Dynamic Multipoint VPN（DMVPN）デザイン ガイド（バージョン 1.1）

Cisco Validated Design

July 11, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-9024-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Validated Design

Cisco Validated Design プログラムは、お客様による信頼性の高い、確実かつ速やかな展開を容易にするために、デザイン、テスト、および文書化されたシステムおよびソリューションで構成されています。詳細については、www.cisco.com/go/validateddesigns にアクセスしてください。

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）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その供給者は、商品性や特定の目的への準拠性、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、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供給者は、このデザインの使用または使用できないことによって発生する利益の損失やデータの損傷などをはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

デザインは予告なしに変更されることがあります。このマニュアルに記載されているデザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコシステムズ、その供給者、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

© 2008 Cisco Systems, Inc. All rights reserved.

はじめに　vii
概要　vii
対象読者　viii
バージョン 1.1 へのアップデート　viii
対象範囲　viii
マニュアルの目的　viii
マニュアルの構成　ix

chapter 1
DMVPN デザインの概要　1-1
概要　1-1
前提条件　1-2
デザインのコンポーネント　1-2
デザイン トポロジ　1-3
デュアル DMVPN クラウド トポロジ　1-4
デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル　1-4
デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル　1-7
シングル DMVPN クラウド トポロジ　1-9
ベスト プラクティスと既知の制限事項　1-10
ハブアンドスポーク展開モデルのベスト プラクティスの概要　1-10
ハブアンドスポーク展開モデルの既知の制限事項の概要　1-12
スポークツースポーク展開モデルのベスト プラクティスの概要　1-12
スポークツースポーク展開モデルの既知の制限事項の概要　1-13

chapter 2
DMVPN のデザインおよび実装　2-1
デザインの考慮事項　2-1
トポロジ　2-1
デュアル DMVPN ハブアンドスポーク　2-2
デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）　2-2
デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（デュアル ティア ヘッドエンド アーキテクチャ）　2-3
デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル　2-4
デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）　2-5
IP アドレス指定　2-6
GRE — p2p GRE および mGRE インターフェイス　2-7
NHRP　2-8
トンネル プロテクション モード　2-9
VPN でのルーティング プロトコルの使用　2-9
ルート伝播の手順　2-10
暗号の考慮事項　2-10

IKE CAC 2-10
設定および実装 2-11
ISAKMP ポリシーの設定 2-11
IPSec トランスフォームおよびプロトコルの設定 2-12
トンネル プロテクションの設定 2-13
ダイナミック crypto map の設定 2-14
crypto map の適用 2-15
mGRE の設定 2-15
トンネル インターフェイスの設定 — ハブアンドスポークのみ 2-15
トンネル インターフェイスの設定 — ダイナミック スポークツースポーク 2-16
NHRP の設定 2-17
ルーティング プロトコルの設定 2-18
EIGRP の設定 2-18
OSPF の設定 2-19
RIPv2 の設定 2-20
ハイ アベイラビリティ 2-21
すべての HA ヘッドエンド デザインに共通の要素 2-22
デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル 2-22
ハブアンドスポーク展開モデル — シングル ティア ヘッドエンド アーキテクチャ 2-22
ハブアンドスポーク展開モデル — デュアル ティア ヘッドエンド アーキテクチャ 2-23
デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル 2-24
QoS 2-26
ハブアンドスポーク展開モデルでの QoS 2-26
スポークツースポーク展開モデルでの QoS 2-30
IP マルチキャスト 2-30
その他のネットワーキング機能との相互作用 2-32
NAT と PAT 2-32
ファイアウォールの考慮事項 2-33
ヘッドエンドまたはブランチ 2-33
暗号アクセスの確認 2-33
よくある設定ミス 2-34
ルーティング プロトコルでのトンネル エンドポイントのアドバタイズ 2-34
IPSec トランスフォーム セットの一致 2-34
ISAKMP ポリシーの一致 2-34

chapter 3
スケーラビリティに関する考慮事項 3-1
スケーラビリティに関する一般的な考慮事項 3-1
IPSec 暗号化スループット 3-1
パケット / 秒 — 最重要要因 3-2
トンネルの数によるスループットへの影響 3-2
GRE カプセル化によるスループットへの影響 3-2
ルーティング プロトコルによる CPU オーバーヘッドへの影響 3-3

スケーラブルなデュアル DMVPN クラウド トポロジ ― ハブアンドスポーク展開モデル　3-3
ヘッドエンドのスケーラビリティ　3-3
トンネル集約のスケーラビリティ　3-3
集約のスケーラビリティ　3-3
顧客の要件に応じた集約のスケーラビリティの事例　3-3
ブランチ オフィスのスケーラビリティ　3-7
スケーラブルなデュアル DMVPN クラウド トポロジ ― スポークツースポーク デザイン　3-7
リージョナル スポークツースポーク クラスタ　3-12
その他のスポークツースポーク デザインの考慮事項と警告　3-13
耐障害性　3-13
パスの選択　3-13
スポーク ルータの過負荷　3-14

chapter 4
スケーラビリティ テストの結果（ユニキャストのみ）　4-1
スケーラビリティ テストの方法　4-3
DMVPN ― ハブアンドスポーク展開モデル　4-3
ヘッドエンドのスケーラビリティ テストの結果　4-3
ブランチ オフィスのスケーラビリティ テストの結果　4-4
DMVPN ― スポークツースポーク展開モデル　4-5
AES および 3DES のスケーラビリティ テストの結果　4-8
評価対象のソフトウェア リリース　4-9

appendix A
スケーラビリティ テスト ベッドのコンフィギュレーション ファイル　A-1
Cisco 7200VXR/NPE-G1/SA-VAM2 ヘッドエンドの設定　A-1
Cisco ASR1004 ヘッドエンドの設定　A-2
Cisco 7600/Sup720/VPN SPA ヘッドエンドの設定　A-5
Cisco 7200VXR/Cisco 7600 デュアル ティア アーキテクチャ ヘッドエンドの設定　A-9
ティア 1（mGRE）　A-9
ティア 2（IPsec）　A-11
Cisco ISR ブランチ オフィスの設定　A-14

appendix B
レガシー製品のテスト結果　B-1

appendix C
略語　C-1

はじめに

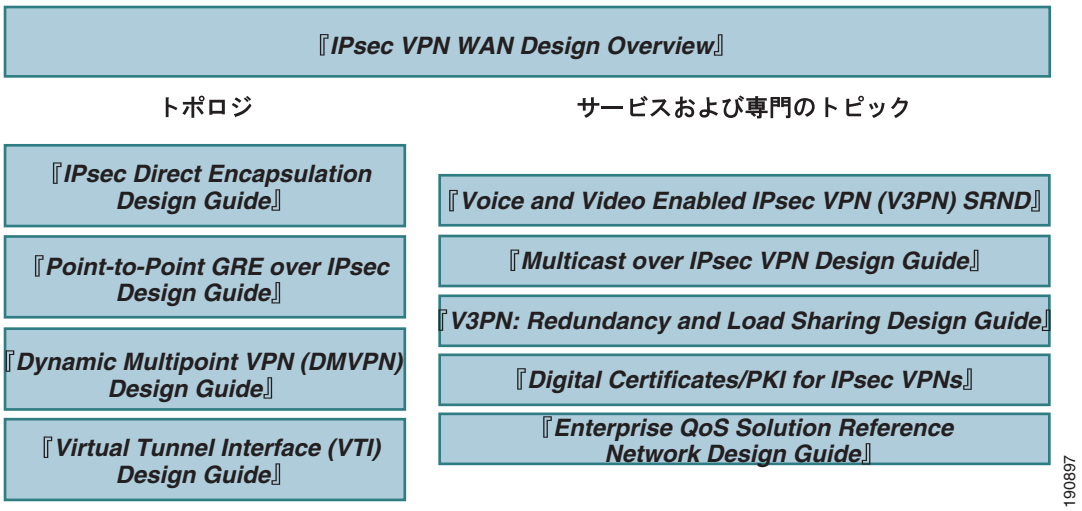
このデザイン ガイドでは、エンタープライズ Wide Area Network（WAN）接続環境でサイト間 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）システムを構築するのに必要な、総合的な機能コンポーネントを定義します。このガイドでは、Dynamic Multipoint VPN（DMVPN）のデザイン トポロジを扱います。

このガイドは、VPN ソリューションを対象とした一連のマニュアルのうちの一冊であり、最新のシスコの VPN 技術を使用し、拡張のためテストした実用的なデザイン原理に基づいています。

概要

図 1 に、IPSec VPN WAN アーキテクチャのマニュアルを示します。次の URL にアクセスしてください。http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html

図 1　　IPSec VPN WAN アーキテクチャのマニュアル



IPSec VPN WAN アーキテクチャは、IPSec を使う技術に基づいて複数のデザイン ガイドに分けられています。対象読者は、IPSec の基礎を理解していることが前提となります。『*IPsec VPN WAN Design Overview*』では、特定の IPSec VPN WAN 技術を選択する際の基準を示します。このマニュアルは、指定されたネットワーク デザインにおいて適切な技術を選択するために使用します。

本マニュアルは、Cisco DMVPN 技術の展開を目的とするユーザのデザイン ガイドとなります。このバージョンのデザイン ガイドでは Cisco IOS VPN ルータ製品に焦点を置いています。

このデザイン ガイドでは、概要、デザインの推奨事項、製品の選択、およびパフォーマンス情報の順に説明します。最後に、設定例が提示されます。

対象読者

このデザイン ガイドでは、システム エンジニアを対象に、顧客環境におけるガイドラインやベスト プラクティスを提供します。

バージョン 1.1 へのアップデート

本マニュアルのバージョン 1.1 では、Cisco ASR 1000 のハブアンドスポーク スケーラビリティ テストの結果を提供します。

対象範囲

このバージョンのデザイン ガイドは、次のソリューション アプリケーションを扱っています。

- Internetwork Operating System（IOS）が稼働する Cisco VPN ルータ
- トンネリング方式は、IPSec を介した Multipoint GRE（mGRE）および point-to-point（p2p; ポイントツーポイント）GRE トンネリング
- サイト間 VPN トポロジ
- mGRE が設定された VPN 上のルーティング プロトコルとして Enhanced IGRP（EIGRP）を使用
- スタティック GRE エンドポイントのあるダイナミック crypto ピア アドレス
- Next Hop Routing Protocol（NHRP）
- トンネル プロテクション モード
- データおよび VoIP トラフィックの統合要件
- QoS（Quality Of Service）機能は有効
- スケーラブルな耐障害デザインにおける Cisco VPN 製品のパフォーマンスの評価

マニュアルの目的

このデザイン ガイドでは、以下の用途における技術を扱っています。

- ハブアンドスポーク デザインで使用する DMVPN
- スポークツースポーク デザインで使用する DMVPN

デバイスに負荷をかけて行った、シスコによるデザインのスケーラビリティ テストの結果を、デザイン ガイダンス用に提示します。

マニュアルの構成

このガイドの内容は次のとおりです。

セクション	説明
第 1 章「DMVPN デザインの概要」	DMVPN デザイン トポロジと特徴の概要を示します。
第 2 章「DMVPN のデザインおよび実装」	デザインに関する一般的な考慮事項の概要、実装、ハイ アベイラビリティ、QoS、およびマルチキャストについて説明します。
第 3 章「スケーラビリティに関する考慮事項」	ヘッドエンドのサイズ指定、ヘッドエンド デバイス向けに展開できるシスコ製品の選択、ブランチ デバイス製品のサイズ指定および選択に関する情報など、VPN ソリューション用のシスコ製品の選択についてのガイダンスを提示します。
第 4 章「スケーラビリティ テストの結果（ユニキャストのみ）」	シスコによるテストの結果を提示し、DMVPN 構成でのさまざまなプラットフォームのスケーラビリティに関するデザイン ガイダンスを提供します。
付録 A「スケーラビリティ テスト ベッドのコンフィギュレーション ファイル」	セントラル サイトとブランチ サイトの設定について説明します。
付録 B「レガシー製品のテスト結果」	レガシー製品のスケーラビリティ テスト結果について説明します。
付録 C「略語」	略語の定義が記載されています。

CHAPTER 1

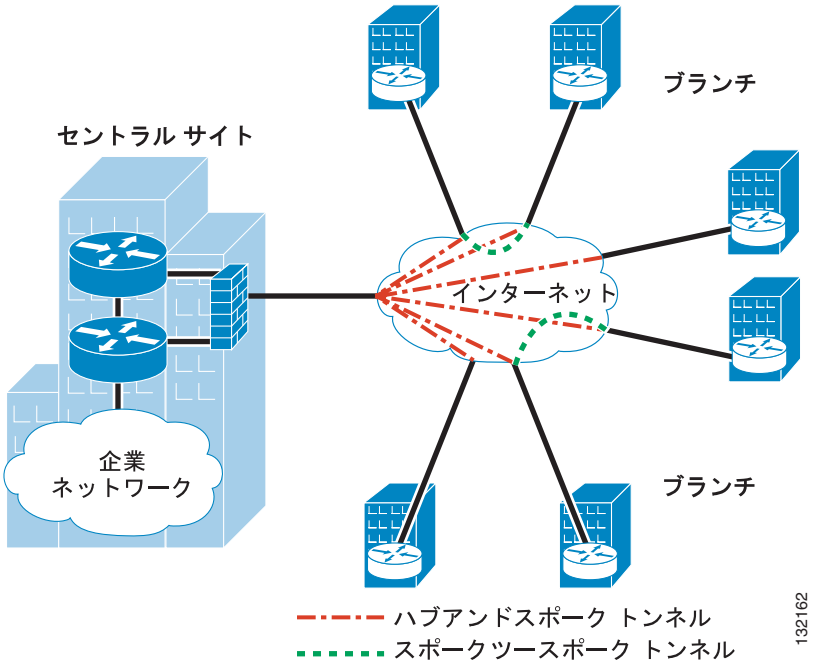
DMVPN デザインの概要

この章では、DMVPN デザイン トポロジの概要を示します。第 2 章「DMVPN のデザインおよび実装」により具体的なデザインに関する考慮事項を示します。第 3 章「スケーラビリティに関する考慮事項」にデザインを展開するために選択できるシスコ製品を示します。

概要

ここで紹介する主なトポロジは、ハブアンドスポーク展開モデルです。ここでは、主な企業リソースは大規模なセントラル サイトに置かれ、多数の中小のサイトまたはブランチ オフィスは VPN 経由で直接、セントラル サイトに接続されています。ただし、一部のシナリオでは、スポークツースポーク展開モデルを使用できます。ここでは、IPSec 暗号化を使用してブランチ オフィスの間を一時的に直接接続できます。両方の DMVPN 展開モデルを図 1-1 に示します。

図 1-1　　DMVPN 展開モデル



前提条件

このデザイン ガイドで示すデザイン方法には、次の前提条件があります。

- デザインは、顧客向けの一般的な各種トラフィックが混在したケースに対応します（第 4 章「スケーラビリティ テストの結果（ユニキャストのみ）」を参照）。
- 顧客には IP マルチキャストやルーティングのサポートなどの多様なトラフィック要件があります。mGRE およびルーティング プロトコルの使用についても、第 2 章「DMVPN のデザインおよび実装」で詳細に説明します。
- シスコ製品では適切な CPU 利用率レベルを維持してください。これに関しては、ヘッドエンド ルータとブランチ ルータ、およびソフトウェア リビジョンの推奨事項を含め、第 3 章「スケーラビリティに関する考慮事項」で詳細に説明します。
- コストは必ず考慮されますが、デザインの推奨事項では、顧客がハードウェアによる高速な暗号化を含めた現在の VPN 技術を導入するものと想定します。
- VoIP およびビデオがネットワーク要件であると想定しています。VoIP および他の遅延の影響を受けやすいトラフィックを処理するためのデザインに関する詳細な考慮事項については、このデザイン ガイドで明示的に扱いません。次の URL にある『*Voice and Video Enabled IPsec VPN (V3PN) Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND.html
- このデザインは企業が所有する VPN を用いた展開向けですが、エッジ トンネリング装置の所有権に関係なく概念と結論は妥当なものです。したがって、サービス プロバイダー管理 VPN に対しても有効です。

デザインのコンポーネント

VPN は、専用線、フレームリレー、ATM などの従来の WAN 技術に代わるものを提供します。VPN 技術により、プライベート WAN をインターネットなどの公共の伝送経路上に構築できます。LAN 間 VPN は主に、企業のブランチ オフィスとセントラル サイトを接続するために導入されています。

従来のプライベート WAN サービスの企業顧客が持つ要件（マルチプロトコルのサポート、ハイアベイラビリティ、スケーラビリティ、セキュリティなど）は、VPN においても要件となります。VPN は通常、プライベート WAN サービスよりも高い費用効果と柔軟性でこれらの要件を満たすことができます。

次に、この DMVPN デザインの重要なコンポーネントを示します。

- セントラル キャンパスで VPN ヘッドエンド終端装置として機能するシスコのハイエンド VPN ルータ（ヘッドエンド デバイス）
- ブランチ オフィスで VPN ブランチ終端装置として機能するシスコの VPN アクセス ルータ（ブランチ デバイス）
- ヘッドエンドとブランチを相互接続する DMVPN ハブアンドスポーク
- ブランチ間を相互接続する DMVPN スポークツースポーク（任意）
- WAN 相互接続メディアとして機能するサードパーティ ISP から取得したインターネット サービス

シスコ VPN ルータは VPN 展開に適切な選択肢です。このルータはフレームリレーまたは専用線ネットワークが従来提供してきたネットワーク要件に対応できます。これらの要件には、マルチキャスト、遅延の影響を受けやすいトラフィック、およびルーティング プロトコルのサポートが含まれます。ヘッドエンド製品およびブランチ製品の選択については、第 3 章「スケーラビリティに関する考慮事項」を参照してください。

デザイン トポロジ

DMVPN デザインでは、次の 2 つのトポロジを実装できます。

- デュアル ハブ / デュアル DMVPN クラウド
- デュアル ハブ / シングル DMVPN クラウド

両方のトポロジで、冗長性のため 2 つのハブまたはヘッドエンドが推薦されます。DMVPN クラウドは、同じアドレス サブネットを共有する multipoint GRE（mGRE）インターフェイスまたは point-to-point（p2p; ポイントツーポイント）GRE インターフェイスのいずれか（または 2 つの組み合わせ）が設定されたルータの集合です。プライマリ ルータと同じ DMVPN サブネットで 2 つめのハブ ルータを使用すると、ハイ アベイラビリティを提供できます。これは、一般的にシングル DMVPN クラウド トポロジと呼ばれます。2 つめのハブ ルータも自身の DMVPN サブネットを処理できます。これはデュアル DMVPN クラウド トポロジとして知られています。デュアル ハブ / シングル DMVPN トポロジは、トンネル外部のメカニズムを使用してフェールオーバーに適切なハブを決定するので、一般的には推奨されません。対照的に、デュアル DMVPN サブネット（デュアル DMVPN クラウド トポロジ）を使用するヘッドエンドは、トンネル内で動作するルーティング プロトコルを使用して、パス選択を決定します。

DMVPN クラウド トポロジは、ハブアンドスポークまたはスポークツースポーク展開モデルのいずれかをサポートできます。ハブアンドスポーク展開モデルでは、各ヘッドエンドに mGRE インターフェイス、各ブランチに p2p GRE インターフェイスを設定しています。スポークツースポーク展開モデルでは、ヘッドエンドとブランチ両方に mGRE インターフェイスを設定しています。

図 1-2 および図 1-3 に、2 つの DMVPN クラウド トポロジを示します。このトポロジでのさまざまな展開モデルの詳細については、次のセクションで説明します。

図 1-2　　デュアル DMVPN クラウド トポロジ

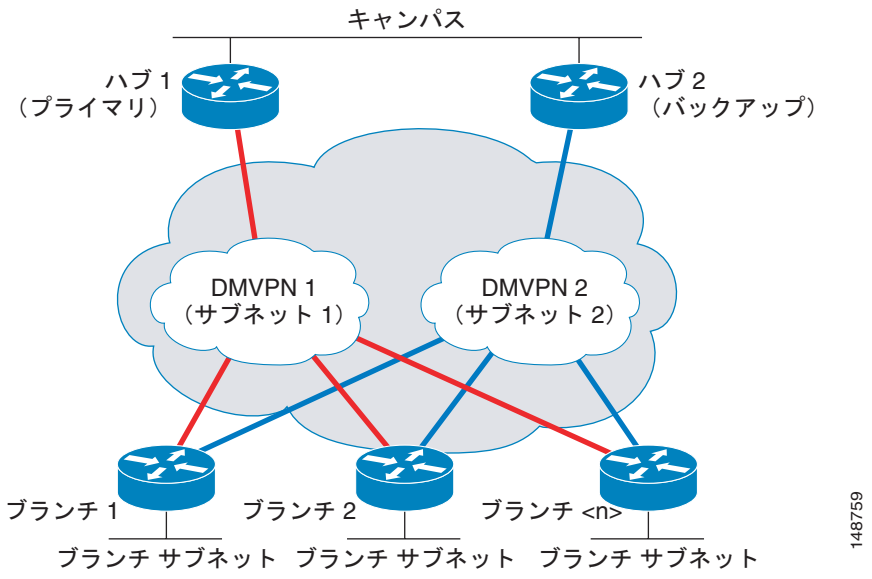
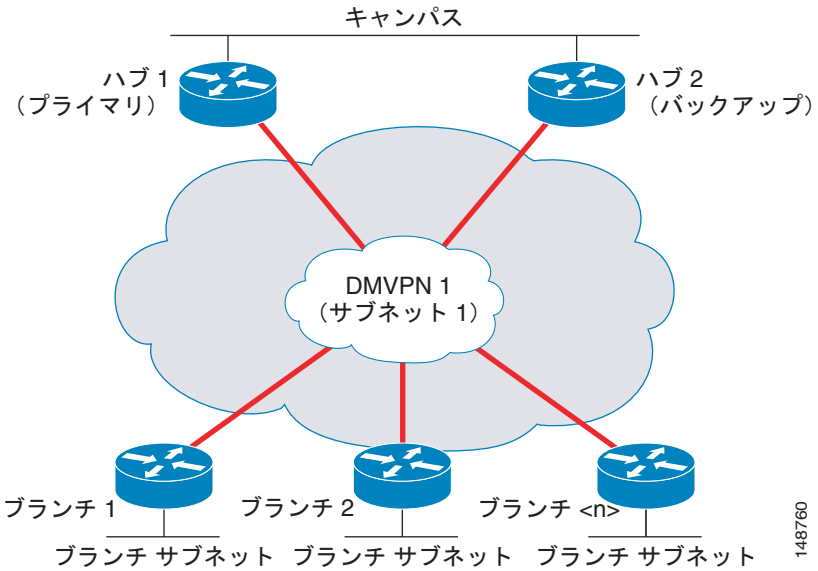


図 1-3　シングル DMVPN クラウド トポロジ



2 つのトポロジの明確な違いはブランチ ルータです。シングル DMVPN サブネットでは、ブランチ ルータに 1 つの mGRE トンネルがあり、両方のヘッドエンドは mGRE インターフェイスを介してこのトンネルにマッピングされます。デュアル DMVPN トポロジでは、ブランチ ルータには単一のヘッドエンドに接続する単一のトンネルがあります。OSPF または EIGRP などの標準的なルーティング プロトコルを使用して、アクティブなハブを決定します。

デュアル DMVPN クラウド トポロジ

次の 2 つの展開モデルはデュアル DMVPN クラウド トポロジ デザインに実装できます。

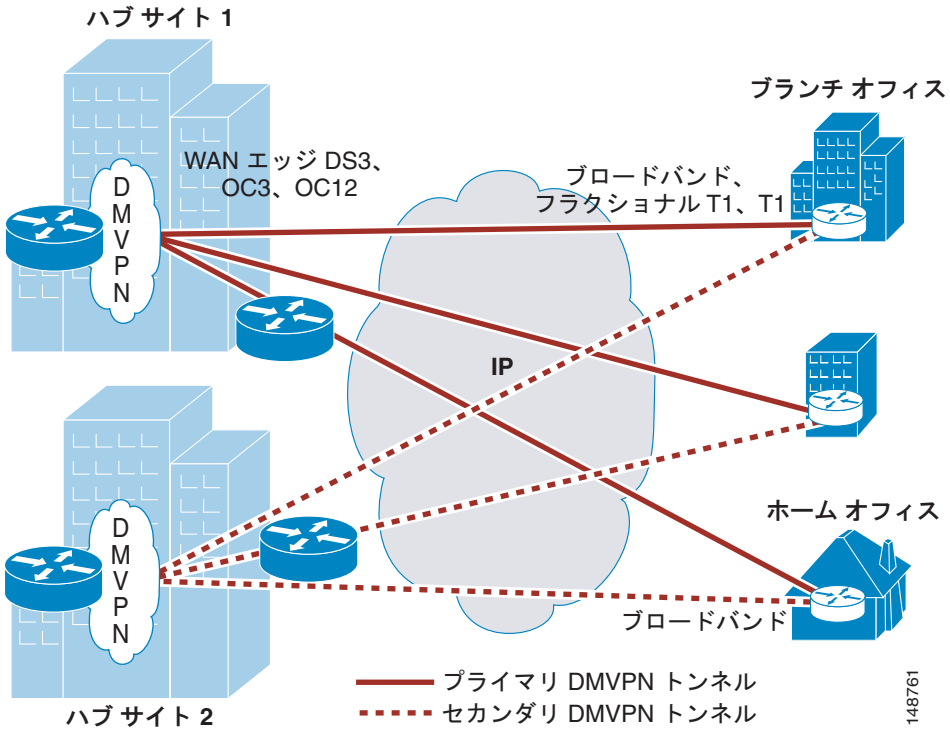
- ハブアンドスポーク
- スポークツースポーク

これらの展開モデルについては、次のセクションでそれぞれ説明します。

デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル

デュアル DMVPN クラウド トポロジのハブアンドスポーク展開モデルは、2 つのヘッドエンド ルータ（ハブ 1 およびハブ 2）で構成されます。各ルータには、すべてのブランチ ルータに接続された 1 つまたは複数の mGRE トンネル インターフェイスがあります（図 1-4 を参照）。

図 1-4　デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル



各 DMVPN クラウドは固有の IP サブネットを表します。1 つの DMVPN クラウドはプライマリとみなされ、すべてのブランチ トラフィックが通過します。各ブランチには、2 つの p2p GRE トンネル インターフェイスが設定されています。このインターフェイスはそれぞれ各ヘッドエンドに接続されます。この展開モデルでは、ブランチ間にトンネルはありません。ブランチ間通信はハブ ルータ経由で行われます。これは、従来のフレームリレー ネットワークと非常に近いものです。ルーティング メトリックを使用して、トラフィックをプライマリ ヘッドエンド ルータ（ハブ 1）に送ります。

ハブアンドスポーク展開モデル — ヘッドエンド システム アーキテクチャ

次の 2 つのヘッドエンド システム アーキテクチャは、スケーラビリティの要件に応じて、ハブアンドスポーク トポロジで実装できます。

- シングル ティア ヘッドエンド アーキテクチャ
- デュアル ティア ヘッドエンド アーキテクチャ

シングル ティア ヘッドエンド アーキテクチャ

シングル ティア ヘッドエンド アーキテクチャでは、mGRE および暗号機能は同じルータ CPU で処理されます。図 1-5 に、このハブアンドスポーク トポロジを示します。

図 1-5　シングル ティア ヘッドエンド アーキテクチャ

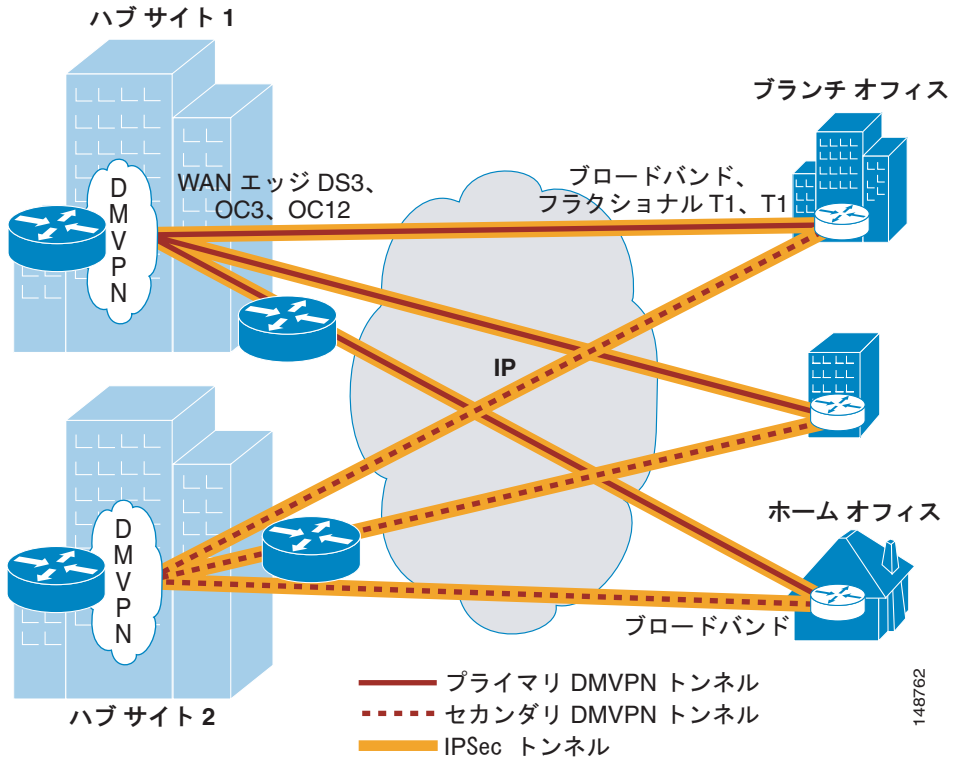


図 1-5 のソリューションは、ハブアンドスポーク展開モデルのデュアル DMVPN クラウド トポロジです。両方のヘッドエンドは、規定数のブランチ オフィスに対する複数の mGRE トンネルを処理する、mGRE および暗号トンネル集約ルータです。ヘッドエンドは、セントラル サイトで VPN トンネルを終端するほかに、DMVPN クラウド パスの選択に関係なく EIGRP または OSPF などの IP ルーティング プロトコルを使用してブランチ ルートをアドバタイズできます。

デュアル ティア ヘッドエンド アーキテクチャ

デュアル ティア ヘッドエンド アーキテクチャでは、mGRE および暗号機能は同じルータ CPU で処理されません。図 1-6 に、このハブアンドスポーク トポロジを示します。

