

Cisco ASR 1000 シリーズ セッション ボーダー コントローラ

このドキュメントでは、分散展開モデルにおける Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの Cisco® Session Border Controller(SBC)の実装の概要について説明します。また、SBC とは何か、SBC の各種展開モデル、およびマルチメディア アプリケーションにおける SBC の役割についても簡単に説明します。Cisco ASR 1000 シリーズ ルータを SBC 分散展開モデルの Data Border Element(DBE)として使用する際のルータの機能について説明します。

SBC の概要

SBC 機能は、企業およびサービス プロバイダーの VoIP およびマルチメディア ネットワークの相互接続に使用される重要なコンポーネントとして、Voice over IP (VoIP) 業界で広く普及しています。

SBC は、企業およびサービス プロバイダーのネットワーク間の IP 本位の安全な相互接続に対する需要の急増に対応するものですが、ここでは、インテリジェントなボーダー エlement機能が強く求められています。SBC を使用すれば、プロトコル、ネットワークの到達可能性、またはネットワークのセキュリティに関する不安を抱くことなく、音声またはビデオ コールを使用できます。このような Elementは、物理的および論理的な入力および出力境界、シグナリングとメディア制御、統合されたセキュリティ、および管理機能を提供します。ある意味で SBC は、シグナリング インターワーキング、ネットワーク隠蔽、セキュリティ、Quality of Service (QoS)などの機能のツールキットとも言えます。

SBC により、複数のネットワークを単純かつ費用有効な方法で接続できます。これにより、直接の IP シグナリングとメディア相互接続が提供されるため、コストおよびパフォーマンス遅延が減少し、マルチメディア セッションのメディア品質が向上します。さらに、従来の時分割多重化 (TDM) からユニファイド コミュニケーション サービスへの移行における柔軟性も向上します。

VoIP の直接相互接続における課題

サービス プロバイダー間の音声コールの接続では、一般的に TDM による相互接続が使用されています。VoIP テクノロジーの台頭に伴い、IP 電話から発信されたコールを最初から最後までパケット ネットワーク上で処理できるように、サービス プロバイダーは他のネットワークとの接続に IP 接続を使用し始めています。ここで、サービス プロバイダーは他のサービス プロバイダーとの VoIP コールの受け渡しに関する新しい課題に直面することになります。

プロトコル、IP アドレス、コーデック、Dual Tone Multifrequency (DTMF)トラフィックの搬送方法など、環境条件は VoIP 加入者ごとに異なるため、2 つのネットワーク ドメインの相互接続は非常に困難なものになる可能性があります。また、プロバイダーは自身のネットワークを他のプロバイダーネットワークから保護したいと考えています。さらに、サービス プロバイダーは、呼詳細レコード (CDR)、課金記録、音声コールの品質、トラブルシューティング、および機能の相互作用などに関する問題にも直面しています。これらすべてにより、エンドツーエンドの VoIP のパフォーマンスの実現は非常に困難な課題となります。

VoIP 相互接続における SBC の役割

VoIP、ビデオ ストリーミング、インスタント メッセージング、マルチメディア会議、および対話型ゲームは、競争熾烈な現在のコミュニケーション市場で急成長を示しているリアルタイムの IP ベース アプリケーションのほんの数例にすぎません。サービス プロバイダーは、自身のリアルタイム VoIP およびマルチメディア ネットワークを、自社の加入者だけでなく、他のサービス プロバイダーのネットワークとも直接に接続することが効率的かつ経済的であることを認識し始めています。この状況下で、サービス プロバイダーは、IP ネットワーク間の境界上でリアルタイムのマルチメディア コミュニケーション セッションを制御および管理するための SBC を必要としています。さらに、SBC は以下のような用途にも使用されます。

- VoIP およびビデオなどのリッチメディア展開を管理できるように、サービス プロバイダー間、または企業とサービス プロバイダーの間に適切な境界点を作成する
- セキュリティ上の理由から、内部ネットワークのトポロジをピアリング パートナーまたは外界に対して隠蔽する
- SBC を使用して、H.323 と SIP、または SIP と SIP の間でプロトコルのインターワーキングを提供する(SIP の標準および実装は急激に変わりつつあるため)
- メディアの変換、VoIP トラフィックのファイアウォール経由のルーティング、Network Address Translation(NAT; ネットワーク アドレス変換)および Port Address Translation(PAT; ポート アドレス変換)の実行、および QoS の適用

