CHAPTER 11

トラブルシューティング ツールについて

この章では、次の内容について説明します。

ネットワーク デバイスとエンドホストのトラブルシューティング

LMS のトラブルシューティング ワークフローは、ネットワークから情報を収集し、ネットワーク管理に関する問題解決を支援します。

このワークフローを使用すると、デバイス、エンドホスト、およびリンクの詳細を表示し、ネットワークの接続に関する問題のトラブルシューティングやデバイスの診断を行うことができます。

次の中から選択できます。

- Device Center：[Device Troubleshooting] ページでデバイスの詳細を表示できます。

または

- End Host Center：[Endhost Troubleshooting] ページでエンドホストの詳細を表示できます。

詳細については、次のトピックを参照してください。

- トラブルシューティングの手順
- トラブルシューティングの詳細
- Device Troubleshooting
- Link Troubleshooting
- Endhost Troubleshooting

トラブルシューティングの手順

ネットワークの問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　メニューから次のいずれかのパスを選択し、ワークフローを起動します。

- **[Monitor] > [Troubleshooting Tools] > [Troubleshooting Workflows]**

または

- **[Inventory] > [Tools] > [Device Center]**

トラブルシューティング ワークフローが表示されます。

デバイスの [Global Search Results] ページでデバイスの IP アドレスまたはホスト名の上にマウスを移動してトラブルシューティング ワークフローを起動できます。

ステップ 2　[Device Center] または [End Host Center] を選択します。

ステップ 3　次の手順を実行します。

- Endhost Center の使用方法の手順を実行して、エンドホストの診断を行います。
- Device Center の使用の手順を実行して、デバイスの診断を行います。

Endhost Center の使用方法

[Endhost Center] を選択した場合、最後に接続したスイッチの詳細を取得するため、エンドホストの詳細を入力します。次の手順を実行します。

ステップ 1　[Attribute] ドロップダウン リストから検索パラメータを選択します。

属性は次のとおりです。

- IP Address
- MAC Address

  サポートされる MAC アドレスの形式は次のとおりです。
  - *xx-xx-xx-xx-xx-xx*
  - *xxxx-xxxx-xxxx*
  - *xxxxxxxxxxxx*
  - *xx:xx:xx:xx:xx:xx*
  - *xxxx:xxxx:xxxx*
  - *xx.xx.xx.xx.xx.xx*
  - *xxxx.xxxx.xxxx*
- Username
- Hostname
- IP Phone Number

属性を選択すると、対応するフィールドが画面に表示されます。

たとえば、[MAC Address] を選択した場合、ラベル名が [MAC Address] のフィールドが表示されます。

ステップ 2　[Attribute] ドロップダウン リストの横にあるフィールドに値を入力します。

たとえば、[MAC Address] を選択した場合、値フィールドにスイッチの MAC アドレスを入力します。

ステップ 3　[Find Last Connected Switch] をクリックします。

最後に接続したスイッチの詳細が表示されます。

ステップ 4　[View] をクリックします。

ステップ 5　別のデバイスのトラブルシューティングを行うには、次の手順を実行します。

a.　スイッチ アイコンをクリックし、目的のスイッチを選択します。

b.　スイッチの目的のポートを選択します。

c.　[View] をクリックします。

選択したデバイスの詳細が、右ペインの [End Host] タブに表示されます。詳細については、Endhost Troubleshooting を参照してください。

Device Center の使用

Device Center では、デバイスを選択し、[Device Troubleshooting] ページでデバイスの詳細を表示できます。選択したデバイスのレポートの表示、選択したデバイスに対するさまざまなツールの実行、選択したデバイスで実行できるタスクの実行が可能です。

Device Center を選択した場合は、デバイスの詳細を入力します。次の手順を実行します。

ステップ 1　デバイス セレクタ アイコンをクリックし、目的のスイッチを選択します。

（注）　デバイス セレクタに 2000 を超えるノードがあると、ノードの展開に時間がかかります。ノードの展開中にロード中画像がすぐに表示されず、ブラウザによってスクリプト停止エラーがスローされる場合があります。ノードのロード中のスクリプト停止エラーは無視でき、[No] オプションを選択してロードを続行します。

ステップ 2　[View] をクリックします。

選択したデバイスの詳細が、右ペインのタブに表示されます。詳細については、Device Troubleshooting を参照してください。

トラブルシューティングの詳細

デバイス、リンク、またはエンドホストのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

マウスクリックで、各ペインの展開または折りたたみオプションが提供されます。各ペインには複数のポートレットがあり、デバイス、エンドホスト、またはリンクに関する情報が表示されます。

ほとんどのポートレットには更新アイコンがあります。このアイコンを使用してポートレットを更新し、ポートレットの内容の最新の詳細を取得できます。

詳細については、次のトピックを参照してください。

- Device Troubleshooting
- Link Troubleshooting
- Endhost Troubleshooting

[View Topology] ボタンを使用してネットワークのトポロジを表示できます。詳細については、ネットワークのトポロジの表示を参照してください。

ネットワークのトポロジの表示

[Device Troubleshooting] ページと [Endhost Troubleshooting] ページには、[View Topology] ボタンがあります。このオプションを使用して、デバイスのネットワーク トポロジを表示できます。

トポロジ ビューを起動するために使用されるデフォルト ホップ カウントは 1 です。

ホップ カウントを変更し、[Refresh] アイコンをクリックして、指定したホップ数のトポロジ ビューを起動できます。入力できる最大ホップ数は 3 です。

トポロジで次のネットワーク要素をクリックし、ネットワークの問題の詳細を表示してトラブルシューティングできます。

- デバイス：詳細については、Device Troubleshooting を参照してください。
- リンク：詳細については、Link Troubleshooting を参照してください。
- エンドホスト：詳細については、Endhost Troubleshooting を参照してください。

ネットワーク要素をクリックすると、マウスホバー ポップアップ ウィンドウに詳細が表示されます。

Device Troubleshooting

Device Troubleshooting では次のペインが表示されます。

- [Device Status]：詳細については、Device Status の詳細を参照してください。
- [Configuration Status]：詳細については、Configuration Status の詳細を参照してください。
- [Reachability Status]：詳細については、Reachability Details を参照してください。
- [Events and Faults]：詳細については、Events and Faults の詳細を参照してください。
- [Port Status]：詳細については、Port Status の詳細を参照してください。
- [Performance Details]：詳細については、Performance Details を参照してください。

Device Status の詳細

[Device Status] ペインには次のポートレットが表示されます。

- Device Information
- Reachability Status
- Latest Configuration Change
- Collector Status
- Technology Details

[Device Status] ペインには、選択したデバイスのレポートの表示、選択したデバイスに対するさまざまなツールの実行、選択したデバイスで実行できるタスクを実行するためのオプションが用意されています。

詳細については、[Device Status] ペインのツール、タスク、レポートへのクイック リンクを参照してください。

Device Information

このポートレットには、Device and Credential Repository（DCR）に格納されているデバイス情報が含まれています。

表 11-1 に、Device Information ポートレットの説明を示します。

表 11-1　Device Information ポートレットのフィールド

フィールド名	説明
Device Name	Device and Credential Repository に入力されているデバイスの名前。
IP Address	デバイスの IP アドレス。
Device Type	デバイス タイプの情報。 たとえば、Cisco 2511 Access Server などです。
Hostname	Device and Credential Repository に入力されているデバイスのホスト名
Software Version	デバイスにインストールされている IOS のバージョン
Image	ソフトウェア イメージの詳細
Location	デバイスがあるエリア、階、または建物
Contact	デバイス管理者の電子メール アドレス

表 11-1　Device Information ポートレットのフィールド （続き）

フィールド名	説明
EOL	デバイス ハードウェアのサポート終了情報
EOS	デバイス ハードウェアの販売終了情報
Discrepancies	選択したデバイスに関連する不一致の数。 デバイス数のリンクをクリックすると、Discrepancies レポートが表示されます。
Best Practice Deviations	選択したデバイスに関連するベスト プラクティスからの逸脱の数。 デバイス数のリンクをクリックすると、Best Practice Deviations レポートが表示されます。
Device Availability (Last polled value)	最後のポーリング サイクル ステータスによるデバイスのアベイラビリティ ステータス。
CPU Utilization (24 hrs Average)	最近の 24 時間におけるデバイスの CPU 使用率の平均（パーセント単位で表示）
Memory Utilization (24 hrs Average)	最近の 24 時間におけるデバイスのメモリ使用率の平均（パーセント単位で表示）
Environmental Temperature (24 hrs Average)	最近の 24 時間におけるモニタ対象デバイスの環境温度の平均（パーセント単位で表示）
Administratively Up	管理上アップ状態のポートの数。 ポート数のリンクをクリックすると、Administratively Up Switch Port レポートが表示されます。
Administratively Down	管理上ダウン状態のポートの数 ポート数のリンクをクリックすると、Administratively Down Switch Port レポートが表示されます。
Operationally Up	動作上アップ状態のポートの数 ポート数のリンクをクリックすると、Operationally Up Switch Port レポートが表示されます。
Operationally Down	動作上ダウン状態のポートの数 ポート数のリンクをクリックすると、Operationally Down Switch Port レポートが表示されます。
Number of Faults	Critical、Warning、および Information 障害の数 Critical、Warning、または Information 障害の数のリンクをクリックすると、[Fault Monitor Fault View] タブに移動し、それぞれの障害の一覧が表示されます。
Last Booted on	デバイスを最後にブートまたはリブートした時刻。
Description	選択したデバイスを管理する LMS アプリケーションのリスト。 これらのアプリケーションは、ローカル LMS サーバか、マルチ サーバ セットアップにおけるリモート LMS サーバのいずれかのアプリケーションです。

Reachability Status

このポートレットには、[Test Now] ボタンをクリックしたときに、デバイス接続性情報が表示されます。

表 11-2 に、Reachability Check ポートレットのフィールドの説明を示します。各フィールドには、接続ステータスに応じて [Success] または [Failed] が表示されます。

