

シスコアクセスサービスソリューション

- アーキテクチャの概要 -

New Worldにおいてサービスプロバイダーが収益を上げるためには、顧客のニーズに合わせた新しいサービスを迅速に導入できるかがカギとなります。これを実現するに当たっては、New Worldに向けて設計され、かつ最適化された、柔軟でマルチサービスのOSS(Operations Support System)が決定的な意味を持つこととなります。インターネットOSSは、シスコによる広範なイニシアティブであり、オープンな標準ベースの参照アーキテクチャを通じて、New Worldオペレーションのビジョンを実現します。New Worldオペレーションは、社会全体が新しいネットワーク情報構造に移行していくなかで、サービスプロバイダーに対して、市場シェアを拡大するための機会を提供します。

はじめに

インターネットへのダイヤルインアクセスは、およそ30年ほど前に初めて、大学の研究者や大学院生の間で行われるようになりました。当時のインターネットは、主として大学、軍隊、および研究所のコンピュータを結ぶためのネットワークであり、パーソナルコンピュータは存在すらしていませんでした。ユーザーは、ダイヤルイン接続を介してさまざまなシステムに単純な端末アクセスを行っていました。このように単純な環境から、初期のアクセス管理システムが開発されました。これらのシステムはその後発展を遂げ、大学や研究機関へのリモートアクセスを管理していたのと同じ技術が、インターネットへのアクセスや企業ネットワークへのアクセスを提供するようになっていきます。

RADIUS(Remote Authentication Dial-In User Service)は、リモートアクセスユーザーの認証、認可、およびアカウント管理(AAA)に関するニーズに対処するために開発されました。RADIUSは、リモートユーザーによる中央のデータベースへのアクセスと認可されたサービスをサポートし、ネットワークアクセスサーバから使用状況やアカウント情報を得るための手段を提供します。RADIUSは、当初はアナログおよびデジタルダイヤルインのサポートに使用されていましたが、現在ではサービスプロバイダーによって、xDSL(xDigital Subscriber Line)、ケーブル、無線、およびVoIP(Voice over IP)サービスのサポートのために使用されています。

多くのサービスプロバイダーは、AAAサービスを実現するために、パブリックドメインのRADIUSサーバソースコードを利用していました。ビジネス上の課題がより高度なものになるに従って、サービスプロバイダーは自らのニーズを満たし、かつそのニーズをサポートするだけの拡張性を備えた商業製品を求めようになりました。技術とサービスがきわめて急速に変化する環境にあっては、自社独自のAAAシステムを維持することはもはや得策とは言えなくなったのです。

こうしたニーズに応えるため、シスコは特にサービスプロバイダー向けとして設計された、Cisco Access RegistrarというRADIUSサーバを提供しています。Cisco Access Registrarは、シスコのサービス管理アーキテクチャのインフラストラクチャコンポーネントとして、新しいサービスを迅速にサポートし、サービスプロバイダーが必要とするパフォーマンスと拡張性を提供します。

RADIUSのAAA管理

RADIUSの仕様は、IETF(Internet Engineering Task Force) RFC 2138(認証と認可)およびRFC 2139(アカウント管理)で規定されています。これらの文書は、NASと中央のAAAサーバ(RADIUSサーバ)間のプロトコルを定義しています。RADIUSは、ネットワークアクセスサーバ(NAS)を製造しているすべてのベンダーがサポートしているAAAプロトコルです。ネットワークアクセスサーバとRADIUSサーバは、両サーバ間のトランザクションの整合性を保つために、認証に関する情報を共有します。

RADIUSサーバのクライアントとして機能するNASは、接続要求を受け取った後、ユーザーからID情報(ユーザー名、パスワード)を入手し、続いてRADIUSサーバに対して標準化された認証要求を発行します。RADIUSサーバはID情報とその他のNAS情報を受け取り、ユーザーの認証を行います。RADIUSサーバはまた、使用するIPアドレスなどの接続設定パラメータ、ネットワークアクセスを制限するためのフィルタ、およびセッションとアイドルタイムアウト値をNASに送ります。認証および認可プロトコルの定義に加え、RADIUSはNASからAAAサーバへ使用状況とアカウント情報を送信するためのプロトコルも定義しています。これらの情報は、課金、モニタリング、およびレポート機能などを処理するバックエンドシステムに送られます。

