チェックマークは、STS が発信 VT トラフィックを伝送していることを示します。トラフィックは、イースト側でドロップされます。
- East Dest — トラフィックをノードのイースト スパンから送信している場合に、宛先の BLSR ノード ID が表示されます。



**(注)** BLSR のスケルチ機能は、STS 回線のトラフィックのみを伝送する STS で実行されます。マルチカードの Ethergroup にプロビジョニングされた E シリーズ イーサネットカードに送受信される VT 回線またはイーサネット回線のトラフィックを伝送する STS では、スケルチ テーブルのエントリは表示されません。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A455 BLSR VT スケルチ テーブルの表示

目的	BLSR VT スケルチ テーブルは、BLSR から VT を廃棄しているノードでのみ表示され、ノードが切り離されているときに VT レベルのスケルチの実行に使用されます。VT スケルチは、ONS 15454 および ONS 15327 プラットフォームでサポートされます。  ONS 15600 プラットフォームは VT スケルチをサポートしません。ただし、ONS 15454 および ONS 15600 が同一ネットワークに存在する場合、ONS 15600 ノードにより、ONS 15454 ノードは VT トンネルの VT 回線を伝送できます。ONS 15600 は、ノードの障害時に切り替え中のノードで各 VT アクセス STS に対して 100 ms STS レベルのスケルチを実行します。BLSR のスケルチ機能の詳細については、Telcordia GR-1230 を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 ビューでスケルチ テーブルを開くには、次の手順を実行します。

- ノード ビューで、**Provisioning > BLSR** タブをクリックします。
- スケルチ テーブルを表示する **BLSR** をクリックします。
- Squelch Table** をクリックします。

**ステップ 2** ネットワーク ビューでスケルチ テーブルを開くには、次の手順を実行します。

- ネットワーク ビューで、**Provisioning > BLSR** タブをクリックします。
- スケルチ テーブルを表示する **BLSR** をクリックします。
- Edit** をクリックします。
- Edit** ウィンドウでノードを右クリックします。
- ドロップダウン リストで **Squelch Table** をクリックします。

**ステップ 3** BLSR STS Squelch Table ウィンドウで、VT チェックマークをダブルクリックします。BLSR VT Squelch Table ウィンドウに、次の情報が表示されます。



**(注)** チェックマークは、各 VT アクセス STS に表示されます。ただし、VT スケルチ テーブルは、VT を廃棄するノード上のチェックマークをダブルクリックしたときにだけ表示されます。VT の中間ノードには、VT スケルチ テーブルは保持されません。

- VT Number — BLSR VT の数を表示します。VT の数には、VT グループおよびチャネルが含まれます (VT グループ 2 およびチャネル 1 は、2-1 と表示されます)。
- West Source — トラフィックをノードのウェスト スパンで受信している場合に、送信元の BLSR ノード ID が表示されます (リングに存在するすべてのノードの BLSR ノード ID を表示する場合は、**Ring Map** ボタンをクリックします)。

- East Source — トラフィックをノードのイースト スパンで受信している場合に、送信元の BLSR ノード ID が表示されます。

**ステップ 4** 元の NTP (手順) に戻ります。

## DLP-A456 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>  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があります。RADIUS サーバの設定手順については、『 <i>User Guide for Cisco Secure ACS for Windows Server</i> 』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



### 注意

ノードに RADIUS 認証を設定する前に、目的のノードを RADIUS サーバに追加し、RADIUS サーバを認証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)

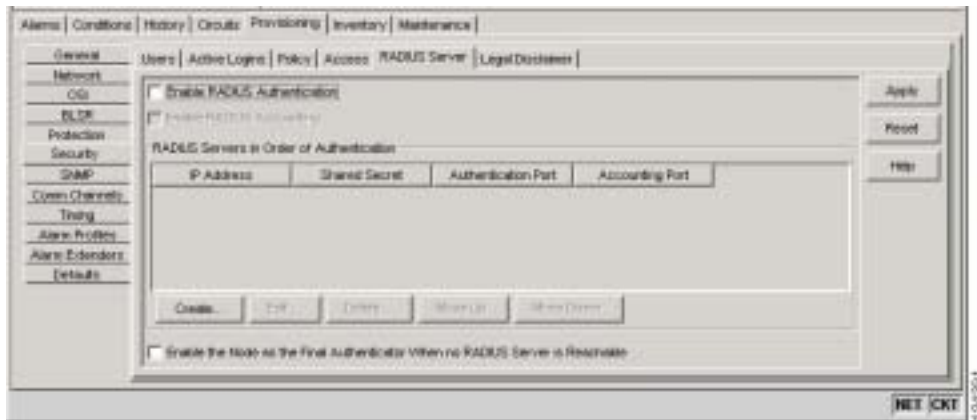
RADIUS サーバにユーザを追加する場合は、次の Cisco Vendor-Specific Attribute (VSA; ベンダー固有属性) を指定する必要があります。

shell:priv-lvl=N。N の値は次のとおりです。

- 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 21-4](#) )。

図 21-4 RADIUS サーバタブ



**ステップ 2** Create をクリックして、認証リストに 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 21-5)。

図 21-5 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 ENE の場合は、このフィールドに GNE 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 フィールドに共有シークレットを入力します。共有シークレットは、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文字列です。

**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、共有シークレット、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。あるサーバが到達不能であった場合、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、ユーザをロックアウトせずに、ノードが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-A457 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 ユーザによる監査ログの検索、データベースの復元、ソフトウェア ロードの有効化および復帰といった作業の実行をイネーブルにします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 > 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** 変更しているデフォルト プロパティの Default Value カラムをクリックし、ドロップダウン リストから 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って変更されることにな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) 現在の CTC セッションを閉じ、変更を反映させるために新規 CTC セッションを再起動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-A459 OC-192 および MRC-12 カードの光スレッシュホールド設定の変更

目的	この作業では、OC-192 および MRC-12 カードの光スレッシュホールド設定を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、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。



(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 3** 変更するフィールドをクリックして、表 21-7 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。

**ステップ 4** Apply をクリックします。

表 21-7 光スレッシュホールドの設定

パラメータ	内容	オプション
Port	(表示専用) ポート番号	<ul style="list-style-type: none"> <li>1 (OC-192、OC192-XFP)</li> <li>1 ~ 12 (MRC_12)</li> </ul>
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	送信光パワー (最小)	デフォルト (15 分 / 1 日): 80%
OPT-HIGH	送信光パワー (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。受信側のパワーが減少すると、受信側のパワーの損失を反映して OPR の割合が小さくなります。たとえば、受信側パワーが 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	アラームまたは TCA 応答をトリガーする、アラートのスレッシュホールド値を設定します。Alarm または TCA を生成するプロビジョニング可能なスレッシュホールドを表示するには、タイプを選択してから Refresh をクリックします。	<ul style="list-style-type: none"> <li>TCA (スレッシュホールド超過アラート)</li> <li>Alarm</li> </ul>
Intervals	パラメータ数を収集する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。	<ul style="list-style-type: none"> <li>15 Min</li> <li>1 Day</li> </ul>

**ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A460 CTC でのトラフィック カードのリセット

目的	この作業では、光カード、電気回路カード、E シリーズ、G シリーズ、ML シリーズ、または CE-1000-4 の各イーサネット カードを CTC でリセットします。CE100T-8 イーサネット カードには、専用のリセット作業があります。詳細については、「 <a href="#">DLP-A54 CTC を使用した CE-100T-8 カードのハードリセット</a> 」(p.17-68) または「 <a href="#">DLP-A224 CTC を使用した CE-100T-8 カードのソフトリセット</a> 」(p.19-19) を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン</a> (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)

トランスポンダ (TXP) またはマックスポンダ (MXP) カードのリセットについては、『*Cisco ONS 15454 DWDM Procedure Guide*』を参照してください。



注意

保護グループの一部である現用電気回路カードをソフト リセットした場合、カードのリポート中に、リセット現用電気回路カードを保護しているカードまたは保護カードのロックを解除しないでください。ロックを解除すると、トラフィック損失が発生します。保護カード上での保護でロックアウトを戻したり、現用カード上でロックオンを戻したりする前に、現用電気回路カードのリポートが完全に終わるまで待機してください。これは、E1-42 カードを除くすべての電気回路カードにもあてはまります。

- 
- ステップ 1** ノード ビューで、トラフィック カードのスロットの上にカーソルを置きます。
- ステップ 2** カードを右クリックして、ショートカット メニューから **Reset Card** を選択します。
- ステップ 3** Resetting 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-A461 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 および OC192-XFP カードに SFP/XFP を事前プロビジョニングします。SFP/XFP は CTC では PPM として表されます。シスコ認定の OC-3、OC-12、OC-48、OC-192、およびマルチレート PPM は、ONS 15454 と互換性があります。リストについては、表 21-9 を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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 カードに SFP を取り付ける前に、『Cisco ONS 15454 Reference Manual』の MRC-12 に関するセクションを参照し、SFP を取り付けるポートおよび使用中のクロスコネクタ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-A444 MRC-12 カードでの PPM のプロビジョニング』(p.21-27) 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。
- 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-A227 アラーム フィルタリングのディセーブル化』(p.19-21) を参照してください。
  - 説明のつかない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。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。
  - 『DLP-A532 CTC データのエクスポート』(p.22-35) 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 ペインで、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 ペインに新規に作成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 ペインの行はライト 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、ペインの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 ペインのリストに 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** 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 9** OK をクリックします。
- ステップ 10** SFP/XFP を取り付ける準備ができたなら、「[DLP-A469 GBIC または SFP/XFP デバイスの取り付け](#)」(p.21-64) を行います。
- ステップ 11** 元の NTP (手順) に戻ります。

## DLP-A462 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	<a href="#">DLP-A60 CTC へのログイン</a> (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	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 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-A463 特定の光回線の送信元または宛先のロール

目的	この作業では、トラフィックを特定の送信元または宛先から同じ回線上の別の送信元または宛先に再ルーティングして、元の送信元または宛先を変更します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Circuits タブをクリックします。

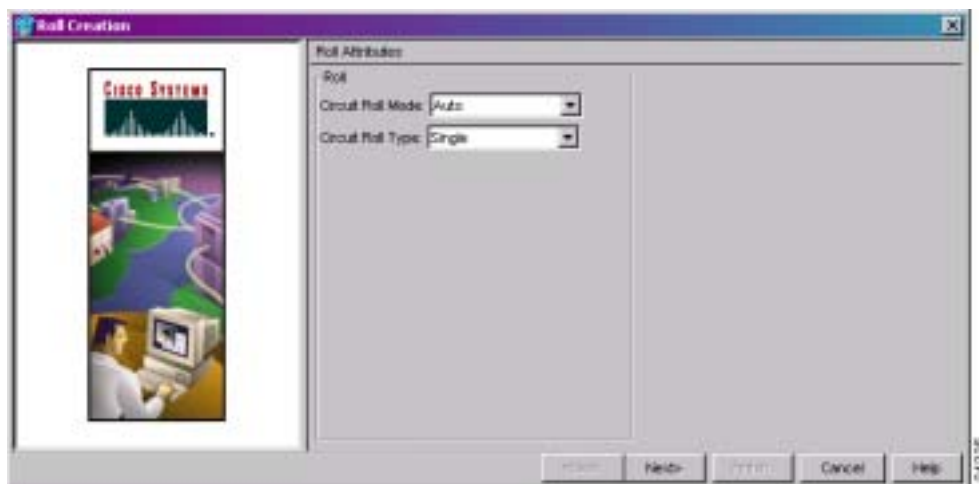
**ステップ 3** ロールする回線をクリックします。ロールを開始するには、回線のステータスが DISCOVERED でなければなりません。

**ステップ 4** Tools メニューから、**Circuits > Roll Circuit** を選択します。

**ステップ 5** Roll Attributes 領域で、次の手順を実行します ( [図 21-6](#) )。

- Circuit Roll Mode ドロップダウン リストで **Auto** を選択して、自動ロール (1 方向送信元ロールの場合に必要) を作成するか、または **Manual** を選択して、手動ロール (1 方向宛先ロールの場合に必要) を作成します。
- Circuit Roll Type ドロップダウン リストで **Single** をクリックして、選択した回線上でクロスコネクタを 1 つロールするように指定します。

**図 21-6 単一ロールアトリビュートの選択**

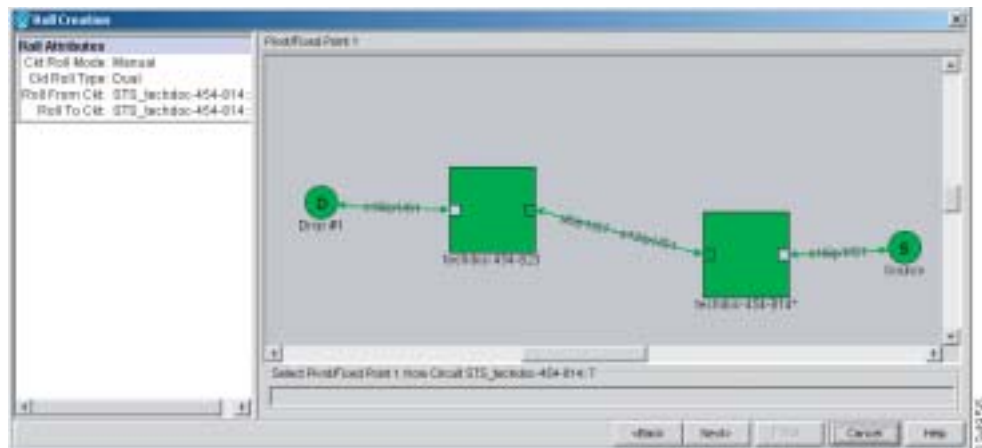


**ステップ 6** Next をクリックします。

**ステップ 7** Pivot/Fixed Point 1 ウィンドウのグラフィック イメージで、保持するファシリティを表す正方形をクリックします (図 21-7)。

このファシリティは、ロール プロセスに関連するクロスコネクットの固定位置を示します。グラフィック イメージの下にあるテキスト ボックスに ID が表示されます。選択されていないファシリティは、Roll From パスです。ロールを実行すると、Roll From パスは削除されます。

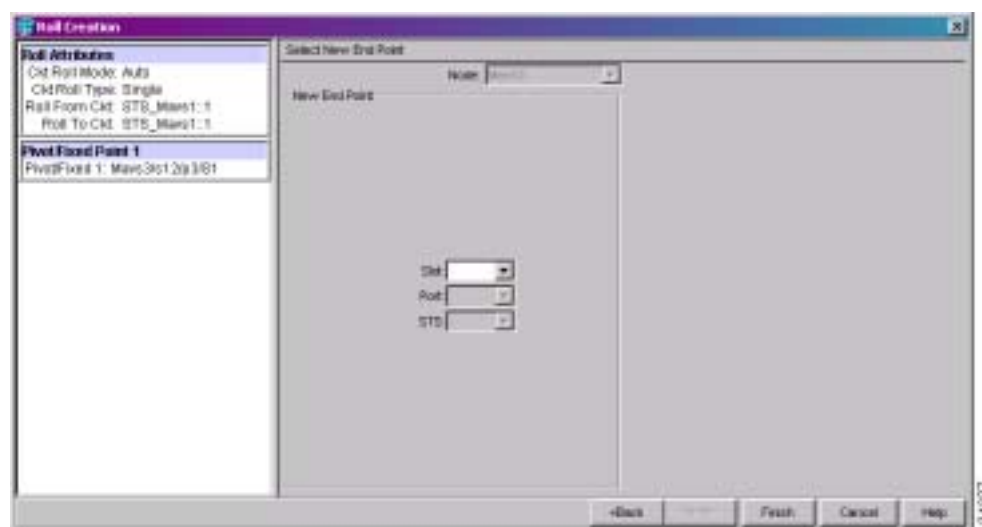
図 21-7 バスの選択



**ステップ 8** Next をクリックします。

**ステップ 9** Select New End Point 領域のドロップダウン リストで、Slot、Port、および STS を選択して、Roll To ファシリティを選択します (図 21-8)。

図 21-8 新しいエンドポイントの選択



**ステップ 10** Finish をクリックします。Circuits タブで Roll From ポートの回線ステータスが、DISCOVERED から ROLL\_PENDING に変わります。



**ステップ 11** Rolls タブをクリックします (図 21-9)。保留中のロールの Roll Valid Signal ステータスを表示します。次のいずれかの条件が満たされる場合は、**ステップ 12**に進みます。

- Roll Valid Signal ステータスが true である場合に、新しいポート上で有効な信号が検出されている。
- Roll Valid Signal ステータスが false である場合に、有効な信号が検出されていない。信号が検出されるまで待機してから、次のステップに進みます。信号が検出されない場合は、『Cisco ONS 15454 Troubleshooting Guide』の「Circuits and Timing」を参照してください。ロールをキャンセルするには、「DLP-A489 ロールのキャンセル」(p.21-69)を参照してください。
- ロールが 1 方向宛先ロールであり、Roll Valid Signal が false である。1 方向宛先ロールの場合は、Roll Valid Signal ステータスが true になることはありません。



**(注)** 有効な信号が検出されたあとに、自動ロールをキャンセルすることはできません。

- Force Valid Signal ボタンを使用して、Roll To 回線に信号を強制的に送ることができる。Force Valid Signal を選択した場合、ロール実行時の回線の反対側の状態によっては、ロールに関連する回線でトラフィックが廃棄されることがあります。回線上に信号がない場合、または信号が不良な場合に、ロールを実行するには、信号を強制的に送る必要があります。



**(注)** マニュアル モードで 1 方向宛先ロールを実行する場合、有効な信号を強制的に送る必要はありません。

図 21-9 Rolls タブの表示



**ステップ 12** ステップ 5 で Manual を選択した場合は、Rolls タブでロール済みのファシリティをクリックしてから、Complete をクリックします。Auto を選択した場合は、**ステップ 13**に進みます。

**ステップ 13** 手動ロールと自動ロールのいずれの場合も、Finish をクリックして、回線ロール プロセスを完了します。Rolls タブのロールがクリアされ、Circuits タブでロール済み回線のステータスが DISCOVERED と表示されます。

**ステップ 14** 元の NTP (手順) に戻ります。

## DLP-A464 光回線間での単一クロスコネクットのロール

目的	この作業では、特定の回線上のクロスコネクットを別の回線に再ルーティングして、新しい宛先を設定します。
工具 / 機器	なし
事前準備手順	DLP-A60 CTC へのログイン ( p.17-71 ) DLP-A156 SDCC 終端の削除 ( p.18-25 ) ( ロールに関連するポートに対して )
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** Circuits タブをクリックします。

**ステップ 3** Ctrl キーを押しながら、ロール プロセスで使用する回線を 2 つクリックします。

回線のステータスはどちらも DISCOVERED でなければなりません。また、ロールを開始するには、これらの回線のサイズと方向が同じである必要があります。設定された Roll To 回線で、トラフィックが伝送されているではありません。Roll To ファシリティは、Roll To 回線の送信元ノードに DCC 接続されている必要があります。

**ステップ 4** Tools メニューから、Circuits > Roll Circuit を選択します。

**ステップ 5** Roll Attributes 領域で、次の手順を実行します ( 図 21-10 )。

- Circuit Roll Mode ドロップダウン リストで、Auto を選択して、自動ロール ( 1 方向送信元ロールの場合に必要 ) を作成するか、または Manual を選択して、手動ロール ( 1 方向宛先ロールの場合に必要 ) を作成します。
- Circuit Roll Type ドロップダウン リストで、Single をクリックして、Roll From 回線から Roll To 回線に接続を 1 つロールするように指定します。
- Roll From Circuit 領域で、Roll From 接続を含む回線をクリックします。

図 21-10 別の回線に割り当てる単一ロールのロール アトリビュートの選択



**ステップ 6** Next をクリックします。

**ステップ 7** Pivot/Fixed Point 1 ウィンドウで、保持するファシリティを表す正方形をクリックします ( [図 21-7](#) )。

このファシリティは、ロール プロセスに関連するクロスコネクットの固定位置を示します。グラフィック イメージの下にあるテキスト ボックスに ID が表示されます。選択されていないファシリティは、Roll From パスです。ロールを実行すると、Roll From パスは削除されます。

**ステップ 8** Next をクリックします。

**ステップ 9** Select New End Point 領域のドロップダウン リストで、Slot、Port、および STS を選択して、ロール中の接続上の Roll To ファシリティを指定します。

**ステップ 10** Finish をクリックします。

Circuits タブの Roll From 回線および Roll To 回線のステータスが、DISCOVERED から ROLL\_PENDING に変わります。

**ステップ 11** Rolls タブをクリックします。保留中のロールの Roll Valid Signal ステータスを表示します。次のいずれかの条件が満たされる場合は、[ステップ 12](#) に進みます。

- Roll Valid Signal ステータスが true である場合に、新しいポート上で有効な信号が検出されている。
- Roll Valid Signal ステータスが false である場合に、有効な信号が検出されていない。信号が検出されるまで待機してから、次のステップに進みます。信号が検出されない場合は、『Cisco ONS 15454 Troubleshooting Guide』の「Circuits and Timing」を参照してください。ロールをキャンセルするには、『[DLP-A489 ロールのキャンセル](#)」(p.21-69)を参照してください。
- ロールが 1 方向宛先ロールであり、Roll Valid Signal が false である。1 方向宛先ロールの場合は、Roll Valid Signal ステータスが true になることはありません。



**(注)** 有効な信号が検出されたあとに、自動ロールをキャンセルすることはできません。

- Force Valid Signal ボタンを使用して、有効な信号がなくても、Roll To Circuit の宛先にロールを強制実行することができる。Force Valid Signal を選択した場合、ロールを実行すると、ロールに関連する回線でトラフィックが廃棄されます。

**ステップ 12** [ステップ 5](#) で Manual を選択した場合は、Rolls タブでロールをクリックしてから、Complete をクリックして、新しいポートにトラフィックをルーティングします。Auto を選択した場合は、[ステップ 13](#) に進みます。

**ステップ 13** 手動ロールと自動ロールのいずれの場合も、Finish をクリックして、回線ロール プロセスを完了します。

Rolls タブのロールがクリアされて、Circuits タブではロール済みの新規回線のステータスが DISCOVERED に戻ります。

**ステップ 14** 元の NTP (手順) に戻ります。

## DLP-A465 自動ルーティングを使用した単一光回線への 2 つのクロスコネクットのロール

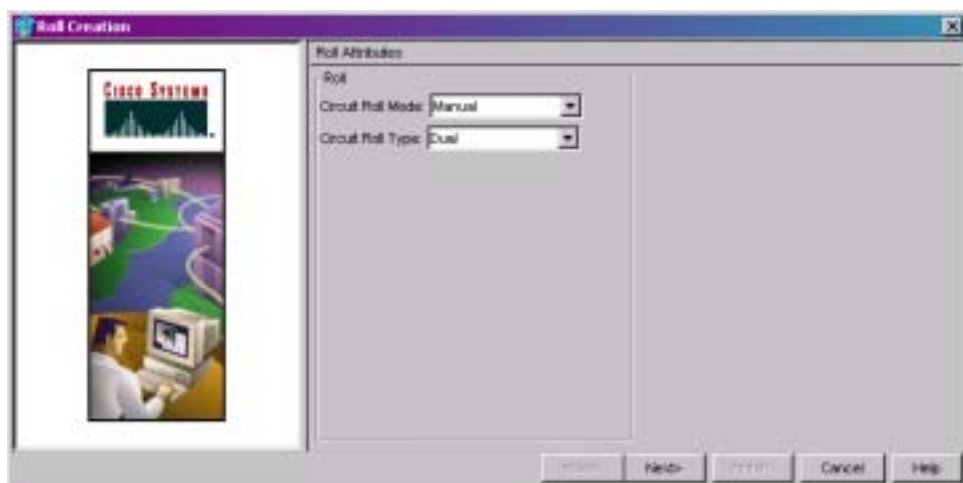
目的	この作業では、同じ送信元および宛先を維持しながら、ネットワークパスを再ルーティングします。CTC は Roll To パスを自動的に選択できます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	プロビジョニング以上のレベル



(注) この作業では、任意で自動ルーティングを使用します。Automatic Circuit Routing NE のデフォルトと Network Circuit Automatic Routing Overridable NE のデフォルトが、ともに FALSE に設定されている場合、自動ルーティングは使用できません。これらのデフォルトの詳細説明については、『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** View メニューから、**Go To Network View** を選択します。
- ステップ 2** **Circuits** タブをクリックします。
- ステップ 3** ロールする接続を含む回線をクリックします。ロールを開始するには、回線ステータスが DISCOVERED でなければなりません。
- ステップ 4** Tools メニューから、**Circuits > Roll Circuit** を選択します。
- ステップ 5** Roll Attributes 領域で、次の手順を実行します ( [図 21-11](#) )。
  - a. Circuit Roll Mode ドロップダウン リストで、**Auto** を選択して自動ロールを作成するか、または **Manual** を選択して手動ロールを作成します。
  - b. Circuit Type ドロップダウン リストで **Dual** をクリックして、選択した回線上で接続を 2 つロールするように指定します。

図 21-11 デュアル ロール アトリビュートの選択



**ステップ 6** Next をクリックします。

**ステップ 7** Pivot/Fixed Point 1 ウィンドウで、ロールする最初の接続の固定パスを表す正方形をクリックします (図 21-7)。

このパスは、ロール プロセスに関連するクロスコネクト内での固定位置を示します。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。選択されていないパスには、Roll From パスが含まれます。ロールを実行すると、Roll From パスは削除されます。

**ステップ 8** Next をクリックします。

**ステップ 9** 次のいずれかを行います。

- 複数の Roll From パスが存在する場合は、Select Roll From ダイアログボックスが表示されます。トラフィックのロール元となるパスを選択し、OK をクリックします。
- 複数の Roll From パスが存在しない場合は、ステップ 10 に進みます。Roll To パスの回線ステータスが、DISCOVERED から ROLL\_PENDING に変わります。

**ステップ 10** Pivot/Fixed Point 2 ウィンドウで、ロールする 2 番目の接続の固定パスを表す正方形をクリックします。

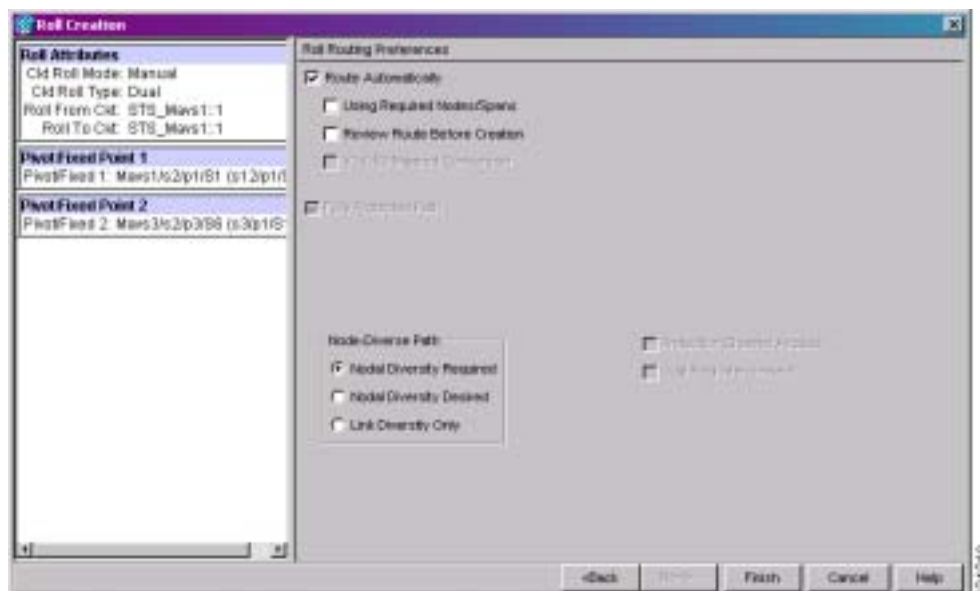
選択されていないパスは、Roll From パスです。ロールを実行すると、Roll From パスは削除されます。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。