表 11-2　Reachability Check ポートレットのフィールドReachability Status ポートレット

フィールド名	説明
ping	選択したデバイスの ping ステータス。 デバイスが到達可能かどうかを確認します。ping は、ICMP エコー メッセージとその応答をテストします。
HTTP	選択したデバイスの ping ステータス。 HTTP 要求を宛先デバイスの HTTP ポート 80 に送信します。
SNMPv1 Read	選択したデバイスの SNMPv1 read コミュニティ ストリング（サービス テスト、ポート 161）のステータス。 **SNMP 読み取り**テスト（SNMPR）を行うために、宛先デバイスに **snmp get** 要求を送信します。
SNMPv1 Write	選択したデバイスの SNMPv1 write コミュニティ ストリング（サービス テスト、ポート 161）のステータス。 **SNMP 書き込み**テスト（SNMPW）を行うために、デバイスに **snmp set** 要求を送信します。
SNMPv2c Read	選択したデバイスの SNMPv1 read コミュニティ ストリング（サービス テスト、ポート 161）のステータス。 **SNMP 読み取り**テスト（SNMPR）を行うために、宛先デバイスに **snmp get** 要求を送信します。
SNMPv2c Write	選択したデバイスの SNMPv1 write コミュニティ ストリング（サービス テスト、ポート 161）のステータス。 **SNMP 書き込み**テスト（SNMPW）を行うために、デバイスに **snmp set** 要求を送信します。
SSHv1	選択したデバイスの SSHv1 クレデンシャルのステータス（サービス テスト、ポート 22）。 SSH がデバイスでイネーブルになっているかどうかをチェックします。宛先デバイスが SSH 要求に応答する場合、LMS サーバがそのデバイスに SSH 要求を行うことができるかどうかもテストします。データベースのパスワードは確認しません。
SSHv2	選択したデバイスの SSHv2 クレデンシャルのステータス（サービス テスト、ポート 22）。 SSH がデバイスでイネーブルになっているかどうかをチェックします。宛先デバイスが SSH 要求に応答する場合、LMS サーバがそのデバイスに SSH 要求を行うことができるかどうかもテストします。データベースのパスワードは確認しません。
Telnet	選択したデバイスの Telnet ステータス（サービス テスト、ポート 23）。 デバイス上で Telnet がイネーブルになっているかどうかと、宛先デバイスが Telnet 要求に応答するかどうかをチェックします。データベース中の Telnet パスワードが正しいかどうかは確認しません。

Latest Configuration Change

このポートレットでは次の情報を表示できます。

- コンフィギュレーション アーカイブに実行コンフィギュレーションをアーカイブした時刻。
- コンフィギュレーション アーカイブ中にアーカイブされた 2 つの実行コンフィギュレーションの差異。

Collector Status

このポートレットは、デバイス上で実行された収集タスクのステータスの要約を表示します。

表 11-3 に、Collector Status ポートレットのフィールドの説明を示します。

表 11-3　Collector Status ポートレットのフィールド

フィールド名	説明
Collector Name	収集タスクの名前。 有効な値は次のとおりです。 • Data Collection • Inventory • Config Collection • User Tracking • Discovery • Fault Discovery
Status	ステータスを Success または Failed で表示します。
Collection Time	収集が完了した時刻。

Technology Details

このポートレットは、デバイスでイネーブルになっているテクノロジーの詳細を要約して表示します。

表 11-4 に、Technology Details ポートレットのフィールドの説明を示します。

表 11-4　Technology Details ポートレットのフィールド

フィールド名	説明
Technology Name	デバイスでイネーブルになっている Work Center テクノロジーの名前。有効な値は次のとおりです。 • EnergyWise • Identity • Smart Install • Auto Smart Ports • IPSLA • Responder
Status	テクノロジーのステータスを表示します。ステータスは、Enabled、Disabled、Software Incapable のいずれかになります。

[Device Status] ペインのツール、タスク、レポートへのクイック リンク

[Device Status] ペインには、さまざまな診断および接続ツール、レポート、タスクへのリンクがあります。

これらすべてのリンクは、メニュー [Tools]、[Tasks]、および [Reports] の下に分類されています。メニューの上にカーソルを移動するか、メニューをクリックすると、クイック リンクのリスト全体が表示されます。

[Tools]、[Tasks]、および [Reports] メニューの下のクイック リンクの一覧を表 11-5 に示します。

表 11-5　[Tools]、[Tasks]、[Reports] メニューの下のリンク

メニュー	クイック リンク	機能
Tools	Chassis View	選択したデバイスのシャーシ ビューを起動します。 詳細については『*Inventory Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Cluster Management Suite	選択したデバイスに対して Cluster Management Suite を起動します。 このリンクは、種類がクラスタ スイッチのデバイスを選択した場合のみ有効です。
	Edit Device Credentials	プライマリ クレデンシャル、セカンダリ クレデンシャル、Auto Update Server 管理クレデンシャル、RxBoot モード クレデンシャルなど、選択したデバイスのクレデンシャルを編集できます。 詳細については『*Inventory Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Edit Device Identity	デバイス名、クラスタ情報など、選択したデバイスの識別情報を編集できます。 詳細については『*Inventory Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Management Station to Device	非管理対象のデバイスまたは応答しないデバイスの問題をトラブルシューティングするために、プロトコルごとのデバイスの接続性を確認できます。 Management Station to Device ツールを使用すると、レイヤ 4（アプリケーション）の接続の問題点を診断することが可能です。 詳細については、ネットワーク デバイスとエンドホストのトラブルシューティングを参照してください。
	Mini-RMON	CiscoView Mini-RMON マネージャを起動できます。 詳細については『*Inventory Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Packet Capture	トラブルシューティングを支援するため、LMS マシンからの生データをキャプチャできます。
	Proxy ping	Proxy ping を使用すると、選択したデバイスから別のデバイスまたはサーバに ping を実行し、ping の出力を表示できます。 詳細については、Proxy ping を参照してください。
	Proxy Traceroute	Proxy Traceroute は、選択したデバイスからのデバイスまたはサーバの traceroute の出力を表示します。 詳細については、Proxy Traceroute を参照してください。
	SNMP Set	このオプションを使用すると、デバイスを制御するために、デバイス上の SNMP オブジェクトまたは複数のオブジェクトを設定できます。
	SNMP Walk	トラブルシューティングのために、デバイスの指定した OID から始まる MIB ツリーをトレースしたり、特定のデバイスに関する情報を収集できます。
	Telnet/SSH	Telnet または SSH を使用して指定したデバイスに接続できます。

表 11-5　[Tools]、[Tasks]、[Reports] メニューの下のリンク （続き）

メニュー	クイック リンク	機能
Tasks	Add Images to Software Repository	デバイスからソフトウェア リポジトリにソフトウェア イメージを追加できます。 詳細については『*Configuration Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Analyze using cisco.com Image	Cisco.com のクレデンシャルとプロキシ サーバのクレデンシャルを入力できます。 入力したこれらのクレデンシャルは、セッション全体を通じて使用されます。 詳細については『*Configuration Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Analyze using Repository Image	詳細については『*Configuration Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Check Device Credential	次の 1 つ以上のデバイス クレデンシャル オプションを確認できます。 • SNMP Read Community String • SNMP Write Community String • SNMPv3 • Telnet • Telnet Enable Mode User Name and Password • SSH • SSH Enable Mode User Name and Password
	Configure IPSLA Collector	[Collector Management] 画面で IPSLA コレクタを設定できます。
	Create Poller	[Poller Management] 画面でポーラーを作成できます。
	Distribute images	ネットワーク内でイメージを配布できます。また、配布前に新しいソフトウェア イメージの影響や前提条件を分析および特定することもできます。 詳細については『*Configuration Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Edit Config	Config Editor を使用してデバイス構成を編集できます。
	Open TAC Case	TAC への新しいサービス要求を作成したり、サービス要求のリストを照会できます
	Run Show Command	選択したデバイスに対して show コマンドを実行できます。
	Search Communities	[Cisco Search Communities] ページにアクセスし、デバイス タイプのキーワードに関連するシスコのフォーラムと投稿のリンクを一覧表示します
	Sync Archive	この機能を使用して、デバイスを実行コンフィギュレーションと手動で同期できます。
	Trigger User Tracking	User Tracking の取得を開始します。
	Update Inventory	デバイス インベントリを更新し、選択したデバイスのインベントリを収集するための即時ジョブを作成します。
	View Config	[Config Viewer] ウィンドウを使用してデバイス構成を表示できます。
	View Pending Jobs	Configuration Browser で保留中のジョブの一覧を表示できます。

表 11-5　[Tools]、[Tasks]、[Reports] メニューの下のリンク （続き）

メニュー	クイック リンク		機能
Reports	24 Hours Change Audit Report		デバイスの 24 Hours Change Audit レポートを生成できます。 このレポートには、Change Audit ログに格納されているデータから過去 24 時間以内に行われた変更を表示します。
	Call Home History		Smart Call Home レポートを起動できます。
	Credential Verification Report		選択したデバイスに対して Device Credential Verification レポートを起動できます。
	Detailed Device Report		選択したデバイスに対して Detailed Device レポートを起動できます。 詳細については『*Reports Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Device Attribute Report		Device Attributes レポートを生成できます。
	Device Dashboard		選択したデバイスに対して Device Dashboard の詳細を起動します。 詳細については『*Reports Management with Cisco Prime LAN Management Solution 4.2*』を参照してください。
	Fault History Report		最近の 31 日間のアラームとイベントに関する履歴情報を収集するための Device Fault History レポートを起動できます。
	Interface Errors Report		Interface Error レポートを表示できます。このレポートには、最近の 24 時間の間のデバイス インターフェイスのエラー率情報が表示されます。
	MAC Reports	Dormant MAC Report	Dormant MAC レポートを生成できます。このレポートには、指定した日数の間非アクティブである MAC アドレスの詳細が含まれています。
		New MAC Report	New MAC レポートを生成できます。このレポートには、新たにネットワークに追加された MAC アドレスの詳細が含まれています。
		Rogue MAC Report	Rogue MAC レポートを生成できます。このレポートには、ネットワークに存在することを許可されていない MAC アドレスの詳細が含まれています。
	Port Attributes Report		Port Attributes レポートを生成できます。

表 11-5　[Tools]、[Tasks]、[Reports] メニューの下のリンク （続き）

メニュー	クイック リンク		機能
Reports （続き）	Switch Port Reports	Recently Down Report	レポート ジェネレータから Recently Down Port レポートを生成できます。 Recently Down Port レポートには次の内容が表示されます。 • 前回のデータ収集でデバイスに接続されていたが、現在のデータ収集で未接続であることが判明したリンク ポート。 • 最後の UT メジャー獲得サイクルでエンドホストに接続されていたが、現在のデータ収集で未接続であることが判明したアクセス ポート。 ポートが次の UT メジャー獲得サイクルの実行でもまだ Unconnected 状態のままだった場合、Unused Up ポートまたは Unused Down ポートに分類されます。 これらのポートは、さらに Reclaim Unused Up Ports レポートまたは Reclaim Unused Down Ports レポートに移動されます。
		Reclaim Unused Down Report	レポート ジェネレータから Reclaim Unused Down Port レポートを生成できます。 リンク ポートとアクセス ポートを問い合わせ、Unused Down レポートを生成できます。これは次のポートを使用します。 • 管理上ダウン状態のポート。 および • 以前エンドホストまたはデバイスに接続されていたが、少なくとも 1 日間未接続であるポート。 指定した期間 Unused Down 状態であるポートについてのレポートを生成できます。
		Reclaim Unused Up Report	レポート ジェネレータから Reclaim Unused Up Port レポートを生成できます。 リンク ポートとアクセス ポートを問い合わせ、Unused Up レポートを生成できます。これは次のポートを使用します。 • 管理上アップ状態のポート。 および • 以前エンドホストまたはデバイスに接続されていたが、少なくとも 1 日間未接続であるポート。 指定した期間 Unused Up 状態であるポートについてのレポートを生成できます。