RADIUSでは、ベンダーが自らのネットワークアクセスサーバやその他のネットワークアクセス機器に新しい機能を追加できるように、IETFによって定義された「辞書」属性だけでなく、ベンダーごとの属性(VSA)を使用することも許されています。主要ベンダー各社は、自社製機器の付加価値機能をサポートし、製品を差別化するためにVSAを使用しています。したがって、RADIUSサーバには拡張可能な辞書が必要であり、またマルチベンダーをサポートできるようになっている必要もあります。

しかし、VSAと拡張可能な辞書だけでは、今日の運営環境のニーズを満たすことはできません。サービスプロバイダーは、AAAに対する要求レベルをさらに高いものへと推し進めてきました。RADIUSシステムには、マルチベンダーのサポートだけでなく、このような環境において必要とされるパフォーマンスと拡張性を備え、サービス管理システムの他の項目と統合でき、かつ新しいサービスを迅速にサポートできることが求められているのです。従来から「自社製」のRADIUSシステムを開発していたサービスプロバイダーは、そのようなシステムの維持と拡張を行うことはもはや不可能であることに気づいています。

Cisco Access Registrar

Cisco Access Registrar は、AAA に対するサービスプロバイダーの厳しい要求に応えられるように設計された RADIUS サーバです。これはパブリックドメインの RADIUS「フリーウェア」を拡張あるいは移植しただけのものではありません。常に変化し続ける環境に適した、拡張可能なパフォーマンスとプラットフォームを提供できるように、基本から設計されています。Cisco Access Registrar は、マルチスレッドアーキテクチャをベースとしたもので、ロジックを追加するための多数の拡張ポイントを備えており、バックエンドのディレクトリシステムとの統合を行えるよう LDAP (Directory Access Protocol) に対応しています。Cisco Access Registrar は、Solaris オペレーティングシステムが稼働している SPARC サーバ上で実行され、1 秒あたり数百件単位の AAA トランザクションを実行できます。これによって、サービスインフラストラクチャのサポートに必要なサーバの数を削減することができます。

拡張ポイント

Cisco Access Registrar の拡張ポイントは、RADIUS サーバロジックの追加をサポートすることにより、基本機能の強化あるいはカスタマイズを可能にします。この拡張には、C/C++ 共有ライブラリまたは Tcl スクリプトを使います。これにより、機能拡張のプロトタイプを Tcl によって簡単に作成でき、その機能を最大限に発揮するために C または C++ でコーディングすることができます。機能拡張は、10 力所以上のあらかじめ定義されたポイントにおいて、パケット処理に対するサーバの動作を変更できます。具体的には、入力/出力 RADIUS パケットの変更やパケット処理をコントロールするための Cisco Access Registrar 環境変数の変更を使用することができます。たとえば、特定のユーザーやユーザーコミュニティに対し、カスタマイズされた認証サービスを使用するための機能拡張を作成できます。

ディレクトリの統合

ディレクトリシステムは急速に、サービス管理システムと OSS (Operations Support System) 全体を統合するための仕組みとなりつつあります。ディレクトリはユーザー情報、サービスプロファイル、課金プロファイル、およびその他のサービス情報のための、中央のリポジトリとして機能します。マルチマスターの複製されたディレクトリは、この情報を任意の場所に迅速に配付したり、あるいはこの情報に任意の場所からアクセスするための手段となります。ディレクトリが X.500、マイクロソフト社の Active Directory、またはノベル社の NDS のいずれであっても、Cisco Access Registrar はその LDAP 機能を使用してこの情報にアクセスできます (図 1 参照)。

Cisco Access Registrar は、ユーザーを LDAP ディレクトリと照合して認証し、さまざまなディレクトリ設定に対応できるようにします。Cisco Access Registrar は、すべてのユーザーに関して単一のディレクトリを参照するようにも、あるいは特定のユーザーコミュニティに関して別のディレクトリ(またはディレクトリのブランチ)を参照するようにも設定できます。Cisco Access Registrar は、ユーザーレコードを探すために LDAP ルックアップを実行し、ディレクトリ中に保存されているユーザーパスワードを検証します。Cisco Access Registrar はまた、LDAP ユーザーレコードの属性を RADIUS の属性に対してマッピングすることもできます。したがって、ユーザーの RADIUS プロファイルに対応する LDAP ユーザーレコード中に設定することができ、システムは Access Registrar によって認証および認可されるユーザーを直接設定するために LDAP を使用できます。