図 1-6　デュアル ティア ヘッドエンド アーキテクチャ

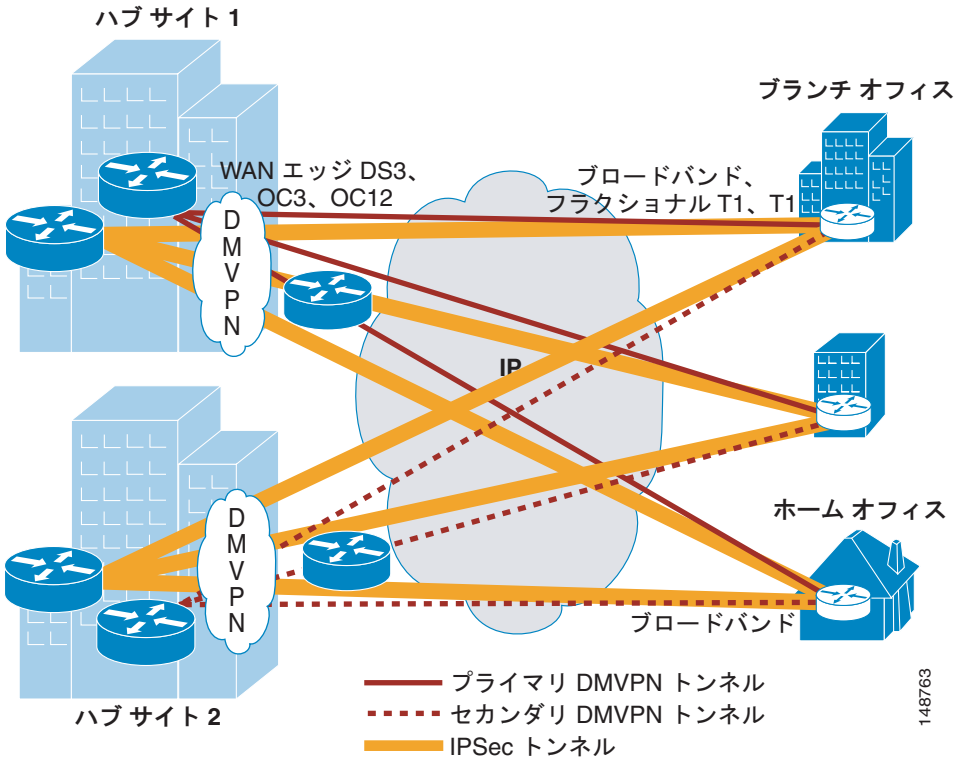


図 1-6 のソリューションは、ハブアンドスポーク展開モデルのデュアル DMVPN クラウド トポロジです。別々の mGRE ヘッドエンドと暗号ヘッドエンドがあり、ともに規定数のブランチ オフィスに対する複数の mGRE トンネルを処理します。暗号ヘッドエンドは各ブランチからの VPN トンネルをセントラル サイトで終端し、mGRE ヘッドエンドにトラフィックを転送します。mGRE ヘッドエンドは EIGRP または OSPF などの IP ルーティング プロトコルを使用してブランチ ルートをアドバタイズします。

デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデルでのブランチ ルータの考慮事項

ハブアンドスポーク展開モデルのデュアル DMVPN クラウド トポロジのブランチは、ブランチ オフィスからセントラル サイトに、p2p GRE over IPSec トンネルを提供します。VPN トンネルを終端するほかに、ブランチ ルータは通常 WAN アクセスを提供し、一部の実装ではファイア ウォールとして機能します。

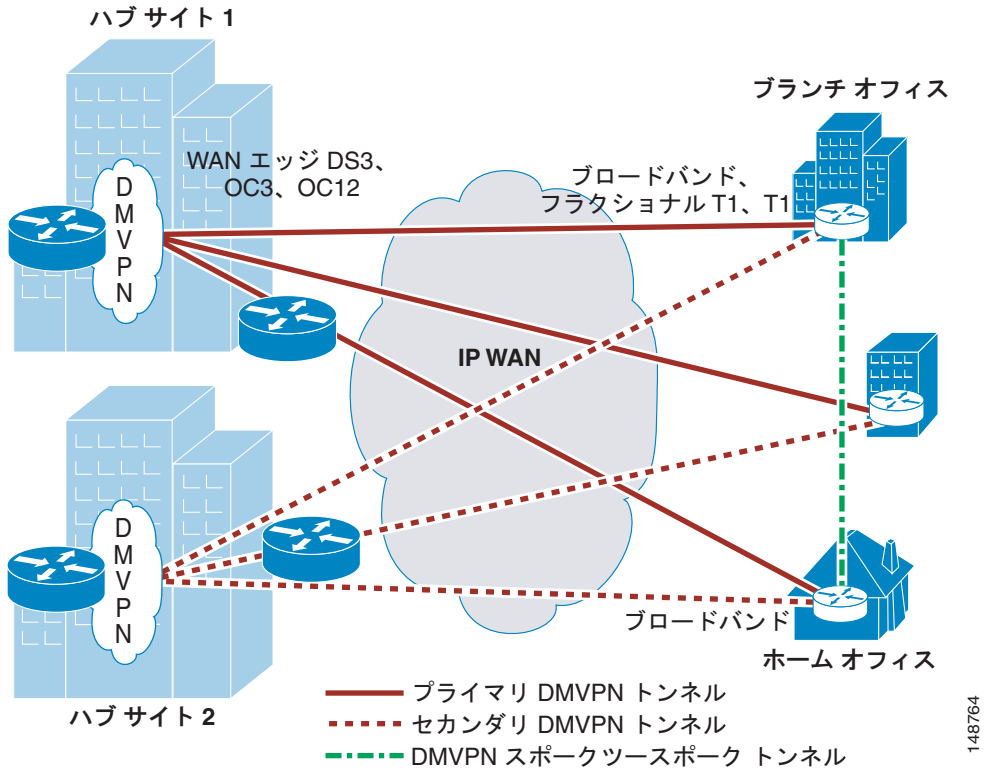
ブランチ ルータのパブリック IP アドレスは、静的に定義されたかまたは動的に割り当てられた IP アドレスです。p2p GRE トンネルと暗号トンネルの両方が、パブリック IP アドレスを発信元としています。このアドレスは、ブランチのプライベート アドレスへのマッピングを提供するヘッドエンドに登録されます。

デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル

スポークツースポーク展開モデルのデュアル DMVPN クラウド トポロジは、2 つのヘッドエンド ルータ（ハブ 1 およびハブ 2）で構成されます。各ルータには、すべてのブランチ ルータに接続された 1 つまたは複数の mGRE トンネル インターフェイスがあります（図 1-7 を参照）。各 DMVPN クラウドは固有の IP サブネットを表します。1 つの DMVPN クラウドはプライマリとみなされ、すべてのブランチ トラフィックが通過します。各ブランチ ルータでは、冗長性のため各 DMVPN クラウドに対して mGRE インターフェイスがあります。すべてのブランチ間の通信は、ダイナミック スポークツースポーク トンネルが作成されるまで、プライマリ ヘッドエンド

を通過します。ダイナミック スポークツースポーク トンネルは 1 つの DMVPN クラウドまたはサブネット内にある必要があります。スポークツースポーク トンネルは 2 つの DMVPN クラウドの間には作成できません。

図 1-7　デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル



スポークツースポーク展開モデル — ヘッドエンド システム アーキテクチャ

スポークツースポーク展開モデルのデュアル DMVPN クラウド トポロジは、シングル ティア ヘッドエンド アーキテクチャのみをサポートします。スポークツースポーク接続はトンネル プロファイルを使用する必要があるので、デュアル ティア ヘッドエンド アーキテクチャは、このトポロジの有効なオプションではありません。暗号トンネルと GRE トンネルが異なるエンドポイントを使用している場合、トンネル プロファイルは使用できません。

シングル ティア ヘッドエンド アーキテクチャ

シングル ティア ヘッドエンド アーキテクチャでは、mGRE および暗号機能は同じルータ CPU で処理されます。図 1-8 に、このスポークツースポーク トポロジを示します。

図 1-8　シングル ティア ヘッドエンド アーキテクチャ

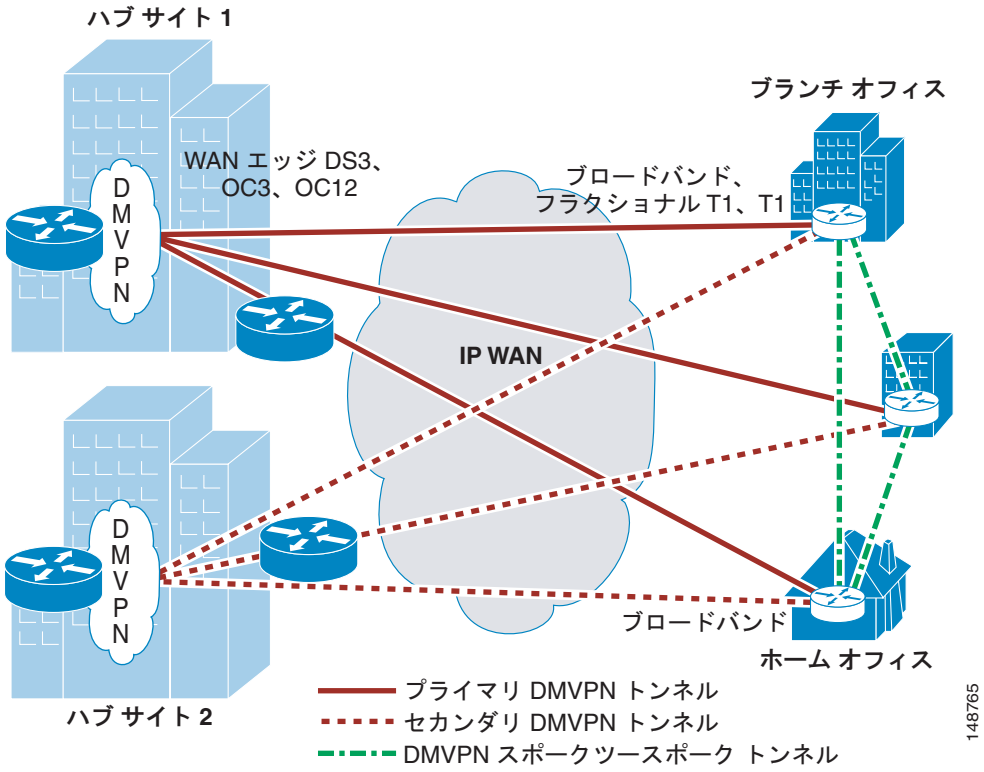


図 1-8 のソリューションは、スポークツースポーク展開モデルのデュアル DMVPN クラウド トポロジです。両方のヘッドエンドは、規定数のブランチ オフィスに対する複数の mGRE トンネルを処理する、mGRE および暗号トンネル集約ルータです。ヘッドエンドは、セントラル サイトで VPN トンネルを終端するほかに、DMVPN クラウド パスの選択に関係なく EIGRP または OSPF などの IP ルーティング プロトコルを使用してブランチ ルートをアドバタイズできます。

デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデルでのブランチ ルータの考慮事項

スポークツースポーク展開モデルのデュアル DMVPN クラウド トポロジのブランチは、ブランチ オフィスからセントラル サイトに、mGRE over IPSec トンネルを提供し、ブランチ間通信を確立できます。VPN トンネルを終端するほかに、ブランチ ルータは通常 WAN アクセスを提供し、一部の実装ではファイアウォールとして機能します。

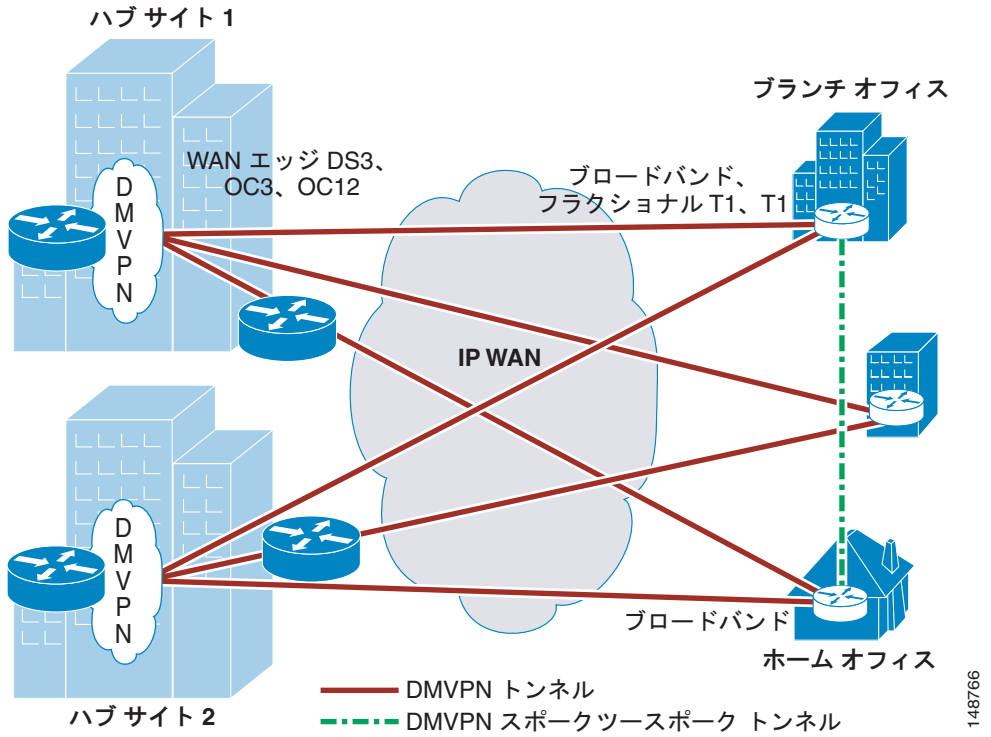
ブランチ ルータのパブリック IP アドレスは、静的に定義されたかまたは動的に割り当てられた IP アドレスです。p2p GRE トンネルと暗号トンネルの両方が、パブリック IP アドレスを発信元としています。このアドレスは、ブランチのプライベート アドレスへのマッピングを提供するヘッドエンドに登録されます。

シングル DMVPN クラウド トポロジ

シングル DMVPN クラウド トポロジでは、同じ DMVPN サブネット上に 2 つのヘッドエンド ルータがあります。したがって、ブランチ ルータには mGRE インターフェイスが必要です。この mGRE インターフェイスにより、ルーティング テーブルによって指示されれば、ブランチ ルータはブランチ間通信を試行します。このことから、このモデルはスポークツースポーク トポロジだと考えられます。ハブアンドスポーク展開モデルは、1 つのヘッドエンド ルータのみがあるシングル DMVPN クラウド トポロジで構成できます。ヘッドエンド ルータのフェールオーバー メカニズムがないので、この構成のテストは行っていませんし、推奨されません。

スポークツースポーク展開モデルのシングル DMVPN クラウド トポロジにも 2 つのヘッドエンド ルータが使われています。ヘッドエンド ルータは、デュアル DMVPN クラウド トポロジのヘッドエンド ルータの設定と同様に設定されていますが、1 つの IP サブネットのみを使用しています。ヘッドエンドが同じ場所に展開されている場合、トラフィックを 2 つのヘッドエンド ルータの間でロード バランシングできます。このトポロジでは、すべてのブランチおよびヘッドエンド mGRE インターフェイスは 1 つのサブネット上にあります。これは、複数のサブネット（各 DMVPN クラウド）が存在するデュアル DMVPN クラウド トポロジとは異なります。このシナリオでは、ルーティング プロトコルの制御には制限があり、非対称ルーティングの問題が発生する可能性があります。図 1-9 に、この展開モデルを示します。

図 1-9　シングル DMVPN クラウド トポロジ — スポークツースポーク展開モデル



これは有効なトポロジ オプションですが、このトポロジは推奨されません。このマニュアルでは詳細な説明を行いません。スポークツースポーク展開モデルが必要な場合、デュアル DMVPN クラウド トポロジを使用してください。

ベスト プラクティスと既知の制限事項

ここでは、デュアル DMVPN クラウド トポロジ デザインのベスト プラクティスと制限事項の概要について説明します。詳細については、第 2 章「DMVPN のデザインおよび実装」を参照してください。

ハブアンドスポーク展開モデルのベスト プラクティスの概要

ここでは、ハブアンドスポーク展開のデュアル DMVPN クラウド トポロジのベスト プラクティスについて説明します。このトポロジでは、ルーティング プロトコルを含めた IP マルチキャスト（IPmc）トラフィックをサポートします。

次に、一般的なベスト プラクティスを示します。

- トンネル モードで IPSec を使用します。
- 転送データの暗号化のために Triple DES（3DES）または AES を設定します（特定の国への暗号化アルゴリズムの輸出は法律によって禁止されています）。
- Dead Peer Detection（DPD）を実装して、ピア間の通信の喪失を検出します。
- IPSec のハードウェア アクセラレーションを導入してルータの CPU のオーバーヘッドを最小限にし、遅延およびジッタを抑制する必要のあるトラフィックをサポートして、コスト パフォーマンスを最高にします。
- MTU サイズの設定、または Path MTU Discovery（PMTUD）の使用によって、顧客ネットワーク上で IPSec パケット フラグメンテーションを最小限にします。
- スケーラブルなトンネル認証用に、デジタル証明書 /PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）を使用します。
- ダイナミック ルーティング用に、経路集約を行うルーティング プロトコル（EIGRP または OSPF など）を設定します。
- QoS（Quality of Service）サービス ポリシーをヘッドエンドおよびブランチ ルータ インターフェイス上に適宜設定して、インターフェイスの輻輳問題を解消し、優先度の高いトラフィックを廃棄しないようにします。

次に、一般的なヘッドエンドのベスト プラクティスを示します。

- ヘッドエンドが DMVPN デザインの重要なスケーラビリティ パラメータよりも低くなるように構成をデザインします。
  - mGRE インターフェイスごとのスポークの最大数
  - ヘッドエンドごとのスポークの最大総数

  詳細については、第 3 章「スケーラビリティに関する考慮事項」を参照してください。
- 次の考慮事項に基づいて、ヘッドエンド用のシスコ VPN ルータ製品を選択します。
  - 集約するトンネルの数
  - 集約するスループットの最大値（packets per second [pps; パケット / 秒] と bits per second [bps; ビット / 秒] 両方）
  - 耐障害性およびフェールオーバーを想定したパフォーマンス マージン
  - デザイン目標より低い CPU 利用率の維持

  詳細については、第 3 章「スケーラビリティに関する考慮事項」を参照してください。
- 複数のヘッドエンド ルータにブランチ オフィス トンネルを分散して、ハブの負荷と集約容量を均衡化します。

次に、シングル ティア ヘッドエンド アーキテクチャのベスト プラクティスを示します。

- mGRE および IPSec トンネル プロテクションをヘッドエンド ルータに設定して、新しいブランチの設定とプロビジョニングを簡素化します。

次に、デュアル ティア ヘッドエンド アーキテクチャのベスト プラクティスを示します。

- 暗号化ヘッドエンドでダイナミック crypto map を使用して、必要な IPSec 設定の量を削減します。

次に、ブランチ オフィスのベスト プラクティスを示します。

- p2p GRE および IPSec トンネル プロテクションをブランチに設定します。
- ルーティング メトリックを使用してプライマリおよびセカンダリ パスを指定するため、別々のヘッドエンドへのトンネルを 2 つ設定します。
- 次の考慮事項に基づいて、ブランチ オフィス用のシスコ VPN ルータ製品を選択します。
  - 最大スループット（pps と bps 両方）

  - ファイアウォール、IPS、および NAT/PAT など、ルータで動作する他の統合サービスの許可

詳細については、第 3 章「スケーラビリティに関する考慮事項」を参照してください。

- QoS と IPSec の両方が同じシステムで実行される VPN デザインに **qos pre-classify** を設定します。ネットワーク管理者は動作が正しいか検証してください。

ハブアンドスポーク展開モデルの既知の制限事項の概要

ここでは、ハブアンドスポーク展開のデュアル DMVPN クラウド トポロジに関する既知の制限事項の概要を説明します。

次に、一般的な制限事項を示します。

- mGRE アクセラレーションは、VPNSM または VPN SPA を搭載した Cisco Catalyst 6500/7600 ルータでは現在サポートされていません。どちらの VPN サービス モジュールも mGRE トンネル キーをサポートしていないからです。これらのプラットフォームは、mGRE トンネル キーを必要としないデザインで使用できます。詳細については、第 2 章「DMVPN のデザインおよび実装」を参照してください。
- DMVPN デザイン上での IP マルチキャストのサポートについては、スケーラビリティに関する重要な制限事項があります。詳細については、次の URL にある『*Multicast over IPsec VPN Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html
- IPSec トンネル プロテクションによって現在サポートされていないので、**qos pre-classify** を mGRE トンネル インターフェイスに適用してください。

次に、一般的なヘッドエンドの制限事項を示します。

- サービス ポリシーをトンネル レベルで設定できないので、制限された QoS を外部インターフェイスのハブ / ブランチ方向に実装できます。これはブランチ単位ではなく、インターフェイス レベルの QoS で、暗号化のあとで実行されます。

次に、デュアル ティア ヘッドエンド アーキテクチャの制限事項を示します。

- トンネル プロテクションはサポートされていません。
- **qos pre-classify** は、mGRE トンネルおよび VPN トンネル用に 2 つの異なるヘッドエンドを実装しているアーキテクチャではサポートされません。

次に、ブランチ オフィスの制限事項を示します。

- 必ず、ブランチ側からヘッドエンド ルータに対して DMVPN トンネルの確立を開始する必要があります。ヘッドエンドからブランチ ルータに対してトンネルの確立を開始できません。

スポークツースポーク展開モデルのベスト プラクティスの概要

ここでは、スポークツースポーク展開のデュアル DMVPN クラウド トポロジのベスト プラクティスを要約します。これらのベスト プラクティスは、ハブアンドスポーク展開のベスト プラクティス*と共に*考慮する必要があります。

次に、一般的なベスト プラクティスを示します。

- IPSec SA ライフタイムを考慮し、NHRP ホールド タイムを使って目的のトンネル持続タイマーを設定します。詳細については、第 2 章「DMVPN のデザインおよび実装」を参照してください。
- /24 プレフィクスを使用して特定の DMVPN クラウド（サブネット）内のスポーク数を実用的なものにします。複数の mGRE インターフェイスを DMVPN ハブに展開してスケーラビリティを向上します。

- スポークツースポーク展開モデル用に EIGRP または RIPv2 ルーティング プロトコルを使用します。

次に、ブランチ オフィスのベスト プラクティスを示します。

- ブランチ ルータが受け入れ可能なスポークツースポーク トンネルの最大数を制限し、トンネルがスポークツーハブツースポークに接続するよう IKE コール アドミッション コントロール（IKE CAC）を設定します。

  詳細については、IKE CAC（p.2-10）を参照してください。
- mGRE をブランチ ルータに設定してください。

スポークツースポーク展開モデルの既知の制限事項の概要

ここでは、スポークツースポーク展開のデュアル DMVPN クラウド トポロジに関する既知の制限事項の概要を説明します。これらの制限事項は、ハブアンドスポーク展開の既知の制限事項と*共に*考慮する必要があります。

次に、一般的な制限事項を示します。

- ODR はスポークツースポーク トポロジに使用できません。
- OSPF は、スケーリングの制限事項により、スポークツースポーク展開モデルのルーティング プロトコルとして使用しないでください。詳細については、第 3 章「スケーラビリティに関する考慮事項」を参照してください。

次に、ヘッドエンドの制限事項を示します。

- mGRE および IPSec の送信元および宛先 IP アドレスは、スポークツースポーク モードが機能するために同一にしてください。これは、デュアル ティア ヘッドエンド アーキテクチャでは機能できません。

次に、ブランチ オフィスの制限事項を示します。

- 非常に制限された QoS をスポーク間に提供できます。したがって、VoIP やビデオなどの遅延の影響を受けやすいアプリケーションは、スポークツースポーク DMVPN 展開では「ベストエフォート型」とみなされます。
- ダイナミック ルーティングは、スポークツースポーク トンネル上のスポーク間では交換されません。その結果、トンネルがダウン状態であることを認識せずに通信が失われる可能性があります。
- pNAT デバイスの背後のスポークは、スポークツースポーク トンネルを確立できません。
- IP マルチキャスト トラフィックはスポーク間では交換できません。
- スポークツースポーク トポロジでは、あらゆるトラフィックにおいて IPSec トンネルをその DMVPN クラウド内の別のブランチに移行できます。これは L3（ルーティング）レベルで行われるので、IP ユニキャスト トラフィックはそのスポークツースポーク トンネルで伝送されます。これは、一部の展開ではセキュリティ上の問題になります。チェック ポイントとしてヘッドエンドを使用しないのでウイルス、ワーム、または攻撃ソフトウェアがブランチ間で広がる可能性があるためです。スポークツースポーク対応ブランチごとに、IPS などの他の保護メカニズムを実装してください。
- IKE CAC には制限事項と、ブランチ プラットフォームごとに最大数の ISAKMP SA があります。詳細については、IKE CAC（p.2-10）を参照してください。

これらの推奨事項の詳細については、次章以降で説明します。

CHAPTER 2

DMVPN のデザインおよび実装

顧客用の Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の構成をデザインする際には、ハイ アベイラビリティや耐障害性などのデザインにおけるより幅広い考慮事項、IP マルチキャスト、および QoS（Quality of Service）を組み入れることが不可欠です。この章では、最初にデザインの一般的な考慮事項について説明し、次に実装、ハイ アベイラビリティ、QoS、およびマルチキャストについて説明します。

デザインの考慮事項

ヘッドエンド サイトは一般的に DS3、OC3、または OC12 の帯域幅で接続されていますが、ブランチ オフィスはフラクショナル T1、T1、E1、T3、またはブロードバンド DSL かケーブル アクセス（次第に増加しつつある）によって接続されます。

冗長性を提供するには、ブランチ ルータにキャンパス ヘッドエンドへのトンネルを 2 つ以上設定してください。これらのヘッドエンド ルータは、地理的に分離させるか、または同じ場所に展開することができます。最大限の保護を提供するために、ヘッドエンドとサイトの両方に冗長機能を実装してください。このデザイン ガイドでは、ハブアンドスポーク展開モデルとスポークツースポーク展開モデルの両方を使った、デュアル DMVPN クラウド トポロジに焦点を当てています。

デュアル DMVPN クラウド トポロジの各展開モデルには、次の 3 つのコントロール プレーンがあります。IPSec コントロール プレーン、Generic Routing Encapsulation（GRE）コントロール プレーン、およびルーティング コントロール プレーンです。どのヘッドエンド システム アーキテクチャを選ぶかにより、各コントロール プレーンの実装方法が決定されます。次のセクションで、詳細について説明します。

トポロジ

次の 2 つのトポロジを DMVPN デザインで実装できます。

- デュアル ハブ / デュアル DMVPN クラウド
- デュアル ハブ / シングル DMVPN クラウド

シスコは DMVPN デザインにはデュアル ハブ / デュアル DMNPN クラウド トポロジを推奨しているため、このデザイン ガイドでは、このトポロジについてのみ説明します。デュアル トポロジでは、シングル トポロジと比較して、ネットワーク マネージャがパス選択においてより優れた制御を行うことができます。さらに、プライマリ フェールオーバー方式としてダイナミック ルーティング プロトコルを使用します。シングル クラウド トポロジは、NHRP ハンドル エラー イベントに依存します。デュアル DMVPN クラウド トポロジでは、ハブアンドスポーク展開モデルとスポークツースポーク展開モデルの両方をサポートできます。

ハブアンドスポーク展開モデルは、最も一般的な展開モデルです。このモデルは最もスケーラブルで、従来のレイヤ 2 専用線、フレームリレー、または ATM ハブアンドスポーク型ネットワークの大部分を模倣します。ヘッドエンドには mulitpoint GRE（mGRE）インターフェイスが設定され、ブランチには point-to-point（p2p; ポイントツーポイント）GRE インターフェイスが設定されます。

スポークツースポーク展開モデルでは、ブランチは、相互通信のために、同じ DMVPN クラウド内のほかのブランチ間にトンネルを動的に作成できます。この展開モデルはフルメッシュ トポロジで、ヘッドエンドとすべてのブランチの両方で mGRE インターフェイスを設定してください。

デュアル DMVPN ハブアンドスポーク

デュアル クラウド トポロジでのハブアンドスポーク展開モデルは、2 つのヘッドエンド ルータで構成されており、各ヘッドエンド ルータには、すべてのブランチ ルータに接続される 1 つまたは複数の mGRE トンネル インターフェイスがあります。各 DMVPN クラウドは固有の IP サブネットを表します。1 つの DMVPN クラウドはプライマリとみなされ、すべてのブランチ トラフィックが通過します。各ブランチには、p2p GRE トンネル インターフェイスが設定されていて、インターフェイスはそれぞれ各ヘッドエンドに接続されます。この展開モデルでは、1 つのブランチを別のブランチに接続するトンネルはありません。ブランチ間のトラフィックは、ハブ ルータを経由します。どのヘッドエンドが優先パスになるのかを決定するために、ルーティング メトリックが使用されます。

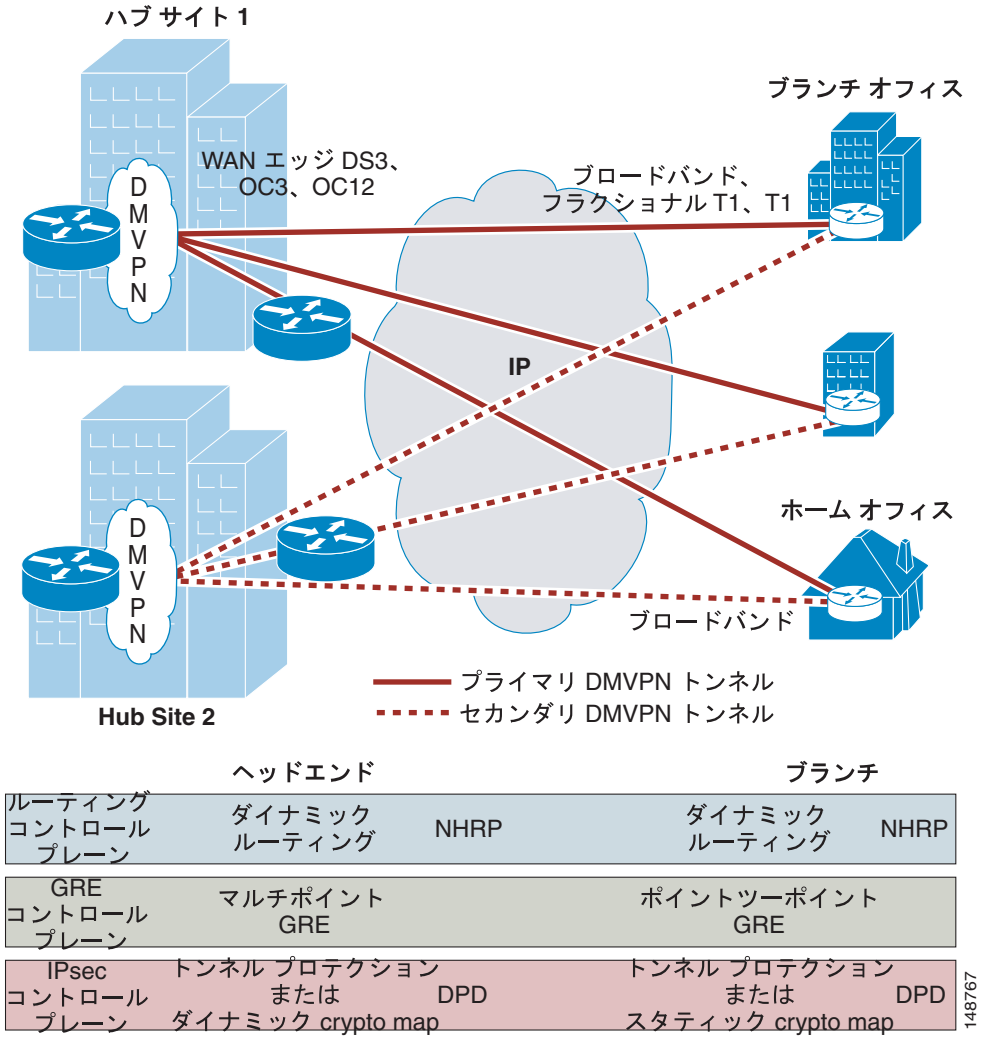
このデザイン ガイドでは、次の 2 つのヘッドエンド システム アーキテクチャについて説明します。