**ステップ 11** Next をクリックします。

**ステップ 12** Circuit Routing Preferences 領域で、Route Automatically をオンにして、ルートを自動検索します (図 21-12)。Route Automatically をオンにした場合は、次のオプションを選択できます。

- Using Required Nodes/Spans — オンにした場合は、CTC が生成した回線ルートに含める、または除外するノードとスパンを指定できます (ステップ 15)。
- Review Route Before Creation — オンにした場合は、回線を作成する前にその回線ルートを確認して編集することができます。

図 21-12 ロール ルーティングのプリファレンス設定



**ステップ 13** 保護されているパスで回線をルーティングする場合は、**Fully Protected Path** をオンにします（保護されたパスで回線をルーティングしない場合は、**ステップ 14** へ進みます）。CTC は、次に示すノード ダイバーシティ オプションに基づいて、プライマリ回線ルートおよび代替回線ルート（仮想 UPSR）を作成します。次の選択肢から 1 つを選択し、表示されるウィンドウ プロンプトに従ってルーティングを実行します。

- Nodal Diversity Required — 完全回線パスの Path-Protected Mesh Network (PPMN; パス保護メッシュ ネットワーク) 部分にあるプライマリ パスと代替パスを、ノード ダイバーシティ にします。
- Nodal Diversity Desired — ノード ダイバーシティ を試行するように指定します。ただし、ノード ダイバーシティ ができない場合、CTC は完全回線パスの PPMN 部分にリンク ダイバーシティ パスを作成します。
- Link Diversity Only — 完全回線パスの PPMN 部分にあるプライマリ パスと代替パスにはリンク ダイバーシティ だけが必要であることを指定します。パス全体がノード ダイバーシティ になっていても、CTC ではそのことをチェックしません。

**ステップ 14** **ステップ 12** で Route Automatically をオンにした場合は、次のサブステップを実行します。

- Using Required Nodes/Spans をオンにした場合は、**ステップ 15** に進みます。
- Review Route Before Creation のみをオンにした場合は、**ステップ 16** に進みます。
- Using Required Nodes/Spans または Review Route Before Creation をオンにしなかった場合は、**ステップ 17** に進みます。

**ステップ 15** **ステップ 12** で Using Required Nodes/Spans を選択した場合は、次のサブステップを実行します。

- a. Roll Route Constraints 領域の回線マップで、ノードまたはスパンをクリックします。
- b. 回線にそのノードまたはスパンを含める場合は、**Include** をクリックします。回線からそのノードまたはスパンを除外する場合は、**Exclude** をクリックします。含めるノードおよびスパンを選択した順序によって、回線の順序が設定されます。回線の方向を変更する場合は、スパンを 2 回クリックします。
- c. 含めたり除外したりするノードまたはスパンごとに、**ステップ b** を繰り返します。
- d. 回線のルートを確認します。回線のルーティング順序を変更する場合は、Required Nodes/Lines リストまたは Excluded Nodes Links リストでノードを選択し、**Up** または **Down** ボタンをクリックして、回線のルーティング順序を変更します。ノードまたはスパンを削除する場合は、**Remove** をクリックします。

**ステップ 16** **ステップ 12** で Review Route Before Creation を選択した場合は、次のサブステップを実行します。

- a. Roll Route Review and Edit 領域で、回線ルートを確認します。回線のスパンを追加または削除する場合は、回線のルートにあるノードを選択します。ブルーの矢印で回線のルートが示されます。グリーン矢印は、追加できるスパンを表しています。スパンの矢印部分をクリックしてから、**Include** をクリックしてスパンを含めるか、**Remove** をクリックしてスパンを削除します。
- b. プロビジョニングした回線が予定のルートと設定を反映していない場合は **Back** をクリックし、回線の情報を確認して変更します。

**注意**

次のようになるのは、回線の両端でここに記載されたカードが使用されていて、DUAL ロール モードの場合のみです。終端カードが DS1/E1-56、DS1-14、DS1-N-14、DS3XM-6、または DS3XM-12 カードの場合は、Roll To ポートで有効な信号が検出されなくても、ロールが実行されます。Loss of Signal (LOS; 信号損失)、Loss of Frame Alignment (LOF)、および AIS (アラーム表示信号) 回線障害に関する ペイロード障害表示パス (PDI-P) ダウンストリームが存在しない場合は、有効な信号がなくても、ロールは継続します。DS1/E1-56、DS1-14、および DS1-N-14 カードの場合、Send AIS-V For Ds1 AIS チェックボックスをオンにして、LOS および LOF AIS 回線障害の PDI-P ダウンストリームを正常に生成させることができます。このチェックボックスは、カード ビューの Provisioning > Line タブで選択されます。DS1-14 および DS1-N-14 カードの場合、Send AIS-V for Ds1 AIS は VT 回線にのみ機能します。DS1/E1-56 カードの場合、Send AIS-V for Ds1 AIS は STS および VT 回線の両方に機能します。

**ステップ 17** Finish をクリックします。

Circuits タブで、新しい回線が表示されたことを確認します。この回線は Roll To 回線です。この回線には、Roll From 回線名に ROLL\*\* を付加した名前が付けられます。

**ステップ 18** Rolls タブをクリックします。新しいロールが 2 つ表示されます。保留中のロールごとに、Roll Valid Signal ステータスを表示します。次のいずれかの条件が満たされる場合は、[ステップ 19](#) に進みます。

- Roll Valid Signal ステータスが true である場合に、新しいポート上で有効な信号が検出されている。
- Roll Valid Signal ステータスが false である場合に、有効な信号が検出されていない。信号が検出されるまで待機してから、次のステップに進みます。有効な信号が検出されなかった場合は、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。ロールをキャンセルするには、『DLP-A489 ロールのキャンセル』(p.21-69) を参照してください。
- ロールが 1 方向宛先ロールであり、Roll Valid Signal ステータスが false である。1 方向宛先ロールの場合は、Roll Valid Signal ステータスが true になることはありません。



**(注)** ロールを完了した場合、片方のロールをキャンセルすることはできません。2 つのロールは同時にキャンセルする必要があります。



**(注)** 有効な信号が検出されたあとに、自動ロールをキャンセルすることはできません。

- Force Valid Signal ボタンを使用して、有効な信号がなくても、Roll To Circuit の宛先にロールを強制実行することができる。Force Valid Signal を選択した場合、ロールを実行すると、ロールに関連する回線でトラフィックが廃棄されます。

**ステップ 19** [ステップ 5](#) で Manual を選択した場合は、Rolls タブで両方のロールをクリックしてから、Complete をクリックして、新しいポートにトラフィックをルーティングします。Auto を選択した場合は、[ステップ 20](#) に進みます。

**(注)** 片方のロールをキャンセルした場合は、ロールを完了できません。2 つのロールは同時に完了する必要があります。

## ■ DLP-A466 手動ルーティングを使用した単一光回線への 2 つのクロスコネクタのロール

**ステップ 20** 手動ロールと自動ロールのいずれの場合も、**Finish** をクリックして、回線ロール プロセスを完了します。

**ステップ 21** 元の NTP (手順) に戻ります。

## DLP-A466 手動ルーティングを使用した単一光回線への 2 つのクロスコネクタのロール

目的	この作業では、手動ルーティングを使用して光回線のネットワークパスを再ルーティングします。
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** View メニューから、**Go To Network View** を選択します。

**ステップ 2** **Circuits** タブをクリックします。

**ステップ 3** 新しいパスにロールする回線をクリックします。ロールを開始するには、回線のステータスが **DISCOVERED** でなければなりません。

**ステップ 4** Tools メニューから、**Circuits > Roll Circuit** を選択します。

**ステップ 5** Roll Attributes 領域で、次の手順を実行します (図 21-11)。

- Circuit Roll Mode ドロップダウン リストで、**Auto** を選択して自動ロールを作成するか、または **Manual** を選択して手動ロールを作成します。
- Circuit Type ドロップダウン リストで **Dual** をクリックして、選択した回線上で接続を 2 つロールするように指定します。

**ステップ 6** **Next** をクリックします。

**ステップ 7** Pivot/Fixed Point 1 ウィンドウで、ロールする最初のクロスコネクタの固定パスを表す正方形をクリックします (図 21-7)。

このパスは、ロール プロセスに関連するクロスコネクタ内での固定位置を示します。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。選択されていないパスには、Roll From パスが含まれます。ロールを実行すると、Roll From パスは削除されます。

**ステップ 8** **Next** をクリックします。

**ステップ 9** 次のいずれかを行います。

- 複数の Roll From パスが存在する場合は、Select Roll From ダイアログボックスが表示されます。トラフィックのロール元となるパスを選択し、**OK** をクリックしてから、**Next** をクリックします (図 21-12)。



- 複数の Roll From パスが存在しない場合は、Next をクリックして、[ステップ 10](#) に進みます。Roll From パスの回線ステータスが、DISCOVERED から ROLL\_PENDING に変わります。

**ステップ 10** Pivot/Fixed Point 2 ウィンドウで、ロールする 2 番めの接続の固定パスを表す正方形をクリックします。

選択されていないパスは、Roll From パスです。ロールを実行すると、Roll From パスは削除されます。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。

**ステップ 11** Next をクリックします。

**ステップ 12** Circuit Routing Preferences 領域で、Route Automatically をオフにします。

**ステップ 13** 次のように、回線パスの保護を設定します。

- 保護されているパスで回線をルーティングする場合は、Fully Protected Path をオンにしたままで[ステップ 14](#)へ進みます。
- 保護されていない回線を作成する場合は、Fully Protected Path をオフにして[ステップ 15](#)へ進みます。

**ステップ 14** Fully Protected Path をオンにした場合は、次のいずれかを選択します。

- Nodal Diversity Required — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスを、ノード ダイバースにします。
- Nodal Diversity Desired — ノード ダイバーシティを優先するように指定します。ただし、ノード ダイバースにできない場合は、CTC によって、完全回線パスの UPSR 部分にファイバダイバースパスが作成されます。
- Link Diversity Only — 完全回線パスの UPSR 部分にあるプライマリ パスと代替パスにはファイバダイバースだけが必要であることを指定します。パス全体がノード ダイバースになっていても、CTC ではそのことをチェックしません。

**ステップ 15** Next をクリックします。Route Review and Edit 領域にノード アイコンが表示されるので、回線を手動でルーティングします。

送信元ノードから他のネットワーク ノードまでを示す緑色の矢印は、回線のルーティングに使用できるスパンを表しています。

**ステップ 16** 「[DLP-A369 OC-N 回線ルートのプロビジョニング](#)」(p.20-59) を実行します。



#### 注意

次のようになるのは、回線の両端でここに記載されたカードが使用されていて、DUAL ロール モードの場合のみです。終端カードが DS1/E1-56、DS1-14、DS1-N-14、DS3XM-6、または DS3XM-12 カードの場合は、Roll To ポートで有効な信号が検出されなくても、ロールが実行されます。LOS、LOF、および AIS 回線障害に関する PDI-P ダウンストリームが存在しない場合は、有効な信号がなくても、ロールは継続します。DS1/E1-56、DS1-14、および DS1-N-14 カードの場合、Send AIS-V For Ds1 AIS チェックボックスをオンにして、LOS および LOF AIS 回線障害の PDI-P ダウンストリームを正常に生成させることができます。このチェックボックスは、カード ビューの Provisioning > Line タブで選択されます。DS1-14 および DS1-N-14 カードの場合、Send AIS-V for Ds1 AIS は VT 回線にのみ機能します。DS1/E1-56 カードの場合、Send AIS-V for Ds1 AIS は STS および VT 回線の両方に機能します。

**ステップ 17** **Finish** をクリックします。Circuits タブで、新しい回線が表示されたことを確認します。

この回線は Roll To 回線です。この回線には、Roll From 回線名に ROLL\*\* を付加した名前が付けられます。

**ステップ 18** **Rolls** タブをクリックします。Rolls タブに新しいロールが 2 つ表示されます。保留中のロールごとに、Roll Valid Signal ステータスを表示します。次のいずれかの条件が満たされる場合は、[ステップ 19](#) に進みます。

- Roll Valid Signal ステータスが true である場合に、新しいポート上で有効な信号が検出されている。
- Roll Valid Signal ステータスが false である場合に、有効な信号が検出されていない。信号が検出されるまで待機してから、次のステップに進みます。信号が検出されない場合は、『Cisco ONS 15454 Troubleshooting Guide』の「Circuits and Timing」を参照してください。ロールをキャンセルするには、「[DLP-A489 ロールのキャンセル](#)」(p.21-69)を参照してください。
- ロールが 1 方向宛先ロールであり、Roll Valid Signal ステータスが false である。1 方向宛先ロールの場合は、Roll Valid Signal ステータスが true になることはありません。



**(注)** 有効な信号が検出されたあとに、自動ロールをキャンセルすることはできません。

- Force Valid Signal ボタンを使用して、有効な信号がなくても、Roll To Circuit の宛先にロールを強制実行することができる。Force Valid Signal を選択した場合、ロールを実行すると、ロールに関連する回線でトラフィックが廃棄されます。

**ステップ 19** [ステップ 5](#) で Manual を選択した場合は、各ロールをクリックし、**Complete** をクリックして、新しいポートにトラフィックをルーティングします。Auto を選択した場合は、[ステップ 20](#) に進みます。



**(注)** 片方のロールをキャンセルした場合は、ロールを完了できません。2 つのロールは同時に完了する必要があります。

**ステップ 20** 手動ロールと自動ロールのいずれの場合も、**Finish** をクリックして、回線ロール プロセスを完了します。

**ステップ 21** 元の NTP (手順) に戻ります。

## DLP-A467 光回線間での 2 つのクロスコネクットのロール

目的	この作業では、2 番めの回線の Roll To パスを CTC で自動選択できるように設定して、2 つの光回線を使用したネットワーク パスを再ルーティングします。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** Circuits タブをクリックします。

**ステップ 3** Ctrl キーを押しながら、ロール プロセスで使用する回線を 2 つクリックします。

Roll From パスと Roll To パスは別々の回線に設定されます。回線のステータスはどちらも DISCOVERED でなければなりません。また、ロールを開始するには、これらの回線のサイズと方向が同じである必要があります。設定された Roll To 回線で、トラフィックが伝送されてはなりません。最初の Roll To パスは、Roll To 回線の送信元ノードに DCC 接続されていなければなりません。2 番めの Roll To パスは、Roll To 回線の宛先ノードに DCC 接続されていなければなりません。

**ステップ 4** Tools メニューから、**Circuits > Roll Circuit** を選択します。

**ステップ 5** Roll Attributes 領域で、次の手順を実行します。

- Circuit Roll Mode ドロップダウン リストで、**Auto** を選択して、自動ロール (1 方向送信元ロールの場合に必要な) を作成するか、または **Manual** を選択して、手動ロール (1 方向宛先ロールの場合に必要な) を作成します。
- Circuit Roll Type ドロップダウン リストから **Dual** を選択します。
- Roll From Circuit 領域で、Roll From パスを含む回線をクリックします。

**ステップ 6** Next をクリックします。

**ステップ 7** Pivot/Fixed Point 1 ウィンドウで、ロールする最初のクロスコネクットの固定パスを表す正方形をクリックします ( [図 21-7](#) )。

このパスは、ロール プロセスに関連するクロスコネクット内での固定位置を示します。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。選択されていないパスには、Roll From パスが含まれます。ロールを実行すると、Roll From パスは削除されます。

**ステップ 8** Next をクリックします。

**ステップ 9** 次のいずれかを行います。

- 複数の Roll From パスが存在する場合は、Select Roll From ダイアログボックスが表示されます。トラフィックのロール元となるパスを選択し、**OK** をクリックします ( [図 21-12](#) )。
- 複数の Roll From パスが存在しない場合は、[ステップ 10](#) に進みます。

Roll From パスの回線ステータスが、DISCOVERED から ROLL PENDING に変わります。

**ステップ 10** Pivot/Fixed Point 2 ウィンドウで、ロールする 2 番めの接続の固定パスを表す正方形をクリックします。

選択されていないパスは、Roll From パスです。ロールを実行すると、Roll From パスは削除されます。グラフィック イメージの下にあるテキスト ボックスにパスの ID が表示されます。

**ステップ 11** Next をクリックします。



#### 注意

次のようになるのは、回線の両端でここに記載されたカードが使用されていて、DUAL ロール モードの場合のみです。終端カードが DS1/E1-56、DS1-14、DS1-N-14、DS3XM-6、または DS3XM-12 カードの場合は、Roll To ポートで有効な信号が検出されなくても、ロールが実行されます。LOS、LOF、および AIS 回線障害に関する PDI-P ダウンストリームが存在しない場合は、有効な信号がなくても、ロールは継続します。DS1/E1-56、DS1-14、および DS1-N-14 カードの場合、Send AIS-V For Ds1 AIS チェックボックスをオンにして、LOS および LOF AIS 回線障害の PDI-P ダウンストリームを正常に生成させることができます。このチェックボックスは、カード ビューの Provisioning > Line タブで選択されます。DS1-14 および DS1-N-14 カードの場合、Send AIS-V for Ds1 AIS は VT 回線にのみ機能します。DS1/E1-56 カードの場合、Send AIS-V for Ds1 AIS は STS および VT 回線の両方に機能します。

**ステップ 12** Finish をクリックします。Circuits タブで Roll From 回線および Roll To 回線のステータスが、DISCOVERED から ROLL PENDING に変わります。

**ステップ 13** Rolls タブをクリックします。Rolls タブに新しいロールが 2 つ表示されます。保留中のロールごとに、Roll Valid Signal ステータスを表示します。次のいずれかの条件が満たされる場合は、[ステップ 14](#)に進みます。

- Roll Valid Signal ステータスが true である場合に、新しいポート上で有効な信号が検出されている。
- Roll Valid Signal ステータスが false である場合に、有効な信号が検出されていない。信号が検出されるまで待機してから、次のステップに進みます。信号が検出されない場合は、『Cisco ONS 15454 Troubleshooting Guide』の「Circuits and Timing」を参照してください。ロールをキャンセルするには、「[DLP-A489 ロールのキャンセル](#)」(p.21-69)を参照してください。
- ロールが 1 方向宛先ロールであり、Roll Valid Signal ステータスが false である。1 方向宛先ロールの場合は、Roll Valid Signal ステータスが true になることはありません。



**(注)** 有効な信号が検出されたあとに、自動ロールをキャンセルすることはできません。

- Force Valid Signal ボタンを使用して、有効な信号がなくても、Roll To Circuit の宛先にロールを強制実行することができる。Force Valid Signal を選択した場合、ロールを実行すると、ロールに関連する回線でトラフィックが廃棄されます。

**ステップ 14** [ステップ 5](#) で Manual を選択した場合は、Rolls タブで両方のロールをクリックしてから、Complete をクリックして、新しいポートにトラフィックをルーティングします。Auto を選択した場合は、[ステップ 15](#)に進みます。



(注) 片方のロールをキャンセルした場合は、ロールを完了できません。2つのロールは同時に完了する必要があります。

**ステップ 15** 手動ロールと自動ロールのいずれの場合も、**Finish** をクリックして、回線ロール プロセスを完了します。

**ステップ 16** 元の NTP (手順) に戻ります。

## DLP-A468 ロールの削除

目的	この作業では、ロールを削除します。このオプションを選択する場合は、トラフィックに影響することがあるので注意してください。ロールを削除するのは、ロールを完了できないか、または通常の方法でキャンセルできない場合に限定してください。このオプションが選択されている場合、回線は PARTIAL ステータスになることがあります。回線ステータスについては、表 21-2 を参照してください。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">NTP-A334 トラフィックのブリッジおよびロール (p.7-15)</a>
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** **Circuits > Rolls** タブをクリックします。

**ステップ 3** 削除するロール済み回線をクリックします。

**ステップ 4** Tools メニューから、**Circuits > Delete Rolls** を選択します。

**ステップ 5** 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** 元の NTP (手順) に戻ります。

## DLP-A469 GBIC または SFP/XFP デバイスの取り付け

目的	この作業では、GBIC (E シリーズ イーサネット カード、G シリーズ イーサネット カード、CE-1000-4 カード、および FC_MR-4 カードに必要) と SFP/XFP (ML1000-2、ML100X-8、MXP、MRC-12、および OC192-XFP カードに必要) を取り付け、デバイスにファイバを接続します。GBIC、SFP、および XFP は、光ファイバ ネットワークとポートをリンクするためにトラフィック カード ポートに装着される、ホットスワップ対応の入出力デバイスです。トランスポンダ カードまたは マックスポンダ カードの SFP/XFP デバイスについては、『Cisco ONS 15454 DWDM Reference Manual』を参照してください。
工具 / 機器	E1000-2-G、G1K-4、CE-1000-4、または FC_MR-4 カードには、SX、LX、ZX、または DWDM GBIC を使用します (表 21-8 を参照)。  ML1000-2、ML100X-8、MRC-12、および OC192-XFP カードには、SFP と XFP を使用します (表 21-9 を参照)。
事前準備手順	GBIC または SFP/XFP デバイスを取り付けるカードに応じて、次の手順を 1 つまたは複数実行します。 <ul style="list-style-type: none"> <li>• <a href="#">NTP-A16 光カードおよびコネクタの取り付け (p.2-8)</a></li> <li>• <a href="#">DLP-A39 イーサネット カードの取り付け (p.17-49)</a></li> <li>• <a href="#">NTP-A274 FC_MR-4 カードの取り付け (p.2-15)</a></li> </ul>
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



警告

クラス 1 レーザー製品です。



警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器 (ルーペ、拡大鏡、顕微鏡など) で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。



(注)

2003 年 8 月より前に製造された G シリーズ カードは、DWDM GBIC をサポートしていません。DWDM GBIC と互換性がある G1K-4 カードには、WM51RWPCAA の Common Language Equipment Identification (CLEI) コードがあります。



(注)

G1K-4 カードはすべてのバージョンで、Coarse Wavelength Division Multiplexing (CWDM; 低密度波長分割多重) GBIC をサポートします。



(注) GBIC、SFP、および XFP はホットスワップ可能で、そのためカードやシェルフ アセンブリに電源が入って動作しているときでも、取り付けや取り外しができます。

**ステップ 1** GBIC、SFP、または XFP を保護パッケージから取り出します。

**ステップ 2** ラベルをチェックして、GBIC、SFP、または XFP のタイプがネットワークに合っていることを確認します。

表 21-8 に使用可能な GBIC を示します。



(注) これらの GBIC は外見が非常に似ています。取り付ける前に、GBIC のラベルをよく確認してください。

表 21-8 使用可能な GBIC

GBIC	対応カード	説明	ファイバ	製品番号
1000BaseSX	E1000-2-G G1K-4 CE-1000-4	短距離	マルチモード ファイバ (最大長 550 m)	15454E-GBIC-SX= 15454-GBIC-SX ONS-GC-GE-SX
1000BaseLX	E1000-2-G G1K-4 CE-1000-4	長距離	シングルモード ファイバ (最大長 5 km)	15454E-GBIC-LX= 15454-GBIC-LX ONS-GC-GE-LX
1000BaseZX	G1K-4 CE-1000-4	超長距離	シングルモード ファイバ (最大長 70 km)	15454E-GBIC-ZX= 15454-GBIC-ZX ONS-GC-GE-ZX
	FC_MR-4	長距離	シングルモード ファイバ、 1310 nm	ONS-GX-2FC-SML=
	FC_MR-4	中距離	マルチモード ファイバ、 850 nm	ONS-GX-2FC-MMI=

表 21-9 に使用可能な SFP および XFP を示します。

表 21-9 使用可能な SFP および XFP

SFP/XFP	対応カード	説明	ファイバ	製品番号
1000BaseSX	ML1000-2	短距離	マルチモード ファイバ(最大長 550 m)	15454E-SFP-LC-SX=
1000BaseLX		長距離	シングルモード ファイバ(最大長 5 km)	15454E-SFP-LC-LX=
1000BaseFX	ML100X-8	短距離	1310 nm マルチモード ファイバ(最大長 2 km)	ONS-SE-100-FX
1000BaseLX-10		中距離	1310 nm シングルモード ファイバ(最大長 15 km)	ONS-SE-100-LX10

表 21-9 使用可能な SFP および XFP (続き)

SFP/XFP	対応カード	説明	ファイバ	製品番号	
OC-48 SR	MRC-12	短距離	1310 nm シングルモード ファイバ (最大長 2 km)	ONS-SI-2G-S1	
OC-48 IR1		中距離	1310 nm シングルモード ファイバ (最大長 15 km)	ONS-SI-2G-I1	
OC-48 LR1		長距離	1310 nm シングルモード ファイバ (最大長 40 km)	ONS-SI-2G-L1	
OC-48 LR2		長距離	1550 nm シングルモード ファイバ (最大長 80 km)	ONS-SI-2G-L2	
OC-48 LR2 DWDM		長距離	1530.33 ~ 1560.61 nm シングルモード ファイバ (最大長 120 km)	ONS-SC-2G-30.3 ~ ONS-SC-2G-60.6	
OC-3/OC-12 IR1 デュアルレート		中距離	1310 nm シングルモード ファイバ (最大長 15 km)	ONS-SI-622-I1	
OC-12 LR1		長距離	1310 nm シングルモード ファイバ (最大長 40 km)	ONS-SI-622-L1	
OC-12 LR2		長距離	1550 nm シングルモード ファイバ (最大長 80 km)	ONS-SI-622-L2	
OC-12 CWDM		長距離	1470 ~ 1610 nm シングルモード ファイバ (最大長 80 km)	ONS-SE-622-1470 ~ ONS-SE-622-1610	
OC-3 IR1		中距離	1310 nm シングルモード ファイバ (最大長 15 km)	ONS-SI-155-I1	
OC-3 LR1		長距離	1310 nm シングルモード ファイバ (最大長 40 km)	ONS-SI-155-L1	
OC-3 LR2		長距離	1550 nm シングルモード ファイバ (最大長 80 km)	ONS-SI-155-L2	
OC-3 CWDM		長距離	1470 ~ 1610 nm シングルモード ファイバ (最大長 80 km)	ONS_SE-155-1470 ~ ONS-SE-155-1610	
OC-192 SR1		OC192SR1/STM64 IO Short Reach <sup>1</sup>	短距離	1310 nm シングルモード ファイバ (最大長 10 km)	ONS-XC-10G-S1
OC-192 SR1、IR1、LR2		OC192/STM64 Any Reach <sup>1</sup>	短距離	1310 nm シングルモード ファイバ (最大長 10 km)	ONS-XC-10G-S1
	中距離		1550 nm シングルモード ファイバ (最大長 15 km)	ONS-XC-10G-I2	
	長距離		1550 nm シングルモード ファイバ (最大長 80 km)	ONS-XC-10G-L2	

1. CTC では、このカードを OC192-XFP として表します。



(注) MRC-12 カードに SFP を取り付ける前に、『Cisco ONS 15454 Reference Manual』の MRC-12 カードの情報を参照し、SFP を取り付けるポートおよび使用中のクロスコネクタカードに基づいた帯域幅制限を確認してください。



**ステップ 3** 使用する GBIC、SFP、または XFP のタイプを確認します。

- クリップ付きの GBIC を使用する場合は、[ステップ 4](#) へ進みます。
- ハンドル付きの GBIC を使用する場合は、[ステップ 5](#) へ進みます。
- SFP または XFP を使用する場合は、[ステップ 6](#) へ進みます。

**ステップ 4** クリップ付き GBIC の場合

- a. 親指と人差し指で GBIC の両側をつかんで、カード上のスロットにその GBIC を挿入します。



**(注)** GBIC には、誤って取り付けられないようにキーが付いています。

- b. 開口部を覆っているフラップを通して、カチッという音がするまで GBIC をスライドします。カチッという音は、GBIC がスロットにロックされたことを示します。
- c. ネットワーク用の光ファイバケーブルを取り付ける準備ができたなら、GBIC から保護プラグを取り外し、今後のために保管しておきます。GBIC にファイバコネクタを差し込みます。
- d. [ステップ 7](#) へ進んでください。