表 11-5　[Tools]、[Tasks]、[Reports] メニューの下のリンク （続き）

メニュー	クイック リンク		機能
Reports（続き）	Switch Port Reports（続き）	Switch Port Capacity Report	レポート ジェネレータから Switch Port Capacity レポートを生成できます。 Switch Port Capacity レポートには、使用率しきい値を超えたスイッチの一覧が、ポート使用率のパーセンテージの値とともに表示されます。このレポートを使用すると、ネットワークの拡張のためのキャパシティ プランニングが可能になります。
		Switch Port Summary Report	レポート ジェネレータから Switch Port Summary レポートを生成できます。 Switch Port Summary レポートには、各スイッチの Connected、Free、および Free Down 状態のポートの数が表示されます。 • 管理上アップ状態であるが、デバイスまたはエンドホストに接続されていないポートは Free ポートです。 • 管理上ダウン状態であり、デバイスまたはエンドホストに接続されていないポートは Free Down ポートです。 このレポートには、各スイッチの Connected、Free、および Free Down ポートの合計も表示されます。このレポートには、以前エンドホストに接続されていたかどうかにかかわらず、スイッチのすべての Down ポートの一覧が表示されます。 Connected、Free、および Free Down ポートの数はリンクになっています。リンクをクリックすることで、詳細なレポートが起動され、選択したデバイスのポート、ポート名、管理上および動作上のステータスが表示されます。
	Syslog Messages Report		Syslog Messages レポートを生成できます。 このレポートには、過去 24 時間の間にログに記録された syslog メッセージの数が重大度に基づいて表示されます。
	UT End Host Report		User Tracking End Host レポートを生成できます。
	VLAN Report		デバイス、スイッチ クラウド、または VTP ドメインの VLAN レポートを生成できます。

Configuration Status の詳細

[Configuration Status] ペインには次のポートレットが表示されます。

- Configuration Details
- Inventory Collection

Configuration Details

このポートレットには、デバイスのコンフィギュレーションの詳細が要約して表示されます。

表 11-6 に、Configuration Details ポートレットのフィールドの説明を示します。

表 11-6　Configuration Details ポートレットのフィールド

フィールド名	説明
IPSLA	デバイスで IPSLA がイネーブルになっている場合、true が表示されます。
Responder Enabled	デバイスでレスポンダがイネーブルになっている場合、true が表示されます。
Maximum Number of Collectors	使用可能なコレクタの最大数が表示されます。

表 11-6　Configuration Details ポートレットのフィールド （続き）

フィールド名	説明
Configured Collectors	すでに設定されているコレクタの数が表示されます。
Configurable Collectors	設定可能なコレクタの数が表示されます。
PSIRTs	デバイスに適用される PSIRT アナウンスの数が表示されます。ハイパーリンクになっている値をクリックすると、PSIRT レポートが表示されます。
Endhosts	デバイスに接続されているエンドホストの数が表示されます。
IP Phones	デバイスに接続されている IP Phone の数が表示されます。
VTP Domain	エンドホストが接続されているデバイスの VTP ドメイン名。
VTP Mode	エンドホストが接続されているデバイスの VTP モード。
VTP Version	VTP のバージョンが表示されます。
Number of VLANs	デバイスに関連付けられている VLAN の数が表示されます。ハイパーリンクになっている値をクリックすると、VLAN レポートが表示されます。

Inventory Collection

このポートレットでは次の詳細を表示できます。

- RAM サイズ（MB 単位）
- シャーシのシリアル番号
- パーティション
- モジュール数

Reachability Details

[Reachability Details] ペインには次のポートレットが表示されます。

- Device Availability
- ping device from LMS Server
- Traceroute device from LMS Server

Device Availability

Device Availability ポートレットを使用すると、ネットワーク内で管理されている選択したデバイスの、最近の 1 日または 1 時間のアベイラビリティ ステータスを表示できます。

最後にポーリングしたデバイスの次の情報が、ポートレットにグラフィック形式で表示されます。

- [Last Polled Status]：最後のポーリング サイクルにネットワーク内で使用可能だったデバイスのパーセンテージが表示されます。
- [Minimum (%)]：最後のポーリング サイクルにネットワーク内で使用可能だったデバイスの最小パーセンテージが表示されます。
- [Maximum (%)]：最後のポーリング サイクルにネットワーク内で使用可能だったデバイスの最大パーセンテージが表示されます。
- [Average (%)]：最後のポーリング サイクルにネットワーク内で使用可能だったデバイスの平均パーセンテージが表示されます。
- [Histograph]：アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます。
- [Livegraph]：アイコンが表示され、クリックすることでライブグラフ チャートが表示されます。

表 11-7 に、デバイスのアベイラビリティ ステータスの色とパーセンテージを示します。

表 11-7　デバイスのアベイラビリティ ステータスの色とパーセンテージ

色	パーセント単位でのデバイスのアベイラビリティ ステータス
グリーン	デバイスのアベイラビリティ ステータスは 90 ～ 100 %
イエロー	デバイスのアベイラビリティ ステータスは 50 ～ 90 %
オレンジ	デバイスのアベイラビリティ ステータスは 10 ～ 50 %
レッド	デバイスのアベイラビリティ ステータスは 0 ～ 10 %

ping device from LMS Server

このポートレットには、[Test Now] ボタンをクリックすると、LMS サーバからデバイスへの ping の出力または結果と、ping の統計情報が表示されます。

ping 統計情報には、送信パケット数、受信パケット数、パケット損失のパーセンテージが含まれています。

Traceroute device from LMS Server

このポートレットには、[Test Now] ボタンをクリックすると、LMS サーバからデバイスへの traceroute の出力と、traceroute の統計情報が表示されます。

Events and Faults の詳細

[Events and Faults] ペインには次のポートレットが表示されます。

- Faults
- Syslogs
- Change Audit

Faults

このポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 時間または 1 日の障害の詳細が要約して表示されます。

表 11-8 に、Fault Details ポートレットのフィールドの説明を示します。

表 11-8　Fault Details ポートレットのフィールド

フィールド名	説明
Severity	障害の重大度。Critical、Informational、Warning のいずれかになります。
Event ID	障害の ID。
Description	障害に関する説明
Status	障害のステータス。ユーザが所有しているかクリアされたか
Category	障害のカテゴリ。 このフィールドは次のいずれかの値になります。 • Application • Connectivity • Environment • Interface • Other • Reachability • System Hardware • Utilization
Duration	アクティブな障害または所有されている障害の場合、障害の発生から現在のサーバ時間までの期間。 障害の発生から障害のクリアまでの期間。
Last Occurrence	障害が発生した日付と時刻。

Syslogs

このポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 日または 1 時間の syslog の詳細が要約して表示されます。

表 11-9 に、Syslogs ポートレットの説明を示します。

表 11-9　Syslog Details ポートレットのフィールド

フィールド名	説明
Source	syslog メッセージを生成しているデバイスの名前。
Severity	メッセージの重大度。LMS でキャプチャされる重大度は、Emergencies（0）、Alerts（1）、Critical（2）、Errors（3）です。
Mnemonic	エラー メッセージを一意に識別するコード。以前の Catalyst メッセージにはニーモニックが表示されないことに注意してください。 IOS メッセージのニーモニックの例は、CONFIG I です。
Description	syslog メッセージの説明。

表 11-9　Syslog Details ポートレットのフィールド （続き）

フィールド名	説明
Timestamp	メッセージがロギングされた日付と時刻。これは、デバイスによって渡されたタイムスタンプです。 デバイスがタイムスタンプを渡さない場合、syslog デーモンがタイムスタンプを提供します。
Details	syslog メッセージの名前。 syslog メッセージの説明が表示された新しいウィンドウを開きます。User_URL アイコンをクリックすると、カスタマイズされた Web ページが定義されていればそれが表示されます。定義していない場合は、ユーザ URL を作成するためのサンプル Perl スクリプトがデフォルトで表示されます。 「*」をクリックすると、syslog メッセージの説明が表示されます

Change Audit

このポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 時間または 1 日の Change Audit の詳細が要約して表示されます。

表 11-10 に、Change Audit ポートレットのフィールドの説明を示します。

表 11-10　Change Audit Details ポートレットのフィールド

フィールド名	説明
User Name	自動化されたアクションを起動する必要があるユーザ名
Connection Mode	変更を行ったユーザの名前。ユーザがログインするときに入力した名前です
Message	ネットワーク変更の簡潔な要約。
Application Name	自動化されたアクションを起動する必要があるアプリケーション名。
Creation Time	自動化されたアクションを作成する時刻。

Port Status の詳細

[Port Status] ペインには次のポートレットが表示されます。

- Link Ports
- Access Ports
- Trunk Ports

これらのポートレットには、デフォルトで 100 件のレコードを表示できます。

Link Ports

このポートレットは、デバイスのリンク ポートのステータスの要約を表示します。更新アイコンを使用して、ポートレットの最新の内容を表示できます。

表 11-11 に、Link Ports ポートレットのフィールドの説明を示します。

表 11-11　Link Ports ポートレットのフィールド

フィールド名	説明
Port	リンク ポートの名前
Admin Status	ポートが意図的に停止されたかどうかを表示します
Operational Status	ポートがアクティブか非アクティブかを表示します
Port Description	ユーザが入力したポートの説明
Type	メディア タイプ。イーサネットなど
Speed	リンク ポートの速度
Duplex Mode	デュプレックス モード。半二重または全二重。
VLAN	VLAN の名前。
L2L3	ポートがレイヤ 2 とレイヤ 3 のいずれであるか、スイッチド ポートとルーテッド ポートのいずれであるかを示します。

Access Ports

このポートレットは、デバイスのアクセス ポートのステータスの要約を表示します。更新アイコンを使用して、ポートレットの最新の内容を表示できます。

表 11-12 に、Access Ports ポートレットのフィールドの説明を示します。

表 11-12　Access Ports ポートレットのフィールド

フィールド名	説明
Port	アクセス ポートの名前
Admin Status	ポートが意図的に停止されたかどうかを表示します
Operational Status	ポートがアクティブか非アクティブかを表示します
Port Description	ユーザが入力したポートの説明
Type	メディア タイプ。イーサネットなど
Speed	アクセス ポートの速度
Duplex Mode	デュプレックス モード。半二重または全二重

