Catalyst 6500 シリーズ スイッチ 合法的傍受 コンフィギュレーション ガイド

Cisco IOS Software Release 12.2(33)SXH and later releases

August 2007

Text Part Number: OL-14149-01-J

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

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

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

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

Catalyst 6500 シリーズ スイッチ 合法的傍受 コンフィギュレーション ガイド

CONTENTS

はじめに

このマニュアルでは、Catalyst 6500 シリーズ スイッチに Lawful Intercept（LI; 合法的傍受）機能を実装する方法について説明します。

LI とは、Law Enforcement Agency（LEA; 法執行機関）が、裁判所の命令による権限に基づいて、個人に対して電子的サーベイランスを実行するプロセスのことです。サービス プロバイダーはこのサーベイランスを援助するために、ターゲットのトラフィックがサービス プロバイダーのルータを通過する際に傍受を行い、傍受したトラフィックのコピーをターゲットに知られることなく LEA に送信します。

対象読者

このマニュアルは、LI をサポートするようにルータを設定する必要のあるシステム管理者を対象にしています。また、LI と併用する管理アプリケーションを開発するアプリケーション開発者にも役立ちます。

マニュアルの構成

このマニュアルの内容は、次のとおりです。

- 第 1 章「LI の概要」では、LI とその実装に関する背景情報について説明します。また、LI に使用される CISCO-TAP2-MIB と CISCO-IP-TAP-MIB についても説明します。MIB（管理情報ベース）を使用すると、SNMP（簡易ネットワーク管理プロトコル）を使用してルータを制御できます。
- 第 2 章「LI のサポートの設定」では、ルータで LI をサポートするための設定手順について説明します。

表記法

このマニュアルのコマンドの説明では、次の表記法を使用しています。

太字	コマンド、ユーザ入力、およびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数および新しい用語は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。

例では、次の表記法を使用しています。

screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の **screen** フォント	ユーザが入力しなければならない情報は、**太字**の **screen** フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

注釈および注意は次の表記法を使用しています。

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

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

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨するエイリアスと一般的なシスコのマニュアルに関する情報については、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。『*What's New in Cisco Product Documentation*』には、シスコの新規および改訂版の技術マニュアルの一覧が示されています。この情報には、次の URL からアクセスしてください。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Japan TAC Web サイト

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

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

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

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

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

CHAPTER 1

LI の概要

この章では、Lawful Intercept（LI; 合法的傍受）について説明します。内容は次のとおりです。

注意 このマニュアルでは、LI の実装に関する法律上の義務については扱っていません。サービス プロバイダーには、自社のネットワークが、適用される LI の法規制に準拠していることを確認する責任があります。専門家に相談して、法律上の義務について確認することを推奨します。

LI の概要

LI とは、Law Enforcement Agency（LEA; 法執行機関）が、裁判所または行政の命令による権限に基づいて、個人（ターゲット）に対して電子的サーベイランスを実行するプロセスのことです。LI のプロセスを容易にするため、特定の法規制により、Service Provider（SP; サービス プロバイダー）および Internet Service Provider（ISP; インターネット サービス プロバイダー）は、認可された電子的サーベイランスを自社のネットワーク上で明示的にサポートすることが定められています。

このサーベイランスを実行するには、音声、データ、およびマルチサービス ネットワークの、従来の通信サービスおよびインターネット サービス上で通信傍受を行います。LEA は、ターゲットのサービス プロバイダーに対して通信傍受の要請を行います。サービス プロバイダーは個人に送受信されるデータ通信を傍受する責任があります。サービス プロバイダーは、ターゲットの IP アドレスから、ターゲットのトラフィック（データ通信）を処理しているエッジ Catalyst 6500 シリーズ スイッチを判別します。サービス プロバイダーは、ターゲットのトラフィックがこの Catalyst 6500 シリーズ スイッチを通過する際に傍受を行い、傍受したトラフィックのコピーをターゲットに知られることなく、LEA に送信します。

LI 機能は、米国内のサービス プロバイダーに求められる LI のサポート方法を定めた Communication Assistance for Law Enforcement Act（CALEA）に準拠しています。現在、LI は次の標準規格により定義されています。

- Telephone Industry Association（TIA）仕様 J-STD-025
- Packet Cable Electronic Surveillance Specification（PKT-SP-ESP-101-991229）