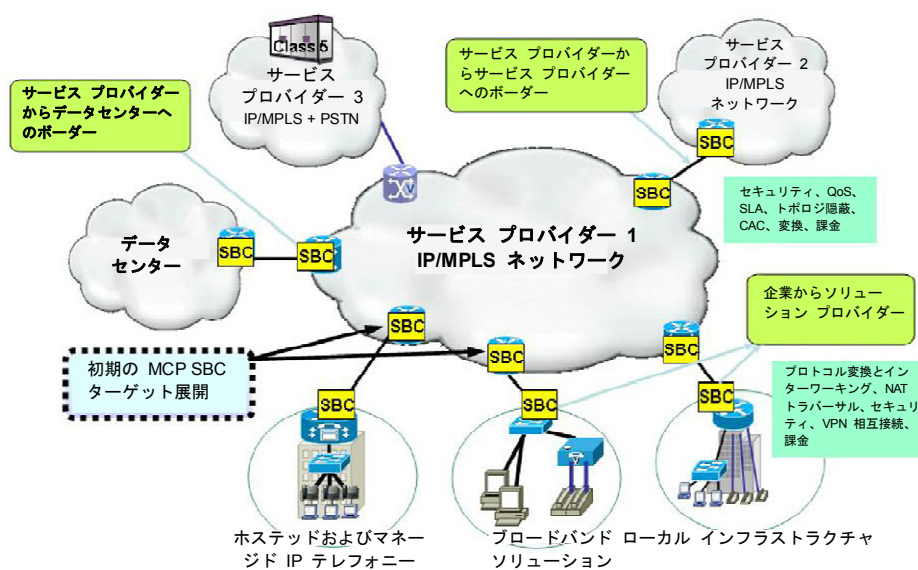
一部の課題の解決には、さまざまな相互接続点で SBC などのデバイスが必要となります。

一般的に SBC は、統合展開モデルまたは分散展開モデルという 2 つのモデルのいずれかを使用して展開されます。このドキュメントでは、分散展開モデルにおける Cisco ASR 1000 シリーズの実装について説明します。

展開シナリオ

SBC は、多くの展開シナリオにおいて重要な役割を果たします。図 1 は、SBC が使用されるネットワークトポロジのいくつかの例を示しています。

図 1 VoIP インターワーキングで使用される SBC



このシナリオでは、あるサービス プロバイダーのコア ネットワークを、データセンター、企業ユーザ、ブロードバンド ユーザ、ホステッドおよびマネージド IP テレフォニー、および公衆電話交換網 (PSTN) ネットワークに接続する音声ゲートウェイなどの各種のネットワークに接続し、さらに、別のサービス プロバイダー ネットワークにも接続しています。このようなさまざまな異なる加入者の観点からセキュリティ要件を考えると、それぞれの加入者が自身のネットワークの保護を必要とするだけでなく、コア サービス プロバイダーもまた、これらの利用者からの自身のネットワークの保護を必要としています。SBC は、ネットワーク アドレスの保護に加えて、これらの加入者からの各種のコーデック、DTMF、Differentiated Services Code Point (DSCP; DiffServ コード ポイント) マーキングなどの変換にも有用です。加入者は、それぞれ独自の必要性から、使用する機能を選択します。たとえば、サービス プロバイダーとサービス プロバイダーの相互接続において、サービス プロバイダーは自身のネットワークの保護、CDR および課金、QoSなどを特に重視しています。一方、サービス プロバイダーと企業の相互接続の場合、サービス プロバイダーの主な関心事は、ネットワークを保護しつつ、ローカルの構内自動交換機 (PABX; コール マネージャ、IP ベースの PABX など) を利用して、QoS およびコーデックの変換を提供することになります。このため、SBC は、提供されるサービスからの要求に応じて必要な機能を提供する、機能のツールキットとすることができます。

