



CHAPTER 10

モニタリング

この章では、モニタリング アクティビティについて説明します。次の事項について説明します。

- 「ping」 (P.10-1)
- 「SLA」 (P.10-3)
- 「タスク マネージャ」 (P.10-25)
- 「レポート」 (P.10-29)

ping

ping を使用して、Prime Provisioning は VPN 接続をモニタリングします。つまり、VPN を構成するさまざまなエッジ デバイス間の接続を確認します。



(注) ping 機能は、IOS XR を稼働しているデバイスではサポートされません。

これを実現するために、これらのデバイスの間で一連の ping を実行できます。ping には次の利点があります。

- サービスは独立しているため、MPLS アプリケーションの機能監査に使用できる。
- サービスが機能しているかどうかに関係なく、サービスの機能監査を行わずに確立できる。
- VPN サービス展開よりも前に CPE における IPv4 接続の検証に使用できる。

ただし、ping は次のことを行いません。

- ping は、ICMP トラフィックがブロックされている環境、たとえば、アクセス リストですべての ICMP トラフィックが拒否される Cisco IOS ルータでは機能できない。
- ping は、接続問題があることだけを通知する。そのため、任意のサービス固有の情報を提供しません。接続の問題は、デバイス障害、設定ミスなど、ping では識別できない多くの問題が原因である可能性があります。
- ルータのの顧客側（または、内部あるいは非セキュア）インターフェイスの背後にある即時のサブネットのみがサポートされます。キャンパス サブネットはサポートできません。

Ping GUI は、MPLS サービス要求で想定されるすべての ping をサポートします。この項では、MPLS サービス要求に ping を実行する例を示します。



(注) Prime Provisioning には役立つ可能性のあるコンポーネントの Prime Diagnostics があります。『[Cisco Prime Provisioning 6.3 User Guide](#)』を参照してください。

[Inventory] > [Device Tools] > [Ping] を選択します。[Services] ウィンドウが表示されます。
[Type] フィールドに [MPLS] が示されます。手順は次のとおりです。

ステップ 1 ping パラメータを設定する各行の横にあるチェックボックスをオンにします。

ステップ 2 [Configure Ping Parameters] ボタンをクリックして、イネーブルにします。

[MPLS Parameters] ウィンドウが表示されます。

次に入力し、[Start Ping] をクリックします。

- [Ping Type: Do PE to CE Ping] : このオプション ボタンを選択すると、MPLS VPN リンクを形成するすべての PE CE ペアに対して VRF ping が行われます。この ping に対する IP アドレスはリンクのエンドポイント アドレスです。たとえば、MPLS サービス要求に 2 つのリンク PE1<>CE1 と PE2<>CE2 があるとします。この選択の場合、(PE1, CE1)、(PE2, CE2)、(PE1, CE2)、および (PE2, CE1) という 4 つの VRF ping が開始されます。この選択が選ばれると、[Start Ping] をクリックした後に、に直接移動し、結果のページを受け取ります。
- [Ping Type: Do CE to CE Ping] : このオプション ボタンが選択されると、サービス要求にエンドポイントを作成するすべての CE 間で ping が行われます。この選択が選ばれると、[Start Ping] をクリックした後に、ステップ 3 に移動します。
- [Two-way Ping] (デフォルトでは使用不可で選択されていない) : このチェックボックスは、[Do CE to CE Ping] を選択した場合にのみ使用できます。デバイス 1 からデバイス 2 への ping が発生する場合、このチェックボックスがオンにされていると、デバイス 2 からデバイス 1 への ping も発生します。
- [Packet Repeat Count] (デフォルトは 5) : この値は、ping に使用する ICMP パケットの数を示します。
- [Datagram size] (デフォルトは 100) : この値は、ping に使用する ICMP のパケット サイズです。

ステップ 3 [Do CE to CE Ping] に [MPLS CE Selection] ウィンドウが表示されます。

ステップ 4 CE を選択する各行の横にあるチェックボックスをオンにします。

ステップ 5 [Start MPLS CE Ping] をクリックして、イネーブルにします。

[MPLS Ping Test Results] ウィンドウを受け取ります。

ウィンドウ下部のボタンを次に示します。

- [Redo Ping] : このボタンをクリックすると、すべての ping が再開します。使用されるパラメータは前回の要求で指定されたものと同じです。
- [View Job Logs] : このボタンをクリックすると、ping を実行するために作成されたすべての Prime Provisioning のジョブのログを受け取ります。ping アプリケーションは、選択されたサービス要求ごとに 1 つのジョブを作成します。
- [Refresh] : 選択的に更新するには、[Auto Refresh] ボタンをオフにして、結果を更新したいときにこのボタンをクリックします。
- [Close] : 現在の ping 要求を閉じるには、このボタンをクリックします。[Monitoring] ページに戻ります。



(注) カラム ヘッダが青色の場合、そのカラム ヘッダをクリックすると、カラムをソートできます。

ステップ 6 [Close] をクリックしてこの ping セッションを終了します。

SLA

サービス レベル契約 (SLA) は、顧客にサービス プロバイダーが提供するサービスのレベルを定義します。パフォーマンスは SLA サーバを介してモニタされます。Prime Provisioning は、サービス保証 エージェント (SA エージェント) デバイスをサポートする Cisco IOS ルータで、SLA をプロビジョニング、収集、およびモニタすることにより、サービス関連のパフォーマンス基準をモニタします。SLA をプロビジョニングし、各 SLA の統計情報を収集するには、データ収集タスクで最低限のユーザ入力が必要です。



(注) SLA 機能は、IOS XR を稼働しているデバイスではサポートされません。

SLA 収集タスクは、関連パフォーマンス データを収集、これを永続的に保存、集約し、役に立つレポートを提供します。SLA 収集タスクは、デバイスの SA Agent MIB から収集します。Prime Provisioning は SA Agent MIB を 24 x 7 ベースの SLA パフォーマンスの監視に利用します。MIB を使用して、一般的なプロトコルのネットワーク トラフィックをモニタできます。

- Dynamic Host Configuration Protocol (DHCP)
- ドメイン ネーム システム (DNS)
- ファイル転送プロトコル (FTP)
- Hyper Text Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル)
- Internet Control Message Protocol Echo (ICMP Echo)
- ジッタ (音声ジッタ)
- Transmission Control Protocol Connect (TCP Connect)
- User Datagram Protocol Echo (UDP Echo)。



(注) SLA は Oracle をデータベースとして選択するかどうかとは関係なく、組み込み Sybase データベースを使用します。



(注) SLA は、[Create]、[Delete]、[Enable Probes]、[Disable Probes]、[Enable Traps]、および [Disable Traps] の操作を自動的に行うことでタスクを作成し、それによって実際の操作を実行します。タスクのステータスは、[Inventory] > [Task Manager] > [Logs] にナビゲートすることで表示できます。

この項では、SLA プローブの設定、SLA データの設定、およびこれらの SLA プローブに関する SLA レポートの表示方法を説明します。

「[SLA を使用する前のセットアップ](#)」(P.10-4) でセットアップ手順を実装してから、[Inventory] > [Device Tools] > [SLA] を選択します。

次に、[Inventory] > [Device Tools] > [SLA] を選択すると、次のいずれかを選択できるようになります。

- 「[プローブ](#)」(P.10-7) はデフォルトの選択肢です。
- 「[レポート](#)」(P.10-19)

SLA を使用する前のセットアップ

SLA は SNMP のアクティビティです。SNMP がイネーブルであり、ルータの SNMP 設定がリポジトリの設定と一致することを確認します。

SLA を [From MPLS CPE] または [From MPLS PE or MVRP-CE] を使用して作成する場合、サービスに関連付けられたサービス要求は [Deployed] 状態である必要があります。

SNMP の設定

Prime Provisioning を機能させるには、SNMP がカスタマー ネットワークの各 CPE デバイスで設定されている必要があります。Prime Provisioning で、SNMP は次を行うために使用されます。

- インターフェイス MIB からの収集
- SLA データをプロビジョニングと収集

SNMPv1/v2c と SNMPv3 の 2 つのセキュリティ モデルを使用できます。表 10-1 には、セキュリティ モデルとセキュリティ レベルの組み合わせが示されています。

表 10-1 SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	説明
v1/v2c	認証なし/暗号化なし	Community String	No	コミュニティ スtring の照合を使用して認証します。
v3	認証なし/暗号化なし	Username	No	ユーザ名の照合を使用して認証します。
v3	認証/ 暗号化なし	MD5 または SHA	No	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
v3	認証/ 暗号化	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。CBC-DES (DES-56) 標準に基づいて認証する以外に、DES 56 ビット暗号化を行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：パケットの内容を符号化して許可されていない送信元から読み取れないようにします。

SNMPv3 オブジェクトには次の特性があります。

- 各ユーザは 1 つのグループに属します。

- グループは、一連のユーザに対してアクセス ポリシーを定義し、このユーザが受信できる通知のリストを決定します。グループは、そのユーザのセキュリティ モデルとセキュリティ レベルも定義します。
- アクセス ポリシーは、どの SNMP オブジェクトが読み取り、書き込み、または作成のためにアクセスできるかを定義します。
- SNMPv3 は、検出ではサポートされません。

Cisco IOS ルータでの SNMPv1/v2c の設定

SNMP がイネーブルかどうかを判別し、Cisco IOS ルータで SNMP コミュニティ スtring を設定するには、各ルータに対して次のステップを実行します。

	コマンド	説明
ステップ 1	Router> enable Router> <enable_password>	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ 2	Router# show snmp	show snmp コマンドの出力を確認して、「SNMP agent not enabled.」というステートメントがあるかどうかを確認します。SNMP がイネーブルではない場合、この手順のステップを完了します。
ステップ 3	Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	Router(config)# snmp-server community <userstring> RO	コミュニティ read-only スtring を設定します。
ステップ 5	Router(config)# snmp-server community <userstring> RW	コミュニティ read-write スtring を設定します。
ステップ 6	Router(config)# Ctrl+Z	特権 EXEC モードに戻ります。
ステップ 7	Router# copy running startup	設定の変更内容を不揮発性 RAM (NVRAM) に保存します。



ヒント

ターゲット デバイスごとに Prime Provisioning に定義された SNMP コミュニティ スtring は、デバイスで設定されているものと同じでなければなりません。

Cisco IOS ルータでの SNMPv3 パラメータの設定

この項では、Cisco IOS ルータで SNMPv3 パラメータを設定する方法について説明します。SNMPv3 は、IOS の暗号化イメージのみでサポートされます。認証/暗号化を行うには、IOS イメージに DES56 が必要です。



ヒント

ターゲット デバイスごとに Prime Provisioning に定義された SNMP ユーザは、デバイスで設定されているものと同じでなければなりません。

既存の SNMP コンフィギュレーションを確認するには、ルータ端末セッションで次のコマンドを使用します。

- **show snmp group**
- **show snmp user**

Cisco IOS ルータで SNMPv3 サーバ グループおよびユーザ パラメータを設定するには、次のステップを実行します。



(注) 最初にグループを作成し、次にユーザを作成する必要があります。

	コマンド	説明
ステップ1	Router> enable Router> <enable_password>	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ2	Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	Router(config)# snmp-server group [<groupname> {v1 v2c v3 {auth noauth priv}}] [read <readview>] [write <writeview>] [notify <notifyview>] [access <access-list>]	snmp-server group コマンドは、新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定します。各グループは、特定のセキュリティレベルに属します。 例: snmp-server group v3auth v3 auth read v1default write v1default
ステップ4	Router(config)# snmp-server user <username> [<groupname> remote <ip-address> [udp-port <port>] {v1 v2c v3 [encrypted] [auth {md5 sha} <auth-password> [priv des56 <priv-password>]] [access <access-list>]	snmp-server user コマンドは、新しいユーザを SNMP グループに設定します。 例: snmp-server user user1 v3auth v3 auth md5 user1Pass
ステップ5	Router(config)# Ctrl+Z	特権 EXEC モードに戻ります。
ステップ6	Router# copy running startup	設定の変更内容を不揮発性 RAM (NVRAM) に保存します。

Cisco IOS ルータでの RTR 応答側の手動イネーブル



(注) ルータで SNMP が設定されている必要があります。

Cisco IOS ルータで RTR 応答側を手動でイネーブルにするには、次の手順を実行します。

	コマンド	説明
ステップ1	Router> enable Router> <enable_password>	イネーブル モードに入り、次にイネーブル パスワードを入力します。
ステップ2	Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	Router(config)# rtr responder	SA エージェント操作のターゲット ルータの SA 応答側をイネーブルにします。
ステップ4	Router(config)# Ctrl+Z	特権 EXEC モードに戻ります。
ステップ5	Router# copy running startup	設定の変更内容を不揮発性 RAM (NVRAM) に保存します。

プローブ

[Inventory] > [Device Tools] > [SLA] を選択すると、[SLA Probes] ウィンドウが表示されます。

イネーブルになっているデフォルト ボタンは [Create] であり、[Create] ドロップダウン リストから、SLA プローブを作成するために [From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] から選択できます。ただし、既存のプローブの行をクリックして 1 つ以上の既存のプローブを選択した場合、他のボタン、[Details]、[Delete]、[Enable] および [Disable] にアクセスできます。[Enable] および [Disable] の場合、ドロップダウン リストには、SLA の [Probes] と SLA の [Traps] をイネーブルまたはディセーブルにするオプションが含まれています。