シスコの LI ソリューションの詳細については、シスコの代理店にお問い合わせください。

（注） LI 機能は、音声とデータの傍受を含む CISCO-IP-TAB-MIB のオブジェクト citapStreamprotocol の定義に従って、IPv4 プロトコルの傍受をサポートします。

LI の利点

LI には、次の利点があります。

- 複数の LEA が、互いに知ることなく、同じターゲットに対して LI を実行できます。
- Catalyst 6500 シリーズ スイッチの加入者サービスに影響を与えません。
- 通信傍受を入力と出力の両方向でサポートします。
- レイヤ 1 およびレイヤ 3 トラフィックの通信傍受をサポートします。レイヤ 2 トラフィックは VLAN（仮想 LAN）上の IP トラフィックとしてサポートされます。
- 1 つの物理インターフェイスを共有する個々の加入者に対する通信傍受をサポートします。
- ターゲットは LI を検知できません。ネットワーク管理者も通話当事者も、パケットがコピーされていることや通話が傍受されていることに気付きません。
- SNMPv3（簡易ネットワーク管理プロトコル Verison 3）、および View-based Access Control Model（SNMP-VACM-MIB）や User-based Security Model（SNMP-USM-MIB）などのセキュリティ機能を使用して、LI の情報およびコンポーネントへのアクセスを制限できます。
- LI に関する情報へのアクセスを、最高特権を持つユーザだけに限定できます。管理者は、特権ユーザが LI 情報にアクセスできるように、アクセス権を設定する必要があります。
- 2 つのセキュリティ インターフェイスを使用して、傍受を実行できます。1 つは通信傍受を設定するインターフェイス、もう 1 つは傍受したトラフィックを LEA に送信するインターフェイスです。

CALEA for Voice

CALEA for Voice 機能により、VoIP 上で行われている音声通話の LI が可能です。Catalyst 6500 シリーズ スイッチは音声ゲートウェイ デバイスではありませんが、VoIP パケットは、サービス プロバイダーのネットワークのエッジにある Catalyst 6500 シリーズ スイッチを通過します。

認可された政府機関により通話が傍受の対象になると判断されると、CALEA for Voice 機能によりこの通話の IP パケットがコピーされて、詳しく分析するために、適切なモニタリング デバイスに送信されます。

LI に使用するネットワーク コンポーネント

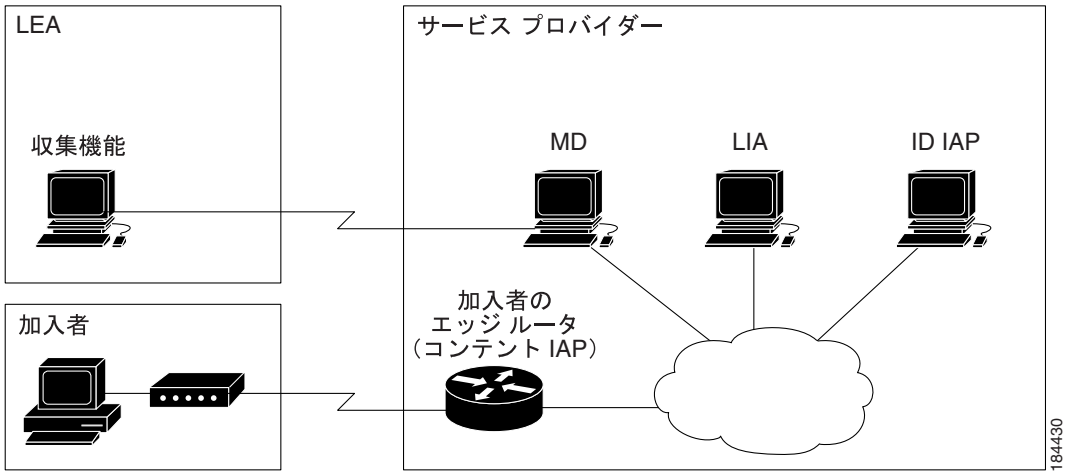
LI では、次のネットワーク コンポーネントを使用します。

- MD
- LIA
- IAP
- コンテント IAP

LI のプロセスについては、「LI のプロセス」（p.1-6）を参照してください。

図 1-1 に、LI モデルの概要を示します。

図 1-1　LI の概要



MD

LI のほとんどのプロセスは、Mediation Device（MD; メディエーション デバイス）（サードパーティ ベンダー製）によって処理されます。MD は、次の機能を実行します。