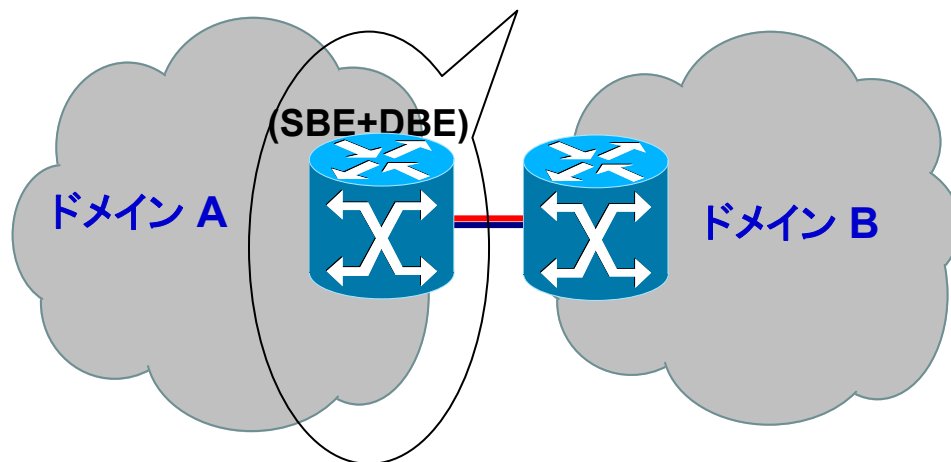
統合展開モデルと分散展開モデル

SBC 機能は、Signaling Path Border Element (SBE) および Data Path Border Element (DBE) という 2 つの論理的なサブエレメントに大きく分類できます。SBE は、プロトコルのインターワーキング (たとえば H.323 から SIP)、アイデンティティとトポロジの隠蔽、Call Admission Control (CAC; コール アドミッション制御) などのシグナリング機能を提供します。DBE は、ディープ パケット インスペクションと修正、メディア リレー、およびファイアウォール サポートなどを SBE の制御下で提供します。

SBC 統合モデル

SBC 統合モデルの場合、SBE および DBE 論理エレメントは通常、1 つの物理的 SBC デバイスに実装されます。図 2 に示すように、SBE と DBE は 1 つのネットワーク エレメントとして統合されています。SBC はドメインのエッジ上に配置されています。

図 2 SBC 統合モデル



このモデルの場合、シグナリングとメディアの両方が、同じ物理デバイスを経由します。

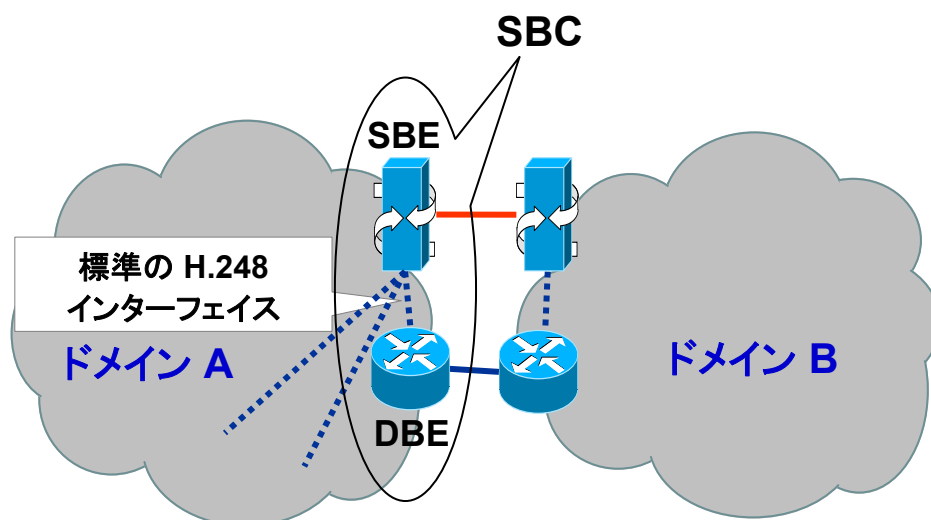
分散展開モデル

多くのキャリアが実感していることですが、音声ネットワークが拡張するにつれて、ネットワーク管理の課題もそれに比例して増加します。サービス プロバイダーは現在、SBC のデータパス機能をシグナリング機能から切り離すための方策を必要としています。SBE 機能を集中化して管理、運用、およびトラブルシューティングを簡素化する一方で、DBE 機能を SBE から切り離してネットワーク内に分散できるような機能が求められているのです。このモデルでは一般的に、SBE 機能は中央の場所に集中化され、DBE 機能は、ネットワーク ルーティング機能とともにネットワーク内に分散されます。

