

Cisco IOS ソフトウェアの機能

レイヤ2 トンネリングプロトコル

アクセスVPNのためのビルディングブロック

概要

シスコは、アクセスVPN(仮想プライベートネットワーク)を、有望なアイデアから現実のものにするための技術提供で業界をリードしています。L2TP(レイヤ2トンネリングプロトコル)をCisco IOS®ソフトウェアに組み込むことによって、シスコではアクセスVPN接続のための標準方式を提案します。シスコのエンドツーエンドハードウェアおよびCisco IOSソフトウェアネットワークワーキング製品は、パブリックなインフラストラクチャを利用したプライベート伝送に対して、高度な安全性を提供します。この中には、トラフィックの差別化によるQoS、重要アプリケーションの信頼性、データの広帯域幅サポートのスケラビリティ、およびアクセスVPNソリューション全体を対象にした包括的なネットワーク管理が含まれます。

VPNは、企業のスタッフが頻繁に移動することがあっても、自社のイントラネットやエクストラネットに場所や時を選ばず必要などきにいつでも接続できるようにして、アクセスコストを削減すると同時に生産性と柔軟性を向上させます。

企業のイントラネットやエクストラネットに低いコストで容易にアクセスできる方法を提供するために、アクセスVPNでは、インターネットのような共有インフラストラクチャ上でプライベートネットワークのシミュレーションを行います。アクセスVPNは、モバイルユーザー、在宅勤務者、小規模のオフィスに対して、ダイヤル、ISDN、xDSL、モバイルIP、およびケーブルなどの技術を利用したアクセスを可能にします。

アクセスVPNの主要なビルディングブロックは、L2TP(レイヤ2トンネリングプロトコル)です。これは、PPP(ポイントツーポイントプロトコル)を拡張したものになっています。L2TPは、シスコのL2F(レイヤ2フォワーディング)とマイクロソフト社のPPTP(Point-to-Point Tunneling Protocol)の2つのトンネリングプロトコルの重要な機能を統合しています。L2TPはIETF(インターネット技術特別調査委員会)の標準で、現在、シスコ、マイクロソフト、アセンド、スリーコムを始めとするネットワーク業界リーダーと協同開発および認定が行われています。

L2TPの主要用語

L2TPアクセスコンセントレータ(LAC) --- LAC装置は、公衆電話交換網(PSTN)やISDNなどの交換網設備に設置されます。また、L2TPプロトコルの処理が可能なPPPエンドシステムにも設置可能です。LACには媒体の実装のみが必要です。ここでは、トラフィックを1つ以上のLNSに渡すためにL2TPを利用します。LACはPPPで転送されるすべてのプロトコルを通すことができます。LACは、着信呼のイニシエータであり、発信呼のレシーバとなります。また、LACは、レイヤ2フォワーディング(L2F)のネットワークアクセスサーバとしても用いられます。

L2TPネットワークサーバ(LNS) --- LNSは、PPP終端が適用可能なすべてのプラットフォーム上で動作します。LNSは、L2TPプロトコルのサーバサイドに対応します。L2TPは、L2TPトンネルが到着する単一のメディアのみを利用するため、1つのLANまたはWANだけを持つ場合があります。ただし、LACのPPPインタフェース(ATMにおける非同期、ISDN、PPP、フレームリレーにおけるPPP)の全範囲に到着する呼を中断することは可能です。LNSは、発信呼のイニシエータであり、着信呼のレシーバとなります。また、LNSは、L2F用語ではHGW(Home Gateway)とも呼ばれています。

ネットワークアクセスサーバ(NAS) --- このデバイスは、ユーザーへの一時的なネットワークアクセスを提供します。このアクセスはポイントツーポイントで、通常はPSTNまたはISDN回線を使用します。シスコの実装では、NASはLACとして用いられます。

シスコのアクセスVPN機能の一覧

シスコは、アクセスVPNソリューション全体を容易に展開するための幅広い技術を提供しています。

レイヤ2 トンネリングプロトコル (L2TP)