- LI の設定およびプロビジョニングのためのインターフェイスを提供します。
- 他のネットワーク デバイスに対して、LI の設定と実行を要求します。
- 傍受したトラフィックを LEA が要求する形式（国により異なる）に変換し、このトラフィックのコピーをターゲットに知られることなく LEA に送信します。

（注） 複数の LEA が同じターゲットを傍受している場合、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。また、障害によって中断された LI を再開するのも MD の役割です。

LIA

Lawful Intercept Administration（LIA）は、LI または通信傍受の要求および管理のための認証インターフェイスを提供します。

IAP

Intercept Access Point（IAP）は、LI の情報を提供するデバイスです。IAP には、次の 2 種類があります。

- Identification（ID）IAP ― 傍受に必要な Intercept-Related Information（IRI; 傍受関連情報）（ターゲットのユーザ名、システム IP アドレスなど）、または VoIP に必要なコール エージェントを提供する Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバなどのデバイス。IRI の情報により、サービス プロバイダーはターゲットのトラフィックが通過するコンテント IAP（Catalyst 6500 シリーズ スイッチ）を特定します。
- コンテント IAP ― ターゲットのトラフィックが通過する、Catalyst 6500 シリーズ スイッチなどのデバイス。コンテント IAP には次の機能があります。
  - 裁判所の命令により指定された期間、ターゲットの送受信トラフィックを傍受します。Catalyst 6500 シリーズ スイッチは、宛先にトラフィックの転送を続けて、通信傍受が検知されないようにします。
  - 傍受したトラフィックのコピーを作成し、UDP パケットにカプセル化し、このパケットをターゲットに知られることなく MD に転送します。IP オプション ヘッダーはサポートされません。

（注） コンテント IAP は、MD に、傍受したトラフィックのコピーを 1 つ送信します。複数の LEA が同じターゲットを傍受している場合、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。

コンテント IAP

コンテント IAP は、対象となるデータ ストリームを傍受してコンテントを複製し、MD に送信します。MD は ID IAP およびコンテント IAP からデータを受信し、要求された形式（国により異なる）に変換して LEA に送信します。

LI のプロセス

LEA は、裁判所からサーベイランスを実行する命令または令状を取得したあと、ターゲットが加入しているサービス プロバイダーにサーベイランスを要請します。サービス プロバイダーの担当者は、MD で管理機能を実行して、（裁判所命令に従い）ターゲットの電子トラフィックを特定の期間モニタリングするために LI の設定を行います。

傍受を設定したあとは、ユーザが介入する必要はありません。管理機能が他のネットワーク デバイスと通信し、LI の設定を行って実行します。LI では、次の一連の処理が行われます。

1. 管理機能は ID IPA と通信し、ターゲットのユーザ名やシステム IP アドレスなどの IRI を取得し、ターゲットのトラフィックが通過するコンテント IAP（Catalyst 6500 シリーズ スイッチ）を特定します。
2. ターゲットのトラフィックを処理する Catalyst 6500 シリーズ スイッチが特定されると、管理機能により、その Catalyst 6500 シリーズ スイッチの MIB（管理情報ベース）に対して **get** および **set** 要求が送信され、LI が設定されてアクティブになります。CISCO-TAP2-MIB は、加入者ごとの傍受がサポートされている LI MIB です。
3. LI の間に、Catalyst 6500 シリーズ スイッチは次の機能を実行します。
   a. 着信および発信トラフィックを調べ、LI 要求の条件に一致するすべてのトラフィックを傍受します。
   b. 傍受したトラフィックのコピーが作成され、元のトラフィックはそのまま宛先に転送されるので、ターゲットに気付かれることはありません。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、このパケットをターゲットに知られることなく MD に転送します。

（注） ターゲットのトラフィックの傍受および複製の処理によって、トラフィック ストリームに検知可能な遅れが生じることはありません。

4. MD は、この傍受したトラフィックを要求された形式に変換し、LEA で稼働している収集機能に送信します。傍受したトラフィックは、ここで格納され処理が行われます。

（注） 裁判所命令で許可されていないトラフィックを Catalyst 6500 シリーズ スイッチが傍受した場合は、MD により不要なトラフィックがフィルタリングされ、裁判所命令で許可されたトラフィックのみが LEA に送信されます。