図 3 は、分散展開モデルにおいて、SBE と DBE の間の通信が、IP Multimedia Subsystem (IMS) で採用された ITU-T H.248 などの定義済みの標準を使用して行われることを示しています。これにより、ネットワーク内の複数のプラットフォームに SBE および DBE エレメントを実装できます。分散 SBC というアプローチは、ネットワーク内のさまざまなエレメントおよびアプリケーションから SBE 機能を提供するという、IMS、ITU、および Telecoms and Internet Converged Services and Protocols for Advanced Networks (TISpan) アーキテクチャの指針に沿うものです。TISpan の用語を使用すると、Cisco ASR 1000 シリーズ ルータの DBE 機能は Border Gateway Function (BGF) を提供し、Service Policy Decision Function (SPDF) と対話します。SPDF は H.248 プロトコルを使用して、ルータ上のメディア パス(ゲート)をセットアップおよびティアドアウンし、セッション単位のポリシーを適用します。

分散展開モデルの場合、ベアラ トラフィックまたはメディア パケットのフローは常に DBE を経由し、SBE はシグナリング フローにのみ関与します。DBE は、ディープ パケット インスペクション (Real-Time Transport Protocol [RTP] および Real-Time Streaming Protocol [RTCP])、パケット ヘッダーの修正、NAT トラバースルを処理するメディア リレー、トポロジ隠蔽など、メディア関連の機能を処理します。

図 3 SBC 分散モデル



SBC が組み込まれた柔軟なネットワーク コンポーネントにより、統合展開モデルと分散展開モデルの両方をサポートできます。ネットワークは絶えず成長および進化しているため、SBC が組み込まれた、適切な拡張が可能な今日のマルチメディア IP トランスポート ネットワークの成長は、統合モデルを凌駕するものになると考えられます。このため、分散アプローチが必要となります。オペレータはネットワークとともに成長可能な SBC を必要としています。莫大な資本投資を必要とする、稼働中のネットワーク エレメントの機器全体のアップグレードは歓迎されません。

表 1 は、SBC の統合モデルと分散モデルの主な相違を示しています。

表 1 SBC 統合モデルと分散モデルの相違点

SBC 統合モデル	SBC 分散モデル
必要なすべての SBC 機能を統合 他のアプリケーションに依存しない	シグナリングおよびコントロール ロジックの集中化 スケーラブルな設計により、「成長に応じた投資」型のビジネス モデルが可能

Cisco ASR 1000 シリーズにおける SBC の実装

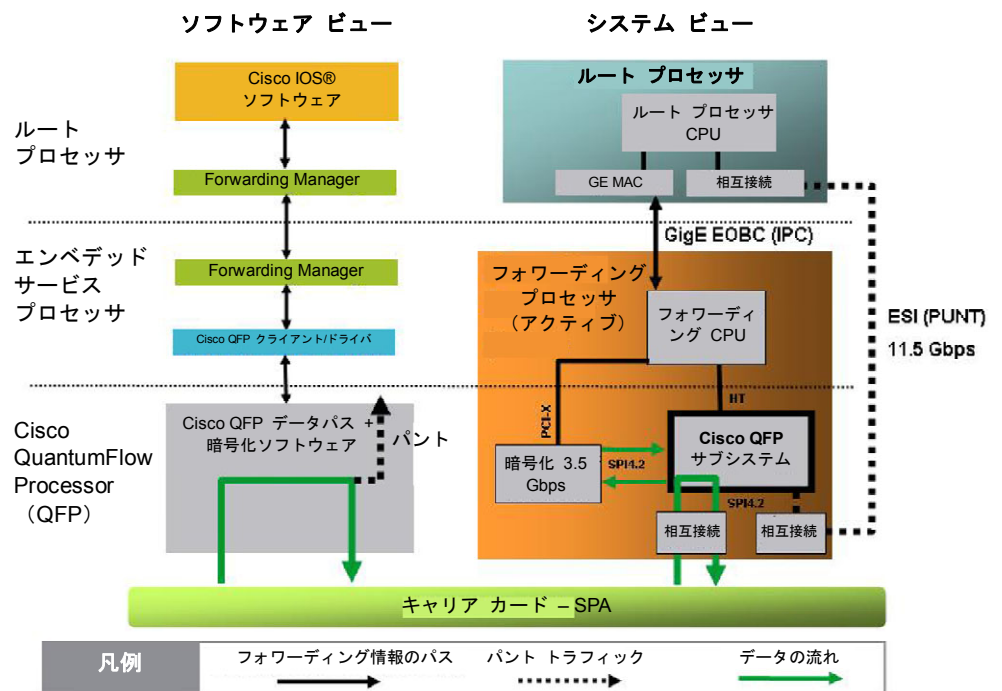
分散展開モデルの項で説明したように、SBE および DBE エンティティはそれぞれ異なるネットワーク エlement上に配置されます。SBE は H.248 標準インターフェイスを使用して DBE エンティティと対話します。