シスコのL2TP実装サポートは、L2TP標準の最新版をベースにしています。シスコは、すべての標準L2TP機能とほとんどのオプション機能をサポートしています。シスコのL2TP実装では以下が提供されます。

マルチプロトコル環境のサポート --- L2TPは、IP、IPX、およびAppletalkを含めたすべてのルーティング対象プロトコルを転送します。

媒体非依存 --- シスコのL2TP実装は、IPフレームの提供が可能なすべてのネットワーク上で動作します。L2TPは、フレームリレー、ATM、X.25、およびSONETを含めたすべてのWANバックボーン技術をサポートします。また、イーサネット、ファーストイーサネット、トークンリング、FDDIなどのLANメディアもサポートします。

安全性

L2TPは、トンネルおよびユーザー認証をサポートする、トンネリングプロトコルです。アクセスVPNのセキュリティ保護をさらに強化するために、シスコは以下の機能を提供します。

AAA(認証、権限、およびアカウントिंग)--- ここには以下が含まれます。

アクセスVPNサービスの権限を識別するためのユーザー名/パスワード、またはDNIS(Dialed Number Identification Service)

PAP、CHAP、MS-CHAP(MD4-CHAP)およびワンタイムパスワードを含めたユーザー権限サポート

IPアドレス割り当て、スタティックルータ、およびアクセスフィルタについてのユーザー別設定サポート

接続、スタート/ストップ、障害接続復帰用完全ログ情報など、LACおよびLNS上で利用可能なアカウントング

RADIUSおよびTACACS+サポート

プロキシの提供およびアクセスVPNローミングユーザー権限の解釈を行う、AAAサポートおよびCisco Secure GRS(グローバルローミングサーバ)

IPSec --- IPSecは、ネットワーク内のピア参加における、データの機密性、統合性、および信頼性を提供します。シスコは、ESP(カプセル化セキュリティペイロード)およびAH(認証ヘッダ)サポートを提供します。IPSecは、AS5300やAS5800などのネットワークアクセスサーバ、Cisco 1600や7500などのルータプラットフォーム、PIXファイアウォールといったシスコ製品から利用することができます。またIPSecは、Windows 95およびWindows NT 4.0でも、RavlinSoft IPSecソフトウェアによって利用可能になっています。

IKE --- ISAKMP(Internet Security Association Key Management Protocol)/Oakleyとも呼ばれるIKEは、セキュリティ提携管理を提供します。IKEは、IPSecトランザクション内のそれぞれのピアを認証し、セキュリティ方針を取り決め、セッションキーのやり取りを処理します。シスコは、IKE標準化をリードしています。

CET(Cisco Encryption Technology)--- CETは、ネットワークをベースとしたオリジナルの暗号化ソリューションです。

認証管理 --- シスコは、IKEに必要なデバイス認証用にX.509-V3認証の使用をサポートします。

Cisco IOS Firewallフィーチャセット --- Cisco IOS Firewall機能は、Cisco IOSソフトウェアの付加価値オプションで、既存のCisco IOSセキュリティ機能を強化します。Cisco IOS Firewallフィーチャセットには、ネットワーク接続の状態とコンテキストを追跡して、トラフィックフローの安全性を確保する、CBAC(コンテキストベースアクセス制御)が組み込まれています。また、不正とみなされるアプレットのダウンロードを制御するJavaブロック、サービス拒否の検知と回避、リアルタイムアラート、送信元/宛先アドレスとポートペアごとのユーザーアクセスを追跡するUDPトランザクションログといった機能も含まれています。

QoS(Quality of Service)--- Cisco IOSソフトウェアは、IP優先、プライオリティキューイング、カスタムキューイング、WFQ、WRR、GTS、CAR、フラグメンテーションとインターリーピング、ABR、WRED、およびBGP4優先伝搬をサポートします。該当するLNSへの複数トンネルにIP優先を活用すれば、サービスプロバイダーは企業ユーザーに、異なる帯域幅レベルで差別化したトンネルを提供することができます。