ボタンとそれに続いて表示されるドロップダウン リストの説明は、次のとおりです。

- 「共通パラメータの作成」 (P.10-7) : この項では、すべてのプローブ作成タイプの SLA 共通パラメータ、[From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] を説明します。
- 「任意の SA エージェントデバイスからの作成」 (P.10-10) : この項では、任意の SA エージェントデバイスからのプローブを作成する方法を説明し、共通パラメータを作成した後に開始します。
- 「MPLS CPE からの作成」 (P.10-11) : この項では、MPLS CPE からプローブを作成する方法について説明し、共通パラメータを作成した後に開始します。
- 「MPLS PE または MVRF-CE からの作成」 (P.10-13) : この項では、MPLS PE または MVRF-CE からプローブを作成する方法について説明し、共通パラメータを作成した後に開始します。
- 「プロトコル」 (P.10-15) : 各 [Create] パスの共通プローブ情報を提供します。
- 「詳細」 (P.10-17) : この項では、特定のプローブに関する詳細を説明します。
- 「削除」 (P.10-17) : この項では、プローブを削除する方法について説明します。
- 「プローブのイネーブル化」 (P.10-18) : この項では、プローブをイネーブルにして、[Created] から [Active] 状態にステータスを変更する方法を説明します。
- 「トラップのイネーブル化」 (P.10-18) : この項では、トラップをイネーブルにする方法について説明します。
- 「プローブのディセーブル化」 (P.10-19) : この項では、プローブをディセーブルにして、[Active] から [Disabled] 状態にステータスを変更する方法を説明します。
- 「トラップのディセーブル化」 (P.10-19) : トラップをディセーブルにする方法について説明します。

共通パラメータの作成

[Inventory] > [Device Tools] > [SLA] を選択すると、デフォルトは [Probes] ページになり、[Create] ボタンのみがイネーブルになります。[Create] ドロップダウン リストから、[From Any SA Agent Device(s)]、[From MPLS CPE]、または [From MPLS PE or MVRF-CE] を選択できます。作成中に表示される最初のウィンドウは、すべてここで指定します。その後、選択した特定の作成タイプに進みます。

手順は次のとおりです。

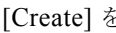
-
- ステップ 1** [Create] を選択すると、 10-1 に示されているようなウィンドウが表示されます。

図 10-1 SLA Common Parameters

SLA Common Parameters

SLA Common Parameters		
SLA Life* :	<input type="text" value="-1"/>	(secs)
Threshold* :	<input type="text" value="5000"/>	(msecs)
Timeout* :	<input type="text" value="5000"/>	(msecs)
Frequency (1 - 604800)* :	<input type="text" value="60"/>	(secs)
TOS Category:	<input checked="" type="radio"/> Precedence <input type="radio"/> DSCP	
TOS (0 - 7)* :	<input type="text" value="0"/>	
Keep History:	<input type="checkbox"/>	
Number of Buckets (1 - 60)* :	<input type="text" value="15"/>	
Enable Traps:	<input type="checkbox"/>	
Falling Threshold (1 - Threshold)* :	<input type="text" value="3000"/>	(msecs)
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> <input type="button" value="Close"/>		
Note: * - Required Field		

デフォルトを受け入れるか、次のように、共通の SLA パラメータのフィールドの情報を返納し、[Next] をクリックします。

- [SLA Life] (必須) : プローブがアクティブである秒数 (最大値は秒単位での 32 ビット整数の最大値です)。値を一般的なデフォルト値である **-1** に設定すると、プローブは永久にアクティブになります。
- [Threshold] (必須) : しきい値制限をミリ秒で定義する整数。このしきい値を超過し、トラップがイネーブルである場合、トラップが送信されます。最大値は 32 ビット整数の最大値です。エージェント (SA エージェント) の動作時間に影響を与えるサービスがこの制限を超えた場合、しきい値超過が SA エージェントによって記録されます。[Threshold] の値が、[Timeout] の値を超えることはできません。デフォルト値は **5000** です。
- [Timeout] (必須) : SA エージェントの操作の完了を待機する時間 (ミリ秒単位)。[Timeout] の値は、[Frequency] の値以下であり、[Threshold] の値以上である必要があります。デフォルト値は **5000** です。
- [Frequency] (0 ~ 604800) (必須) : 各 SA エージェント操作が開始されるまでの期間 (秒単位)。[Frequency] の値は、[Timeout] の値以上である必要があります。デフォルト値は **60** です。
- [TOS Category] (デフォルトは [Precedence]) : [TOS Category] の [Precedence] オプション ボタンを選択した場合、Type of Service (TOS; タイプ オブ サービス) 値の 1 のセットを使用できます。[TOS Category] の [DSCP] オプション ボタンを選択すると、TOS 値の異なるセットが得られます。
- [TOS] (必須) : 任意の整数。値の範囲と意味は、[TOS Category] のオプション ボタンが [Precedence] (値 : 0 ~ 7) または [DSCP] (値 : 0 ~ 63) のどちらに設定されているかによって異なります。
 - [TOS Category] が [Precedence] に設定されている場合、有効な値は **0 ~ 7** です。これらの値は、IP ヘッダーの [ToS] フィールドの 3 つの最上位ビットを表します。デフォルト値は **0** です。[Precedence] 値の意味は、表 10-2 に指定されています。



(注) タイプ オブ サービスは、SLA プローブの [DNS] および [DHCP] タイプには適用されません。Prime Provisioning はこれらの 2 つのタイプの SLA プローブに設定されたすべての ToS 値を無視します。たとえば、まず ToS 値に 5 を選択し、SLA プローブに [DNS]、[DHCP]、および [ICMP Echo] プロトコルを選択すると、Prime Provisioning は選択した ToS 値を ICMP Echo プローブのみに適用します。

表 10-2 [Precedence] の値の意味

ToS 値	バイナリ値	意味
7	111	ネットワーク制御
6	110	インターネットワーク制御
5	101	CRITIC/ECP
4	100	フラッシュ オーバーライド
3	011	フラッシュ
2	010	即時
1	001	優先順位
0	000	ルーチン

- [TOS Category] が [DSCP] に設定されている場合、有効な値は **0** から **63** です。これらの値は、IP ヘッダーの [ToS] フィールドの 6 つの最上位ビットを表します。デフォルト値は **0** です。これらの [TOS] 値は、ユーザ指定です。



(注) Prime Provisioning は、0 ~ 7 の [PRECEDENCE] 値を 3 つの最上位 ToS ビットにマッピングします (値は 5 ビット左に移動します)。同様に、0 ~ 63 の [DSCP] 値は、2 ビット左に移動します。

- [Keep History] (デフォルトはオフ) : [Keep History] チェックボックスがオンの場合、ルータの最近の [History Table] が保持されます。特に、ロー ラウンドトリップ時間 (RTT) SLA 測定を維持する SA Agent MIB で保持されます。このように選択することで、保持する未加工の履歴データの [Number of Buckets] を示すこともできます。[Keep History] のチェックボックスをデフォルトのオフのままにしていると、未加工の履歴データは保持されません。[Keep History] は HTTP および Jitter についてはサポートされません。
- [Number of Buckets] (1 ~ 60) (必須) : [Keep History] チェックボックスがオンの場合、デフォルトは 15 です。範囲は 1 ~ 60 であり、未加工の履歴データに保存される最新の未加工データ エントリの数を示します。指定した [Number of Buckets] を超過すると、最も古いバケットからバケットの削除が開始され、指定された数のみ未加工のデータ エントリが保持されるようになります。
- [Enable Traps] (デフォルト : オフ、つまり [No] に設定) : [Enable Traps] チェックボックスをオンにすると、作成された SLA は 3 つのタイプのトラップを送信するように設定されます。このように選択すると、[Falling Threshold] を示すことができるようになります。[Enable Traps] チェックボックスがオフの場合、このタスクで作成される SLA でトラップがディセーブルにされます。
- [Falling Threshold] (1 ~ [Threshold]) (必須) : [Enable Traps] チェックボックスがオンの場合、デフォルト値は、**3000** (ミリ秒単位) です。範囲は、ミリ秒単位で **1** から [Threshold] 値までです。トラップがイネーブルで、遅延が指定されたミリ秒に達している場合、トラップが送信されます。

- ステップ 2** 次に、「任意の SA エージェント デバイスからの作成」(P.10-10)、「MPLS CPE からの作成」(P.10-11) または「MPLS PE または MVRP-CE からの作成」(P.10-13) に進みます。

任意の SA エージェント デバイスからの作成

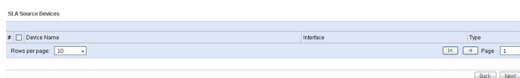
「共通パラメータの作成」(P.10-7) での手順を完了したら、次の手順に従います。



(注) IP 接続が SA Agent デバイス間で使用できる必要があります。

- ステップ 1** 表示される次のウィンドウは、[図 10-2](#) に示されているようになります。

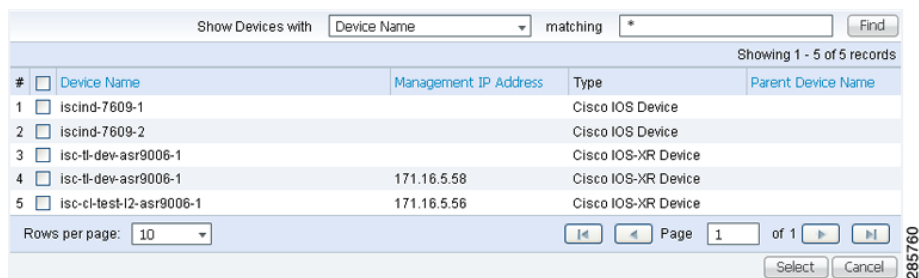
図 10-2 SLA 送信元デバイス



285759

- ステップ 2** [Add] ボタンをクリックすると、[図 10-3](#) に示すようなウィンドウが表示されます。このウィンドウには、少なくとも 1 つのインターフェイスがある、データベースのすべてのデバイスがリストされます。選択するデバイスの各行の横にあるチェックボックスをオンにして、[Select] をクリックします。

図 10-3 [SLA Devices] > [Add]



285760

[図 10-2](#) に戻ります。新しく追加された送信元デバイスが表示されます。この送信元デバイスに関する情報は、次のコラムで指定します。

- [Device Name] : このヘッダーをクリックすると、デバイス名がアルファベット順にソートされます。
- [Interface] : [Select] をクリックすると、ウィンドウが表示されます。このウィンドウから、IP アドレスを更新できます。インターフェイスのいずれかのオプション ボタンを選択し、[Select] をクリックすると、[図 10-2](#) に示すように IP アドレスが変わります。
- [Type] : 送信元デバイスのタイプを指定します。

ステップ 3 ステップ 2 から を繰り返して複数のデバイスを追加したり、現在選択されている送信元デバイスを削除したりできます。デバイスを削除するには、削除するデバイスの各行の横にあるチェックボックスをオンにして、[Delete] をクリックします。



(注) 送信元デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 4 [Next] をクリックします。
表示される次のウィンドウは、[図 10-4](#) に示されているようになります。

図 10-4 SLA の宛先デバイス



ステップ 5 [Add] ボタンをクリックすると、[図 10-3](#) に示すようなウィンドウが表示されます。選択するデバイスの各行の横にあるチェックボックスをオンにします。次に、[Select] をクリックします。

ステップ 6 [図 10-4](#) に戻ります。新しく追加された宛先デバイスが表示されます。この宛先デバイスに関する情報は、次のカラムで指定します。

- [Device Name] : このヘッダーをクリックすると、デバイス名がアルファベット順にソートされます。
- [Interface] : [Select] をクリックすると、ウィンドウが表示されます。このウィンドウから、IP アドレスを更新できます。インターフェイスのいずれかのオプション ボタンを選択し、[Select] をクリックすると、[図 10-4](#) に示すように IP アドレスが変わります。
- [Type] : 送信元デバイスのタイプを指定します。

ステップ 7 ステップ 5 からステップ 6 を繰り返してさらにデバイスを追加したり、現在選択されている宛先デバイスを削除したりできます。デバイスを削除するには、削除するデバイスの各行の横にあるチェックボックスをオンにして、[Delete] をクリックします。



(注) 宛先デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 8 [Next] をクリックします。「[プロトコル](#)」(P.10-15) に進みます。

MPLS CPE からの作成

「[共通パラメータの作成](#)」(P.10-7) での手順を完了したら、次の手順に従います。

ステップ 1 「[共通パラメータの作成](#)」(P.10-7) のステップを完了して、次のウィンドウを表示します ([図 10-5](#) を参照)。

図 10-5 SLA CPE パラメータ

SLA Source and Destination Devices

VPN Information

VPN*:

Customer:

Source Device

CPE*:

CPE Interface*:

Destination Device(s)

Type: Connected PE
 CPEs

Connected PE:

Connected PE Interface:

Note: * - Required Field

285762

- ステップ 2** [VPN] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースのすべての VPN がリストされます。
- ステップ 3** 選択する VPN のオプション ボタンをクリックします。次に、[Select] をクリックします。図 10-5 に戻ります。新しく追加された [VPN] および [Customer] の情報が表示され、[CPE] の [Select] ボタンが表示されます。ステップ 2 を繰り返して、VPN を変更できます。
- ステップ 4** [CPE] の [Select] ボタンをクリックすると、選択した VPN に関連付けられた CPN がリストされたウィンドウが表示されます。選択する CPE のオプション ボタンをクリックします。次に、[Select] をクリックします。
- ステップ 5** 図 10-5 に戻ります。新しく追加された [CPE] とその最初のインターフェイスが表示され、[CPE Interface] に [Select] ボタンが表示されます。ステップ 4 を繰り返して CPE を変更できます。
- ステップ 6** 表示されるデフォルトの [CPE Interface] 情報を変更する場合、[Select] をクリックして、ウィンドウを表示します。
- ステップ 7** 選択するインターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。図 10-5 に戻ります。新しく追加された [CPE Interface] が表示されます。
- ステップ 8** ステップ 6 を繰り返して CPE インターフェイスを変更できます。
- ステップ 9** [Connected PE] のオプション ボタンを選択したままにすることで、デフォルトの [Type] を維持することができます。これにより、CPE とその直接接続された PE の間に SLA が作成されます。あるいは、同じ VPN 内で [CPEs] のオプション ボタンを選択できます。[Connected PE] のデフォルトを使用する場合は、ステップ 10 に進みます。[CPEs] オプション ボタンをクリックする場合は、ステップ 14 に進みます。
- ステップ 10** [Connected PE Interface] の [Select] をクリックして、ウィンドウを表示します。
- ステップ 11** 選択するインターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。
- ステップ 12** 図 10-5 に戻ります。新しく追加された [Connected PE Interface] が表示されます。ステップ 10 を繰り返して、[Connected PE Interface] を変更できます。
- ステップ 13** [Next] をクリックして、「プロトコル」(P.10-15) に進みます。
- ステップ 14** [CPEs] をクリックすると、図 10-6、「CPEs」のようなウィンドウが表示されます。