Cisco ASR 1000 シリーズ ルータ内のデータ フローを考えてみます。図 4 は、この実装をソフトウェア ビューおよびシステム ビューという 2 つの観点から示しています。ハードウェアの観点から、Cisco ASR 1000 ルータの主なコンポーネントは、Cisco ASR 1000 シリーズ ルート プロセッサ、Cisco ASR 1000 シリーズ エンベデッド サービス プロセッサ (ESP)、Cisco QuantumFlow Processor (QFP)、および、エンドポイントからのデータを取り込む Cisco ASR 1000 シリーズ SPA インターフェイス プロセッサ (SIP) です。システム ビューを見ると、ルート プロセッサに制御機能を実行する CPU が装備され、ESP にメディア パケットを処理する Cisco QuantumFlow Processor が装備されていることが分かります。

ルート プロセッサの役割は、SBE から到着した H.248 制御パケットを処理し、SBE から受信したセッション単位のポリシーを使用して、ESP 上で条件を処理するためのピンホールおよびメディア パケットを設定することです。ESP は、Cisco QuantumFlow プロセッサの助けを得て、これらの条件に基づいてメディア パケットのフォワーディングを行います。データが SIP から Cisco QuantumFlow Processor に到着すると、H.248 制御パケットであるか、通常のメディア パケットであるかが判別されます。H.248 制御パケットの場合は、処理のためにルート プロセッサ宛てにパントされます。定義されたピンホールに対する通常のメディア パケットの場合は、フォワーディング プロセッサが Cisco QuantumFlow Processor の助けを借りてデータ自体を処理します。DBE の場合、メディア ピンホールが作成されると、ESP が音声およびビデオのメディア パケットを処理します。ルート プロセッサはこれに関与しません。ルート プロセッサは、ピンホールおよびポリシーの定義および修正に関して、H.248 プロトコルを使用して SBE と SBC 制御パケットを交換する以外、このプロセスに関与しません。

また、Cisco ASR 1000 シリーズ ルータの ESP には、暗号化データの処理を支援するハードウェアの暗号化エンジンが組み込まれています。Cisco QuantumFlow Processor に暗号化データが到着すると、プロセッサはデータを暗号化エンジンにパントして、復号化および暗号化を行います。ハードウェアの暗号化エンジンが組み込まれているため、暗号化データを迅速に処理できます。