**ステップ 5** ハンドル付き GBIC の場合

- a. SC タイプ コネクタから保護プラグを取り外します。
- b. 親指と人差し指で GBIC の両側をつかんで、カード上のスロットにその GBIC を挿入します。
- c. ハンドルを下に閉めて、GBIC を所定の位置にロックします。SC タイプ コネクタへ手を伸ばすのにハンドルが邪魔にならなければ、正しく閉めた位置にあります。
- d. カバー フラップを通して、カチッという音がするまで GBIC をスライドします。カチッという音は、GBIC がスロットにロックされたことを示します。
- e. ネットワーク用の光ファイバケーブルを取り付ける準備ができたなら、GBIC から保護プラグを取り外し、今後のために保管しておきます。GBIC にファイバコネクタを差し込みます。
- f. [ステップ 7](#) へ進んでください。

**ステップ 6** SFP および XFP の場合

- a. ファイバの LC デュプレックス コネクタを、シスコ対応の SFP または XFP に差し込みます。
- b. 新しい SFP または XFP にラッチが付いている場合は、ケーブル上でラッチを閉めて固定します。
- c. ケーブルを付けた SFP または XFP を、カチッと音がするまで、カードポートに差し込みます。SFP と XFP を CTC でプロビジョニングする必要があります。マルチレート PPM を取り付けた場合、「[DLP-A444 MRC-12 カードでの PPM のプロビジョニング](#)」(p.21-27) を実行します (シングルレート XFP は、CTC でプロビジョニングする必要はありません)。

**ステップ 7** 元の手順 (NTP) に戻ります。

## DLP-A470 GBIC または SFP/XFP デバイスの取り外し

目的	この作業では、GBIC、SFP、または XFP に接続されているファイバを外し、GBIC、SFP、または XFP をカードから外します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A469 GBIC または SFP/XFP デバイスの取り付け (p.21-64)</a>
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



## 警告

終端していない光ファイバ ケーブルの先端やコネクタからは、目に見えないレーザー光が放射されている可能性があります。光学機器を使用してレーザー光を直接見ないでください。光学機器（ルーペ、拡大鏡、顕微鏡など）で 100 mm 以内から放射されるレーザーを見ると、目を痛める恐れがあります。

- ステップ 1** GBIC SC コネクタまたは SFP/XFP LC デュプレックス コネクタから、ネットワーク用の光ファイバ ケーブルを取り外します。光ファイバ ケーブルを固定するためのラッチが SFP/XFP コネクタに付いている場合は、そのラッチを上引き上げてケーブルを解放します。
- ステップ 2** クリップ付きの GBIC を使用する場合は、次のサブステップを実行します。
- GBIC の両側にある 2 つのプラスチック タブを強く握って、スロットから GBIC を解放します。
  - GBIC をスライドさせてスロットから外します。スロットを覆うフラップが閉じて、ギガビットイーサネット カードのコネクタが保護されます。
- ステップ 3** ハンドル付きの GBIC を使用する場合は、次のサブステップを実行します。
- ハンドルを開けて、GBIC を解放します。
  - GBIC のハンドルを引きます。
  - GBIC をスライドさせてスロットから外します。スロットを覆うフラップが閉じて、ギガビットイーサネット カードのコネクタが保護されます。
- ステップ 4** SFP/XFP を使用する場合は、次のサブステップを実行します。
- 光ファイバ ケーブルを固定するためのラッチが SFP/XFP コネクタに付いている場合は、そのラッチを上引き上げてケーブルを解放します。
  - コネクタから光ファイバ ケーブルを真っ直ぐに引き抜きます。
  - カードから SFP/XFP コネクタとファイバを外します。
  - SFP/XFP をスライドさせてスロットから取り外します。
- ステップ 5** 元の NTP (手順) に戻ります。

## DLP-A489 ロールのキャンセル

目的	この作業では、ロールをキャンセルします。ロール モードが Manual の場合は、Complete ボタンをクリックする前でないと、ロールをキャンセルできません。ロール モードが Auto の場合は、ノードで正常な信号が検出される前、または ForceValid Signal ボタンをクリックする前でないと、ロールをキャンセルできません。デュアル ロールまたは単一ロールは、ロール ステートが ROLL_COMPLETED に変わる前であればキャンセルできます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a> <a href="#">NTP-A334 トラフィックのブリッジおよびロール (p.7-15)</a>
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

Manual モードでデュアル ロールを実行しているときにキャンセルをクリックすると、両方のロールで有効な信号が検出されている場合は、トラフィックが中断する可能性があることを示すダイアログボックスが表示され、キャンセルを継続するかどうか確認されます。有効な信号が検出された後は、なるべくデュアル ロールをキャンセルしないでください。回線を元の状態に戻すには、ロールを実行してから、ブリッジおよびロールを再使用して、回線をロール バックすることを推奨します。

- 
- ステップ 1** ノード ビューまたはネットワーク ビューで、Circuits > Rolls タブをクリックします。
  - ステップ 2** キャンセルするロール済み回線をクリックします。
  - ステップ 3** Cancel をクリックします。
  - ステップ 4** 元の NTP (手順) に戻ります。
- 

## DLP-A495 ネットワーク ビューでのリンクの統合

目的	この作業では、CTC ネットワーク ビューの DCC、GCC、Optical Transport Section (OTS)、Provisionable Patchcord (PPC; プロビジョニング可能なパッチコード)、およびサーバ証跡リンクを統合します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) CTC が再起動されても、ローカル統合が再起動されないと、グローバル統合が解消されません。

**ステップ 1** View メニューから **Go to Network View** を選択します。デフォルトでは、CTC にリンク アイコンが表示されます。

**ステップ 2** 必要に応じて、次のステップを実行します。

- リンク間を切り替えるには、**ステップ 3** に進みます。
- ネットワーク マップ上のすべてのリンクを統合するには、**ステップ 4** に進みます。
- 2つのノード間でリンクを統合するには、**ステップ 5** に進みます。
- 統合されたリンクに関する情報を表示するには、**ステップ 6** に進みます。
- 統合されたリンク内の個々のリンクにアクセスするには、**ステップ 7** に進みます。
- 統合されたリンクを展開表示するには、**ステップ 8** に進みます。
- クラスでリンクをフィルタするには、**ステップ 9** に進みます。

**ステップ 3** ネットワーク マップで右クリックし、**Show Link Icons** を選択してリンク アイコンのオンとオフを切り替えます。

**ステップ 4** ネットワーク マップ上のすべてのリンクを統合 (グローバル統合) するには、次の手順を実行します。

- a. ネットワーク マップの任意の場所を右クリックします。
- b. ショートカットメニューで **Collapse/Expand Links** を選択します。Collapse/Expand Links ダイアログウィンドウが表示されます。
- c. 統合するリンク クラスのチェックボックスをオンにします。
- d. **OK** をクリックします。ネットワーク マップ全体で、選択したリンク クラスが統合されます。

**ステップ 5** 2つのノード間でリンクを統合 (ローカル統合) するには、次の手順を実行します。

- a. ネットワーク マップのリンクを右クリックします。
- b. ショートカットメニューで **Collapse Link** を選択します。選択したリンク タイプが統合され、1つのリンクのみが表示されます。



(注) リンクはクラスで統合されます。たとえば、DCC リンクを統合するように選択した場合、DCC リンクだけが統合され、他のリンク クラスは展開表示されたままになります。

図 21-13 には、統合されていない DCC および PPC リンクのネットワーク ビューを示します。

図 21-13 ネットワーク ビューの統合されていないリンク



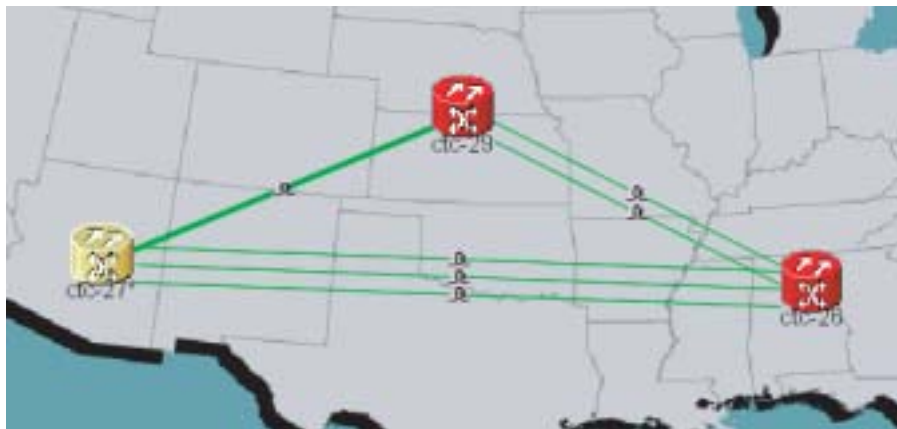
図 21-14 では、グローバル統合されたリンクのネットワーク ビューを示します。

図 21-14 ネットワーク ビューの統合されたリンク



図 21-15 では、2つのノード間でのローカル DCC リンク統合のネットワーク ビューを示します。

図 21-15 ローカル リンク統合のネットワーク ビュー



- ステップ 6** 統合されたリンクに関する情報を表示するには、そのリンク上にマウスを移動するか（ツールチップでリンクの数およびリンク クラスが表示されます）、リンクを 1 回クリックしてウィンドウの左側に詳細情報を表示します。
- ステップ 7** 統合されたリンク内の個々のリンクにアクセスする（たとえば、スパン アップグレードの実行が必要な場合など）には、次の手順を実行します。
- a. 統合されたリンクを右クリックします。ショートカット メニューと個々のリンクのリストが表示されます。
  - b. 選択したリンクの上にマウスを移動します。カスケード メニューが表示され、個々のリンクに対するアクションを選択したり、リンクの接続先であるノードの 1 つに移動したりできます。
- ステップ 8** ローカル統合されたリンクを展開表示するには、統合されたリンクを右クリックし、ショートカットメニューから **Expand [link class] Links** を選択します。この [link class] は DCC、GCC、OTS、PPC、またはサーバ証跡です。
- ステップ 9** クラスでリンクをフィルタするには、次の手順を実行します。
- a. ウィンドウの右上の領域にある **Link Filter** ボタンをクリックします。Link Filter ダイアログが表示されます。

Link Filter ダイアログに表示されるリンク クラスは、ネットワーク ビューで選択した Network Scope によって決定されます（表 21-10）。

表 21-10 Network Scope によるリンク クラス

Network Scope	表示されるリンク クラス
ALL	DCC、GCC、OTS、PPC、サーバ証跡
DWDM	GCC、OTS、PPC
TDM	DCC、PPC、サーバ証跡

- b. 表示したいリンクの隣にあるチェックボックスをオンにします。
- c. OK をクリックします。

ステップ 10 元の NTP (手順) に戻ります。

## DLP-A498 TDM と DWDM のネットワーク ビューの切り替え

目的	この作業では、Time-Division Multiplexing (TDM; 時分割多重) と DWDM との間でネットワーク ビューを切り替えます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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** View メニューから **Go to Network View** を選択します。

**ステップ 2** ツールバーの Network Scope ドロップダウン リストから、次のいずれかを選択します。

- **All** — TDM ノードと DWDM ノードを両方とも表示します。
- **TDM** — トランスポンダ (TXP) カードとマックスポンダ (MXP) カードが実装されている SONET または SDH カード付きの ONS 15454 だけを表示します。
- **DWDM** — TXP カードと MXP カードが実装されている DWDM カード付きの ONS 15454 だけを表示します。



**(注)** DWDM、TXP、および MXP の各カードについては、『Cisco ONS 15454 DWDM Reference Manual』を参照してください。

**ステップ 3** 元の NTP (手順) に戻ります。







## DLP A500 ~ A599

---

### DLP-A507 OC-N PM パラメータの表示

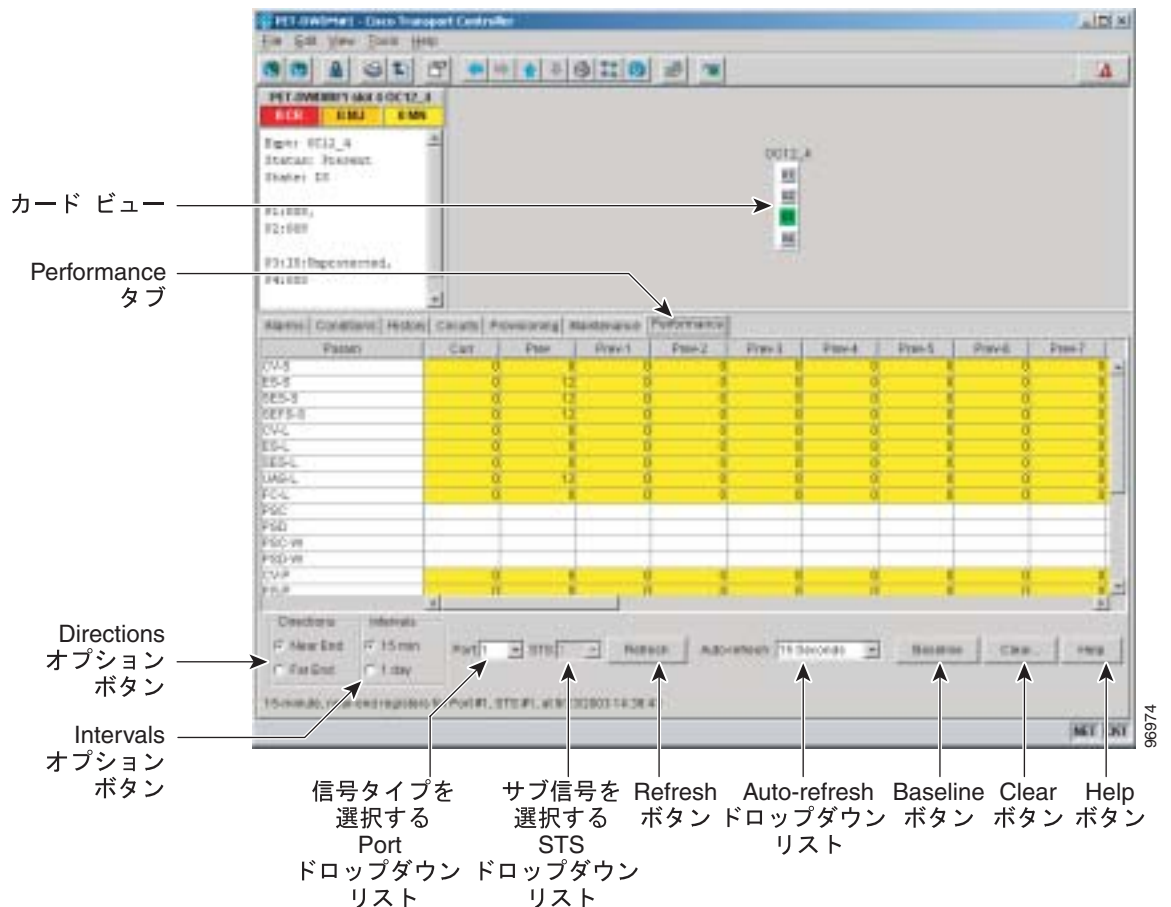
目的	この作業では、OC-N カードおよびポートの Performance Monitoring (PM; パフォーマンス モニタリング) カウントを表示して、パフォーマンスの問題を事前に検出します。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
必須 / 適宜	適宜
オンサイト / リモート	オンサイトまたはリモート
セキュリティ レベル	検索以上のレベル

---

**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、トラフィックを送送する 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- Performance > Ether Ports > Statistics タブをクリックします。
- 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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ト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ト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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- Performance > POS Ports > Statistics タブをクリックします。
- 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役に立ちます。
工具 / 機器	なし
事前準備手順	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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タ (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值に達すると、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) が表示されません。

**ステップ 5** 元の手順 (NTP) に戻ります。

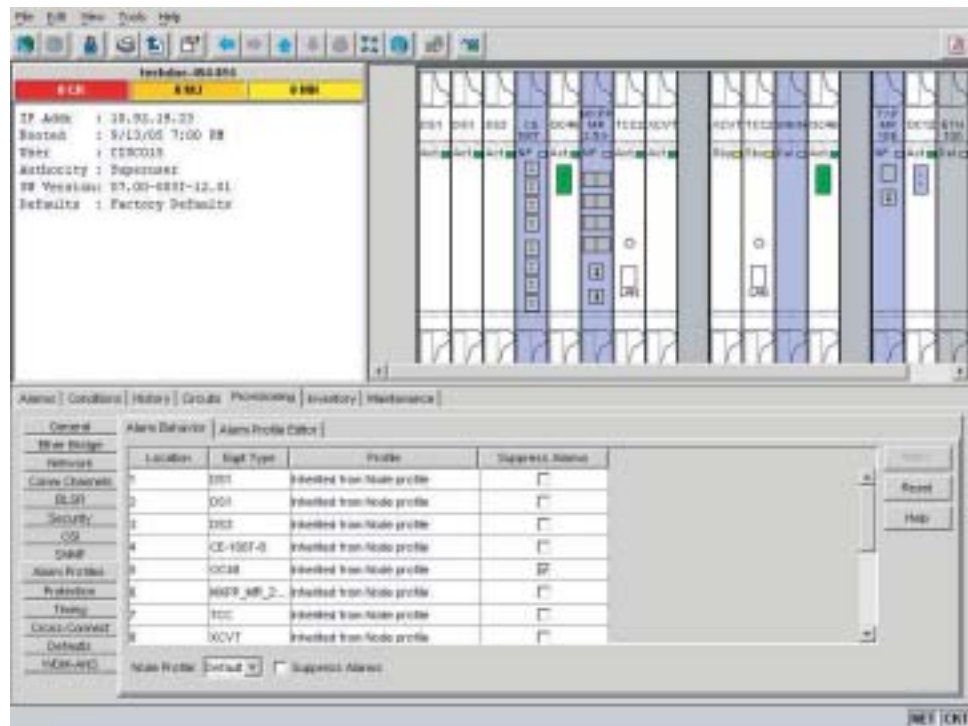
## DLP-A518 アラーム重大度プロファイルの新規作成または複製

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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) のものはすべて、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一覧表示する場合は、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。

- 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。
- ドロップダウン リストから重大度を選択します。
- 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。

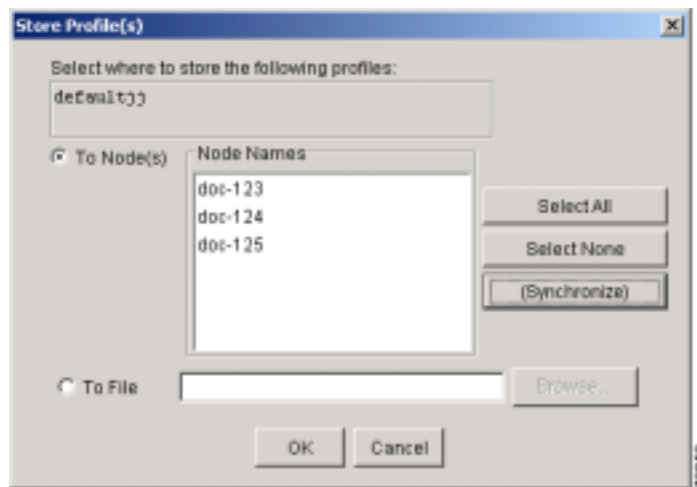
- デフォルトまたはユーザ定義で重大度が Critical (CR) または Major (MJ) に設定されているものでも、サービスに影響しない (NSA) ものはすべて、Telcordia GR-474 の定義に従って Minor (MN) に格下げされます。
- 新しいプロファイルを作成して適用するまでは、デフォルトの重大度がすべてのアラームおよび状態に適用されます。
- 重大度を継承 (I) または未設定 (U) に変更しても、アラームの重大度は変化しません。

**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



- 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。
- 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	<a href="#">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)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、アラーム プロファイルをカードに適用できます。

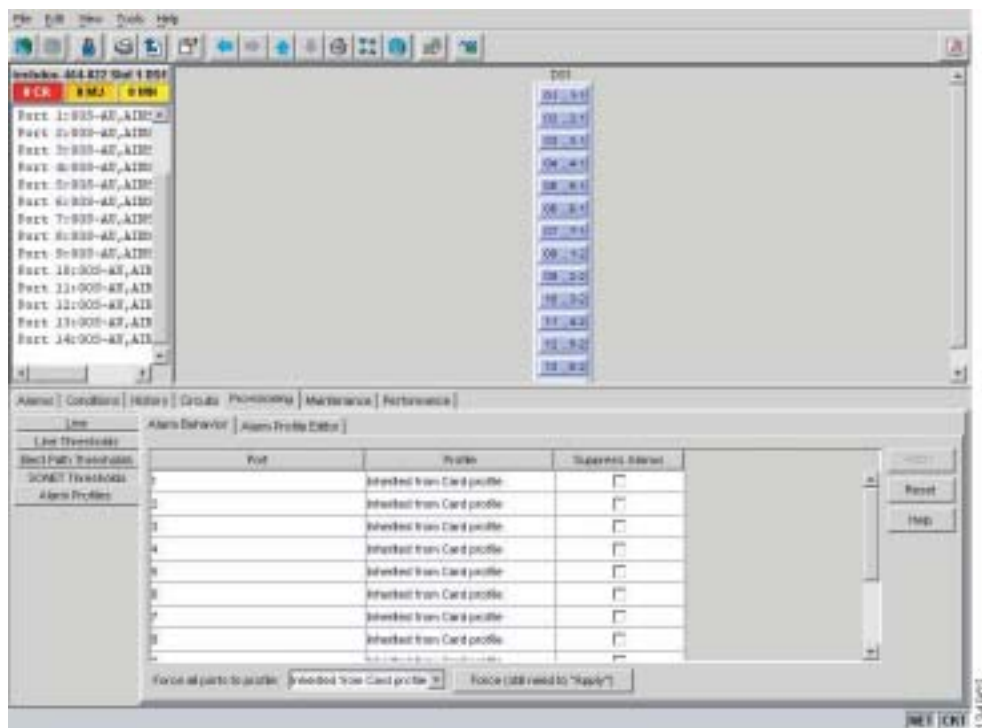


(注) TCC2/TCCP またはクロスコネクトカードでは、カード ビューを利用できません。

**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。

- 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。
- 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。
- 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。

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

カードビューの 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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、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。

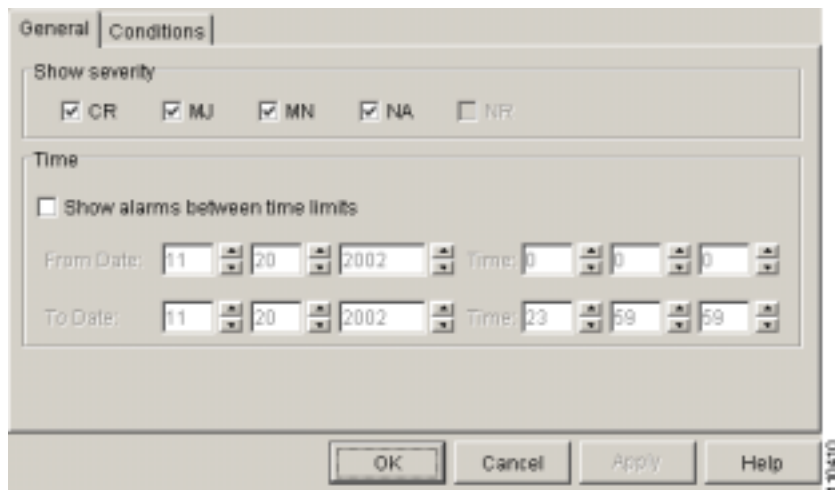
## DLP-A521 アラーム、状態、および履歴フィルタのパラメータ変更

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	<a href="#">DLP-A225 アラーム フィルタリングのイネーブル化 (p.19-20)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

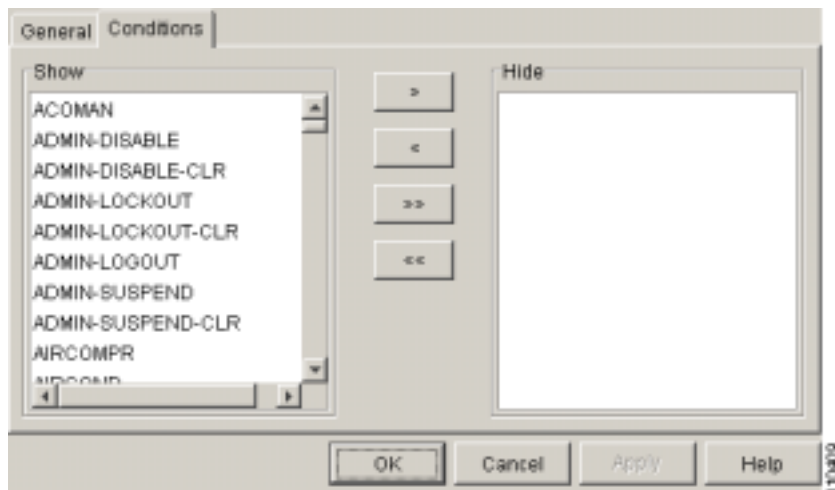
アラームフィルタをディセーブルにすると、すべてのアラームが表示されます。

- 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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事です。

**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。

## ■ DLP-A523 アラーム抑制の中止

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	<a href="#">DLP-A522 アラーム レポートの抑制 (p.22-21)</a> <a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。デフォルトは空白です。  「DLP-A314 ポートへの名前割り当て」(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。	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	信号劣化ビットエラーレートを設定します。	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	ライン フレーミング タイプを指定します。	<ul style="list-style-type: none"> <li>• Unframed</li> <li>• M13</li> <li>• C Bit</li> <li>• Auto Provisioned</li> </ul>
Detected Line Type	検出された回線のタイプを表示します。	<ul style="list-style-type: none"> <li>• M13</li> <li>• C Bit</li> <li>• Unframed</li> <li>• Unknown</li> </ul>
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。	<ul style="list-style-type: none"> <li>• 0 ~ 225 (デフォルト)</li> <li>• 226 ~ 450</li> </ul>

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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>
AINS Soak	自動稼働のソーク時間を設定します。	<ul style="list-style-type: none"> <li>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。</li> <li>0 ~ 48 時間、15 分刻み</li> </ul>

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 カードの電気回路バス 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。 <ul style="list-style-type: none"> <li>• Disable — ALS を無効にします。</li> <li>• 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。</li> <li>• 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。</li> <li>• Manual Restart for Test — テストのため、レーザーを手動で再起動します。</li> </ul>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">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 )</a> <a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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。



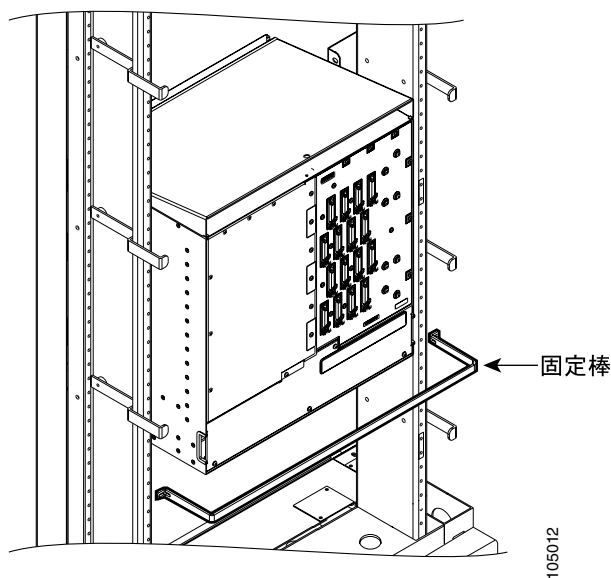
## DLP-A530 固定棒の取り付け

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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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](#) )。