AAA プロキシ

インターネットの成長とサービスプロバイダーの増加に伴い、AAA システムの統合を必要とする合併や提携などが増加しています。リモートアクセスによるアウトソーシングを企業向けに提供するサービスプロバイダーには、エンドユーザーの顧客 AAA システムを統合する必要も生じています。Cisco Access Registrar は RADIUS プロキシをサポートしているため、サーバはユーザーの認証と認可を直接ディレクトリに対して行う代わりに、他のディレクトリやデータベースに対してユーザーの認証と認可を行う他のサービスプロバイダー(または顧客)の RADIUS サーバに、AAA 要求を選択的に送ることができます。

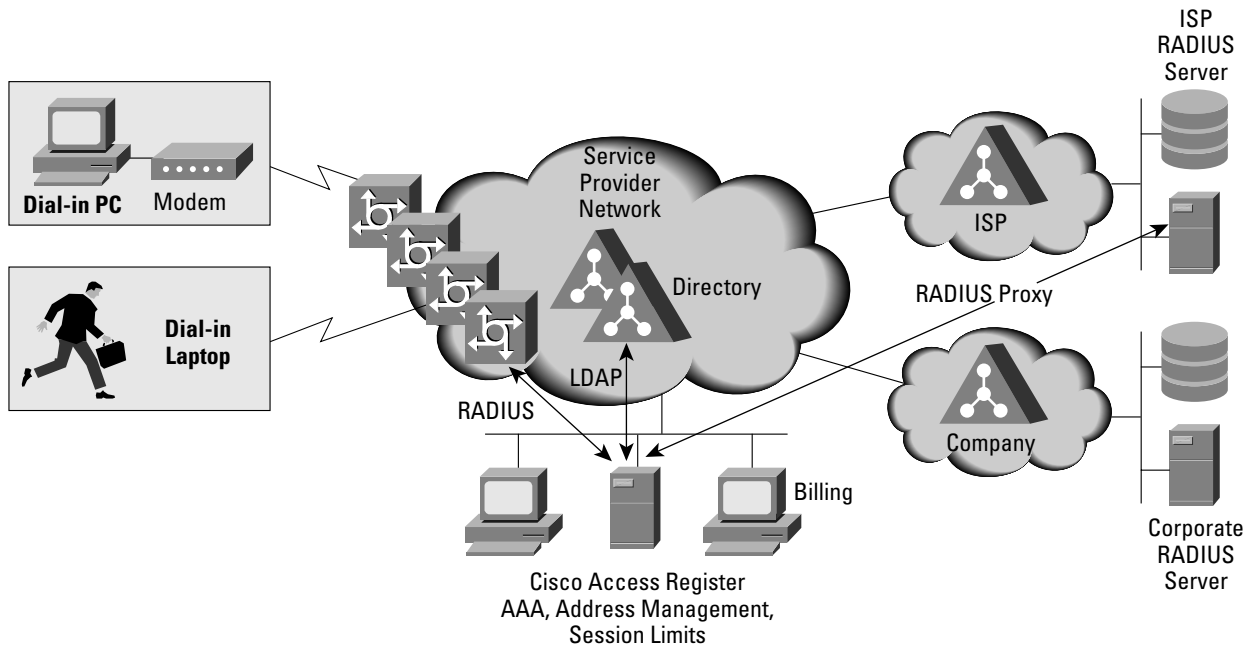
Access Registrar では、ダイヤルされた番号 (DNIS) または要求パケット中の一部(たとえば bill@isp_a.com 中の「isp_a」)に基づいて、サーバが RADIUS 要求を代理送信するようにサービスフィルタを設定できます。拡張ポイントを経由すれば、要求パケット中の他の任意の情報に基づいて代理送信することも可能です。なお、RADIUS プロキシについては、この後にある「Cisco Access Registrar のアプリケーション」の節を参照してください。

アドレスとセッションの管理

RADIUS サーバは受信する要求を受信ごとに処理する、ステートレスのサーバです。これはベーシックな AAA には十分ですが、今日のアクセスネットワークを効率的に運営し、活用するためには、IP プール管理やアドレス割り当てのような「ステートフル」の処理や、セッション制限の設定などが必要です。これらの処理は、従来は個々の NAS によって行われていましたが、ベンダーから独立した形で集中管理を行う必要があります。Cisco Access Registrar は、IP または IPX の動的な割り当てを処理し、ユーザーとグループ両方のセッション制限を複数のネットワークアクセスサーバに対して適用する、リソースマネージャを提供します。ちなみに、Cisco Access Registrar 機能拡張を選択したり、デフォルトの IP アドレスプールまたはセッションマネージャをその機能拡張によって置き換えたりすることもできます。