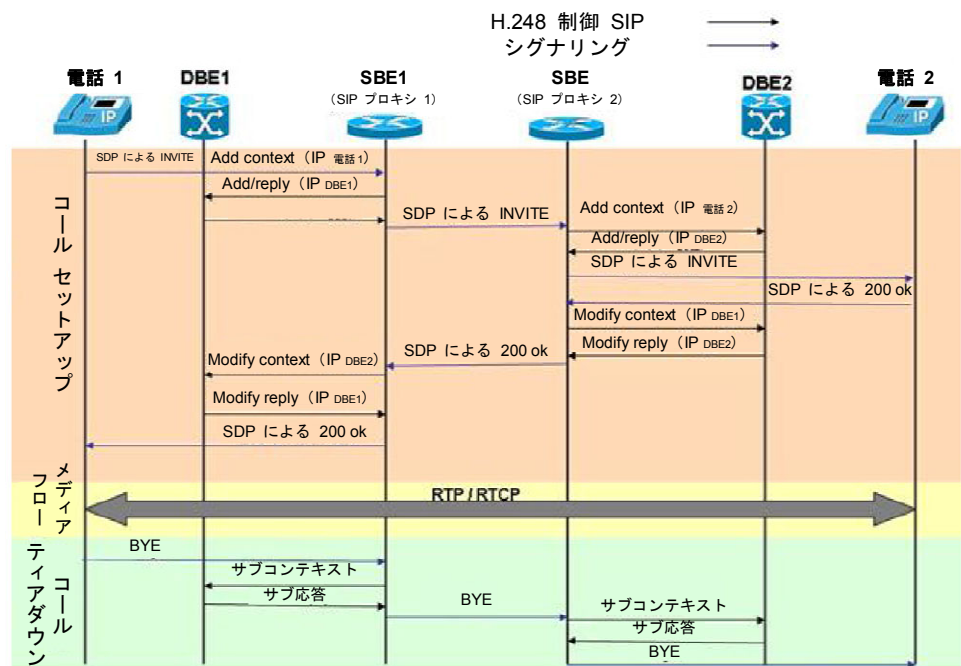
図 4 Cisco ASR 1000 シリーズ ルータの機能図



SBC のコールの基本フロー

図 5 は、SBC 分散モデルにおけるシグナリング フローを示しています。

図 5 SBC のコールの基本フロー



この図は、SIP INVITE メッセージが、エンド デバイス(電話 1)から SBE1 へ直接に送信されることを示しています。SBE1 はこの SIP メッセージに基づき、H.248 を通じて、H.248 コマンドを使用してメディア ピンホールを開くように DBE に指示します。SBE1 は DBE から応答を受け取ると、SIP INVITE メッセージを終端側の他の SBE に送信します。この SBE もまた、H.248 インターフェイスを使用して、SBE の自身の側にメディア ピンホールを開きます。SBE2 は DBE2 から応答を受け取ると、エンドユーザ(電話 2)に INVITE メッセージを送信します。SBE2 はエンドユーザから 200 ok SIP メッセージを受け取ると、H.248 の modify context コマンドを使用して SendReceive モードでストリームを構成するように DBE に指示し、この 200 ok メッセージを発信側の SBE に転送します。発信側の SBE もまた、H.248 の modify コマンドを使用して、DBE でメディア ストリームを修正して受信メッセージを送信し、発信側ユーザ(電話 1)に対して 200 ok メッセージを転送します。これにより、メディア トラフィックが開始されます。メディアはこのようにして確立されます。同様に、いずれかのエンドユーザから BYE メッセージが送信されると、SBE は、該当する DBE に接続を終了するように指示します。コールはこうして解除されます。

DBE はメディア パケットのみを処理しますが、シグナリング パケットも DBE を通過します。DBE は SBE からの指示を受けて、シグナリング パケットの中継に使用されるシグナリング ピンホールを作成できます。シグナリング ピンホールは、メディア ピンホールと同じように作成され、それぞれに異なるポリシーを適用できます。シグナリング ピンホールのサポートにより、NAT トラバーサルパッケージを使用するエンドユーザから SBE インフラストラクチャを保護できます。

DBE 機能

前に説明したように、SBC は、さまざまな設計基準や要件に対応できるように個々の機能を支援する、機能のツールキットです。SBC DBE の分散構成は、シグナリング インターワーキングや制御パス管理、トポロジ隠蔽、課金と CDR、QoS など、さまざまな機能に対応しています。分散展開モデルの場合、DBE の多数の機能は、H.248 シグナリング制御を通じて SBE によって制御されます。Cisco ASR 1000 シリーズ ルータでは、以下の DBE 機能がサポートされています。