5. LI の期間が終了すると、Catalyst 6500 シリーズ スイッチはターゲットのトラフィックの傍受を停止します。

LI MIB

LI を実行するために、Catalyst 6500 シリーズ スイッチは次の MIB を使用します。これらの MIB については、次のセクションで説明します。

- CISCO-TAP2-MIB ― LI のプロセスに使用します。
- CISCO-IP-TAP-MIB ― レイヤ 3（IPv4）トラフィックの傍受に使用します。

CISCO-TAP2-MIB

CISCO-TAP2-MIB には、Catalyst 6500 シリーズ スイッチ上の LI を制御する SNMP 管理オブジェクトが含まれています。MD はこの MIB を使用して、トラフィックが Catalyst 6500 シリーズ スイッチを通過するターゲットに対して LI を設定し、実行します。

CISCO-TAP2-MIB には、Catalyst 6500 シリーズ スイッチ上で実行される LI の情報を提供するための複数のテーブルが含まれています。

- cTap2MediationTable ― 現時点で、Catalyst 6500 シリーズ スイッチ上で LI を実行している各 MD に関する情報が含まれています。テーブルの各エントリには、Catalyst 6500 シリーズ スイッチが MD と通信するための情報（デバイスのアドレス、傍受したトラフィックを送信するインターフェイス、傍受したトラフィックの転送に使用するプロトコルなど）が含まれています。
- cTap2StreamTable ― 傍受するトラフィックを特定するための情報が含まれています。テーブルの各エントリには、LI のターゲットに関連するトラフィック ストリームを特定するための、フィルタへのポインタが含まれています。フィルタに一致するトラフィックが傍受され、コピーされて、対応する MD のアプリケーション（cTap2MediationContentId）に送信されます。

  cTap2StreamTable テーブルには、傍受したパケット数および傍受対象であっても傍受されなかった廃棄パケット数のカウントも含まれています。
- cTap2DebugTable ― LI のエラーをトラブルシューティングするためのデバッグ情報が含まれています。

CISCO-TAP2-MIB には、LI イベントに関する SNMP 通知も含まれています。MIB オブジェクトの詳細な説明については、MIB を参照してください。

CISCO-TAP2-MIB のプロセス

管理機能（MD 上で実行）により、Catalyst 6500 シリーズ スイッチの CISCO-TAP2-MIB に対し SNMPv3 の **set** および **get** 要求が発行され、LI が設定および開始されます。具体的には、次の処理が行われます。

1. cTap2MediationTable のエントリを作成し、Catalyst 6500 シリーズ スイッチと傍受を実行する MD との通信方法を定義します。

   （注） cTap2MediationNewIndex オブジェクトは、メディエーション テーブル エントリの固有のインデックスです。

2. cTap2StreamTable にエントリを作成し、傍受するトラフィック ストリームを特定します。
3. cTap2StreamInterceptEnable を true(1) に設定して、傍受を開始します。Catalyst 6500 シリーズ スイッチは、傍受期間（cTap2MediationTimeout）が終了するまでストリーム内のトラフィックを傍受します。

CISCO-IP-TAP-MIB

CISCO-IP-TAP-MIB には、Catalyst 6500 シリーズ スイッチを通過する IPv4 トラフィック ストリームに対して LI を設定および実行するための SNMP 管理オブジェクトが含まれています。この MIB は CISCO-TAP2-MIB の拡張版です。

CISCO-IP-TAP-MIB を使用して Catalyst 6500 シリーズ スイッチに LI を設定し、次の 1 つまたは複数のフィールドの値と一致する IPv4 パケットを傍受できます。

- 宛先 IP アドレスおよびマスク
- 宛先ポート範囲
- 発信元 IP アドレスおよびマスク
- 発信元ポート範囲
- プロトコル ID

CISCO-IP-TAP-MIB のプロセス

データを傍受する場合は 2 つのストリームが作成されます。1 つは、任意のポートを使用してターゲット IP アドレスから任意の IP アドレスに発信されるパケットのストリームです。もう 1 つは、任意のポートを使用して任意のアドレスからターゲット IP アドレスにルーティングされるパケットのストリームです。VoIP の場合も 2 つのストリームが作成されます。1 つは、ターゲットからの RTP パケットのストリームです。もう 1 つは、特定の発信および宛先 IP アドレスとポートからターゲットに向かう RTP パケットのストリームで、IP アドレスとポートは RTP ストリームのセットアップに使用する SDP 情報で指定します。