CNS (Cisco Network Services) の Concurrency Control Services を用いれば、必要な箇所にさらなるセッション管理機能を追加することができます。CNS Concurrency Control Services は分散型の Solaris アプリケーションなので、複数の Access Registrar サーバにわたってセッション制限を管理でき、単一障害点の発生を回避できます。

図1 : Cisco Access Registrar



Cisco Access Registrar のアプリケーション

ホールセールダイヤル

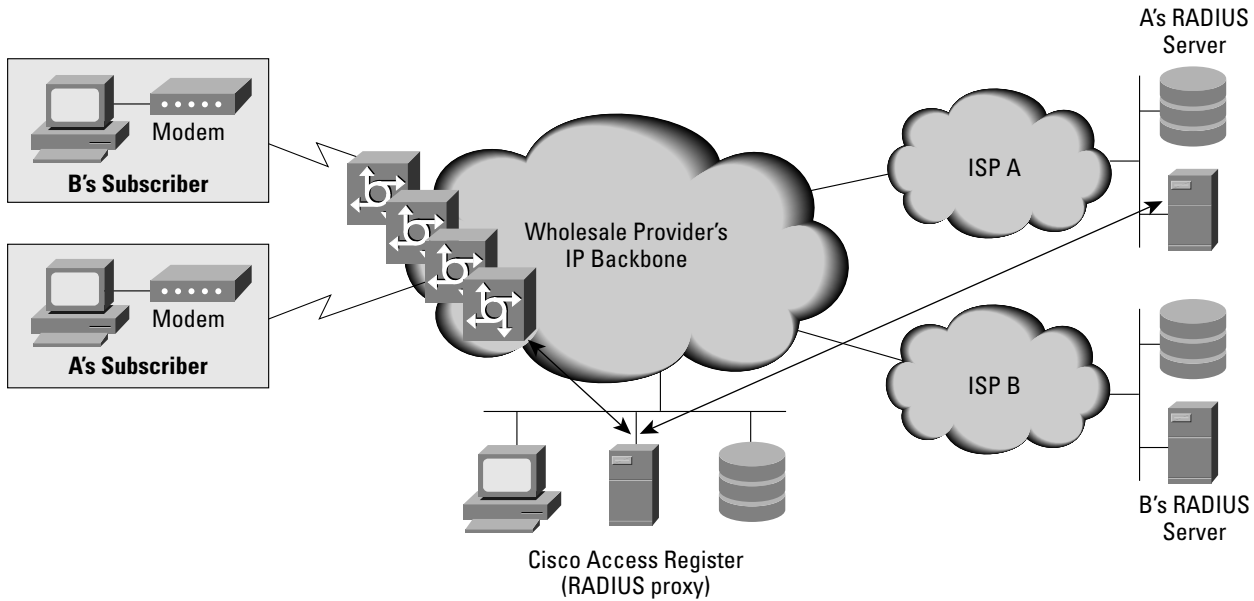
インターネットサービスプロバイダー(ISP)、アプリケーションサービスプロバイダー(ASP)、およびコンテンツプロバイダー(または「ポータル」)の多くは、サービスパッケージの一環として、ダイヤルアップによるインターネットアクセスを提供しなければなりません。しかし、これらのプロバイダーの多くは、ダイヤルアップアクセスのためのインフラストラクチャ構築に時間を費やしたくなかったり、あるいはインフラストラクチャ構築を迅速に行うことができなかつたりします(新しい地域への拡大を行っているときにはとくにそうです)。また、小売企業の場合も、ブランド戦略の一環として「プライベートブランド」によるインターネットアクセスの提供を行いたいと考えてはいても、なかなか自らサービスを構築するまでには至らないものです。

ホールセールダイヤルは、ホールセールサービスプロバイダーにダイヤルアップの管理を委ねることにより、コスト削減と効率改善をもたらすとともに、運用に至るまでに必要な時間を短縮します。このモデルを用いれば、関与するすべての企業は、それぞれが最も得意とする分野に集中できるようになります。つまり、ホールセール業者はインフラストラクチャに集中して、ポートアクセスをサービスプロバイダーに販売します。一方サービスプロバイダーは、コンテンツとそのサービスの販売およびマーケティングに集中するのです。