アドレスの割り当てと管理 --- L2TPは、企業ごとに管理するIPアドレスプールからの動的なIPアドレス割り当てをサポートします。このサポートには、RFC 1918に定義されるプライベートアドレスも含まれます。また、L2TPはDHCPサーバからの動的なアドレス割り当てもサポートします。Cisco IOSソフトウェアは、ネットワークアドレス変換(NAT)をサポートします。同時に、内部アドレスが外部に公表されることを防ぎます。

信頼性 --- シスコのL2TP実装は、バックアップ機能を提供します。これによって、複数のLNSピアをバックアップLNSに設定できるようになります。プライマリLNSへの接続ができない場合、NAS(LAC)がバックアップLNSとの接続を確立します。

スケーラビリティ --- シスコのL2TP実装は、LACごとの無制限セッションをサポートします。また、Cisco ルータプラットフォーム上でLNSごとに2000以上のセッションをサポートします。Cisco 6400ユニバーサルアクセスコンセントレータ(UAC)では、8000以上のセッションがサポートされます。これによって、大規模のISP、インターネットホールセラー、および企業に膨大なスケーラビリティが提供されます。

シスコのL2TP実装の負荷分散とスタック可能なLNS機能を使用する際、1つのLACと複数のLNSとの間で負荷分散が実行されます。複数のLNSに渡る統計負荷分散機能は、新たな信頼性とスケーラビリティを付加します。スタック可能なLNS機能は、マルチリンクPPPセッションへの新たなサポートを提供します。LNSの中の1つが、複数のトンネル全体のセッションごとにフラグメントされたパケットのアセンブルを管理します。

管理 --- 障害管理を強化するために、シスコのL2TP実装はIETF標準MIBに先立ち、L2TP SNMP MIBをサポートします。MIBサポートは、全障害コードおよび接続不能の原因レポートを提供します。また、L2TPには、syslogサーバに送信するメッセージのセットも含まれています。このような一連の機能によって、L2TP上に構築されたアクセスVPNのための完全なエンドツーエンドトラブルシューティングソリューションが提供されます。

L2TP アクセスVPN アーキテクチャ

ダイヤル環境では、L2TPトンネルには、ネットワークアクセスサーバ(NAS)からルータまでのNAS開始トンネルと、クライアントソフトウェアからルータまでのクライアント開始トンネルがあります。このようなルータは、トンネル終端ポイントとして動作します。

xDSL環境では、ユーザーATM PVCが、CPEから中央に位置するNAS機能まで拡張されます。これが、L2TPトンネルをLNSまで到達させます。このNAS(Cisco 6400 UACなど)がILEC/PTTによって動作してADSLサービスを提供するか、あるいは、ILECの終端でCLECまたはISPによって動作します。

利点

L2TPは標準プロトコルであるため、サービスプロバイダーや企業のネットワーク管理者は、多数のベンダーからの幅広いサービスを楽しむことができます。ベンダ間の相互運用性が、標準アクセスVPNサービスの確実で迅速な国際規模の展開を支援します。

シスコのL2TP実装は、企業ユーザーに数々の利点を提供するソリューションです。シスコのL2TP実装には以下のような利点があります。

- ミッションクリティカルなアプリケーションに対する安全性および優位性の確保
- 改良された接続性、少ないコスト、主要機能におけるリソースの変更
- ミッションクリティカルなアプリケーションを危険にさらすことなく、また企業の安全性を低下させない、柔軟でスケラブルなりモートネットワークアクセス環境

L2TPが組み込まれたCisco IOSソフトウェアを基盤としてアクセスVPNを構築することによって、サービスプロバイダーは以下のような利点を得ることができます。

- 優位な競合性を提供し、方向転換を最小限に抑え、収益性を向上させるアクセスVPNを提供、課金、管理することができます。
- Cisco IOSソフトウェアのL2TP実装を使用して、多数の異なるアーキテクチャに幅広いVPNサービスを提供する柔軟性を獲得することができます。
- パブリックなインターネットまたはサービスプロバイダーバックボーンにアクセスVPNを使用して、安全な企業規模のリモートアクセスのために差別化サービスを提供できます。