CHAPTER 2

LI のサポートの設定

この章では、Lawful Intercept（LI; 合法的傍受）の設定方法について説明します。不正ユーザが LI を実行したり、傍受に関連する情報にアクセスしたりできないようにする必要があります。

この章の内容は、次のとおりです。

前提条件

LI のサポートを設定するには、次の前提条件を満たす必要があります。

- Secure Shell（SSH; セキュア シェル）をサポートするイメージを実行していること。たとえば、イメージ s72033-adventerprisek9-mz です。SSH をサポートしないイメージでは LI はサポートされません。
- Catalyst 6500 シリーズ スイッチには、最高レベルのアクセス権（レベル 15）でログインする必要があります。レベル 15 のアクセス権でログインするには、**enable** コマンドを入力し、Catalyst 6500 シリーズ スイッチに定義されている最高レベルのパスワードを指定します。
- CLI（コマンドライン インターフェイス）を使用して、グローバル コンフィギュレーション モードでコマンドを入力する必要があります。すべてのインターフェイスまたは特定のインターフェイスで、LI をグローバルに設定できます。
- Supervisor Engine 720 または Supervisor Engine 720-10GE（PFC3A、PFC3B、PFC3BXL、PFC3C、PFC3CXL をサポート）を搭載した Catalyst 6500 シリーズで、LI はサポートされます。
- Catalyst 6500 シリーズ スイッチと Mediation Device（MD; メディエーション デバイス）の時刻が同期されていること。Catalyst 6500 シリーズ スイッチと MD の両方で Network Time Protocol（NTP）を使用することを推奨します。
- （任意）Catalyst 6500 シリーズ スイッチが MD との通信に使用するインターフェイスに、ループバック インターフェイスを使用すると役立つことがあります。ループバック インターフェイスを使用しない場合は、Catalyst 6500 シリーズ スイッチの複数の物理インターフェイスを使用して MD を設定し、ネットワーク障害に対処する必要があります。

セキュリティに関する考慮事項

Catalyst 6500 シリーズ スイッチに LI を設定する際は、次のセキュリティ事項を考慮してください。

- LI の SNMP 通知は、MD の UDP ポート 162（SNMP のデフォルト）ではなく、ポート 161 に送信する必要があります。手順については、「LI の SNMP 通知のイネーブル化」（p.2-8）を参照してください。
- LI MIB にアクセスできるユーザは、Catalyst 6500 シリーズ スイッチ上の LI について知る必要性のあるシステム管理者と MD に制限する必要があります。これらのユーザには、authPriv または authNoPriv アクセス権限を付与して LI MIB にアクセスできるようにする必要があります。NoAuthNoPriv アクセス権を所有するユーザは、LI MIB にアクセスできません。
- SNMP-VACM-MIB を使用して、LI MIB を含むビューを作成することはできません。
- デフォルトの SNMP ビューでは、次の MIB が除外されています。

  CISCO-TAP2-MIB
  CISCO-IP-TAP-MIB
  SNMP-COMMUNITY-MIB
  SNMP-USM-MIB
  SNMP-VACM-MIB

その他の考慮事項については、「設定時の注意事項および制約事項」を参照してください。また、「前提条件」（p.2-2）も参照してください。

設定時の注意事項および制約事項

これ以降では、LI に関する一般的な制約事項と設定時の注意事項、Catalyst 6500 シリーズ スイッチに固有の注意事項、および加入者単位の注意事項について説明します。