- シングル ティア ヘッドエンド アーキテクチャ — mGRE 機能と暗号機能の両方を 1 つのルータ プロセッサに組み込みます。
- デュアル ティア ヘッドエンド アーキテクチャ — mGRE 機能と暗号機能を 2 つの異なるルータまたはシャーシに分割します。

デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）

図 2-1 に、DMVPN 構成でのシングル ティア ヘッドエンド アーキテクチャを示します。

図 2-1　デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）

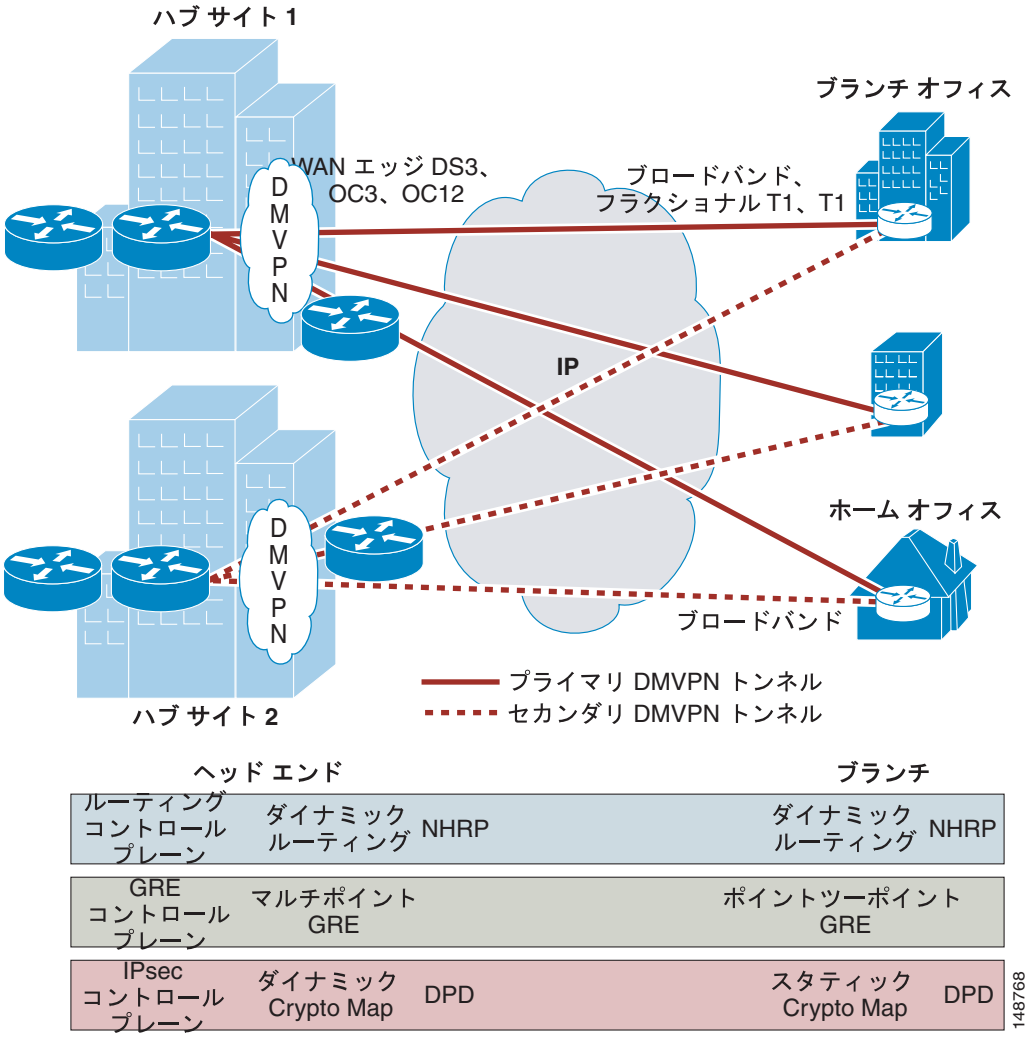


シングル ティア ヘッドエンド アーキテクチャでは、上記の 3 つのコントロール プレーンをすべて 1 つのルータに組み込みます。このアーキテクチャはスケーラビリティに影響を及ぼし、セントラル CPU がゲーティングの要因となります。

デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（デュアル ティア ヘッドエンド アーキテクチャ）

図 2-2 に、DMVPN 構成でのデュアル ティア ヘッドエンド アーキテクチャを示します。

図 2-2　デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル（デュアル ティア ヘッドエンド アーキテクチャ）



デュアル ティア ヘッドエンド アーキテクチャでは、上記の 3 つのコントロール プレーンを 2 つのルータに組み込みます。ルーティング コントロール プレーンと GRE コントロール プレーンが 1 つのルータに収容され、IPSec コントロール プレーンが別のルータに収容されます。さまざまなプラットフォームの制限（特に CPU の依存関係や耐障害性）を考慮すると、機能を分離することが最良のスケーラブルなソリューションとなります。

デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル

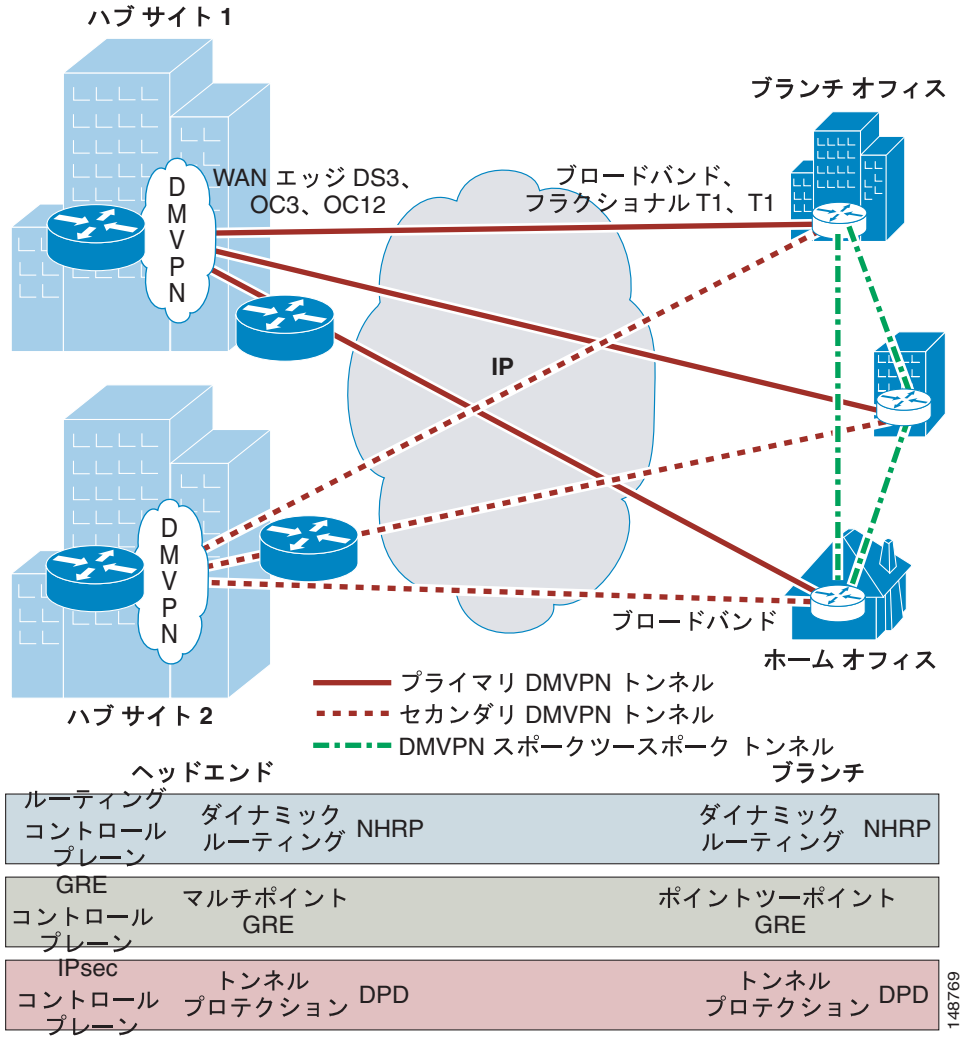
デュアル DMVPN トポロジでのスポークツースポーク展開モデルは、2 つのヘッドエンド ルータで構成されており、各ヘッドエンド ルータには、すべてのブランチ ルータに接続される 1 つまたは複数の mGRE トンネル インターフェイスがあります。各 DMVPN クラウドは固有の IP サブネットを表します。1 つの DMVPN クラウドはプライマリとみなされ、すべてのブランチ トラフィックが通過します。各ブランチ ルータでは、冗長性のため各 DMVPN クラウドに対して mGRE インターフェイスがあります。すべてのブランチ間の通信は、ダイナミック スポークツー

スポーク トンネルが作成されるまで、プライマリ ヘッドエンドを通過します。ダイナミック スポークツースポーク トンネルは 1 つの DMVPN クラウドまたはサブネット内にある必要があります。2 つの DMVPN クラウドの間にスポークツースポーク トンネルを動的に作成することはできません。

デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）

図 2-3 に、DMVPN 構成でのシングル ティア ヘッドエンド アーキテクチャを示します。

図 2-3　デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル（シングル ティア ヘッドエンド アーキテクチャ）



シングル ティア ヘッドエンド アーキテクチャでのデュアル DMVPN クラウド トポロジ スポークツースポーク展開モデルは、ヘッドエンドおよびブランチ内のすべての GRE インターフェイスが mGRE インターフェイスであることを除いて、ハブアンドスポーク展開モデルときわめて類似しています。ブランチ ルータでは、ほかのブランチ オフィスからのダイナミック トンネルの受け入れと、ダイナミック トンネルの確立の開始が可能です。

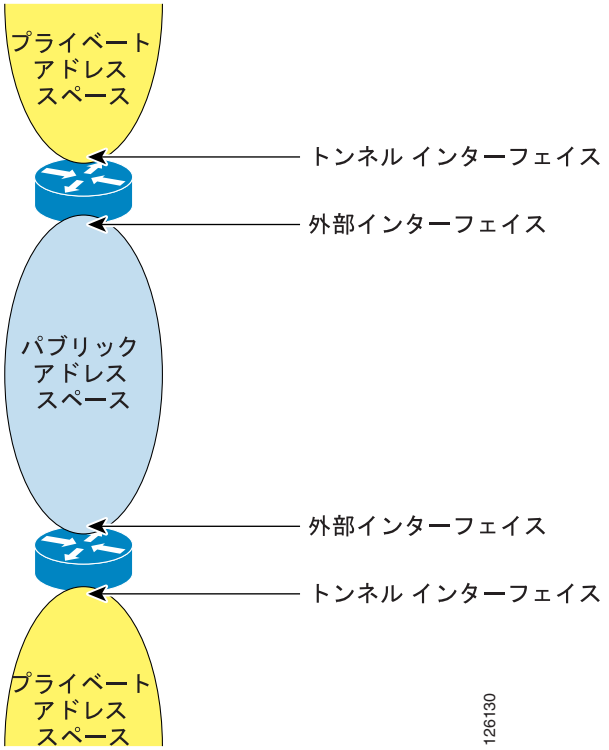
IP アドレス指定

適切なアドレス集約を使用してください。集約によって以下が可能になります。

- ルータ リソースを節約し、ルーティング テーブルのサイズを小さくする
- ルータのメモリを節約し、トラブルシューティング タスクを容易にする
- IPSec ネットワーク内のルータの構成を簡易化する

VPN は、インターネットなどの共有パブリック インフラストラクチャを介した安全な企業通信のために使用されます。次の 2 つの異なる IP アドレスのドメインを考慮してください。企業アドレス指定スペース（「プライベート アドレス」または「内部アドレス」と呼ばれることもある）とインフラストラクチャ アドレス指定スペース（「サービス プロバイダー アドレス」、「パブリック アドレス」、または「外部アドレス」とも呼ばれる）です（図 2-4 を参照）。

図 2-4　プライベートおよびパブリック アドレス スペース



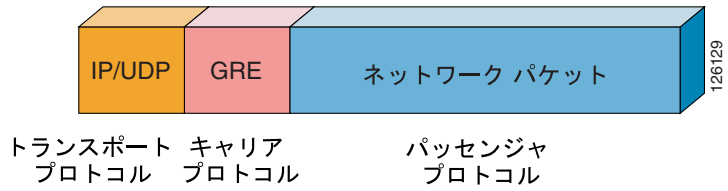
ほとんどの DMVPN デザインでは、ルータの外部インターフェイスは、サービス プロバイダーによって割り当てられるインフラストラクチャ（またはパブリック）アドレス スペース内にアドレス指定されます。トンネル インターフェイスは、企業プライベート ネットワーク アドレス スペースに属しています。ブランチ ルータのパブリック IP アドレスは、静的に定義されたかまたは動的に割り当てられた IP アドレスです。ハブアンドスポーク展開モデルの場合、p2p GRE トンネルと暗号トンネルの両方がパブリック IP アドレスを発信元としています。スポークツースポーク展開モデルの場合も、mGRE トンネルと暗号トンネルがパブリック IP アドレスを発信元とします。このアドレスは、ブランチのプライベート アドレスへのマッピングを提供するヘッドエンド ルータに登録されます。

GRE — p2p GRE および mGRE インターフェイス

IPSec は IP ネットワークでデータをトンネリングする安全な方法を提供しますが、制限事項がいくつかあります。まず、IPSec はブロードキャストまたは IP マルチキャスト（IPmc）をサポートしておらず、ルーティング プロトコルのような、これらの機能に依存するプロトコルを使用できません。

GRE は、ブロードキャストまたはマルチキャスト IP などのほかのパッセンジャ プロトコルを「運ぶ」ために使用できるプロトコルです（図 2-5 を参照）。

図 2-5　IP のキャリア プロトコルとしての GRE



IPSec と同時に GRE トンネルを使用することにより、ヘッドエンドとブランチ オフィスの間のネットワークで、ダイナミック ルーティング プロトコルまたは IPmc を実行できます。

p2p GRE over IPSec ソリューションを使用することにより、サイト間のすべてのトラフィックが暗号化プロセスの前に p2p GRE パケットにカプセル化され、crypto map 文で使用するアクセス リストが簡素化されます。crypto map 文では、GRE を許可する 1 行のみが必要です（IP プロトコル 47）。ただし、このデザインでは、ヘッドエンド ルータは各ブランチ ルータに固有のトンネル インターフェイスを必要とするため、大規模なデザインでは、ヘッドエンド ルータにきわめて大きな Cisco IOS コンフィギュレーション ファイルを設定することになります。p2p GRE over IPSec デザインの詳細については、次の URL にある『*Point-to-Point GRE over IPsec Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE_IPSec.html

DMVPN デザインでは、複数のハブアンドスポーク トンネルを作成するための「1 対多」のインターフェイスとして機能する、mGRE インターフェイスが採用されます。これは、point-to-multipoint（p2mp; ポイントツーマルチポイント）フレームリレー インターフェイスと同様に機能します。p2p GRE トンネルとは異なり、mGRE トンネルのトンネル宛先を設定する必要はありません。すべての DMVPN デザインにおいて、ヘッドエンドに mGRE インターフェイスが設定されていて、接続された各ブランチ用にトンネルを動的に作成できます。mGRE インターフェイスでは、ネットワーク内の各ブランチに対して、固有のトンネル インターフェイス、固有の crypto map、または固有の crypto ACL を必要としません。mGRE インターフェイスは各ヘッドエンド ルータのコンフィギュレーション ファイルを削減しますが、スタティック p2p GRE トポロジと比較すると、これは大規模なデザインでは利点となります。

選択する展開モデルによって、ブランチ ルータに設定する GRE インターフェイスのタイプが決定されます。ハブアンドスポーク展開モデルでは、各ブランチに p2p GRE インターフェイスを設定してください。スポークツースポーク展開モデルでは、各ブランチに mGRE インターフェイスを設定してください。

p2p GRE と mGRE では、4 バイトの GRE ヘッダー、4 バイトの mGRE トンネル キー、および 20 バイトの追加 IP ヘッダーなどによって、元のデータ パケットのサイズが増加します。

mGRE パケットのプロトコル ヘッダーは、p2p GRE パケットより 4 バイト大きいサイズです。この 4 バイトは、同じルータ内の異なる mGRE インターフェイスを区別するために使用されるトンネル キーの値を構成しています。トンネル キーがない場合、ルータは 1 つの IP ネットワークに対応する 1 つの mGRE インターフェイスしかサポートできません。トンネル キーを使用することにより、ブランチ ルータは、ネットワーク トポロジ内の各 DMVPN クラウドに対応する異な

る mGRE インターフェイスをもつことができます。ヘッドエンド ルータでも、ハイ アベイラビリティと冗長性のために、各 DMVPN クラウドを示す 2 つの mGRE インターフェイスを設定することができます。

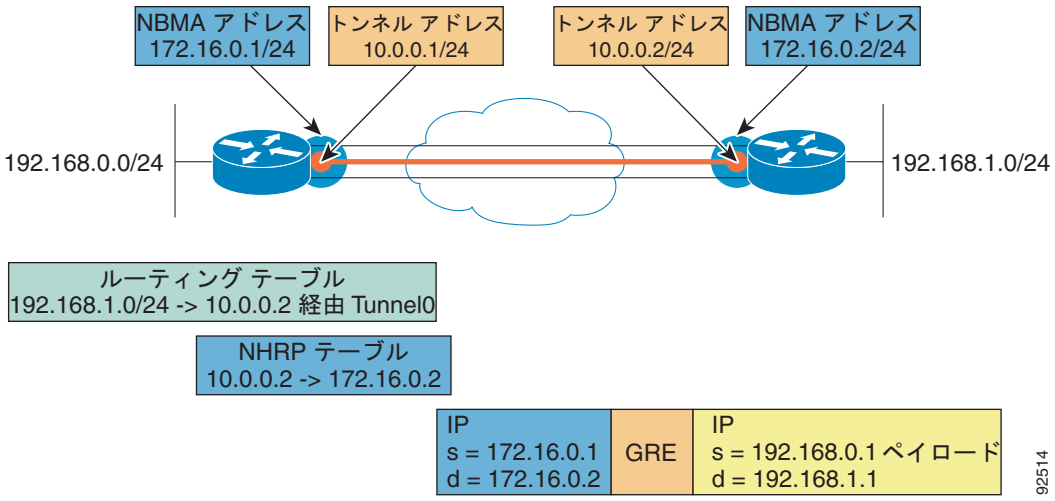
Cisco IOS ソフトウェア Release 12.3(13)T、12.3(11)T3、またはそれ以降では、トンネル キーを使用しないで、1 つのルータに複数の mGRE インターフェイスを設定できます。各 mGRE インターフェイスは、トンネル送信元として一意の IP アドレスを参照する*必要があります*。

NHRP

RFC 2332 で定義される Next Hop Resolution Protocol（NHRP）は、Address Resolution Protocol（ARP; アドレス解決プロトコル）およびフレームリレー インバース ARP と同様に、レイヤ 2 のアドレス解決プロトコルおよびキャッシュです。NHRP は、Non-Broadcast Multi-Access（NBMA; 非ブロードキャスト マルチアクセス）サブネットワークに接続されたブランチ ルータによって、「NBMA ネクストホップ」の IP アドレス（この場合、ヘッドエンド ルータまたはほかのブランチ ルータの 宛先 IP アドレス）を決定するために使用されます。

ブランチ ルータが最初に DMVPN ネットワークに確立される際、ブランチ ルータは事前設定された IP アドレスのヘッドエンド ルータに対して自身の IP アドレスを登録します。この登録によって、ヘッドエンド ルータ上の mGRE インターフェイスから、登録ブランチ ルータに対してダイナミック トンネルを作成できます。CLI（コマンドライン インターフェイス）設定でブランチ トンネルの宛先を確認する必要はありません。NHRP は トンネル IP アドレスを NBMA IP アドレスにマッピングします。NHRP によって、特定のアドレスに到達するためのパケットのトンネリング先が mGRE インターフェイスに通知されます。パケットが mGRE にカプセル化されている場合、IP 宛先アドレスは NBMA アドレスになります。図 2-6 に、NHRP および mGRE アドレス指定の例を示します。

図 2-6　NHRP および mGRE アドレス指定



宛先アドレスが NBMA サブネットワークに接続されている場合、ヘッドエンド ルータ自身が宛先になります。その他の場合、ヘッドエンド ルータは、宛先 IP アドレスを要求するブランチに最も近い出力ルータになります。

ヘッドエンド ルータとブランチ ルータに、NHRP ホールド時間（ルータがほかのルータに指示する NHRP 情報の保持期間を設定する）を設定してください。NHRP ホールド時間が期限切れになり、情報を再学習しなければならなくなるまで、この情報は NHRP キャッシュに保持されます。デフォルトの NHRP ホールド時間は 2 時間ですが、推奨される値は 10 分です。NHRP キャッシュは、スタティック エントリまたはダイナミック エントリのどちらでも読み込むことができます。ヘッドエンド ルータでは、すべてのエントリは、登録要求または解決要求によって動的に

追加されます。ブランチ ルータでは、ヘッドエンド ルータを指すスタティック NHRP マップが設定されます。NHRP 登録プロセスに参加するには、すべてのルータがネットワーク ID によって同じ NHRP ネットワークに属している必要があります。NHRP ネットワーク ID は NHRP ドメインを定義します。

ヘッドエンド ルータに登録するため、ブランチ ルータに、Next Hop Server（NHS）としてヘッドエンド ルータの NBMA アドレスを設定してください。ブランチ ルータは、トンネル IP アドレスと NBMA アドレスを含む登録情報をヘッドエンド ルータに送信します。ヘッドエンド ルータは NHRP キャッシュにエントリを作成し、登録応答を返します。ブランチ ルータはヘッドエンド ルータを有効な NHS とみなし、NHRP ドメイン内のほかのブランチとネットワークを検索するためのソースとして使用します。

トンネル プロテクション モード

一般的な IPSec 設定では、ダイナミックまたはスタティック crypto map が、ヘッドエンド ルータとブランチ ルータに設定されます。これらの crypto map は、使用する IPSec トランスフォーム セットを指定し、crypto map の対象トラフィックを定義する crypto ACL を指定します。Cisco IOS Release 12.2(13)T 以降では、ほとんどのコマンドを crypto map 設定と共有する IPSec プロファイルが採用されています。IPSec プロファイルで必要とされるのは、コマンドの一部のみです。IPSec ポリシーに関連するコマンドのみが IPSec プロファイルで使用できます。暗号化するパケットに一致する IPSec ピア アドレスまたは ACL を指定する必要はありません。

p2p GRE トンネルまたは mGRE トンネルのいずれかを同じルータ上の IPSec プロファイルに関連付けるには、トンネル プロテクションを設定してください。トンネル プロテクションでは、GRE ヘッダーがトンネル パケットに追加されたあとに IPSec 暗号化が行われるように指定されます。p2p GRE トンネルでは、トンネルの宛先 IP アドレスは IPSec ピア アドレスとして使用されます。mGRE トンネルでは、複数の IPSec ピアが可能であり、NHRP マッピングされた対応する NBMA 宛先アドレスは、IPSec ピア アドレスとして使用されます。トンネル プロテクションは、スポークツースポーク展開モデルのヘッドエンド ルータとブランチ ルータの両方に設定してください。

ルータに 複数の mGRE トンネルが設定されている場合、**shared** キーワードを設定し、各インターフェイスで同じトンネル送信元アドレスを参照する必要があります。しかし、各 mGRE トンネル インターフェイスでは、固有のトンネル キー、NHRP ネットワーク ID、および IP サブネット アドレスが必要です。このことは、デュアル DMVPN クラウド トポロジが展開されている場合、ブランチ ルータでは一般的です。

GRE トンネル キープアライブは、トンネル プロテクションと組み合わせて使用できないことに注意してください。また、トンネル プロテクションはデュアル ティア ヘッドエンド アーキテクチャでは使用できません。

VPN でのルーティング プロトコルの使用

このデザインでは、ルートをヘッドエンドからブランチ オフィスへ伝播するために、ダイナミック ルーティング プロトコルを使用してください。ルーティング プロトコルの使用には、IPSec ダイレクト カプセル化単独でのメカニズムに対していくつかの利点があります。

VPN では、ルーティング プロトコルは、以下のような従来のネットワークと同レベルの利点を提供します。

- ネットワーク トポロジ情報
- Topology Change Notification（TCN; トポロジ変更通知）（リンクに障害が発生した場合など）
- リモート ピア ステータス

DMVPN デザインでは、EIGRP、OSPF、RIPv2、および ODR（DMVPN ハブアンドスポークのみ）を含むいくつかのルーティング プロトコルを使用できます。このデザイン ガイドで示されているデザインでは、EIGRP がスケーラビリティ テストで使用されたため、EIGRP をルーティ

ング プロトコルとして使用します。EIGRP は、コンバージェンス時間が短いことに加えて、ルータ CPU サイクルとネットワーク帯域幅を節約できるため、ダイナミック ルーティング プロトコルとして推奨されます。また、EIGRP は、アドレス集約およびデフォルト ルート伝播のための一連のオプションを提供します。

OSPF などのほかのルーティング プロトコルも検証されましたが、詳細な考察は行っていません。ODR はスプリット トンネリングをサポートしないため、スポークツースポーク展開モデルで使用できません。

ルーティング プロトコルはネットワーク デバイスでの CPU 利用率を増加させるため、それらのデバイスのサイズ指定を行う場合、ルーティング プロトコルの影響を考慮する必要があります。

ルート伝播の手順

ネットワークへのブランチ接続が有効になると、ブランチ ルータは、ヘッドエンド ルータへのスタティック NHRP エントリがあるため、ルーティング プロトコル情報の送信を開始できます。ヘッドエンド ルータは NHRP キャッシュにブランチ ルータの情報が読み込まれるのを待たなければならないため、ブランチが NHS に NBMA アドレスを登録するまで、ヘッドエンド ルータはルーティング プロトコル情報の送信を開始できません。

暗号の考慮事項

IPSec は、トランスポート モードとトンネル暗号化モードをサポートします。トランスポート モードは、各パケットのデータ部分（ペイロード）のみを暗号化し、ヘッダー内の送信元および宛先アドレスはそのままの状態にします。より安全なトンネル モードは、元のパケットのヘッダーとペイロードの両方を暗号化します。この 2 つのモードの違いは、トンネル モードが元の IP データグラム ヘッダーを保護するのに対して、トランスポート モードは保護しないという点です。トンネル モードでは、パケットの合計サイズにさらに 20 バイト追加されます。DMVPN 実装では、トンネル モードとトランスポート モードはいずれも機能しますが、トランスポート モードでのいくつかの制約事項について認識しておいてください。暗号トンネルが Network Address Translation（NAT; ネットワーク アドレス変換）または Port Address Translation（PAT; ポート アドレス変換）デバイスのいずれかを通過する場合、トンネル モードが必要です。さらに、このデザイン ガイドでは、GRE トンネル エンドポイントが暗号トンネル エンドポイントと異なる場合（デュアル ティア）に DMVPN を実装するための設定例を示しますが、この場合にはトンネル モードが必要です。

IKE CAC

Cisco IOS Release 12.3(8)T より前のリリースでは、IKE により同時に受信される Internet Security Association and Key Management Protocol（ISAKMP）Security Association（SA; セキュリティ アソシエーション）要求の数とレートを制御する方法がなく、プロセッサが処理できないほど多くの ISAKMP SA が着信した場合、ルータが過負荷になる可能性がありました。これらの機能はプラットフォーム特有です。プロセッサが過負荷になると、IKE ネゴシエーションに障害が発生し、IKE パケットが絶えず再送信され、ルータのパフォーマンスがさらに低下する可能性があります。

IKE Call Admission Control（CAC; コール アドミッション コントロール）は、ルータでの送受信を許可された ISAKMP SA の IKE 認証の数を制限するために、Cisco IOS Release 12.3(8)T で導入されました。作成できるダイナミック crypto ピアの数を制限することによって、ルータに突然 ISKAMP SA 要求が殺到した場合にも、ルータが過負荷になるのを防ぐことができます。理想的な制限数は、特定のプラットフォーム、ネットワーク トポロジ、アプリケーション、およびトラフィック パターンによって異なります。指定された制限に達すると、IKE CAC はすべての新し

い ISAKMP SA 要求を拒否します。現在アクティブな IKE SA の数よりも小さい IKE CAC 制限数を指定した場合、警告が表示されますが、ISAKMP SA は終了しません。新しい ISAKMP SA 要求は、アクティブな ISAKMP SA カウントが設定された制限を下回るまで拒否されます。

CAC は、DMVPN の実装に役立つ、IKE SA を制限する 2 つの実装を提供します。まず、通常の CAC 機能は、IKE を含むすべてのプロセスがルータ CPU またはメモリ バッファを過負荷にしないようにポーリングが行われるグローバル リソース モニタです。ユーザはリソース制限（0 ～ 100 のシステム リソースのパーセンテージで表す）を設定できます。ユーザが 90% のリソース制限を指定した場合、システム リソースの 90% が消費されると、IKE CAC によって ISAKMP SA 要求が破棄されます。この機能は、ハードウェア暗号エンジンでパケットをライン レートで分類および暗号化できるヘッドエンド ルータで有益です。ハブアンドスポーク展開モデルのブランチ ルータでは、それほど有益ではありません。ブランチ ルータは、一般的に、ISAKMP SA によって過負荷になる前に容量が一杯になるからです。

