IBA

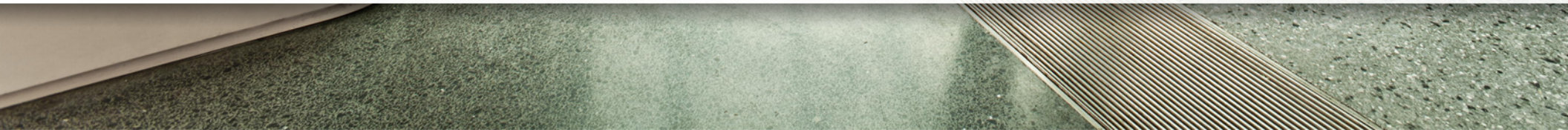
无边界网络

部署指南

VPN广域网部署指南

智能业务平台IBA

2012年8月系列



前言

本指南的目标受众

Cisco®智能业务平台(IBA)指南主要面向承担以下职务的读者:

- 需要用标准程序来实施方案时的系统工程师
- 需要撰写思科IBA实施项目工作说明书的项目经理
- 需要销售新技术或撰写实施文档的销售合作伙伴
- 需要课堂讲授或在职培训材料的培训人员

一般来说,您也可以将思科IBA指南作为增加工程师和项目实施统一性的指导文件,或利用它更好地规划项目成本预算和项目工作范围。

版本系列

思科将定期对IBA指南进行更新和修订。在开发新的思科IBA指南系列时,我们将会对 其进行整体评测。为确保思科IBA指南中各个设计之间的兼容性,您应当使用同一系列 中的设计指南文档。

每一个系列的Release Notes (版本说明) 提供了增加和更改内容的总结。

所有思科IBA指南的封面和每页的左下角均标有指南系列的名称。我们以某系列指南发 布时的年份和月份来对该系列命名,如下所示:

年 月 系列

例如,我们把于2011年8月发布的系列指南命名为:
"2012年8月系列"

您可以在以下网址查看最新的IBA指南系列:

http://www.cisco.com/go/cn/iba

如何阅读命令

许多思科IBA指南详细说明了思科网络设备的配置步骤,这些设备运行着Cisco IOS、 Cisco NX-OS或其他需要通过命令行界面(CLI)进行配置的操作系统。下面描述了系 统命令的指定规则,您需要按照这些规则来输入命令:

在CLI中输入的命令如下所示:

```
configure terminal
```

为某个变量指定一个值的命令如下所示:

```
ntp server 10.10.48.17
```

包含您必须定义的变量的命令如下所示:

```
class-map [highest class name]
```

以交互示例形式显示的命令(如脚本和包含提示的命令)如下所示:

```
Router# enable
```

包含自动换行的长命令以下划线表示。应将其作为一个命令进行输入:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

系统输出或设备配置文件中值得注意的部分以高亮方式显示,如下所示:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

问题和评论

如果您需要评论一个指南或者提出问题, 请使用 IBA反馈表。

如果您希望在出现新评论时获得通知,我们可以发送RSS信息。

目录

本IBA指南的内容

关于IBA无边界网络

思科IBA能帮助您设计和快速部署一个全服务企业网络。IBA系统是一种规范式设计，即购即用，而且具备出色的可扩展性和灵活性。

思科IBA在一个综合的解决方案中集成了局域网、广域网、无线、安全、数据中心、应用优化和统一通信技术，并对其进行了严格测试，确保能实现无缝协作。IBA采用的模块化分类简化了多技术系统集成的复杂度，使您能够根据需要解决企业需求，而无需担心技术复杂性。

思科IBA无边界网络是一个稳固的网络基础架构，为拥有250至10,000名用户的企业网络设计。IBA无边界网络架构集成了有线和无线局域网接入、广域网连接、广域网应用加速以及互联网边缘的安全架构。