- ネットワーク管理者が LI を配置するノードに、Optimized ACL Logging（OAL）、VLAN Access Control List（ACL; アクセス コントロール リスト）キャプチャ、Intrusion Detection System（IDS; 侵入検知システム）を設定することはできません。ノードに LI を配置すると、OAL、VACL キャプチャ、IDS の動作が予測不能になります。
- Catalyst 6500 シリーズ スイッチのパフォーマンスを維持するため、LI はアクティブ コールの 0.2% 以下に制限されています。たとえば、Catalyst 6500 シリーズ スイッチが 4000 コールを処理している場合、これらのうち 8 コールを傍受できます。
- CISCO-IP-TAP-MIB は、Virtual Routing and Forwarding（VRF）の OID citapStreamVRF をサポートしていません。
- キャプチャされたトラフィックの速度は、ルート プロセッサの CPU 使用状況を保護するために 8,500 pps に制限されます。
- プロビジョニング時にはインターフェイス インデックスが使用され、LI を有効にするインデックスだけが選択されます。0 に設定するとすべてのインターフェイスで LI が有効になります。

設定時の一般的な注意事項

Catalyst 6500 シリーズ スイッチが MD と通信して LI を実行するには、次の設定要件を満たす必要があります。

- （任意）Catalyst 6500 シリーズ スイッチと MD の両方のドメイン名が、Domain Name System（DNS; ドメイン ネーム システム）に登録できます。

  DNS では、Catalyst 6500 シリーズ スイッチの IP アドレスは通常、Catalyst 6500 シリーズ スイッチ上の FastEthernet0/0/0 インターフェイスのアドレスです。
- MD には Access Function（AF）が必要です。
- CISCO-TAP2-MIB ビューにアクセスできる SNMP（簡易ネットワーク管理プロトコル）ユーザ グループに MD を追加する必要があります。このグループに追加するユーザの名前には、MD のユーザ名を指定します。

  CISCO-TAP2-MIB のユーザとして MD を追加する場合は、MD の許可パスワードを指定する必要があります。パスワードは 8 文字以上の長さにします。

MIB の注意事項

LI のプロセスでは、次の Cisco MIB が使用されます。これらの MIB を LI MIB の SNMP ビューに含めることで、MD が、Catalyst 6500 シリーズ スイッチを通過するトラフィックに対して通信傍受を設定および実行できるようにする必要があります。

- CISCO-TAP2-MIB ― レギュラーとブロードバンドの両タイプの LI に必要です。
- CISCO-IP-TAP-MIB ― レイヤ 3（IPv4）ストリームに対する通信傍受に必要です。レギュラーおよびブロードバンドの LI に対応しています。CISCO-IP-TAB-MIB には、次の機能に対する制限があります。
  - 次の 1 つまたはすべての機能が設定され正しく動作しており LI がイネーブルの場合、LI が優先され、機能は次のように動作します。

    ・OAL ― 機能しません。

    ・VACL キャプチャ ― 正しく機能しません。

    ・IDS ― 正しく機能しません。

    機能を有効にするには、LI を無効にするか設定解除します。

　－ IDS は単独でトラフィックをキャプチャすることはできず、LI により傍受されたトラフィックのみをキャプチャできます。

設定時の注意事項および制約事項

次に、Catalyst 6500 シリーズ スイッチの LI 設定時の注意事項を示します。この注意事項は、すべての非アクセス（加入者）サブインターフェイス上での LI のプロセスに適用されます。

- Supervisor Engine 720 または Supervisor Engine 720-10GE（PFC3A、PFC3B、PFC3BXL、PFC3C、PFC3CXL をサポート）が必要です。

（注） 1 つのインターフェイスを LI のプロセス専用にすることを推奨します。たとえば、そのインターフェイスでプロセッサを集中的に使用するタスク（QoS やルーティングなど）を実行しないように設定します。