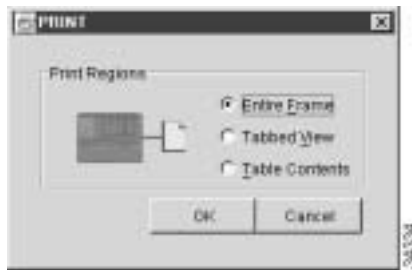
- Entire Frame — カード、ノード、またはネットワークの図も含めて、CTC ウィンドウ全体を印刷します。このオプションはすべてのウィンドウで使用可能です。
- Tabbed View — タブとデータを含む、CTC ウィンドウの下半分を印刷します。印刷結果には、選択したタブ(一番上)とタブ ウィンドウ内の表示データが出力されます。たとえば、History ウィンドウを Tabbed View で印刷すると、ウィンドウに表示されている履歴項目だけが印刷されます。このオプションはすべてのウィンドウで使用可能です。
- Table Contents — シェルフ、カード、またはタブの図を除いて、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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">NTP-A323 カードの取り付けの確認 (p.4-2)</a>
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。

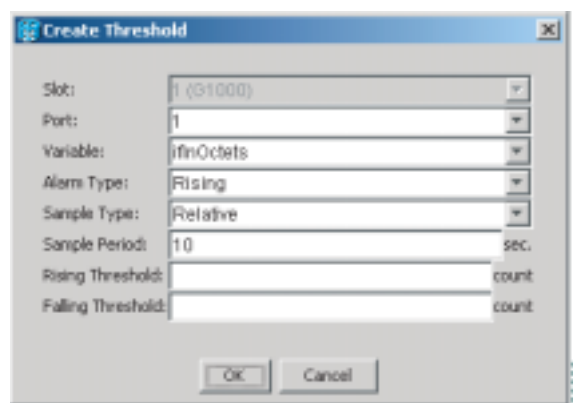


**(注)** CE シリーズ カードおよび ML シリーズ カードの場合、**Provisioning > Ether Ports > RMON Thresholds** タブまたは **Provisioning > POS Ports > RMON Thresholds** タブをクリックします。

**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
ifnOctets	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)。
ifnUcastPkts	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
ifnMulticastPkts	(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
ifnBroadcastPkts	(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
ifnDiscards	(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
ifnErrors	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	<p>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 プロープ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プには、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プよりも多くの衝突が記録される可能性があります。</p> <p>10BaseT の場合は、プロープ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プのどちらでも、同じ数の衝突が記録されます。</p> <p>リピータ内の RMON プロープでは、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。</p>
etherStatsCollisionFrames	<p>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 プロープ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プには、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プよりも多くの衝突が記録される可能性があります。</p> <p>10BaseT の場合は、プロープ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プのどちらでも、同じ数の衝突が記録されます。</p> <p>リピータ内の RMON プロープでは、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。</p>
etherStatsDropEvents	<p>リソース不足が原因で、パケットがプロープ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。</p>



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 ~ 127 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、下限スレッショールドは上限スレッショールドより低く設定します。

下限スレッショールドと上限スレッショールドはペアで使用されます。発生回数が上限スレッショールドより高くなって、その後下限スレッショールドより下に下がると、上限スレッショ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ョ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ョ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ョールドを超えると、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、上限スレッショ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、上限スレッショ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	<a href="#">NTP-A323 カードの取り付けの確認（p.4-2）</a>
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 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** 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	<a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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、LDB 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- 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。
- 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。
- 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	<a href="#">DLP-A539 OSI ルータのプロビジョニング ( p.22-49 )</a> <a href="#">DLP-A60 CTC へのログイン ( p.17-71 )</a>
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。

- 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。
- 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。
- 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。
- 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- 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。

- 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。
- 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。
- 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。

- TID to NSAP ボタンをクリックします。
- 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。
- 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。
- 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	<a href="#">DLP-A60 CTC へのログイン (p.17-71)</a>
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。



## CTC の情報およびショートカット

---

この付録では、Cisco Transport Controller (CTC) のビュー、メニュー オプション、ツール オプション、ショートカット、およびテーブル表示オプションについて説明します。また、CTC から得られるシェルフ インベントリ データについても説明します。CTC の詳細については、『*Cisco ONS 15454 Reference Manual*』を参照してください。



(注)

---

ネットワーク検出がノード上でイネーブルになっている場合、CTC はネットワークの各ノードでより新しいバージョンの CTC ソフトウェアを検索します。より新しいバージョンが見つかったら、CTC により、Java Archive (JAR) ファイルを PC にダウンロードするオプションが提示されます。

---

## ビューの表示：ノードビュー、カードビュー、ネットワークビュー

CTC では、ONS 15454 と ONS ネットワークを次の 3 つのビューで表示することができます。

- ノードビュー — ONS 15454 に最初にログインすると表示されるビューです。このビューには ONS 15454 のシェルフが図で表示され、ノードを管理するためのタブとサブタブにアクセスできます。
- カードビュー — ONS 15454 の各カードに個別にアクセスするためのビューです。このビューにはカードが図で表示され、カードを管理するためのタブとサブタブにアクセスできます。
- ネットワークビュー — リング内のすべてのノードが表示されます。スーパーユーザは、すべてのユーザが同じネットワークビューを見ることができるよう、または、ユーザがマップを使ってカスタムビューを作成できるようにこの機能を設定できます。このビューでは、ネットワークを管理するためのタブとサブタブにアクセスできます。ネットワークビューには、ドメインを含むことができます。ドメインは、メンテナンスを容易にするために、ノードまたはノードのグループを分離するときに使用されます。ドメインをダブルクリックすると、ドメイン内のすべてのノードが表示されます。このノードのうち、ドメインに接続されているものはグレーで表示されます。

表 A-1 に、これらのビューの切り替え方法を示します。方法は何通りかあります。

表 A-1 CTC ビューの切り替え

表示対象	切り替え方法
ノードビュー	<ul style="list-style-type: none"> <li>• ノードにログインします。ノードビューがデフォルトのビューになっています。</li> <li>• ネットワークビューでノードアイコンをダブルクリックするか、またはノードを右クリックしてショートカットメニューから <b>Open Node</b> を選択します。</li> <li>• ネットワークビューでノードアイコンをシングルクリックし、View メニューから <b>Go To Selected Object View</b> を選択します。</li> <li>• View メニューから、<b>Go To Other Node</b> を選択し、次にショートカットメニューからノードを選択します。</li> <li>• CTC のツールバーにある矢印を使用して、ビューのレベルを上下に切り替えます。たとえばネットワークビューからノードビューへ切り替えるには、ネットワークビューでノードをクリックし、次に下向きの矢印をクリックします。</li> </ul>
ホームビュー(ネットワーク内で、ログインしたときの最初のノードのノードビュー)	<ul style="list-style-type: none"> <li>• CTC View メニューから <b>Go To Home View</b> を選択します。</li> </ul>
ネットワークビュー	<ul style="list-style-type: none"> <li>• ノードビューで上向きの矢印をクリックするか、または CTC のツールバーにある <b>Network View</b> ツールをクリックします。</li> <li>• View メニューから、<b>Go To Network View</b> を選択します。</li> </ul>
カードビュー	<ul style="list-style-type: none"> <li>• ノードビューでカードをダブルクリックするか、またはカードを右クリックして <b>Open Card</b> を選択します。</li> <li>• ノードビューでカードアイコンをシングルクリックし、View メニューから <b>Go To Selected Object View</b> を選択します。</li> <li>• CTC のツールバーにある矢印を使用して、ビューのレベルを上下に切り替えます。たとえばノードビューからカードビューへ切り替えるには、ノードビューでカードをクリックし、次に下向きの矢印をクリックします。</li> </ul>



表 A-2 に、ネットワーク ビューのマップにあるノード アイコンを示します。

表 A-2 ネットワーク ビュー マップのノード アイコン









ノード名	アイコン	内容
SONET ハイブリッド OADM ハイブリッド回線 増幅器 ハイブリッド端末 受動ハイブリッド 端末 増幅 TDM		<p>SONET、ハイブリッド、または増幅 Time Division Multiplexing (TDM; 時分割多重) の各ノードは、交差した矢印の付いた円柱型のアイコンで表示されます。</p> <ul style="list-style-type: none"> <li>SONET ノードには、OC-N カード、電気回路カード、クロスコネクタなどが含まれます。</li> <li>ハイブリッドの Optical Add/Drop Multiplexer (OADM; 光分岐挿入装置) ノードには、少なくとも 1 つの AD-xC カードまたは AD-xB カードと、2 つの TCC2/TCC2P カードがあります。TDM カードは、使用可能なスロットであればどのスロットにも取り付けすることができます。</li> <li>ハイブリッド回線増幅ノードには、増幅器、および TDM と Dense Wavelength Division Multiplexing (DWDM; 高密度波長分割多重) の両方のカードがあります。</li> <li>ハイブリッド端末ノードには、少なくとも 1 つの 32MUX-O カード、1 つの 32DMX-O カード、増幅器、2 つの TCC2/TCC2P カード、および TDM カードがあります。</li> <li>受動ハイブリッド端末ノードには、増幅器を除いてハイブリッド端末ノードと同様の機器が含まれています。</li> <li>増幅 TDM ノードは、TDM カードと光増幅器が実装されている ONS 15454 ノード間で、その接続距離を延ばすことができるノードです。増幅 TDM ノードには、OPT-BST 増幅器または AD-1C カードのいずれかが含まれています。</li> </ul>
ハブ		DWDM ハブ ノードは、増幅器のマークが 2 つ付いた 3 次元の円柱型アイコンで表示されます。ハブ ノードには、少なくとも 2 つの 32 チャンネル デマルチプレクサと 2 つの 32 チャンネル マルチプレクサが含まれています。OADM カードはプロビジョニングされていません。
OADM		DWDM OADM ノードは、矢印の付いた 3 次元の円柱型アイコンで表示されます。OADM ノードには、少なくとも 1 つのチャンネル OADM (AD-xC) またはバンド OADM (AD-xB) が含まれています。32 チャンネル マルチプレクサカードと 32 チャンネル デマルチプレクサカードはプロビジョニングされていません。
ROADM		Reconfigurable OADM (ROADM) ノードは、2 つの増幅器のマークとその間に矢印のある、3 次元の円柱型アイコンで表示されます。ROADM ノードには、少なくとも 1 つの 32 チャンネル Wavelength Selective Switch (32WSS) があります。シングル スロットの 32 チャンネル デマルチプレクサ (32DMX) またはダブル スロットの 32DMX-O デマルチプレクサを実装することもできますが、必須ではありません。TXP (トランスポンダ) と MXP (マックスポンダ) は、スロット 6 とスロット 12 に取り付けすることができます。また増幅器を使用しなければ、TXP と MXP はスロット 1 とスロット 17 に取り付けすることもできます。Optical Booster (OPT-BST) が実装されていない場合は、Optical Service Channel and Combiner/Separator Module (OSC-CSM) カードはスロット 2 と 16 に取り付け、スロット 8 と 10 は空になります。

表 A-2 ネットワーク ビュー マップのノードアイコン (続き)

ノード名	アイコン	内容
端末 (ウェスト)		<p>端末 (ウェスト) ノードは、ウェスト側に増幅器のマークが付いた 3 次元の円柱型アイコンで表示されます。</p> <ul style="list-style-type: none"> <li>• 端末ノードには、32 チャンネル デマルチプレクサと 32 チャンネル マルチプレクサが 1 つずつ含まれています。OADM カードはプロビジョニングされていません。</li> <li>• フレキシブル端末ノードには、OADM カードと増幅器カードが一式含まれています。</li> </ul>
端末 (イースト)		<p>端末 (イースト) ノードは、イースト側に増幅器のマークが付いた 3 次元の円柱型アイコンで表示されます。</p> <ul style="list-style-type: none"> <li>• 端末ノードには、32 チャンネル デマルチプレクサと 32 チャンネル マルチプレクサが 1 つずつ含まれています。OADM カードはプロビジョニングされていません。</li> <li>• フレキシブル端末ノードには、OADM カードと増幅器カードが一式含まれています。</li> </ul>
回線 OSC 再生成回線		<p>Optical Service Channel (OSC) 再生成回線ノードは、2 本の矢印がそれぞれウェストとイーストを指している 3 次元の円柱型アイコンで表示されます。</p> <ul style="list-style-type: none"> <li>• 回線ノードには、OPT-PRE 増幅器または OPT-BST 増幅器だけをプロビジョニングします。</li> <li>• OSC 再生成回線ノードには、2 枚の OSC-CSM カードがあります。</li> </ul>
不明		<p>不明な DWDM ノードは、北向きの矢印が付いた 3 次元の円柱型アイコンで表示されます。不明なノードとは、そのノードにプロビジョニングされているカードでは、定義されている DWDM ノードのどのカテゴリにもあてはまらないノードを意味します。</p>

## CTC ウィンドウの管理

CTC のウィンドウでは、ビューのアクセスや管理アクションの実行にさまざまなナビゲーション方式が利用できます。図の領域にあるオブジェクトは、ダブルクリックまたは右クリックすることができます。また、ノード、カード、およびポートは、その上にマウスのポインタを置くと、ステータス情報がポップアップして表示されます。

## CTC のメニューとツールバーのオプション

CTC ウィンドウにあるメニューバーとツールバーには、CTC の主要な機能が用意されています。表 A-3 に、CTC のメニューとツールバーで使用可能なアクションを示します。

表 A-3 CTC のメニューバーとツールバーで使用可能なオプション

メニュー	メニュー オプション	ツールバー	内容
File	Add Node		現在のセッションにノードを追加します。「DLP-A62 現在のセッションまたはログイングループへのノードの追加」(p.17-75)を参照してください。
	Delete Selected Node		現在のセッションからノードを削除します。
	Lock CTC		CTC セッションを閉じないで CTC をロックします。CTC を開くには、ユーザ名とパスワードが必要です。
	Print		CTC のデータを印刷します。「DLP-A531 CTC データの印刷」(p.22-34)を参照してください。
	Export		CTC のデータをエクスポートします。「DLP-A532 CTC データのエクスポート」(p.22-35)を参照してください。
	Exit	—	CTC のセッションを閉じます。
Edit	Preferences		<p>Preferences ダイアログボックスが表示されます。このダイアログボックスには次のタブがあります。</p> <ul style="list-style-type: none"> <li>General — イベントのデフォルトを変更したり、初期設定を管理したりできます。</li> <li>Login Node Groups — ログイン ノード グループを作成できます。「DLP-A61 ログイン ノード グループの作成」(p.17-74)を参照してください。</li> <li>Map — ネットワーク ビューをカスタマイズできます。「DLP-A145 ネットワーク ビューの背景色の変更」(p.18-19)と「DLP-A268 ネットワーク ビューへのカスタム背景マップの適用」(p.19-58)を参照してください。</li> <li>Circuit — 回線スパンの色を変更できます。「DLP-A232 アクティブ スパンおよびスタンバイ スパンの色の変更」(p.19-25)を参照してください。</li> <li>Firewall — ファイアウォールを介して ONS 15454 へアクセスできるようにする場合は、このオプションを使用して Internet Inter-ORB Protocol (IIOP) のリスナー ポートと Secure Sockets Layer Inter-ORB Protocol (SSLIOP) を設定します。「NTP-A27 ファイアウォール アクセスを目的とした ONS 15454 の設定」(p.4-10)を参照してください。</li> <li>JRE — Java Runtime Environment (JRE; Java ランタイム環境) の別のバージョンを選択できます。「DLP-A431 JRE バージョンの入れ替え」(p.21-10)を参照してください。</li> </ul>

## ■ CTC ウィンドウの管理

表 A-3 CTC のメニューバーとツールバーで使用可能なオプション (続き)

メニュー	メニュー オプション	ツールバー	内容
View	Go To Previous View		1 つ前の CTC ビューを表示します。
	Go To Next View		次の CTC ビューを表示します。前のビューに戻った場合にだけ使用できます。Go to Previous View と Go to Next View は、Web ブラウザの「進む」と「戻る」の移動方法に似ています。
	Go To Parent View		ネットワーク ビュー、ノード ビュー、およびカード ビューといった CTC ビューの階層を参照します。カード ビューでこのコマンドを使用するとノード ビューが表示され、ノード ビューでこのコマンドを使用するとネットワーク ビューが表示されます。ネットワーク ビューでは使用できません。
	Go To Selected Object View		CTC ウィンドウに、選択されているオブジェクトを表示します。
	Go To Home View		ノード ビューにログイン ノードを表示します。
	Go To Network View		ネットワーク ビューを表示します。
	Go To Other Node		ネットワーク ノードを表示したいときに使用します。ダイアログボックスが表示されるので、ノード名または IP アドレスを入力します。
	Show Status Bar	—	この項目をクリックすると、CTC ウィンドウの下部にあるステータスバーの表示 / 非表示が切り替わります。
	Show Tool Bar	—	この項目をクリックすると、CTC ツールバーの表示 / 非表示が切り替わります。
—	—		ネットワーク ビュー領域内の表示をズーム アウトします (ツールバーのみ)。
—	—		ネットワーク ビュー領域内の表示をズーム インします (ツールバーのみ)。
—	—		選択されているネットワーク ビュー領域内の表示をズーム インします (ツールバーのみ)。

表 A-3 CTC のメニューバーとツールバーで使用可能なオプション (続き)



メニュー	メニュー オプション	ツールバー	内容
Tools	Circuits	—	次のオプションを表示します。 <ul style="list-style-type: none"> <li>Repair Circuits — ONS 15454 の Alarm Interface Panel (AIP) を交換したあとに、不完全な回線を修復します。詳細については、『Cisco ONS 15454 Troubleshooting Guide』を参照してください。</li> <li>Reconfigure Circuits — 回線を再設定できます。詳細については、「NTP-A298 回線の再設定」(p.7-16)を参照してください。</li> <li>Set Path Selector Attributes — Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) 回線パス セレクタの属性を編集できます。「DLP-A233 UPSR 回線パス セレクタの編集」(p.19-26)を参照してください。</li> <li>Set Circuit State — 回線の状態を変更できます。「DLP-A230 回線のサービス状態の変更」(p.19-22)を参照してください。</li> <li>Roll Circuit — サービスの中断なしにライブ トラフィックを再ルーティングします。</li> <li>Delete Rolls — ロール完了後に、CTC で削除されなかったロールを削除します。</li> </ul>
	Overhead Circuits	—	Repair IP Tunnels オプションを表示します。このオプションによって、ノードの IP アドレスを変更した結果 INCOMPLETE 状態になった回線を修復することができます。「DLP-A336 IP トンネルの修復」(p.20-26)を参照してください。
	Topology Upgrade	—	次のオプションを表示します。 <ul style="list-style-type: none"> <li>Convert UPSR to BLSR — UPSR を Bidirectional Line Switch Ring (BLSR; 双方向ライン スイッチ型リング) に変換します。「NTP-A267 UPSR から 2 ファイバ BLSR への自動変換」(p.13-16)を参照してください。</li> <li>Convert Unprotected to UPSR — ポイントツーポイントまたはリニア Add Drop Multiplexer (ADM; 分岐挿入装置) を UPSR に変換します。「NTP-A342 ポイントツーポイント型またはリニア ADM から UPSR への自動変換」(p.13-13)を参照してください。</li> </ul>
	Manage VLANs	—	作成された VLAN (仮想 LAN) のリストを表示します。このリストから VLAN を作成および削除できます。「NTP-A325 VLAN の管理」(p.7-18)を参照してください。
	Open TL1 Connection		TL1 セッションのダイアログボックスを表示します。ここでは、特定のノードの TL1 セッションを作成できます。『Cisco ONS SONET TL1 Command Guide』および『Cisco ONS SONET TL1 Reference Guide』を参照してください。
	Open IOS Connection		ノードに Cisco IOS の機能を備えたカード (ML シリーズ カード) が取り付けられている場合に、Cisco IOS CLI (コマンドライン インターフェイス) のダイアログボックスを表示します。『Ethernet Card Software Feature and Configuration Guide』を参照してください。
	Update CTC	—	ネットワーク検出中に新しいバージョンが見つかった場合、CTC を新しいバージョンに更新できます。

表 A-3 CTC のメニューバーとツールバーで使用可能なオプション (続き)

メニュー	メニュー オプション	ツールバー	内容
Help	Contents and Index	—	オンライン ヘルプのウィンドウを表示します。
	User Manuals	—	Cisco ONS 15454 のマニュアルを表示します。
	About CTC	—	CTC セッションのソフトウェア バージョンとノードを表示します。
—	Network Scope	—	選択したネットワーク スコープを表示します。ネットワーク スコープ ドロップダウン リストには、DWDM、TEM、All の 3 つのオプションがあります。DWDM を選択すると、DWDM とハイブリッド ノードがネットワーク ビューのマップに表示されます。TDM を選択すると、TDM とハイブリッド ノードがネットワーク ビューのマップに表示されます。All を選択すると、ネットワーク上のすべてのノードがネットワーク ビューのマップに表示されます。
—	Link Filter		<p>Link Filter ダイアログボックスを開き、簡略ネットワーク マップに表示するリンク クラスを選択できるようにします。使用できるクラスは、選択したネットワーク スコープにより異なります。</p> <ul style="list-style-type: none"> <li>• ALL — DCC、GCC、OTS、PPC、サーバ証跡</li> <li>• DWDM — GCC、OTS、PPC</li> <li>• TDM — DCC、PPC、サーバ証跡</li> </ul>
—	—		<p>Collapse/Expand Links ダイアログボックスを開き、リンク タイプに基づいたネットワーク ビューのリンクをグローバルに拡張または統合できるようにします。</p>
—	—	 	<p>CTC Alerts ダイアログボックスを開きます。このダイアログボックスには、特定の CTC バックグラウンド タスクについてそのステータスが表示されます。CTC Alerts ツールバー アイコンに赤い三角形が表示されている場合は、まだ読んでいない通知メッセージがあります。未読の通知メッセージがない場合は、CTC Alerts ツールバー アイコンにグレーの三角形が表示されます。通知メッセージには次のものがあります。</p> <ul style="list-style-type: none"> <li>• Network disconnection ( ネットワークの切断 )</li> <li>• Send-PDIP inconsistency( Send-PDIP の不一致 )— SEND-PDIP の設定がログイン ノードと一致しないノードが CTC によって新しく検出されました。</li> <li>• Circuit deletion status ( 回線削除ステータス )— [Notify when complete] を選択しておく、回線の削除処理が完了したときに報告があります。詳細は、「<a href="#">NTP-A278 オーバーヘッド回線およびサーバ証跡の変更と削除</a>」(p.7-6) を参照してください。回線の削除エラーが発生すると、必ず CTC Alerts ウィンドウに報告されます。</li> <li>• Conditions retrieval error ( 状態の取得エラー )</li> <li>• Software download failure ( ソフトウェアのダウンロード失敗 )</li> </ul> <p>CTC Alerts ダイアログボックスで Save ボタンをクリックしてテキストファイルの保存先ディレクトリを指定すれば、この通知を保存することができます。</p> <p>デフォルトで、CTC Alerts ダイアログボックスは自動的に開くように設定されています。自動ポップアップをディセーブルにする方法については、「<a href="#">DLP-A327 CTC Alerts ダイアログボックスの自動ポップアップ設定</a>」(p.20-18) を参照してください。</p>

## CTC マウス オプション

CTC では、メニュー バーとツールバー以外にも、ウィンドウ内の項目をマウスでダブルクリックするか、右クリックしてショートカットメニューからアクションを選択することで、アクションを起動できます。表 A-4 に、CTC ウィンドウのマウスのショートカットを示します。

表 A-4 CTC ウィンドウのマウスのショートカット

操作	内容
ダブルクリック	<ul style="list-style-type: none"> <li>ネットワーク ビュー内のノード — ノード ビューが表示されます。</li> <li>ネットワーク ビュー内のドメイン — ドメイン ビューが表示されます。</li> <li>ノード ビュー内のカード — カード ビューが表示されます。</li> <li>アラーム / イベント — アラームまたはイベントの発生したオブジェクトが表示されます。</li> <li>回線 — Edit Circuit ウィンドウが表示されます。</li> </ul>
右クリック	<ul style="list-style-type: none"> <li>ネットワーク ビューの図領域 — 次のアクションを行うためのメニューが表示されます。新規ドメインの作成、図の位置またはズーム レベルの変更、マップ レイアウトの保存 (セキュリティ レベルがスーパーユーザの場合)、ネットワーク ビューのデフォルト レイアウトのリセット、背景のイメージと色の設定、変更、または削除、ノード位置の保存またはリセット</li> <li>ネットワーク ビュー内のドメイン — ドメインを開くとき、ドメインの概要を表示するとき、ドメインの名前を変更するとき、およびドメインを削除するときに表示できるメニューが表示されます。</li> <li>ネットワーク ビュー内のノード — 次のアクションを行うためのメニューが表示されます。ノードのオープン、Provisioning &gt; General タブに設定されているノード アイコンの垂直位置および水平位置のリセット、ノードの削除、自動レイアウトによるノード位置の固定、回線のプロビジョニング、チャネルのプロビジョニング、新規ノードに伴う回線またはチャネルの更新</li> <li>ネットワーク ビュー内のスパン — スパンの送信元ポートと宛先ポート、保護スキーム、光または電気レベルの情報を得るためのメニューが表示されます。また、Circuits on Spans ダイアログボックスを表示してその他のスパン情報を表示したり、UPSR の保護切り替えを実行することができます。スパンの更新も、このメニューから行えます。</li> <li>ノード ビュー内のカード — カードのオープン、削除、リセット、変更を行うためのメニューが表示されます。表示されるコマンドは、選択したカードの種類で異なります。</li> <li>カード ビュー内のカード — カードのリセットまたは親ビュー (ノード ビュー) への移動を行うためのメニューが表示されます。</li> <li>ノード ビュー内の空きスロット — 事前プロビジョニングを行うためのメニューが表示されます。メニューには、そのスロットに対して事前プロビジョニングの可能なカードが表示されます。</li> </ul>

表 A-4 CTC ウィンドウのマウスのショートカット (続き)

操作	内容
マウスカーソルの移動	<ul style="list-style-type: none"> <li>ネットワーク ビュー内のノードの上 — ノード アラームの要約が表示され、ノード アイコンがマップの範囲外に移動している場合は、警告が出されます。</li> <li>ネットワーク ビュー内のスパンの上 — 回線 (ノード、スロット、ポート) の帯域幅と保護情報が表示されます。DWDM スパンの場合は、光の方向と光リング ID が表示されます。スパンが TXP/MXP のトランクポートで終端している場合は、対応する DWDM の波長も表示されます。</li> <li>ノード ビューのカードの上 — カードのタイプとステータス、およびアラーム プロファイル ステータスが表示されます。DWDM カードの場合は、カードのタイプに応じて、帯域の数またはチャンネルの数も表示されます。</li> <li>ネットワーク ビューのドメインの上 — ドメイン名およびドメイン内のノード数が表示されます。</li> <li>ノード ビュー内のカード ポートの上 — カードの名前、ポートの状態およびアラーム プロファイル ステータスが表示されます。</li> <li>カード ビュー内のカード ポートの上 — ポートの状態、保護ステータス (該当する場合)、アラーム プロファイル ステータスが表示されます。DWDM カードの場合は、カードのタイプ、ポートの状態、およびアラーム プロファイル ステータスに応じて、ポート番号にチャンネル、帯域、または回線のラベルが付きます。</li> </ul>

## ノード ビューのショートカット

表 A-5 に、CTC ウィンドウでマウスを動かすことによって行える、ONS 15454 カードに対するアクションを示します。

表 A-5 ノード ビューのカードに関連するショートカット

アクション	ショートカット
カード情報の表示	ノード ビューの図でカードの上にマウスを移動させると、カード タイプに応じたツールチップ、カードのステータス (アクティブまたはスタンバイ)、アラームの最高レベル (設定されている場合)、およびそのカードで使用されているアラーム プロファイルが表示されます。
カードのオープン、リセット、または削除	ノード ビューで、カードを右クリックします。カード ビューでカードを表示する場合は <b>Open Card</b> を、カードを削除する場合は <b>Delete Card</b> を、カードをリセットする場合は <b>Reset Card</b> をそれぞれ選択します。
スロットの事前プロビジョニング	ノード ビューで、空きスロットを右クリックします。スロットにプロビジョニングするカードのタイプをショートカット メニューから選択します。
カードの変更	ノード ビューで、OC-N カードまたは DS3 カードを右クリックして、 <b>Change Card</b> を選択します。Change Card ダイアログボックスで、カードのタイプを選択します。Change Card は、Data Communication Channel (DCC; データ通信チャンネル) の終端、保護、回線、およびリングといったカードのプロビジョニング情報をすべて維持します。