2 つめのアプローチでは、ユーザは ISAKMP SA の IKE 認証制限（IKE CAC）を設定できます。この制限に達すると、IKE CAC はすべての新しい ISAKMP SA 要求を破棄します。IPSec SA のキー再生成要求は、その目的が既存のセッションの完全性を保存することであるため、常に許可されます。この機能は、主にスポークツースポーク展開モデルのブランチ ルータを対象としています。デバイスに対して作成できるダイナミック トンネルの数を制限することにより、ユーザは、ルータに突然 SA 要求が殺到した場合にも、ルータが過負荷になるのを防ぐことができます。設定する理想的な IKE CAC 制限値は、特定のプラットフォームと暗号エンジン（CE）、ネットワーク トポロジ、および導入するフィーチャ セットによって大きく異なります。

設定および実装

この章で定義する設定の問題は、デュアル DMVPN デザイン トポロジの VPN 実装に特有の問題です。読者は CLI レベルでの標準的なシスコの設定手法に適度に精通していることが想定されています。

ここで言及されるすべてのプライベートまたはパブリック IP アドレスは、IP アドレス指定（p.2-6）の内容と同じものです。

段階的な手順については、次の URL を参照してください。
http://www.cisco.com/en/US/tech/tk583/tk372/tsd_technology_support_protocol_home.html

ISAKMP ポリシーの設定

2 つの潜在的な crypto ピアの間には、少なくとも 1 つの一致する ISAKMP ポリシーがなければなりません。下記の設定例では、暗号化アルゴリズムとして 3DES、HMAC として SHA を用いる Pre-Shared Key（PSK; 事前共有キー）を使用するポリシーを示します。暗号化アルゴリズム、ハッシュ方式（HMAC）、Diffie-Hellman（D-H; ディッフィーヘルマン）グループ、認証タイプ、および ISAKMP SA ライフタイム パラメータのデフォルト値を含むデフォルト ISAKMP ポリシーがあります。これは優先度が最も低い ISAKMP ポリシーです。

PSK を使用する場合、ワイルドカード キーを使用しないでください。ただし、動的に得られた IP アドレスを使用する DMVPN デザインを実装する場合、ワイルドカード PSK を使用してください。もう 1 つの方法として、デジタル証明書とも呼ばれる PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）を使用することができます。例では、2 つの別々の crypto ピアに設定する 2 つのキーを示します。キーは注意深く選択してください。[bigsecret] は、単に例として使用しています。英数字と特殊文字をキーとして使用してください。

次の設定例では、シングルまたはデュアル ティア ヘッドエンド アーキテクチャでの crypto ピア用の、ブランチ ルータのスタティック パブリック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface FastEthernet1/0
```

```
ip address 192.168.251.1 255.255.255.0
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.161.2
```

- ブランチ ルータ：

```
interface Serial0/0
ip address 192.168.161.2 255.255.255.0
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.251.1
```

次のことに注意してください。

- シングル ティア ヘッドエンド アーキテクチャでは、上記の設定はヘッドエンド ルータに適用されます。
- デュアル ティア ヘッドエンド アーキテクチャでは、上記の設定は暗号ヘッドエンド ルータに適用されます。
- いずれのヘッドエンド アーキテクチャにおいても、ダイナミック パブリック IP アドレスを持つブランチを実装する場合、ワイルドカード PSK または PKI を暗号ヘッドエンド ルータで使用してください。

ISAKMP ポリシーの設定の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_0/security/command/reference/srike.html

IPSec トランスフォームおよびプロトコルの設定

トランスフォーム セットは、2 つの IPSec ピアの間で一致している必要があります。トランスフォーム セットの名前は、ローカルでのみ有効です。ただし、暗号化アルゴリズム、ハッシュ方式、および使用する特定のプロトコル（ESP または AH）は、少なくとも 1 つが一致している必要があります。データ圧縮も設定する場合がありますが、高速リンクをもつピアでは使用しないでください。異なるピア間では複数のトランスフォーム セットが使用でき、最も一致しているものでネゴシエートされます。

次の設定例では、シングルまたはデュアル ティア ヘッドエンド アーキテクチャでの crypto ピア用の、ブランチ ルータのスタティック パブリック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.161.2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

- ブランチ ルータ：

```
interface Serial0/0
ip address 192.168.161.2 255.255.255.0
!
```

```
crypto isakmp policy 10
 encr 3des
 authentication pre-share
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

次のことに注意してください。

- シングル ティア ヘッドエンド アーキテクチャでは、上記の設定はヘッドエンド ルータに適用されます。
- デュアル ティア ヘッドエンド アーキテクチャでは、上記の設定は暗号ヘッドエンド ルータに適用されます。
- いずれのヘッドエンド アーキテクチャにおいても、ダイナミック パブリック IP アドレスを持つブランチを実装する場合、ワイルドカード PSK または PKI を暗号ヘッドエンド ルータで使用してください。

トランスフォーム セットおよび crypto map の設定の詳細については、次の URL を参照してください。http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfipsec.html

トンネル プロテクションの設定

トンネル プロテクションは、GRE トンネルと暗号トンネルが同じエンドポイントを共有する場合に使用できます。この制約事項のために、トンネル プロテクションは、シングル ティア ヘッドエンド アーキテクチャにのみ適用できます。

以前のバージョンの IPSec 設定では、ダイナミックまたはスタティック crypto map で、IPSec トランスフォーム セット（暗号化の強度と D-H グループ）を指定し、crypto アクセス リスト（crypto map の対象トラフィックを定義）も指定します。Cisco IOS ソフトウェア Release 12.2(13)T では、IPSec プロファイルの概念が採用されています。IPSec プロファイルはコマンドのほとんどを crypto map 設定と共有しますが、コマンドの一部のみが必要になります。IPSec プロファイルから実行されるこれらのコマンドは、IPSec ポリシーに関連しています。暗号化するパケットに一致する IPSec ピア アドレスまたは ACL を指定する必要はありません。

次に、IPSec プロファイルの例を示します。

- ヘッドエンド ルータ：

```
crypto ipsec transform-set ESE esp-3des esp-sha-hmac
  mode transport
!
crypto ipsec profile VPN-DMVPN
set security-association lifetime 60
set transform-set ESE
!
```

- ブランチ ルータ：

```
crypto ipsec transform-set ESE esp-3des esp-sha-hmac
mode transport
!
crypto ipsec profile VPN-DMVPN
set security-association lifetime 60
set transform-set ESE
!
```

IPSec プロファイルは、**tunnel protection ipsec profile** *profile-name* コマンド（これも Cisco IOS ソフトウェア Release 12.2(13)T ではじめて導入）を使用して、トンネル インターフェイスに関連付けられます。**tunnel protection** コマンドは、mGRE トンネルと p2p GRE トンネルで使用できます。

p2p GRE トンネルでは、トンネルの宛先アドレスは IPSec ピア アドレスとして使用されます。mGRE トンネルでは、複数の IPSec ピアが可能であり、NHRP マッピングされた対応する NBMA 宛先アドレスは、IPSec ピア アドレスとして使用されます。対象トラフィックを定義する crypto アクセス リストを設定する必要はありません。

ルータに複数の mGRE トンネルが設定されている場合（たとえば、デュアル DMVPN クラウドでのブランチ ルータ）、各トンネル インターフェイスで同じトンネル送信元アドレスを参照できます。この場合、両方のインターフェイスの **tunnel protection** コマンドで **shared** キーワードを使用します。これは、2 つの mGRE トンネルが同じ DMVPN クラウドをホスティングしているということではありません。各トンネル インターフェイスでは、固有の NHRP ネットワーク ID および IP サブネットが必要です。

ダイナミック crypto map の設定

ダイナミック crypto map は、トンネル プロテクションが使用できないデュアル ティア アーキテクチャでのみ必要です。次の設定例では、デュアル ティア ヘッドエンド アーキテクチャを使用するブランチ ルータのダイナミック パブリック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface FastEthernet1/0
ip address 192.168.251.1 255.255.255.0
!
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
!
!
crypto map dynamic-map local-address FastEthernet1/0
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
```

- ブランチ ルータ：

```
interface Serial0/0
ip address dhcp
!
crypto isakmp key bigsecret address 192.168.251.1
!
crypto map static-map local-address Serial0/0
crypto map static-map 20 ipsec-isakmp
 set peer 192.168.251.1
 set transform-set vpn-test
 match address vpn-static2
```

次のことに注意してください。

- ヘッドエンド ルータでは、ブランチ ルータのダイナミック パブリック IP アドレスとの crypto ピアのために、ダイナミック crypto map でワイルドカード PSK が使用されます。
- デュアル ティア ヘッドエンド アーキテクチャでは、上記の設定は暗号ヘッドエンド ルータに適用されます。

さまざまな暗号コンフィギュレーション コマンドの詳細については、次の URL を参照してください。http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfipsec.html

crypto map の適用

crypto map は、デュアル ティア ヘッドエンド アーキテクチャが使用される場合にのみ必要です。crypto map は、ルータのパブリック アドレスの下に適用されます。暗号化トンネルの宛先は GRE トンネルの宛先と異なるため、デュアル ティア ヘッドエンド アーキテクチャを使用する場合、ブランチ ルータにもスタティック crypto map を設定してください。

次の設定例では、デュアル ティア ヘッドエンド アーキテクチャでの crypto ピア用の、ブランチ ルータのパブリック ダイナミック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface FastEthernet1/0
  ip address 192.168.251.1 255.255.255.0
  crypto map dynamic-map
!
```

- ブランチ ルータ：

```
interface Serial0/0
 ip address dhcp
 crypto map static-map
!
```

デュアル ティア ヘッドエンド アーキテクチャでは、上記の設定は暗号ヘッドエンド ルータに適用されます。

mGRE の設定

mGRE では、トンネルに複数の宛先を設定できます。トンネルの片側での mGRE 設定は、出力点のトンネル プロパティとは関係がありません。つまり、ハブ上の mGRE トンネルは、ブランチ上の p2p トンネルに接続できます。逆に、p2p GRE トンネルも mGRE トンネルに接続できます。mGRE インターフェイスと p2p GRE インターフェイスを区別する特徴は、トンネル宛先です。mGRE インターフェイスには、設定された宛先がありません。その代わりに、GRE トンネルには、**tunnel mode gre multipoint** コマンドが設定されます。このコマンドは、p2p GRE トンネルでみられる **tunnel destination** x.x.x.x の代わりに使用されます。複数の宛先が使用できることに加えて、mGRE トンネルでは、NHRP によってトンネル エンドポイントを解決します。

mGRE の設定は次のとおりです。

```
!
interface Tunnel0
 bandwidth 1536
 ip address 10.62.1.10 255.255.255.0
 tunnel source Serial0/0
 tunnel mode gre multipoint
!
```

トンネル インターフェイスの設定 — ハブアンドスポークのみ

ここでは、ブランチ スタティック パブリック IP アドレスを使用したトンネル インターフェイスの設定について説明します。

次の設定例では、シングルまたはデュアル ティア ヘッドエンド アーキテクチャでのブランチ ルータのスタティック パブリック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface Tunnel0
```

```
 bandwidth 1536
 ip address 10.62.1.1 255.255.255.0
 tunnel source 192.168.251.1
 tunnel mode gre multipoint
!
```

- ブランチ ルータ：

```
interface Tunnel0
 bandwidth 1536
 ip address 10.62.1.194 255.255.255.0
 tunnel source 192.168.161.2
 tunnel destination 192.168.251.1
!
```

この設定はシングル ティア ヘッドエンド アーキテクチャにのみ適用されることに注意してください。

トンネル インターフェイスの設定 — ダイナミック スポークツースポーク

ここでは、ブランチ ダイナミック パブリック IP アドレスを使用したトンネル インターフェイスの設定について説明します。

次の設定例では、シングル ティア ヘッドエンド アーキテクチャでの mGRE トンネル用の、ブランチ ルータの ダイナミック パブリック IP アドレスとヘッドエンド ルータのスタティック パブリック IP アドレスを示します。

- ヘッドエンド ルータ：

```
interface FastEthernet1/0
 ip address 192.168.251.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1536
 ip address 10.62.1.1 255.255.255.0
 tunnel source 192.168.251.1
 tunnel mode gre multipoint
!
```

- ブランチ ルータ：

```
interface Serial0/0
 ip address dhcp
!
interface Tunnel0
 bandwidth 1536
 ip address 10.62.1.10 255.255.255.0
 tunnel source Serial0/0
 tunnel mode gre multipoint
!
```

次のことに注意してください。

- シングル ティア ヘッドエンド アーキテクチャでは、上記の設定はヘッドエンド ルータに適用されます。
- デュアル ティア ヘッドエンド アーキテクチャでは、上記の設定は mGRE ヘッドエンド ルータに適用されます。mGRE ヘッドエンド ルータには、暗号ヘッドエンド ルータとは異なるスタティック パブリック IP アドレスが設定されます。mGRE ヘッドエンド ルータは、暗号ヘッドエンド経由で、すべての発信 mGRE トラフィックをブランチに送信します。

NHRP の設定

NHRP は、トンネル エンドポイントの内部アドレスと外部アドレス間をマッピングします。これらのマッピングはスタティックまたはダイナミックに設定できます。ダイナミックの場合、NHS を使用してトンネル エンドポイントのリストを維持します。NHS を使用するエンドポイントは、NHS に対して自身のパブリックおよびプライベート マッピングを登録します。NHS のローカル マッピングは、常にスタティックにしてください。ブランチは NHS サーバの内部アドレスまたは保護アドレスを指し示していることが重要です。

NHRP のホールド時間は、デバイスのキャッシュ エントリが有効であると隣接ルータがみなす期間を決定するために使用されます。スポークツースポーク セッションが開始されると、設定値がリモート スポークに渡されます。リモート スポークはカウントダウン タイマーを開始します。このタイマーが期限切れになると、リモート ルータは、ローカル ルータへのキャッシュ エントリを削除します。トラフィックがまだ流れている場合、リモート ルータは、再び NHS サーバからのマッピングを要求する必要があります。スポーク ルータごとに異なるホールド時間を設定できますが、あまり一般的ではありません。2 つのスポークがセッション中で、1 つのタイマーがもう 1 つのタイマーより早く期限切れになった場合、スポークは、NHRP キャッシュ エントリを期限切れにするよう隣接スポークに知らせます。また、各デバイスはスポークツースポーク暗号化セッションを削除します。

スポークツースポーク Voice（VoIP）over DMVPN は、QoS の問題があるために一般的には推奨されませんが、NHRP のホールド時間は、ほとんどのコールの持続時間より長く設定してください。ただし、ホールド タイマーは、スポークツースポーク セッションが平均してアイドル状態になるほど長くしないでください。この推奨事項は、特にソフトウェアの影響で暗号トンネルの数が制限されるローエンド ルータに当てはまります。アイドル時間を 600 秒に設定することで、アイドル トンネルと過度の再キャッシングの全体的なバランスをとることができます。設定は、次のとおりです。

- ヘッドエンド ルータ：

```
!
interface Tunnel0
description NHRP with mGRE
ip address 10.0.0.11 255.255.255.0
ip mtu 1400
ip nhrp map 10.62.1.1 192.168.251.1
ip nhrp network-id 12345
ip nhrp holdtime 600
ip nhrp nhs 10.62.1.1
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile DMVPN shared
!
```

- ブランチ ルータ：

```
!
interface Tunnel0
description NHRP with p2p GRE
ip address 10.0.0.11 255.255.255.0
ip mtu 1400
ip nhrp map 10.62.1.1 192.168.251.1
ip nhrp network-id 12345
ip nhrp holdtime 600
ip nhrp nhs 10.62.1.1
tunnel source FastEthernet0/0
tunnel destination 172.16.0.1
tunnel key 100000
tunnel protection ipsec profile DMVPN shared
!
```

ルーティング プロトコルの設定

DMVPN クラウドは NBMA ネットワークであるため、ダイナミック ルーティング プロトコルを実行する際には、いくつかの考慮事項があります。これは特にスポークツースポーク デザインを実装する場合に当てはまります。多くのルーティング プロトコルには、ほかの参加ノードを検出するために使用する IP マルチキャスト メカニズムがあります。ハブのパブリック アドレスを指すスタティック multicast map がブランチ ルータに設定されます。ハブ ルータにはダイナミック multicast map が設定されます。これによって、ハブとスポークはブロードキャスト情報を交換できますが、スポークはほかのスポークからのブロードキャスト情報を得ることはできません。

EIGRP の設定

EIGRP は、DMVPN ネットワークを実行する際の優先ルーティング プロトコルです。構成は純粋なハブアンドスポーク構成で簡単です。アドレス スペースはできるだけ集約する必要があり、デュアル クラウド トポロジでは、スポークは EIGRP stub ネットワークに展開する必要があります。すべての EIGRP ネットワークと同様に、ハブ ルータが重大な障害後に通信を再確立できるように、ネイバーの数を制限してください。DMVPN サブネットが /24 ネットワーク プレフィクスによって設定されている場合、ネイバー数は 254（安全な動作制限）に制限されます。この値を超えると、再コンバージェンスと復旧のバランスを取るために妥協すべき点が生まれます。きわめて大きな EIGRP ネットワークでは、ハブがスラッシングなしで復旧するために多くの時間を与えられるよう、EIGRP のホールド時間を調整しなければならない場合があります。ただし、ネットワークのコンバージェンス時間は遅れます。ラボでは、400 のネイバーを確立するためにこの方式を使用しました。最大ホールド時間は、EIGRP hello タイマーの 7 倍（35 秒）を超えてはなりません。タイマーを調整する必要があるネットワーク デザインでは、多くの場合、将来的な拡張に対応することはほとんどできません。

スポークは、同じ論理サブネット上にある場合でも、直接相互に情報を交換できないため、スポークツースポーク DMVPN ネットワークには独自の課題が存在します。そのため、ヘッドエンド ルータは、同じサブネット上のほかのスポークからのサブネットをアドバタイズする必要があります。これは通常ではスプリット ホライズンによって妨げられます。さらに、アドバタイズされたルートには、ハブ ルータにより学習された元のネクストホップが含まれている必要があります。この動作を可能にするために、新しいコマンド（**no ip next-hop-self**）が追加されました。次の設定例では、一般的な EIGRP 設定の詳細を示します。トンネルの外部アドレス スペースは、トンネル内部で稼働しているプロトコルに含めることはできません。

- ヘッドエンド ルータ：

```
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip nhrp authentication test
    ip nhrp map multicast dynamic
    ip nhrp network-id 105600
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
```

- ブランチ ルータ：

```
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.3 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip nhrp authentication test
 ip nhrp map 10.56.0.1 192.168.201.1
    ip nhrp map multicast 192.168.201.1
 ip nhrp network-id 105600
 ip nhrp nhs 10.173.20.1
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source FastEthernet0/0/0
 tunnel mode gre multipoint
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
!
```

OSPF の設定

DMVPN ネットワーク上での OSPF の設定には、ほかのタイプのネットワーク上で OSPF を使用する場合と同じ制約事項がいくつかあります。従来、1 つの OSPF エリアには 50 を超えるルータを含めることはできず、ルータ上に 3 つを超えるエリアを設定することはできません。最新のルータはより強力なプロセッサを搭載していますが、暗号化と NHRP という追加のオーバーヘッドによって、その利点の効果はほとんど失われます。このため、エリアあたり 50 のルータという制限に従ってください。さらに、ハブだけがすべてのブランチと直接通信しているため、ハブを DMVPN サブネット上の Designated Router（DR; 代表ルータ）として設定してください。一般的に、Backup Designated Router（BDR; バックアップ代表ルータ）はありません。同じサブネット上に 2 つめのハブが展開されている場合には、BDR を指定できます。これは、Cisco IOS 12.4 より前の DMVPN ネットワークでより一般的だったシングル クラウドのデュアル ハブ トポロジでよくみられます。

ハブ ルータ上の mGRE トンネルは、DR を選択できるように、OSPF ブロードキャスト ネットワークとして設定してください。各スポーク ルータは、DR にならないように、OSPF プライオリティを 0 に設定します。さらに、スポークに p2p GRE が設定され、ハブが mGRE である場合、スポークの hello タイマーをデフォルトの 10 秒から 30 秒に変更し、mGRE インターフェイスの hello タイマーに一致させてください。トンネル IP MTU は、OSPF で隣接するのすべての GRE インターフェイスと一致している必要があります。さらに、DMVPN で稼働している OPSF エリアは、WAN での Link-State Advertisement（LSA; リンクステート アドバタイズメント）のフラッディングを軽減するために、stubby エリアまたは totally stubby エリアにしてください。設定は次のとおりです。

- ヘッドエンド ルータ：

```
!
interface Tunnel0
 description dmvpn tunn
 ip address 10.173.20.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication secret
    ip nhrp map multicast dynamic
 ip nhrp network-id 10203
```

```
 ip ospf network broadcast
 ip ospf hello-interval 30
 ip ospf priority 200
 tunnel source GigabitEthernet0/1.201
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile dmvpn
!
router ospf 10
 network 10.173.20.0 0.0.0.255 area 10
 area 10 stub no-summary
!
```

- ブランチ ルータ：

```
!
interface Tunnel0
 ip address 10.173.20.21 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication secret
 ip nhrp map multicast 192.168.201.1
 ip nhrp map 10.173.20.1 192.168.201.1
 ip nhrp network-id 10203
 ip nhrp nhs 10.173.20.1
 ip route-cache flow
 ip ospf network broadcast
 ip ospf hello-interval 30
 ip ospf priority 0
 load-interval 30
 qos pre-classify
 no clns route-cache
 tunnel source GigabitEthernet0/0.201
 tunnel mode gre multipoint
 tunnel key 123
 tunnel path-mtu-discovery
 tunnel protection ipsec profile dmvpn
!
router ospf 10
 network 10.173.20.0 0.0.0.255 area 10
 area 10 stub no-summary
!
```

ハブアンドスポークのみのネットワークでは、ヘッドエンド ルータでポイント マルチポイント ネットワーク タイプを使用し、ブランチ ルータでポイント ポイント ネットワーク タイプを使用することによって、OSPF の負荷を軽減できます。この場合、DMVPN サブネットで DR ルータを選出する必要はありません。ヘッドエンド ルータは、サブネットのマスターとして機能します。ブランチはヘッドエンドをサブネットの唯一のパスとみなすので、OPSF エリアのダイクストラ アルゴリズムが簡素化されます。

RIPv2 の設定

DMVPN 上で RIPv2 を使用できます。構成例は示していません。ルーティング プロトコルとして RIPv2 を使用する場合、スポークツースポーク トラフィックを許可するには（ハブ経由の場合も）、ハブの mGRE トンネル インターフェイスで **no ip split-horizon** コマンドを設定してください。RIPv2 の場合デフォルトでは、ルートを学習したインターフェイスからそのルートのアドバタイズを行う際に、インターフェイス自身ではなく元の IP ネクストホップを使用します。したがって、next-hop-self を設定する必要はありません。スポークツースポーク トンネルが使用されている場合、自動集約をディセーブルにしてください。設定は次のとおりです。

- ヘッドエンド ルータ：

```
!
interface Tunnel0
description dmvpn tunn
ip address 10.173.20.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication secret
ip nhrp network-id 10203
ip ospf network point-to-multipoint
ip ospf hello-interval 30
tunnel source GigabitEthernet0/1.201
tunnel mode gre multipoint
tunnel key 123
tunnel protection ipsec profile dmvpn
!
router ospf 10
network 10.173.20.0 0.0.0.255 area 10
area 10 stub no-summary
!
```

- ブランチ ルータ：