シスコのアクセスVPNの機能と利点のまとめ

機能	利点
レイヤ2トンネリングプロトコル(L2TP) L2TPは、アクセスVPN(仮想プライベートネットワーク)の展開を簡易化します。	業界標準のレイヤ2トンネリングプロトコルは、ベンダー間の相互運用性を保証し、ネットワークにおける柔軟性とサービスの利用性を向上させます。
AAAサポート シスコのAAAサポートには、Cisco IOSソフトウェアおよびCisco Secure(RADIUS、TACACS+、および変換サービス) およびローミングユーザー認証用にCisco GRS(グローバルローミングサービス)を使用します。	標準を先行するシスコの集中サーバパッケージを通して、VPNユーザー認証、柔軟な権限方針、および強力なアカウントティングを提供します。
暗号化 機密性の高いデータを保護するために、シスコは、IPSecやDES暗号化などの幅広い暗号化技術を提供します。なお、DES暗号化については、40および56ビットが現在サポートされています。将来は168ビットのサポートが計画されています。	インターネットやサービスプロバイダーのバックボーンでシスコのL2TPおよびIPSecを使用してアクセスVPNを運用して、それぞれのプライベートネットワークと同等のデータの安全性を企業に提供します。
QoS(Quality of Service) 該当するLNSへの複数トンネルにIP優先を活用すれば、サービスプロバイダーは企業ユーザーに、異なる帯域幅レベルの差別化トンネルを提供することができます。	企業ユーザーが待ち時間の影響が大きい重要なアプリケーションに必要なQoSレベルを、サービスプロバイダーが提供することを可能にします。
信頼性 バックアップLNSを用いて、複数トンネルピアの設定を行うことができます。プライマリLNSへの接続ができない場合、NAS(LAC)がバックアップLNSとの接続を確立します。	企業のアクセスVPNの信頼性とフォールトトレランスを強化し、同時にサービスプロバイダーはSLA要件を確実に満たすことができます。
LNSにおけるスケラビリティ シスコのL2TPは、LAC上の無制限セッションをサポートします。また、Ciscoルータプラットフォーム上でLNSごとに2000以上のセッションをサポートします。	VPNのスケラビリティを強化し、ユーザーの広範囲に渡る要求へのネットワークの適合を可能にします。
サイトにおけるスケラビリティ スタック可能なホームLNS機能は、1つのLACと複数のLNS間の複数L2TPトンネル全体の負荷分散によって、マルチリンクセッションのサポートも行います。	トラフィックの負荷の増加に伴う企業ユーザーまたはサービスプロバイダーからの中断を最小限に抑え、スケラビリティとパフォーマンスを強化します。
アドレス管理 DHCPサーバへのDHCPプロキシクライアントのサポート、およびプライベートアドレス使用(RFC 1918)のサポートを含めた、動的アドレス割り当てと管理をサポートします。	パブリックIPアドレスが不足する状況の回避すると同時に、プライベートアドレスによって安全性が強化されます。
ネットワーク管理 L2TP SNMP MIBおよびSYSLOGサポート(IETF標準MIBを先行して実装)	すべての標準管理コンソールからのエンドツーエンドトラブルシューティングを簡易化します。

L2TP のケーススタディ

次の3つのシナリオは、L2TPを使用したCisco IOSソフトウェアを構築することによって、企業ユーザーとサービスプロバイダーがどのようにアクセスVPNの利点を活用できるかを解説しています。

シナリオ1: 費用効果の高い企業リモートアクセス

在宅勤務者やモバイルユーザーの増加、ビジネスのグローバルな運用の必要性、およびサプライヤ、顧客、ディーラ間の強力な戦略的なリンクの構築の価値と必要性が、グローバルな企業ネットワークにおけるリモートアクセスへの膨大な需要をつくり出しています。しかし、専用のプライベートリモートアクセスインフラストラクチャの構築は高価です。このためA社では、自社のリモートユーザーとパートナーのための費用効果の高い方法を探していました。