## ネットワーク ビューで行う作業

ネットワーク ビューの図領域、またはノード、スパン、ドメインのいずれかを右クリックすると、ショートカット メニューが表示されます。表 A-6 に、ネットワーク ビューから行えるアクションを示します。

表 A-6 ネットワーク ビューのネットワーク管理の作業

アクション	機能
ノードを開く	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>ノード アイコンをダブルクリックします。</li> <li>ノード 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 <b>Open Node</b> を選択します。</li> <li>ノードをクリックして、View メニューから <b>Go To Selected Object View</b> を選択します。</li> <li>View メニューから、<b>Go To Other Node</b> を選択します。Select Node ダイアログボックスからノードを選択します。</li> <li>Alarms タブまたは History タブでノード アラームまたはイベントをダブルクリックします。</li> </ul>
ノード アイコンを移動する	Ctrl キーとマウスの左ボタンを同時に押した状態で、ノード アイコンを別の位置までドラッグします。
リンクを統合する	リンクを右クリックして、ショートカット メニューから <b>Consolidate/Expand</b> を選択します。手順の詳細については、 <a href="#">第 11 章「ノード設定の変更」</a> を参照してください。
ノード アイコンの位置をリセットする	ノードを右クリックして、ショートカット メニューから <b>Reset Node Position</b> を選択します。ノード アイコンは、ノード ビューにある Provisioning > General タブの垂直/水平位置指定フィールドで定義されている位置に移動します。
回線をプロビジョニングする	ノードを右クリックします。ショートカット メニューから <b>Provision Circuit To</b> を選択して、回線のプロビジョニング対象となるノードを選択します。回線の作成手順については、 <a href="#">第 6 章「回線と VT トンネルの作成」</a> を参照してください。
新規 ノードの追加に伴って回線を更新する	ノードを右クリックして、ショートカット メニューから <b>Update Circuits With New Node</b> を選択します。このコマンドは、新規ノードを追加し、回線がそのノードを経由するようにしたい場合に使用します。
リンクのエンドポイントを表示する	スパンを右クリックします。ショートカット メニューから、表示したいドロップ ポートに応じて、 <b>Go To &lt;[node]&gt; &lt;[port]&gt; &lt;[slot]&gt;</b> を選択します。CTC によって、カード ビューにカードが表示されます。
スパン プロパティを表示する	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>スパンの上にマウスを移動すると、そのスパンの近くにプロパティが表示されます。</li> <li>スパンをクリックすると、ウィンドウの左上隅にプロパティが表示されます。</li> <li>スパンを右クリックすると、ショートカット メニューの上部にプロパティが表示されます。</li> </ul>
スパン全体に対して UPSR 保護切り替えを実行する	ネットワーク スパンを右クリックして、 <b>Circuits</b> をクリックします。Circuits on Span ダイアログボックスの UPSR Span Switching フィールドに、切り替えオプションが表示されます。

表 A-6 ネットワーク ビューのネットワーク管理の作業 (続き)

アクション	機能
DWDM スパン プロパティを表示する	DWDM ネットワーク スパンを右クリックして、 <b>Circuits</b> をクリックします。Optical Channel Network Connection (OCHNC)、光の方向、および回線が表示されます。
スパンをアップグレードする	スパンを右クリックして、ショートカット メニューから <b>Upgrade Span</b> を選択します。
	 <p>(注) スパンのアップグレード情報と手順の詳細については、<a href="#">第 12 章「カードとスパンのアップグレード」</a>を参照してください。</p>

## テーブル表示オプション

テーブルのカラムを右クリックするとメニューが表示されます。表 A-7 に、テーブルの表示オプションを示します。オプションには、CTC テーブルにあるカラムの再配置または非表示や、プライマリ キーまたはセカンダリ キー (カラム) によるテーブルのソートなどがあります。

表 A-7 テーブル表示オプション

機能	クリック操作	右クリックによるショートカットメニュー
カラムのサイズ変更	カラムの境界をクリックし、そのまま押した状態で左右にドラッグします。	—
カラム順序の再配置	カラム ヘッダーをクリックし、そのまま押した状態で左右にドラッグします。	—
カラム順序のリセット	—	<b>Reset Columns Order/Visibility</b> を選択します。
カラムの非表示	—	<b>Hide Column</b> を選択します。
カラムの表示	—	<b>Show Column &gt; column_name</b> を選択します。
表示されていないすべてのカラムの表示	—	<b>Reset Columns Order/Visibility</b> を選択します。
テーブルのソート (プライマリ)	カラム ヘッダーをクリックすると、クリックのたびにソートの方向が変わります (昇順または降順)。	<b>Sort Column</b> を選択します。
テーブルのソート (セカンダリ ソート キー)	<b>Shift</b> キーを押した状態で、カラム ヘッダーをクリックします。	<b>Sort Column (incremental)</b> を選択します。
ソートのリセット	—	<b>Reset Sorting</b> を選択します。
テーブル行数の表示	—	[ <b>Row count=;</b> ] のあとに表示されている行数を表示します。この項目は、ショートカット メニューの最後にあります。

## 装置インベントリ

ノード ビューの Inventory タブには、ONS 15454 装置に関する次のようなボタンと情報が表示されます。

- Delete ボタン — ノード ビューからカードを削除する場合は、マウスでカードを選択したあと、このボタンを押します。
- Reset ボタン — カードをリセットする場合は、マウスでカードを選択したあと、このボタンを押します。
- Location — 機器の設置場所（シャーシまたはスロット番号）です。
- Eqpt Type — 特定のカード名ではなく、たとえば OC-12 や DS-1 といった、装置のタイプが表示されます。
- Actual Eqpt Type — たとえば OC12 IR/STM4 SH 1310 といった、実際の装置のタイプが表示されます。
- Admin State — ネットワークがカードのサービスを変更できる状態にあれば、カードのサービス状態が変更されます。カード状態の詳細については、『Cisco ONS 15454 Reference Manual』の付録「Administrative and Service States」を参照してください。
  - IS — カードのサービス状態を In-Service and Normal (IS-NR) にします。
  - OOS,MA — カードのサービス状態を Out-of-Service and Autonomous, Maintenance (OOS-AU,MT) にします。
- Service State — カードの現在のサービス状態が表示されます。この情報は自律的に生成され、カードの全体的な状態を表します。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。カード状態の詳細については、『Cisco ONS 15454 Reference Manual』の付録「Administrative and Service States」を参照してください。カードのサービスには、次の状態があります。
  - IS-NR ( In-Service and Normal )
  - OOS-AU,AINS & MEA ( Out-of-Service and Autonomous, Auto In-Service and Mismatched Equipment )
  - OOS-AU,AINS & SWDL ( Out-of-Service and Autonomous, Auto In-Service and Software Download )
  - OOS-AU,AINS & UEQ ( Out-of-Service and Autonomous, Auto In-Service and Unequipped )
  - OOS-AU,MEA ( Out-of-Service and Autonomous, Mismatched Equipment )
  - OOS-AU,SWDL ( Out-of-Service and Autonomous, Software Download )
  - OOS-AU,UEQ ( Out-of-Service and Autonomous, Unequipped )
  - OOS-AUMA,MEA & MT ( Out-of-Service and Autonomous Management, Mismatched Equipment and Maintenance )
  - OOS-AUMA,MEA & UAS ( Out-of-Service and Autonomous Management, Mismatched Equipment and Unassigned )
  - OOS-AUMA,MT & SWDL ( Out-of-Service and Autonomous Management, Maintenance and Software Download )
  - OOS-AUMA,MT & UEQ ( Out-of-Service and Autonomous Management, Maintenance and Unequipped )
  - OOS-AUMA,UAS ( Out-of-Service and Autonomous Management, Unassigned )
  - OOS-AUMA,UAS & UEQ ( Out-of-Service and Autonomous Management, Unassigned and Unequipped )
  - OOS-MA,MT ( Out-of-Service and Management, Maintenance )
- HW Part # — ハードウェアの部品番号が表示されます。この番号は、カードまたは装置の上面に印刷されています。
- HW Rev — ハードウェアのリビジョン番号が表示されます。
- Serial # — 装置のシリアル番号が表示されます。カードごとに固有の番号です。

## ■ 装置インベントリ

- CLEI Code — Common Language Equipment Identifier (CLEI) コードが表示されます。
- Firmware Rev — ONS 15454 カードには Application Specific Integrated Circuit (ASIC; 特定用途向け IC) チップが実装されていますが、そのチップで使用しているソフトウェアのリビジョン番号が表示されます。
- Product ID — ファントレイ、シャーシ、カードといったハードウェアコンポーネントの製造時のプロダクト ID が表示されます。Software Release 4.6 より前の旧装置については、Product ID カラムに [N/A] と表示されます。
- Version ID — ファントレイ、シャーシ、カードなどの製造時のバージョン ID が表示されます。Software Release 4.6 より前の旧装置については、Version ID カラムに [N/A] と表示されます。



## Numerics

### 1+1 光ポート保護

- 削除 18-25
- 作成 17-87
- 説明 4-13
- テスト 17-92
- トラフィックの切り替え、外部切り替えコマンドを参照
- 変更 18-24
- ポートのアクティブ/スタンバイ状態の確認 18-59

### 1:1 電気回路カード保護

- DS-1 カードの 1:N 保護への変換 18-53
- DS-3 カードの 1:N 保護への変換 18-55
- DS3-12E カードの 1:1 から 1:N 保護への変換 18-57
- 削除 18-25
- 作成 17-85
- 説明 4-12
- 変更 18-22

### 1:N 電気回路カード保護

- DS-1 カードの 1:1 保護からの変換 18-53
- DS-3 カードの 1:1 保護からの変換 18-55
- DS3-12E カードの 1:1 保護からの変換 18-57
- 削除 18-25
- 作成 17-86
- 説明 4-12
- 変更 18-23

15454\_MRC-12 カード、MRC-12 カードを参照

## A

Add Drop Multiplexer、リニア ADM を参照

ADM、リニア ADM を参照

### AEP

- AIC-I カードも参照
- 外付けワイヤラップ パネルの接続 1-19

バックプレーンへの取り付け 1-15

ピン割り当て 1-17

### AIC-I カード

- オーダーワイヤ設定のプロビジョニング 17-91
- オーダーワイヤ設定の変更 19-8
- 外部アラームの変更 19-7
- 外部制御の変更 19-8
- 設定の変更 10-4
- 取り付け 2-2, 17-50
- バックプレーンのピン割り当て 17-24

### AINS Soak

- DS1/E1-56 カード 20-70
- DS1-14 カード 18-33
- DS3/EC1-48 カード 20-100
- DS3-12 カード 18-37
- DS3-12E カード 18-41
- DS3i-N-12 カード 22-27
- DS3XM-12 カード 20-95
- DS3XM-6 カード 18-45
- EC1-12 カード 18-49
- 定義 19-11
- 光カード 20-81

AIP の交換 15-33

AIS スレッシュホールド 17-83

Alarm Expansion Panel、AEP を参照

A\_LAW 17-91

ALS 22-29

AMI 17-83

### AMP Champ EIA

- DS-1 AMP Champ ケーブルの取り付け 17-30
- 取り付け 17-16
- ピン割り当て 17-32

ARP スニッフィング 17-63

### AWG

- #10 1-3
- #22 および #24 1-4
- #29 1-4

- #6 1-4
- B**
- B8ZS 17-83
- BER テスター 1-4
- BIC、EIA を参照
- BITS
- BITS Facilities 17-82, 18-26
  - BITS Out 基準 17-82, 18-27
  - BITS-1 Out 15-25, 17-82, 17-84
  - BITS-2 Out 15-25, 17-82, 17-84
  - 外部タイミング ピン割り当て 17-26
  - タイミングの設定 4-11
  - バックプレーンへのタイミング線の取り付け  
17-26
- BLSR
- 2 ファイバ BLSR の手動作成 20-21
  - 2 ファイバから 4 ファイバへのアップグレード  
13-21
  - 2 ファイバの受け入れテスト 5-17
  - 4 ファイバ BLSR の手動作成 20-53
  - 4 ファイバ スパンの負荷テスト 17-99
  - 4 ファイバの受け入れテスト 5-20
  - BLSR のサブテンディング 5-48
  - DRI、DRI を参照
  - K3 バイトの再マップ 17-94
  - STS スケルチ テーブル 21-38
  - UPSR からのアップグレード 13-16, 13-19
  - UPSR のサブテンディング 5-45
  - VT スケルチ テーブル 21-40
  - ウィザードによる 2 ファイバ BLSR の作成  
20-19
  - ウィザードによる 4 ファイバ BLSR の作成  
20-51
  - 拡張バイト マッピングの確認 21-7
  - 切り替え、外部切り替えコマンドを参照
  - 単一ノードでの作成 19-28
  - ノード ID の変更 20-17
  - ノードの削除 14-7
  - ノードの削除後のタイミングの確認 18-66
  - ノードの追加 14-2
  - 半回線の作成 6-65
  - ファイバ接続の確認 5-14
  - ファイバの取り付け 17-55
  - 復元切り替え 13-8, 13-17, 13-23, 20-19, 20-51
  - プロパティの選択 5-16
  - リニア ADM からのアップグレード 13-7, 13-10
  - リングの削除 18-67
  - リングの負荷テスト 19-12
  - リング名、ノード ID、またはリングとスパンの復元  
時間の変更 13-23
- BNC EIA
- 高密度 BNC EIA も参照
  - 同軸ケーブルの取り付け 17-33
  - 取り付け 17-12
  - 取り付け工具 1-4
- BNC 取り付け工具 17-35
- C**
- CARLOSS 6-88
- CAT-5 ケーブル、LAN ケーブルを参照
- CE シリーズ イーサネット カード
- CE-1000-4 カードも参照
  - CE-100T-8 カードも参照
  - POS ポートのプロビジョニング 22-8
  - STS 回線の作成 6-47, 6-54
  - VCAT 回線の作成 6-99, 6-104
  - VCAT 回線も参照
  - 互換性のある GBIC 21-65
  - 使用率 PM パラメータの表示 20-105
  - 統計情報 PM パラメータの表示 20-103
  - 取り付け 2-13
  - パストレース機能 19-52
  - 履歴 PM パラメータの表示 20-106
- CE-1000-4 カード
- CE シリーズ イーサネット カードも参照
  - GBIC の取り付け 21-64
  - イーサネット ポートのプロビジョニング 22-3
  - フロー制御水準点 21-6
  - リセット 21-46
- CE-100T-8 カード
- CE シリーズ イーサネット カードを参照
  - イーサネット ポートのプロビジョニング 22-7
  - リセット 17-68, 19-19
- Cisco MDS 9000 スイッチ 21-18
- Cisco Transport Controller、CTC を参照
- CLEI コード A-14
- CLETOP 19-5
- CORBA、IIOP を参照
- CTC
- CTC Alerts 20-18

- CTC Alerts の情報の保存 20-24
  - IP アドレスの非表示 21-12, 21-14
  - PC の接続 3-4, 3-6
  - PC の設定も参照
  - UNIX ワークステーションの要件 20-31
  - Windows PC の要件 20-27
  - インストール ウィザード (UNIX) 20-31
  - インストール ウィザード (Windows) 20-27
  - ソフトウェア リリースの確認 17-46
  - タイミングのセットアップ 4-11
  - ツールバーにあるアイコン、ツールバーにあるアイコンを参照
  - データの印刷 22-34
  - データのエクスポート 22-35, A-5
  - データベースのバックアップ 15-6
  - ネットワーク アクセスの設定 4-9
  - ノードの設定 4-6
  - ノードのタイミングの変更 11-8
  - パフォーマンスの向上 3-2
  - ビュー、ビューを参照
  - ファイアウォール アクセス 4-10
  - ユーザのログアウト 20-9, 20-10
  - より新しいソフトウェア リリースの自動検出 3-8, A-1
  - リモート サイト アクセス 3-7
  - ログイン 3-8, 17-71
  - ログイン ノード グループ 17-74
  - CTC データの印刷 22-34, A-5
  - CTC ネットワーク ビューのカスタマイズ 11-5
  - CTC へのログイン 3-8, 17-71
- D**
- DCC**
- DCC トンネルも参照
  - IP カプセル化トンネルの作成 20-36
  - LDCC 終端の削除 20-50
  - LDCC 終端の作成 20-77
  - LDCC 終端の変更 20-67
  - SDCC 終端の削除 18-25
  - SDCC 終端の作成 20-74
  - SDCC 終端の変更 20-66
  - 自動検出のディセーブル化 17-73
- DCC トンネル**
- IP カプセル化トンネルへの変換 20-22
  - 削除 20-25
- 作成 20-7
  - DCN 4-17, 22-43
  - DCU の設置 21-1
  - DHCP
    - PC のセットアップ 17-61
    - アクセスの変更 19-57
    - イネーブル化 19-36
    - プロビジョニング 4-9
  - Dispersion Compensation Unit、DCU を参照
  - DLP、定義 xxiv
  - DNS 設定 3-6, 17-59, 17-61, 17-64
  - DRI
    - BLSR DRI 回線ルートのプロビジョニング 20-60
    - UPSR DRI 回線ホールドオフ タイマーの編集 19-50
    - インサービストポロジ アップグレード 13-21
    - 従来型 BLSR DRI 5-23
    - 従来型 BLSR/UPSR DRI 5-36
    - 従来型 UPSR DRI 5-32
    - 統合 BLSR DRI 5-25
    - 統合 BLSR/UPSR DRI 5-38
    - 統合 UPSR DRI 5-34
  - DS-1 回線、電気回線を参照
  - DS-1 ケーブル
    - 56 線ケーブル 17-30
    - AMP Champ 17-30
    - UBIC-H EIA への取り付け 21-22
    - UBIC-V EIA への取り付け 20-90
    - 固定棒 22-33
    - ツイストペアの配線 17-38
    - 電気インターフェイス アダプタ (バラン) 17-29
    - ワイヤラップ ピン フィールドへのフェライトの接続 17-40
  - DS1/E1-56 カード
    - J2 パストレースの作成 7-12
    - 回線とスレッシュホールドの設定変更 20-68
    - 低密度カードからのアップグレード 12-10
    - 電気回路カードも参照
    - 取り付け 2-11
  - DS1-14 カード
    - 1:N 保護へのアップグレード 10-5, 18-53
    - DS-1 ケーブルも参照
    - 回線とスレッシュホールドの設定変更 18-31
    - 電気回路カードも参照
  - DS1N-14 カード、DS1-14 カードを参照
  - DS-3 回線、電気回線を参照

- DS3/EC1-48 カード  
 UBIC 要件 18-60  
 回線とスレッシュホールドの設定変更 20-98  
 低密度保護からのアップグレード 12-10  
 電気回路カードも参照  
 取り付け 2-11
- DS3-12 カード  
 1:N 保護へのアップグレード 10-5  
 DS3-12E へのアップグレード 12-8  
 カードの保護グループの変更 18-55  
 回線とスレッシュホールドの設定変更 18-35  
 電気回路カードも参照
- DS3-12E カード  
 1:N 保護へのアップグレード 18-57  
 DS3-12 へのダウングレード 12-14  
 カードの保護グループの変更 18-57  
 回線とスレッシュホールドの設定変更 18-39  
 電気回路カードも参照
- DS3-12E カードの DS3-12 へのダウングレード 12-14
- DS3E、DS3-12E カードを参照
- DS3i-N-12 カード  
 回線とスレッシュホールドの設定変更 22-25  
 電気回路カードも参照  
 取り付け 2-11
- DS3XM-12 カード  
 BFDL PM パラメータの表示 20-109  
 DS-1 回線のプロビジョニング 17-104  
 DS-3 回線のプロビジョニング 22-4  
 DS-N/SONET PM パラメータの表示 20-108  
 J2 パストレースの作成 7-12  
 UBIC 要件 18-60  
 VT-DS3 Mapped Conversion 6-24, 6-42, 6-50  
 カードの保護グループの変更 21-30  
 回線とスレッシュホールドの設定変更 20-94  
 電気回路カードも参照
- DS3XM-6 カード  
 DS-1 回線のプロビジョニング 17-104  
 DS-3 回線のプロビジョニング 22-4  
 カードの保護グループの変更 21-30  
 回線とスレッシュホールドの設定変更 18-43  
 電気回路カードも参照
- DS-N カード、電気回路カードを参照
- DWDM  
 『Cisco ONS 15454 DWDM Procedure Guide』も参照  
 DWDM GBIC との互換性 21-64
- TDM と DWDM のネットワーク ビュー切り替え 21-73
- アイコン A-3
- Dynamic Host Configuration Protocol、DHCP を参照
- E
- E シリーズ イーサネット カード  
 E シリーズ カード モードのプロビジョニング 19-32
- EtherSwitch 回線 6-69
- MAC アドレス テーブル 20-4
- MAC アドレス テーブルの表示 20-4
- PM カウントのリフレッシュ 20-37
- SPR 回線 6-76
- VLAN メンバーシップ用のポートのプロビジョニング 19-17
- VLAN 容量の確認 17-108
- XC10G および XC-VXC-10G カードとのスロット互換性 2-6
- XCVT カードとのスロット互換性 2-3
- イーサネット トランク使用状況の表示 20-5
- 互換性のある GBIC 21-65
- 使用率 PM パラメータの表示 19-44
- シングルカード EtherSwitch 手動クロスコネク 6-82
- スパニングツリー情報の表示 21-9
- 統計情報 PM パラメータの表示 19-44
- 取り付け 2-13
- 光ファイバ ケーブルの配線 2-22
- ポートのプロビジョニング 19-15
- ポートマップ モードでの回線の作成 6-73
- マルチカード EtherSwitch 手動クロスコネク 6-85
- メンテナンス情報の表示 15-23
- リセット 21-46
- 履歴 PM パラメータの表示 19-45
- E1000-2 カード、E シリーズ イーサネット カードを参照
- E1000-2-G カード、E シリーズ イーサネット カードを参照
- E100T-12 カード、E シリーズ イーサネット カードを参照
- E100T-G カード、E シリーズ イーサネット カードを参照
- EC-1 カード  
 SMB EIA も参照  
 UBIC-V EIA への EC-1 ケーブルの取り付け 20-90



- 遠端側パスのモニタリング 18-9
- 回線とスレッシュホールドの設定変更 18-47
- 回線の作成 6-22, 6-28, 6-31
- 電気回路カードも参照
- EIA
  - AMP Champ EIA も参照
  - BNC EIA も参照
  - MiniBNC EIA も参照
  - SMB EIA も参照
  - UBIC-H も参照
  - UBIC-V も参照
  - 高密度 BNC EIA も参照
  - 取り付け 1-9
- EIA/TIA-232 ポート 17-28
- EMI ガスケット 17-14
- End Network Element、ENE を参照
- ENE
  - ENE のための SNMP のセットアップ 21-34
  - NMS コミュニティ スtring の入力 21-36
  - NMS コミュニティ スtring のフォーマット化 21-36
  - RADIUS 認証のノードの設定 21-41
  - ノードのプロビジョニング 19-37
- ES 22-43, 22-51
- ES-IS 22-59
- F
- FC\_MR-4 カード
  - FICON スtring 21-18
  - PM カウントのリフレッシュ間隔の変更 20-44
  - RMON アラーム スレッシュホールドの削除 20-50
  - RMON アラーム スレッシュホールドの作成 20-46
  - VCAT 回線の作成 6-99, 6-104
  - VCAT 回線も参照
  - XC10G および XC-VXC-10G カードとのスロット互換性 2-6
  - XCVT カードとのスロット互換性 2-5
  - 互換性のある GBIC 21-65
  - 使用率 PM パラメータの表示 20-42
  - スレッシュホールド変数 (MIB) 20-46
  - 統計情報 PM パラメータの表示 20-41
  - 取り付け 2-15
  - パストレース機能 19-52
  - 汎用ポートの設定変更 21-17
- 光ファイバ ケーブルの配線 2-22
- ポート設定とスレッシュホールド設定の変更 10-6
- ポートの拡張 FC/FICON 設定の変更 21-21
- ポートの距離延長設定の変更 21-19
- 履歴 PM パラメータの表示 20-43
- G
- G シリーズ イーサネット カード
  - PM カウントのリフレッシュ 20-37
  - 互換性のある GBIC 21-65
  - 使用率 PM パラメータの表示 19-44
  - 統計情報 PM パラメータの表示 19-44
  - トランスポンダ モードのポートのプロビジョニング 6-93
  - パストレース機能 19-52
  - 光ファイバ ケーブルの配線 2-22
  - フロー制御水準点 21-6
  - ポートのプロビジョニング 19-18
  - メンテナンス情報の表示 15-22
  - リセット 21-46
  - 履歴 PM パラメータの表示 19-45
- Gateway Network Element、GNE を参照
- GBIC
  - 使用可能なタイプ 21-65
  - 取り付け 21-64
  - 取り外し 21-68
- GBIC SC コネクタをネットワーク ケーブルから外す 21-68
- GNE
  - GNE のための SNMP のセットアップ 21-32
  - NMS コミュニティ スtring の入力 21-36
  - NMS コミュニティ スtring のフォーマット化 21-36
  - RADIUS 認証のノードの設定 21-41
  - 再初期化による IP アドレスの設定 19-30, 19-31
  - セキュア モードのイネーブル化 (デュアル IP アドレス) 21-11
  - ノードのプロビジョニング 19-37
- I
- IIOP
  - CTC でのリスナー ポートのプロビジョニング 17-80

- ノードでのリスナー ポートのプロビジョニング 17-79
  - リスナー ポートの変更 19-57
  - Intermediate Path Performance Monitoring、IPPM を参照
  - Internet Explorer
    - 必須バージョン 3-2
    - プロキシ サービスのディセーブル化 17-69
    - ログイン 17-71
  - IP アドレス
    - CTC によるプロビジョニング 19-35
    - CTC ログインの選択 17-73
    - LCD での場所 17-46
    - LCD による変更 17-76
    - LCD 上での設定および表示の防止 19-36
    - 修復 20-26
    - スタティック IP アドレスでのクラフト接続のセットアップ 17-58
    - セキュア (デュアル IP アドレス) モードのロック 21-12
    - セキュア (ロック) モードのときのプロキシ サーバのディセーブル化 17-70
    - セキュア (ロック) モードのときのプロキシ サーバの変更 17-69
    - デフォルト 17-71
    - ノードに対する 2 つのプロビジョニング (セキュア モード) 21-10
  - IP カプセル化トンネル
    - DCC トンネルへ変更 20-22
    - 削除 20-25
    - 作成 20-36
    - 修復 20-26
  - IP カプセル化トンネルの修復 20-26
  - IP 設定
    - プロビジョニング 19-35
    - 変更 19-57
  - IP-over-CLNS トンネル
    - 削除 22-58
    - 作成 22-52
    - 編集 22-57
  - IPPM
    - イネーブル化 18-9
    - ディセーブル化 18-9
    - モニタ対象 IPPM 18-9
  - IS Level 1 22-43
  - IS Level 1/Level 2 22-43
  - IS-IS 22-58
- J**
- J0 セクショントレース 7-9
  - J1 パストレース
    - 回線の送信元および宛先ポートでのプロビジョニング 19-51
    - 作成 7-11
    - 光ポートでのプロビジョニング 18-16
  - J2 パストレース 7-12
  - JAR ファイル、自動ダウンロード 17-73
  - Java
    - Plug-in Security Warning ダイアログボックス 21-5
    - 仮想メモリ ヒープ サイズの調整 22-61
    - ポリシー ファイル 21-6
  - JRE バージョンの入れ替え 21-10
  - JVM ヒープ サイズの調整 3-2, 22-61
- K**
- K3 バイトの再マップ 17-94
- L**
- LAN
    - LAN モデムによるリモート アクセスのセットアップ 3-7
    - OSPF のセットアップ 19-39
    - OSPF のディセーブル化 18-19
    - OSPF の変更 19-39
    - TCC2 および TCC2P カードの LAN (RJ-45) ポート 3-5
    - VLAN も参照
    - アクセスの設定 (セキュリティ) 22-5
    - ケーブルの取り付け 17-27
    - 社内 LAN 接続のセットアップ 3-6
    - デフォルト ルータの設定 19-36
    - バックプレーン LAN ポートの IP アドレスのプロビジョニング 21-10
    - プロキシ サービスをディセーブル化しているときの設定の変更 17-69
  - LAN ケーブル
    - PC から ONS 15454 への接続 3-5
    - PC から社内 LAN ポートへの接続 3-6
    - TL1 クラフト インターフェイスのための使用 17-28
    - 圧着 3-5