表 11-12　Access Ports ポートレットのフィールド （続き）

フィールド名	説明
VLAN	VLAN 名
L2L3	ポートがレイヤ 2 なのかレイヤ 3 なのか、スイッチド ポートなのかルーテッド ポートなのかを示します

Trunk Ports

このポートレットは、デバイスのトランク ポートのステータスの要約を表示します。更新アイコンを使用して、ポートレットの最新の内容を表示できます。

表 11-13 に、Trunk Ports ポートレットのフィールドの説明を示します。

表 11-13　Trunk Ports ポートレットのフィールド

フィールド名	説明
Port	トランク ポートの名前
Admin Status	ポートが意図的に停止されたかどうかを表示します
Operational Status	ポートがアクティブか非アクティブかを表示します
Port Description	ユーザが入力したポートの説明
Type	メディア タイプ。イーサネットなど
Speed	トランク ポートの速度
Duplex Mode	デュプレックス モード。半二重または全二重
VLAN	VLAN 名
L2L3	ポートがレイヤ 2 なのかレイヤ 3 なのか、スイッチド ポートなのかルーテッド ポートなのかを示します
Trunk Encapsulation	ISL または IEEE 802.1Q のカプセル化がスイッチ ポートでイネーブルになっているかどうかを示します
Trunk Mode	ポートのトランク モード。トランク モードには、desirable、on、off、auto、no negotiate があります。

Performance Details

[Performance Details] ペインには次のポートレットが表示されます。

- CPU Utilization
- Memory Utilization
- Environmental Temperature
- PathEcho Information
- IPSLA Statistics

CPU Utilization

CPU Utilization ポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 日または 1 時間の CPU 使用率パーセンテージに関する情報が表示されます。

表 11-14 に、デバイスの CPU 使用率の色とパーセンテージを示します。

表 11-14　デバイスの CPU 使用率の色とパーセンテージ

色	パーセント単位のデバイスの CPU 使用率
グリーン	デバイスの CPU 使用率は 0 ～ 10 %
イエロー	デバイスの CPU 使用率は 10 ～ 30 %
オレンジ	デバイスの CPU 使用率は 30 ～ 80 %
レッド	デバイスの CPU 使用率は 80 ～ 100 %

表 11-15 に、CPU Utilization ポートレットの詳細を示します。

表 11-15　CPU Utilization ポートレットの詳細

フィールド	説明
Instance Name	特定の期間に CPU を占有しているインスタンス
Current Value (%)	デバイスの現在の CPU 使用率パーセンテージの値
Minimum (%)	デバイスの最小 CPU 使用率パーセンテージの値
Maximum (%)	デバイスの最大 CPU 使用率パーセンテージの値
Average (%)	デバイスの平均 CPU 使用率パーセンテージの値
HistoGraph	アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます
LiveGraph	アイコンが表示され、クリックすることでライブグラフ チャートが表示されます

Memory Utilization

Memory Utilization ポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 日または 1 時間のメモリ使用率パーセンテージに関する情報が表示されます。

表 11-16 に、デバイスのメモリ使用率の色とパーセンテージを示します。

表 11-16　デバイスのメモリ使用率の色とパーセンテージ

色	パーセント単位のデバイスのメモリ使用率
グリーン	デバイスのメモリ使用率は 0 ～ 50 %
イエロー	デバイスのメモリ使用率は 50 ～ 70 %
オレンジ	デバイスのメモリ使用率は 70 ～ 90 %
レッド	デバイスのメモリ使用率は 90 ～ 100 %

表 11-17 に、Memory Utilization ポートレットの詳細を示します。

表 11-17　Memory Utilization ポートレットの詳細

フィールド	説明
Instance Name	特定の期間にメモリを占有しているインスタンス
Current Value (%)	デバイスの現在のメモリ使用率パーセンテージの値
Minimum (%)	デバイスの最小メモリ使用率パーセンテージの値

表 11-17　Memory Utilization ポートレットの詳細 （続き）

フィールド	説明
Maximum (%)	デバイスの最大メモリ使用率パーセンテージの値
Average (%)	デバイスの平均メモリ使用率パーセンテージの値
HistoGraph	アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます
LiveGraph	アイコンが表示され、クリックすることでライブグラフ チャートが表示されます

Environmental Temperature

Environmental Temperature ポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 日または 1 時間の温度が表示されます。

表 11-18 に、Environmental Temperature ポートレットの詳細を示します。

表 11-18　Environmental Temperature ポートレットの詳細

フィールド	説明
Instance Name	環境温度をモニタするインスタンスの名前
Current Value ºC	デバイスの現在の温度値
Minimum (ºC)	デバイスの最低温度値
Maximum (ºC)	デバイスの最高温度値
Average (ºC)	デバイスの平均温度値
HistoGraph	アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます
LiveGraph	アイコンが表示され、クリックすることでライブグラフ チャートが表示されます

PathEcho Information

PathEcho は、IP ネットワーク内のホップごとの遅延を測定します。

PathEcho Information ポートレットの [Target] ドロップダウン リストボックスからターゲット デバイスを選択し、PathEcho 情報を表示します。PathEcho Information ポートレットには、ソース デバイスからターゲット デバイスへのホップごとの遅延が表示されます。

IPSLA Statistics

IPSLA Statistics ポートレットの [Target] ドロップダウン リストボックスからターゲット デバイスを選択し、IPSLA 統計情報を表示します。

IPSLA Statistics ポートレットには、表 11-19 に示す情報が表示されます。

表 11-19　IPSLA Statistics ポートレットの詳細

フィールド	説明
Collector Name	IPSLA 統計情報を収集するコレクタの名前
Service Name	IPSLA 統計情報を収集するサービスの名前

表 11-19　IPSLA Statistics ポートレットの詳細 （続き）

フィールド	説明
Last Polled Time	IPSLA 統計情報を最後に収集した時刻が表示されます
Latency (ms)	遅延の値をミリ秒単位で表示します
Average (%)	パーセント単位の平均遅延の値。平均パーセンテージは、次の式で計算されます。 平均 % = ラウンドトリップ時間の合計 / 完了の数。 ラウンドトリップ時間は、IP パケットがソースからターゲットに到達し、ターゲットからソースに戻るのに要した時間を表します。
Error (%)	IPSLA 統計情報に関連するエラーのパーセンテージ。エラーのパーセンテージは、式 (エラー / 試行回数) X 100 で計算されます。
SD Jitter (ms)	ソースからターゲット方向のジッター（ミリ秒単位）
DS Jitter (ms)	ターゲットからソース方向のジッター（ミリ秒単位）

Link Troubleshooting

[Link troubleshooting] タブには、トポロジ マップで選択したリンクの詳細が表示されます。

[Link troubleshooting] タブには次のペインが表示されます。

- [Port Status]：詳細については、Port Status を参照してください。
- [Event and Faults]：詳細については、Events and Faults を参照してください。
- [Utilization and Errors]：詳細については、Utilization and Errors を参照してください。

Port Status

[Port Status] ペインには次のポートレットが表示されます。

- Port Details
- コンフィグレット

Port Details

このペインにはは、デバイスのリンク ポートのステータスの要約が表示されます。

表 11-20 に、[Port Status] ペインのフィールドの説明を示します。

表 11-20　[Port Status] ペイン

フィールド名	説明
Device	リンクを構成するデバイスの IP アドレス
Port	リンクを構成するデバイスのポート番号
Port Description	ユーザが入力したポートの説明
Type	メディア タイプ。イーサネットなど

表 11-20　[Port Status] ペイン （続き）

フィールド名	説明
Reset Port	このリンクをクリックすると、ポートがシャットダウンされてからイネーブルになります。デバイスで syslog がイネーブルになっている場合、Change Audit レポートで変更をモニタできます（[Reports] > [Change Audit]）。 [Reset Port] リンクをクリックすると、デバイスのインベントリが起動され、ステータスが MIB から更新されます。インベントリが正常に収集された後、データベースからデータを取得するには、ポートレットの更新アイコンをクリックします。
Admin Status	ポートの管理ステータス。 ポートが意図的にダウンされたかどうかが表示されます。
Operational Status	ポートがアクティブか非アクティブかが表示されます。
Speed	リンク ポートの速度が表示されます。
Duplex Mode	デュプレックス モード。半二重または全二重。
Protocol Enabled	デバイスでイネーブルになっているプロトコル。 例：IP、IPX
Protocol Seen	デバイスで認識されるプロトコル。 例：IP、IPX
VLAN	ポートが属する VLAN。
L2L3	ポートがルーテッドかスイッチドかを示します。
isChannel	ポートが LMS で管理されている別のデバイスに接続されているかどうかを示します。
Discrepancies Found	ポートに関連して検出された不一致の数が表示されます。数値をクリックすると、Discrepancies レポートが起動します。
Best Practice Deviations Found	ポートに関連する、検出されたベスト プラクティスからの逸脱の数が表示されます。値をクリックすると Best Practice Deviations レポートが起動されます。

コンフィグレット

LMS では、リンク ポート上のコンフィギュレーションを表示するためのコンフィグレットを利用できます。各ポートには個別のコンフィグレットがあり、特定のサービスおよび機能の CLI コマンドが表示されます。

Events and Faults

[Events and Faults] ペインには次のポートレットが表示されます。

- Faults
- Syslogs

Faults

このポートレットには、ネットワーク リンクの、最近の 1 時間または 1 日の障害の詳細が要約して表示されます。

表 11-21 に、Fault Details ポートレットのフィールドの説明を示します。

表 11-21　Fault Details ポートレットのフィールド

フィールド名	説明
Severity	障害の重大度。Critical、Informational、Warning のいずれかになります。
Event ID	障害の ID。
Description	障害に関する説明
Status	障害のステータス。ユーザが所有しているかクリアされたか
Event Category	障害の種類。 このフィールドは次のいずれかの値になります。 • Connectivity • Environment • Other • Reachability • Utilization
Duration	アクティブな障害または所有されている障害の場合、障害の発生から現在のサーバ時間までの期間。 障害の発生から障害のクリアまでの期間。
Last Occurrence	障害が発生した日付と時刻。

Syslogs

このポートレットには、ネットワーク内で管理されているデバイスの、最近の 1 日または 1 時間の syslog の詳細が要約して表示されます。選択したインターフェイスの詳細が表示されます。

表 11-22 に、Syslogs ポートレットの説明を示します。

表 11-22　Syslog Details ポートレットのフィールド

フィールド名	説明
Port Number	syslog メッセージを生成しているデバイスのインターフェイスの名前または IP アドレス。
Source	syslog メッセージを生成しているデバイスの名前。
Severity	メッセージの重大度。LMS でキャプチャされる重大度は、Emergencies（0）、Alerts（1）、Critical（2）、Errors（3）です。
Mnemonic	エラー メッセージを一意に識別するコード。以前の Catalyst メッセージにはニーモニックが表示されないことに注意してください。 IOS メッセージのニーモニックの例は、CONFIG I です。
Description	syslog メッセージの説明。

表 11-22　Syslog Details ポートレットのフィールド （続き）

フィールド名	説明
Timestamp	メッセージがロギングされた日付と時刻。これは、デバイスによって渡されたタイムスタンプです。 デバイスがタイムスタンプを渡さない場合、syslog デーモンがタイムスタンプを提供します。
Details	syslog メッセージの名前。 syslog メッセージの説明が表示された新しいウィンドウを開きます。User_URL アイコンをクリックすると、カスタマイズされた Web ページが定義されていればそれが表示されます。定義していない場合は、ユーザ URL を作成するためのサンプル Perl スクリプトがデフォルトで表示されます。 「*」をクリックすると、syslog メッセージの説明が表示されます