- IPv4 ユニキャスト トラフィックのみをサポートします。また、傍受対象のトラフィックは、入力と出力の両方のインターフェイスで IPv4 である必要があります。たとえば、出力側が MPLS で、入力側が IPv4 の場合は、トラフィックを傍受できません。
- IPv4 マルチキャスト、IPv6 ユニキャスト、および IPv6 マルチキャスト フローはサポートされません。
- レイヤ 2 インターフェイス上ではサポートされません。ただし、レイヤ 2 インターフェイス上で動作する VLAN 上のトラフィックは傍受できます。
- 他のパケットでカプセル化されたパケット（トンネル パケットや Q-in-Q パケットなど）はサポートされません。
- Q-in-Q パケットはサポートされません。LI ではレイヤ 2 傍受はサポートされません。
- レイヤ 3 またはレイヤ 4 での書き換えが行われるパケット（Network Address Translation［NAT; ネットワーク アドレス変換］や TCP リフレクシブ）はサポートされません。
- 入力方向では、（レート制限または ACL **deny** ステートメントなどにより）あとになって廃棄されるパケットであっても、Catalyst 6500 シリーズ スイッチはパケットを傍受し複製します。出力方向では、パケットが（ACL などにより）廃棄されると複製されません。
- LI ACL は、インターエイス内部で入力と出力の両方向に適用されます。
- 特定のユーザからのトラフィックを傍受するには、通常それぞれの方向のフローが設定されます。
- ハードウェアのレート リミットの対象になるパケットは、LI で次のように処理されます。
  - レート リミットにより廃棄されるパケットは、傍受または処理されません。
  - レート リミッタが通過させたパケットは、傍受および処理されます。
- 複数の LEA が 1 つの MD を使用し、それぞれが同じターゲットに対する通信傍受を実行している場合、Catalyst 6500 シリーズ スイッチは 1 つのパケットを MD に送信します。各 LEA にパケットを複製するのは MD の役割です。
- Catalyst 6500 シリーズ スイッチ上の LI は、次の 1 つまたは複数のフィールドの組み合わせに一致する値を持つ IPv4 パケットを傍受できます。
  - 宛先 IP アドレスおよびマスク
  - 宛先ポート範囲
  - 発信元 IP アドレスおよびマスク
  - 発信元ポート範囲
  - プロトコル ID

LI MIB へのアクセス

機密情報の扱いに関わることから、シスコの LI MIB は、LI 機能をサポートするソフトウェア イメージの形でのみ提供されています。これらの MIB は、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

LI MIB へのアクセスの制限

LI MIB へのアクセスは、MD および LI について知る必要性のあるユーザのみに許可されます。これらの MIB へのアクセスを制限するには、次の作業を行います。

1. シスコの LI MIB を含むビューを作成します。
2. このビューへの読み書きアクセス権限を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザのみが MIB の情報にアクセスできます。
3. シスコの LI ユーザ グループにユーザを追加して、MIB および LI に関連する情報にアクセスできるユーザを定義します。このグループのユーザとして、必ず MD を追加してください。これを行わないと、Catalyst 6500 シリーズ スイッチで LI を実行できません。

（注） シスコの LI MIB ビューへのアクセスは、Catalyst 6500 シリーズ スイッチ上の LI について知る必要性のあるシステム管理者と MD に制限する必要があります。MIB にアクセスするには、Catalyst 6500 シリーズ スイッチ上でレベル 15 のアクセス権限を所有している必要があります。

SNMPv3 の設定

次の手順を実行するには、Catalyst 6500 シリーズ スイッチに SNMPv3 が設定されている必要があります。SNMPv3 の設定方法および以降のセクションで説明するコマンドの詳細情報については、次のシスコのマニュアルを参照してください。

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』Part 3: System Management の「Configuring SNMP Support」。次の URL から入手できます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm
- 『*Cisco IOS Configuration Fundamentals and Network Management Command Reference*』。次の URL から入手できます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

LI MIB を含む、制限付き SNMP ビューの作成

シスコの LI MIB を含む SNMP ビューを作成して、ユーザを割り当てるには、CLI のグローバル コンフィギュレーション モードでレベル 15 のアクセス権限を使用して、次の手順を実行します。コマンドの例については、「設定例」（p.2-7）を参照してください。

（注） 次の手順のコマンド構文には、各作業の実行に必要なキーワードのみが示されています。コマンド構文の詳細については、前のセクション（「SNMPv3 の設定」）に記載されているマニュアルを参照してください。

ステップ 1　Catalyst 6500 シリーズ スイッチに SNMPv3 が設定されていることを確認します。詳細については、「SNMPv3 の設定」（p.2-6）に記載されているマニュアルを参照してください。

ステップ 2　CISCO-TAP2-MIB を含む SNMP ビューを作成します（*view_name* は、MIB 用に作成するビューの名前です）。この MIB は、レギュラーとブロードバンドの両方の LI に必要です。

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

ステップ 3　SNMP ビューに次の MIB の 1 つまたは両方を追加して、IPv4 ストリームに対する通信傍受のサポートを設定します（*view_name* は、ステップ 2 で作成したビューの名前）。

```
Router(config)# snmp-server view view_name ciscoIpTapMIB included
```