- 漏話 17-27
- LAN ケーブルの圧着 3-5
- LAP-D 22-43
- LC コネクタ 21-68, 21-67
- LCD
  - IP アドレス設定の非表示 19-36
  - IP アドレスの非表示 21-12, 21-14
  - IP アドレス、デフォルト ルータ、ネットワーク マスクの変更 17-76
  - アラーム カウントの表示 8-6
  - ソフトウェア バージョンの確認 17-46
  - ネットワーク設定のプロビジョニング 4-9
  - ポート ステータスの表示 20-35
- LDCC、DCC を参照
- LGX 19-6
- Line Coding
  - DS1/E1-56 カード 20-70
  - DS1-14 カード 18-32
  - DS3/EC1-48 カード 20-100
  - DS3-12E カード 18-40
  - DS3i-N-12 カード 22-26
  - DS3XM-12 カード 20-96
  - DS3XM-6 カード 18-44
- Line Length
  - DS1/E1-56 カード 20-70
  - DS1-14 カード 18-32
  - DS3/EC1-48 カード 20-100
  - DS3-12 カード 18-36
  - DS3-12E カード 18-40
  - DS3i-N-12 カード 22-26
  - DS3XM-12 カード 20-96
  - DS3XM-6 カード 18-44
  - イーサネット デバイス 21-7
- Line Type
  - DS1/E1-56 カード 20-70
  - DS1-14 カード 18-32
  - DS3/EC1-48 カード 20-100
  - DS3-12E カード 18-40
  - DS3i-N-12 カード 22-26
  - DS3XM-12 カード 20-95, 20-97
  - DS3XM-6 カード 18-44
- Link State Protocol、LSP バッファを参照
- LSP バッファ 22-43, 22-44
- M
- MAC アドレス
  - イーサネット テーブルの表示 20-4
  - セキュア モード 19-36
  - 表示専用 19-35
- MIB 20-46, 22-38
- MiniBNC EIA の取り付け 20-63
- ML シリーズ イーサネット カード
  - Cisco IOS コマンドライン インターフェイス A-7
  - POS ポートの PM パラメータ 20-12
  - VCAT 回線のプロビジョニング 6-99, 6-104
  - XC10G および XC-VXC-10G カードとのスロット互換性 2-6
  - XCVT カードとのスロット互換性 2-4
  - イーサネット ポートの PM パラメータ 20-11
  - カード モードのプロビジョニング 22-62
  - 互換性のある SFP 21-65
  - 取り付け 2-13
  - バス トレース機能 19-52
  - 光ファイバ ケーブルの配線 2-22
  - リセット 21-46
- ML1000-2 カード、ML シリーズ イーサネット カードを参照
- ML100T-12 カード、ML シリーズ イーサネット カードを参照
- ML100X-8 カード、ML シリーズ イーサネット カードを参照
- MRC-12 カード
  - PPM のプロビジョニング 21-27
  - PPM も参照
  - 光カードも参照
  - 光回線レートのプロビジョニング 21-28
  - 光回線レートの変更 21-29
  - ファイバクリップの取り付け 21-25
- MTU 22-43
- MU\_LAW 17-91
- N
- NE デフォルト値、ネットワーク要素のデフォルト値を参照
- Netscape Navigator
  - UNIX 設定時の接続のテスト 17-67
  - 必須バージョン 3-2
  - プロキシ サービスのディセーブル化 17-70

- ログイン 17-71
- Network Time Protocol 4-6
- NMS
  - SNMP セットアップによる IP アドレスのプロビジョニング 4-15, 21-32, 21-34
  - コミュニティ スtring のフォーマット化 21-36
- NMS コミュニティ スtring のフォーマット化 21-36
- NTP
  - Network Time Protocol を参照
  - 問題のない手順を参照
- NTP サーバ 4-6
  
- O
- OC-192 カード、光カードを参照
- OCH フィルタ 20-57
- OC-N カード、光カードを参照
- OSI
  - ES-IS RIB の表示 22-59
  - IP-over-CLNS トンネルの削除 22-58
  - IP-over-CLNS トンネルの作成 22-52
  - IP-over-CLNS トンネルの編集 22-57
  - IS-IS RIB の表示 22-58
  - TARP も参照
  - サブネットのイネーブル化 22-51
  - サブネットワーク接続ポイントの編集 22-56
  - 情報の管理 15-11
  - 情報の表示 15-11
  - プライマリ マニュアル エリア アドレス 22-49
  - プロビジョニング 4-17
  - プロビジョニングの変更 11-4
  - マニュアル エリア アドレスのプロビジョニング 22-50
  - ルータ設定の編集 22-55
  - ルータのプロビジョニング 22-49
  - ルーティング モードのプロビジョニング 22-43
  - ルーティング モードの変更 22-54
- OSPF
  - セットアップ 19-39
  - ディセーブル化 18-19
  - 変更 19-39
  
- P
- PC のセットアップ
  - DHCP によるクラフト接続 17-61
  - JRE のインストール 20-27
  - PC から ONS 15454 への接続 3-2
  - クラフト接続 (接続ごとに IP アドレスの設定が必要) 17-58
  - クラフト接続 (接続ごとに IP アドレスを設定しなくてよい) 17-63
  - 社内 LAN 接続 3-6
  - ブラウザのインストール 3-2
  - プロキシ サービスのディセーブル化 17-69
  - 要件 20-27
  - リモート (モデム) アクセス 3-7
- PCM 17-91
- Pluggable Port Module、PPM を参照
- PPM
  - MRC-12 カードでのプロビジョニング 21-27
  - MRC-12 カードの回線レートの変更 21-29
  - MRC-12 カード光回線レートのプロビジョニング 21-28
  - SFP も参照
  - XFP も参照
  - 管理 10-8
  - 削除 21-29
  - 事前プロビジョニング 21-47
  
- R
- RADIUS
  - 設定 21-41
  - 定義 4-5
- RAM
  - CTC の PC 要件 20-28
  - CTC の UNIX 要件 20-31
- RIP 4-9, 19-41
- RJ-45
  - LAN アクセスの防止 22-5
  - LAN ピンの割り当て 17-27
  - TCC2/TCC2P RJ-45 LAN ポート 3-5
  - バックプレーンのピン割り当て 17-24
- RMON
  - FC\_MR-4 スレッシュホールドの削除 20-50
  - FC\_MR-4 スレッシュホールドの作成 20-46
  - イーサネット スレッシュホールドの削除 22-32
  - イーサネット スレッシュホールドの作成 22-37

Routing Information Protocol、RIP を参照

## S

### SC コネクタ

- GBIC からケーブルを外す 21-68
- LGX の前面プレート 19-6
- ファイバブーツの要件 17-57

### SC ファイバジャンパ 1-4

### SD BER パラメータ

- DS1/E1-56 カード 20-70
- DS3/EC1-48 カード 20-100
- DS3-12E カード 18-40
- DS3i-N-12 カード 22-26
- DS3XM-12 カード 20-95
- DS3XM-6 カード 18-44
- EC-1 カード 18-48
- 光カード 20-79
- DS1-14 カード 18-32
- DS3-12 カード 18-36

### SDCC、DCC を参照

### SDH 18-52

### SD-P BER 4-7

### SF BER パラメータ

- DS3/EC1-48 カード 20-100
- DS3i-N-12 カード 22-26
- DS1-14 カード 18-32
- DS3-12E カード 18-40
- DS3XM-12 カード 20-95
- DS3XM-6 カード 18-44
- EC-1 カード 18-48
- 光カード 20-79

### SFP

#### PPM も参照

- 事前プロビジョニング 21-47
- 取り付け 21-64
- 取り外し 21-68
- プロビジョニングの削除 21-29

### Shell Access 22-6

### Simple Network Time Protocol、SNTP を参照

### Small Form-Factor Pluggable ( SFP )、SFP を参照

### SMB EIA

- 同軸ケーブルの取り付け 17-35
- 取り付け 17-14
- バランへの取り付け 17-29

## SNMP

- ENE のためのセットアップ 21-34
- FC\_MR-4 RMON スレッシュホールドの削除 20-50
- GNE のためのセットアップ 21-32
- イーサネット RMON スレッシュホールドの削除 22-32
- コミュニティ スtring の入力 21-36
- コミュニティ スtring のフォーマット化 21-36
- 設定の変更 11-10
- セットアップ 4-15
- トラップ宛先の削除 18-30
- トラップ宛先の修正 19-63

### SNTP 4-6

### SOCKS 4-7, 4-15, 17-79, 19-37

### Solaris、UNIX を参照

### SONET DCC、DCC を参照

### SPR 6-76

## SSM

- Message Set 17-81, 18-26
- イネーブル化 17-83, 18-26, 20-80
- ステータス 15-27

### Standard Constant 17-80

## STP

- TCC2/TCC2P のリセット 6-70
- VLAN 回線の制約 6-72
- VLAN ブロッキング 17-108
- イネーブル化 19-16
- 再収束 15-7, 15-34, 19-57
- 情報の表示 21-9
- ディセーブル化 6-71

### VT、光回線を参照

## T

### T ハンドル六角レンチ 1-3

## TARP

- MAT エントリの削除 22-53
- MAT エントリの追加 22-48
- TARP 動作パラメータのプロビジョニング 22-45
- TARP 動作パラメータの変更 22-45
- TDC からの NSAP エントリの削除 22-48
- TDC の管理 22-60
- スタティック TID/NSAP エントリの TDC への追加 22-47

- TCA
- OC-192 および MRC-12 カードのプロビジョニング  
21-45
  - イーサネット PM の表示 20-37
  - 表示 18-11, 18-12
- TCC2 カード
- LAN アクセス 3-5, 3-7, 17-27
  - LCD によるリポート 17-78
  - TCC2P へのアップグレード 12-6
  - TL1 アクセス 17-28
  - XC10G および XC-VXC-10G カードとのスロット互換性 2-5
  - XCVT カードとのスロット互換性 2-3
  - 切り替えテスト 20-45
  - クラフト線対 EIA/TIA-232 ポート 17-28
  - 障害回復のためのデータベースのクリア 15-12
  - ソフトリセット 15-21
  - データベースのバックアップ 15-6
  - データベースの復元 15-7
  - 取り付け 2-2, 17-44
  - 取り付けの確認 4-2
  - リセット 20-54
  - リポート時間 17-80
  - リポート中の LED 動作 19-37
- TCC2/TCC2P データベースのバックアップ 15-6
- TCC2P カード
- LAN アクセス 3-5, 3-7, 17-27
  - LCD によるリポート 17-78
  - TCC2 からのアップグレード 12-6
  - TL1 アクセス 17-28
  - XC10G および XC-VXC-10G カードとのスロット互換性 2-5
  - XCVT カードとのスロット互換性 2-3
  - 切り替えテスト 20-45
  - 障害回復のためのデータベースのクリア 15-12
  - セキュアモード オプション 4-9
  - セキュア(ロック)モードのイネーブル化 21-10
  - ソフトリセット 15-21
  - データベースのバックアップ 15-6
  - データベースの復元 15-7
  - 取り付け 2-2, 17-44
  - 取り付けの確認 4-2
  - リセット 20-54
  - リポート時間 17-80
  - リポート中の LED 動作 19-37
- TCP/IP
- Windows 2000 の設定変更 17-60, 17-62, 17-65
  - Windows 98 の設定変更 17-59, 17-61, 17-64
  - Windows NT の設定変更 17-59, 17-62, 17-64
  - Windows XP の設定変更 17-60, 17-63
  - ノードのセキュリティ モードのイネーブル化 21-10
- Telcordia 9-1
- Threshold Crossing Alert、TCA を参照
- TL1
- TCC2/TCC2P EIA/TIA-232 ポート接続 17-28
  - TXP または MXP トランク カードの自動調整 20-57
  - クラフト インターフェイス接続 17-28
  - ツールバーにあるアイコン A-7
  - ピン割り当て 17-29
- U
- UBIC-H EIA
- ケーブルの取り付け 21-22
  - 取り付け 20-113
- UBIC-V EIA
- ケーブルの取り付け 20-90
  - 交換 15-41
  - 取り付け 18-60
- UDC、User Data Channel を参照
- UNIX
- CTC インストール ウィザードの実行 20-31
  - ONS 15454 とのケーブル接続 3-5
  - ONS 15454 へのクラフト接続の設定 17-66
  - ソフトウェアのアップロード 19-31
  - データベースのクリア 19-31
  - プロキシ サービスのディセーブル化 17-70
- UPC 光沢剤 1-4
- UPSR
- BLSR のサブテンディング 5-47
  - BLSR へのアップグレード 13-16, 13-19
  - DRI、DRI を参照
  - アップグレード時の回線の自動ルーティング 20-111
  - アップグレード時の回線の手動ルーティング 20-111
  - 受け入れテスト 5-29
  - 回線パス セレクタの編集 19-26
  - 開放端 5-40, 5-42
  - スパンの保護切り替えテストの実行 17-103
  - ノードの削除 14-14
  - ノードの削除後のタイミングの確認 18-66

- ノードの追加 14-11
- パス セレクタのプロビジョニング 19-14
- 半回線の作成 6-67
- 半回線の送信元と宛先のプロビジョニング 20-6
- ファイバの取り付け 17-51
- ポートのプロビジョニング 5-27
- リニア ADM からのアップグレード 13-13, 13-15
- User Data Channel
  - 削除 20-25
  - 作成 19-9
- V
- VAP
  - 作成 6-40
  - 定義 6-3
- VCAT 回線
  - J1 パストレースのプロビジョニング 19-51
  - 回線ルートのプロビジョニング 20-16
  - 自動ルーティングによる回線のプロビジョニング 6-99
  - 手動ルーティングによる回線のプロビジョニング 6-104
  - 送信元と宛先のプロビジョニング 20-15
  - 名前の変更 19-24
  - メンバーのサービス状態の変更 21-16
  - メンバーの削除 20-89
  - メンバーの追加 20-85
  - メンバー名の編集 19-24
- VLAN
  - E シリーズ EtherSwitch 回線の作成 6-71
  - E シリーズ SPR 回線の作成 6-77
  - E シリーズ ハブアンドスポーク回線の作成 6-80
  - E シリーズ マルチカード EtherSwitch 手動クロスコネクタでの作成 6-83, 6-86
  - アベイラビリティの確認 17-108
  - 削除 20-26
  - 作成 21-37
  - スパニングツリーの制約 6-72
  - トポロジー ホストの管理 7-18
  - メンバーシップ用のポートのプロビジョニング 19-17
- VT トンネル
  - 自動ルーティング 6-35
  - 手動ルーティング 6-38
- 説明 6-3
- ルートのプロビジョニング 19-15
- VT、回線を参照
- W
- WINS 設定 3-6, 17-59, 17-62, 17-64
- WTR 状態 15-8
- X
- XC10G カード
  - XC-VXC-10G カードへのアップグレード 12-4
  - 切り替えテスト 19-42
  - 交換 15-28
  - スロットの互換性 2-5
  - 取り付け 2-2, 17-47
  - 取り付けの確認 4-2
- XCVT カード
  - XC10G カードへのアップグレード 12-2
  - XC-VXC-10G カードへのアップグレード 12-4
  - 切り替えテスト 19-42
  - 交換 15-28
  - スロットの互換性 2-3
  - 取り付け 2-2, 17-47
  - 取り付けの確認 4-2
- XC-VXC-10G カード
  - 切り替えテスト 19-42
  - スロットの互換性 2-5
  - 取り付け 2-2, 17-47
  - 取り付けの確認 4-2
- XFP
  - PPM も参照
  - 事前プロビジョニング 21-47
  - 取り付け 21-64
  - 取り外し 21-68
  - プロビジョニングの削除 21-29
- Y
- Y 字ケーブル保護 4-13
- あ
- アース 1-11, 17-18

- アース ケーブル 1-4
- アース ストラップ 2-25, 17-9
- アイドル時間 17-89, 17-90
- アクティブ ログイン
  - 終端 21-48
  - 表示 21-48
- アクティブ ログインの終端 21-48
- 圧着工具 1-4, 17-21
- 圧着端子 2-24, 2-25
- アップグレード
  - 1+1 ポイントツーポイント型からリニア ADM へ 13-2, 13-5
  - 1+1 リニア ADM から 2 ファイバ BLSR へ 13-7
  - 1:1 保護から 1:N 保護 への DS-1 および DS-3 保護 カード 10-5
  - 2 ファイバ BLSR から 4 ファイバ BLSR へ 13-21
  - 2 ファイバ BLSR へのアップグレード 13-16, 13-19
  - BLSR、UPSR、または 1+1 の自動 12-16
  - DS1-14 カードの 1:1 から 1:N 保護 18-53
  - DS3-12 カードから DS3-12E へ 12-8
  - DS3XM カードの 1:1 から 1:N 保護 21-30
  - SONET トポロジー 13-1
  - TCC2 カードから TCC2P カードへ 12-6
  - XCVT カードから XC10G カードへ 12-2
  - XCVT または XC10G カードから XC-VXC-10G カードへ 12-4
  - スパン A-12
  - スパン アップグレードも参照
  - 低密度電気回路カードから高密度電気回路カード へ 12-10
  - トポロジー、インサービストポロジー アップグ レードウィザードを参照
  - 光カードとスパン 12-16
  - 光スパン 12-1
  - 非保護ポイントツーポイント型から 2 ファイバ BLSR へ 13-7
  - 変換も参照
  - ポイントツーポイント型から UPSR へ 13-13, 13-15
  - リニア ADM から UPSR へ 13-13, 13-15
- アラーム
  - Alarm Expansion Panel、AEP を参照
  - LCD のアラーム カウント表示 8-6
  - アラーム レポートの抑制 22-21
  - イーサネット RMON スレッシュホールド 22-37, 22-32
  - 環境アラーム、AIC-I カードを参照
  - クリアされたアラームの表示からの削除 8-4
  - 重大度、アラーム プロファイルを参照
  - 同期 18-3
  - トラブルシューティング、『Cisco ONS 15454 Troubleshooting Guide』を参照
  - ネットワークのチェック 19-71
  - 発生（抑制なし） 22-22
  - 表示 8-3, 20-102
  - フィルタリング、アラーム フィルタリングを参照
  - 履歴 18-1
  - 履歴の表示 22-9
- アラーム ケーブル 17-23
- アラーム フィルタリング
  - イネーブル化 19-20
  - ディセーブル化 19-21
  - 変更 22-18
- アラーム プロファイル
  - カードおよびノードへの適用 18-6
  - 削除 22-17
  - 作成 22-11
  - ダウンロード 22-23
  - ポートへの適用 22-15
- アラーム プロファイルのダウンロード 22-23
- アラームおよび状態に対するネットワークのチェック 19-71
- アラームの同期 18-3
- アラームの発生 22-22
- アラーム表示信号、AIS を参照
- 安全性
  - 警告の定義 xxvi
  - 情報の検索 xxvi
- い
- イーサネット
  - E シリーズ、ML シリーズ、G シリーズおよび CE シ リーズのイーサネット カードも参照
  - PM カウントのリフレッシュ 19-46
  - RMON スレッシュホールドの削除 22-32
  - RMON スレッシュホールドの作成 22-37
  - VLAN メンバシップ用のポートのプロビジョニ ング 19-17
  - 回線 6-69 6-107
  - 回線のテスト 6-89
  - 極性検出 17-28
  - 使用率 PM パラメータの表示 19-44
  - スレッシュホールド変数（MIB） 22-38



- ハブアンドスポーク回線 6-79
  - パフォーマンスのモニタリング 9-5
  - ポートマップモードでの手動クロスコネクットの作成 6-91
  - 履歴 PM パラメータの表示 19-45
  - イーサネットカード
    - CE シリーズイーサネットカードを参照
    - E シリーズイーサネットカードを参照
    - G シリーズイーサネットカードを参照
    - ML シリーズイーサネットカードを参照
  - 緯度 4-6
  - イネーブル化
    - DHCP 19-36
    - IPPM 18-9
    - LDCC による外部ノード設定 20-67
    - OSI サブネット 22-51
    - SDCC による外部ノード 20-66
    - SSM 17-83, 18-26, 20-80
    - STP 19-16
    - アラームフィルタリング 19-20
    - セキュアモード 21-10
    - ダイアログボックスの非表示オプション 19-59
    - ポインタ位置調整カウント 18-7
  - イベント
    - 時間帯による表示 18-3
    - 履歴の表示 22-9
  - インストール
    - CD-ROM 20-28
    - CTC インストールウィザード (UNIX) 20-31
    - ブラウザ 3-2
  - インターオペラビリティ、Cisco MDS 9000 スイッチ 21-18
  - インターフェイス、ポートを参照
  - インベントリ A-13
- え
- エアーフィルタ
    - 外部ブラケット 1-3
    - 外部ブラケットの取り付け 17-4
    - 取り付け 17-4
    - 場所 1-13
    - 要件 1-13
  - エクスポート
    - CTC データ 22-35, A-5
    - オフロードも参照
  - ネットワーク要素のデフォルト値 15-48
  - エリア範囲テーブル (OSPF) 19-40
- お
- オーダーワイヤ
    - 削除 20-25
    - 設定の変更 19-8
    - プロビジョニング 17-91
    - ループの防止 17-91
  - オーバーヘッド回線
    - 回線も参照
    - 削除 7-6, 20-25
    - 作成 6-107
    - 変更 7-6
  - オフィスアース 17-18
  - オフィス電源
    - 確認 17-22
    - シェルフへの接続 17-19
    - 電源投入 17-22
  - オフロード
    - エクスポートも参照
    - 監査証跡レコード 15-16
    - 診断ファイル 15-17
  - オフ、ディセーブル化を参照
- か
- カード
    - アラームインターフェイス、AIC-I カードを参照
    - イーサネット、ML シリーズ、G シリーズ、E シリーズまたは CE シリーズのイーサネットカードを参照
    - 回線終端カード 18-7
    - 管理状態 A-13
    - 共通コントロール、TCC2 カード、TCC2P カード、XCVT カード、XC10G カード、XC-VXC-10G カードを参照
    - サービス状態 10-7, A-13
    - サービス状態の変更 19-10
    - 削除 18-65
    - シリアル番号 A-13
    - スロットの互換性 2-3
    - 電気回路、電気回路カードを参照
    - 取り付けの確認 4-2
    - 取り外しおよび交換 2-23

- 光、光カードを参照
- 部品番号 A-13
- リビジョン番号 A-13
- カード保護
  - 1:1 電気回路カード保護も参照
  - 1:1 光ポート保護も参照
  - 1:N 電気回路カード保護も参照
  - DS-1 および DS-3 カードの保護グループのアップグレード 10-5
  - 最適化 1+1 光保護も参照
  - 保護グループの作成 4-12
  - 保護グループの変更 11-6
- 回線
  - OOS-PARTIAL ステータスの修復 20-26
  - UPSR 回線の編集 19-26
  - UPSR パス セレクタのプロビジョニング 19-14
  - VCAT 回線も参照
  - VT スケルチ テーブル 21-40
  - 宛先 6-3
  - アラームの表示 8-5
  - イーサネットも参照
  - オーバーヘッド回線も参照
  - 回線のテストも参照
  - 検索 7-2, 18-15
  - サービス状態の変更 19-22
  - サービス状態も参照
  - サービス中断のない再ルーティング、ブリッジおよびロールを参照
  - 削除 20-23
  - 作成前のルートの確認 21-56
  - 情報の表示 21-2
  - ショートカットによるプロビジョニング A-11
  - ステータス 21-3
  - スパンでの表示 19-21
  - スパンのアップグレード A-12
  - 設定 7-16
  - 送信元 6-3
  - 電気回線も参照
  - 名前の編集 19-24
  - ノードの追加 A-11
  - ノード名の変更による影響 15-12
  - パススルーの確認 21-24
  - パススルー、取り外し 20-61
  - 半回線も参照
  - 光 (STS) 回線も参照
  - 表示 7-2
  - フィルタリング 19-48
  - 複数ドロップ 6-17, 6-31, 6-58
  - ブリッジおよびロール 7-15
  - 保護タイプ 21-3
  - マージ 7-17
  - モニタ回線 7-7
  - リングを対象にした STS テスト回線の作成 6-108
  - ロール 21-49 21-63
  - ロールも参照
  - ログイン時の検出のディセーブル化 17-73
  - 回線の自動ルーティング 21-54
  - 回線の手動ルーティング 21-58
  - 回線のテスト
    - E シリーズ イーサネット 6-89
    - G シリーズ イーサネット 6-97
    - STS (リングを対象) 6-108
    - 回線も参照
    - 電気 6-44
    - 光 6-63
  - 回線のマージ 7-17
  - 外部アラームおよび制御
    - アラーム ケーブルの取り付け 17-23
    - アラーム ピン 17-24
    - 外部アラームの変更 19-7
    - 外部制御の変更 19-8
    - セットアップ 8-11
  - 外部切り替えコマンド
    - BLSR 強制リング切り替えの開始 20-3
    - BLSR 強制リング切り替えのクリア 18-65
    - BLSR 手動リング切り替えの開始 20-2
    - BLSR 手動リング切り替えのクリア 19-27
    - BLSR スパン ロックアウトの開始 19-72
    - BLSR スパン ロックアウトのクリア 20-1
    - BLSR スパン切り替えテスト 17-101
    - BLSR リング切り替えテスト 17-94
    - UPSR 強制切り替えの開始 18-68
    - UPSR 強制切り替えのクリア 18-69
    - UPSR スパン切り替えテスト 17-103
    - 開始 15-18
    - クリア 15-18
    - 電気保護切り替えの開始 20-56
    - 光保護切り替えの開始 20-55
    - ロックアウトの開始 19-2
    - ロックオンの開始 19-1
    - ロックオンまたはロックアウトのクリア 19-3
  - 外部切り替えコマンドの開始 15-18

## 外部ノードの設定

- LDCC 終端の作成 20-67
- LDCC によるディセーブル化 20-67
- LDCC によるプロビジョニング 20-77
- SDCC 終端の作成 20-66
- SDCC によるディセーブル化 20-66
- SDCC によるプロビジョニング 20-74

カウント、パフォーマンス モニタリングを参照  
拡張バイト 21-7

## 確認

- BLSR 拡張バイト マッピング 21-7
- UPSR ファイバ接続 5-27, 5-40
- VLAN アベイラビリティ 17-108
- オフィス電源 17-22
- カードの取り付け 4-2
- 現用スロットの状態 18-59
- シェルフ アセンブリ 17-1
- 縮小されたリングでのタイミング 18-66
- ソフトウェア パージョン 17-46
- ネットワーク起動 6-5
- パススルー回線 21-24
- バックプレーン アライメント 17-41
- ファイバ接続の確認 5-14

仮想リンク テーブル (OSPF) 19-40

仮想リンク、プロビジョニング可能なパッチコードを参照

## 稼働中のトポロジー アップグレード ウィザード

- 2 ファイバ BLSR への UPSR のアップグレード  
13-16
- 非保護ポイントツーポイント型またはリニア ADM  
から 2 ファイバ BLSR への変換 13-7
- ポイントツーポイント型からリニア ADM への変換  
13-2
- ポイントツーポイント型またはリニア ADM から  
UPSR への変換 13-13
- リニア ADM ノードの追加 14-18