Utilization and Errors

[Utilization and Errors] ペインには次のポートレットが表示されます。

- Utilization
- Errors

Utilization

このポートレットには、ネットワーク内で管理されている選択したデバイス インターフェイスの、最近の 1 日または 1 時間の使用率の詳細が要約して表示されます。

表 11-23 に、Utilization ポートレットの説明を示します。

表 11-23　Utilization ポートレットのフィールド

フィールド名	説明
Utilization Parameter	選択したインターフェイスの、最近の 1 日または 1 時間にモニタされた使用率パラメータの名前
Minimum (%)	デバイス インターフェイスの最小使用率パーセンテージの値
Maximum (%)	デバイス インターフェイスの最大使用率パーセンテージの値
Average (%)	デバイス インターフェイスの平均使用率パーセンテージの値
HistoGraph	アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます
LiveGraph	アイコンが表示され、クリックすることでライブグラフ チャートが表示されます

Errors

このポートレットには、ネットワーク内で管理されている選択したデバイス インターフェイスの、最近の 1 日または 1 時間の使用率エラーの詳細が要約して表示されます。

表 11-24 に、Utilization Errors ポートレットの説明を示します。

表 11-24　Utilization Errors ポートレットのフィールド

フィールド名	説明
Utilization Parameters	選択したインターフェイスの、最近の 1 日または 1 時間にモニタされた使用率パラメータの名前
Minimum (Pkts/s)	デバイスの最小使用率エラーの値
Maximum (Pkts/s)	デバイスの最大使用率パーセンテージの値
Average (Pkts/s)	デバイスの平均使用率パーセンテージの値
HistoGraph	アイコンが表示され、クリックすることでヒストグラフ チャートが表示されます
LiveGraph	アイコンが表示され、クリックすることでライブグラフ チャートが表示されます

Endhost Troubleshooting

[Endhost troubleshooting] タブには、選択したエンドホストの詳細が表示されます。

[Endhost troubleshooting] タブには次のペインが表示されます。

- [End Host Status]：詳細については、End Host Status を参照してください。
- [Identity Status Details]：詳細については、Identity Status Details を参照してください。
- [EnergyWise Details]：詳細については、EnergyWise Details を参照してください。

End Host Status

[End Host Status] ペインには次のポートレットが表示されます。

- User Tracking Report
- ping the endhost from LMS Server
- Traceroute the endhost from LMS Server

User Tracking Report

このポートレットには、ネットワークから収集したエンドホストの User Tracking の詳細が要約して表示されます。

表 11-25 に、User Tracking ポートレットの説明を示します。

表 11-25　User Tracking Report ポートレットのフィールド

フィールド名	説明
MAC Address	エンドホストの MAC アドレス
IP Address	エンドホストの IP アドレス
Username	エンドホストのユーザ名
Hostname	エンドホストのホスト名
Switch	エンドホストが接続されているスイッチの名前
Switch IP Address	エンドホストが接続されているスイッチの IP アドレス

表 11-25　User Tracking Report ポートレットのフィールド （続き）

フィールド名	説明
Port Name	エンドホストに接続されているスイッチ ポートの名前
Status	エンドホストに接続されているスイッチ ポートのステータス
Port Speed	スイッチ ポートの速度
VTP Domain	エンドホストが接続されているデバイスの VTP ドメイン名
VLAN Details	VLAN 名
Duplex Mode	デュプレックス モード。半二重または全二重
Type	Medianet エンドポイントの種類が表示されます。 （注）　このフィールドは、エンドポイントが Medianet エンドポイントの場合のみ表示されます。
Location	Medianet エンドポイント上で設定されているすべての場所属性が表示されます。詳細については、「Default Layout of Location Attributes」を参照してください。 次の場所にある medianet.properties ファイルを使用して、場所属性の表示をカスタマイズできます。 • Windows の場合：*NMSROOT*¥lib¥classpath • Solaris または Soft Appliance の場合：/opt/CSCOpx/lib/classpath LMS には、場所属性のデフォルト レイアウトが格納された medianet.properties.orig ファイルもあります。このファイルは、medianet.properties ファイルが壊れた場合に使用できます。[Endhost details] ポップアップに表示される場所属性は、Medianet エンドポイントの種類によって異なります。詳細については、場所属性の表示のカスタマイズを参照してください。 （注）　このフィールドは、エンドポイントが Medianet エンドポイントの場合のみ表示されます。

場所属性の表示のカスタマイズ

Medianet ポートレットの MAC アドレス欄の上にマウスを移動すると、[Endhost details] ポップアップに場所属性が表示されます。次の場所にある medianet.properties ファイルを使用して、このポップアップの場所属性の表示をカスタマイズできます。

- Windows の場合：*NMSROOT*¥lib¥classpath
- Solaris または Soft Appliance の場合：/opt/CSCOpx/lib/classpath

LMS には、場所属性のデフォルト レイアウトが格納された medianet.properties.orig ファイルもあります。このファイルは、medianet.properties ファイルが壊れた場合に使用できます。medianet.properties ファイルが壊れた場合、medianet.properties.orig ファイルをコピーし、壊れた medianet.properties ファイルを置き換える必要があります。

[Endhost details] ポップアップに表示される場所属性は、Medianet エンドポイントの種類によって異なります。デフォルトの medianet.properties ファイルの例を参照してください。

任意のアドレス行に任意の場所属性を追加できます。デフォルトでは、Medianet エンドポイント のアドレスは 5 行あります。行を追加または削除するには、プロパティ MOUSEHOVER.DMP.LOCATION.NUMBER_OF_LINES の値を変更する必要があります。

たとえば、[Endhost details] ポップアップで 6 行目を DMP エンドポイント アドレスに追加するには、次のようにします。

- MOUSEHOVER.DMP.LINE6={1}, {2}, を追加します。
- MOUSEHOVER.DMP.LOCATION.NUMBER_OF_LINES を 6 に変更します。

中括弧の中の数字は、プロパティ ファイルに記載されている場所属性を指します。この例では、それぞれ State と County です。デフォルトの medianet.properties ファイルの例を参照してください。

途中に行を追加するには、以降の行を変更する必要があります。

検索結果のエンドホスト レコードの上にマウスを移動して、Medianet エンドポイントの場所属性のみを表示することもできます。

デフォルトの medianet.properties ファイルの例

```
### Location attributes order
#
#SNo     Fields                      Description
#-------------------------------------------------------------------------------
#1       State                       National subdivision (state)
#2       County                      Land area of local government
#3       City                        City
#4       City Division               City division
#5       Neighborhood                Neighborhood
#6       Street Group                Group of streets
#7       Leading Street Direction    Leading street direction
#8       Trailing Street Direction   Trailing street direction
#9       Street Suffix               Street suffix
#10      House                       House number
#11      Street Number               Street number suffix
#12      Landmark                    Landmark
#13      Additional Location         Additional location information
#14      Name                        Name of the resident
#15      Zipcode                     Postal/Zip Code
#16      Building                    Building name
#17      Unit                        Unit
#18      Floor                       Floor number
#19      Room                        Room number
#20      Place                       Place type
#21      PostalCommunity Name        Postal community name
#22      PostOffice Box              PO Box
#23      Additional Code             Additional code information
#24      Seat                        Seat number
#25      Primary Road                primary road or street name
#26      Road Section                Road section name
#27      Road Branch                 Road branch name
#28      Road SubBranch              Road sub-branch name
```

```
#29     StreetName PreMod           Street pre modifier name
#30     StreetName PostMod          Street post modifier name
#31     Country Code                Country

# Location Attributes format for DMP Mouse Hover
MOUSEHOVER.DMP.LOCATION.NUMBER_OF_LINES=5
MOUSEHOVER.DMP.LINE1={14},
MOUSEHOVER.DMP.LINE2={17}, {18}, {19},
MOUSEHOVER.DMP.LINE3={25}, {9},
MOUSEHOVER.DMP.LINE4={5},
MOUSEHOVER.DMP.LINE5={3}, {1}- {15}

# Location Attributes format for IPVSC Mouse Hover
MOUSEHOVER.IPVSC.LOCATION.NUMBER_OF_LINES=5
MOUSEHOVER.IPVSC.LINE1={14},
MOUSEHOVER.IPVSC.LINE2={17}, {18},
MOUSEHOVER.IPVSC.LINE3={25}, {9},
MOUSEHOVER.IPVSC.LINE4={5},
MOUSEHOVER.IPVSC.LINE5={3}, {1}- {15}

# Location Attributes format for End Host Troubleshooting
TS.LOCATION.NUMBER_OF_LINES=12
TS.LOCATION.LINE1={14},
TS.LOCATION.LINE2={18}, {17}, {24}, {19},
TS.LOCATION.LINE3={16}, {10},
TS.LOCATION.LINE4={11}, {7}, {29}, {30}, {8}, {9},
TS.LOCATION.LINE5={6},
TS.LOCATION.LINE6={25}, {29}, {27}, {28},
TS.LOCATION.LINE7={12},
TS.LOCATION.LINE8={20}, {13}, {5},
TS.LOCATION.LINE9={22}, {21},
TS.LOCATION.LINE10={4},
TS.LOCATION.LINE11={3}, {2}, {1}, {31},
TS.LOCATION.LINE12={15}, {23}

# Property to enable/disable location collection.Default is TRUE
# To disable, change it to FALSE
LOCATION_COLLECTION=TRUE
```

ping the endhost from LMS Server

このポートレットには、LMS サーバからエンドホストへの ping の出力または結果と、ping の統計情報が表示されます。

[Test Now] ボタンを使用して、統計情報を取得し、ポートレットの最新の内容を表示できます。

Traceroute the endhost from LMS Server

このポートレットには、LMS サーバからデバイスへの traceroute の出力または結果と、ping の統計情報が表示されます。

[Test Now] ボタンを使用して、統計情報を取得し、ポートレットの最新の内容を表示できます。

Identity Status Details

[Identity Status Details] ペインには、次のポートレットが表示されます。

- Identity Information from MAC History
- Identity Information from User History
- Identity Information for Switch Port

Identity Information from MAC History

このポートレットには、MAC History レポートから得た ID 情報の要約が表示されます。

表 11-26 に、Identity Information from MAC History ポートレットのフィールドの説明を示します。

表 11-26　Identity Information from MAC History ポートレットのフィールド

フィールド名	説明
Switch IP Address	エンドホストが接続されているスイッチの IP アドレス
Port Name	ホストが接続されているデバイスのポート名
Status	認証ステータス（success または failure）
Type	認証タイプ（MAB、dot1x、または webauth など）
VLAN	デバイスが属する VLAN の名前
DACL	RADIUS サーバからダウンロードできるアクセス コントロール リスト
Authentication time	認証の時刻