図 10-6 CPEs

SLA Source and Destination Devices

VPN Information

VPN*: d-vpn-pw
 Customer: d-customer

Source Device

CPE*:

CPE Interface*:

Destination Device(s)

Type: Connected PE
 CPEs

CPEs:

Showing 0 of 0 records	
#	Device Name Interface
Rows per page: 10	
Page 1 of 1	

Note: * - Required Field

- ステップ 15** [CPEs] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースの指定 VPN に関連するすべての CPE がリストされます。
- ステップ 16** 選択する CPE の各行の横にあるチェックボックスをオンにします。次に、[Select] をクリックします。



(注) [Source Device] として選択されているデバイスを [Destination Device(s)] に追加しないでください。

図 10-6 に戻ります。新しく追加された [Device Name] が表示されます。

- ステップ 17** [Interface] カラムの [Select] をクリックして、ウィンドウを表示します。
- ステップ 18** 選択する CPE の行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。
- ステップ 19** 図 10-6 に戻ります。新しく追加された [CPE Interface] が表示されます。ステップ 17 を繰り返して CPE インターフェイスを変更できます。
- ステップ 20** 削除するデバイスの各行の横にあるチェックボックスをオンにします。[Remove] ボタンをクリックします。デバイスが削除された状態でウィンドウが表示されます (図 10-6 を参照)。
- ステップ 21** 図 10-6 の表示内容を反映するには、[Next] をクリックして、「プロトコル」(P.10-15) に進みます。

MPLS PE または MVRF-CE からの作成

「共通パラメータの作成」(P.10-7) での手順を完了したら、次の手順に従います。

- ステップ 1** 「共通パラメータの作成」(P.10-7) の手順を完了すると、図 10-7 の「SLA Source and Destination Devices」に示されているウィンドウが次に表示されます。

図 10-7 SLA Source and Destination Devices

SLA Source and Destination Devices

VPN Information

VPN*: d-vpn-pw
 Customer: d-customer

Source Device

PE/MVRF-CE*:
 VRF*:

Destination Device(s)

PEs and CPEs:

Showing 0 of 0 records	
#	Interface
Rows per page: 10	
Page 1 of 1	

Note: * - Required Field

- ステップ 2** [VPN] の [Select] ボタンをクリックして、ウィンドウを表示します。このウィンドウには、データベースのすべての VPN がリストされます。選択する VPN の行の横にあるオプション ボタンをクリックします。
- ステップ 3** 次に、[Select] をクリックします。
- ステップ 4** 図 10-7 に戻ります。新しく追加された [VPN] および [Customer] の情報が表示されます。ステップ 2 を繰り返して、[VPN] および [Customer] を変更できます。
- ステップ 5** [PE/MVRF-CE] の新しい [Select] ボタンをクリックして、ドロップダウン リストを表示します。このドロップダウン リストから、[PE] または [MVRF-CE] を選択できます。[PE] を選択すると、ウィンドウが表示されます。このウィンドウでは、選択した VPN に関連するすべての PE がリストされます。[MVRF-CE] を選択すると、ウィンドウが表示されます。このウィンドウでは、選択した VPN に関連するすべての MVRF-CE がリストされます。選択する PE または MVRF-CE の行の横にあるオプション ボタンをクリックします。次に、[Select] または [OK] をクリックします。
- ステップ 6** 図 10-7 に戻ります。新しく追加された [PE] および [MVRF-CE] の情報が表示されます。ステップ 5 を繰り返して、この選択を変更できます。
- ステップ 7** ステップ 5 で MVRF-CE 情報を選択すると、[VRF] ドロップダウン リストをクリックできるようになります。
- ステップ 8** 宛先デバイスの新しい [Select] ボタンをクリック : PE と CPE、およびドロップダウンリストから、[PEs] または [CPEs] を選択します。[PEs] を選択すると、ウィンドウが表示されます。このウィンドウでは、データベースのすべての PE インターフェイスがリストされます。[CPEs] を選択すると、ウィンドウが表示されます。このウィンドウでは、データベースのすべての CPE インターフェイスがリストされます。選択するデバイス インターフェイスの行の横にあるオプション ボタンをクリックします。次に、[Select] をクリックします。



(注)

[Source Device] として選択されているデバイスを [Destination Device(s)] に追加しないでください。

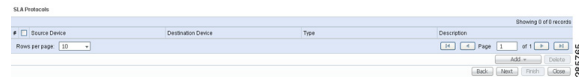
- ステップ 9** 図 10-7 に戻り、インターフェイス情報を表示します。[Select] をクリックして、ウィンドウを表示します。このウィンドウでは、別のインターフェイスの横にあるオプション ボタンをクリックできます。[Select] をクリックすると、古いインターフェイスが新しいインターフェイスに置き換えられます。このステップを繰り返して、インターフェイスを変更できます。
- ステップ 10** [Next] をクリックして、「プロトコル」(P.10-15) に進みます。

プロトコル

いずれかの [Create] 機能のすべてのステップ、「共通パラメータの作成」(P.10-7)、「MPLS CPE からの作成」(P.10-11) または 「MPLS PE または MVRF-CE からの作成」(P.10-13) を完了したら、この場所を選択します。手順は次のとおりです。

ステップ 1 「共通パラメータの作成」(P.10-7) のステップを完了して、次のウィンドウを表示します (図 10-8 を参照)。

図 10-8 プロトコル



- ステップ 2** [Add] ドロップダウン リストをクリックして、次のものを選択します。
- [ICMP Echo] (宛先デバイスが使用できる場合だけ使用できます) : [ステップ 3](#) に進みます。
 - [TCP Connect] (MPLS PE または MVRF-CE からの作成では使用できません。その他のすべての作成方法では、[TCP Connect] は宛先デバイスが使用できる場合だけ使用できます) : [ステップ 4](#) に進みます。
 - [UDP Echo] (宛先デバイスが使用できる場合だけ使用できます) : [ステップ 5](#) に進みます。
 - [Jitter] (宛先デバイスが使用できる場合だけ使用できます) : [ステップ 6](#) に進みます。
 - [FTP] (MPLS PE または MVRF-CE からの作成では使用できません) : [ステップ 7](#) に進みます。
 - [DNS] (MPLS PE または MVRF-CE からの作成では使用できません) : [ステップ 8](#) に進みます。
 - [HTTP] (MPLS PE または MVRF-CE からの作成では使用できません) : [ステップ 9](#) に進みます。
 - [DHCP] (MPLS PE または MVRF-CE からの作成では使用できません) : [ステップ 10](#) に進みます。
- ステップ 3** [ステップ 2](#) から [ICMP Echo] を選択した場合、プロトコル [ICMP Echo] ウィンドウが表示されます。次のように、必須情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。
- [Request Size] (0 ~ 16384) (必須) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは **28** です。
- ステップ 4** [ステップ 2](#) から [TCP Connect] を選択した場合、プロトコル [TCP Echo] ウィンドウが表示されます。次のように、必須およびオプション情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。
- [Destination Port] (1 ~ 65535) (必須) : モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **23** が使用されます。
 - [Request Size] (1 ~ 16384) (任意) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは、**1** です。
- ステップ 5** [ステップ 2](#) から [UDP Echo] を選択した場合、プロトコル [UDP Echo] ウィンドウが表示されます。次のように、必須およびオプション情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。
- [Destination Port] (1 ~ 65535) (必須) : モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **7** が使用されます。
 - [Request Size] (4 ~ 8192) (任意) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは **16** です。
- ステップ 6** [ステップ 2](#) から [Jitter] を選択した場合、プロトコル [Jitter] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。

- [Destination Port] (1 ~ 65535) (必須) : モニタリング パケットが送信されるターゲットのポート番号。特定のポートを指定しない場合、ポート **8000** が使用されます。
- [Request Size] (16 ~ 1500) (任意) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは、**32** です。
- [Number of Packets] (1 ~ 1000) (任意) : 転送する必要があるパケットの数を表す整数。デフォルト値は、**10** です。
- [Interval] (1 ~ 1000) (任意) : パケット間のパケット間遅延をミリ秒単位で表す整数 (**1 ~ 1,000**)。デフォルト値は、**20** です。

ステップ 7 [ステップ 2](#) から [FTP] を選択した場合、プロトコル [FTP] ウィンドウが表示されます。

次のように、必須およびオプション情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。

- [User Name] (任意) : 空の場合、**anonymous** が使用されます。
- [Password] (任意) : 空の場合、**test** が使用されます。
- [Host IP Address] (必須) : ファイル転送プロトコル (FTP) の IP アドレスを入力します。
- [File Path] (必須) : FTP サーバの FTP 対象ファイルのパスを入力します。

ステップ 8 [ステップ 2](#) から [DNS] を選択した場合、プロトコル [DNS] ウィンドウが表示されます。

次のように、必須情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。

- [Name Server] (必須) : ネーム サーバの IP アドレスを指定する文字列。このアドレスは、ドット付き IP アドレス形式です。
- [Name to be Resolved] (必須) : DNS サーバにより解決される名前または IP アドレスのいずれかである文字列。文字列が名前の場合、長さは **255** 文字です。文字列が IP アドレスの場合、ドット付き IP アドレス形式です。
- [Request Size] (0 ~ 16384) (必須) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは、**1** です。

ステップ 9 [ステップ 2](#) から [HTTP] を選択した場合、プロトコル [HTTP] ウィンドウが表示されます。

次のように、オプションおよび必須情報を入力し、[OK] をクリックして、[ステップ 11](#) に進みます。

- [Version] (デフォルトは 1.0) : HTTP サーバのバージョンを指定する文字列。これは変更しないでください。Prime Provisioning は、バージョン 1.0 だけをサポートします。
- [URL] (必須) : HTTP プロローブが通信する URL、*HTTPServerName[/directory]/filename* または *HTTPServerAddress[/directory]/filename* (たとえば、**http://www.cisco.com/index.html** または **http://209.165.201.22/index.html**) を表す文字列。[HTTPServerName] を指定した場合、[Name Server] は必須です。[HTTPServerAddress] を指定した場合、[Name Server] は必須ではありません。
- [Cache] (デフォルトでは選択済み (オン) : チェックボックスがオフの場合、HTTP 要求は、キャッシュされたページをダウンロードしません。チェックボックスがオンの場合、HTTP 要求は、使用できる場合、キャッシュされたページをダウンロードします。そうでない場合、要求は、HTTP サーバに転送されます。
- [Proxy Server] (任意) : プロキシ サーバ情報を表す文字列 (最大 255 文字)。デフォルトは、ヌル文字列です。
- [Name Server] (任意、[URL] 設定により異なります) : ネーム サーバの IP アドレスを指定する文字列。このアドレスは、ドット付き IP アドレス形式です。

- [Operation] (デフォルトは [HTTPGet]) : HTTP get 要求を表すデフォルトの [HTTPGet] ではなく、ユーザ定義ペイロードで HTTP 要求を表す [HTTPRaw] が必要な場合、ドロップダウン リストを使用して、選択します。
- [Raw Request] ([Operation] が [HTTPRaw] の場合必須。[Operation] が [HTTPGet] の場合は使用できません) : [Operation] が [HTTPRaw] の場合だけ必要な文字列。これにより、単純な GET 動作以外の他のタイプの HTTP 動作を呼び出すことができます。
- [Request Size] (1 ~ 16384) (必須) : パケットのデータ部分に置かれるオクテット (バイト単位) の数を表す数値。デフォルトは **28** です。

ステップ 10 ステップ 2 から [DHCP] を選択した場合、プロトコル [DHCP] ウィンドウが表示されます。

次のように、必須情報を入力し、[OK] をクリックして、ステップ 11 に進みます。

- Destination IP Address (必須)

ステップ 11 図 10-8 に戻ります。提供した [Protocol] 情報に基づいて、情報の追加カラムが表示されます。[Next] をクリックして作業を進める前に、[Add] でプロトコルをさらに追加するか決定します。この場合、ステップ 2 ~ ステップ 10 を繰り返します。または、[Delete] で現在選択されている任意のプロトコルを削除します。この場合、[Delete] をクリックして、ステップ 2 ~ ステップ 10 を繰り返してプロトコルを削除します。



(注) 宛先デバイスの削除は元に戻すことはできません。確認ウィンドウは表示されません。

ステップ 12 次に表示されるウィンドウは、定義した [Description] (作成日時)、[Common Parameters]、[Source Devices]、[Destination Devices] および [Protocols] を示す [Probe Creation Task Summary] ウィンドウです。表示内容で変更しない場合、[Finish] をクリックします。変更する場合、[Back] をクリックして変更します。