## カバー

- 下部バックプレーンからの取り外し 17-10
- 背面カバーの取り付け 1-25
- バックプレーンの金属製カバーの取り外し  
17-11

下部ブラケット、エアー フィルタ、外部ブラケットを参照

簡易ネットワーク管理プロトコル、SNMP を参照

## 監査証跡

- レコードのオフロード 15-16
- レコードの表示 15-14

## 管理

- OSI 情報 15-11
- PPM 10-8
- TDC 22-60
- VLAN 7-18
- ドメイン アイコン 18-21

## 管理状態

- DS1/E1-56 カードの設定 20-69
- DS1-14 カードのプロビジョニング 18-32
- DS3/EC1-48 カードの設定 20-99
- DS3-12 カードのプロビジョニング 18-36
- DS3-12E カードのプロビジョニング 18-40
- DS3i-N-12 カードの設定 22-27
- DS3XM-12 カードのプロビジョニング 20-96
- DS3XM-6 カードのプロビジョニング 18-44
- EC1-12 カードのプロビジョニング 18-48
- FC\_MR-4 カードの設定 21-18
- VCAT 回線の変更 21-16
- サービス状態も参照
- 光カードの設定 20-80

## き

## 機器

- カード、名前別の各カードを参照
- 機器インベントリ リスト A-13
- 設置 1-3
- ユーザが準備する部品 1-3

キャビネット コンパートメント、前面扉を参照

共通コントロール カード、TCC2 カード、TCC2P カード、XCVT カード、XC10G カード、または XC-VXC-10G カードを参照

共有パケット リング、SPR を参照

共有リソース リング グループ 6-111

## 切り替え

- TDM と DWDM のネットワーク ビュー 21-73
- 外部切り替えコマンドも参照
- 復元切り替えも参照

## &lt;

クラフト接続 3-4

## クリア

- BLSR 強制切り替え 18-65
- BLSR 手動リング切り替え 19-27
- BLSR スパン ロックアウト 20-1

- UPSR 強制切り替え 18-69
- 外部切り替えコマンド 15-18
- 現在の PM カウント 18-14
- 障害回復中のデータベース 15-12, 19-29, 19-31
- 選択した PM カウント 20-40
- ノードのタイミング基準の切り替え 20-14
- ロックオンおよびロックアウト 19-3
- クロスコネクトカード
  - XC10G カードを参照
  - XCVT カードを参照
  - XC-VXC-10G カードを参照
- クロスコネクト回線
  - E シリーズ シングルカード EtherSwitch 6-82
  - E シリーズ マルチカード EtherSwitch 6-85
  - 回線も参照
  - 定義 6-82
  - ポートマップ モードの G シリーズまたは E シリーズカード 6-91
- クロスコネクト (回線)
  - 単一光回線への 2 つのクロスコネクトのロール 21-58
  - 光回線間での 2 つのクロスコネクトのロール 21-61
- け
- 警告
  - 情報の検索 xxvi
  - 定義 xxvi
- 経度 4-6
- ゲートウェイ設定 19-37, 19-57
- ケーブル
  - CAT-5、LAN ケーブルを参照
  - DS-1 ケーブルも参照
  - LAN のための取り付け 17-27
  - RG179、同軸ケーブルを参照
  - RG59、同軸ケーブルを参照
  - TL1 クラフト インターフェイスのための取り付け 17-28
  - アラーム ケーブルの取り付け 17-23
  - コネクタ、EIA を参照
  - タイミングのための取り付け 17-26
  - 同軸ケーブルも参照
  - パッチ、パッチ ケーブルを参照
  - ユーザが準備する部品 1-4
- 権限、セキュリティを参照
- 検査
  - シェルフ アセンブリ 17-2
  - シェルフの取り付けと接続 17-41
- 検索
  - 安全性および警告に関する情報 xxvi
  - 回線 7-2, 18-15
- 検索、検索を参照
- こ
- 公開鍵セキュリティ証明書 17-72, 21-5
- 交換
  - AIP 15-33
  - UBIC-V EIA 15-41
  - カード 2-23
  - 稼働中のクロスコネクトカード 15-28
  - 下部バックプレーン カバー 15-39
  - 前面扉 2-24
  - 光カード 19-33
  - ファントレイ アセンブリ 15-30
- 工具 (機器) 1-3
- 構成、ネットワークを参照
- 高密度 BNC EIA
  - 同軸ケーブルの取り付け 17-35
  - 取り付け 17-12
- 高密度カード
  - DS1/E1-56 カードを参照
  - DS3/EC1-48 カードを参照
- 高密度シェルフ
  - AEP の取り付け 1-15
  - UBIC-H EIA 20-113
  - UBIC-V EIA 18-60
  - XC10G および XC-VXC-10G カードの要件 2-5
  - 高密度カードの要件 1-5
  - 低密度電気回路保護カードから高密度電気回路保護カードへのアップグレード 12-10
  - ヒューズ パネルの要件 17-5, 17-6, 17-8
- コスト 17-79, 18-18, 19-39
- 固定棒 22-33
- コンピュータ、PC を参照
- さ
- サードパーティ製の機器
  - BLSR の K3 バイトの再マップ 17-94
  - DCC トンネルの作成 20-7

- FC\_MR-4 カードとの相互運用 21-21
- 開放端 UPSR 5-40
- サーバ証跡の作成 6-111
- サーバ証跡
  - 削除 7-6, 21-38
  - 作成 6-111
  - 変更 7-6
- サービス状態
  - Inventory タブの表示 A-13
  - VCAT 回線の変更 21-16
  - カードのサービス状態の変更 10-7
  - カードの状態遷移 10-7
  - 回線の表示 21-5
  - 回線の変更 19-22
  - 管理状態も参照
  - ポートの変更 19-10
- 再初期化ツール 15-12, 19-29, 19-31
- 再初期化によるデータベースのアップロード 19-29, 19-31
- 最適化 1+1 光保護
  - 作成 17-42
  - 説明 4-13
  - 変更 17-43
- サイド切り替え 19-42
- 削除
  - BLSR ノード 14-7
  - CTC からのカード 18-65
  - DCC トンネル 20-25
  - FC\_MR-4 カードの RMON アラーム スレッシュ  
ホールド 20-50
  - IP カプセル化トンネル 20-25
  - IP-over-CLNS トンネル 22-58
  - LDCC 終端 20-50
  - PPM 21-29
  - PPM プロビジョニング 21-29
  - SDCC 終端 18-25
  - SNMP トラップの宛先 18-30
  - TARP MAT エントリ 22-53
  - TDC からのスタティック TID/NSAP エントリ  
22-48
  - UDC 20-25
  - UPSR ノード 14-14
  - VCAT メンバー 20-89
  - VLAN 20-26
  - アラーム プロファイル 22-17
  - イーサネット RMON スレッシュホールド 22-32
  - オーダーワイヤ 20-25
  - オーバーヘッド回線 7-6, 20-25
  - カード保護設定 11-6
  - 回線 20-23
  - 現在のセッションまたはログイン グループからの  
ノード 20-34
  - サーバ証跡 21-38
  - 指定されたログイン グループからのノード  
20-62
  - スタティック ルート 18-18
  - 単一ノードからの BLSR 18-67
  - ドメイン 18-22
  - 表示からのクリアされたアラーム 8-4
  - ファイアウォール トンネル 20-84
  - プロキシ トンネル 20-84
  - プロビジョニング可能なパッチコード 20-58
  - 保護グループ 18-25
  - ユーザ 18-28, 18-30
  - リニア ADM ノード 14-21
  - ロール 21-63
- 作成
  - 1+1 保護グループ 17-87
  - 1:1 保護グループ 17-85
  - 1:N 保護グループ 17-86
  - 2 ファイバ BLSR 20-19, 20-21
  - 4 ファイバ BLSR 20-51, 20-53
  - BLSR 5-16
  - BLSR および 1+1 ノードの半回線 6-65, 20-5
  - DCC トンネル 20-7
  - DS-3 および EC-1 回線 6-22, 6-28, 6-31
  - FC\_MR-4 カードのアラーム スレッシュホールド  
20-46
  - IP カプセル化トンネル 20-36
  - IP-over-CLNS トンネル 22-52
  - J0 セクション トレース 7-9
  - J1 パス トレース 7-11
  - J2 パス トレース 7-12
  - LDCC 終端 20-77
  - SDCC 終端 20-74
  - UDC 19-9
  - UPSR の半回線 6-67, 20-6
  - VAP 6-40
  - VCAT 回線 6-99
  - VLAN 6-71, 6-77, 6-80, 6-83, 6-86, 21-37
  - アラーム重大度プロファイル 22-11
  - イーサネット RMON スレッシュホールド 22-37
  - オーバーヘッド回線 6-107
  - カード保護グループ 4-12

- サーバ証跡 6-111
  - 最適化 1+1 保護グループ 17-42
  - スタティック ルート 17-78
  - 単一ノードの BLSR 19-28
  - 単一ノードのユーザ 17-89
  - ドメイン アイコン 18-20
  - 光回線 6-47, 6-54
  - 複数ノードのユーザ 17-90
  - プロビジョニング可能なパッチコード 20-56
  - ポートマップ モードの E シリーズ回線 6-73
  - ポートマップ モードの E シリーズおよび G シリーズ  
クロスコネク ト 6-91
  - モニタ回線 7-7
  - ユニバーサル ネットワーク マップ 5-50
  - リングを対象とした STS テスト回線 6-108
  - ログイン ノード グループ 17-74
  - 作成前の回線ルートの確認 21-56
  - サブテンディング
    - BLSR からの BLSR 5-48
    - BLSR からの UPSR 5-45
    - UPSR からの BLSR 5-47
  - サブネット マスク
    - OSPF エリア範囲テーブル 19-40
    - Windows の設定 17-59, 17-60
    - スタティック ルートでのプロビジョニング  
17-79
    - セキュア モードでの修正 21-13
    - 長さのプロビジョニング 19-35
    - 変更 19-57
  - サマータイム 4-7, 18-17
- し
- シェルフ
    - DCU シェルフ アセンブリの設置 21-1
    - 受け入れテスト 1-32
    - オフィス アースの接続 17-18
    - オフィス電源の接続 17-19
    - 開梱 1-5, 17-1
    - 確認 17-1
    - シェルフ アセンブリの検査 17-2
    - 隙間の要件 1-6
    - 接続の検査 17-41
    - 前面扉 1-7
    - 取り付け 1-1, 17-5, 17-6, 17-7
    - バックプレーン カバー 1-8
    - 必要な工具 1-4
    - 付属部品 1-3
    - ユーザが準備する部品 1-3
    - 連絡先の変更 18-17
  - シェルフ アセンブリの開梱 1-5, 17-1
  - 時間帯
    - 使用したイベントの表示 18-3
    - 選択 4-7
    - 変更 18-17
  - 時刻
    - 時間の変更 18-17
    - 時刻の設定 4-7
    - リセット 17-20
  - 事前プロビジョニング
    - XFP および SFP 21-47
    - スロット 20-22
    - プロビジョニングも参照
  - 自動ホスト検出 17-63
  - 自動レーザー シャットダウン、ALS を参照
  - 社内 LAN 3-6
  - 受信レベル 2-20
  - 出荷時の設定、ネットワーク要素の詳細を参照
  - 状態
    - ネットワークのチェック 19-71
    - 表示 18-4
    - フィルタ パラメータの変更 22-18
  - 診断ファイル、オフロード 15-17
- す
- 水準点、フロー制御 21-6
  - スーパーユーザ
    - CTC IP アドレスの非表示 19-36
    - アイドル時間 17-89
    - セキュア モードでの IP アドレスの表示 19-36
    - セキュリティも参照
    - 二重 IP アドレスの割り当て 21-10
    - ノード アクセスの設定 22-5
    - ノードでのセキュリティ ポリシーの変更 19-60
    - 複数ノードでのセキュリティ ポリシーの変更  
19-61
    - 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 21-43
    - 別のユーザの削除 18-28, 18-30
    - 別ユーザのセキュリティ設定の変更 18-27,  
18-29

- ズーム A-6
- スケルチ テーブル
  - STS 21-38
  - VT 21-40
- スタティック ルート
  - 削除 18-18
  - 作成 17-78
  - 変更 18-18
- スタンドオフ 1-25
- スタンドオフ キット 1-3, 17-4
- スパニングツリー プロトコル、STP を参照
- スパン
  - 色の変更 19-25
  - 回線の表示 19-21
  - 切り替え (UPSR) 17-104
  - 情報の表示 A-9
  - スパン アップグレードも参照
  - ハードウェアの互換性 12-21
  - 光のアップグレード 12-16
  - 復元時間 (BLSR) 13-23, 20-51, 20-53
  - プロパティの表示 A-11
- スパン アップグレード
  - 1+1 保護、手動アップグレード 19-69
  - 2 ファイバ BLSR、手動アップグレード 19-64
  - 4 ファイバ BLSR、手動アップグレード 19-66
  - BLSR、UPSR、または 1+1 の自動アップグレード 12-16
  - UPSR、手動アップグレード 19-67
  - エラー回復 12-20
  - 非保護スパン、手動アップグレード 19-70
- スパン アップグレードからのバックアップ
  - 1+1 保護グループ 19-69
  - 2 ファイバ BLSR 19-64
  - 4 ファイバ BLSR 19-66
  - UPSR 19-67
  - 非保護スパン 19-70
- スプリッタ保護グループ 4-14
- スペーサ 1-3
- スロット
  - 1+1 現用スロットがアクティブであることの確認 18-59
  - AIC-I カード 4-2
  - XC10G および XC-VXC-10G カードとの互換性 2-5
  - XCVT カードとの互換性 2-3
  - クロスコネクタ 4-2
  - 事前プロビジョニング 20-22
- せ
- 清掃
  - ファイバ アダプタ 19-4, 19-5
  - ファイバ コネクタ 15-20, 19-4, 19-5
- セキュア モード
  - IP アドレス表示の制限 19-36
  - IP 設定のプロビジョニング 19-35
  - IP 設定の変更 19-57
  - MAC アドレス 19-36
  - イネーブル化 21-10
  - ディセーブル化 21-14
  - データベースのロード制限 15-7
  - バックプレーンの IP 設定の修正 21-13
  - プロビジョニング 4-9
  - プロビジョニングの変更 17-76
  - ログイン ノード グループに使用する IP アドレス 17-74, 17-76
  - ロック 21-12
  - ロックされているときのプロキシ サーバ IP アドレスのディセーブル化 17-70
  - ロックされているときのプロキシ サーバ IP アドレスの変更 17-69
- セキュリティ
  - CISCO15 スーパーユーザ 17-73
  - アイドル時間 17-89, 17-90
  - 監査証跡レコード 15-14
  - セキュア モードも参照
  - セキュリティ ポリシーの変更 19-60, 19-61
  - 設定の変更 11-9
  - セットアップ 4-5
  - ノード アクセスの設定 22-5
  - 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 21-43
  - ユーザのセキュリティ レベル 17-89, 17-90
  - レベルの変更 18-27, 18-29
- セクション トレース、J0 セクション トレースを参照
- 接続
  - 4 ノード UPSR へのファイバ 17-52
  - 4 ノードへのファイバ、4 ファイバ BLSR 17-56
  - 6 ノードへのファイバ、統合 UPSR-DRI 17-54
  - 8 ノードへのファイバ、従来型 UPSR-DRI 17-53
  - AEP への外付けワイヤラップ パネル 1-19
  - ONS ノードとサードパーティ製の機器 6-111
  - PC から ONS 15454 3-2, 3-4, 3-5
  - PC から社内 LAN ポート 3-6
  - PC と CTC 3-6

- UNIX ワークステーションと ONS 15454 3-5
- シェルフへのオフィス アース 17-18
- シェルフへのオフィス電源 17-19
- 取り付けも参照
- 切断
  - ノードの電源 16-1
- 設置
  - DCU 21-1
  - シェルフ アセンブリ 1-6, 21-1
  - 必要な工具 1-3
- 設定
  - LAN アクセス 22-5
  - PM 自動リフレッシュ間隔 19-46
  - RADIUS 認証のノード 21-41
  - 再初期化による GNE IP アドレス 19-30, 19-31
  - 時刻 4-7
  - デフォルト ルータ 19-36
  - 電力モニタ スレッシュホールド 4-8
- セットアップ
  - CTC ネットワーク アクセス 4-9
  - ENE のための SNMP 21-34
  - GNE のための SNMP 21-32
  - LAN モデムによるリモート アクセス 3-7
  - OSPF 19-39
  - SNMP 4-15
  - 外部アラームおよび制御 8-11
  - 外部またはライン タイミング 17-81
  - クラフト接続用 Windows PC 17-58, 17-61, 17-66
  - 社内 LAN 接続 3-6
  - セキュリティ 4-5
  - タイミング 4-11
  - 内部タイミング 17-84
  - ノード日付、時刻、連絡先情報 4-6
  - 復元のタイミング 17-82
  - ユーザ 4-5
- 選択
  - CTC ログインの IP アドレス 17-73
  - 時間帯 4-7
- 前面扉
  - 交換 2-24
  - 取り外し 15-4, 17-9
  - 開く 17-8
- そ
- 送信レベル 2-20
- 測定
  - 電圧 17-41
  - ヒューズ アラーム パネル ケーブル 17-20
  - ソケット固定ネジ 1-3
  - 外付けワイヤラップ パネル 1-19
  - ソフトウェア
    - CD-ROM のインストール 20-28
    - CTC による新しいリリースの自動検出 3-8, A-1
    - CTC も参照
    - 互換性のないアラーム 17-72
    - 再初期化によるアップロード 19-29, 19-31
    - バージョンの確認 17-46, 17-72
    - バージョンのミスマッチ 17-72
- た
- タイラップ 1-3, 1-4
- ダイアログボックス
  - CTC Alerts の自動ポップアップのプロビジョニング 20-18
  - 非表示オプションのイネーブル化 19-59
- タイミング
  - BITS、BITS を参照
  - NE Reference 17-82
  - 外部タイミング 17-81
  - 切り替えタイプ 15-27
  - ケーブルの取り付け 17-26
  - 縮小されたリングでの確認 18-66
  - 手動または強制切り替えの開始 20-14
  - 手動または強制切り替えのクリア 20-14
  - ステータス 15-26
  - セットアップ 4-11
  - 内部タイミング 17-84
  - ノード時刻の設定 4-7
  - ノードのタイミング基準の変更 15-24
  - ノードのタイミングの変更 11-8, 18-26
  - モード 17-82
  - ライン タイミング 17-81
- タイミング レポート 15-25
- タイムアウト、アイドル時間を参照
- 端末ネットワーク、ポイントツーポイントを参照
- ち
- 中止、ディセーブル化を参照



- つ
- 追加
- BLSR ノード 14-2
  - TARP MAT エントリ 22-48
  - TDC へのスタティック TID/NSAP エントリ 22-47
  - UPSR ノード 14-11
  - VCAT 回線のメンバー 20-85
  - 現在のセッションまたはログイン グループへのノード 17-75
  - ツールバーからのノード A-5
  - ドメインへのノード 18-21
  - ネットワーク ビューからの回線 A-11
  - ファイアウォール トンネル 20-83
  - プロキシ トンネル 20-82
  - リニア ADM へのノード 14-16, 14-18
- ツイストペア ワイヤラップ 17-38
- ツールバーにあるアイコン
- Open TL1 Connection A-7
  - 印刷 A-5
  - エクスポート A-5
  - 上位のビューへ移動 A-6
  - 初期設定 A-5
  - ズーム イン A-6
  - 選択したオブジェクトのビューへ移動 A-6
  - 選択領域のズーム イン A-6
  - 次の CTC ビューへ進む A-6
  - ネットワーク ビューへ移動 A-6
  - ノードの追加 A-5
  - ノードのロック A-5
  - ホーム ビューへ移動 A-6
  - 前の CTC ビューに戻る A-6
- て
- ディセーブル化
- Internet Explorer によるプロキシ サービス 17-69
  - IPPM 18-9
  - LDCC による外部ノード設定 20-67
  - Netscape によるプロキシ サービス 17-70
  - OSPF 18-19
  - SDCC による外部ノード 20-66
  - STP 6-71
  - アラーム フィルタリング 19-21
  - アラームの抑制 22-22
  - セキュア モード 21-14
  - セキュア(ロック)モードのときのプロキシ サーバ IP アドレス 17-70
  - ネットワーク調査 17-73
  - プロキシ サービス 3-6
  - ポインタ位置調整カウント 18-7
- データ通信チャンネル、DCC を参照
- データベース
- 障害回復によるクリア 15-12, 19-29, 19-31
  - 障害回復によるデフォルト値のクリア 15-12, 19-29, 19-31
  - バックアップ 15-6
  - 復元 15-7
  - 復元されないパラメータ 15-12
- テーブル
- カラムのサイズ変更 A-12
  - データの印刷 22-34
  - データのソート A-12
  - テーブルのリストも参照
  - 表示形式の変更 A-12
  - 表示されていないカラムの表示 A-12
- テーブル カラムのサイズ変更 A-12
- テーブル データのソート A-12
- 適用
- カードおよびノードへのアラーム プロファイル 18-6
  - カスタム ネットワーク ビューの背景マップ 19-58
  - ポートへのアラーム プロファイル 22-15
  - ロックアウト 19-2
  - ロックオン 19-1
- テスト
- 1+1 光の保護 17-92
  - 4 ファイバ BLSR スパン 17-99
  - 4 ファイバ BLSR スパンの切り替え 17-101
  - BLSR 保護の切り替え 17-94
  - E シリーズ回線 6-89
  - G シリーズ回線 6-97
  - UNIX 設定時の Netscape Navigator への接続 17-67
  - UPSR 保護の切り替え 17-103
  - 電気回線 6-44
  - 光回線 6-63
- デフォルト ルータ
- CTC での変更 19-57
  - IP アドレスの入力 19-36
  - セキュア モードでの修正 21-13
- デュアル リング相互接続、DRI を参照

- 電圧計 1-4, 17-22, 17-41
- 電気インターフェイス アダプタ
  - DS-1 ケーブルの取り付け 17-29
  - SMB EIA 17-15
  - 取り付け 17-29
- 電気回線
  - DS-1、自動ルーティング 6-8
  - DS-1、手動ルーティング 6-13
  - DS-1 または DS-3 ルートのプロビジョニング 17-106
  - DS-1、送信元と宛先のプロビジョニング 17-104
  - DS-3、送信元と宛先のプロビジョニング 22-4
  - DS-1、複数ドロップ 6-17
  - DS-3 または EC-1、自動ルーティング 6-22
  - DS-3 または EC-1、手動ルーティング 6-28
  - DS-3 または EC-1、複数ドロップ 6-31
  - VAP 6-40
  - 回線も参照
- 電気回路カード
  - EIA も参照
  - STS 回線の送信元および宛先のオプション 6-4
  - VT 回線の送信元と宛先のオプション 6-3
  - XC10G および XC-VXC-10G カードとのスロット互換性 2-5
  - XCVT カードとのスロット互換性 2-3
  - 回線タイプ、電気回線を参照
  - 回線とスレッシュホールドの設定変更 10-2
  - 削除 18-65
  - 低密度カードから高密度カードへのアップグレード 12-10
  - 取り付け 2-11
  - 取り付け時の LED の動作 2-12
  - 取り付けの確認 4-3
  - パストレース機能 19-52
  - 保護 17-85, 17-86
  - リセット 21-46
- 電気回路ケーブル
  - DS-3 ケーブル 20-90
  - DS-1 ケーブルも参照
  - DS-3 ケーブル 21-22
  - EC-1 ケーブル 20-90, 21-22
  - 同軸ケーブルも参照
- 電源
  - オフィス電源の確認 17-22
  - シェルフへのオフィス電源の接続 17-19
  - 電圧の測定 17-41
  - 電力モニタ スレッシュホールドの設定 4-8
  - むき出しの導体へのコーティング 17-21
  - 電源コード
    - 固定棒 22-33
    - フェライトの取り付け 17-39
    - ユーザが準備する部品 1-3
  - 電源投入
    - イネーブル化も参照
    - オフィス電源 17-22
- と
- 同軸ケーブル
  - BNC コネクタ 17-33
  - SMB コネクタ 17-35
  - 減衰率 17-37
  - 高密度 BNC コネクタ 17-35
  - 固定棒 22-33
  - 配線 17-37
- トポロジー アップグレード
  - 稼働中のトポロジー アップグレード ウィザードを参照
  - ネットワーク、変換を参照
- トポロジー ホスト (VLAN)、管理 7-18
- ドメイン
  - 移動 18-21
  - 管理 18-21
  - 削除 18-22
  - 作成 18-20
  - ドメイン ビュー、説明 A-2
  - 名前の変更 18-21
  - ノードの追加 18-21
  - 開く 18-22
  - ローカルドメインを許可するための NE デフォルトの変更 18-20
- ドメインの移動 18-21
- ドメイン名の変更 18-21
- ドライバ
  - 小型スロット ヘッド 1-4
  - 中型スロット ヘッド 1-4
- トラップ 4-15
- トラフィック モニタリング
  - J1 パストレースの作成 7-11
  - J2 パストレースの作成 7-12
  - パフォーマンス モニタリング も参照
  - 光ポートでの J1 パストレースのプロビジョニング 18-16

- モニタ回線の作成 7-7
- トラフィックのブリッジおよびロール 7-15
- トランスポンダ モード 6-93
- トランスマック カード
  - DS3XM-12 カードを参照
  - DS3XM-6 カードを参照
- 取り付け
  - AEP 1-15
  - AIC-I カード 17-50
  - AMP Champ EIA 17-16
  - BLSR のファイバ 17-55
  - BNC EIA 17-12
  - BNC コネクタ付き同軸ケーブル 17-33
  - CTC インストール ウィザード( Windows ) 20-27
  - CTC コンピュータの JRE 20-27
  - DS-1 AMP Champ ケーブル 17-30
  - EIA 1-9
  - FC\_MR-4 カード 2-15
  - GBIC 21-64
  - LAN ケーブル 17-27
  - LGX インターフェイスのケーブル 19-6
  - MiniBNC EIA 20-63
  - MRC-12 カードのファイバクリップ 21-25
  - SFP/XFP 21-64
  - SMB EIA 17-14
  - SMB コネクタ付き同軸ケーブル 17-35
  - TCC2/TCC2P カード 17-44
  - TL1 クラフト インターフェイス 17-28
  - UBIC-H EIA 20-113
  - UBIC-H EIA ケーブル 21-22
  - UBIC-V EIA 18-60
  - UBIC-V EIA ケーブル 20-90
  - UPSR のファイバ 17-51
  - アラーム ケーブル 17-23
  - イーサネット カード 2-13
  - 外部ブラケットおよびエア フィルタ 17-4
  - 共通コントロール カード 2-2
  - クロスコネクタ カード 2-2, 17-47
  - 高密度 BNC EIA 17-12
  - シェルフ 1-1
  - シェルフ アセンブリ 17-5, 17-7
  - 接続も参照
  - 外付けワイヤラップ パネル 1-19
  - 電気インターフェイス アダプタ 17-29
  - 電気回路カード 2-11
  - 電源コードへのフェライト 17-39
- 電源装置 1-11
- 取り付けも参照
- 背面カバー 1-25
- バックプレーン アラーム ケーブル 17-23
- バックプレーン タイミング ケーブル 17-26
- バックプレーンのタイミング線 17-26
- バラン コネクタを使用した DS-1 ケーブル 17-29
- 光カードとコネクタ 2-8
- 光ファイバ ケーブル 2-18
- ファイバ ブーツ 17-57
- ファントレイ アセンブリ 1-13
- フィルター カード 2-17
- フェライト 1-31
- マウント ブラケットの反転 17-2
- ラック取り付けも参照
- ワイヤラップ ピン フィールドへのフェライト 17-40
- 取り外し
  - GBIC 21-68
  - SFP/XFP 21-68
  - カード 2-23
  - 下部バックプレーン カバー 17-10
  - 前面扉 15-4, 17-9
  - パススルー回線 20-61
  - バックプレーンの金属製カバー 17-11
  - ファントレイ アセンブリ 15-4
- ドロップ
  - DS-1 回線の複数ドロップ 6-17
  - DS-3 または EC-1 回線の複数ドロップ 6-31
  - パストレース内の宛先ポート 7-13, 19-54
  - 光回線の複数ドロップ 6-58
  - 保護されたドロップ 6-9
- トンネル
  - DCC、DCC トンネルを参照
  - IP カプセル化、IP カプセル化トンネルを参照
  - IP-over-CLNS、IP-over-CLNS トンネルを参照
  - VT、VT トンネルを参照
  - タイプの変更 20-22
  - ファイアウォール、ファイアウォール トンネルを参照
  - プロキシ、プロキシ トンネルを参照