Identity Information from User History

このポートレットには、User History レポートから得た ID 情報の要約が表示されます。

表 11-27 に、Identity Information from User History ポートレットのフィールドの説明を示します。

表 11-27　Identity Information from User History ポートレットのフィールド

フィールド名	説明
Switch IP Address	エンドホストが接続されているスイッチの IP アドレス
Port Name	ホストが接続されているデバイスのポート名
Status	認証ステータス（success または failure）
Type	認証タイプ（MAB、dot1x、または webauth など）
VLAN	デバイスが属する VLAN の名前
DACL	RADIUS サーバからダウンロードできるアクセス コントロール リスト
Authentication time	認証の時刻

Identity Information for Switch Port

このポートレットには、Switch Port レポートから得た ID 情報の要約が表示されます。

表 11-28 に、Identity Information for Switch Port ポートレットのフィールドの説明を示します。

表 11-28　Identity Information for Switch Port のフィールド

フィールド名	説明
Switch IP Address	エンドホストが接続されているスイッチの IP アドレス
Port Name	ホストが接続されているデバイスのポート名
Status	認証ステータス（success または failure）
Type	認証タイプ（MAB、dot1x、または webauth など）
VLAN	デバイスが属する VLAN の名前
DACL	RADIUS サーバからダウンロードできるアクセス コントロール リスト
Timestamp	認証の時刻

EnergyWise Details

[EnergyWise Details] ペインには、Endhost EnergyWise Details ポートレットが表示されます。

Endhost EnergyWise Details

このポートレットは、選択したエンドホストの EnergyWise Details の情報の要約が表示されます。

表 11-29 に、Identity Information for Switch Port ポートレットのフィールドの説明を示します。

表 11-29　lEndhost EnergyWise Details

フィールド名	説明
Power Level	EnergyWise の電力レベルが 0 ～ 10 の範囲で表示されます。EnergyWise 電力レベルは、エンドポイントの電力ステータスに常に対応する電力使用量を管理します。
Current Value (W)	エンドホストの現在の電力の値がワット単位で表示されます。

トラブルシューティング ツールの使用

ここでは、次の内容について説明します。

- Management Station to Device ツールの使用方法
- ping の使用
- traceroute の使用
- Proxy ping
- Proxy Traceroute
- SNMP Walk の使用方法
- SNMP Set の使用方法
- Packet Capture の使用方法

Management Station to Device ツールの使用方法

非管理対象デバイスまたは応答しないデバイスの問題をトラブルシューティングするために、プロトコルごとのデバイスの接続性をチェックできます。Management Station to Device ツールを使用すると、レイヤ 4（アプリケーション）の接続の問題点を診断することが可能です。

レイヤ 4 のテストは、ネットワーク デバイスの管理に欠くことのできない次のようなサービス要素を対象とします。デバッグ ツールおよび測定ツール（UDP および TCP）、Web サーバ（HTTP）、ファイル転送（TFTP）、端末（Telnet）、および読み取り / 書き込みアクセス（SNMP）。

（注）　Management Station to Device のチェックは、プロトコル接続に対してのみ実行されます。対応するプロトコルのクレデンシャルはテストまたは確認されません。

IP アドレスではなくホスト名を入力すると、アドレスを見つけるため名前検索が実行されます。このタスクは、アドレスが見つからないと失敗します。

次のものをテストできます。

- UDP（エコー テスト、ポート 7）

  エコー要求を UDP ポート 7 に送信します。

- TCP（エコー テスト、ポート 7）

  エコー要求を TCP ポート 7 に送信します。

- HTTP（アベイラビリティ テスト、ポート 80）

  HTTP 要求を宛先デバイスの HTTP ポート 80 に送信します。

- TFTP（アベイラビリティ テスト、ポート 69。デバイスは TFTP サーバとして設定されている必要があります）

  TFTP 要求を宛先デバイスの TFTP ポート（69）に送信します。

- Telnet（サービス テスト、ポート 23）

  デバイス上で Telnet がイネーブルになっているかどうかと、宛先デバイスが Telnet 要求に応答するかどうかをチェックします。データベース内の Telnet パスワードが正しいかどうかは確認しません。

  Telnet は TCP の上で動作するため、Telnet が成功した場合、デバイスで TCP がイネーブルになっていることを示します。Telnet が失敗する場合、TCP がイネーブルになっているかどうかを自動的に判定するための方法はありません。TCP がアップ状態かどうかを確認するには、TCP テストを実行します。

- SNMP（サービス テスト、ポート 161）

  SNMP 読み取りテスト（SNMPR）を行うために、宛先デバイスに **snmp get** 要求を送信します。また、SNMP 書き込みテスト（SNMPW）を行うために、デバイスに **snmp set** 要求も送信します。プロトコルのバージョン v1、v2c、および v3 がサポートされています。

- SSH（サービス テスト、ポート 22）

  SSH がデバイスでイネーブルになっているかどうかをチェックします。宛先デバイスが SSH 要求に応答する場合、LMS サーバがそのデバイスに SSH 要求を行うことができるかどうかもテストします。データベースのパスワードは確認しません。

Management Station To Device を、ネットワーク オペレータまたはヘルプ デスク特権で起動した場合、デバイス クレデンシャルの取得に失敗し、SNMP v1/v2c の read/write コミュニティ ストリング、read/write SNMPv3 クレデンシャルはデフォルト値に設定されます。SNMP v1/v2c/v3 のクレデンシャルを手動で入力する必要があります。

Management Station to Device ツールを起動するには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　[Problem Type] ドロップダウン リストから問題の種類を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインをクリックします。

ステップ 5　クイック リンクのリストから、[Management Station to Device] をクリックします。

[Management Station to Device] ダイアログボックスが表示されます。

ステップ 6　目的の接続アプリケーションを選択します。

フィールドに入力するすべての情報で大文字と小文字が区別されます。

SNMP v1 または v2c を選択する場合、次のことを行う必要があります。

- SNMP v1 または v2c を選択します。デフォルトは SNMP v2c です。
- read コミュニティ ストリングを入力します。
- write コミュニティ ストリングを入力します。
- タイムアウトを秒単位で入力します。デフォルトは 2 秒です。

SNMP v3（セキュリティ レベルが NoAuthNoPriv）を選択する場合、次の内容を入力します。

- read ユーザ名。
- write ユーザ名。
- タイムアウト（秒単位）。デフォルト値は 2 秒です。

SNMP v3（セキュリティ レベルが AuthNoPriv）を選択する場合、次の内容を入力します。

- read ユーザ名。
- read 認証パスワード。
- read 認証プロトコル。ドロップダウン リストから [MD5] または [SHA] を選択します。
- write ユーザ名。
- write 認証パスワード。
- write 認証プロトコル。ドロップダウン リストから [MD5] または [SHA] を選択します。
- タイムアウト（秒単位）。デフォルト値は 2 秒です。

SNMP v3（セキュリティ レベルが AuthPriv）を選択する場合、次の内容を入力します。

- read ユーザ名。
- read 認証パスワード。
- read 認証プロトコル。ドロップダウン リストから [MD5] または [SHA] を選択します。
- read プライバシー パスワード。
- read プライバシー プロトコル。ドロップダウン リストからプライバシー プロトコルを選択します。リスト項目は次のとおりです。
  - DES
  - 3DES
  - AES128

  - AES192
  - AES256
- write ユーザ名。
- write 認証パスワード。
- write 認証プロトコル。ドロップダウン リストから [MD5] または [SHA] を選択します。
- write プライバシー パスワード。
- write プライバシー プロトコル。ドロップダウン リストからプライバシー プロトコルを選択します。リスト項目は次のとおりです。
  - DES
  - 3DES
  - AES128
  - AES192
  - AES256
- タイムアウト（秒単位）。デフォルト値は 2 秒です。

接続アプリケーションとして SSH を選択する場合、次のことを行う必要があります。

- [SSH ver1] または [SSH ver2] を選択します。

ステップ 7　タイムアウトを秒単位で入力し、[OK] をクリックします。

デフォルトは 2 秒です。

[Interface Test Results] ポップアップに結果が表示されます。[Interface Details Results] 画面には、テスト済みのインターフェイスおよび各オプションのテスト結果が表示されます。

（注）　SNMPv3 の read/write ユーザ名およびパスワードと、SNMP v1/v2c の read/write コミュニティ ストリングはどちらも、大文字と小文字が区別されます。

ping の使用

デバイスが到達可能かどうかをテストするには、ping ツールを使用します。**ping** は、ICMP エコー メッセージとその応答をテストします。**ping** はデバイスの最も単純なテストであるため、最初に使用します。

送信パケット数、受信パケット数、パケット損失のパーセンテージ、およびラウンドトリップ時間（ミリ秒単位）を表示できます。**ping** が失敗する場合は、**traceroute** の使用を試みます。

詳細については、ping device from LMS Server および Proxy ping を参照してください。

traceroute の使用

ネットワーク管理ステーションとターゲット デバイスの間のルーティング エラーを検出するには、traceroute ツールを使用します。

traceroute は、**ping** が失敗する原因や、アプリケーションがタイムアウトする原因を理解するのに役立ちます。そのために、TCP/IP レイヤ 3（トランスポート）の問題が診断されます。デバイスまでのルート上の各ホップ（または、ゲートウェイ）とそこに到達するまでの時間を表示できます。

詳細については、Traceroute device from LMS Server および Proxy Traceroute を参照してください。

Proxy ping

Proxy ping を使用すると、選択したデバイスから別のデバイスまたはサーバに ping を実行し、ping の出力を表示できます。

proxy ping を実行するには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

ステップ 5　[Proxy ping] をクリックします。

ステップ 6　ping 対象のデバイスまたはサーバの IP アドレスを、[Proxy ping] ダイアログボックスに入力します。

ステップ 7　[Proxy ping] ボタンをクリックします。

ping 統計情報が、[Proxy ping] ダイアログボックスのテキスト領域に表示されます。

Proxy Traceroute

Proxy Traceroute は、選択したデバイスからのデバイスまたはサーバの traceroute の出力を表示します。

proxy traceroute を実行するには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

ステップ 5　[Proxy Traceroute] をクリックします。

ステップ 6　ping 対象のデバイスまたはサーバの IP アドレスを [Proxy Traceroute] ダイアログボックスに入力します。

ステップ 7　[Proxy Traceroute] ボタンをクリックします。

traceroute 統計情報が、[Proxy Traceroute] ダイアログボックスのテキスト領域に表示されます。

SNMP Walk の使用方法

SNMP Walk では、トラブルシューティングのために、デバイスの指定した OID から始まる MIB ツリーをトレースしたり、特定のデバイスに関する情報を収集できます。