ステップ 4　LI MIB ビューにアクセスできる SNMP ユーザ グループ（*groupname*）を作成し、このグループのビューへのアクセス権限を定義します。

```
Router(config)# snmp-server group groupname v3 noauth read view_name
write view_name
```

ステップ 5　作成したユーザ グループにユーザを追加します（*username* はユーザ名、*groupname* はユーザ グループ名、および *auth_password* は認証パスワード）。

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

（注） この SNMP ユーザ グループに、必ず MD を追加してください。これを行わないと、Catalyst 6500 シリーズ スイッチで LI を実行できません。LI MIB ビューへのアクセスは、Catalyst 6500 シリーズ スイッチ上の LI について知る必要性のあるシステム管理者と MD に制限する必要があります。

これで MD は LI MIB にアクセスして、SNMP **set** および **get** 要求を発行し、Catalyst 6500 シリーズ スイッチ上で LI を設定および実行することができるようになります。

MD に SNMP 通知を送信するための Catalyst 6500 シリーズ スイッチの設定方法については、「LI の SNMP 通知のイネーブル化」（p.2-8）を参照してください。

設定例

次に、MD が LI MIB にアクセスできるように設定する例を示します。

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
Router(config)# snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server engineID local 1234
```

1. 該当する LI MIB（CISCO-TAP2-MIB および CISCO-IP-TAP-MIB）を含むビュー（tapV）を作成します。
2. tapV ビューの MIB への読み取り、書き込み、および通知のアクセス権限を持つユーザ グループ（tapGrp）を作成します。
3. このユーザ グループに MD（ss8user）を追加し、パスワード（ss8passwd）を設定して、MD5 認証を指定します。
4. （任意）Catalyst 6500 シリーズ スイッチに管理用の 24 文字の SNMP エンジン ID（123400000000000000000000 など）を割り当てます。指定しない場合は、エンジン ID が自動的に生成されます。上記の例の最後の行にあるように、エンジン ID の後続のゼロは省略できます。

（注） エンジン ID を変更すると、SNMP ユーザのパスワードおよびコミュニティ ストリングにも影響します。

LI の SNMP 通知のイネーブル化

SNMP は、LI イベントの通知を自動的に生成します（表 2-1 を参照）。
これは、cTap2MediationNotificationEnable オブジェクトが、デフォルトで true(1) に設定されているためです。

MD に LI 通知を送信するように Catalyst 6500 シリーズ スイッチを設定するには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権限を使って、次の CLI コマンドを発行します（*MD-ip-address* は MD の IP アドレス。*community-string* は通知要求と一緒に送信されるパスワードに似たコミュニティ ストリング）。

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
Router(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
```

- LI の場合、**upd-port** は 162（SNMP のデフォルト）ではなく、161 に設定します。
- 2 番めのコマンドでは、Catalyst 6500 シリーズ スイッチが RFC 1157 規定の通知を MD に送信するように設定しています。これらの通知は、認証エラー、リンク ステータス（アップまたはダウン）、およびシステムの再起動を知らせます。

表 2-1 に、LI イベントで生成される SNMP 通知を示します。

表 2-1　LI イベントの SNMP 通知

通知	意味
cTap2MIBActive	Catalyst 6500 シリーズ スイッチは、CISCO-TAP2-MIB に設定されたトラフィック ストリームのパケットを傍受する準備ができています。
cTap2MediationTimedOut	LI が終了しました（cTap2MediationTimeout の時間切れなど）。
cTap2MediationDebug	cTap2MediationTable エントリに関するイベントには、対処が必要です。
cTap2StreamDebug	cTap2StreamTable エントリに関するイベントには、対処が必要です。

SNMP 通知のディセーブル化

SNMP 通知をディセーブルにするには、**no snmp-server enable traps** コマンドを使用します。

LI 通知をディセーブルにするには、SNMPv3 を使用して、CISCO-TAP2-MIB オブジェクトの cTap2MediationNotificationEnable を false(2) に設定します。LI 通知を再びイネーブルにするには、SNMPv3 を使用して、このオブジェクトを true(1) に戻します。

INDEX

い

か

こ

さ

し

す

せ

つ

て

と

ひ

ほ

め