- に
- 入力
  - SNMP の NMS コミュニティ スtring 21-36
  - セキュア (ロック) モードのときのログイン ノード IP アドレス 17-74, 17-76
- ね
- ネットワーク
  - BLSR、BLSR を参照
  - CTC ネットワーク アクセスの設定 4-9
  - CTC ネットワーク アクセスの変更 11-3
  - ONS ノードとサードパーティ製の機器の接続 6-111
  - 回線の管理 6-1, 7-1
  - デフォルト設定、UPSR を参照
  - トポロジ検出 3-8, 17-73
  - ネットワーク起動の確認 6-5
  - 変換 13-1
  - ポイントツーポイント型、ポイントツーポイント を参照
  - リニア ADM、リニア ADM を参照
- ネットワーク ビュー
  - TDM と DWDM のネットワーク ビュー切り替え 21-73
  - アラームおよび状態に対するネットワークのチェック 19-71
  - カスタマイズ 11-5
  - カスタム背景マップの適用 19-58
  - 作業 A-11
  - デフォルト背景マップの変更 22-31
  - トポロジ検出エラー 6-5
  - ノード アイコンの説明 A-3
  - 背景色の変更 18-19
  - マップへのノードの追加、ドメインを参照
  - ユーザの削除 18-30
  - より新しいソフトウェア リリースの自動検出 3-8, A-1
  - リンクの統合 21-69
  - 論理ネットワーク マップの作成 5-50
- ネットワーク管理システム、NMS を参照
- ネットワーク要素のデフォルト値
  - インポート 15-46
  - エクスポート 15-48
  - 復元 19-29, 19-31
  - 編集 15-44
- ネットワーク要素のデフォルト値のインポート 15-46
- の
- ノード
  - IP アドレスの修復 20-26
  - RADIUS 認証の設定 21-41
  - 管理情報の変更 11-2
  - 現在のセッションへの追加 17-75
  - 削除 20-34, 20-62
  - 時刻のリセット 17-20
  - セキュア モードのディセーブル化 21-14
  - セキュア モードのロック 21-12
  - 電源の切断 16-1
  - 名前の変更 18-17
  - ネットワーク ビュー マップのアイコン A-3
  - ノード アクセスの設定 22-5
  - 日付、時刻、連絡先情報の設定 4-6
  - ユーザのログアウト 20-9, 20-10
- は
- ハードウェアの切り替えテスト 20-45
- 配線
  - DS-1 ツイストペア ケーブル 17-38
  - 同軸ケーブル 17-37
  - 光ファイバケーブル 2-22
- ハイブリッド ノード アイコン A-3
- 背面カバー 1-25
- パストレース
  - J1 パストレースを参照
  - J2 パストレースを参照
- パススルー回線
  - 確認 21-24
  - 取り外し 20-61
- パスワード
  - 新規ユーザの作成 17-89, 17-90
  - デフォルト CTC パスワード 17-73
  - ログイン 17-72
- バックプレーン
  - アライメントの確認 17-41
  - インターフェイス接続 (ピン)、バックプレーン接続を参照
  - カバー 1-8
  - 下部カバーの取り付け 15-39

- 下部バックプレーン カバーの取り外し 17-10
  - 金属製カバーの取り外し 17-11
  - セキュア モードも参照
  - バックプレーン LAN ポートへの IP アドレスの割り当て 21-10
  - バックプレーン接続
    - AEP 接続 1-17
    - LAN ケーブル 17-27
    - TBOS 17-26
    - TL1 クラフト インターフェイス ケーブル 17-28
    - X.25 17-26
    - アラーム ケーブル 17-23
    - 外部アラーム ピン 17-25
    - 確認 17-41
    - タイミング ケーブル 17-26
    - モデム 17-26
  - パッチ ケーブル
    - 2 ファイバ BLSR テスト 5-18
    - 4 ファイバ BLSR テスト 5-21
    - UPSR テスト 5-30, 5-43
    - ポイントツーポイント テスト 5-7
    - リニア ADM テスト 5-12
  - バッテリー接続の終端 17-21
  - ハブアンドスポーク 6-79
  - パフォーマンス モニタリング
    - 1 日間隔でのリフレッシュ 18-12
    - 15 分間隔でのリフレッシュ 18-11
    - FC\_MR-4 スレッシュホールドの変更 10-6
    - FC\_MR-4 リフレッシュ間隔の変更 20-44
    - IPPM 18-9
    - PM クリア権限 22-5
    - Threshold Crossing Alert、TCA を参照
    - イーサネット PM カウントのリフレッシュ 20-37
    - イーサネット カードおよびポート 9-5
    - イーサネット リフレッシュ間隔の変更 19-46
    - イーサネット使用率の表示 19-44
    - イーサネット履歴 PM パラメータの表示 19-45
    - 遠端側のカウンターの表示 18-13
    - 近端側のカウンターの表示 18-13
    - 現在のカウンターのリセット 18-14
    - 異なるポートのリフレッシュ間隔 19-47
    - 自動リフレッシュ間隔の設定 19-46
    - 選択した信号の PM カウント 20-38
    - 手順 9-1 9-8
    - 電気回路カードのスレッシュホールドの変更 10-2
    - 特定のカウンターのクリア 20-40
    - 光カード 9-7
    - 光カードのスレッシュホールドの変更 10-3
    - ポインタ位置調整カウント、ポインタ位置調整カウントを参照
  - パフォーマンスのモニタリング、パフォーマンス モニタリングを参照
  - バラン、電気インターフェイス アダプタを参照
  - パルス符号変調 17-91
  - パワー メータ 1-4
  - 半回線
    - BLSR および 1+1 ノードでの作成 6-65, 20-5
    - UPSR での作成 6-67, 20-6
    - 回線も参照
- ## ひ
- 非 ONS ノード、外部ノード設定を参照
  - ヒープ サイズ、調整 3-2
  - 光カード
    - 4 ポート OC-12 カード スロット 12-16, 12-21
    - ALS 設定の変更 22-29
    - PM パラメータの表示 22-1
    - PPM の削除 21-29
    - SDH へのポートの変更 18-52
    - VT 回線の送信元と宛先のオプション 6-3
    - XC10G および XC-VXC-10G カードとのスロット互換性 2-6
    - XCVT カードとのスロット互換性 2-4
    - カード保護のプロビジョニング 17-87
    - 回線終端カード 18-7
    - 回線とスレッシュホールドの設定変更 10-3
    - 回線の伝送設定の変更 20-78
    - 減衰量 2-19
    - 交換 19-33
    - 削除 18-65
    - スレッシュホールドの変更 18-50
    - 取り付け 2-8
    - 取り付け時の LED の動作 2-10
    - 取り付けの確認 4-3
    - パストレース機能 19-52
    - パストレースのプロビジョニング 18-16
    - パフォーマンスのモニタリング 9-7
    - 光スレッシュホールド設定の変更 21-44
    - 光伝送速度の変更 19-33
    - 光ファイバ ケーブルの配線 2-22

- ファイバクリップ 2-22
- ファイバブーツの取り付け 17-57
- ファイバの取り付け 2-18
- リセット 21-46
- 光カードの送受信レベル 2-20
- 光 (STS) 回線
  - STS スケルチ テーブル 21-38
  - STS の送信元および宛先のオプション 6-4
  - 回線のテスト 6-63
  - 回線も参照
  - 回線ルートのプロビジョニング 20-59
  - 自動ルーティングによる回線のプロビジョニング 6-47
  - 手動ルーティングによる回線のプロビジョニング 6-54
  - スパンでの未使用 STS の表示 19-21
  - 送信元と宛先のプロビジョニング 17-107
  - ドロップが複数の回線のプロビジョニング 6-58
  - リングを対象にした STS テスト回線の作成 6-108
- 日付
  - デフォルト 17-20
  - プロビジョニング 4-7
  - 変更 18-17
- 非表示
  - CTC IP アドレスの表示 19-36
  - IP アドレスの表示 21-12, 21-14
  - LCD からの IP アドレス設定 19-36
- ビュー
  - 概要 A-2
  - ネットワーク ビューのショートカット A-11
  - ネットワーク ビューも参照
  - ノード ビューのショートカット A-10
  - ビューの切り替え A-2
- ヒューズ アラーム パネル
  - 100 アンペア 1-12, 17-5, 17-6, 17-8, 17-22
  - 80 アンペア 1-12, 17-5, 17-6, 17-8, 17-22
  - ケーブルの測定および切断 17-20
- 表示
  - BLSR VT スケルチ テーブル 21-40
  - CE シリーズ イーサネット カード使用率 PM パラメータ 20-105
  - CE シリーズ イーサネット カード統計情報 PM パラメータ 20-103
  - CE シリーズ イーサネット カード履歴 PM パラメータ 20-106
  - DS3XM-12 カード BFDL PM パラメータ 20-109
  - DS3XM-12 カード DS-N/SONET PM パラメータ 20-108
  - E シリーズ イーサネット MAC アドレス テーブル 20-4
  - E シリーズ イーサネットのメンテナンス情報 15-23
  - ES-IS RIB 22-59
  - FC\_MR-4 カードの使用率 PM パラメータ 20-42
  - FC\_MR-4 カードの統計情報 PM パラメータ 20-41
  - FC\_MR-4 カードの履歴 PM パラメータ 20-43
  - G シリーズ イーサネットのメンテナンス情報 15-22
  - Inventory タブのサービス状態 A-13
  - IS-IS RIB 22-58
  - LCD でのポート ステータス 20-35
  - LCD のアラーム カウント 8-6
  - OSI 情報 15-11
  - TCA 18-11, 18-12
  - アクティブ ログイン 21-48
  - アラーム 8-3, 20-102
  - アラームおよびイベントの履歴 22-9
  - イーサネット トランク使用状況 20-5
  - イーサネット使用率 PM パラメータ 19-44
  - イーサネットの統計情報 PM パラメータ 19-44
  - イーサネット履歴 PM パラメータ 19-45
  - 遠端側の PM カウント 18-13
  - 回線 7-2
  - 回線情報 21-2
  - 回線でのアラーム 8-5
  - 回線のサービス状態 21-5
  - 監査証跡レコード 15-14
  - 近端側の PM カウント 18-13
  - 時間帯によるイベント 18-3
  - 状態 18-4
  - スパンングツリー情報 21-9
  - スパン プロパティ A-11
  - スパン情報 A-9
  - スパンでの未使用 STS 19-21
  - スパンの回線 19-21
  - ノード ソフトウェア バージョン 17-72
  - 光カード PM 22-1
  - 表示されていないテーブル カラム A-12
  - 表示も参照
  - ログイン ノード グループ 17-73
- 開く
  - Cisco IOS Connection A-7

- TL1 接続 A-7
  - 前面扉 17-8
  - ドメイン 18-22
- ふ
- ファイアウォール
    - IOP リスナー ポートのプロビジョニング 17-79, 17-80
    - アクセスを目的としたノードのプロビジョニング 4-10
    - ファイアウォール トンネルも参照
  - ファイアウォール トンネル
    - 削除 20-84
    - 追加 20-83
  - ファイバ
    - 1+1 構成 21-8
    - BLSR からの UPSR のサブテンディング 5-45
    - BLSR 構成 17-55
    - LGX インターフェイスへの光カードの取り付け 19-6
    - SC ファイバ ジャンパ 1-4
    - UPSR からの BLSR のサブテンディング 5-47
    - UPSR 構成 17-51
    - UPSR 接続の確認 5-27, 5-40
    - アダプタの清掃 19-4, 19-5
    - コネクタの清掃 15-20, 19-4, 19-5
    - 配線 2-22
    - 光カードへの取り付け 2-18
    - ファイバ ブーツの取り付け 17-57
    - 方向反転可能なファイバ ガイド 2-22
  - ファイバクリップ、取り付け 2-22, 21-25
  - ファイバチャネルカード、FC\_MR-4 カードを参照
  - ファイバブーツ 17-57
  - ファントレイ アセンブリ
    - 交換 15-30
    - 取り付け 1-13
    - 取り外し 15-4
  - ファントレイ エアー フィルタ、エアー フィルタを参照
  - フィルター カード、取り付け 2-17
  - フィルタ ストップ 17-4
  - フィルタリング
    - アラーム、アラーム フィルタリングを参照
    - 回線の表示 19-48
  - フェライト
    - 電源コードへの取り付け 1-31, 17-39
  - ワイヤラップ ピン フィールドへの接続 17-40
  - 負荷テスト
    - 4 ファイバ BLSR スパン 17-99
    - BLSR リング 19-12
  - 不完全な回線の再設定 7-16
  - 復元
    - TCC2/TCC2P データベース 15-7
    - ネットワーク要素のデフォルト値 19-29, 19-31
  - 復元切り替え
    - BLSR 20-19, 20-21, 20-53
    - UPSR 回線 19-14, 19-26
    - 電気回路の保護 17-86, 17-87
    - 光の保護 17-88
  - 復元のタイミング
    - 切り替えのクリア 20-14
    - 手動または強制切り替えの開始 20-14
    - セットアップ 17-82
  - 複数ドロップ、回線を参照
  - ブラウザの必須バージョン 3-2
  - プラグイン ユニット、カードを参照
  - プラス
    - #2 ドライバ 1-4
    - プラス ヘッド ネジ 1-3
  - フランジ 17-4
  - ブレード、カードを参照
  - フレーミング 17-83, 18-26
  - フレーム アース ピン 17-28
  - フロー制御水準点
    - CE-1000-4 カードのプロビジョニング 21-6, 22-3
    - G シリーズ カードのプロビジョニング 21-6
  - プロキシ サーバ
    - 機能 19-37
    - セキュア モードのイネーブル化 21-11
    - セキュア モードのディセーブル化 21-15
    - セキュア (ロック) モードのときの IP アドレスのディセーブル化 17-70
    - セキュア (ロック) モードのときの IP アドレスの変更 17-69
    - ファイアウォール トンネルの要件 20-83
    - プロキシ トンネルの要件 20-82
  - プロキシ サービス
    - Internet Explorer によるディセーブル化 17-69
    - Netscape によるディセーブル化 17-70
    - ディセーブル化 3-6
  - プロキシ トンネル
    - 削除 20-84
    - 追加 20-82

## プロトコル

- DHCP 19-36
- NTP 4-6
- SNMP を参照
- SNTP 4-6

## プロビジョニング

- 2つのIPアドレス 21-10
- BLSR または 1+1 設定の半回線 20-5
- CE シリーズ POS ポート 22-8
- CE-1000-4 イーサネットポート 22-3
- CE-1000-4 カードのフロー制御水準点 22-3
- CE-100T-8 イーサネットポート 22-7
- CTC Alerts の自動ポップアップ 20-18
- CTC コンピュータの IOP リスナー ポート 17-80
- DHCP 4-9
- DS-1 回線の送信元と宛先 17-104
- DS-1 および EC-3 回線ルート 17-106
- DS-3 回線 22-4
- E シリーズ イーサネットカードモード 19-32
- E シリーズ イーサネットポート 19-15
- ENE としてのノード 19-37
- FC\_MR-4 カードの管理状態 21-18
- G シリーズ イーサネットポート 6-93, 19-18
- GNE としてのノード 19-37
- IP 設定 19-35
- J1 パストレース 18-16, 19-51
- LCD からのノード情報 4-9
- LDCC 終端 20-77
- LDCC による外部ノード設定 20-77
- ML シリーズ イーサネットカードモード 22-62
- MRC-12 カード PPM 21-27
- MRC-12 カード光回線ルート 21-28
- OC-N 回線ルート 20-59
- OSI 4-17
- OSI マニュアルエリアアドレス 22-50
- OSI ルータ 22-49
- OSI ルーティングモード 22-43
- SDCC 終端 20-74
- SDCC による外部ノード設定 20-74
- SNMP セットアップによる IP アドレス 4-15
- SNMP セットアップによる NMS IP アドレス 21-32, 21-34
- TARP 動作パラメータ 22-45
- UPSR ノード 5-27
- UPSR の半回線 20-6
- UPSR パスセレクタ 19-14

- VCAT 回線 6-99, 6-104, 20-15, 20-16
- VLAN メンバーシップ用の E シリーズ ポート 19-17
- VT トンネル ルート 19-15
- オーダーワイヤ 17-91
- 回線 A-11
- 管理状態 18-32, 18-36, 18-40, 18-44, 18-48, 20-69, 20-80, 20-96, 20-99, 22-27
- サブネットマスク長 19-35
- セキュアモード 4-9, 21-10, 21-11
- セットアップも参照
- ドロップが複数の単方向光回線 6-58
- ノードの IOP リスナー ポート 17-79
- バックプレーンポートの IP アドレス 21-10
- 光カードの TCA 21-45
- 光回線 6-47, 6-54, 17-107
- 日付 4-7
- ファイアウォール アクセスを目的としたノード 4-10
- フロー制御水準点 21-6
- プロビジョニングも参照
- ポイントツーポイント ネットワーク 5-5
- リニア ADM 5-9
- 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 21-43
- プロビジョニング可能なパッチコード
  - 削除 20-58
  - 作成 20-56

## へ

### 変換

- 23 インチ ラックから 19 インチ ラックへ 17-2
- アップグレードも参照
- カードの 1:1 から 1:N 保護 18-55, 18-57
- ネットワーク構成 13-1

### 変更

- 1+1 保護グループ 18-24
- 1:1 保護グループ 18-22
- 1:N 保護グループ 18-23
- AIC-I カードの設定 10-4
- BLSR 13-23
- BLSR ノード ID 20-17
- CTC による IP 設定 19-57
- CTC ネットワーク アクセス 11-3
- DS1/E1-56 カード回線とスレッシュホールド設定 20-68



- DS1-14 カード回線とスレッシュホールド設定 18-31
- DS3/EC1-48 カード回線とスレッシュホールド設定 20-98
- DS3-12 カード回線とスレッシュホールド設定 18-35
- DS3i-N-12 カード回線とスレッシュホールド設定 22-25
- DS3XM-12 カード回線とスレッシュホールド設定 20-94
- DS3XM-6 カード回線とスレッシュホールド設定 18-43
- EC-1 カード回線とスレッシュホールド設定 18-47
- FC-MR-4 カード ポート設定と PM スレッシュホールド 10-6
- FC\_MR-4 カードにある汎用ポートの設定 21-17
- FC\_MR-4 カードの拡張 FC/FICON ポート設定 21-21
- FC\_MR-4 カードの距離延長ポート設定 21-19
- JRE バージョン 21-10
- LCD による IP 設定 17-76
- LDCC 終端 20-67
- MRC-12 カード光回線レート 21-29
- OSI プロビジョニング 11-4
- OSI ルーティング モード 22-54
- OSPF 19-39
- SDCC 終端 20-66
- SDH への光ポート 18-52
- SNMP 設定 11-10
- TARP 動作パラメータ 22-45
- TCP/IP 設定 17-59, 17-60, 17-61, 17-62, 17-63, 17-64, 17-65
- VCAT メンバーのサービス状態 21-16
- オーダーワイヤ設定 19-8
- オーバーヘッド回線 7-6
- カードの光伝送速度 19-33
- カード保護設定 11-6
- カードまたは PPM サービス状態 10-7
- 回線のサービス状態 19-22
- 回線名 19-24
- 外部アラームの設定 19-7
- 外部制御の設定 19-8
- 最適化 1+1 保護グループ 17-43
- 時間 18-17
- 時間帯 18-17
- スタティック ルート 18-18
- スパンの色 19-25
- セキュア モードでのバックプレーン IP 設定 21-13
- セキュア (ロック) モードのときのプロビジョニング 17-76
- セキュリティ 11-9, 19-60, 19-61
- テーブルの形式 A-12
- デフォルト ネットワーク ビューの背景マップ 22-31
- 電気回路カードの回線設定と PM スレッシュホールド 10-2
- トンネル タイプ 20-22
- ネットワーク ビューの背景色 18-19
- ノード アクセスおよび PM クリア権限 22-5
- ノードがセキュア (ロック) モードのときのプロキシ サーバの IP アドレス 17-69
- ノード管理情報 11-2, 18-17
- ノードのタイミング 11-8, 15-24, 18-26
- 光カードの回線設定と PM スレッシュホールド 10-3
- 光カードの設定 18-50, 20-78, 21-44, 22-29
- 日付 18-17
- ビューの切り替え A-2
- フィルタ パラメータ 22-18
- プロキシ サービスをディセーブル化しているときの LAN の設定 17-69
- 変更も参照
- 編集も参照
- ポートのサービス状態 19-10
- ユーザ設定 11-9
- ユーザのパスワードとセキュリティ レベル 18-27, 18-29
- ローカル ドメインを許可するための NE デフォルト 18-20
- 編集
  - IP-over-CLNS トンネル 22-57
  - OSI サブネットワーク接続ポイント 22-56
  - OSI ルータ設定 22-55
  - UPSR DRI 回線ホールドオフ タイマー 19-50
  - UPSR 回線バス セレクタ 19-26
  - VCAT 回線のメンバー名 19-24
  - 回線名 19-24
  - ネットワーク要素のデフォルト値 15-44
  - 変更も参照
- ほ
  - ポインタ位置調整カウント
    - イネーブル化 18-7

- ディセーブル化 18-7
    - 目的 18-7
  - ポイントツーポイント型
    - 2 ファイバ BLSR へのアップグレード 13-10
    - UPSR へのアップグレード 13-13, 13-15
    - 受け入れテスト 5-6
    - プロビジョニング 5-5
    - リニア ADM へのアップグレード 13-2, 13-5
  - 防止
    - LCD からの IP アドレス表示および設定 19-36
    - RJ-45 ポートを介した LAN アクセス 22-5
    - オーダーワイヤループ 17-91
  - 法的免責事項 19-56
  - ポート
    - 1+1 保護のプロビジョニング 17-88
    - CE シリーズ POS ポートのプロビジョニング 22-8
    - CE-1000-4 イーサネット ポートのプロビジョニング 22-3
    - CE-100T-8 イーサネット ポートのプロビジョニング 22-7
    - E シリーズ イーサネット ポートのプロビジョニング 19-17
    - E シリーズ イーサネットのプロビジョニング 19-15
    - G シリーズ イーサネットのプロビジョニング 19-18
    - LCD のステータス表示 20-35
    - SDH への光ポートの変更 18-52
    - SNMP のデフォルトの UDP ポート 19-63
    - UDP ポート 4-15
    - アラーム プロファイルの適用 22-15
    - サービス状態の変更 19-10
    - 最適化 1+1 保護のプロビジョニング 17-42
    - トランスポンダ モードの G シリーズのプロビジョニング 6-93
    - 名前の割り当て 20-9
    - 光のプロビジョニング、PPM を参照
    - ファイアウォールのプロビジョニング 17-79, 17-80
  - ポートの命名 20-9
  - ポートレス トランスマックス 6-24
  - 保護
    - SONET トポロジを参照
    - カード保護を参照
    - 自動保護切り替えを参照
  - ホップ 17-79, 18-18
- ま
- マウント ブラケット 17-2
  - マウント、取り付けを参照
  - マップ (ネットワーク) 5-50, 19-58, 22-31
  - マニュアル
    - このマニュアルの関連資料 xxv
    - 対象読者 xxiii
    - 表記法 xxvi
    - マニュアルの構成 xxiv
    - 目的 xxiii
- む
- むき出しの電源コンダクタへのコーティング 17-21
- も
- モジュール、カードを参照
  - モニタ回線 7-7
- ゆ
- ユーザ
- 削除 18-28, 18-30
  - セットアップ 4-5
  - 単一ノードでの作成 17-89
  - パスワードとセキュリティ レベルの変更 18-27, 18-29
  - 複数ノードでの作成 17-90
- ユーザのログアウト
- 単一ノード 20-9
  - 複数ノード 20-10
- よ
- 抑制
    - アラーム レポート 22-21
- ら
- ラックの取り付け
    - 23 インチ ラックから 19 インチ ラックへの変換 17-2
    - シェルフの取り付け 17-5

- 複数のシェルフの取り付け 17-7
- り
- リストストラップのプラグ差し込み口 17-8
- リセット
  - CE-100T-8 カード 17-68, 19-19
  - PM カウント 18-14
  - TCC2/TCC2P カード 20-54
  - イーサネット カード 21-46
  - 電気回路カード 21-46
  - ノード クロック 17-20
  - 光カード 21-46
- リニア ADM
  - 1+1 ポイントツーポイント型からのアップグレード 13-2, 13-5
  - 2 ファイバ BLSR へのアップグレード 13-7, 13-10
  - UPSR へのアップグレード 13-13, 13-15
  - 受け入れテスト 5-11
  - ノードの削除 14-21
  - ノードの追加 14-16, 14-18
  - プロビジョニング 5-9
- リピータ モード
  - IP 設定のプロビジョニング 19-35
  - IP 設定の変更 19-57
  - データベースのロード制限 15-7
- リフレッシュ
  - 1 日間隔での PM カウント 18-12
  - 15 分間隔での PM カウント 18-11
  - E シリーズおよび G シリーズ イーサネット PM カウント 20-37
  - 異なるポートの PM カウント 19-47
  - 異なるリフレッシュ間隔での FC\_MR-4 PM カウント 20-44
  - 異なるリフレッシュ間隔でのイーサネット PM カウント 19-46
- リング
  - BLSR を参照
  - UPSR を参照
  - サブテンディングリングを参照
- リング ID 13-23
- リンクの統合 21-69
- リンク、統合 21-69
- る
- ルーティング テーブル、セキュア モードでの IP アドレスの表示 19-36
- ループバック
  - 2 ファイバ BLSR 5-18
  - 4 ファイバ BLSR 5-21
  - 『Cisco ONS 15454 Troubleshooting Guide』も参照
  - UPSR 5-30, 5-43
  - ポイントツーポイント型 5-7
  - リニア ADM 5-12
- ろ
- ローカル オーダーワイヤ 17-91
- ロール
  - キャンセル 21-69
  - 削除 21-63
  - 単一光回線への 2 つのクロスコネク (自動ルーティング) 21-54
  - 単一光回線への 2 つのクロスコネク (手動ルーティング) 21-58
  - 特定の光回線の送信元または宛先 21-49
  - トラフィックのブリッジおよびロール 7-15
  - 光回線間での 2 つのクロスコネク 21-61
  - 光回線間での単一クロスコネク 21-52
- ロールのキャンセル 21-69
- ロゲイン ノード グループ
  - 現在のグループからのノードの削除 20-34
  - 作成 17-74
  - 指定されたグループからのノードの削除 20-62
  - セキュア (ロック) モードのときの IP アドレスの入力 17-74, 17-76
  - ノードの削除による CTC の表示への影響 14-10, 14-15
  - ノードの追加 17-75
  - 表示 17-73
- ロック
  - セキュア モード 21-12
  - ツールバーを使用するノード A-5
- ロック ワッシャ 2-25
- ロックアウト、外部切り替えコマンドを参照
- ロックオン、外部切り替えコマンドを参照
- 論理ネットワーク マップ 5-50

わ

ワイヤ

- カッター 1-4
- ストリッパ 1-4
- ラッパー 1-4

ワイヤラップ パネル、外付け 1-19

割り当て

- 二重 IP アドレス 21-10
- バックプレーン ポートの IP アドレス 21-10
- ポート名 20-9