- シグナリング インターワーキングまたは制御パス管理:シグナリングに関して、DBE はシグナリング ピンホールを開き、トラフィックを SBE に転送します。制御パスに関して、DBE は SBE と対話してメディア ピンホールを開き、H.248 インターフェイスを通じて SBE によって定義されたポリシーを実行します。
- トポロジ隠蔽:DBE は NAT および PAT を使用してシグナリング インフラストラクチャおよびメディア パケットを保護します。各種(なし、1 度、および 2 度)の NAT および PAT トラバーサルスキームがサポートされます。
- セキュリティ:ゲート管理やトラフィック管理などの各種の H.248 パッケージにより、インフラストラクチャのセキュリティおよび帯域幅保護を提供します。DBE はこれらのパッケージを使用して、許可されたトラフィックおよび許可された帯域幅の発信元アドレスの確認など、さまざまなポリシーを適用できます。また、着信パケットのアドレスを監視して疑わしいソース パケットを削除することで、DoS 攻撃(サービス拒絶攻撃)を監視できます。このようなタイプのイベントが発生した場合は、SBE に対してアラートが発行されます。
- QoS:DBE 実装は QoS に関して、パケットのセッション単位の DSCP マーキング、および帯域幅管理用のトラフィック管理パッケージ(2 つのレート、3 色のポリシングを使用する)をサポートしています。Cisco ASR 1000 シリーズ ルータ プラットフォームは、Low Latency Queuing (LLQ; 低遅延キューイング)、Class-Based Weighted Fair Queuing (CBWFQ; クラスベース WFQ)、トラフィック シェーピングなどの QoS 機能も(サブ)インターフェイス レベルでサポートします。

- **メディア管理:** Cisco ASR 1000 の DBE 実装は、メディア パケットに関して RTP および RTCP をサポートします。DBE は、5 つのアドレス(ソース IP アドレス、ソース ポート アドレス、ディストリビューション IP アドレス、ディストリビューション ポート アドレス、および IP アドレス)によってサポートされるメディアをチェックします。DBE 実装は、コーデック タイプに依存しないため、すべてのコーデックがサポートされます。また、DBE は、H.248 パッケージの助けを借りて、メディア ストリームで DTMF デジットを検出および挿入できます。また、非アクティビティ タイマーを使用して、ハング状態のコールを検出できます。
- **課金:** コールが終了すると、正確な課金情報および CDR が SBE に提供されます。また、DBE はセッションの終了時に、パケット損失、ジッタ、およびラウンドトリップ時間に関する情報を生成できます。

ハイアベイラビリティ

DBE のハイアベイラビリティは他の機能と同じです。Cisco ASR 1000 シリーズ ルータは Stateful Switchover (SSO) および In Service Software Upgrade (ISSU) をサポートします。Cisco ASR 1000 シリーズ ルータ プラットフォームから提供される 2 ラックユニット (2RU)、4RU、および 6RU のプラットフォームでは、それぞれ異なる種類の冗長性を実現できます。

6RU の Cisco ASR 1000 シリーズ ルータ シャーシでは、DBE に冗長ルート プロセッサおよび冗長 ESP を構成できます。アクティブ ルート プロセッサの障害の場合は、スタンバイ ルート プロセッサがアクティブになるため、パケットの損失は発生しません。同様に、アクティブ ESP の障害の場合、スタンバイ ESP がアクティブになりますが、移動中の一部のパケットの損失が発生します。処理中のコール統計は維持され、スイッチオーバーは透過ですが、コールの SSO は、セットアップ済みのアクティブ コールにのみ適用されます。セットアップ途中のコールはリダイヤルする必要があります。

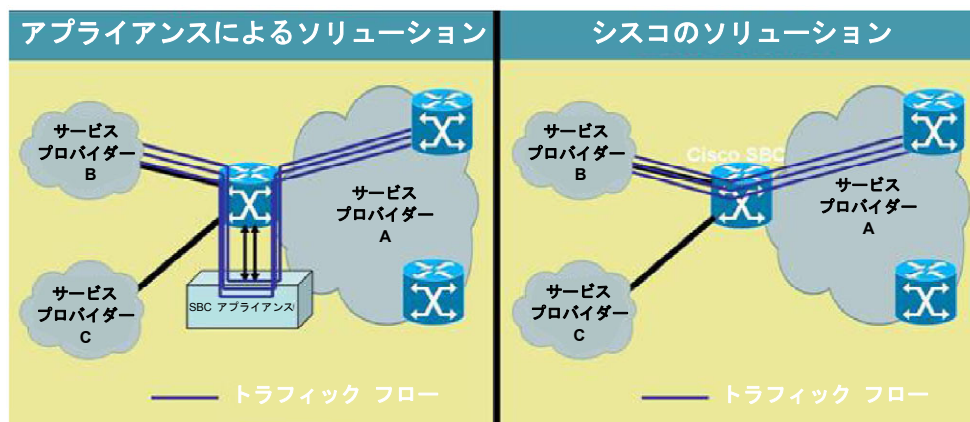
4RU の Cisco ASR 1000 ルータ シャーシの場合、ルート プロセッサまたは ESP の冗長性は提供されませんが、2 つの Cisco IOS ソフトウェア デモンを、1 つはアクティブ モード、1 つは冗長モードで実行できます。これにより、Cisco ASR 1000 シリーズ ルータ プラットフォームの SBC の実装において、SSO 機能を含めて、広範囲のハードウェアおよびソフトウェアの冗長性が実現されます。