詳細

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、詳細を表示できます。

- ステップ 1** 詳細を表示するプローブに対応するチェックボックスをオンにして、既存のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。
- ステップ 2** [Details] ボタンをクリックすると、[SLA Probes Details] ウィンドウが表示されます。このウィンドウには、最初に [Create] を実行したときに定義された [Common Attributes] の情報、およびプロトコルで定義された [Protocol Specific Attributes] の情報が含まれます。
- ステップ 3** [OK] をクリックして戻ります。さらに [Details] を選択するか、別の機能を実行できます。

削除

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、リストからプローブを削除できます。

- ステップ 1** 既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Delete] ボタンにアクセスできるようになります。
- ステップ 2** [Delete] ボタンをクリックすると、確認ウィンドウが表示されます。

ステップ 3 削除した状態が反映された場合は [OK] をクリックします。反映されていない場合は [Cancel] をクリックします。



(注) プローブが削除されると、プローブがプローブ リスト ページから削除されますが、データベースには残ります。

情報が更新された状態のウィンドウが表示されます。

プローブのイネーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、プローブをイネーブルにできます。

ステップ 1 既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Enable] ボタンにアクセスできるようになります。[Enable] ドロップダウン リストから、[Probes] にアクセスできます。

ステップ 2 [Enable] > [Probes] を選択すると、プローブのイネーブルを確認するウィンドウが表示されます。

ステップ 3 プローブがイネーブルにされた場合は [OK] をクリックします。イネーブルにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] に緑色のチェックマークが付きます。[Status] カラムは、プローブがルータで正常に作成された場合、[Active] に設定されます。

トラップのイネーブル化

[Inventory] > [Device Tools] > [SLA] を選択し、次のステップを実行することで、トラップをイネーブルにできます。

ステップ 1 既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Enable] ボタンにアクセスできるようになります。[Enable] ドロップダウン リストから、[Traps] にアクセスできます。

ステップ 2 [Enable] > [Traps] を選択すると、トラップのイネーブルを確認するウィンドウが表示されます。すべてのトラップには、下限しきい値として 3000 ms が自動的に設定されます。

ステップ 3 トラップがイネーブルにされた場合は [OK] をクリックします。トラップにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] に緑色のチェックマークが付きます。[Traps Enabled] カラムは、ルータのプローブが正常に変更されると、[yes] に設定されます。

プローブのディセーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、[Disable Probes] を使用して、デバイスのプローブを削除できます。手順は次のとおりです。

ステップ 1 既存のプローブの行のチェックボックスをオンにして、イネーブルにされた 1 つ以上のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。[Disable] ドロップダウン リストから、[Probes] にアクセスできます。

ステップ 2 [Disable] > [Probes] を選択すると、プローブのディセーブルを確認するウィンドウが表示されます。

ステップ 3 プローブがディセーブルにされた場合は [OK] をクリックします。ディセーブルにされていない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] に緑色のチェックマークが付きます。プローブのステータスは、ルータのプローブが正常に削除されると、[Disabled] になります。

トラップのディセーブル化

[Inventory] > [Device Tools] > [SLA] を選択すると、次のステップを実行して、トラップをディセーブルにできます。

ステップ 1 既存のプローブの行のチェックボックスをオンにして、1 つ以上の既存のプローブを選択します。これで、[Disable] ボタンにアクセスできるようになります。[Disable] ドロップダウン リストから、[Traps] にアクセスできます。

ステップ 2 [Disable] > [Traps] を選択すると、トラップのディセーブルを確認するウィンドウが表示されます。

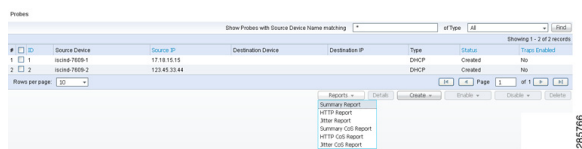
ステップ 3 トラップをディセーブルにする場合は [OK] をクリックします。ディセーブルにしない場合は [Cancel] をクリックします。

成功した場合、[Status] ウィンドウが表示され、[Succeeded] に緑色のチェックマークが付きます。ルータのプローブが正常に変更されると、トラップはディセーブルにされます。

レポート

[Inventory] > [Device Tools] > [SLA] を選択すると、[図 10-9](#) に示されているウィンドウが表示されます。

図 10-9 SLA レポート



次のいずれかをクリックして、そのレポートを表示できます。

- 「[Summary Report](#)」 (P.10-20) : このレポートは、HTTP およびジッタ以外のすべての情報 (ICMP Echo、TCP Connect、UDP Echo、FTP、DNS および DHCP) を要約します。
- 「[HTTP Report](#)」 (P.10-23) : HTTP 情報の要約レポートです。
- 「[Jitter Report](#)」 (P.10-23) : ジッタ情報の要約レポートです。
- 「[Summary CoS Report](#)」 (P.10-24) : HTTP およびジッタ以外のサービス クラス (CoS) (ICMP Echo、TCP Connect、UDP Echo、FTP、DNS および DHCP) の要約レポートです。
- 「[HTTP CoS Report](#)」 (P.10-25) : HTTP CoS 情報のレポートです。
- 「[Jitter CoS Report](#)」 (P.10-25) : ジッタ CoS 情報のレポートです。

Summary Report

図 10-9 から、[Summary Report] を選択して、次のステップを実行します。

ステップ 1 [Summary Report] を選択すると、図 10-10 のようなウィンドウが表示されます。

図 10-10 Parameters of Summary Report

Parameters of Summary Report

Layout

Value Displayed* : All

Aggregate By* : All Customer Provider VPN Source Router Probe

Timeline* : All Yearly Monthly Weekly Daily Hourly

2012 JUL 12 00:00

Filtering

Customer: Select

Provider: Select

VPN: Select

Source Routers: Select

Destination Routers: Select

Probes: Select

Precedence: [dropdown]

DSCP: [dropdown]

Probe Type: [dropdown]


OK Cancel

Note: * - Required Field

285767

ステップ 2 図 10-10 で、次のように、[Layout] フィールドに入力します。






- [Value Displayed] (必須) (デフォルトは [All]) : ドロップダウン リストをクリックして、次のいずれかを選択します。
 - [All] : すべての値を表示します。
 - [Connections (#)] : 接続数を表示します。
 - [Timeouts (#)] : タイムアウト数を表示します。
 - [Connectivity (%)] : 接続の割合を表示します。
 - [Threshold Violations (%)] : しきい値超過の割合を表示します。
 - [Max Delay (ms)] : ミリ秒単位の最大遅延を表示します。
 - [Min Delay (ms)] : ミリ秒単位の最小遅延を表示します。
 - [Avg Delay (ms)] : ミリ秒単位の平均遅延を表示します。
- [Aggregate By] (必須) (デフォルトは [All]) : [All]、[Customer]、[Provider]、[VPN]、[Source Router] または [Probe] 別から、データ平均方法のオプション ボタンをクリックします。
- [Timeline] (必須) (デフォルトは [Weekly]、選択した週の最初の日付の午前 0 時から開始) : 表示するレポート データ ([All] データ、[Yearly] データ、[Monthly] データ、[Weekly] データ、[Daily] データまたは [Hourly] データ) のオプション ボタンをクリックします。レポートを開始する、年、月、日付、時刻のドロップダウン リストをクリックします。

ステップ 3  10-10 で、次のように、[Filtering] フィールドに入力します。



(注)

レポートには、フィルタリング フィールドのすべての条件を満たすデータだけが含まれます（すべての条件は、論理積で結合されます）。

- [Customer] (任意) : [Select] ボタンをクリックして、カスタマーの結果リストから、リストをフィルタリングします（選択した場合）。リストされた [Customers] から、この SLA レポートの [Customer] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、選択されたカスタマーが、[Customer] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Provider] (任意) : [Select] ボタンをクリックして、プロバイダーの結果リストから、リストをフィルタリングします（選択した場合）。リストされた [Providers] から、この SLA レポートの [Provider] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、選択されたプロバイダーが、[Provider] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [VPN] (任意) : [Select] ボタンをクリックして、VPN の結果リストから、リストをフィルタリングします（選択した場合）。リストされた [VPNs] から、この SLA レポートの [VPN] のオプション ボタンをクリックします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、選択された VPN が、[VPN] でリストされます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Source Routers] (任意) : [Select] ボタンをクリックして、デバイスの結果リストから、リストをフィルタリングします（選択した場合）。リストされたデバイスから、デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、[Source Routers] に選択されたデバイスが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Destination Routers] (任意) : [Select] ボタンをクリックして、デバイスの結果リストから、リストをフィルタリングします（選択した場合）。リストされたデバイスから、デバイスのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、[Destination Routers] に選択されたデバイスが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Probes] (任意) : [Select] ボタンをクリックして、送信元プローブの結果リストから、リストをフィルタリングします（選択した場合）。リストされた送信元プローブから、送信元プローブのチェックボックスをオンにします。次に、[Select] をクリックします。クリックすると  10-10 に戻り、[Probes] に選択された送信元プローブが含まれます。選択を変更する場合は、このプロセスを繰り返すことができます。
- [Precedence] (デフォルトは [All]) : ドロップダウン リストをクリックして、他の [Precedence] の [TOS] の選択肢、0 ~ 7 を選択します。これらの値は、IP ヘッダーの [ToS] フィールドの 3 つの最上位ビットを表します。[Precedence] 値の意味は、表 10-2 に指定されています。



(注)

Prime Provisioning は、0 ~ 7 の [PRECEDENCE] 値を 3 つの最上位 ToS ビットにマッピングします（値は 5 ビット左に移動します）。



(注)

タイプ オブ サービスは、SLA プロブの [DNS] および [DHCP] タイプには適用されません。Prime Provisioning はこれらの 2 つのタイプの SLA プロブに設定されたすべての ToS 値を無視します。たとえば、まず ToS 値に 5 を選択し、SLA プロブに [DNS]、[DHCP]、および [ICMP Echo] プロトコルを選択すると、Prime Provisioning は選択した ToS 値を ICMP Echo プロブのみに適用します。

- [DSCP] (デフォルトは [All]) : ドロップダウン リストをクリックして、他の [DSCP] の [TOS] の選択肢、0 ~ 63 を選択します。これらの値は、IP ヘッダーの [ToS] フィールドの 6 つの最上位ビットを表します。これらの [TOS] 値は、ユーザ指定です。



(注) Prime Provisioning は、0 ~ 63 の [DSCP] 値を 6 つの最上位 ToS ビットにマッピングします (値は 2 ビット左に移動します)。

- [Probe Type] (デフォルトは [All]) : ドロップダウン リストをクリックして、プローブのタイプ、[ICMP Echo]、[UDP Echo]、[TCP Connect]、[HTTP]、[DNS]、[Jitter]、[DHCP]、[FTP] から選択します。



(注) これらのプローブタイプについては、「[プロトコル](#)」(P.10-15) で詳しく説明されています。

ステップ 4 必要な情報が表示されたら、[OK] をクリックします (図 10-10 を参照)。

選択した項目がリストされた要約レポートが表示されます。該当するボタンを使用して、このレポートで [Modify]、[Refresh]、[Print]、[Close] を実行できます。



(注) [Modify] を選択すると、図 10-10 のようなウィンドウが表示されます。このウィンドウでは、前述のステップで説明されているように、選択項目を変更できます。

HTTP Report

図 10-9 から、[HTTP Report] を選択して、「[Summary Report](#)」(P.10-20) と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] のドロップダウン リストの項目が異なります。
- [Destination Routers] 選択はありません。
- プローブタイプは自動的に [HTTP] になるため、図 10-10 に [Probe Type] ドロップダウン リストはありません。結果は HTTP レポートです。

Jitter Report

図 10-9 から、[Jitter Report] を選択して、「[Summary Report](#)」(P.10-20) と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] のドロップダウン リストの項目が異なります。
- [Destination Routers] 選択はありません。
- プローブタイプは自動的に [Jitter] になるため、図 10-10 に [Probe Type] ドロップダウン リストはありません。結果はジッタ レポートです。

Summary CoS Report

図 10-9 から、サービス クラス (CoS) の要約レポート (SLA プロープの TOS 値に基づきます) の [Summary CoS Report] を選択して、次のステップを実行します。

ステップ 1 [Summary CoS Report] を選択します。図 10-11 のようなウィンドウが表示されます。

図 10-11 Parameters of CoS Summary Report

ステップ 2 図 10-11 で、「Summary Report」(P.10-20) のステップ 2 に示すように、[Layout] フィールドに入力します。ただし、次のことが異なります。[Value Displayed] の後、[Aggregate By] の前で、新しい [TOS Type] のオプション ボタン [Precedence] (デフォルト) または [DSCP] を選択します。説明が [Filtering] セクションに示されます (「Summary Report」(P.10-20) のステップ 3 を参照)。

ステップ 3 図 10-11 で、「Summary Report」(P.10-20) のステップ 3 に示すように、[Filtering] フィールドに入力します。ただし、[Precedence] または [DSCP] ドロップダウン リストはありません。この項のステップ 2 で説明されているように、これらは [Layout] フィールドにあります。

ステップ 4 必要な情報が表示されたら、[OK] をクリックします (図 10-11 を参照)。

選択した項目がリストされた CoS 要約レポートが表示されます。該当するボタンを使用して、このレポートで [Modify]、[Refresh]、[Print]、[Close] を実行できます。



(注)

[Modify] を選択すると、図 10-11 のようなウィンドウが表示されます。このウィンドウでは、前述のステップで説明されているように、選択項目を変更できます。

HTTP CoS Report

図 10-9 から、[HTTP Report] を選択して、「Summary CoS Report」(P.10-24) と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] には、[HTTP Report] と同じドロップダウン項目があります。
- [Destination Routers] 選択はありません。
- プロブタイプは自動的に [HTTP CoS] になるため、図 10-11 に [Probe Type] ドロップダウンリストはありません。結果は CoS HTTP レポートです。この CoS HTTP レポートは、SLA プローブの TOS 値に基づいています。