ホールセール業者のダイヤルインフラストラクチャ(図2 参照)において、Cisco Access Registrar は次のような機能を提供します。

1. NAS から RADIUS 認証および認可要求を受信する。
2. ホールセール顧客の身元(たとえば ISP A)をダイヤルされた番号(DNIS)、ユーザー名の一部(たとえば「bill@isp_a.com」)、またはその他の基準により識別する。
3. AAA トランザクションを、ホールセール顧客に指定された RADIUS サーバに、必要であればユーザー名を変更して(「bill@isp_a.com」を「bill」に)代理送信する。
4. 有効な認証とユーザーのサービス認可パラメータ(または拒否された認証)を受け取る。
5. IP アドレスを発行し、設定されたセッション制限をチェックする。
6. ホールセール業者のアクセス機器との互換性、または顧客との間に締結されているサービスレベル契約に従うため、必要であれば応答を修正する。
7. 応答を NAS に戻す。
8. RADIUS アカウントレコードを NAS から受け取り、そのレコードを顧客の RADIUS サーバに代理送信し、また課金のためにローカルなコピーを維持する。

図2 : Cisco Access Registrar によるホールセールダイヤル



仮想プライベートネットワークによる企業ダイヤルインのアウトソーシング

サービスプロバイダーにとってのもう1つの大きなビジネスチャンスは、企業ダイヤルインネットワークのアウトソーシングです。企業のネットワーク管理者は、ダイヤルインモデムやISDNアダプタをワールドワイドで取り扱えるようなサービスをサービスプロバイダーに求めています。また彼らは、こうしたダイヤルイントラフィックがすべて、主要な企業内サイトにおいて高速リンク経由で伝送されることを望んでいます。さらに彼らは、サービスプロバイダーに対しては、可用性が高くセキュアなVPN（仮想プライベートネットワーク）サービスを求める一方で、その所有権は自社で確保し、さらに社員やその他の正規スタッフを識別するための認証データベースの運用も自社で行いたいと考えています。

サービスプロバイダーは、特定のネットワークアクセスサーバやモデムのセットを特定の企業専用とするのではなく、資源を共有することによってスケールメリットを得るようにすべきです。ホールセールダイヤルの場合と同様、Cisco Access Registrarはそれぞれのアクセス要求をリアルタイムで検証し、そのコミュニティ（つまり、その要求を出した企業）を判断します。続いて、プロキシRADIUS経由で該当する適切なAAAサーバが参照され、認証が成功してかつセッション制限を超えていなければ、NASから宛先のホームゲートウェイまでの間にセキュアなトンネルを確立することが可能となります。

CSRCによるテレコリターンとローミング

ケーブル経由のデータサービスは、ケーブル業界にとっての新たなビジネスチャンスとなります。データ、音声、およびビデオオンデマンドなどのサービスを効率的に提供しようと考えているケーブル多重システムオペレータ（MSO）やケーブルサービスプロバイダーには、管理コストを削減でき、加入者の急速な成長に対応できるようなシステムが必要です。このようなニーズに応えるために、シスコではCSRC（Cisco Subscriber Registration Center）を提供しています。これは、ブロードバンドモデムの設定や管理を行うための製品で、加入者のセルフサービスによる登録や管理もサポートしています。

Cisco Access RegistrarはCSRCのコンポーネントの1つで、DOCSIS対応モデムにRADIUSサービスを提供します。これにより、アップストリームデータにテレコリターンを必要とする単方向ケーブルプラントにおいても、高速データサービスの配備が可能となります。ケーブルのサービス区域外からのローミングをユーザーに提供したいMSOやケーブルサービスプロバイダーは、ダイヤルサービスにAAAサポートを提供するためにCisco Access Registrarを使用することができます。

まとめ

サービスプロバイダーは、マルチベンダーをサポートし、既存および今後のシステムとの統合が可能な、拡張性に富んだインフラストラクチャコンポーネントを必要としています。AAAシステムは、ダイヤルのみにとどまらない、広範なアクセスサービスに対するアクセスポリシーの適用を実現するためのカギとなるインフラストラクチャコンポーネントです。シスコは、サービスプロバイダーの特殊なニーズに応える先進的な管理ソリューションの提供を約束します。Cisco Access Registrar は、キャリアクラスのAAAプラットフォームを提供することにより、新しいサービスの迅速な配備と効率的な運営を実現します。

©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 富士ビルヂング
TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先