Cisco ASR 1000 シリーズ ルータは In-Service Software Upgrade (ISSU) のサポートも提供します。このサポートにより、ソフトウェア統合パッケージ内の特定のソフトウェア コンポーネント(サブパッケージと呼ばれます)をアップグレードできます。たとえば、ルート プロセッサ サブパッケージを、他のサブパッケージや、実行中のサービスに影響を与えることなくアップグレードできます。統合パッケージおよびサブパッケージの詳細については、<http://www.cisco.com/jp/go/asr1000/> で、Cisco ASR 1000 シリーズのソフトウェア リリースに関する資料を参照してください。

シスコを選択する理由

シスコはネットワーキングおよび VoIP テクノロジーにおける世界的リーダーです。図 6 は、シスコのソリューションとアプライアンスによるソリューションの相違、およびトポロジ図を示しています。アプライアンス モデルの場合、SBC 機能とルーティング機能が複数のシステムに配置されるのに対して、シスコのソリューションでは、両方が同じシステムに配置されています。

図 6 シスコの統合モデルとアプライアンス モデルの比較



- シスコのソリューションでは、DBE を Cisco ASR 1000 シリーズ ルータに統合した SBC 分散展開モデルを使用することで、導入コストと運用コストを削減できます。
- DBE 機能をルータに統合した SBC 分散モデルは、アプライアンス モデルに比べてホップ数が少ないため、パケットの遅延が減少します。VoIP およびビデオなどのリアルタイムトラフィックアプリケーションにおいては、遅延が少ないことが重要です。
- SBC は Cisco IOS ソフトウェア ベースのソリューションであるため、QoS、アクセスコントロールリスト(ACL)、IP ルーティングなど、Cisco IOS ソフトウェアの機能を活用できます。
- Cisco ASR 1000 シリーズ ルータでは、ルートプロセッサおよび ESP のデュアル モジュールを使用することで、ステータフルな冗長性を提供することもできます。

結論

VoIP ネットワークにおける SBC コンポーネントの重要性は増しつつあります。SBC は、シグナリング インターワーキング、トポロジ隠蔽、QoS、セキュリティなどの重要な機能を提供します。Cisco ASR 1000 シリーズ ルータは、SBC 分散展開モデルにおいて、DBE として機能できます。この設計は、IMS および TISpan の定義に対応したのもでもあります。Cisco ASR 1000 シリーズ ルータに DBE 機能を組み込むことで、企業およびサービス プロバイダーの導入コストと運用コストを削減できます。

Cisco ASR 1000 の分散アーキテクチャと、高性能のデータ フォワーディング エンジンにより、SBC の DBE 部分の実装がさらにスケーラブルになります。この機能は Cisco IOS ソフトウェア上で実行されるため、SBC と併せてソフトウェアの機能を使用できます。さらに、ルーティング プロセッサおよびエンベデッド サービス プロセッサの高度な冗長性により、サービス プロバイダーは、ユーザに対してノンストップ サービスを提供できます。

関連情報

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータにおける Cisco SBC の実装の詳細については、以下の資料を参照してください。

- H.323 フォーラム (英語) : <http://www.h323forum.org/papers/>
- VoIP の情報 (英語) : <http://www.packetizer.com/>
- サービス プロバイダー ネットワークのためのスケーラブルな SBC 機能 (英語) :
http://www.cisco.com/en/US/products/ps6342/products_white_paper0900aecd80391b66.shtml
- H.248 プロトコルの概要 (英語) : <http://www.packetizer.com/voip/h248/>
- SIP (英語) : <http://www.cs.columbia.edu/sip/>
- TISpan (英語) : <http://www.etsi.org/tispan/>
- Cisco ASR 1000 シリーズ Session Border Controller データシート :
<http://www.cisco.com/jp/go/asr1000/>

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先 (シスコ コンタクトセンター)

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

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先