```
!
interface Tunnel0
ip address 10.173.20.21 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication secret
ip nhrp map multicast dynamic
ip nhrp map 10.173.20.1 192.168.201.1
ip nhrp network-id 10203
ip nhrp nhs 10.173.20.1
ip route-cache flow
ip ospf network point-to-point
ip ospf hello-interval 30
load-interval 30
qos pre-classify
no clns route-cache
tunnel source GigabitEthernet0/0.201
tunnel mode gre multipoint
tunnel key 123
tunnel path-mtu-discovery
tunnel protection ipsec profile dmvpn
!
router ospf 10
network 10.173.20.0 0.0.0.255 area 10
area 10 stub no-summar
```

ハイ アベイラビリティ

ハイ アベイラビリティ（HA）によって、ネットワークの耐障害性と障害の際のアベイラビリティが提供されます。ここでは、アベイラビリティの高い DMVPN 実装のためのデザインについて説明します。ハイ アベイラビリティの詳細については、次の URL にある『*IPsec VPN Redundancy and Load Sharing Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/VPNLoad/VPN_Load.html

すべての HA ヘッドエンド デザインに共通の要素

VPN デザインにおいて一定の耐障害性を提供するために、各ブランチ ルータに少なくとも 2 つのトンネルを設定してください。DMVPN トポロジまたは展開モデルに関係なく、各ブランチ ルータには、プライマリ ヘッドエンドへのトンネルとセカンダリ ヘッドエンド ルータへの代替トンネルが必要です。

通常の動作条件では、プライマリ トンネルとセカンダリ トンネルの両方で、ルーティング プロトコル ネイバーが確立されています。ルーティング プロトコルは両方のパスを維持し、セカンダリ トンネルは優先度の低いパスとして設定されます。

すべての HA ヘッドエンドの耐障害デザインにおける共通の懸念事項は、ルーティング プロトコル ネイバーの数です。多くの冗長性のあるネイバー関係は、ルーティング コンバージェンスに必要な時間を増大させます。

ルーティング プロトコルでのコンバージェンスは、すべての HA ヘッドエンド デザインで共通の要素です。ただし、各展開モデルに応じた、ルーティング プロトコルでのコンバージェンスによる HA の実現方法があります。

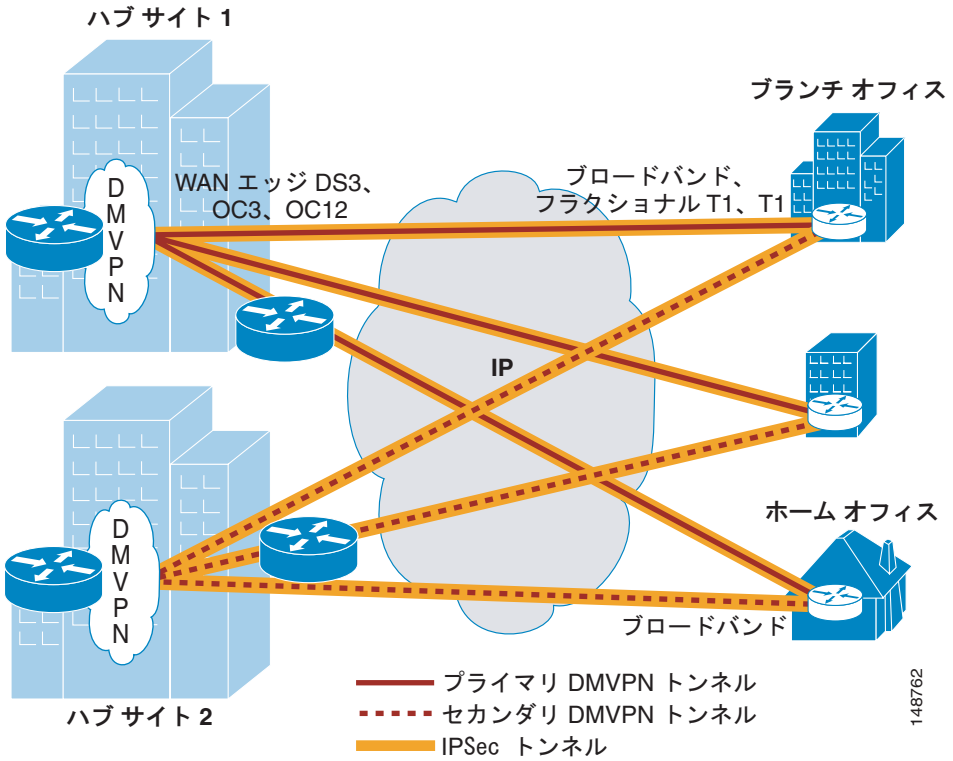
デュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル

ここでは、デュアル DMVPN クラウド トポロジの 2 つのヘッドエンド システム アーキテクチャについて説明します。説明されているヘッドエンド アーキテクチャごとに異なる HA 対策が採用されています。次のセクションでは、異なるヘッドエンド アーキテクチャをもつハブアンドスポーク展開モデルの HA について説明します。

ハブアンドスポーク展開モデル — シングル ティア ヘッドエンド アーキテクチャ

図 2-7 に、シングル ティア ヘッドエンド アーキテクチャのハブアンドスポーク展開モデルによる一般的な HA 対応を示します。

図 2-7　ハブアンドスポーク展開モデル — シングル ティア ヘッドエンド アーキテクチャ



ヘッドエンド デバイスの 1 つで障害が発生した場合、ルーティング プロトコルによって、プライマリ トンネルを通るルートがもはや有効ではないことが検出され、コンバージェンス後、セカンダリ トンネルを通るルートが使用されます。プライマリ トンネルが再び使用できるようになると、トラフィックのルートはプライマリ トンネル（ルーティング メトリックでは優先ルートであるため）に戻されます。ここで示すヘッドエンドの耐障害デザインでは、1 つのヘッドエンド ルータの障害に対応でき、IP サブネットや DMVPN クラウドに関係なく、障害のないヘッドエンド ルータに適切にフェールオーバーされます。

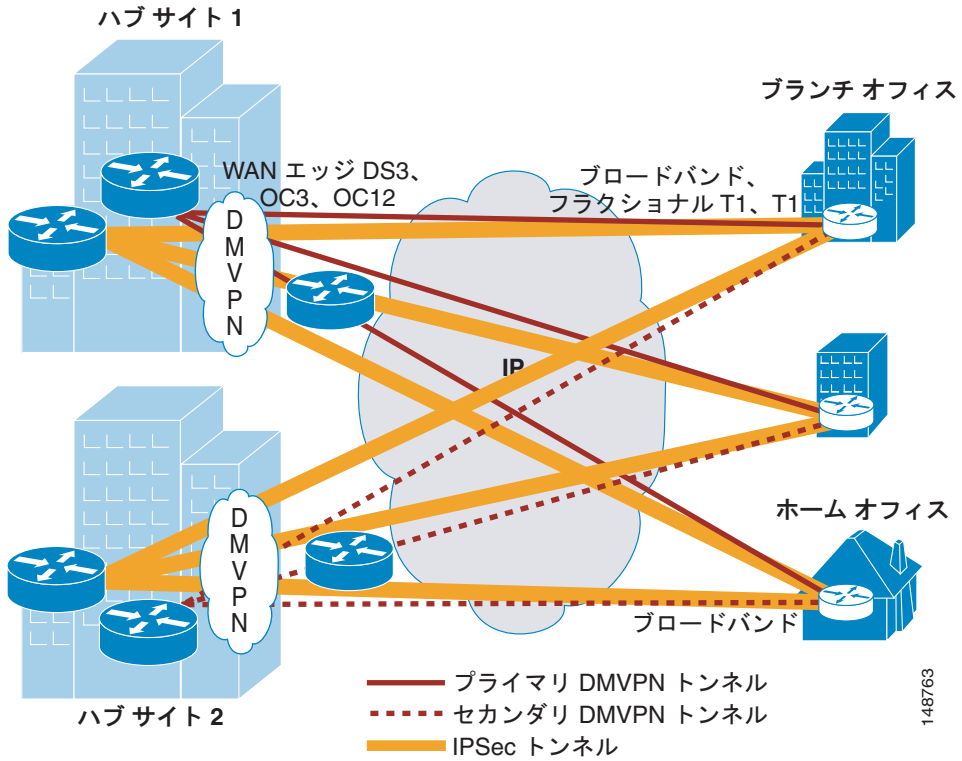
ハブ ルータには複数の mGRE インターフェイスを設定できます。**tunnel protection** コマンドで **shared** キーワードを指定した場合、同じトンネル送信元で 2 つの mGRE トンネルを設定できます。ただし、この 2 つの mGRE トンネルは、各トンネル インターフェイス固有のトンネル キー、NHRP ネットワーク ID、および IP サブネットを使用して、2 つの別個の DMVPN ネットワークを作成します。

一般的なブランチ ルータには、2 つ以上の VPN ヘッドエンドに対する 2 つ以上のトンネル インターフェイスがあります。ブランチ ルータからヘッドエンド ルータへのすべてのトンネルが稼働しています。ルーティング プロトコルは、どのトンネルがユーザ トラフィックを通過させるかを決定します。このデザインにおけるさまざまなパスは、トンネル間での優先順位を指定するために、少しずつ異なるメトリックが設定されます。ルーティング メトリックは、非対称ルーティングを防ぐために、アップストリームとダウンストリームで同一にしてください。

ハブアンドスポーク展開モデル — デュアル ティア ヘッドエンド アーキテクチャ

図 2-8 に、デュアル ティア ヘッドエンド アーキテクチャのハブアンドスポーク展開モデルによる一般的な HA 対応を示します。

図 2-8　ハブアンドスポーク展開モデル — デュアル ティア ヘッドエンド アーキテクチャ



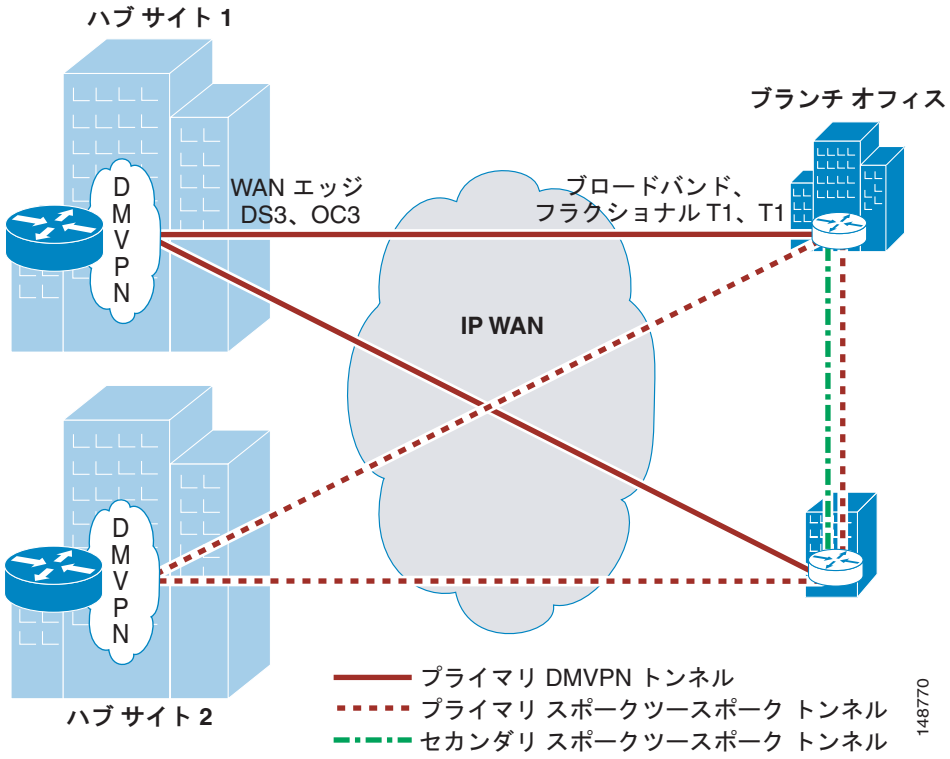
デュアル ティア ヘッドエンド アーキテクチャが実装されている場合、暗号化機能は GRE およびルーティング プロトコル機能から分離されています。これによって、ヘッドエンドの両方のペア間が接続されている場合に障害が発生したとき、追加パスが提供されます。逆に、このアーキテクチャには、故障する可能性があるデバイスも追加されています。デュアル ティア アーキテクチャでは、トンネル プロファイルを実装できません。ブランチでの暗号設定では、使用できる両方の暗号ヘッドエンドに手動でマッピングを行ってください。いずれかの暗号ヘッドエンドが使用できるようにするフェールオーバー設定の詳細については、次の URL にある『*IPsec Direct Encapsulation Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html

GRE トンネルの障害は、シングル ティア ヘッドエンド アーキテクチャと同じ方法で処理されます。この場合、ダイナミック ルーティング プロトコルによってバックアップ DMVPN サブネットが選択されます。

デュアル DMVPN クラウド トポロジ — スポークツースポーク展開モデル

図 2-9 に、スポークツースポーク展開モデルによる一般的な HA 対応を示します。

図 2-9　スポークツースポーク展開モデル



ハブアンドスポーク展開モデルに類似したプライマリおよびセカンダリ パスを判定するルーティング プロトコルに加えて、スポークツースポーク展開モデルには、ほかの HA の考慮事項が含まれています。

スポークツースポーク トンネルをブランチ ルータ間で動的に作成するには、各ブランチが 1 つの DMNPN クラウドを経由し、プライマリ ルートともう 1 つのブランチの適切な NHRP アドレスの両方を取得する必要があります。つまり、図 2-9 のブランチ 1 とブランチ 2 の間にあるスポークツースポーク トンネルを 1 つの DMVPN クラウドに接続する必要があります。DMVPN クラウド 1 を通るブランチ 1 からブランチ 2 へのスポークツースポーク トンネルを作成するために、ブランチ 1 とブランチ 2 には、各ブランチの IP アドレスを動的に取得するためのヘッドエンド 1 へのスタティック NHRP マップと、ブランチ同士が通信できるようにする各ブランチのルーティング テーブル内のルートがあります。

ヘッドエンド 1 が故障した場合、ハブアンドスポーク展開モデルの場合と同様に、ルーティング プロトコルでのコンバージェンスが発生します。ブランチ 1 は、ヘッドエンド 2 を通ってブランチ 2 に到達するようにルーティングされます。ヘッドエンド 2 は別の DMVPN クラウドにありますが、これは、ブランチ 1 とブランチ 2 の間に、今度は DMVPN クラウド 2 を通る新しいスポークツースポーク トンネルを作成することを意味します。DMVPN クラウド 1 を通る元のスポークツースポーク トンネルは、NHRP ホールド時間と IPSec SA タイマーがアクティブな間は存続します。NHRP ホールド時間と IPSec SA タイマーが期限切れになると、元のスポークツースポーク トンネルは終了します。ヘッドエンド 1 が回復すると、コンバージェンスによってルートが戻ります。トラフィックは元の DMVPN サブネットに展開され、バックアップ DMVPN サブネット上のスポークツースポーク セッションで使用された IPSec SA は、タイマーが期限切れになったあとに解除されます。

QoS

遅延の影響を受けやすいトラフィック アプリケーションをサポートするには、QoS を設定しなければならない場合があります。QoS と IPSec は、Cisco Voice and Video Enabled IPSec VPN（V3PN）テクノロジーの一部として統合されています。詳細については、次の URL にある『*Voice and Video Enabled IPsec VPN (V3PN) Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND.html

サービス プロバイダーが、各ブランチ ルータへのアクセス リストとヘッドエンド キャンパスの場所へのリンクの両方で、QoS 設定を実装することが理想的です。暗号化された音声とデータを転送するためにこの QoS 機能を提供する Cisco Powered Network サービス プロバイダーがあります。これらのサービス プロバイダーは、次の URL にある Cisco Powered Network ― Find Recommended Service Providers ユーティリティを使用して検索できます。
http://www.cisco.com/pcgi-bin/cpn/cpn_pub_bassrch.pl
ダイアログボックスを [IP VPN-Multiservice] 検索条件にしてください。

ただし、キャンパス ヘッドエンドとブランチ ルータ間へ QoS をプロビジョニングする必要がある場合もあります。次のセクションでは、その方法について説明します。

ハブアンドスポーク展開モデルでの QoS

ハブアンドスポーク展開モデルでは、ブランチ ルータは、外部物理インターフェイスで QoS サービス ポリシーを実装し、インターフェイス クロック レートが実際のアップリンク レートである物理インターフェイスから輻輳フィードバックを取得できます。このインターフェイスの例として、シリアル T1 または E1 インターフェイス、またはフレームリレーがあります。サービス プロバイダーの Customer Premises Equipment（CPE; 宅内装置）ルートからブロードバンドまたはイーサネット ハンドオフで接続されるブランチ ルータは、外部物理インターフェイスに Hierarchical Class-Based Weighted Fair Queueing（HCBWFQ; 階層化クラスベース WFQ）を実装し、契約上のアップリンク レートから得られたシェーピング レート内でキューイングする必要があります。

ヘッドエンドから見ると、すべてのスポーク ルータは、多くの場合、高速インターフェイスからアクセスされます。たとえば、ハブ ルータはギガビット イーサネット または OC3 リンクなど、スポーク ルータのアクセス リンクを過負荷にする可能性があるインターフェイスを使います。フレームリレー ネットワークでは、ハブ ルータで Frame Relay Traffic Shaping（FRTS; フレームリレー トラフィック シェーピング）を実装することでこの問題に対応できます。

DMVPN ネットワークでは、ダイナミック マルチポイント VPN ハブで QoS クラス機能をサポートすることで対応できます。この機能は Cisco 7200 シリーズ ルータおよび 7301 ルータの Cisco IOS ソフトウェア Release 12.4(9)T 以降で使用可能であり、トンネル単位（SA 単位またはブランチ単位）の QoS サービス ポリシーを実装できます。

次に、この設定を実装する方法の例を示します。この例では、次に示すように、10.0.92.0/24 および 10.0.94.0/24 の内部 LAN ネットワーク アドレスをもつ 2 つのスポーク ルータがあることを想定しています。

- スポーク ルータ 1

```
!
hostname vpn-jk2-831-1
!
interface Ethernet0
 description Inside LAN Interface
 ip address 10.0.92.1 255.255.255.0
!
end
```

- スポーク ルータ 2

```
!
```

```
hostname vpn-jk2-831-2
!
interface Ethernet0
 description Inside LAN Interface
 ip address 10.0.94.1 255.255.255.0
!
end
```

これらのブランチをサポートするヘッドエンドの設定では、キャンパスの任意のネットワークから各ブランチのリモート内部 LAN ネットワークに宛てられたパケットにマッチする IP アクセス リストが各ブランチに対して設定されています。

```
!
hostname HEAD_END
!
ip access-list extended B000
 permit ip any 10.0.92.0 0.0.0.255
ip access-list extended B001
 permit ip any 10.0.94.0 0.0.0.255
```

また、適切な IP 拡張アクセス リストを参照するよう、class map が各ブランチに設定されます。

```
class-map match-all B001-class
 match access-group name B001
class-map match-all B000-class
 match access-group name B000
!
```

class map は、各ブランチに対して優先するトラフィックを識別するために定義されます。

```
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
!
```

これらの class map は、policy map 設定によって参照されます。各ブランチへのダウンリンクはサービス プロバイダーからブランチ ルータへのフレームリレーまたは HDLC カプセル化 T1 リンクであると想定し、VOICE クラスは 9 つの G.729 音声コールのために設定されます。これは HCBWFQ 設定での child サービス ポリシーです。

```
policy-map branch-policy
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 504
 class class-default
  fair-queue
  random-detect
!
```

HCBWFQ 設定での parent サービス ポリシーが定義されます。各ブランチは T1（1.54 Mbps）データ レートでサービス プロバイダーに接続されていることを想定しています。シェーパーは、サービス プロバイダー ネットワーク内のキューイングとバッファリングによって生じるすべてのパケットの到着レートにおけるある程度のジッタを許容するために、あるレートのパーセント（この場合、85%）に設定されます。例の 85% は控えめな値であり、帯域幅の浪費を避けるために値を増加させることができます。ただし、目的は、リンクが処理できないほど多くのパケットを決して発生させないことです。サービス プロバイダーがパケットを無差別に廃棄できるような

シェーパー値を設定しないでください。サービス プロバイダーがアクセス リンクに QoS を適用していないことを想定しています。サービス プロバイダーがシスコ製ルータを使用していて、T1 リンクに fair-queue のデフォルト設定が適用されている場合、WFQ はデフォルトで precedence-aware、従って本質的に QoS-aware のため、シェーピング レートに 90 ～ 95% を超える値を設定できます。

```
policy-map Shaper-1544K-all
 description 1544K * .85 = 131K
 class B000-class
  shape average 1310000 13100
  service-policy branch-policy
 class B001-class
  shape average 1310000 13100
  service-policy branch-policy
!
! ... <その他のブランチについても同様>
!
```

ヘッドエンド ハブ ルータでは、サービス ポリシーが元の暗号化されていない IP ヘッダー内の宛先 IP アドレスを照合するため、mGRE トンネル インターフェイスで *qos pre-classify* が設定されます。ただし、サービス ポリシーは外部インターフェイスに適用され、QoS の照合が呼び出される際にはパケットは暗号化されています。*qos pre-classify* を設定することにより、サービス ポリシーは、クリア テキストの値を照合できます。

```
!
interface Tunnel0
...
 qos pre-classify
!
interface FastEthernet0/1.100
 description Outside interface
...
 service-policy output Shaper-1544K-all
```

この設定のパフォーマンス特性については、第 4 章「スケーラビリティ テストの結果（ユニキャストのみ）」で説明します。

次に、ルータのパフォーマンス スケール テスト中に表示された **show policy-map** の出力例を示します。

```
show policy-map interface
 GigabitEthernet0/1

  Service-policy output: Shaper-1544K-all

    Class-map: b000-class (match-all)
      158299 packets, 48139994 bytes
      30 second offered rate 1299000 bps, drop rate 0 bps
      Match: access-group name b000
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          1310000/1310000   3275   13100     13100     10        1637

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      12        158304    48140792  147759    45034738  yes

      Service-policy : branch-policy

        Class-map: CALL-SETUP (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af31 (26)
```

```
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: ip dscp cs3 (24)
      0 packets, 0 bytes
      30 second rate 0 bps
    Queueing
      Output Queue: Conversation 73
      Bandwidth 2 (%)
      Bandwidth 26 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0

  Class-map: INTERNETWORK-CONTROL (match-any)
    5 packets, 870 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp cs6 (48)
      5 packets, 870 bytes
      30 second rate 0 bps
    Match: access-group name IKE
      0 packets, 0 bytes
      30 second rate 0 bps
    Queueing
      Output Queue: Conversation 74
      Bandwidth 5 (%)
      Bandwidth 65 (kbps) Max Threshold 64 (packets)
      (pkts matched/bytes matched) 5/870
  (depth/total drops/no-buffer drops) 0/0/0
    QoS Set
      dscp cs6
        Packets marked 5

  Class-map: VOICE (match-all)
    118416 packets, 18709728 bytes
    30 second offered rate 502000 bps, drop rate 0 bps
    Match: ip dscp ef (46)
    Queueing
      Strict Priority
      Output Queue: Conversation 72
      Bandwidth 50 (%)
      Bandwidth 655 (kbps) Burst 16375 (Bytes)
      (pkts matched/bytes matched) 110494/17458052
      (total drops/bytes drops) 0/0

  Class-map: class-default (match-any)
    39878 packets, 29429396 bytes
    30 second offered rate 795000 bps, drop rate 0 bps
    Match: any
    Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 64
  (total queued/total drops/no-buffer drops) 6/0/0
       exponential weight: 9

class    Transmitted      Random drop      Tail drop    Minimum Maximum  Mark
         pkts/bytes       pkts/bytes       pkts/bytes    thresh  thresh  prob
    0   39344/29075840        0/0              0/0           20      40  1/10
    1       0/0               0/0              0/0           22      40  1/10
    2     536/353824          0/0              0/0           24      40  1/10
    3       0/0               0/0              0/0           26      40  1/10
    4       0/0               0/0              0/0           28      40  1/10
    5       0/0               0/0              0/0           30      40  1/10
    6       0/0               0/0              0/0           32      40  1/10
    7       0/0               0/0              0/0           34      40  1/10
 rsvp       0/0               0/0              0/0           36      40  1/10
```

```
Class-map: b001-class (match-all)
  158223 packets, 48128074 bytes
  30 second offered rate 1301000 bps, drop rate 0 bps
  Match: access-group name b001
  Traffic Shaping
       Target/Average   Byte   Sustain   Excess    Interval  Increment
         Rate           Limit  bits/int  bits/int  (ms)      (bytes)
      1310000/1310000   3275   13100     13100     10        1637

    Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
    Active Depth                         Delayed   Delayed   Active
    -      8         158231    48130666  148135    45116434  yes
```

＜各ブランチに対してシェーパーと class map のインスタンスが 1 つあるが、テキスト出力は省略＞

次のことに注意してください。

- 1299000 bps のレートは 1310000 のシェーパー比率に近く、このブランチへのダウンリンクは十分に利用されています。
- シェーパーは b000 クラス で稼働しており、現在 12 個のパケット（キューの長さ）がキューイングされています。
- VOICE クラスに一致するパケットがあります。テスト トラフィック プロファイルには CS3/AF31 とマークされたパケットが含まれていないため、CALL-SETUP には一致がありません。
- INTERNETWORK-CONTROL には一致があり、これらのパケットは EIGRP hello パケットです。
- デフォルト クラスでは、IP precedence 0 および 2 の両方に一致があります。トラフィック プロファイルには、DSCP BE（ベストエフォート）と DSCP AF21（IP precedence 2）の両方があります。WRED は有効で、これらのマーキングは適切なカウンタに表示されます。

スポークツースポーク展開モデルでの QoS

スポークツースポーク展開モデルでは、ブランチ ルータは QoS クラス機能をサポートするダイナミック マルチポイント VPN ハブと構成することができます。Cisco 800、1700、1800、2600XM、2800、3700、3800 シリーズ ルータで構成されるスポークでは、Cisco IOS Release 12.4(9)T 以降が必要です。Cisco 831 シリーズのスポークでは、Cisco IOS Release 12.3(11)T10 が必要です。

スポークツースポーク モデルでの課題は、トラフィックがハブ サイトから送信されるのと同様に 1 つまたは複数のスポーク サイトからも送信されることです。ハブ サイトとスポーク サイトがすべてアクセス リンク データ レート（または、前のセクションで説明されたように、そのレートの何パーセントか）で QoS シェーパーを設定した場合、ハブとスポークの集合が 1 つのスポークを過負荷にするほどのトラフィックを送信する可能性があります。プライオリティおよび帯域幅キューと両方のシェーパーに適切な値を決定することが課題となります。

このため、ブランチまたはスポーク ルータへのアクセス リンクに QoS を提供する、QoS に対応したサービス プロバイダーが、最良のソリューションです。

IP マルチキャスト

IP マルチキャストには、2 つの問題があります。1 つめの問題は、ソリューションを拡張することで、多数の受信者がストリームに加わる可能性があることです。2 つめの問題は、p2mp GRE インターフェイスによって機能が制約されることです。

IP マルチキャストおよび IPSec 暗号化によるスケーラビリティ テストでは、多くのパケットが即座に複製されることでパケット損失の問題があることを示しています。IP マルチキャストの複製は、加入した各宛先用に新しいヘッダーを生成します。ペイロードは変更されません。各パケットは、暗号化などのダウンストリーム ソフトウェア プロセスに対してヘッダーとペイロードをリンクするポインタとして参照されます。1 つのパケットが複製されたあと、暗号化に渡されるポインタのリストによって、暗号カードのインバウンド RxRing が過負荷になる可能性があります。加入した宛先の数が RxRing のサイズを超えた場合、この現象は確実に発生します。暗号化プロセスでは、パケット バーストを受信する前に RxRing を空にすることができない可能性があるため、ストリームでの pps レートが高いか、複数のマルチキャスト ストリームが流れている場合、この現象が発生する可能性は高くなります。

たとえば、VPN Shared Port Adapter（SPA; 共有ポート アダプタ）が搭載されている Cisco Catalyst 6500 を使用し､ブランチ オフィスに 1000 の p2p GRE over IPsec トンネルを設定するデザインについて考えてみます。各ブランチ オフィスが 1 つのマルチキャスト ストリームに加入している場合、VPN SPA は、VPN トンネルごとに 1 つずつ、各マルチキャスト パケットを 1000 回複製する必要があります。Sup720 がストリームの複製スピードを持続できると想定すると、VPN SPA の入力キューに多くのパケット（最大 1000）が到着し、過負荷またはパケットの廃棄が発生します。顧客に IP マルチキャストの要件がある場合、適切なスケーラブルなデザインについて、次の URL にある『*Multicast over IPsec VPN Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html

DMVPN ネットワークは非ブロードキャスト サブネットであるため、DMVPN ネットワークで IP マルチキャストを導入する前に、特殊な状況を考慮する必要があります。まず、同じサブネットのメンバーであるスポークは、相互に PIM 隣接関係を形成できません。スポークツースポークトポロジでは、RPF チェックによって、マルチキャスト フローがハブを通過することはできません。フローは常にハブを通過する必要があるので、スポーク間の IP マルチキャストは不可能です。さらに、これと同じ理由で、スポークは Rendezvous Point（RP; ランデブー ポイント）として使用できません。

ハブアンドスポーク構成では、すべてのスピーカーが NHRP ハブ ルータの背後にあり、加入したブランチの数が暗号化エンジンの RxRing 制限を超えない場合、DMVPN での IP マルチキャストは機能します。IP マルチキャスト ストリームがブランチから発生した場合、ハブ サイトのクライアントのみがストリームを受信できます。次の設定例では、DMVPN でのマルチキャストを示します。

- ハブ ルータ：

```
!
interface Tunnel0
 description dmvpn tunnel
 ip address 10.173.20.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-mode
 ip nhrp authentication secret
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.168.201.1
 ip nhrp network-id 10203
 tunnel source GigabitEthernet0/1.201
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile dmvpn
!
```

- スポーク ルータ：

```
!
interface Tunnel0
 description dmvpn tunnel
 ip address 10.173.20.10 255.255.255.0
 no ip redirects
 ip mtu 1400
```