A社は、アクセスVPNを構築し、自社のリモートアクセスリンクをアウトソーシングすることをサービスプロバイダーに依頼しました。L2TP機能を用いたCisco IOSソフトウェアは、機密性の高い内部トラフィックをサービスプロバイダーのパブリックなインフラストラクチャを利用して転送するために必要とされる安全性、信頼性、およびスケーラビリティを提供します。A社が依頼したサービスプロバイダーは、L2TPを使用して、従業員のトラフィックと、エクストラネットの外部ユーザーのトラフィックとを分離しました。またL2TPによって、パフォーマンスへの信頼性が最優先される、企業のデスクトップビデオやミッションクリティカルな顧客サービスアプリケーションのQoSを確保しています。

シナリオ2: インターネットサービスプロバイダーの競争性

インターネットの爆発的な増加による、より高速なインターネットサービスの提供へのニーズは、インターネットサービスプロバイダーにとって、チャレンジであり、また同時に好機でもあります。競争性の高いインターネット市場において、成長率を促進させ、自社の存在をより強力に誇示するために、中規模のサービスプロバイダーは新たに複数の場所にPoPを設置し、すべてのビジネスロケーションからのローカルアクセスを顧客に提供する戦略を示します。

このインターネットサービスプロバイダー(ISP)の目標は、地理的に分散したPoPの低コストのネットワークを構築および管理することです。インターネットホールセラーや電話会社、RBOC、キャリア、またはすでに分散PoPを導入している他のサービスプロバイダーからのダイヤルおよびxDSLアクセスをアウトソーシングすることによって、中規模のISPは、リソースの制限を克服すると同時に収益を上げることができます。“ホールセールインターネット”または“ホールセールアクセス”と呼ばれるこれらのアウトソーシングサービスにL2TP技術を用いれば、サービスプロバイダーの従来の音声ネットワークからインターネットダイヤルアップネットワークトラフィックを分離して、利用率の低い既存のリンクに新しい収益の方向をつくりだし、成長するISPの柔軟性を向上させることが可能になります。

シナリオ3: 音声インフラストラクチャについてのインターネット利用

インターネット利用の急増は、広域に渡る地域電話の従来の音声ネットワークに著しい負担をかけています。音声ネットワークは、通常、3分間の従来の電話による会話用につくられています。インターネット利用の平均時間はほとんどの場合、30分以上です。

インターネットにおいてVPNの展開を求める企業が増え、気軽な電子メールやWebサーフィンがビジネスアプリケーションを絶え間なく利用することになり、接続時間の長さが指数関数的に増加する危機にみまわれています。

L2TPは、データアプリケーションを音声スイッチから分割し、目的別のデータネットワークにデータを分離できるソリューションを、RBOCおよび通信事業者に提供します。

L2TPを用いたCisco IOSソフトウェアにサポートされている製品

Cisco IOS バージョン 11.3(5)AA

L2TP機能は、Cisco IOSソフトウェアバージョン11.3(5)AAに含まれています。

サポートされる製品: Cisco AS5200、AS5300、AS5800、および7200シリーズ

Cisco IOS バージョン 12.0(1)T

サポートされる製品: Cisco 1600、2500、2600、3600、4000、4500、7500、およびUAC 6400

Cisco IOS イメージ

L2TP機能は、Cisco AS5800ではIP Plusでサポートされます。Cisco AS5200およびAS5300では、IP Plus、Desktop Plus、Enterprise、Enterprise Plus、IP Plus 40、IP Plus IPS 56、Enterprise Plus 40、Enterprise Plus IPSec 56でサポートされます。Cisco 7200ルータシリーズではEnterpriseバージョンでサポートされます。

©2000 Cisco Systems, Inc. All rights reserved.

CiscoとCisco Systemsは商標です。CiscoのロゴはCisco Systems, Inc.の登録商標です。

この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。

本仕様は予告なしに変更される場合があります。



シスコシステムズ株式会社

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

E-mail: cnac@cisco.com

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルディング
TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先