この機能を使用するには、システム管理者権限が必要です。

SNMP Walk を使用するには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

ステップ 5　[SNMP Walk] をクリックします。

[SNMP Walk] ダイアログボックスが表示されます。

ステップ 6　IP アドレスまたは DNS 名を入力します。

ステップ 7　使用する SNMP バージョンを選択します。

SNMP バージョン 1 および 2c の場合（64 ビット カウンタの場合は SNMP v2 を使用します）

a. read コミュニティ ストリングを入力します。

SNMP バージョン 3（セキュリティ レベルが NoAuthNoPriv および AuthNoPriv）の場合

a. SNMPv3 ユーザ名を入力します。

b. SNMPv3 認証パスワードを入力します。

c. SNMP v3 認証プロトコルを指定します。[MD5] オプション ボタンまたは [SHA] オプション ボタンを選択します。

d. SNMP コンテキスト名を入力します。これは任意です。

SNMP バージョン 3（セキュリティ レベルが AuthPriv）の場合

a. SNMPv3 ユーザ名を入力します。

b. SNMPv3 認証パスワードを入力します。

c. SNMP v3 認証プロトコルを指定します。[MD5] オプション ボタンまたは [SHA] オプション ボタンを選択します。

d. プライバシー パスワードを入力します。

e. ドロップダウン リストからプライバシー プロトコルを選択します。選択可能な項目は次のとおりです。

- DES
- 3DES
- AES128
- AES192
- AES256

f. SNMP コンテキスト名を入力します。これは任意です。

ステップ 8　開始 OID を入力します（任意）。このフィールドを空にした場合は 1 から開始されます。

ステップ 9　SNMP タイムアウト時間を入力します。デフォルト値は 10 秒です。

ステップ 10　出力される OID を数値として表示する場合は、[Output OIDs Numerically] チェックボックスをオンにします（任意）。これは任意です。

デフォルトでは、OID に対応する名前が出力ウィンドウに表示されます。

ステップ 11　出力されるインデックスを数値として出力する場合は、[Output Indexes Numerically] チェックボックスをオンにします。これは任意です。

ステップ 12　デバッグ オプションを有効にする場合は、[Debug] チェックボックスをオンにします。これは任意です。

（注）　これらのフィールドに入力する文字列はすべて、大文字と小文字が区別されます。

ステップ 13　[OK] をクリックして結果を得ます。

結果は、入力したパラメータに基づきます。ウォークが完了したら、結果をテキストとして保存できます。完全なウォークを実行すると、時間がかかる場合があります。

SNMPv3 の read/write ユーザ名およびパスワードと、SNMP v1/v2c の read/write コミュニティ ストリングはどちらも、大文字と小文字が区別されます。[SNMP walk] ダイアログボックスには、Device Credential Repository にデバイスのクレデンシャル（SNMP v1/v2c/v3）があれば、それらが表示されます。クレデンシャルがない場合は、各 SNMP バージョンのデフォルト値が表示されます。

SNMP Walk 機能を、ネットワーク オペレータまたはヘルプ デスク特権で起動した場合、デバイス クレデンシャルの取得に失敗し、SNMP v1/v2c の read/write コミュニティ ストリング、read/write SNMPv3 クレデンシャルはデフォルト値に設定されます。

SNMP v1/v2c/v3 のクレデンシャルを手動で入力する必要があります。

SNMP Set の使用方法

このオプションを使用すると、デバイスを制御するために、デバイス上の SNMP オブジェクトまたは複数のオブジェクトを設定できます。この機能を使用するには、システム管理者権限が必要です。

SNMP set を使用するには、以下の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

[SNMP set] ダイアログボックスが表示されます。

ステップ 5　IP アドレスまたは DNS 名を入力します。

ステップ 6　SNMP のバージョンを選択します。

SNMP バージョン 1 および 2c の場合（64 ビット カウンタの場合は SNMP v2 を使用します）

a. read/write コミュニティ ストリングを入力します。

b. 設定するオブジェクト ID と、インスタンス ID または番号を入力します。

c. ドロップダウン リストからオブジェクトの型を選択します。選択可能な値は次のとおりです。

- Integer
- Unsigned Integer
- TimeTicks
- IP Address
- Object ID
- String
- Hex String
- Decimal String

d. 新しい値を入力します。これは、指定したオブジェクトの型に依存します。

SNMP バージョン 3（セキュリティ レベルが NoAuthNoPriv および AuthNoPriv）の場合

a. SNMPv3 ユーザ名を入力します。

b. SNMPv3 認証パスワードを入力します。

c. SNMPv3 認証プロトコルを指定します。[MD5] オプション ボタンまたは [SHA] オプション ボタンを選択します。

d. 設定しようとしているオブジェクト ID と、インスタンス ID または番号を入力します。

e. ドロップダウン リストからオブジェクトの型を選択します。選択可能な項目は次のとおりです。

- Integer
- Unsigned Integer
- TimeTicks
- IP Address
- Object ID
- String
- Hex String
- Decimal String
- Bits
- Unsigned 64-bit Integer
- Signed 64-bit Integer

f. 新しい値を入力します。これは、指定したオブジェクトの型に依存します。

g. SNMPv3 コンテキスト名を入力します。これは任意です。

SNMP バージョン 3（セキュリティ レベルが AuthPriv）の場合

a. SNMPv3 ユーザ名を入力します。

b. SNMPv3 認証パスワードを入力します。

c. SNMP v3 認証プロトコルを指定します。[MD5] オプション ボタンまたは [SHA] オプション ボタンを選択します。

d. プライバシー パスワードを入力します。

e. ドロップダウン リストからプライバシー プロトコルを選択します。選択可能な項目は次のとおりです。

- DES
- 3DES
- AES128
- AES192
- AES256

f. 設定しようとしているオブジェクト ID と、インスタンス ID または番号を入力します。

g. ドロップダウン リストからオブジェクトの型を選択します。選択可能な項目は次のとおりです。

- Integer
- Unsigned Integer
- TimeTicks
- IP Address
- Object ID
- String
- Hex String
- Decimal String
- Bits
- Unsigned 64-bit Integer
- Signed 64-bit Integer

h. 新しい値を入力します。これは、指定したオブジェクトの型に依存します。

i. SNMPv3 コンテキスト名を入力します。これは任意です。

ステップ 7　SNMP タイムアウト時間を入力します。デフォルトは 10 秒です。

ステップ 8　デバッグ オプションを有効にする場合は、[debug] チェックボックスをオンにします。

ステップ 9　デバイス上の他の SNMP オブジェクトを追加する場合は [Next] をクリックします。

[SNMP Set] ダイアログ ボックスが表示されます。

ステップ 10　必要なすべてのフィールドに入力し、[Next] をクリックします。必要なオブジェクトをすべて追加するまでこの手順を繰り返します。

ステップ 11　[OK] をクリックして結果を得ます。

結果は、入力したパラメータに基づきます。SNMP オブジェクトの設定を完了した後、テキストとして保存し、出力をメール送信できます。

SNMPv3 の read/write ユーザ名およびパスワードと、SNMP v1/v2c の read/write コミュニティ ストリングはどちらも、大文字と小文字が区別されます。[SNMP Set] ダイアログボックスには、Device and Credential Repository にデバイスのクレデンシャル（SNMP v1/v2c/v3）があれば、それらが表示されます。クレデンシャルがない場合は、各 SNMP バージョンのデフォルト値が表示されます。

SNMP Set 機能を、ネットワーク オペレータまたはヘルプ デスク特権で起動した場合、デバイス クレデンシャルの取得に失敗し、SNMP v1/v2c の read/write コミュニティ ストリング、read/write SNMPv3 クレデンシャルはデフォルト値に設定されます。

SNMP v1/v2c/v3 のクレデンシャルを手動で入力する必要があります。

Packet Capture の使用方法

Packet Capture ツールを使用すると、LMS マシンから生データをキャプチャして、トラブルシューティングに役立てることができます。この機能を使用するには、システム管理者権限が必要です。

（注）　この機能を Windows マシンで使用するには、WinPcap がインストールされている必要があります。実行可能ファイルは *NMSROOT*¥objects¥jet¥bin¥winpcap.exe です。*NMSROOT* は LMS のインストール ディレクトリです。

データをマシンからキャプチャするには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

ステップ 5　[Packet Capture] をクリックします。

[Packet Capture] ダイアログボックスが表示されます。

アーカイブされたキャプチャ ファイルの一覧が表示されます。アーカイブされているキャプチャ ファイルがない場合、このダイアログ ボックスに、レコードがないことが表示されます。

ステップ 6　[Packet Capture] ダイアログボックスの [Create] をクリックします。

[Packet Capture Inputs] ダイアログ ボックスが、デフォルト値が設定された状態で表示されます。

ステップ 7　次の情報を入力します。

- Interface

  マシンに複数のインターフェイスがある場合、まずキャプチャで使用するインターフェイスを選択する必要があります。

- Address

  このフィールドには、1 つ以上のアドレスを指定できます（1 個のスペースで区切ります）。この値は、パケットをキャプチャするときにネットワーク内の LMS マシンの場所を特定するために使用されます。

- Protocols and Ports または Applications（データ キャプチャ用）

  次のいずれかを使用してデータをキャプチャできます。

  - プロトコルとポート

    デフォルトでは、指定したマシンから指定したプロトコルとポートを使用してパケットがキャプチャされます。

    ポート番号がわかっている場合はこのオプションを選択できます。

    キャプチャに含めるプロトコル（**TCP**、**UDP**、または **ICMP**）を選択します。

    3 つのプロトコル（TCP、UDP、ICMP）すべてを含めるには [Any] を選択します。デフォルトでは TCP プロトコルが選択されます。

    TCP と UDP の場合、データをキャプチャするポートのリストを入力できます。[Port(s)] フィールドには、1 つ以上の TCP または UDP ポートを、1 つのスペースで区切って指定できます。[Address] フィールドにアドレスを指定せずにポートを指定した場合、アクティブなすべてのデバイスのそのポートに対してデータがキャプチャされます。

または

- Applications

  アプリケーションを使用してデータをキャプチャする場合は、[Applications] オプション ボタンをクリックし、設定済みの一般的な LMS アプリケーションおよび標準アプリケーションのリストから選択します。

- Cycle

  パケット キャプチャをいつ停止するかを指定する必要があります。次の後でキャプチャを停止できます。

  - 特定の期間。
  - フィルタが特定の量のデータをキャプチャした場合。
  - 特定の数のパケットをキャプチャした場合。

  デフォルトでは、キャプチャ サイクルは 60 秒後に停止します。

ステップ 8　[OK] をクリックします。

[Packet Capture] ステータス ポップアップが開き、キャプチャの現在のステータスが表示されます。デフォルト値を使用して（パラメータを設定せずに）[OK] をクリックすると、次の 60 秒間キャプチャが行われます。

キャプチャを実行した後、[Packet Capture] ダイアログボックスに新しいパケッ キャプチャ ファイルと、アーカイブされたキャプチャ ファイルの一覧が表示されます。

ポップアップで [Stop Capture] をクリックすると、キャプチャが停止します。パケット キャプチャ情報が、[Packet Capture] ダイアログボックスのアーカイブ ファイルの間に追加されます。