Jitter CoS Report

図 10-9 から、[Jitter Report] を選択して、「Summary CoS Report」(P.10-24) と同様に処理を進めます。ただし、次のことが異なります。

- [Value Displayed] には、[Jitter Report] と同じドロップダウン項目があります。
- [Destination Routers] 選択はありません。
- プロブタイプは自動的に [Jitter CoS] になるため、図 10-11 に [Probe Type] ドロップダウンリストはありません。結果は CoS ジッタ レポートです。この CoS ジッタ レポートは、SLA プローブの TOS 値に基づいています。

タスク マネージャ

Prime Provisioning にはタスク マネージャが備わっており、これを使用して、すべてのタイプの現在および期限切れのタスクの両方についての関連情報の表示、新しいタスクの作成とスケジュール設定、指定したタスクの削除、およびアクティブおよび期限切れのタスクの削除を行えます。

ここでは、次の内容について説明します。

- 「タスク」(P.10-25)
- 「タスク ログ」(P.10-29)

タスク

ここでは、次の内容について説明します。

- 「タスク マネージャの起動」(P.10-26)
- 「作成」(P.10-26)
- 「監査」(P.10-27)
- 「詳細」(P.10-28)
- 「スケジュールリング」(P.10-28)
- 「ログ」(P.10-28)
- 「削除」(P.10-28)

タスク マネージャの起動

タスク マネージャを起動するには、[Operate] > [Tasks] > [Task Manager] をクリックします。[Tasks list] ページが表示されます。

[Tasks] ウィンドウには、[Task Name]、[Type]、[Targets]、[Schedules] の日時、[User Name] (タスクの作成者)、および [Created on] の日付ごとに、各タスクの情報が表示されます。リストされたタスクを表示、スケジュール設定、または削除するには、対応するチェックボックスをオンにします。

このウィンドウを使用して新しいタスクを作成または監査することもできます。

作成

新しいタスクを作成するには、次の手順に従ってください。

ステップ 1 [Task Manager] ウィンドウで、[Create] をクリックします。表示されるドロップダウン リストから、次のいずれかを選択します。選択した項目が、[Type] になります (図 10-12 を参照)。

- [Collect Config] : デバイスからコンフィギュレーションを収集します。
- [Collect Config From Files] : Prime Diagnostics に対してのみ、ファイルからコンフィギュレーションを収集します。
- [Enable Disable VFW Traps] : VFW トラップをイネーブルまたはディセーブルにします。
- [L2VPN (L2TPv3) Functional Audit] :
- [Password Management] : ユーザ パスワードと SNMP コミュニティ スtring を管理します。
- [SLA Collection] : SLA がイネーブルなデバイスからデータを収集します。
- [Service Deployment] : 既存の SR を展開します。
- [TE Full Discovery] :
- [TE Incremental Discovery] :
- [TE Interface Performance] : SNMP を使用するトンネルおよびインターフェイス帯域利用率を計算します。

図 10-12 タスクの作成

Create Task

Config Collection - Task Information

Name*: Collect Config 2012-07-12 09:43:14.199

Type: Collect Config

Description: Created on 2012-07-12 09:43:14.199

Back Next Finish Close

Note: * - Required Field

ステップ 2 [Name] : タスクの名前を入力します。デフォルト値を受け入れることができます。

ステップ 3 [Type] : ステップ 1 で定義されています。

ステップ 4 [Description] (オプション) : 説明を入力します。

- ステップ 5** [Task Configuration Method] (デフォルト : [Simplified]) : [Simplified] または [Advanced (via wizard)] を選択します。[Simplified] を選択すると、1 つのウィンドウの多くの選択を行うことができます。[Advanced (via wizard)] を選択すると、多数のウィンドウを移動して選択を行います。
- ステップ 6** [Next] をクリックして続行します。
 選択するタスクのタイプに従って、[Task Devices]、[Task Service Requests]、または [Configurations File Directory] ページがバリエーションとともに表示されます。
- ステップ 7** 必要な場合は、[Select/Deselect] をクリックしてデバイスまたはサービス要求を追加します。
-  **(注)** ステップ 7 からステップ 10 は [Collect Config From Files] と [TE Interface Performance] には適用されません。
-
- ステップ 8** 結果の選択ウィンドウで、デバイスまたはサービス要求を選択し、[Select] をクリックします。
 選択したデバイスまたはサービス要求が表示されます。
- ステップ 9** [Groups] は、前の手順で指定するタスクによって、表示される場合と表示されない場合があります。これが表示された場合、ステップ 7 およびステップ 8 と同様に、デバイスのグループを追加できます。これが表示されない場合、またはこのデバイス グループ選択を完了した後、ステップ 10 に進みます。
- ステップ 10** [Options] を選択します。
 [Retrieve Interfaces] チェックボックスがオンの場合、Prime Provisioning は Simple Network Management Protocol (SNMP) を使用して ifIndex などのデバイス インターフェイス情報を取得します。[Retrieve Interfaces] チェックボックスがオフの場合でも、コンフィギュレーション収集情報は取得されますが、SNMP は使用されません。IP Service Level Agreement (SLA; サービス レベル契約) プローブ以外では、SNMP またはこのオプションは必要ありません。
- ステップ 11** [Configuration File Directory] が表示されたら、Prime Provisioning サーバのディレクトリへのパスを [Configuration File Directory] テキスト ボックスに入力して、オフライン コンフィギュレーション ファイルが保存されている Prime Provisioning サーバのディレクトリを示します。
- ステップ 12** [Schedule] については、[Now]、[Later]、または [None] をクリックします。[Later] を選択すると、[Later Schedule category] が表示されます。次に、[Edit] ボタンをクリックして、[Task Scheduler] ページを表示する必要があります。
- ステップ 13** タスクをスケジュールリングする情報を選択して、[OK] をクリックします (デフォルトのスケジュールは [Now] です)。
- ステップ 14** 続行するには、[Submit] をクリックします。
 新しいタスクがタスクのリストに追加されます。

監査

監査情報を取得するには、[Tasks] ページで [Audit] をクリックします。表示されるドロップダウン リストから、次のいずれかを選択します。選択した項目が、[Type] になります。

- [Config Audit] : Prime Provisioning により生成されるコンフィグレットをデバイスのコンフィグレットと比較します。
- [L2VPN (L2TPv3) Functional Audit] : L2TPv3 機能を監査します。
- [MPLS Functional Audit] : MPLS 機能を監査します。
- [TE Functional Audit] : ルータの Label Switch Path (LSP; ラベル スイッチ パス) をリポジトリに格納されている LSP と比較します。

詳細

特定のタスクに関する詳細情報を取得するには、次の手順を実行します。

-
- ステップ 1** [Tasks] ページから、情報の詳細リストを表示する、いずれかのタスクのチェックボックスをオンにします。
 - ステップ 2** [Details] をクリックします。
 - ステップ 3** [OK] をクリックして戻ります。
-

スケジューリング

既存のタスクのスケジューリングを変更するには、次のステップを実行します。

-
- ステップ 1** [Tasks] ページから、スケジューリング方法をリセットする、いずれかのタスクのチェックボックスをオンにします。
 - ステップ 2** [Schedules] をクリックします。
 - ステップ 3** このタスクを削除する場合は、[ステップ 4](#)に進みます。スケジューリング方法をリセットする場合は、[ステップ 5](#)に進みます。
 - ステップ 4** 新しいウィンドウで、削除するタスクのチェックボックスをオンにして、[Delete] ボタンをクリックします。次に、[ステップ 7](#)に進みます。
 - ステップ 5** 新しいウィンドウで、[Create] をクリックします。
 - ステップ 6** 新しいスケジューリングの選択を行い、[Save] をクリックして、スケジューリング指示をリセットします。
 - ステップ 7** すべてのチェックボックスをオフにして、[OK] をクリックして戻ります。
-

ログ

[Tasks] ページでこの選択を行って、「[タスク ログ](#)」(P.10-29) で説明されている事柄を行うこともできます。

削除

1 つ以上のタスクを削除するには、次のステップを実行します。

-
- ステップ 1** [Tasks] ページで、削除するタスクの 1 つ以上のチェックボックスをオンにします。確認ウィンドウが表示されます。
 - ステップ 2** 削除する場合は、[OK] をクリックします。削除しない場合は、[Cancel] をクリックします。
 - ステップ 3** 更新された [Tasks] ページに戻ります。
-

タスク ログ

タスク ログを使用して、タスクが正常に完了したかどうか、タスクのステータスを確認できます。また、タスク ログを使用して、失敗したタスクをトラブルシューティングすることもできます。タスク ログを表示するには、次の手順に従います。

ステップ 1 [Operate] > [Tasks] > [Task Logs] をクリックします。

[Task Logs] ウィンドウが表示されます。

このウィンドウには、タスクの [Runtime Task Name]、[Action]、[Start Time]、[End Time]、および [Status] ごとにタスクが表示されます。このウィンドウを使用して、ログを表示または削除できます。

ステップ 2 ログを表示するには、タスクを表す行にあるチェックボックスをオンにして、[View Log] ボタンをクリックします。

[Task Log] ページが表示されます。

表示するログ レベルのタイプを設定できます。[Log Level] を指定し、[Filter] ボタンをクリックして表示する情報を表示します。

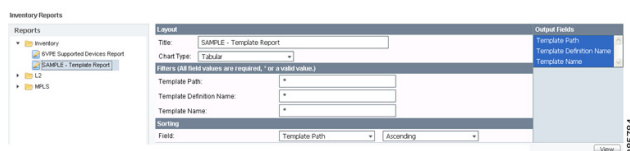
ステップ 3 [Return to Logs] をクリックして、表示する別のログを指定します。

レポート

[Inventory] > [Reports] > [Inventory Reports] を選択すると、レポートのツリーがデータ ペインに表示されます。データ ペインで各フォルダの + 記号をクリックすると、提供されたすべてのレポートのリストが表示されます。L2VPN フォルダの SAMPLE 以外のレポートと、MPLS フォルダの SAMPLE 以外のレポートについては、『Cisco Prime Provisioning 6.3 User Guide』で説明されています。

特定のレポートをクリックして、レポートの設定方法を定義できます。図 10-13 には、フォルダ **Inventory** の下にあるサンプル ファイルが示されています。

図 10-13 [Inventory] > [SAMPLE - Template Report - Report] ウィンドウ



この項では、レポート機能と、次の領域でそれを使用する方法について説明します。

- 「レポートの概要」(P.10-30)
- 「レポートへのアクセス」(P.10-30)
- 「レポート GUI の使用」(P.10-30)
- 「レポートの実行」(P.10-31)
- 「カスタム レポートの作成」(P.10-33)

レポートの概要

ネットワーク オペレータは、通常、プロビジョニングされるサービスに関する詳細なレポートが必要となることがあります。たとえば、特定の顧客に対して、PE-CE 接続およびそれらの詳細な PE-CE 設定パラメータのリストを表示したり、PE での特定の Layer2 または Layer3 サービス要求を表示したりできます。これらのレポートは、一箇所から Service Request (SR; サービス要求) および VPN 情報を検出できるため、ネットワーク オペレータに役に立ちます。

[Inventory] > [Reports] > [Inventory Reports] を選択すると、タイプごとにレポートがグループ化され、簡単にナビゲーションできるようになります。Prime Provisioning には、ユーザが RBAC 権限を持つ、事前定義された (can された) レポートのみが表示されます。


フィルタリング基準と、レポートに表示される出力を選択できます。レポートは、さまざまな形式で保存できます。

『Cisco Prime Provisioning 6.3 User Guide』で説明されている事前定義されたレポートのほかに、Prime Provisioning は追加のサンプル レポートを提供します。サンプル レポートは参考用としてのみ提供され、テストおよびサポートは行われません。

Prime Provisioning が GUI にレポートを提供するために使用するデータ構造は XML 形式で定義されません。

レポートへのアクセス

レポートにアクセスするには、次の手順を実行します。

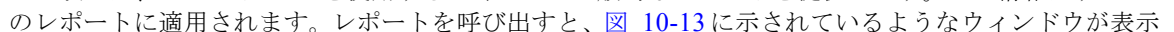
-
- ステップ 1** Prime Provisioning GUI のレポート フレームワークにアクセスするには、[Inventory] > [Reports] > [Inventory Reports] を選択します。
 - ステップ 2** フォルダをクリックして、使用可能なレポートを表示します。

図 10-13 に示すように、[Reports] ウィンドウが表示されます。
 - ステップ 3** 左側のナビゲーション ツリーのいずれかのフォルダの下にリストされているレポートから、目的のレポートをクリックすると、そのレポートに関連付けられたウィンドウが開きます。
-



(注)

各レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。ユーザは独自のカスタム レポートを作成するベースとしてこのレポートをサポートされているレポートとともに使用できます。カスタム レポートについては、「[カスタム レポートの作成](#)」(P.10-33) を参照してください。

レポート GUI の使用

この項では、レポート GUI を使用するいくつかの一般的なコメントを提供します。この情報はすべてのレポートに適用されます。レポートを呼び出すと、 **図 10-13** に示されているようなウィンドウが表示されます。

ウィンドウは複数のエリアに分割されています。

- 「[レイアウト](#)」(P.10-31)

- 「フィルタ」 (P.10-31)
- 「出力フィールド」 (P.10-31)
- 「ソート」 (P.10-31)

レイアウト

この領域にはレポートのタイトルが表示され、チャートタイプを選択することができます。[Title] フィールドを上書きすることで、独自のレポート タイトルを入力できます。