```
 ip pim sparse-mode
 ip nhrp authentication secret
 ip nhrp map multicast dynamic
 ip nhrp map 10.173.20.1 192.168.201.1
 ip nhrp map multicast 192.168.201.1
 ip nhrp network-id 10203
 ip nhrp nhs 10.173.20.1
 load-interval 30
 tunnel source GigabitEthernet0/0.201
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile dmvpn
!
```

その他のネットワーキング機能との相互作用

NAT、PAT、DHCP、およびファイアウォールなど、その他のネットワーキング機能に関する考慮事項も、DMVPN ネットワークのデザインに適用されます。ここでは、これらの機能について説明します。

NAT と PAT

NAT と PAT によって、セキュリティの強化とアドレスの節約が可能になりますが、これらは両方とも IPSec VPN の実装における問題を提起します。ISAKMP は、適切な動作のために、crypto ピアごとの個々の IP アドレスを使用します。PAT は 1 つの IP アドレスの背後に複数の crypto ピアを隠します。

IPSec NAT Traversal（NAT-T）機能は、IPSec SA と ISAKMP トラフィックの両方を UDP wrapper でカプセル化することによって、IPSec トラフィックが NAT デバイスまたは PAT デバイスを通過できるようにします。NAT-T は最初に Cisco IOS バージョン 12.2(13)T で導入され、VPN デバイスによって自動検出されます。このリリース以降を実行している Cisco IOS ルータでは、グローバル コマンドとしてデフォルトで有効になっているため、設定する必要はありません。NAT-T 機能は、crypto ピア間にある PAT デバイスを検出し、NAT-T（存在する場合）をネゴシエートします。

IPSec NAT-T（トランスペアレンシーとしても知られる）の詳細については、次の URL を参照してください。http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftipsnat.html

DMVPN デザインは、ハブアンドスポーク展開モデルでの NAT-T と互換性があります。ヘッドエンド ルータが NAT の背後にある DMVPN トポロジをサポートするには、ヘッドエンド ルータとブランチ ルータの両方で、Cisco IOS Release 12.3(9a) または 12.3(12)T2 以降が必要です。

スポークツースポーク デザインでは、NAT はさらに大きな懸念事項です。NHRP レジストレーションでは、1 つのスポークが NAT デバイスの背後にある場合、スポークツースポーク暗号セッションが適切に形成されません。この状況では、IPSec SA は確立されず、ブランチはハブ経由でリモート ブランチにパケットを送信し続けます。ソフトウェア バージョンによっては、これらのパケットはプロセッサでスイッチングされる場合があります。このため、スポークが NAT 境界の背後にある場合、スポークツースポーク トポロジは構成しないでください。

デュアル DMVPN クラウド トポロジでは、展開モデルに関係なく、シングル ティア ヘッドエンド アーキテクチャにトランスポート モードの IPSec を設定できます。一般的には IPSec トンネル モードが DMVPN デザインで推奨されていますが、NAT および PAT による IPSec トランスポート モードの実行には、次のような考慮事項があります。

- ブランチが NHRP レジストレーション情報をヘッドエンドに送信する場合、ヘッドエンドは、ブランチの外部 NAT アドレスと内部ホスト GRE アドレスの両方を確認します。ヘッドエンドは、ブランチからの外部 NAT アドレスを選択して使用します。

- 外部 NAT アドレスは一意であるため、異なるブランチ ルータが同じ（重複している）内部ホスト GRE アドレスを使用できます。

デュアル ティア ヘッドエンド アーキテクチャでは、IPSec トンネルをトンネル モードで設定する必要があります。この設定では、次の警告に注意してください。

- ヘッドエンド ルータは、ブランチ ルータから送信される NHRP レジストレーション情報内のブランチ ルータの内部ホスト GRE アドレスのみを確認できます。
- したがって、ブランチ ルータは固有の内部ホスト GRE アドレスをもっており、DMVPN クラウド内のすべてのブランチのために調整が必要です。

（注） ヘッドエンドとブランチの間に DMVPN 経由で生成される IPSec トンネルは、VPNSM が搭載された Cisco Catalyst 6500 または Cisco 7600 を使用する場合、NAT および PAT の背後にあるヘッドエンドではサポートされないことに注意してください。これがデザイン上必要な場合、ヘッドエンドで Cisco 7200VXR またはその他の Cisco IOS ルータを使用してください。

1 つの NAT デバイスの背後に複数のブランチ ルータがある状況では、DMVPN は、NAT デバイスが各ブランチ ルータを一意の外部 NAT IP アドレスに変換する場合にのみ、この設定をサポートできます。

ファイアウォールの考慮事項

ここでは、DMVPN デザインを実装する際のさまざまなファイアウォールの考慮事項について説明します。

ヘッドエンドまたはブランチ

暗号と DMVPN ヘッドエンドまたはブランチの配置によって、次のプロトコルおよびポートを許可する必要があります。

- UDP ポート 500 — ISAKMP の送信元および宛先
- UDP ポート 4500 — NAT-T の宛先
- IP プロトコル 50 — ESP
- IP プロトコル 51 — AH（AH が実装されている場合）
- IP プロトコル 47 — GRE

ヘッドエンド ファイアウォールと関連した暗号ヘッドエンドのネットワークの場所は、両方のシステムのアクセス性とパフォーマンスの両方に影響を及ぼします。ネットワーク管理者は、トンネル トラフィックが双方向に許可されるように、すべてのファイアウォールを適切に設定してください。すべての暗号セッションはブランチ ルータから開始されるため、暗号ヘッドエンドは、ブランチ ルータにアクセスできる必要があります。

暗号アクセスの確認

DMVPN でトンネル プロファイルを使用すると、通常では暗号化を必要とするパケットの照合に使用される crypto ACL を静的に定義する必要がありません。ただし、この機能は、ソフトウェアによって動的に処理されています。**show crypto map** Cisco IOS コマンドを使用して、生成されるアクセス リストを表示することができます。アクセス リストは、トンネル エンドポイントからの GRE パケットを照合します。暗号化と GRE トンネルが同じエンドポイントを使用していない場合、トンネル プロファイルを使用できず、crypto アクセス リストまたはダイナミック crypto map を設定する必要があります。アクセス リストには、GRE エンドポイントではなく、暗号エンドポイントを反映してください。この設定は、デュアル ティア ヘッドエンド アーキテクチャを実装する際に必要です。

よくある設定ミス

次のセクションでは、DMVPN を設定する際に発生する、一般的な誤りと問題について説明します。

ルーティング プロトコルでのトンネル エンドポイントのアドバタイズ

内部ルーティング プロトコルにトンネル エンドポイントを含めることができます。この場合、ヘッドエンド アドレスは、一般的にパブリック インターネットでグローバルにルーティングされるアドレスです。推奨はされませんが、このアドレスは内部にもアドバタイズできます。この状況では、DMVPN サブネットは最初は適切に機能しますが、ルーティングでコンバージェンスが行われると、ブランチは、外部インターフェイス経由ではなく、DMVPN トンネル経由でヘッドエンドのパブリック アドレスに到達しようと試みる可能性があります。これによってトンネルで障害が発生し、その結果、ルーティング プロトコルはパブリック アドレスのアドバタイズを中止しますが、DMVPN トンネルは再び正しく機能するようになります。このプロセスは継続的に繰り返され、「リカーシブ ルーティング」と呼ばれることがあります。

IPSec トランスフォーム セットの一致

2 つの crypto ピアの間に、少なくとも 1 つの一致する IPSec トランスフォーム セットを設定してください。特定の暗号化アルゴリズムの強度を指定する場合、ヘッドエンドとブランチの両方に、共通の強度の暗号化アルゴリズムとトランスフォーム セットを設定する必要があります。そうしない場合には、IPSec トンネルが始動しません。

ISAKMP ポリシーの一致

すべての Cisco IOS デバイスに、デフォルトの ISAKMP ポリシーが設定されています。このデフォルトの内容は、DES 暗号化、HMAC SHA、RSA シグニチャの IKE 認証、および DH グループ 1 です。より強力な ISAKMP ポリシーを希望する場合、両側でポリシーをサポートするようにしてください。

ISAKMP ポリシーと IPSec トランスフォーム セットで、同じ暗号化レベルのトランスフォーム セットとハッシュ方式を使用することは一般的ですが、必須ではありません。

CHAPTER 3

スケーラビリティに関する考慮事項

この章では、VPN ソリューション用のシスコ製品を選択する際の、以下の手順について説明します。

- ヘッドエンドのサイズ指定
- ヘッドエンド デバイス用に導入できるシスコ製品の選択
- ブランチ デバイス製品のサイズ指定と選択に関する情報

スケーラビリティに関する一般的な考慮事項

ここでは、デザイン上の要件を検討するうえで役に立つ、スケーラビリティに関する一般的な考慮事項について説明します。

IPSec 暗号化スループット

暗号化される各パケットは暗号化エンジンを通過するので、各プラットフォーム（ヘッドエンドまたはブランチ）の IPSec 暗号化エンジンのスループット容量は、スケーラブルなデザインにする必要があります。したがって、暗号化スループットでは双方向速度を考慮してください。表 3-1 および表 3-2 に、一般的なヘッドエンドおよびブランチ接続の速度に関する例を示します。

表 3-1　ヘッドエンド接続速度

接続タイプ	速度（Mbps 単位）	必要な暗号化スループット（Mbps 単位）
T3/DS3	44.7	90.0
OC3	155.0	310.0
OC12	622.0	1250.0

表 3-2　ブランチ接続速度

接続タイプ	速度（Mbps 単位）	必要な暗号化スループット（Mbps 単位）
T1	1.5	3.0
2 × T1	3.0	6.0

表 3-2　ブランチ接続速度（続き）

T3/DS3	44.7	90.0
ブロードバンド ケーブル /DSL	384 Kbps アップリンク / 2 Mbps ダウンリンク	2.4

一般的にスループットが増加すると、ルータ CPU の負荷も増加します。ただし、Cisco 871 ～ 7600 のシスコ ルータ製品すべてで使用可能なハードウェア アクセラレーション 暗号化を使用すると、メイン CPU の負荷を VPN ハードウェアが負担します。それでもやはり、メイン ルータ CPU での処理は発生するため、一般的にスループットが高いと CPU の使用率が高くなります。

パケット / 秒 — 最重要要因

帯域幅スループット容量を考慮する必要はありますが、終端または集約している接続速度のパケット レートはより重要です。

一般的に、ルータおよび暗号化エンジンには 1 秒あたりに処理するパケット数（pps）の上限があります。テストとスループットの評価に使用するパケットのサイズによって、実際のパフォーマンスよりも低いまたは高い結果が出る可能性があります。たとえば、VPN モジュールを搭載したルータが 20 Kpps を処理できる場合、100 バイトのパケットだと 16 Mbps のスループットになり、同じパケット レートで 1400 バイトのパケットだと 224 Mbps になります。

スループットはこのように変化が大きいので、ルータの転送能力を判断するパラメータとしては、一般的に bits per second（bps; ビット / 秒）よりも pps の方が適切です。ヘッドエンドのスケーラビリティは、ヘッドエンドへのトンネルを終端するすべてのブランチの転送能力を集約したものです。したがって、すべてのブランチの集約 pps はヘッドエンドの pps レートに影響します。

トンネルの数によるスループットへの影響

スループットはプラットフォームのアーキテクチャに大きく依存しますが、一般的にトンネルの数が増加すると全体的なスループットは減少します。ルータが、復号化されたパケットの送信元ピアとは異なるピアからパケットを受信すると、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）に基づいて新しいパケットに関する検索を行う必要があります。次に、新しいパケットのトランスフォーム セット情報とネゴシエーションされたセッション キーが、処理のためハードウェア復号化エンジンにロードされます。多数の SA 上でトラフィックが流れると、スループットのパフォーマンスに悪影響を与えます。

しかし、ハードウェア アクセラレーション IPSec 暗号化を備えたプラットフォームで、トンネル処理のオーバーヘッドを軽減するデザインが増えてきています。したがって、トンネルの数に関係なく、パフォーマンスを維持できます。たとえば、Cisco 7600 の VPN SPA ブレードのスループットは、トラフィック ロードが少数または数千のトンネルから流れてくるかに関係なく、ほとんど変わりません。

GRE カプセル化によるスループットへの影響

ルータ暗号化のスループットは、GRE の設定によって影響を受けます。各パケットの先頭にヘッダーが追加されるだけでなく、これらのヘッダーを暗号化する必要があります。ハードウェア アクセラレーションを実行していないと、GRE カプセル化プロセスにより全体的な CPU 利用率が上昇します。DMVPN デザインの総スループットは、IPSec ダイレクト カプセル化デザインのスループットよりも低くなります。

ルーティング プロトコルによる CPU オーバーヘッドへの影響

ルーティング プロトコルを実行すると、CPU のオーバーヘッドが影響を受けます。キープアライブまたは hello パケットの処理と、ルーティング テーブルの維持では、限られた CPU 時間を使用します。この時間は、ルーティング ピアの数とルーティング テーブルのサイズによって変化します。ネットワーク管理者は、特定のルーティング プロトコルに関する周知の実践方法に基づいてそのルーティング プロトコルをデザインしてください。

スケーラブルなデュアル DMVPN クラウド トポロジ — ハブアンドスポーク展開モデル

ここでは、ハブアンドスポーク展開モデルのデュアル DMVPN クラウド トポロジにおけるヘッドエンドとブランチのスケーラビリティについて説明します。

ヘッドエンドのスケーラビリティ

ここでは、ハブアンドスポーク展開モデルのデュアル DMVPN クラウド トポロジで考慮すべき、ヘッドエンドのスケーラビリティのさまざまな要因について説明します。

トンネル集約のスケーラビリティ

ヘッドエンドが終端できる IPSec トンネルの最大数を考慮してください。トンネルのスケーラビリティとは、ヘッドエンドの集約ポイントで終端されるブランチ ルータの数を表します。この数には、プライマリ トンネルと、フェールオーバーの発生時に各ヘッドエンドが対応する代替トンネルを含める必要があります。

プラットフォームが集約できる IPSec トンネルの数は、プラットフォームを推奨する際の主要な判断要因として使用できます。ただし、暗号化 pps レートの方がより重要です。

集約のスケーラビリティ

ヘッドエンドが終端するトンネルの数のほかに、集約 pps を考慮してください。要件は、次のさまざまな要因によって影響を受けます。

- ヘッドエンド接続速度 — ブランチ ルータの IPSec トンネルを伝送するヘッドエンドでの WAN リンク速度（DS3、OC3、OC12 など）
- ブランチ接続速度 — 各ブランチ オフィスの一般的な帯域幅（フラクショナル T1、T1、T3、ブロードバンド DSL/ ケーブルなど）
- 予定利用率 — 通常動作時の WAN 帯域幅の最大利用率（または顧客要件に応じてピーク）

pps レート（トラフィック サイズおよびトラフィックの構成）は、ルータのスケーラビリティにおける最大の要因です。

顧客の要件に応じた集約のスケーラビリティの事例

ここでは、ヘッドエンドのスケーラビリティの要因の例を示します。

顧客事例 — 1000 のブランチ

以下のような顧客の要件を想定します。

- ブランチ オフィスの数 — 1000

- ブランチ アクセス速度 — 384 k/1.5 M ケーブル /DSL
- ヘッドエンド アクセス速度 — OC12（622 Mbps）
- 予定利用率 — 33%

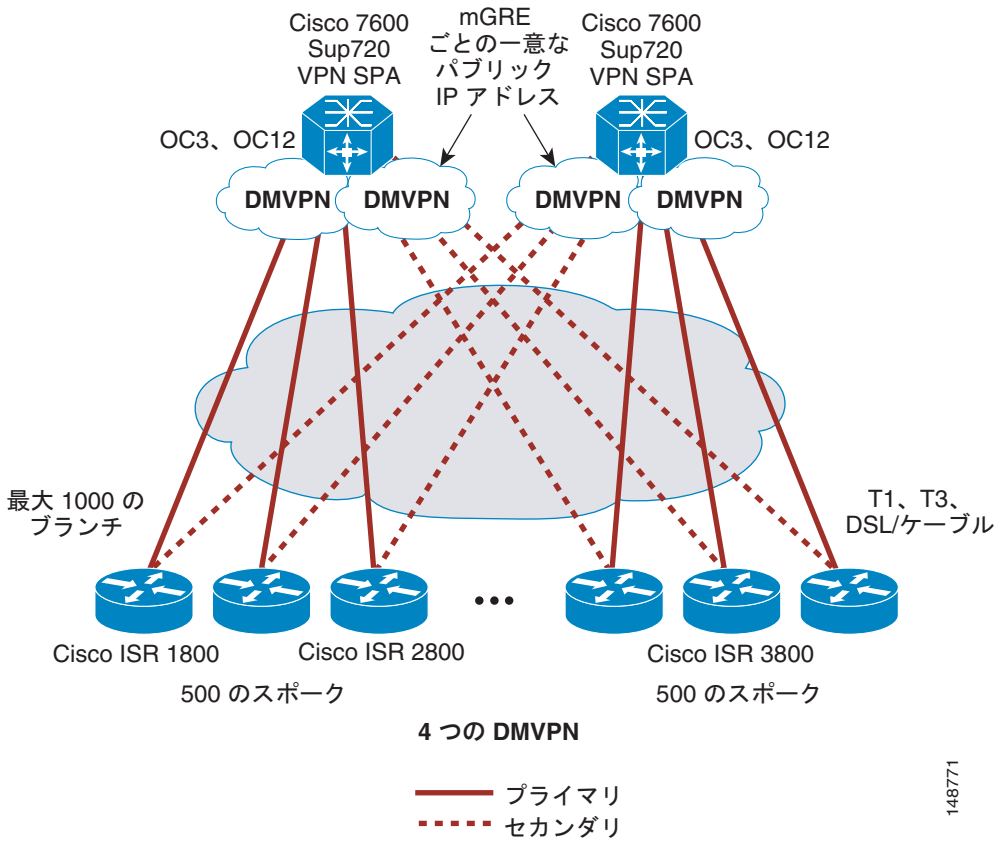
集約帯域幅要件の計算式は次のとおりです。

- 通常 — 1000 ×（384 kbps + 1.5 Mbps）× 33% の利用率 = 628 Mbps
- 最悪の場合 — 1000 ×（384 kbps + 1.5 Mbps）× 100% の利用率 = 1.9 Gbps

スタック構成の Cisco 7200VXR プラットフォームをデザインの選択肢として推奨できます。1000 のトンネルを集約するには少なくとも 4 台が必要です。ただし、これでは必要な集約帯域幅（628 Mbps 以上）を提供できません。

別のデザインとして、Sup720 および VPN SPA をそれぞれ搭載した Cisco 7600 ルータのペアを推奨できます（図 3-1 を参照）。VPN SPA はそれぞれ、最大 1.2 Gbps の暗号化パフォーマンスを提供するので、このデザインでは最大で OC12 の接続速度を各ヘッドエンドでサポートできます。

図 3-1　Cisco 7600 ベースの DMVPN デザイン



VPN SPA は最大 5000 の IPSec トンネルと 1000 のアクセラレート GRE トンネルを処理できますが、アクセラレート mGRE は現在サポートされていません。これは、4 バイトのフィールドを GRE パケット ヘッダーに追加する、mGRE トンネル キーがサポートされていないからです。ただし、VPN SPA でアクセラレート GRE 機能を利用するための方法があります。

mGRE トンネル キーは、複数の DMVPN クラウドが同じルータ上に設定されている場合に、パケットがどの DMVPN クラウドに所属しているかを区別するために使用されます。DMVPN クラウドを区別する別の方法として、個別のパブリック IP アドレスを mGRE インターフェイスごとに割り当てることができます。リモート ルータは割り当てられた mGRE インターフェイスに接

続し、トンネル キーの代わりに IP アドレスを使用してヘッドエンド上の宛先である DMVPN クラウドを指定します。このようにすれば、Sup720 で mGRE を処理し、VPN SPA で、IPSec アクセラレーションを利用できます。

上記のデザインで、最大 1000 のブランチ オフィスをサポートできます。ルーティング ピアは制限の要因となる傾向にあり、Cisco 7200VXR プラットフォームでは、ルーティング ピアは 500 ～ 700 に制限されます。しかし、Sup720 を搭載した Cisco 7600 では、最大 1000 のルーティング ピアが動作することがシスコのスケーラビリティ テスト ラボで実証されました。

顧客事例 — 5000 のブランチ

以下のような顧客の要件を想定します。

- ブランチ オフィスの数 — 5000
- ブランチ アクセス速度 — 128 Kpps/1 Mbps DSL
- ヘッドエンド アクセス速度 — OC12（622 Mbps）
- 予定利用率 — 25%

集約帯域幅要件の計算式は次のとおりです。

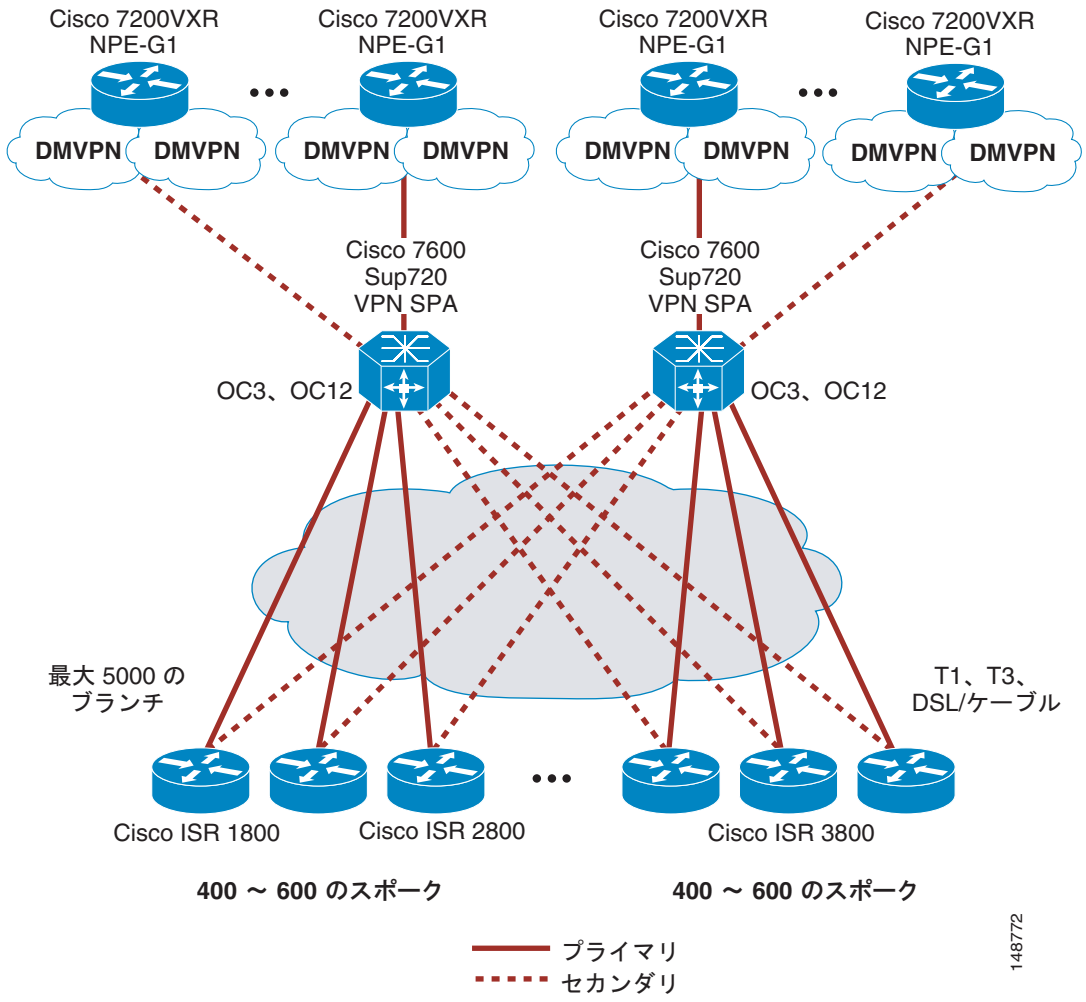
- 通常 — 1000 ×（128 kbps + 1 Mbps）× 25% の利用率 = 1.24 Gbps
- 最悪の場合 — 1000 ×（128 kbps + 1 Mbps）× 100% の利用率 = 5.64 Gbps

現在、単一のハードウェアで 5000 の DMVPN トンネルを集約できるシスコのプラットフォームはありません。このような大規模なデザインのオプションには以下が含まれます。

- 500 ～ 700 のブランチ スポーク用の Cisco 7200VXR ベースのデザイン、または 1000 のスポーク用の Cisco 7600 ベースのデザインなど、小規模のデザインを複製します。
- mGRE 接続を終端する Cisco 7200VXR プラットフォームと大容量 IPSec 暗号化用の Cisco 7600 プラットフォームを使用して、デュアル ティア アーキテクチャを実装します。

図 3-2 に、デュアル ティア アーキテクチャを示します。

図 3-2　DMVPN デュアル ティア ヘッドエンド アーキテクチャ



Cisco 7200VXR プラットフォームは、mGRE インターフェイスで DMVPN クラウドを終端します。デザインのこのティアでは IPSec 暗号化が必要ないので、SA-VAM2+ は必要ありません。さらに、これらのプラットフォームは一般的に、mGRE と IPSec の両方を実行する場合よりも多くのスポークを処理できます。

このデザインの暗号化ティアでは、Sup720 と VPN SPA を搭載した Cisco 7600 が IPSec 暗号化サービスを実行します。これにより、1 台の Cisco 7600 で最大で OC12 の暗号化速度を提供し、最大 5000 のトンネルの IPSec トンネル集約ポイントとして動作できます。

このデザイン方式には非常に重要な次の 2 つの制限事項があります。

- mGRE および IPSec は別々の IP アドレスで終端されるので、DMVPN スポークツースポーク トポロジはこのデザイン トポロジではサポートされません。スポークツースポーク機能の場合、送信元および宛先 IP アドレスは同一でなければいけません。
- IP マルチキャストによって、VPN SPA で終端できるトンネルの総数が制限されます。トンネルの数が多すぎると、VPN SPA の入力キューを過負荷にする瞬間的な IP マルチキャスト ファンアウト パケット レプリケーション バーストが発生します。IP マルチキャストが必要な場合、VPN SPA を通過するストリームの総数を 1000 未満にしてください。

ブランチ オフィスのスケーラビリティ

ブランチ ルータの主な役割は次のとおりです。

- ヘッドエンド ルータからの、p2p GRE over IPSec トンネルまたは mGRE トンネルを終端します。
- GRE トンネル内部でルーティング プロトコルを実行し、内部ルートをアドバタイズします。

ブランチ オフィス向けの製品を選択する場合に考慮すべき最重要要因には、以下が含まれます。

- ヘッドエンドに対するブランチ アクセス速度と予定トラフィック スループット（たとえば、フラクショナル T1、T1、T3、ブロードバンド ケーブル /DSL）
- ブランチ ルータが提供する他のサービス（たとえば、DHCP、NAT/PAT、VoIP、Cisco IOS ファイアウォール、IOS-IPS）

pps レート（トラフィック サイズおよびトラフィックの構成）は、ブランチ ルータのスケーラビリティにおける最大の要因です。

各ブランチ ルータは、ハブアンドスポーク モデルのデザイン上、1 組のトンネル（プライマリおよびセカンダリ）を終端する必要があるので、p2p GRE over IPSec トンネルの数はブランチのサイズ指定にあまり関係ありません。

主な考慮点は、トラフィックのスループット量（pps および bps）と、対応する CPU 利用率です。CPU 利用率が通常の動作条件下で 65% を超えないようにブランチ ルータを選択してください。ブランチ ルータには、処理しなければいけない定期的なイベントを処理するのに十分な CPU サイクルが必要です。この例では、ISAKMP および IPSec SA の確立とキーの再生成、SNMP、Syslog アクティビティ、ローカル CLI EXEC 処理が含まれます。

初期導入時とテスト後には、通常の動作条件下で CPU 利用率が 65% を超えるレベルでブランチ ルータを稼働させることも可能です。ただし、このデザイン ガイドでは 65% 以下を推奨します。

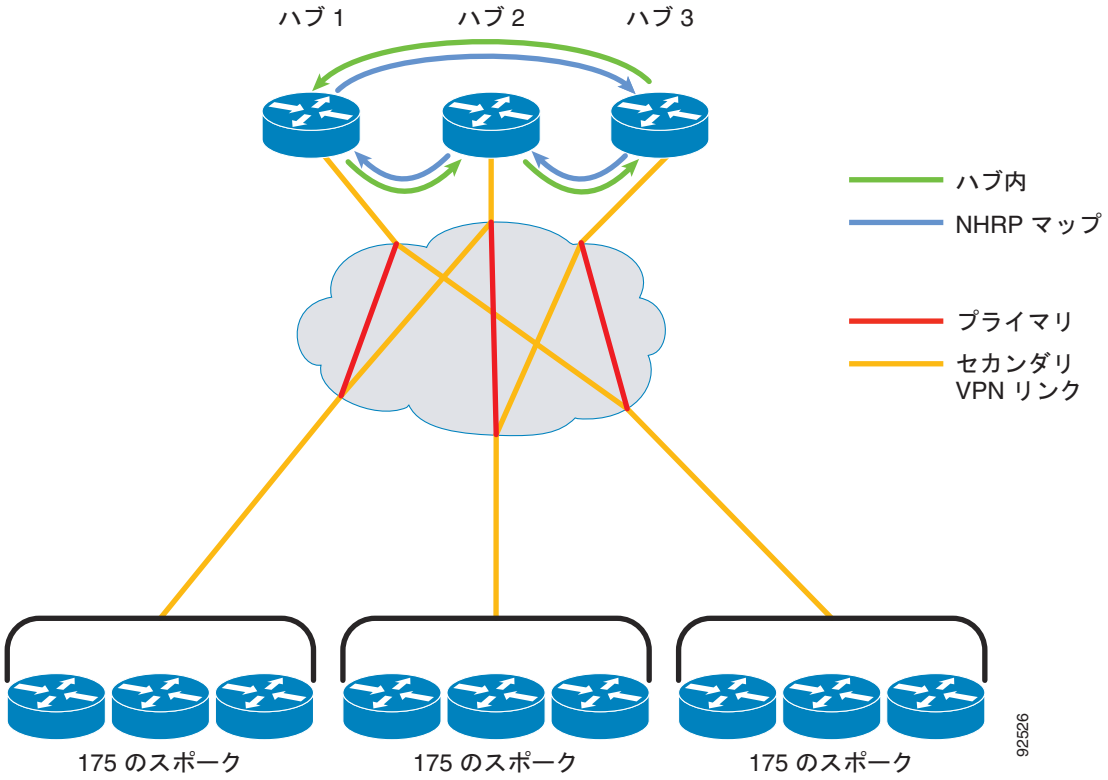
シスコ サービス統合型ルータ（ISR）1840、2800、および 3800 シリーズ製品は、旧来の製品よりも高い CPU パフォーマンスを発揮します。ISR はマザーボードに暗号化モジュールが搭載されていて、暗号パフォーマンスを向上するため、AIM 暗号化モジュールにアップグレードできます。

スケーラブルなデュアル DMVPN クラウド トポロジ — スポークツースポーク デザイン

スケーラブルなスポークツースポーク デザインは、少々複雑になります。まず、このデザインで耐障害性を実現するには、ブランチ ルータごとに 2 つのヘッドエンドへのリンクを構成してください。デュアル DMVPN トポロジでは、クラウドごとに 1 つのヘッドエンドがあります。ルーティングによって、プライマリ クラウドを決定します。ヘッドエンド ルータが 2 つのクラウドを処理する場合（1 つはあるブランチ群のプライマリとして、もう 1 つは別のブランチ群のセカンダリとし使用）、ヘッドエンドでのロード バランシングが可能です。この方法により、追加のブランチ ルータをネットワークに接続するためより多くの DMVPN クラウドが必要になった場合に、ヘッドエンド ルータを追加できます。

この方式の欠点は、スポークツースポーク セッションが別の DMVPN クラウド間では許可されないことです。スポークツースポーク セッションを実現するには、プライマリ接続のための大きな DMVPN クラウド 1 つと、プライマリに障害が発生した場合に使用する 2 番めの DMVPN クラウドが 1 つ必要です。大きな DMVPN クラウドを構築するには、ヘッドエンド ルータをデイジーチェーン接続してください。異なるヘッドエンドとリンクされたブランチの間にスポークツースポーク トンネルを構築するには、ブランチにヘッドエンドへの NHRP マップがあるのと同様に、ヘッドエンド同士がお互いへの NHRP マップを持つ必要があります。3 つのヘッドエンド ルータが 1 つの DMVPN クラウドにデイジーチェーン接続されている事例を考慮します（図 3-3 を参照）。

図 3-3　1 つの DMVPN クラウドのスケーリング



次の事項に注意してください。

- スポーク グループは異なるハブ（プライマリとセカンダリ）にマッピングされます。それぞれオレンジとグレーの線で示します。各ハブには、スポークからのプライマリおよびセカンダリ トンネルを集約する mGRE インターフェイスが 1 つしかないので、スポーク ファンアウトは 175 ルータ / グループに制限されます（総数で 350 スポーク / ハブ）。
- 各ハブには相互に NHRP マップがあります。ブルーとグリーンの線で示します。
- ハブ内通信は、mGRE トンネル上で行われる必要があります。
- ハブは、mGRE トンネル上で相互にルーティング ピアでなければいけません。

以下のハブ設定の抜粋を参照してください。関連する NHRP および NHS コマンドはイタリック体で表示されています。

- ハブ 1 ルータ：

```
version 12.3
!
hostname Hub1
!
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile VPN-DMVPN
 set transform-set ENTERPRISE
!
interface Tunnel0
 description mGRE Template Tunnel
 bandwidth 1000
 ip address 10.0.0.1 255.255.240.0
 ip mtu 1400
 no ip next-hop-self eigrp 1
```

```
 ip nhrp authentication cisco123
 ip nhrp map 10.0.0.2 172.16.0.5
 ip nhrp map multicast 172.16.0.5
 ip nhrp map 10.0.0.3 172.16.0.9
 ip nhrp map multicast 172.16.0.9
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.2
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile VPN-DMVPN
!
interface FastEthernet0/0
 description Outside Interface
 ip address 172.16.0.1 255.255.255.252
!
```

- ハブ 2 ルータ：

```
version 12.3
!
hostname Hub2
!
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile VPN-DMVPN
 set transform-set ENTERPRISE
!
interface Tunnel0
 description mGRE Template Tunnel
 bandwidth 1000
 ip address 10.0.0.2 255.255.240.0
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp authentication cisco123
 ip nhrp map 10.0.0.1 172.16.0.1
 ip nhrp map multicast 172.16.0.1
 ip nhrp map 10.0.0.3 172.16.0.9
 ip nhrp map multicast 172.16.0.9
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.3
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile VPN-DMVPN
!
interface FastEthernet0/0
 description Outside Interface
 ip address 172.16.0.5 255.255.255.252
!
```

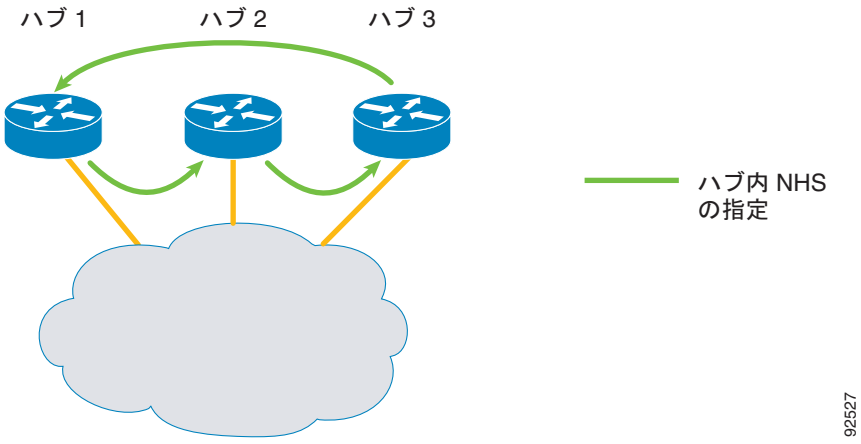
- ハブ 3 ルータ：

```
version 12.3
!
hostname Hub3
!
crypto ipsec transform-set ENTERPRISE esp-3des esp-sha-hmac
```