ステップ 9　新しいパケット キャプチャ ファイルのリンクをクリックすると、LMS サーバが受信したパケットのスニファ出力が表示されます。

結果は、Ethereal など任意のスニファ アプリケーションで開くことができます。これらのファイルはバイナリの libpcap 形式で、拡張子は .jet です。これらのファイルを Web ブラウザを通じて直接ダウンロードし、TAC に電子メールで送信してさらに解析を依頼できます。

既存のパケット キャプチャ ファイルを削除するには、次の手順を実行します。

ステップ 1　[Inventory] > [Tools] > [Device Center] を選択します。

ステップ 2　Device Center を選択します。

ステップ 3　Device Center の使用に示す手順に従い、デバイスの診断を進めます。

デバイスのトラブルシューティング情報が、新しいタブに、それぞれのペインの中のポートレットの形で表示されます。

ステップ 4　[Device Status] ペインで [Tools] メニューをクリックします。

ステップ 5　[Packet Capture] をクリックします。

[Packet Capture] ダイアログボックスが表示されます。

ステップ 6　削除するパケット キャプチャ ファイルを選択します。

ステップ 7　[Packet Capture] ダイアログボックスの [Delete] をクリックします。

アーカイブされているキャプチャ ファイルのリストからファイルが削除されます。

VRF のトラブルシューティング

ネットワーク管理者は、トラブルシューティング機能を使用して、VRF が設定されたデバイスのエンドツーエンドの接続性を確認できます。VRF に参加している、VRF が設定されたデバイスの到達可能性を確認できます。

ここでは、次の内容について説明します。

ping または traceroute

次の項では、VRF の ping または traceroute コマンドの使用方法について説明します。

- ping

  ping コマンドを使用すると、選択した VRF に属する送信デバイスと宛先デバイスの間の VRF の接続性を、ネットワーク上のさまざまな場所で確認できます。また、ping を使用して、VRF が設定されたネットワークのデバイスのアクセス可能性を確認できます。

  ping コマンドは、指定した IP アドレスにあるリモート デバイス（選択した VRF の一部）にエコー要求を送信します。宛先インターフェイスが到達可能でない場合、パケットが失われ、パケットが成功したか失敗したかが表示されます。

  ping を使用して、VRF が設定されたネットワークのデバイスのアクセス可能性を確認できます。送信元デバイスから宛先デバイスへのデバイスの到達可能性をテストできます。

- traceroute

  特定の VRF の宛先デバイスに到達するために、データ パケットが通過したルートのリストを表示します。

次のユーザのみが VRF をトラブルシューティングできます。

- ネットワーク オペレータ
- ネットワーク管理者
- システム管理者

ping または traceroute を使用するには、次の手順を実行します。

ステップ 1　VRF のホーム ページで [Troubleshooting] タブをクリックします。

[ping or Traceroute] ページが表示され、[ping or Traceroute] オプションがデフォルトで選択されます。

ステップ 2　表 11-30 に従って必要な情報を入力します。

表 11-30　[ping or Traceroute] の設定

ウィンドウ要素	説明	使用方法
Operation	VRF の動作をトラブルシューティングするために使用するプロセスを表し、次のいずれかになります。 • ping • traceroute	デバイスをトラブルシューティングするために実行するプロセスをクリックします
Enable Bi-directional	双方向のトラブルシューティングを有効にします（traceroute の場合のみ）。このオプションは、ping コマンドをサポートしていません。	双方向 traceroute を有効にするには、[Enable Bi-directional ping] チェックボックスをオンにします。
Source Device		
Source Device	ソース デバイスの詳細。 • [Select] をクリックして、トラブルシューティング対象の VRF が設定されたデバイスを選択します。 [Device Selector] ダイアログボックスが、[Device selector] ウィンドウに表示されます。 または • ソース デバイスの詳細を入力します。	[Select] を使用してデバイスを選択します。デバイス セレクタが画面に表示されます。 • オプション ボタンをクリックし、デバイス セレクタに一覧表示されているデバイスを選択します。 または • ソース デバイス名を入力します。 先頭の 4 文字を入力すると、10 個のデバイス名が表示されます。
VRF Details		
VRF	ネットワーク上のすべてのデバイスで設定されている VRF が表示されます。表示される内容は、グローバル テーブルから取得されます。 [Global Table] を選択すると、トラブルシューティングのためにグローバル テーブルが使用され、どの VRF にも割り当てられていないすべてのインターフェイスが [Source Interface] フィールドと [Destination Interface] フィールドに設定されます。	[VRF] ドロップダウン リストから、トラブルシューティング対象の VRF を選択します。

表 11-30　[ping or Traceroute] の設定 （続き）

ウィンドウ要素	説明	使用方法
Destination Device		
Destination Device	次の組み合わせからなります。 • [VRF] ドロップダウン リストで選択した VRF 固有の、VRF が設定されたデバイス • 送信元デバイスを除く 例： デバイス A と B で VRF が設定されており、デバイス B の VRF 名が「Red」に設定されているとします。 送信元からデバイス A を選択し、[VRF] ドロップダウン リストから VRF [Red] を選択した場合、宛先デバイスのデバイス セレクタには、デバイス B のみが表示されます。	デバイス セレクタを使用してデバイスを選択します。 • オプション ボタンをクリックして、一覧表示されたグループ内のデバイスを選択し、[Select] をクリックします。 または • 宛先デバイス名を入力します。 先頭の 4 文字を入力すると、デバイス名の候補が表示されます。
Interface Details		
Source Interface	送信元デバイスのすべてのインターフェイスが表示されます。 送信元インターフェイスを選択すると、データ パケットが選択した送信元インターフェイスを通じてルーティングされ、ping コマンドが実行されます。	[Source Interface] ドロップダウン リストから、送信元インターフェイスを選択します
Destination Interface	宛先デバイスに接続されているすべてのインターフェイスが表示されます	[Destination Interface] ドロップダウン リストから、宛先インターフェイスを選択します
View Command	ping または traceroute で使用されるコマンドが表示されます	ping または traceroute で使用されるコマンドを表示するには、[View Command] をクリックします
Monitor Real Time	VRF が設定されたデバイスのインターフェイスのリアルタイム ステータスを表示できます。 リアルタイム ステータスに関する詳細は IPSLA を使用して取得され、ステータスはグラフィカル形式で表示されます。	[Monitor Real Time] をクリックします。
Ping or Traceroute	ping または traceroute コマンドが実行されます。	[ping] または [Traceroute] をクリックします
Result	VRF-Lite トラブルシューティング プロセス（ping または traceroute）の結果が表示されます。	表示のみ。
Reset	ping または traceroute に渡される詳細をリセットします。	[Reset] をクリックします
Clear Result	[ping or Traceroute] ページの [Result] フィールドに表示されている結果をクリアします	[Clear Result] をクリックして結果をクリアします

ステップ 3　[ping or Traceroute] をクリックしてトラブルシューティング プロセスを実行します。

ping の例

```
cmx-uranus#ping vrf GreenVRF 10.77.22.2 source 10.77.22.3
Primary Login Succeeded / Primary Enable Succeeded

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.77.22.2, timeout is 2 seconds:
Packet sent with a source address of 10.77.22.3.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms PE3745-L3-2#
*******************************************************************************
```

ping コマンドについて

次の VRF コンフィギュレーションの詳細が選択したデバイスにプッシュされます。VRF コンフィギュレーションの詳細の説明を表 11-31 に示します。

表 11-31　ping コマンドの詳細

コマンド	目的
ping vrf *vrf-name ip-address*	特定の VRF がある IP アドレスに ping を実行します
ping *destination interface* **source** *source interface*	インターフェイス コンフィギュレーション モードを開始し、VRF に関連付けるレイヤ 3 インターフェイスを指定します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。

Show Results

[Show Results] ページには、VRF 固有の show コマンドの結果が表示されます。

たとえば、次のコマンドの出力を表示できます。

show ip route vrf *<selected vrf> <selected protocol>*

[Show Results] ページを使用するには、次の手順を実行します。

ステップ 1　Virtual Network Manager のホーム ページで [Troubleshooting] タブをクリックします。

[ping or Traceroute] ページが表示されます。

ステップ 2　[Troubleshooting] > [Show Results] を選択します

[Show Results] ページが表示されます。

ステップ 3　表 11-32 に従って必要な情報を入力します。

表 11-32　[Show Results] での設定

ウィンドウ要素	説明	使用方法
Source Device	ソース デバイスの詳細。 • [Select] をクリックして、トラブルシューティング対象の VRF が設定されたデバイスを選択します。 [Device Selector] ウィンドウが表示されます。 または • ソース デバイス名を入力します。	[Select] を使用してデバイスを選択します。デバイス セレクタが画面に表示されます。 • オプション ボタンをクリックし、デバイス セレクタに一覧表示されているデバイスを選択します。 または • ソース デバイス名を入力します。 先頭の 4 文字を入力すると、10 個のデバイス名が表示されます。
Routing Protocol	VNM のトラブルシューティングに使用するルーティング プロトコルを表します。使用されるルーティング プロトコルは次のとおりです。 • OSPF • EIGRP	デバイスのトラブルシューティングに使用するルーティング プロトコルをクリックします。
View Command	VRF 固有の show コマンドを表示します。 • OSPF の場合、次のコマンドが使用されます。 **show ip protocol vrf** *vrf name* **show ip** *OSPF* • EIGRP の場合、次のコマンドが使用されます。 **show ip eigrp vrf** *vrf name neighbors* ここで、ネイバーは VRF に参加する隣接デバイスを表します。	[View Command] をクリックして、VRF 固有の show コマンドを表示します
Show Results	VRF 固有の show コマンドの結果が表示されます。	[Show Results] をクリックします 結果は [Result] ペインに表示されます。
Result	特定の VRF に対する show コマンドの結果を表示します。	表示のみ。
Reset	[Show Command] ページの詳細をリセットします。	[Reset] をクリックします
Clear Result	[Show Results] ページの [Result] ペインに表示される結果をクリアします	[Clear Result] をクリックします

[Show Results] の例

```
cmx-uranus# show ip eigrp vrf Green neighbors
Primary Login Succeeded
/ Primary Enable Succeeded
```

```
IP-EIGRP neighbors for process 65
PE3745-L3-2#
********************************************************************************
```

[Show Results] のコマンドについて

次の VRF コンフィギュレーションの詳細が選択したデバイスから取得されます。VRF の [Show Results] の詳細の説明を表 11-33 に示します。

表 11-33　[Show Results] の詳細

コマンド	目的
show ip vrf *vrf-name*	VRF とインターフェイスを表示します
show ip route *vrf* vrf-name	VRF の IP ルーティング テーブルを表示します
show ip protocols vrf *vrf-name*	VRF に関連付けられたルーティング プロトコル情報を表示します
show ip *OSPF*	OSPF ネットワークの設定を確認します
show ip eigrp vrf *vrf-name neighbor*	インターフェイス上にあり、指定した VRF インスタンスに属している Enhanced Interior Gateway Routing Protocol（EIGRP）ネイバーを表示します。 特定の種類のトランスポートの問題をデバッグするためにも使用します。