(注) 表形式の出力のみがサポートされています。

フィルタ

このペインで、レポートの入力または検索条件を定義できます。ここに入力する値は、Prime Provisioning のリポジトリにあるデータ オブジェクト関連付けられた、対応する値と比較されます。値はすべてのフィールドに入力する必要があります。ストリング全体に、アスタリスク (*) をワイルドカードとして使用できます。

フィルタリング可能な各フィールドには、GUI でラベルとテキストの入力フィールドが表示されます。特定のフィールドについては、GUI で [Select] ボタンも表示され、既存のオブジェクトを選択できます (たとえば、[Customer]、[Service Type]、[SR State] など)。使用可能なすべての出力フィールドがウィンドウに表示され、レポートに含めるフィールドを選択できます。すべての出力フィールドはデフォルトで選択されています。



(注) フィルタ値は、Prime Provisioning 内で表される値と同じ形式にする必要があります。たとえば、Service Request (SR) ID は数値にする必要があります。

出力フィールド

このペインでは、レポートに表示する出力フィールドを選択できます。マウスで出力フィールドの一部またはすべてを選択できます。出力値の連続した範囲を選択するには、Shift キーを使用します。出力値をランダムに選択するには Ctrl キーを使用します。

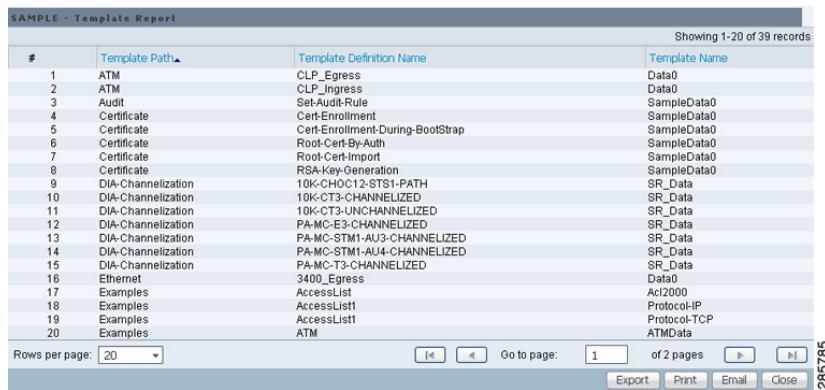
ソート

このペインでは、レポート出力をどのようにソートするかを選択できます。フィールドの場合は、最初のドロップダウン リストを選択して各フィルタ フィールドを選択し、2 番目のドロップダウン リストでレポート フィールドを昇順または降順のどちらかで表示するかを選択します。レポート出力を表示した後に、ソート順序を変更することもできます (図 10-14 を参照)。

レポートの実行

レポートを実行するには、レポート ウィンドウの右下隅の [View] をクリックします。これにより、レポート出力が生成されます。レポート出力の例を図 10-14 に示します。

図 10-14 レポート出力



#	Template Path	Template Definition Name	Template Name
1	ATM	CLP_Egress	Data0
2	ATM	CLP_Ingress	Data0
3	Audit	Set-Audit-Rule	SampleData0
4	Certificate	Cert-Enrollment	SampleData0
5	Certificate	Cert-Enrollment-During-BootStrap	SampleData0
6	Certificate	Root-Cert-By-Auth	SampleData0
7	Certificate	Root-Cert-Import	SampleData0
8	Certificate	RSA-Key-Generation	SampleData0
9	DIA-Channelization	10K-CHOC12-ST31-PATH	SR_Data
10	DIA-Channelization	10K-CT3-CHANNELIZED	SR_Data
11	DIA-Channelization	10K-CT3-UNCHANNELIZED	SR_Data
12	DIA-Channelization	PA-MC-E3-CHANNELIZED	SR_Data
13	DIA-Channelization	PA-MC-STM1-AU3-CHANNELIZED	SR_Data
14	DIA-Channelization	PA-MC-STM1-AU4-CHANNELIZED	SR_Data
15	DIA-Channelization	PA-MC-T3-CHANNELIZED	SR_Data
16	Ethernet	3400_Egress	Data0
17	Examples	AccessList	Ac12000
18	Examples	AccessList1	Protocol-IP
19	Examples	AccessList1	Protocol-TCP
20	Examples	ATM	ATMData

レポート GUI は表形式の出力をサポートします。出力はレポート ウィンドウで選択した出力から取得された列でリストされます。

各行（またはレコード）は、レポート ウィンドウのフィルタ フィールドを使用して設定した検索基準との一致を示します。

場合によっては、フィールドに返される値は次のいずれかとして表示できます。

- **-1** は、このフィールドに更新された情報がないことを意味します
- **F** は **false** を意味します
- **T** は **true** を意味します

三角形アイコンの付いたカラム見出しは、レコードのソート基準になる出力です。カラムの見出しをクリックすることにより、ソートの昇順と降順を切り替えることができます。別の出力値でソートするには、その値のヘッダーをクリックします。

レポート出力のウィンドウから、次のボタンを使用して、エクスポート、印刷、または電子メールを行います。

- [Export]（「レポートのエクスポート」(P.10-32) を参照）
- [Print]（「レポートの印刷」(P.10-33) を参照）
- [E-mail]（「電子メール レポート」(P.10-33) を参照）

レポートのエクスポート

図 10-14 の [Export] アイコンをクリックして、次の手順を実行します。

ステップ 1 目的の形式に該当するオプション ボタンを選択します。

- [PDF file] : Adobe の Portable Document Format。
- [CSV file] : データをさまざまなアプリケーションに簡単にエクスポートできるカンマ区切り値。

ステップ 2 保存する行を選択して、[OK] をクリックします。

Prime Provisioning は選択した形式でレポートを生成します。



(注)

出力を表示および保存するには、システムに適切なアプリケーションが必要です（たとえば、Acrobat Reader または Excel）。

レポートの印刷

図 10-14 で、[Print] アイコンをクリックします。

このウィンドウを使用して、印刷により適した形式でレポートを表示することができます。目的の行を選択して、[OK] をクリックします。結果が Web ブラウザに表示されます。そこから、レポートを印刷できます。

電子メール レポート

図 10-14 の [E-mail] アイコンをクリックして、次の手順を実行します。

- ステップ 1** [To:] フィールド（必須）で、レポートの送信先となる 1 つ以上の電子メール アドレスを指定します。
- ステップ 2** [From:] フィールド（任意）に、メッセージ ヘッダに表示される電子メール アドレスを入力します。これにより、応答メッセージが有効な電子メール アドレスに送信されるようになります。
- ステップ 3** [CC:] フィールド（任意）に、このレポートのコピーを受信する受信者の電子メールアドレスを入力します。
- ステップ 4** 件名フィールドは送信されたレポートのタイトルを示します。
このフィールドを上書きして、レポートの名前を変更できます。これは、電子メール メッセージの [Subject] フィールドに表示されます。
- ステップ 5** レポートを送信するときの出力形式（PDF または CSV）のオプション ボタンを選択します。
- ステップ 6** 送信する行数を選択します。
- ステップ 7** 必要に応じて、[Message] フィールドに、レポートをアナウンスするにメッセージを入力してから [Send] をクリックします。

カスタム レポートの作成

各フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーション ファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

\$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/<folder_name>_report.xml

ここで、<folder_name> はインベントリ、L2、または MPLS です。

使用できる各レポート（サンプル レポートを含む）は、**packageDef name = "<folder_name>"** 下の <objectDef name> 開始および終了タグ内に含まれる XML コンテンツで定義されます。介入 XML コンテンツによって、レポートのタイトル、すべての許容可能なフィルタ パラメータ、出力、およびデフォルトのソート動作が指定されます。既存のレポートを変更したり、既存のレポートをコピーして新しいレポートのテンプレートとして使用したりできます。

これを実行するには、次のステップを実行します。

-
- ステップ 1** `./prime.sh stopall` コマンドを使用して Prime Provisioning サーバを停止します。
Prime Provisioning の開始および停止の詳細については、『[Cisco Prime Provisioning Administrator's Guide 6.3](#)』を参照してください。
- ステップ 2** 適切な編集ツールを使用して、
`$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/<folder_name>_report.xml` (ここで、`<folder_name>` は `Inventory`、`L2` または `MPLS`) コンフィギュレーション ファイルを開きます。
-  **(注)** ファイルを変更する前に保存してください。
-
- ステップ 3** 必要に応じて、既存のレポートを変更するか、レポートをコピーして新しいレポートの基礎として使用します。
- ステップ 4** 変更した `$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/<folder_name>_report.xml` ファイルを保存します。
- ステップ 5** `./prime.sh startwd` コマンドを使用して、Prime Provisioning を再始動します。
Prime Provisioning の開始および停止の詳細については、『[Cisco Prime Provisioning Administrator's Guide 6.3](#)』を参照してください。
-

Prime Provisioning を再始動した後、
`$PRIMEP_HOME/resources/nbi/reports/PrimeProvisioning/<folder_name>_report.xml` ファイル
に行った変更に基づき、変更内容が反映されます。

L2 および VPLS のレポートの生成

Prime Provisioning のレポート GUI は、L2 や VPLS などの複数の Prime Provisioning モジュールで使用します。レポート GUI の使用、レポートの実行、レポートからの出力の使用、およびカスタマイズされたレポートの作成に関する全般的な説明については、「[レポート](#)」(P.10-29) を参照してください。この項の残りの部分では、Prime Provisioning で利用可能な L2 および VPLS のレポートについて説明します。

この項では、L2 および VPLS のレポートの生成について説明します。次の事項について説明します。

- 「[L2 および VPLS のレポートへのアクセス](#)」(P.10-34)
- 「[L2 および VPLS のレポート](#)」(P.10-35)
- 「[L2 および VPLS のカスタム レポートの作成](#)」(P.10-42)

L2 および VPLS のレポートへのアクセス

L2 および VPLS のレポートにアクセスするには、次の手順を実行します。

-
- ステップ 1** Prime Provisioning GUI のレポート フレームワークにアクセスするには、`[Inventory] > [Reports] > [Inventory Reports]` を選択します。
`[Reports]` ウィンドウが表示されます。
- ステップ 2** `[L2]` フォルダをクリックして使用可能な L2 および VPLS のレポートを表示します。

ステップ 3 レポートのアイコンをクリックすると、当該レポートの関連ウィンドウが表示されます。

各レポートの詳細については、「[L2 および VPLS のレポート](#)」(P.10-35) を参照してください。

L2 および VPLS のレポート

この項では、次の L2 および VPLS のレポートの詳細について説明します。

- 「[L2 エンドツーエンド配線レポート](#)」(P.10-35)
- 「[L2 PE サービス レポート](#)」(P.10-38)
- 「[L2 VPN サービス レポート](#)」(P.10-39)
- 「[VPLS 接続回線レポート](#)」(P.10-39)
- 「[VPLS PE サービス レポート](#)」(P.10-41)
- 「[VPLS VPN レポート](#)」(P.10-41)



(注)

L2 レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。独自のカスタム レポートを作成するベースとして、このレポートを使用できます。詳細については、「[L2 および VPLS のカスタム レポートの作成](#)」(P.10-42) を参照してください。

各レポートで提供される情報は次のとおりです。

- レポートの説明または目的。
- レポート ウィンドウの図。
- フィルタ値と説明のリスト。
- 出力値と説明のリスト。

L2 エンドツーエンド配線レポート

L2 エンドツーエンド配線とは、2 本の接続回線を含むポイントツーポイント接続を指します。L2 エンドツーエンド配線レポートは、L2 エンドツーエンド接続上で実行中のサービスを表示します。このレポートを使用すると、接続ごとのすべてのサービスと該当する接続回線の属性を表示できます。

L2 エンドツーエンド配線レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [EndToEndWire ID]：エンドツーエンド配線の ID 番号。
- [Customer Name]：カスタマーの名前。
- [VC ID]：仮想回線の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [Service Type]：サービスのタイプ。値は次のとおりです。
 - ATM
 - ATM_NO_CE
 - FRAME_RELAY

- FRAME_RELAY_NO_CE
- L2VPN_ERS
- L2VPN_ERS_NO_CE
- L2VPN_EWS
- L2VPN_EWS_NO_CE
- [SR State] : サービス要求の状態。値は次のとおりです。
 - BROKEN
 - DEPLOYED
 - FAILED_AUDIT
 - FAILED_DEPLOY
 - FUNCTIONAL
 - INVALID
 - LOST
 - PENDING
 - REQUESTED
 - WAIT_DEPLOY
- [AC1-ID] : 第 1 接続回線 (AC1) の ID 番号。
- [AC2-ID] : 第 2 接続回線 (AC2) の ID 番号。

出力値 :

- [EndToEndWire ID] : エンドツーエンド配線の ID 番号。
- [Customer Name] : カスタマーの名前。
- [VPN] : VPN の名前。
- [VC ID] : 仮想回線の ID 番号。
- [SR ID] : サービス要求の ID 番号。
- [SR Job ID] : サービス要求ジョブ ID 番号。
- [Service Type] : サービスのタイプ。
- [SR State] : サービス要求の状態。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [AC1-ID] : 第 1 接続回線 (AC1) の ID 番号。
- [AC1-UNI Device Interface] : 第 1 接続回線 (AC1) の UNI デバイス インターフェイス。
- [AC1-NPC] : 第 1 接続回線 (AC1) の名前付き物理回線。
- [AC2-VLAN ID/DLCI/VCD] : 第 1 接続回線 (AC1) の VLAN ID 番号、Data-Link Connection Identifier (DLCI; データリンク接続識別子) または Virtual Circuit Descriptor (VCD; 仮想回線記述子)。
- [AC1-VPI] : 第 1 接続回線 (AC1) の仮想パス ID。
- [AC1-VCI] : 第 1 接続回線 (AC1) の仮想チャンネル ID。