```
 mode transport
!
crypto ipsec profile VPN-DMVPN
 set transform-set ENTERPRISE
!
interface Tunnel0
 description mGRE Template Tunnel
 bandwidth 1000
 ip address 10.0.0.3 255.255.240.0
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp authentication cisco123
 ip nhrp map 10.0.0.2 172.16.0.5
 ip nhrp map multicast 172.16.0.5
 ip nhrp map 10.0.0.1 172.16.0.1
 ip nhrp map multicast 172.16.0.1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile VPN-DMVPN
!
interface FastEthernet0/0
 description Outside Interface
 ip address 172.16.0.9 255.255.255.252
!
```

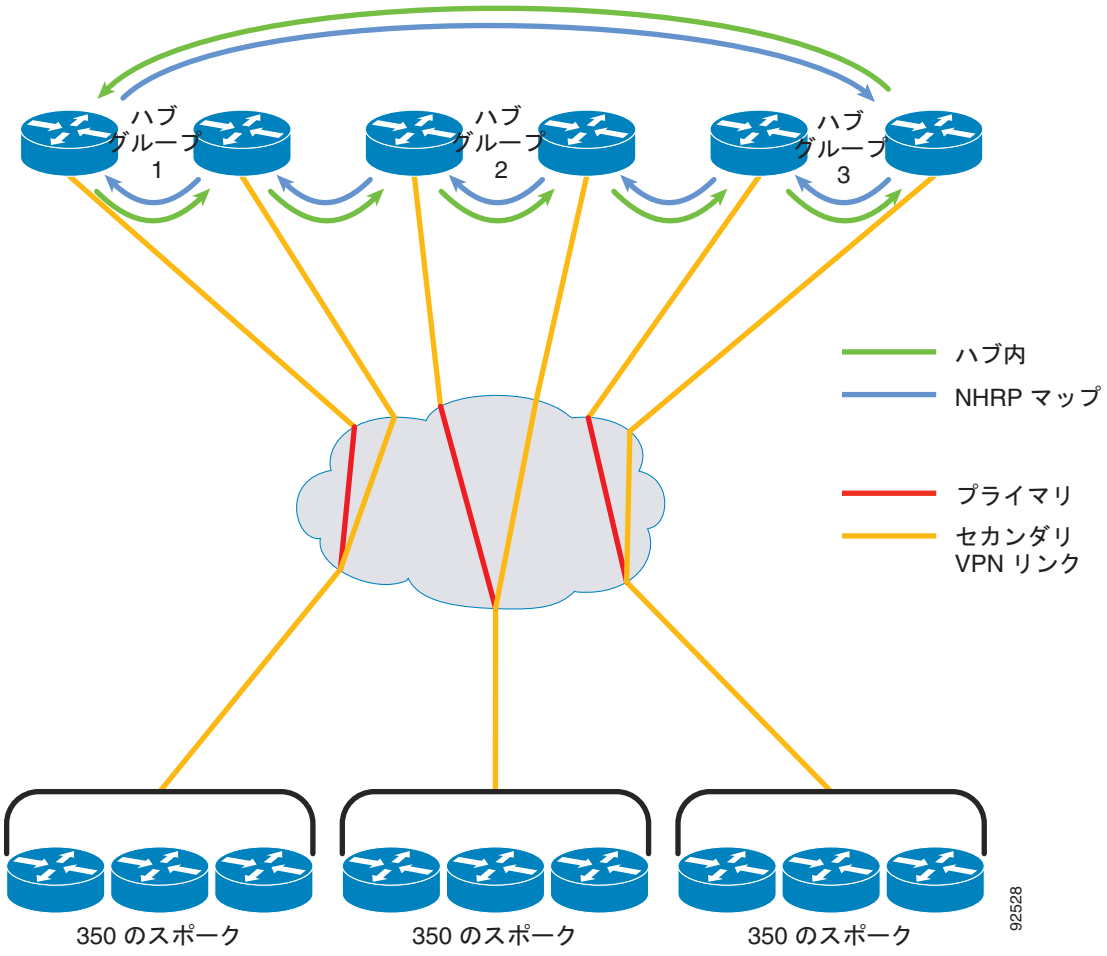
ハブの間の NHRP マップは、設定で示すように双方向です（1->2、2->1、2->3、3->2、3->1、1->3）。さらに、ハブはネクストホップ サーバとして互いに指定する必要があります。これはデイジーチェーン方法（1->2、2->3、3->1）で行われます（図 3-4 を参照）。

図 3-4　シングル DMVPN クラウド NHS デイジーチェーン



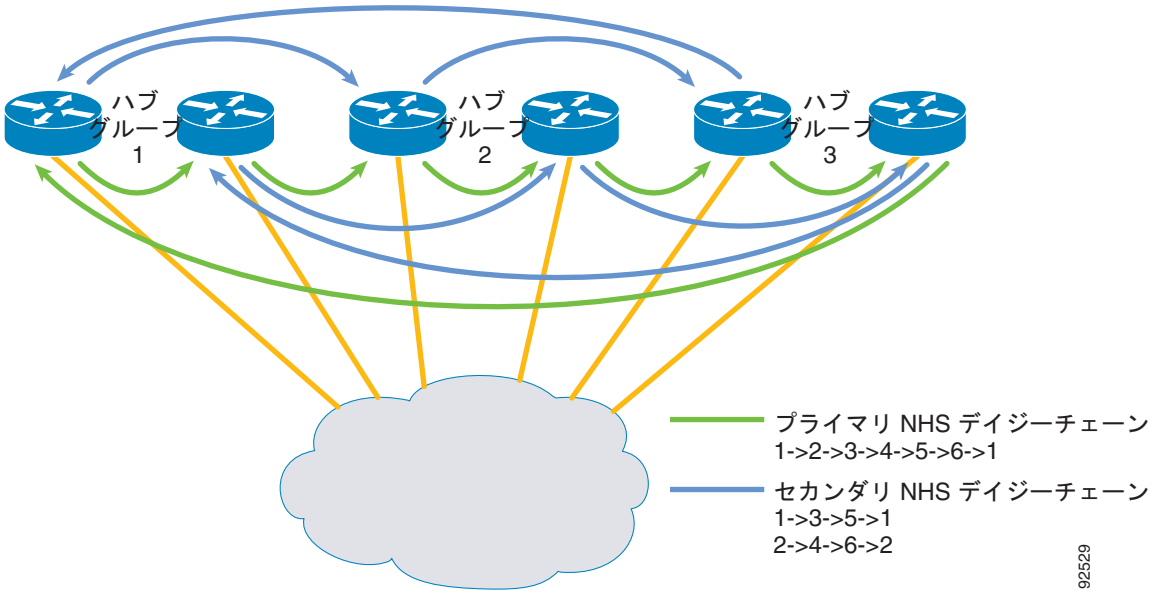
この方法で NHS デイジーチェーンを導入すると、マルチハブ デザインはシングル ポイント障害の対象になります。1 つのハブが失われると、残ったハブに接続されたスポークの間でスポークツースポーク トンネルは確立できません。図 3-5 に、耐障害性を持つデザインを示します。

図 3-5　プライマリ / セカンダリ ハブを使ったシングル DMVPN クラウド



このデザインでは、ハブ ルータはペアで展開され、専用プライマリまたはセカンダリ ハブとして動作し、スポーク ファンアウトは 350 スポーク / ハブになります。すべてのハブは互いに NHRP でマッピングされ、ルーティング アップデートを伝送させるため DMVPN 内に双方向パスが作成されます。先ほどと同様、すべてのハブは互いにルーティング ピアまたはネイバーになります。ネクストホップ サーバのマッピングに関して、このデザインでは、すべてのルータはプライマリ デイジーチェーンに属します。セカンダリ デイジーチェーンは、各ハブ グループでプライマリまたはセカンダリとして機能するルータ同士を接続します（図 3-6 を参照）。

図 3-6　NHS デイジーチェーンを使ったデュアル DMVPN

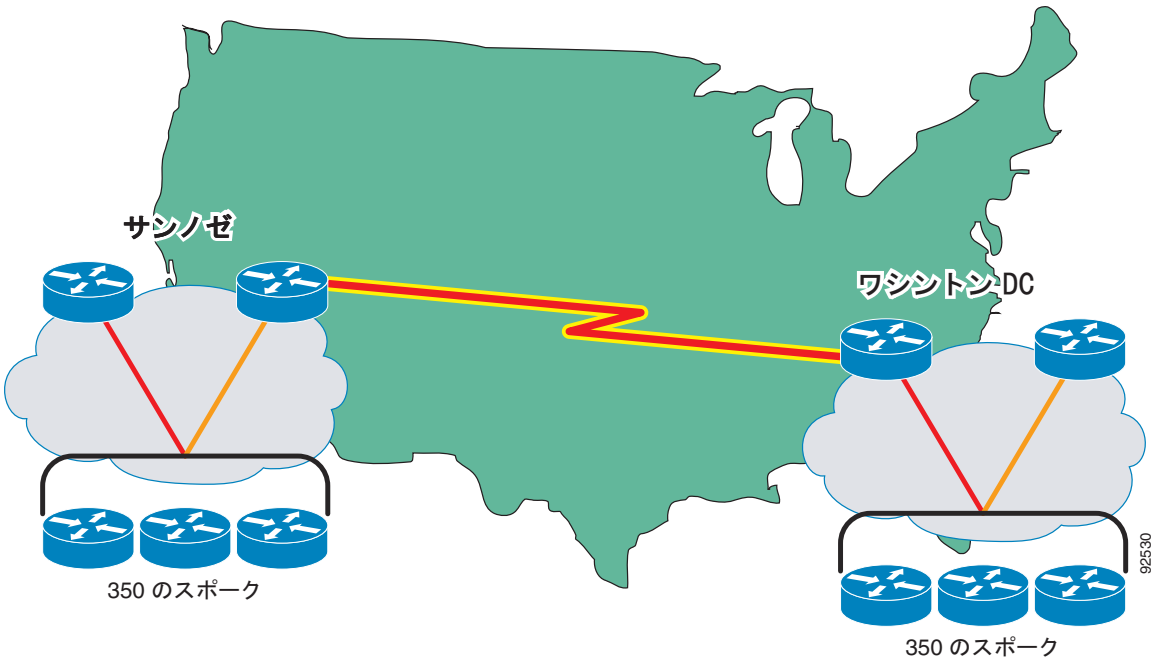


このデザインでは、スポークがセカンダリ ハブ ルータへフェールオーバーしなければならない場合でも、セカンダリ NHS デイジーチェーンを通じてパスを見つけ、異なるハブ グループにあるスポークに対してスポークツースポーク トンネルを開くことができます。

リージョナル スポークツースポーク クラスタ

スポークツースポークを必要とする大規模な DMVPN ネットワーク、特に地理的に広範囲をカバーするネットワークでは、ローカル スポークを小さなリージョナル グループとしてまとめ、ハブを専用高速リンクで接続することもできます（図 3-7 を参照）。

図 3-7　リージョナル スポークツースポーク クラスタ



スポークツースポーク応答時間が重要視される場合、2 つのハブが高速リンク経由で接続されているならば、インターネット経由で長距離のスポークツースポーク接続を介してトラフィックを送信するよりも、スポーク / ハブ / ハブ / スポークで送信する方が便利です。このタイプのデザインでは、異なるクラスタのハブ デバイスは任意のタイプの IP 転送方式で接続されます。

その他のスポークツースポーク デザインの考慮事項と警告

ダイナミック スポークツースポーク IPSec トンネルの作成が可能な場合、ネットワーク内に動作上の問題が発生する可能性があります。上記のとおり、スポークツースポーク トンネルはネットワーク内でルーティング ピアを作成せず、フル メッシュ ルーティングに関する問題をなくします。ただし、他の問題が存在する可能性があります。ここでは、簡単に説明します。

耐障害性

一部の形式の障害に対するスポークツースポーク トンネルの耐性は、スポークツーハブ トンネルより劣ります。ルーティング プロトコルはトンネル経由では実行されないので、スポークツースポーク トンネルに障害が発生しても、エンドポイントは認識せず、トラフィックのブラックホール化が発生します。暗号化されたデータ トンネルがダウン状態になっても、ISAKMP キープアライブ（設定されている場合）は継続します。エンドポイントがスポークツースポーク パスの損失に対応し、スポークハブスポーク パスの使用を再開するのに非常に長い時間かかることがあります。

パスの選択

スポークツースポーク トンネルが経由するパブリック インフラストラクチャのパス（インターネットなど）は、実際はスポークツーハブツースポーク パスよりも低速な場合があります。DMVPN では、応答時間の増加または他のネットワーク品質の低下によってスポークツースポーク パスで発生する遅延を測定し、パス選択を調整することはできません。

スポーク ルータの過負荷

複数のリモート スポークからの着信トラフィックによってスポークが過負荷になるのを防ぐ確実なメカニズムはありません。特に、スポーク ルータは小型のルータ（すなわち、性能の劣る CPU）である可能性が高く、あるスポーク デバイスに対して多数の他のスポークがトンネルを作成しようとした場合、複数のトンネルの確立が原因でスポーク デバイスの動作に問題が発生することがあります。IOS 12.3(8)T で最初に導入された 2 つの Cisco IOS 機能（IKE コール アドミッション コントロール [CAC] とシステム CAC）が、この状況を緩和するのに役立ちます。IKE CAC は、絶対値に基づいて、ルータが設定できる ISAKMP SA の数を制限します。システム CAC は、システム リソースの使用状況に基づいて SA の数を制限します。

IKE CAC はルータ上で次のように設定されます。

```
Spoke1#crypto call admission limit ike sa 25
```

この例では、ISAKMP SA の数を 25 に制限します。25 の ISAKMP SA がアクティブになると、ルータは新しい SA 要求を拒否します。IKE CAC の状態は **show crypto call admission statistics** コマンドでモニタできます。

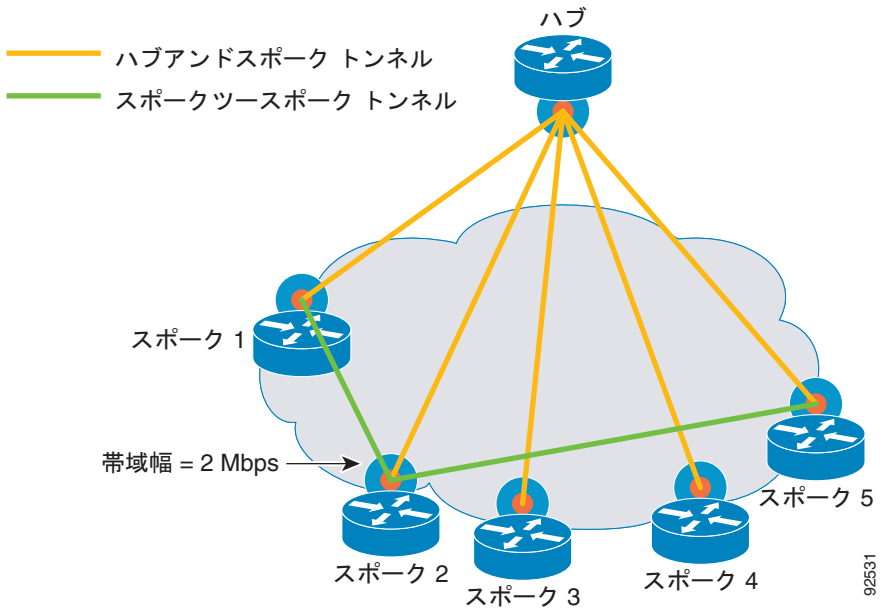
システム CAC はルータ上で次のように設定されます。

```
Spoke1#call admission limit 80
```

この例では、システム リソースの 80% が使用されると、ルータは新しい SA 要求を破棄します。システム CAC の状態は **show call admission statistics** コマンドでモニタできます。

CAC 機能で対処できないスポークツースポーク デザインの他の問題は、複数の同時スポークツースポーク IPSec トンネルによるスポーク帯域幅の単純な過負荷です。これは、ISAKMP SA の IKE 認証またはシステム リソースの上限に到達しなかった場合でも発生します（図 3-8 を参照）。

図 3-8　スポーク ルータ帯域幅の過負荷



この例では、スポーク 2 は 2 Mbps でインターネットに接続しています。このスポークには、スポーク 1 とスポーク 5 の間に確立した既存のスポークツースポーク トンネルがあります。ハードウェアに設定された IKE CAC またはシステム CAC の制限をいずれも超えていませんが、他の 2 つのスポークと確立したトンネルのトラフィックによって 2 Mbps の帯域幅が完全に消費されます。ここで、スポーク 3 がスポーク 2 とスポークツースポーク トンネルを設定しようとします。

NHRP 要求と、ISAKMP および IPSec セッションを確立するのに十分な帯域幅はありますが、トンネルの確立後にアプリケーション トラフィックを送受信するのに十分な帯域幅はありません。ここでの問題は単純に、スポーク 2 がスポーク 1 および 5 に対して、データ フローを抑制し、2 Mbps のアクセス リンクを適切に共有するよう通知する方法はないということです。UDP や TCP などの Upper-Layer Protocol（ULP; 上位層プロトコル）は最終的に適応しますが、RTP にはフロー制御メカニズムがありません。これは、先で述べた QoS のジレンマの一部です。

この場合、帯域幅の過負荷問題の回避策は、次のとおりです。

- 予想されるアプリケーション負荷に応じて、適切な帯域幅のネットワークをデザインします。
- スポークツーハブ フローとスポークツースポーク フローの割合を適切にします。デザイン推奨は、ハブツースポークが 80%、スポークツースポークが 20% です。
- 応答時間とリンクのアベイラビリティに関するユーザの希望を適切に設定します。

CHAPTER 4

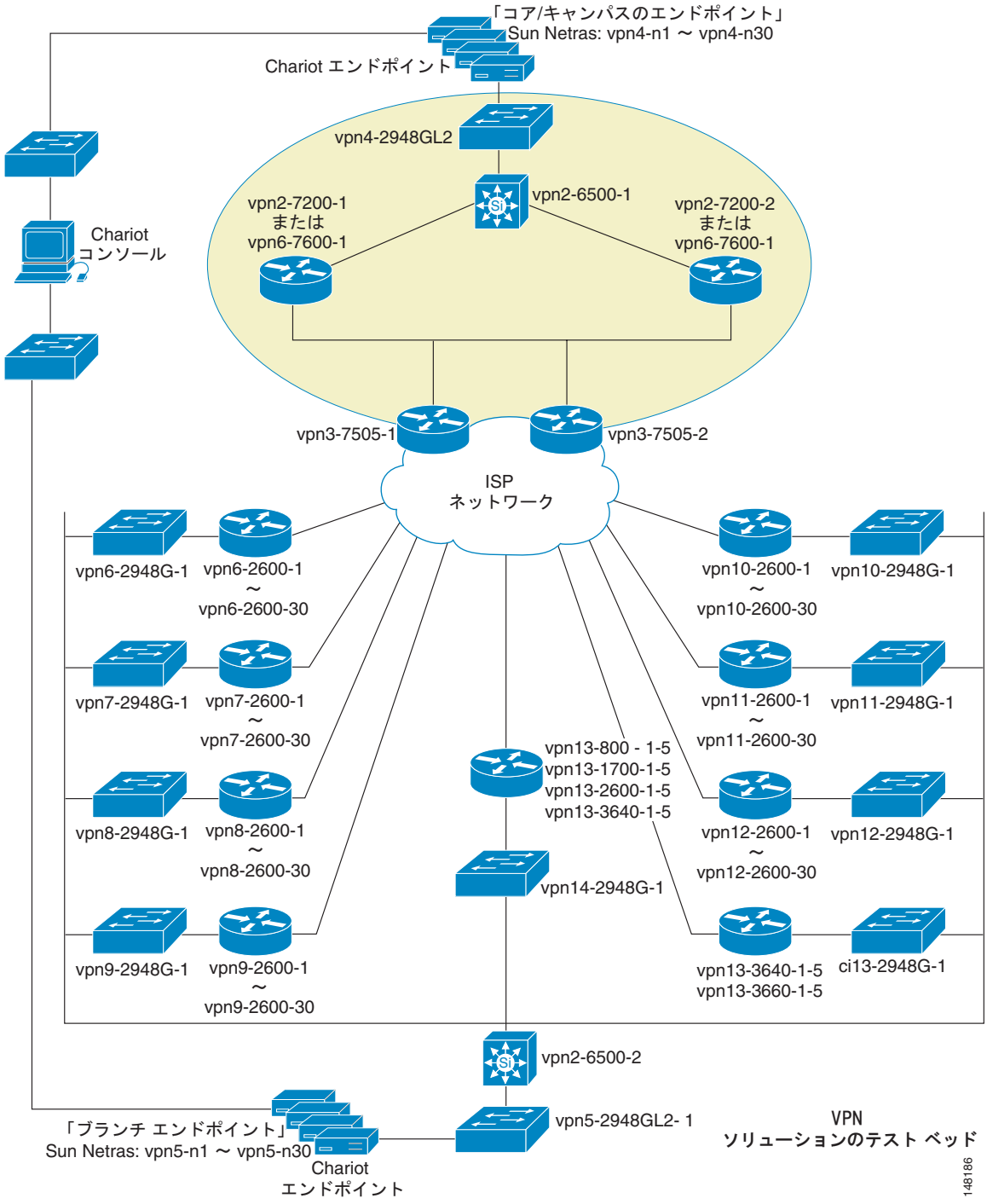
スケーラビリティ テストの結果（ユニキャストのみ）

この章では、シスコによるテストの結果を提示し、DMVPN 構成でのさまざまなプラットフォームのスケーラビリティに関するデザイン ガイダンスを提供します。

（注） IP マルチキャスト（IPmc）の結果は含まれません。

図 4-1 に、スケーラビリティ テスト ベッドのネットワーク ダイアグラムを示します。

図 4-1　DMVPN ハブアンドスポーク モードのテスト ベッド



スケーラビリティ テストの方法

ヘッドエンド スケーラビリティ テスト ベッドは、多くのシスコ ブランチ ルータ（1700、2600、3600、3700、ISR 1800、ISR 2800、および ISR 3800 シリーズを含めた各種）で構成され、さまざまなタイプのヘッドエンドに接続されています。ネットワークを伝送される大半のトラフィックについては、Ixia Chariot テスト ツールを使用してフローが確立されます。トラフィックの構成は、UDP が約 35%、TCP が約 65% です。使用されたアプリケーション タイプには、VoIP、FTP、DNS、HTTP、POP3、および TN3270 が含まれます。平均パケット サイズは、ヘッドエンドからブランチでは 188 バイト、ブランチからヘッドエンドでは 144 バイトです。これらの平均パケット サイズが比較的小さいため、以下に提示されるスケーラビリティのテスト結果は、各種トラフィックが混在したネットワーク デザインの場合でも適用可能です。またテスト結果の数値はかなり控えめな（コンサバティブな）ものとなっています。平均パケット サイズの大きい、データのみのトラフィックを伝送するネットワークは、ここで述べたものより bps パフォーマンスが向上します。ただし、特定の CPU 値の場合の pps パフォーマンスは同一となるはずです。

HTTP Get スクリプトを使用する、Cisco IOS の Cisco IP SLA 機能（以前の SA エージェント [Service Assurance Agent]）によってもトラフィックが生成されます。ブランチ ルータはコア内の HTTP サーバへ HTTP Get コールを発信します。テスト エンドポイントで MTU を 1300 バイトに設定することで、ネットワーク内でフラグメンテーションを発生させることなくテストを実行しました。

次の表に、DMVPN トンネル集約構成でテストを行った結果を示します。特に明記されていないかぎり、テスト中に使用したルーティング プロトコルは EIGRP です。上述の通り、統合データと g.729 VoIP を混在させたトラフィックを使用しました。

DMVPN — ハブアンドスポーク展開モデル

ヘッドエンドのスケーラビリティ テストの結果

表 4-1 に、DMVPN ハブアンドスポーク展開モデル構成でのスケーラビリティ テストの結果を示します。QoS は DMVPN ヘッドエンド ハブ ルータではなく、WAN ルータで有効です。

表 4-1　ヘッドエンドのスケーラビリティ テストの結果 — DMVPN ハブアンドスポーク モデル

プラットフォーム	トンネル数	音声コール数	スループット（kpps）	スループット（Mbps）	CPU%
Cisco 7200VXR NPE-G1 デュアル SA-VAM2	400（1 mGRE）	285	47.5	106.3	80%
	800（2 mGRE）	250	45.2	104.3	82%
VPN サービス アダプタを搭載した Cisco 7200VXR NPE-G2	600（1 mGRE）	600	122	416	75%
RP1 および ESP 10 を備えた Cisco ASR 1004	1000（1 mGRE）	2570	545	1.2 Gbps	該当なし

表 4-1　ヘッドエンドのスケーラビリティ テストの結果 — DMVPN ハブアンドスポーク モデル（続き）

Cisco 7600 Sup720 VPN SPA	1000（2 mGRE）	4137	515.4	1.09 Gbps	該当なし
Cisco 7200VXR/Cisco 7600 デュアル ティア アーキテクチャ	3000 （3 台の Cisco 7200VXR それぞれで 1000 の p2p GRE トンネル、VPN SPA で IPSec トンネル）	約 4000	601（総数） 3 台の 7200VXR のそれぞれで最大 203 Kpps	-	該当なし

（注）　ハードウェアで暗号化が行われ、メイン プロセッサに影響を与えないので、Cisco ASR 1000 および Cisco 7600 については、CPU の数は報告されません。

表 4-2 に、DMVPN ハブアンドスポーク展開モデル構成でのスケーラビリティ テストの結果を示します。QoS は、DMVPN ヘッドエンド ハブ ルータの外部物理インターフェイス（このテストでは GigEthernet）で有効です。シェーパーはブランチごとに設定され、*qos pre-classify* はトンネル インターフェイスで有効です。外部物理インターフェイスのサービス ポリシーによって宛先 IP アドレスの照合が行われます。したがって、各ブランチは内部 LAN ネットワーク アドレスのネットワーク アドレスによって識別されます。シェーピングされたレートは 1.54 Mbps の 85%、または 1,310,000 bps です。

表 4-2　ヘッドエンドのスケーラビリティ テストの結果 — ブランチ単位の QoS が有効の場合の DMVPN ハブアンドスポーク モデル

プラットフォーム 7200VXR NPE G2	IPSec トンネルの数	アクティブ トラフィックのあるトンネル	EMIX トラフィックのあるトンネル	G.729 コールの数	スループット（kpps）	スループット（Mbps）	CPU %
VAM2+	40	25	25	160	26.4	69	74
VSA	40	40	40	280	40	104.6	75

ブランチ オフィスのスケーラビリティ テストの結果

表 4-3 に、DMVPN ハブアンドスポーク展開モデル構成でのテストの結果を示します。集約ヘッドエンドへのトンネルを 1 つ設定しました。Cisco IOS-FW および NAT サービスもテストに組み入れました。

表 4-3　ブランチ オフィスのスケーラビリティ テストの結果 — DMVPN ハブアンドスポーク モデル

プラットフォーム	ハードウェア暗号化	音声コール数	スループット（kpps）	スループット（Mbps）	CPU%
Cisco ISR 3845	オンボード	187	24.0	48.8	81%
	AIM-VPN/HPII-Plus	420	27.1	50.1	80%
Cisco ISR 3825	オンボード	143	18.2	36.6	81%
	AIM-VPN/EPII-Plus	156	20.1	42.8	79%

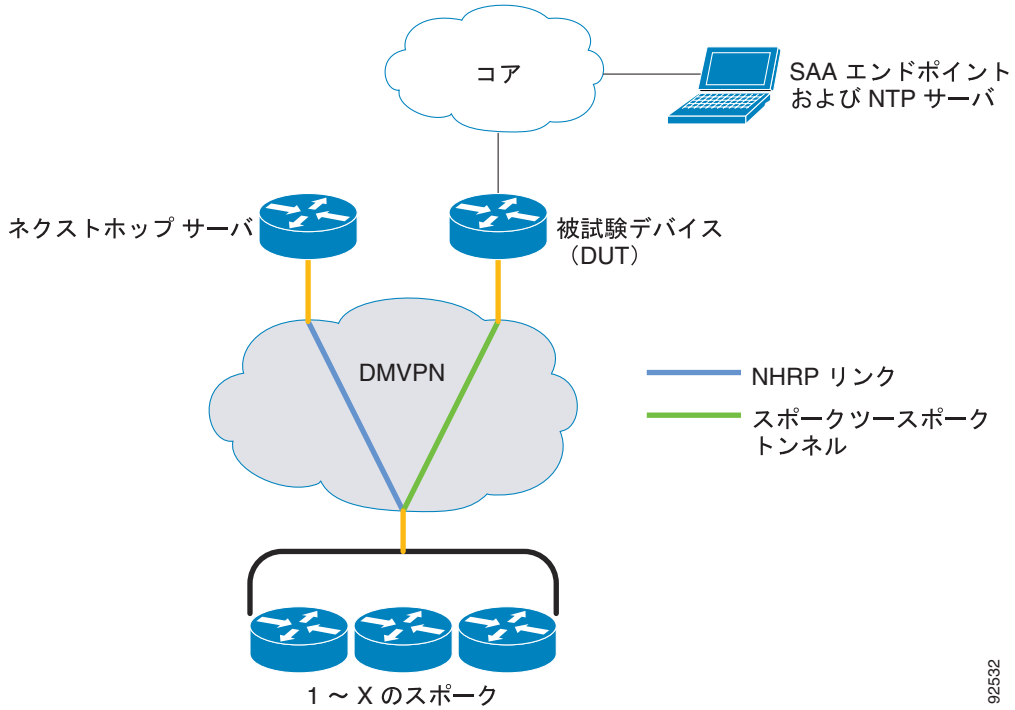
表 4-3　ブランチ オフィスのスケーラビリティ テストの結果 — DMVPN ハブアンドスポーク モデル（続き）

Cisco ISR 2851	オンボード	90	11.4	23.8	79%
	AIM-VPN/EPII-Plus	120	14.9	30.8	80%
Cisco ISR 2821	オンボード	45	6.0	13.6	53%
	AIM-VPN/EPII-Plus	97	12.3	25.9	78%
Cisco ISR 2811	オンボード	19	2.6	5.8	79%
	AIM-VPN/EPII-Plus	27	3.6	8.0	80%
Cisco ISR 2801	オンボード	19	2.6	5.8	83%
	AIM-VPN/EPII-Plus	30	3.9	8.4	79%
Cisco ISR 1841	オンボード	19	2.5	5.7	82%
	AIM-VPN/BPII-Plus	30	3.9	8.8	80%
Cisco 1811W（BVI 未設定）	オンボード	33	7.6	16.0	81%
Cisco 1811W（BVI 設定）	オンボード	60	4.3	9.3	82%
Cisco 871W（BVI 未設定）	オンボード	8	2.0	4.4	85%
Cisco 871W（BVI 設定）	オンボード	15	1.1	2.4	84%

DMVPN — スポークツースポーク展開モデル

図 4-2 に、スポークのスケーラビリティ テスト ベッドを示します。

図 4-2　DMVPN スポークツースポーク テスト ベッド



Cisco 831 ～ ISR 3845 の各ルータがテスト対象で、被試験デバイス（DUT）の位置に順次設置されます。また、「1 ～ X」の数のスポークがテスト ベッドに組み込まれます。これらのルータはそれぞれ、1 つの IPSec SA（またはトンネル）をネクストホップ サーバに対して開きます。これにより、DUT の NBMA アドレスが提供されます。各スポークは DUT に対して、スポークツースポーク トンネルを開きます。Cisco IP SLA および Network Time Protocol（NTP; ネットワーク タイム プロトコル）を通じてトンネルは維持されます。その後、特定数のトンネルでトラフィックを生成し、「安全な最大」数のトンネルを維持した状態で、DUT ルータのパフォーマンスを pps および bps の点で評価します。各スポーク ルータの外部インターフェイス（DUT 以外）は 192 Kbps にシェーピングされ、DUT が集約を行っていることが通知されます（192 Kbps ×トンネル数）。トラフィック プロファイルでは、トンネルごとに 1 つの音声コール（G.729 コーデック）が含まれます。VoIP 品質メトリックはテスト中にトラッキングされます。適切な VoIP 品質がテスト中に維持されない限り、テスト結果は有効になりません（または表示されません）。

スポーク ルータはさまざまなセキュリティ リスクにさらされており（特に、インターネットに接続されている場合）、スポーク サイトは専用のセキュリティ アプライアンスを導入するほど大きくないことが多いため、スポーク ルータでは通常、着信パケットに対して何らかの精査を実行する必要があります。したがって、DMVPN のほかに、次の機能を有効にした状態ですべてのテストを実行します。

- アウトバウンド ファイアウォール検査
- インバウンドおよびアウトバウンド Access Control List（ACL; アクセス コントロール リスト）
- NAT

新しい Cisco ISR プラットフォーム（1841、2801、2811、2821、2851、3825、および 3845）には、暗号化ハードウェアが内蔵されています。暗号化機能を強化するため、暗号化 / 圧縮 AIM カードを購入することもできます。これらのプラットフォームについては、オンボード暗号化カードと AIM を使用したそれぞれの結果が示されます。

表 4-4 に、DMVPN スポークツースポーク展開のテスト結果を示します。

表 4-4　DMVPN スポークツースポーク展開モデル — テスト結果

プラットフォーム	トンネル数	音声コール数	スループット（kpps）	スループット（Mbps）	CPU%
Cisco 871W オンボード（BVI 未設定）	1	15	2.0	4.4	85%
	5	14	1.6	3.8	82%
	9	13	1.9	3.9	85%
Cisco 871W オンボード（BVI 設定）	1	8	1.1	2.4	84%
	5	7	1.0	2.1	84%
	9	6	0.9	1.9	81%
Cisco 1811W オンボード（BVI 未設定）	1	60	7.6	16.0	81%
	25	49	6.8	14.1	80%
	50	44	6.8	13.7	82%
Cisco 1811W オンボード（BVI 設定）	1	33	4.3	9.3	82%
	25	23	3.2	6.9	81%
	50	22	3.4	6.9	81%
Cisco 1841 オンボード	1	19	2.5	5.7	82%
	25	14	2.2	4.7	81%
	50	13	2.1	4.1	79%

表 4-4　DMVPN スポークツースポーク展開モデル — テスト結果（続き）

Cisco 1841 AIM-VPN/BPII-Plus	1	30	4.0	8.8	80%
	25	20	3.1	6.8	79%
	50	20	3.1	6.8	79%
Cisco ISR 2801 オンボード	1	19	2.6	5.8	83%
	25	14	2.2	4.7	83%
	50	13	2.1	4.5	81%
Cisco ISR 2801 AIM-VPN/EPII-Plus	1	30	3.9	8.4	79%
	25	20	3.1	6.8	79%
	50	20	3.1	6.8	81%
Cisco ISR 2811 オンボード	1	19	2.6	5.8	79%
	25	14	2.2	4.8	80%
	50	14	2.2	4.8	83%
Cisco ISR 2811 AIM-VPN/EPII-Plus	1	27	3.6	8.0	80%
	25	18	2.8	6.1	79%
	50	18	2.8	6.1	82%
Cisco ISR 2821 オンボード	1	45	6.0	13.6	53%
	50	50	7.8	17.0	79%
	100	50	7.8	17.0	80%
Cisco ISR 2821 AIM-VPN/EPII-Plus	1	97	12.3	25.9	78%
	100	59	9.2	20.1	80%
	200	55	8.8	18.9	80%
Cisco ISR 2851 オンボード	1	90	11.4	23.8	79%
	55	55	8.5	18.6	81%
	100	54	8.5	18.5	80%
Cisco ISR 2851 AIM-VPN/EPII-Plus	1	120	14.9	30.8	80%
	100	72	11.2	24.5	80%
	200	71	11.2	24.3	87%
Cisco ISR 3825 オンボード	1	143	18.2	36.6	81%
	150	91	14.2	29.0	80%
	300	89	14.2	28.8	80%
Cisco ISR 3825 AIM-VPN/EPII-Plus	1	156	20.1	42.8	79%
	150	108	16.8	35.7	80%
	300	104	16.5	34.8	80%
Cisco ISR 3845 オンボード	1	187	24.0	48.8	81%
	200	118	18.4	37.7	80%
	400	114	18.1	36.7	80%

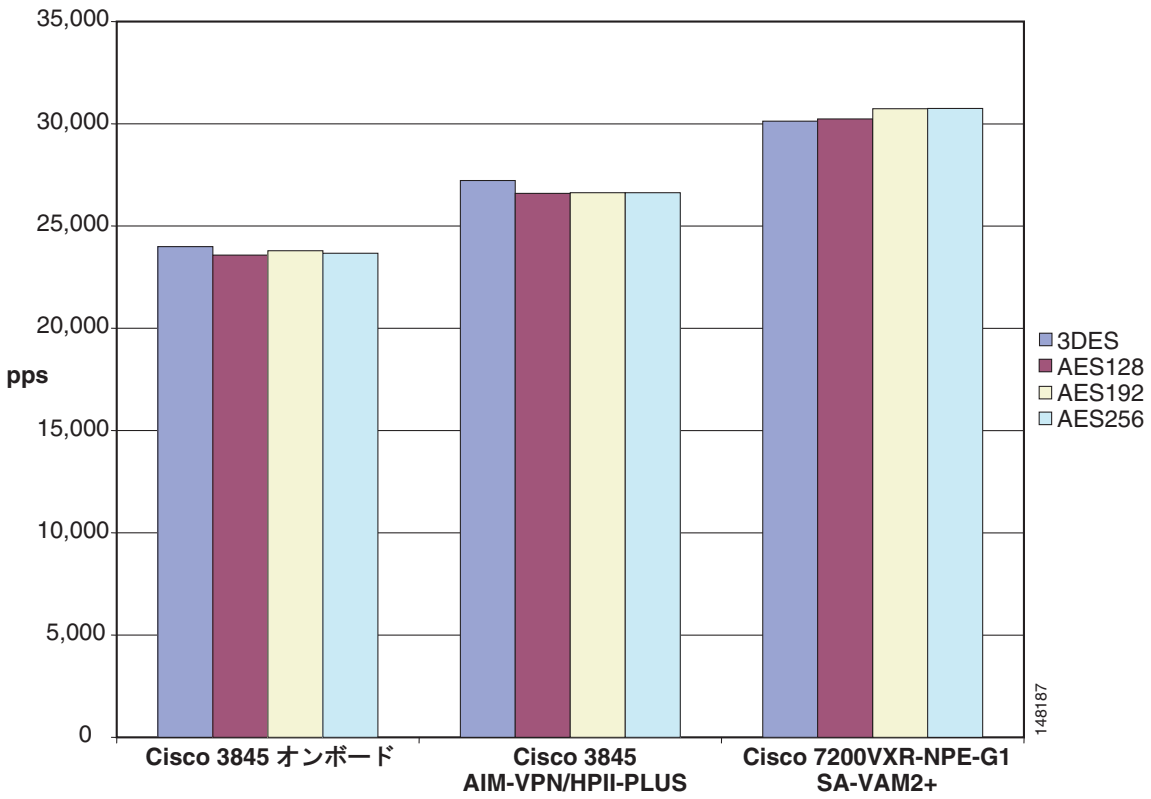
表 4-4　DMVPN スポークツースポーク展開モデル — テスト結果（続き）

Cisco ISR 3845 AIM-VPN/HPII-Plus	1	420	27.1	58.1	80%
	200	280	21.7	46.3	80%
	400	270	21.4	45.2	80%
Cisco 7200VXR NPE-G1 デュアル SA-VAM2	1	480	30.4	63.1	79%
	200	340	26.4	56.2	79%
	400	320	25.2	53.3	80%
Cisco 7301 SA-VAM2	1	240	31.0	66.1	80%
	200	160	24.7	50.1	79%
	400	150	23.6	47.6	79%

AES および 3DES のスケーラビリティ テストの結果

3DES および AES 暗号化は、ここで示すすべての製品で使用できます（ハードウェア アクセラレーション IPSec を含む）。すべてのテストで 3DES と AES 両方が実行されたわけではありません。ただし、パフォーマンスを比較するため、いくつかのスナップショット テストを実行しました。図 4-3 のグラフに示すように、キー長が長い AES の場合でもパフォーマンスの変化はほとんどなく、結果はほぼ同等です。

図 4-3　3DES および AES のパフォーマンスの比較



評価対象のソフトウェア リリース

表 4-5 に示すソフトウェア リリースが、スケーラビリティ テストで使用されました。

表 4-5　評価対象のソフトウェア リリース

シスコ製品ファミリ	ソフトウェア リリース
Cisco ASR 1000	12.2(33)XNA
Cisco 7600	IOS 12.2(18)SXE2
Cisco 6500 VPNSM	IOS 12.2(18)SXE2
Cisco 7200VXR	IOS 12.2(11)T2 IOS 12.3(5)
VPN サービス アダプタを搭載した Cisco 7200VXR NPE-G2	IOS 124-4.XD-0629
Cisco ブランチ オフィス ルータ（17xx、26xx、36xx、37xx）	IOS 12.3(8)T5
Cisco ブランチ オフィス ISR（1841、28xx、38xx）	IOS 12.3(8)T5 IOS 12.3(11)T2
Cisco リモート オフィス ルータ（831、871W、および 1811W）	831 — IOS 12.3(8)T5 871W — IOS 12.3(8)Y1 1811W — IOS 12.3(14)YT1

通常通り、Cisco IOS ソフトウェアを選択する前に、適切な調査を行ってください。また、ルータに設定された他の機能に影響を与えるコード レベルの問題を理解している必要があります。

APPENDIX A

スケーラビリティ テスト ベッドのコンフィギュレーション ファイル

次に、セントラル サイトおよびブランチ サイトの設定を示します。これらの設定は、シスコのスケーラビリティ テストで使用した実際の設定から抽出したもので、参照用としてのみ提供されます。

Cisco 7200VXR/NPE-G1/SA-VAM2 ヘッドエンドの設定

テスト ベッドには 2 つのヘッドエンド デバイスがあり、それぞれ 1 つの mGRE トンネルが設定されています。デュアル ハブ / デュアル DMVPN クラウド デザインであることを想定しています。次の設定は最初のヘッドエンドの抜粋であり、設定全体を示すものではありません。ISAKMP 認証を簡易化するために、ワイルドカード アドレスと事前共有キーをヘッドエンドで使用します。ただし、これは顧客向けには推奨されません。

ヘッドエンド 1：

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
interface Loopback0
 description Loopback0
 ip address 10.57.1.255 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map multicast dynamic
```

```
 ip nhrp network-id 105600
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.251.1 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/2
 description GigabitEthernet0/2
 ip address 10.57.1.1 255.255.255.248
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip route 192.168.0.0 255.255.0.0 192.168.251.2
!
```