- [AC1-Interface Encap Type] : 第 1 接続回線 (AC1) で使用されるカプセル化のタイプ。
- [AC1-AccessDomain] : 第 1 接続回線 (AC1) のアクセス ドメイン名。
- [AC1-Customer Facing UNI] : 第 1 接続回線 (AC1) のカスタマー側の UNI ポート。
- [AC1-Loopback IP Address] : 第 1 接続回線 (AC1) のループバック アドレス。
- [AC1-STP Shutdown Threshold] : 第 1 接続回線 (AC1) のスパニングツリー プロトコルのシャットダウンしきい値 (パケット数/秒)。
- [AC1-VTP Shutdown Threshold] : 第 1 接続回線 (AC1) の VLAN トランク プロトコルのシャットダウンしきい値 (パケット数/秒)。
- [AC1-CDP Shutdown Threshold] : 第 1 接続回線 (AC1) の Cisco Discovery Protocol のシャットダウンしきい値 (パケット数/秒)。
- [AC1-STP Drop Threshold] : 第 1 接続回線 (AC1) のスパニングツリー プロトコルのドロップしきい値 (パケット数/秒)。
- [AC1-CDP Drop Threshold] : 第 1 接続回線 (AC1) の Cisco Discovery Protocol のドロップしきい値 (パケット数/秒)。
- [AC1-VTP Drop Threshold] : 第 1 接続回線 (AC1) の VLAN トランク プロトコルのドロップしきい値 (パケット数/秒)。
- [AC1-UNI Recovery Interval] : 第 1 接続回線 (AC1) の UNI ポートの回復間隔 (秒)。
- [AC1-UNI Speed] : 第 1 接続回線 (AC1) の UNI ポートの速度。
- [AC1-UNI Shutdown] : 第 1 接続回線 (AC1) の UNI ポートのシャットダウン ステータス。
- [AC1-UNI PortSecurity] : 第 1 接続回線 (AC1) の UNI ポートのセキュリティのステータス。
- [AC1-UNI Duplex] : 第 1 接続回線 (AC1) の UNI ポートのデュプレックス ステータス ([none]、[full]、[half] または [auto])。
- [AC1-Maximum MAC Address] : 第 1 接続回線 (AC1) の UNI ポートに許可される最大 MAC アドレス。
- [AC1-UNI Aging] : 第 1 接続回線 (AC1) の UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。
- [AC2-ID] : 第 2 接続回線 (AC2) の ID 番号。
- [AC2-UNI Device Interface] : 第 2 接続回線 (AC2) の UNI デバイス インターフェイス。
- [AC2-NPC] : 第 2 接続回線 (AC2) の名前付き物理回線。
- [AC2-VLAN ID/DLCI/VCD] : 第 2 接続回線 (AC2) の VLAN ID、DLCI または VCD。
- [AC2-VPI] : 第 1 接続回線 (AC2) の仮想パス ID。
- [AC2-VCI] : 第 1 接続回線 (AC2) の仮想チャネル ID。
- [AC2-Interface Encap Type] : 第 2 接続回線 (AC2) で使用されるカプセル化のタイプ。
- [AC2-AccessDomain] : 第 2 接続回線 (AC2) のアクセス ドメイン名。
- [AC2-Customer Facing UNI] : 第 2 接続回線 (AC2) のカスタマー側の UNI ポート。
- [AC2-Loopback IP Address] : 第 2 接続回線 (AC2) のループバック アドレス。
- [AC2-STP Shutdown Threshold] : 第 2 接続回線 (AC2) のスパニングツリー プロトコルのシャットダウンしきい値。
- [AC2-VTP Shutdown Threshold] : 第 2 接続回線 (AC2) の VLAN トランク プロトコルのシャットダウンしきい値。

- [AC2-CDP Shutdown Threshold] : 第 2 接続回線 (AC2) の Cisco Discovery Protocol のシャットダウンしきい値。
- [AC2-STP Drop Threshold] : 第 2 接続回線 (AC2) のスパニングツリー プロトコルのドロップしきい値。
- [AC2-CDP Drop Threshold] : 第 2 接続回線 (AC2) の Cisco Discovery Protocol のドロップしきい値。
- [AC2-VTP Drop Threshold] : 第 2 接続回線 (AC2) の VLAN トランク プロトコルのドロップしきい値。
- [AC2-UNI Recovery Interval] : 第 2 接続回線 (AC2) の UNI ポートの回復間隔。
- [AC2-UNI Speed] : 第 2 接続回線 (AC2) の UNI ポートの速度。
- [AC2-UNI Shutdown] : 第 2 接続回線 (AC2) の UNI ポートのシャットダウン ステータス。
- [AC2-UNI PortSecurity] : 第 2 接続回線 (AC2) の UNI ポートのセキュリティのステータス。
- [AC2-UNI Duplex] : 第 2 接続回線 (AC2) の UNI ポートのデュプレックス ステータス ([none]、[full]、[half] または [auto])。
- [AC2-Maximum MAC Address] : 第 2 接続回線 (AC2) の UNI ポートに許可される最大 MAC アドレス。
- [AC2-UNI Aging] : 第 2 接続回線 (AC2) の UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。

L2 PE サービス レポート

L2 PE サービス レポートを使用すると、PE を選択したり、PE のロール (たとえば、[N-PE]、[U-PE] または [PE-AGG]) やその場所で実行中の L2 関連のサービスを表示したりできます。

L2 PE サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値 :

- [PE Role] : PE デバイスのロール (N-PE、U-PE、または PE-AGG)。
- [PE Name] : PE デバイス名。

出力値 :

- [PE Role] : PE デバイスのロール (N-PE、U-PE、または PE-AGG)。
- [PE Name] : PE デバイス名。
- [SR ID] : サービス要求の ID 番号。
- [SR Job ID] : サービス要求ジョブ ID 番号。
- [SR State] : サービス要求の状態。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [Service Type] : サービスのタイプ。

L2 VPN サービス レポート

L2 VPN レポートを利用すると、VPN を遡って VLAN ID または VC ID あるいはその両方を追跡できるため、カスタマーはすべてのリンクやすべての VPN サービスを繰り返したる必要がなくなります。VLAN ID または VC ID を指定すると、該当するカスタマーおよび VPN の詳細がレポートに表示されます。

L2 VPN レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [VLAN ID]：VLAN ID 番号。
- [VC ID]：仮想回線の ID 番号。
- [Customer Name]：カスタマーの名前。
- [Access Domain]：アクセス ドメイン名。

出力値：

- [VLAN ID]：VLAN ID 番号。
- [VC ID]：仮想回線の ID 番号。
- [SR Job ID]：サービス要求ジョブの ID 番号。
- [VPN]：VPN の名前。
- [Customer Name]：カスタマーの名前。
- [Service Type]：サービスのタイプ。
- [Access Domain]：アクセス ドメイン名。
- [Provider Name]：プロバイダー名。

VPLS 接続回線レポート

VPLS 接続回線レポートは、指定されたカスタマーの VPN の接続回線の詳細情報を表示します。

VPLS 接続回線レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値：

- [SR ID]：サービス要求の ID 番号。
- [SR Job ID]：サービス要求ジョブ ID 番号。
- [SR State]：サービス要求の状態。値は次のとおりです。
 - BROKEN
 - DEPLOYED
 - FAILED_AUDIT
 - FAILED_DEPLOY
 - FUNCTIONAL
 - INVALID
 - LOST
 - PENDING
 - REQUESTED
 - WAIT_DEPLOY

- [Customer Name] : カスタマーの名前。
- [VPN] : VPN の名前。
- [Service Type] : サービスのタイプ。値は次のとおりです。
 - VPLS_ERS
 - VPLS_ERS_NO_CE
 - VPLS_EWS
 - VPLS_EWS_NO_CE
- [VLAN ID] : VLAN ID 番号。
- [AccessDomain] : アクセス ドメイン名。

出力値 :

- [VPLS Link ID] : VPLS リンクの ID 番号。
- [SR ID] : サービス要求の ID 番号。
- [SR Job ID] : サービス要求ジョブ ID 番号。
- [SR State] : サービス要求の状態。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [Customer Name] : カスタマーの名前。
- [VPN] : VPN の名前。
- [Service Type] : サービスのタイプ。
- [VLAN ID] : VLAN ID 番号。
- [Policy Name] : VPLS ポリシー名。
- [VFI Interface] : 仮想転送インターフェイス名。
- [Customer Facing UNI] : カスタマー側の UNI ポート。
- [AccessDomain] : アクセス ドメイン名。
- [NPC] : 名前付き物理回線。
- [UNI Port] : UNI ポート。
- [UNI Shutdown] : UNI ポートのシャットダウン ステータス。
- [UNI Aging] : UNI ポートのセキュリティ テーブルに MAC アドレスが存在できる秒単位の時間長。
- [UNI Speed] : UNI ポートの速度。
- [UNI Duplex] : UNI ポートのデュプレックス ステータス ([none]、[full]、[half] または [auto])。
- [Maximum MAC Address] : UNI ポートで許可される最大 MAC アドレス。
- [CDP Shutdown Threshold] : UNI ポートの Cisco Discovery Protocol のシャットダウンしきい値 (パケット数/秒)。
- [STP Shutdown Threshold] : UNI ポートのスパニングツリー プロトコルのシャットダウンしきい値 (パケット数/秒)。

- [VTP Shutdown Threshold]: UNI ポートの VLAN トランク プロトコルのシャットダウンしきい値 (パケット数/秒)。
- [CDP Drop Threshold]: UNI ポートの Cisco Discovery Protocol のドロップしきい値 (パケット数/秒)。
- [VTP Drop Threshold]: UNI ポートの VLAN トランク プロトコルのドロップしきい値 (パケット数/秒)。
- [STP Drop Threshold]: UNI ポートのスパンニングツリー プロトコルのドロップしきい値 (パケット数/秒)。
- [Recovery Interval]: UNI ポートの回復間隔 (秒)。

VPLS PE サービス レポート

VPLS PE サービス レポートを使用すると、PE を選択したり、PE のロール (たとえば、[N-PE]、[U-PE] または [PE-AGG]) やその場所で実行中の VPLS サービスを表示したりできます。

VPLS PE サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値:

- [PE Role]: PE デバイスのロール (N-PE、U-PE、または PE-AGG)。
- [PE Name]: PE デバイス名。

出力値:

- [PE Role]: PE デバイスのロール (N-PE、U-PE、または PE-AGG)。
- [PE Name]: PE デバイス名。
- [SR ID]: サービス要求の ID 番号。
- [SR Job ID]: サービス要求ジョブ ID 番号。
- [Service Type]: サービスのタイプ。
- [SR State]: サービス要求の状態。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

VPLS VPN レポート

VPLS VPN レポートを利用すると、VPN を遡って VLAN ID または VFI 名あるいはその両方を追跡できるため、カスタマーはすべてのリンクやすべての VPN サービスを繰り返したどる必要がなくなります。VLAN ID または VFI 名を指定すると、該当するカスタマーおよび VPN の詳細がレポートに表示されます。

VPLS VPN レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます。

フィルタ値:

- [VLAN ID]: VLAN ID 番号。
- [Customer Name]: カスタマーの名前。
- [VFI Name]: 仮想転送インターフェイス名。
- [Access Domain]: アクセス ドメイン名。

出力値:

- [VLAN ID] : VLAN ID 番号。
- [SR Job ID] : サービス要求ジョブ ID 番号。
- [VPN] : VPN の名前。
- [Customer Name] : カスタマーの名前。
- [Service Type] : サービスのタイプ。
- [VFI Name] : 仮想転送インターフェイス名。
- [Access Domain] : アクセス ドメイン名。
- [Provider Name] : プロバイダー名。

L2 および VPLS のカスタム レポートの作成

L2 フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーション ファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

`$ISC_HOME/resources/nbi/reports/ISC/l2_report.xml`

レポート コンフィギュレーション ファイルを変更して、カスタム レポートを作成する方法の詳細については、「レポート」(P.10-29) を参照してください。

MPLS レポートの生成

Prime Provisioning のレポート GUI は、MPLS などの複数の Prime Provisioning モジュールで使用します。この章の残りの部分では、ISC で使用可能な MPLS レポートについて説明します。

この項では、MPLS のレポートの生成について説明します。次の事項について説明します。

- 「レポートへのアクセス」(P.10-30)
- 「レポートの実行」(P.10-31)
- 「MPLS PE サービス レポート」(P.10-43)
- 「MPLS サービス要求レポート」(P.10-44)
- 「MPLS サービス要求のレポート : 6VPE」(P.10-45)
- 「6VPE サポート対象デバイスのレポート」(P.10-46)
- 「カスタム レポートの作成」(P.10-33)

MPLS レポートへのアクセス

MPLS レポートにアクセスするには、次の手順を実行します。


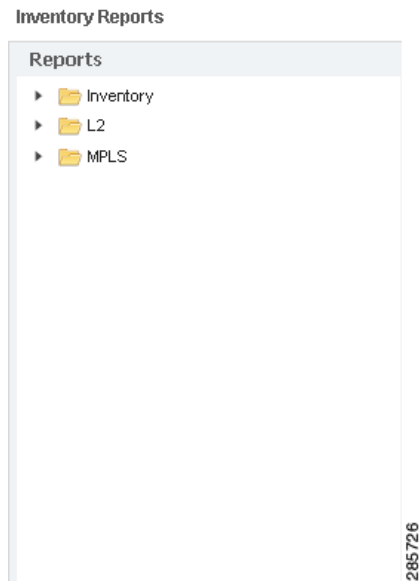
-
- ステップ 1** Prime Provisioning にログインします。
 - ステップ 2** [Inventory] > [Reports] > [Inventory Reports] に移動します。
 - ステップ 3** [MPLS] フォルダをクリックして使用可能な MPLS のレポートを表示します。


図 10-15 レポート リスト



ステップ 4 左側のナビゲーション ツリーの **MPLS** の下にリストされているレポートから、目的のレポートをクリックすると、そのレポートに関連付けられたウィンドウが開きます。



(注)

MPLS レポートのフォルダには、複数のサンプル レポートが用意されています。サンプル レポートのタイトルは、**SAMPLE-** で始まります。このレポートは情報提供だけを目的としています。テスト済みではなく、サポートもされません。ユーザは独自のカスタム レポートを作成するベースとしてこのレポートをサポートされているレポートとともに使用できます。カスタム レポートの詳細については、「[カスタム レポートの作成](#)」(P.10-47) を参照してください。

レポートの実行

レポートを実行するには、レポート ウィンドウの右下隅の **[View]** をクリックします。これにより、レポート出力が生成されます。MPLS サービス要求レポート出力の例。

ISC の現在のリリースでは、レポート GUI が表形式での出力をサポートしています。出力はレポート ウィンドウで選択した出力から取得された列でリストされます。

各行（またはレコード）は、レポート ウィンドウのフィルタ フィールドを使用して設定した検索基準との一致を示します。

三角形アイコンの付いたカラム見出しは、レコードのソート基準になる出力です。カラムの見出しをクリックすることにより、ソートの昇順と降順を切り替えることができます。別の出力値でソートするには、その値のヘッダーをクリックします。

MPLS PE サービス レポート

MPLS PE サービス レポートを使用すると、PE を選択したり、PE のロール（たとえば、[N-PE]、[U-PE] または [PE-AGG]）やその場所で実行中の MPLS 関連のサービスを表示したりできます。

MPLS サービス レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます (図 10-16 を参照)。

図 10-16 MPLS PE サービス レポート

フィルタ値

- [PE Role] : PE デバイスのロール (N-PE、U-PE、または PE-AGG)。
- [PE Name] : PE デバイス名。

出力値

- [PE Role] : PE デバイス ロール (N-PE、U-PE または PE-AGG) 別にリストされます。
- [PE Name] : PE デバイス名ごとにリストします。
- [Policy Type] : ポリシーのタイプごとにリストします。
- [SR State] : サービス要求状態別にリストされます (「サービス要求状態」(P.8-13) を参照)。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [SR ID] : サービス要求 ID ごとにリストします。
- [SR Job ID] : サービス要求ジョブ ID ごとにリストします。

MPLS サービス要求レポート

MPLS サービス要求のレポート機能を使用して、[PE]、[CE]、[VPN]、[SR ID]、[SR STATE] に関連するサービス要求をリストできます。

MPLS サービス要求レポートのアイコンをクリックすると、このレポートのウィンドウが表示されます (図 10-17 を参照)。

図 10-17 MPLS サービス要求レポート

Layout	
Title:	MPLS SR Report (PE,CE,VPN,SR ID,SR STATE)
Chart Type:	Tabular
Filters (All field values are required, * or a valid value.)	
PE_ROUTER:	* <input type="text"/> <input type="button" value="Select"/>
CE_ROUTER:	* <input type="text"/> <input type="button" value="Select"/>
Job_ID:	* <input type="text"/>
SR_STATE:	* <input type="text"/>
VPN_ID:	* <input type="text"/> <input type="button" value="Select"/>
Output Fields	
<div style="border: 1px solid blue; background-color: #0056b3; color: white; padding: 5px;"> PE_ROUTER CE_ROUTER Job_ID SR_STATE VPN_ID CREATION_DATE_TIME </div>	
Sorting	
N/A	

285729

フィルタ値

- [PE ROUTER] : 一部またはすべて (*) の PE ルータを選択します。
- [CE ROUTER] : 一部またはすべて (*) の CE ルータを選択します。
- [Job ID] : サービス要求のジョブ ID。
- [SR STATE] : サービス要求のステータス (「サービス要求状態」(P.8-13) を参照)。
- [VPN ID] : 一部またはすべて (*) の VPN を ID によって選択します。

出力フィルタ

- [PE ROUTER] : PE ルータを示します。
- [CE ROUTER] : CE ルータを示します。
- [Job ID] : ジョブ ID ごとにリストします。
- [SR STATE] : サービス要求のステータス (「サービス要求状態」(P.8-13) を参照)。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [VPN ID] : VPN ID ごとにリストします。
- [CREATION DATE TIME] : レポートが作成された日付および時間ごとにリストします。

MPLS サービス要求のレポート : 6VPE

MPLS サービス要求のレポート : 6VPE レポート機能を使用して、[PE]、[CE]、[VPN]、[SR ID]、[SR STATE] に関連するサービス要求をリストできます。

[MPLS Service Request Report - 6VPE] のアイコンをクリックすると、このレポートのウィンドウが表示されます (図 10-18 を参照)。

図 10-18 MPLS サービス要求のレポート : 6VPE

フィルタ値

- [Job ID] : サービス要求のジョブ ID。
- [SR STATE] : サービス要求のステータス（「サービス要求状態」(P.8-13) を参照）。
- [VPN ID] : 一部またはすべて (*) の VPN を ID によって選択します。
- [PE ROUTER] : 一部またはすべて (*) の PE ルータを選択します。
- [CE ROUTER] : 一部またはすべて (*) の CE ルータを選択します。

出力フィルタ

- [Job ID] : ジョブ ID ごとにリストします。
- [SR STATE] : サービス要求のステータス（「サービス要求状態」(P.8-13) を参照）。



(注) [SR State] 出力は、[CLOSED] 状態のサービス要求をリストしません。他の状態のサービス要求は、フィルタ値で決められたとおりにリストされます。

- [VPN ID] : VPN ID ごとにリストします。
- [PE ROUTER] : PE ルータを示します。
- [CE ROUTER] : CE ルータを示します。
- [CREATION DATE TIME] : レポートが作成された日付および時間ごとにリストします。

6VPE サポート対象デバイスのレポート



(注) Prime Provisioning GUI では、このレポートは [Inventory] > [Reports] > [Inventory Reports] の下にあります。

[6VPE Supported Devices Report] アイコンをクリックすると、このレポートのウィンドウが表示されます（図 10-19 を参照）。

図 10-19 6VPE サポート対象デバイスのレポート

フィルタ値

- [Host Name] : ホスト名。
- [Management Address] : 管理アドレス。
- [Software Version] : ソフトウェアのバージョン。

出力フィルタ

- [Host Name] : ホスト名。
- [Management Address] : 管理アドレス。
- [Software Version] : ソフトウェアのバージョン。

カスタム レポートの作成

MPLS フォルダの Prime Provisioning GUI にリストされるレポートは、基本のコンフィギュレーションファイルから派生します。このファイルは、XML 形式です。ファイルには次の場所からアクセスできます。

```
$ISC_HOME/resources/nbi/reports/ISC/mpls_report.xml
```

TEM レポートおよびログの生成

すべての展開および収集タスクはモニタされ、タスクの詳細が記録されます。この情報は、タスク モニタリング ページを使用して表示できます。

この項では、次の内容について説明します。

- 「TE タスク ログ」 (P.10-47)
 - 「SR 展開ログ」 (P.10-48)
 - 「タスク マネージャから作成されるログ」 (P.10-48)
 - 「タスク ログの表示」 (P.10-48)
- 「TE パフォーマンス レポート」 (P.10-49)。

TE タスク ログ

TE タスク ログは、1 つ以上の TE タスクを実行した結果を表示するときに使用されます。イベントにより、異なるタスク ログが生成されます。

- SR 展開ログ

- 次のような、タスク マネージャから発行されるタスクにより生成されるログ
 - TE ディスカバリ
 - TE 機能監査
 - TE インターフェイス パフォーマンス

SR 展開ログ

サービス要求が展開されると、管理対象または対象外のプライマリ トンネルまたはバックアップ トンネルに関係なく、ログが生成されます。トンネル SR では、展開は、SR のタイプに応じて、複数の段階で発生します。また、同様に、タスク ログが作成されます。

- プライマリ トンネル SR : 3 段階の展開に対応する 3 段階のロギング プロセス
- 保護 SR : 2 段階の展開に対応する 2 段階のロギング プロセス

展開ログのほか、展開が成功した場合、SR 展開のタイプに関係なく、ConfigAudit ログが作成されます。

タスク マネージャから作成されるログ

TE ディスカバリ タスクのタスク ログを生成および表示する手順については、「[タスク ログ](#)」(P.10-29) を参照してください。

TE 機能監査および TE インターフェイス パフォーマンス タスクのタスク ログを生成および表示する手順については、「[TE タスクの作成](#)」(P.7-76) を参照してください。

タスク ログの表示

タスク ログは、異なる 2 つの場所からアクセスできます。

- [Tasks] ウィンドウ
- [Service Requests] ウィンドウ

[Tasks] ウィンドウから

TE タスクのタスク ログを表示するには、次のことを実行する必要があります。

1. [Task Logs] ウィンドウにアクセスします。
2. 必要なログを選択して開きます。

タスク ログを表示するには、次のステップを実行します。管理対象のプライマリ トンネルの展開のタスク ログを例として使用します。

ステップ 1 [Operate] > [Task Logs] を選択します。

[Task Logs] ウィンドウが表示されます。

[Task Logs] ウィンドウに次の情報が示されます。

- [Runtime Task Name] : 実行時タスクがいつ作成されたかを指定する、属性が自動的に指定されたタスク名。
- [Action] : タスクのタイプ。たとえば、[TE Discovery]、[TE Functional Audit]、または [TE Interface Performance]。
- [Start Time] : 実行時タスクが開始したときの日付および時刻。
- [End Time] : 実行時タスクが終了した日時。

- [Status] : 実行時タスクの事前設定ステータスを示します。

ステップ 2 表示するタスク ログを選択します。

複数の実行がスケジュールされているタスクには、表示するインスタンスが複数ある場合があります。

ステップ 3 [Action] カラムで目的のタスクをクリックします。

対応する [Task Log] ウィンドウが表示されます。このウィンドウの GUI 要素は、[Service Request Manager] ウィンドウにもあります。

記録されたメッセージがテーブルに表示されます。これには、ログメッセージが作成された時刻、およびログメッセージに割り当てられた重大度が含まれます。

ロギングのフィルタ設定（デフォルトは [SEVERE]）があります。デフォルトの場合、[SEVERE] のログメッセージだけが表示されます。目的の詳細レベルに応じて選択できるいくつかの異なるフィルタ設定があります。フィルタ レベルを変更するには、必要なフィルタ レベルを選択し、[Filter] をクリックします。

ログの構造は、実行されたタスクのタイプにより異なります。

ステップ 4 [Return to Logs] をクリックして、ログ ウィンドウを閉じます。

これにより、メインの [Task Logs] ウィンドウに戻ります。

ステップ 5 タスク SR（特定のタスク ログに関連付けられている場合があります）を参照するには、目的のタスク ログを選択して、[Service Requests] ボタンをクリックします。

[Task SRs] ウィンドウが表示されます。

[Service Requests] ウィンドウから

[Service Requests] ウィンドウからログにアクセスするには、次の手順を実行します。

ステップ 1 [Operate] > [Service Request Manager] を選択します。

ステップ 2 サービス要求（1 つだけ）を選択します。

ステップ 3 [Status] ボタンをクリックして、[Logs] を選択します。

ステップ 4 表示するログを選択して、[View Log] をクリックします。

[Task Log] ウィンドウが表示されます。

ステップ 5 ドロップダウン メニューからログ レベルを選択して、[Filter] をクリックします。

ログ レベルには、[All]、[Severe]、[Warning]、[Info]、[Config]、[Fine]、[Finer]、および [Finest] があります。

TE パフォーマンス レポート

TE パフォーマンス レポートは、TE インターフェイス パフォーマンス タスクを実行するときに作成されます（「[TE インターフェイス パフォーマンス タスクの作成](#)」(P.7-78) を参照）。

このレポートには、選択されたトンネルまたはリンクあるいはその両方の TE インターフェイス パフォーマンス タスクから収集されたトラフィック データが表示されます。TE インターフェイス パフォーマンス タスクは、複数回実行できます。

TE パフォーマンス レポートを表示するには、次のステップを実行します。

ステップ 1 [Inventory] > [Reports] > [Inventory Reports] を選択します。

[TE Performance Report Table] が表示されます。

[TE Performance Report Table] ウィンドウには、次の GUI 要素があります。

- [Report table] : インターフェイス パフォーマンス タスクのリストを示します。
 - [Start Time] : 実行時タスクが開始したときの日付および時刻。
 - [End Time] : 実行時タスクが終了した日時。
 - [Device Name] : デバイスの名前。
 - [Interface Name] : リンク上のインターフェイスの IP アドレス。
 - [Octets In] : トラフィックの着信オクテットの数。
 - [Octets Out] : トラフィックの発信オクテットの数。
 - [Speed] : インターフェイスの速度。
 - [Util In] : 着信トラフィックのインターフェイスの使用率。
 - [Util Out] : 発信トラフィックのインターフェイスの使用率。
- [Reconcile Data] : インターフェイス パフォーマンス タスクがインターフェイスで複数回実行された場合は、次の基準に従ってデータを調整するように選択できます。
 - [Peak] : 最高のインターフェイス使用率を選択します。
 - [Valley] : 最低のインターフェイス使用率を選択します。
 - [Average] : 平均のインターフェイス使用率を選択します。
 - [First] : インターフェイス使用率の最初のオカレンスを選択します。