Cisco ASR1004 ヘッドエンドの設定

次の設定は、Cisco ASR1004 のものです。ここでは ASR が 1000 の DMVPN ハブアンドスポークトンネルを集約します。

ヘッドエンド 1：

```
boot-start-marker
boot system flash bootflash:asr1000rp1-adventerprisek9.02.01.00.122-33.XNA.bin
boot-end-marker
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
logging buffered 1024000
enable password cisco
!
no aaa new-model
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
no ip ftp passive
ip ftp source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
```

```
no ip domain lookup
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
redundancy
 mode sso
 no policy config-sync bulk prc reload
!
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-aes esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
!
buffers tune automatic
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.248.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 qos pre-classify
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface Loopback0
 ip address 192.168.30.1 255.255.255.255
!
interface GigabitEthernet0/2/0
 description GigabitEthernet0/2/0
 ip address 192.168.32.252 255.255.255.0
 no ip proxy-arp
 load-interval 30
```

```
 negotiation auto
 plim qos input map ip dscp-based
 plim qos input map ip dscp  34  40  queue strict-priority
 no cdp enable
 hold-queue 4096 in
 hold-queue 4096 out
!
!
interface GigabitEthernet0/3/0
 description GigabitEthernet0/3/0
 ip address 10.204.0.1 255.252.0.0
 load-interval 30
 negotiation auto
 plim qos input map ip dscp-based
 plim qos input map ip dscp  34  40  queue strict-priority
 no cdp enable
 service-policy input INGRESS
 service-policy output campus
!
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 172.26.182.168 255.255.252.0
 speed 100
 duplex full
 no negotiation auto
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 passive-interface GigabitEthernet0/2/2
!
router eigrp 100
 network 192.168.32.0
!
ip classless
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 172.26.180.1
!
no ip http server
no ip http secure-server
!
!
snmp-server community public RO
snmp-server community private RW
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
ntp clock-period 17175902
end
```

Cisco 7600/Sup720/VPN SPA ヘッドエンドの設定

次の設定は、Sup720 および VPN SPA を搭載した Cisco 7600 用のものです。ここでは、7600 ルータが 1000 の DMVPN ハブアンドスポーク トンネルを集約します。

ヘッドエンド 1：

```
hostname vpn6-7600-1
!
no aaa new-model
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
ip subnet-zero
ip rcmd rsh-enable
!
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
no scripting tcl init
no scripting tcl encdir
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap-vlan100 10
 set transform-set vpn-test
!
crypto dynamic-map dmap-vlan101 10
 set transform-set vpn-test
!
crypto map dynamic-map-vlan100 local-address Vlan100
crypto map dynamic-map-vlan100 10 ipsec-isakmp dynamic dmap-vlan100
!
crypto map dynamic-map-vlan101 local-address Vlan101
crypto map dynamic-map-vlan101 10 ipsec-isakmp dynamic dmap-vlan101
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
no diagnostic cns publish
no diagnostic cns subscribe
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
```

```
interface Loopback0
 description Loopback0
 ip address 10.57.255.251 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source 192.168.241.1
 tunnel mode gre multipoint
!
interface Tunnel1
 description Tunnel1
 bandwidth 100000
 ip address 10.56.8.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105680
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source 192.168.242.1
 tunnel mode gre multipoint
!
interface GigabitEthernet3/1
 description GigabitEthernet3/1 Outside Interface
 no ip address
 load-interval 30
 crypto connect vlan 100
!
interface GigabitEthernet3/2
 description GigabitEthernet3/2 Outside Interface
 no ip address
 load-interval 30
 crypto connect vlan 101
!
interface GigabitEthernet3/3
 description GigabitEthernet3/3
 no ip address
 load-interval 30
 shutdown
!
interface GigabitEthernet4/0/1
 description GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
```

```
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 description GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/1
 description GigabitEthernet5/1 Inside Interface
 ip address 10.57.1.1 255.255.255.0
 no ip redirects
 load-interval 30
!
interface GigabitEthernet6/2
 description FlashNet
 ip address 172.26.177.251 255.255.252.0
 load-interval 30
 media-type rj45
 speed 100
 duplex full
!
interface Vlan1
 description Vlan1
 no ip address
 load-interval 30
 shutdown
!
interface Vlan100
 description Vlan100
 ip address 192.168.241.1 255.255.255.0
 no ip redirects
 load-interval 30
 no mop enabled
 crypto map dynamic-map-vlan100
 crypto engine subslot 4/0
!
interface Vlan101
 description Vlan101
 ip address 192.168.242.1 255.255.255.0
 no ip redirects
 load-interval 30
 no mop enabled
 crypto map dynamic-map-vlan101
 crypto engine subslot 4/0
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.26.176.1
ip route 10.60.0.254 255.255.255.255 192.168.241.2
ip route 10.60.1.254 255.255.255.255 192.168.241.2
ip route 10.60.2.254 255.255.255.255 192.168.241.2
ip route 10.60.3.254 255.255.255.255 192.168.241.2
```

```
ip route 10.60.4.254 255.255.255.255 192.168.241.2
ip route 10.60.5.254 255.255.255.255 192.168.241.2
ip route 10.60.6.254 255.255.255.255 192.168.241.2
ip route 10.60.7.254 255.255.255.255 192.168.241.2
ip route 10.60.8.254 255.255.255.255 192.168.241.2
ip route 10.60.9.254 255.255.255.255 192.168.241.2
ip route 10.60.10.254 255.255.255.255 192.168.241.2
. . . <テキスト出力は省略> . . .
ip route 10.67.0.254 255.255.255.255 192.168.242.2
ip route 10.67.1.254 255.255.255.255 192.168.242.2
ip route 10.67.2.254 255.255.255.255 192.168.242.2
ip route 10.67.3.254 255.255.255.255 192.168.242.2
ip route 10.67.4.254 255.255.255.255 192.168.242.2
ip route 10.67.5.254 255.255.255.255 192.168.242.2
ip route 10.67.6.254 255.255.255.255 192.168.242.2
ip route 10.67.7.254 255.255.255.255 192.168.242.2
ip route 10.67.8.254 255.255.255.255 192.168.242.2
ip route 10.67.9.254 255.255.255.255 192.168.242.2
ip route 10.67.10.254 255.255.255.255 192.168.242.2
ip route 10.67.11.254 255.255.255.255 192.168.242.2
ip route 10.67.12.254 255.255.255.255 192.168.242.2
ip route 10.67.13.254 255.255.255.255 192.168.242.2
ip route 10.67.14.254 255.255.255.255 192.168.242.2
ip route 10.67.15.254 255.255.255.255 192.168.242.2
ip route 10.67.16.254 255.255.255.255 192.168.242.2
ip route 10.67.17.254 255.255.255.255 192.168.242.2
ip route 10.67.18.254 255.255.255.255 192.168.242.2
ip route 10.67.19.254 255.255.255.255 192.168.242.2
ip route 172.26.0.0 255.255.0.0 172.26.176.1
ip route 192.168.0.0 255.255.0.0 192.168.241.2
ip route 192.168.0.0 255.255.0.0 192.168.242.2
!
no ip http server
!
snmp-server community public RO
snmp-server community private RW
snmp-server system-shutdown
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 password cisco
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
ntp clock-period 17180019
ntp server 172.26.176.1
no cns aaa enable
end
```

Cisco 7200VXR/Cisco 7600 デュアル ティア アーキテクチャ ヘッドエンドの設定

次の設定は、mGRE を終端する Cisco 7200VXR と、大容量 IPSec 暗号化を提供する Sup720 および VPN SPA を搭載した Cisco 7600 用です。

ティア 1（mGRE）

```
hostname vpn2-7200-1
!
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
no aaa new-model
ip subnet-zero
ip rcmd rsh-enable
!
ip cef
no ip domain lookup
!
ip multicast-routing
ip ips po max-events 100
no ftp-server write-enable
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
 load-interval 30
 tunnel source 192.168.161.1
 tunnel mode gre multipoint
 tunnel key 105600
!
interface Tunnel1
 description Tunnel1
 bandwidth 100000
 ip address 10.56.16.1 255.255.252.0
 no ip redirects
 ip hold-time eigrp 1 35
 no ip next-hop-self eigrp 1
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 1056160
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 no ip split-horizon eigrp 1
```

```
 load-interval 30
 tunnel source 192.168.181.1
 tunnel mode gre multipoint
 tunnel key 1056160
!
interface Loopback0
 description Loopback0
 ip address 10.57.255.251 255.255.255.255
!
interface FastEthernet0/0
 description FlashNet
 ip address 172.26.176.14 255.255.252.0
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet0/1
 description FastEthernet0/1
 no ip address
 load-interval 30
 shutdown
 duplex full
 speed 100
!
interface GigabitEthernet0/1
 description GigabitEthernet0/1
 ip address 192.168.181.1 255.255.255.0 secondary
 ip address 192.168.161.1 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/2
 description GigabitEthernet0/2
 ip address 10.57.1.1 255.255.255.0
 ip pim sparse-mode
 load-interval 30
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
interface GigabitEthernet0/3
 description GigabitEthernet0/3
 no ip address
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.26.176.1
ip route 172.26.0.0 255.255.0.0 172.26.176.1
ip route 192.168.0.0 255.255.0.0 192.168.161.2
ip route 192.168.0.0 255.255.0.0 192.168.181.2
!
```

```
ip http server
no ip http secure-server
!
ip pim autorp listener
!
snmp-server community public RO
snmp-server community private RW
snmp-server system-shutdown
snmp-server enable traps tty
!
control-plane
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 password cisco
 login
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 password cisco
 login
 transport preferred all
 transport input all
 transport output all
!
ntp clock-period 17180034
ntp server 172.26.176.1
!
end
```

ティア 2（IPsec）

```
hostname vpn6-7600-1
!
no aaa new-model
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
ip subnet-zero
ip rcmd rsh-enable
!
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
```

```
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
no scripting tcl init
no scripting tcl encdir
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
!
crypto map dynamic-map local-address Vlan100
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
no diagnostic cns publish
no diagnostic cns subscribe
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
interface GigabitEthernet3/1
 description GigabitEthernet3/1 Outside Interface
 no ip address
 load-interval 30
 crypto connect vlan 100
!
interface GigabitEthernet3/2
 description GigabitEthernet3/2
 no ip address
 load-interval 30
 shutdown
!
interface GigabitEthernet4/0/1
 description GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 load-interval 30
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
```

```
interface GigabitEthernet4/0/2
 description GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 load-interval 30
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/1
 description GigabitEthernet5/1 to vpn2-7200-1 GE0/1
 ip address 192.168.181.2 255.255.255.0 secondary
 ip address 192.168.161.2 255.255.255.0
 no ip redirects
 load-interval 30
!
interface GigabitEthernet5/2
 description GigabitEthernet5/2 to vpn2-7200-2 GE0/1
 ip address 192.168.191.2 255.255.255.0 secondary
 ip address 192.168.171.2 255.255.255.0
 no ip redirects
 load-interval 30
!
interface GigabitEthernet5/3
 description GigabitEthernet5/3
 no ip address
 load-interval 30
 shutdown
!
interface GigabitEthernet6/2
 description FlashNet
 ip address 172.26.177.251 255.255.252.0
 load-interval 30
 media-type rj45
 speed 100
 duplex full
!
interface Vlan1
 description Vlan1
 no ip address
 load-interval 30
 shutdown
!
interface Vlan100
 description Vlan100
 ip address 192.168.241.1 255.255.255.0
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 4/0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.26.176.1
ip route 172.26.0.0 255.255.0.0 172.26.176.1
ip route 192.168.0.0 255.255.0.0 192.168.241.2
!
no ip http server
!
snmp-server community public RO
snmp-server community private RW
```

```
snmp-server system-shutdown
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 password cisco
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
ntp clock-period 17180035
ntp server 172.26.176.1
no cns aaa enable
end
```

Cisco ISR ブランチ オフィスの設定

次に、1 つのブランチ サイト ルータに関連する設定を示します。2 つのトンネルを使用して（ヘッドエンドごとに 1 つ）、デュアル ハブ / デュアル DMVPN クラウド デザインを採用しています。EIGRP 遅延メトリックを使用して、Tunnel0 を優先パスにします。次の設定では、物理（外部）インターフェイスに適用された VoIP フロー用 QoS（シェーピングおよびキューイング）、集約経路の推奨用途、および EIGRP スタブ設定を示します。

ブランチ 1：

```
ip cef
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.251.1
crypto isakmp key bigsecret address 192.168.252.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
class-map match-all VOICE
  match ip dscp ef
 class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
 class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
 class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
 policy-map 192kb
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
```

```
  class TRANSACTIONAL-DATA
   bandwidth percent 22
   queue-limit 16
  class VOICE
   priority 64
  class class-default
   fair-queue
   queue-limit 6
 policy-map 192kb-shaper
  class class-default
   shape average 182400 1824 0
   service-policy 192kb
!
interface Loopback0
 description Loopback0
 ip address 10.61.138.254 255.255.255.255
!
interface Tunnel0
 description Tunnel0
 bandwidth 192
 ip address 10.56.3.10 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.0.1 192.168.251.1
 ip nhrp map multicast 192.168.251.1
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 ip nhrp nhs 10.56.0.1
 ip summary-address eigrp 1 10.61.148.0 255.255.255.0 5
 qos pre-classify
 tunnel source 192.168.100.6
 tunnel destination 192.168.251.1
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface Tunnel1
 description Tunnel1
 bandwidth 192
 ip address 10.56.7.10 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.4.1 192.168.252.1
 ip nhrp map multicast 192.168.252.1
 ip nhrp network-id 105640
 ip nhrp holdtime 300
 ip nhrp nhs 10.56.4.1
 ip summary-address eigrp 1 10.61.148.0 255.255.255.0 5
 delay 60000
 qos pre-classify
 tunnel source 192.168.100.6
 tunnel destination 192.168.252.1
 tunnel key 105640
 tunnel protection ipsec profile vpn-dmvpn
!
interface Serial0/0
 description Serial0/0
 bandwidth 192
 ip address 192.168.100.6 255.255.255.252
 service-policy output 192kb-shaper
!
interface FastEthernet0/1
 description FastEthernet0/1
 ip address 10.61.148.129 255.255.255.192 secondary
 ip address 10.61.148.1 255.255.255.128
```

```
 speed 100
 full-duplex
!
router eigrp 1
 network 10.0.0.0
 no auto-summary
 eigrp stub connected summary
!
ip route 0.0.0.0 0.0.0.0 192.168.100.5!
ip access-list extended IKE
 permit udp any any eq isakmp
!
```

APPENDIX B

レガシー製品のテスト結果

この章では、レガシー製品のスケーラビリティ テスト結果について説明します。

使用する暗号化強度は 3DES です。Cisco IOS バージョンは特に明記されていない限り、すべてのスポーク デバイスで 12.3(8)T5 です。NHRP 処理ハブ ルータでは 12.3(8)T4 です。各デバイスの性能曲線を割り出すために、3 または 4 段階の CPU 使用率（およそ 50%、60% など）で分析されています。すべてのデバイスは、ハードウェア暗号化モジュール、Cisco IOS-FW、NAT を有効にしてテストされています（表 B-1 を参照）。

表 B-1　　レガシー製品のスケーラビリティ テストの結果

プラットフォーム	トンネル数	スループット（kpps）	スループット（Mbps）	CPU %
Cisco 831	1	0.48	1.1	75%
オンボード	5	0.47	1.0	74%
	10	0.47	1.0	75%
Cisco 1711	1	0.9	2.1	81%
オンボード	12	0.8	1.7	82%
	25	0.8	1.7	84%
Cisco 1760	1	1.0	2.0	81%
MOD1700-VPN	12	0.9	1.8	83%
	25	0.9	1.8	85%
Cisco 2651XM	1	1.3	3.0	85%
AIM-VPN/BPII	12	1.1	2.4	78%
	25	1.1	2.4	79%
Cisco 2691	1	5.1	11.4	82%
AIM-VPN/EPII	50	4.5	9.9	82%
	100	4.4	9.7	81%
Cisco 3725	1	6.9	15.5	81%
AIM-VPN/BPII	62	6.1	13.3	80%
	125	5.9	12.8	80%

表 B-1　レガシー製品のスケーラビリティ テストの結果（続き）

Cisco 3745 AIM-VPN/HPII	1	13.4	28.8	82%
	100	11.6	25.4	79%
	200	11.2	24.1	81%

APPENDIX C

略語

用語	定義
3DES	Triple Data Encryption Standard：トリプル データ暗号規格
ACL	Access Control List：アクセス コントロール リスト
AES	Advanced Encryption Standard：高度暗号化規格
AH	Authentication Header：認証ヘッダー
AIM	Advanced Integration Module
ATM	Asynchronous Transfer Mode：非同期転送モード
CA	Certificate Authority：認証局
CAC	Call Admission Control：コール アドミッション コントロール
CBWFQ	Class-Based Weighted Fair Queuing：クラスベース WFQ
CEF	Cisco Express Forwarding：シスコ エクスプレス フォワーディング
CPE	Customer Premises Equipment：宅内装置
cRTP	compressed Real-Time Protocol
DES	Data Encryption Standard：データ暗号規格
DHCP	Dynamic Host Configuration Protocol
DLSw	Data Link Switching：データ リンク スイッチング
DMVPN	Dynamic Multipoint Virtual Private Network : ダイナミック マルチポイント VPN
DMZ	De-Militarized Zone：非武装地帯
DNS	Domain Name Service：ドメイン ネーム サービス
DPD	Dead Peer Detection
DSL	Digital Subscriber Line：デジタル加入者線
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Protocol：カプセル化セキュリティ プロトコル
FIFO	First In First Out：ファーストイン ファーストアウト
FQDN	Fully Qualified Domain Name：完全修飾ドメイン名
FR	Frame Relay：フレームリレー

FRTS	Frame Relay Traffic Shaping：フレームリレー トラフィック シェーピング
FTP	File Transfer Protocol：ファイル転送プロトコル
GRE	Generic Routing Encapsulation
HSRP	Hot Standby Router Protocol：ホットスタンバイ ルータ プロトコル
ICMP	Internet Control Message Protocol：インターネット制御メッセージ プロトコル
IKE	Internet Key Exchange：インターネット キー エクスチェンジ
IOS	Internetwork Operating System
IP	Internet Protocol：インターネット プロトコル
IPmc	IP multicast：IP マルチキャスト
IPSec	IP Security：IP セキュリティ
IP GRE	GRE を参照
ISP	Internet Service Provider：インターネット サービス プロバイダー
LFI	Link Fragmentation and Interleaving：リンクフラグメンテーション / インターリーブ
LLQ	Low Latency Queuing：ローレイテンシー キューイング
L2TP	Layer 2 Tunneling Protocol：レイヤ 2 トンネリング プロトコル
MDRR	Modified Deficit Round Robin
mGRE	multipoint Generic Route Encapsulation：マルチポイント GRE
MLPPP	Multi-Link Point to Point Protocol：マルチリンク PPP
MPLS	Multi-Protocol Label Switching : マルチプロトコル ラベル スイッチング
MTU	Maximum Transmission Unit：最大伝送ユニット
NAT	Network Address Translation：ネットワーク アドレス変換
NetFlow	Cisco IOS のコンポーネントで、トラフィック統計情報を収集およびエクスポート
NHRP	Next Hop Resolution Protocol
NHS	Next-Hop Server：ネクストホップ サーバ
ODR	On-Demand Routing：オンデマンド ルーティング
OSPF	Open Shortest Path First
p2p GRE	point-to-point GRE：ポイントツーポイント GRE
PAT	Port Address Translation：ポート アドレス変換
PBR	Policy-Based Routing：ポリシーベース ルーティング
PE	Premises Equipment
PPTP	Point-to-Point Tunneling Protocol：ポイントツーポイント トンネリング プロトコル
PVC	Permanent Virtual Circuit：相手先固定接続
QoS	Quality of Service

RADIUS	Remote Authentication Dial In User System
RTP	Real-Time Protocol
SA	Security Association：セキュリティ アソシエーション
SAA	Service Assurance Agent：サービス保証エージェント
SHA-1	Secure Hash Algorithm One
SLA	Service Level Agreement：サービス レベル契約
SNMP	Simple Network Management Protocol：簡易ネットワーク管理プロトコル
SOHO	Small Office/Home Office：スモール オフィス、ホームオフィス
SPA	Shared Port Adapter：共有ポート アダプタ
SRST	Survivable Remote Site Telephony
TCP	Transmission Control Protocol
TED	Tunnel Endpoint Discovery：トンネル エンドポイント検出
ToS	Type of Service：タイプ オブ サービス
UDP	User Datagram Protocol：ユーザ データグラム プロトコル
VAD	Voice Activity Detection：音声アクティビティ検出
VoIP	Voice over IP
V^3PN	Voice and Video Enabled IPSec VPN
VAM	VPN Acceleration Module：VPN アクセラレーション モジュール
VPN	Virtual Private Network：バーチャル プライベート ネットワーク
VPNSM	VPN Service Module：VPN サービス モジュール
VPN SPA	VPN Shared Port Adapter：VPN 共有ポート アダプタ
WAN	Wide Area Network：ワイドエリア ネットワーク
WRED	Weighted Random Early Detection