成功部署路线图

为确保您能够按照本指南中的设计成功完成部署，您应当阅读本指南所依据的所有相关指南——即如下路线中本指南之前的所有指南。

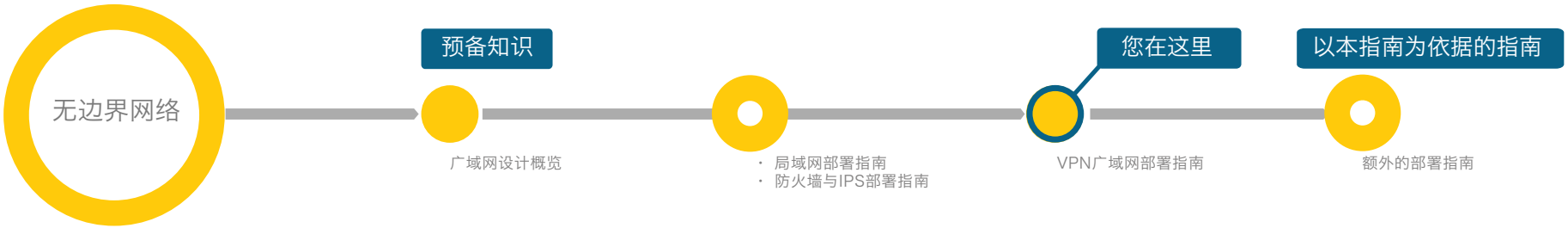
关于本指南

本部署指南包括一个或多个部署章节，其中包含如下内容：

- **业务概述**——描述本设计的商业用例，业务决策者可通过本章内容来了解解决方案与企业运营的相关性。
- **技术概述**——描述该商业用例的技术设计，包含思科产品如何应对业务挑战。技术决策者可利用本章节理解该设计如何实现。
- **部署详情**——提供解决方案的逐步实施和配置的指导。系统工程师可以在这些步骤的指导下快速和可靠的设计和部署网络。

您可以在以下网址查看最新的IBA指南系列：

http://www.cisco.com/go/cn/iba



简介

思科IBA智能业务平台—无边界网络是一个稳固的网络基础架构，为拥有至10,000名互联用户的网络带来了出色的灵活性，无需重新设计网络，即可支持新用户或新的网络服务。我们撰写了一份详细全面并可直接使用的部署指南，它以最佳实践设计原则为基础，并提供了灵活性和可扩展性。

所有的广域网架构在《广域网设计概览》中进行了介绍。

为帮助重点了解该架构的具体组成部分，我们提供了三个广域网部署指南：

- 《VPN广域网部署指南》为主用/备用宽带或互联网传输提供了配置和指导。
- 《MPLS广域网部署指南》为多协议标签交换（MPLS）传输提供了灵活的指导和配置。
- 《二层广域网部署指南》为VPLS或城域以太网传输提供了指导和配置。

相关内容

《局域网部署指南》介绍了有线网络接入，旨在为较大规模的园区级局域网和较小的远端站点局域网提供无所不在的联网功能。此外，为提供强大的通信环境，该指南还包括了永续性、安全性和可扩展性方面的内容。服务质量（QoS）也集成在本指南中，以确保基础架构能够支持大量应用，包括在单一网络上与数据应用共存的、对丢弃敏感的低延迟多媒体应用。

《防火墙和IPS部署指南》重点介绍防火墙和入侵防御系统等安全服务，以保护您企业的互联网网关。互联网服务提供商连接和路由方案，与服务器负载均衡相结合，为设计提供了永续性。

设计目标

本架构以收集自客户、合作伙伴及思科现场人员的需求为基础，旨在服务于联网用户数至10000之间的企业。在设计架构时，我们考虑了收集到的需求和以下设计目标。

易于部署、灵活性和可扩展性

拥有至10000名用户的企业通常在多个不同地点设有业务运营机构，这使得灵活性和可扩展性成为其网络的关键要求。在此设计中，我们采用了几种方法来创建和维护一个可扩展的网络。

- 通过为网络常用部分保持少量标准设计，支持人员能够更高效地实施、支持这些网络并为其设计服务。
- 我们采用了模块化设计方法来增强可扩展性。从一系列标准的全局构建模块开始，我们能够组建一个满足需求的可扩展网络。
- 对于多个服务区域来说，许多插件模块看上去是相同的，这样提供了一致性和可扩展性，从而可使用相同的支持方法来维持多个网络区域☒£这些模块遵循标准的核心层－分布层－接入层网络设计方法，并进行了分层，以确保正确定义插件间的接口。

永续性和安全性

保持高可用性网络的要点之一就是建立适当的冗余性，以防御网络中的故障。我们的架构精心平衡了冗余性和冗余系统复杂性这两个因素。

随着语音和视频会议等对延迟和丢包敏感的流量大量出现，我们还将恢复时间作为了一个重要考虑因素。选择能够缩短从发现故障到恢复正常所需时间的设计，对于确保网络在发生某个较小的组件故障时仍然可用非常关键。

网络安全性也是本架构的一个重要组成部分。在大型网络中有许多入口点，我们要确保它们尽可能安全，同时不会对网络易用性造成较大影响。保护网络不仅能防止网络受到攻击，而且对于实现网络级永续性也至关重要。

易于管理

虽然本指南的重点是网络基础架构的部署，但本设计方案也考虑到了下一个阶段，即管理和运行。部署指南中的配置既允许通过SSH和HTTPS等普通的设备管理连接进行设备管理，也允许经由NMS管理设备。本指南中不包括NMS的配置。

支持先进技术

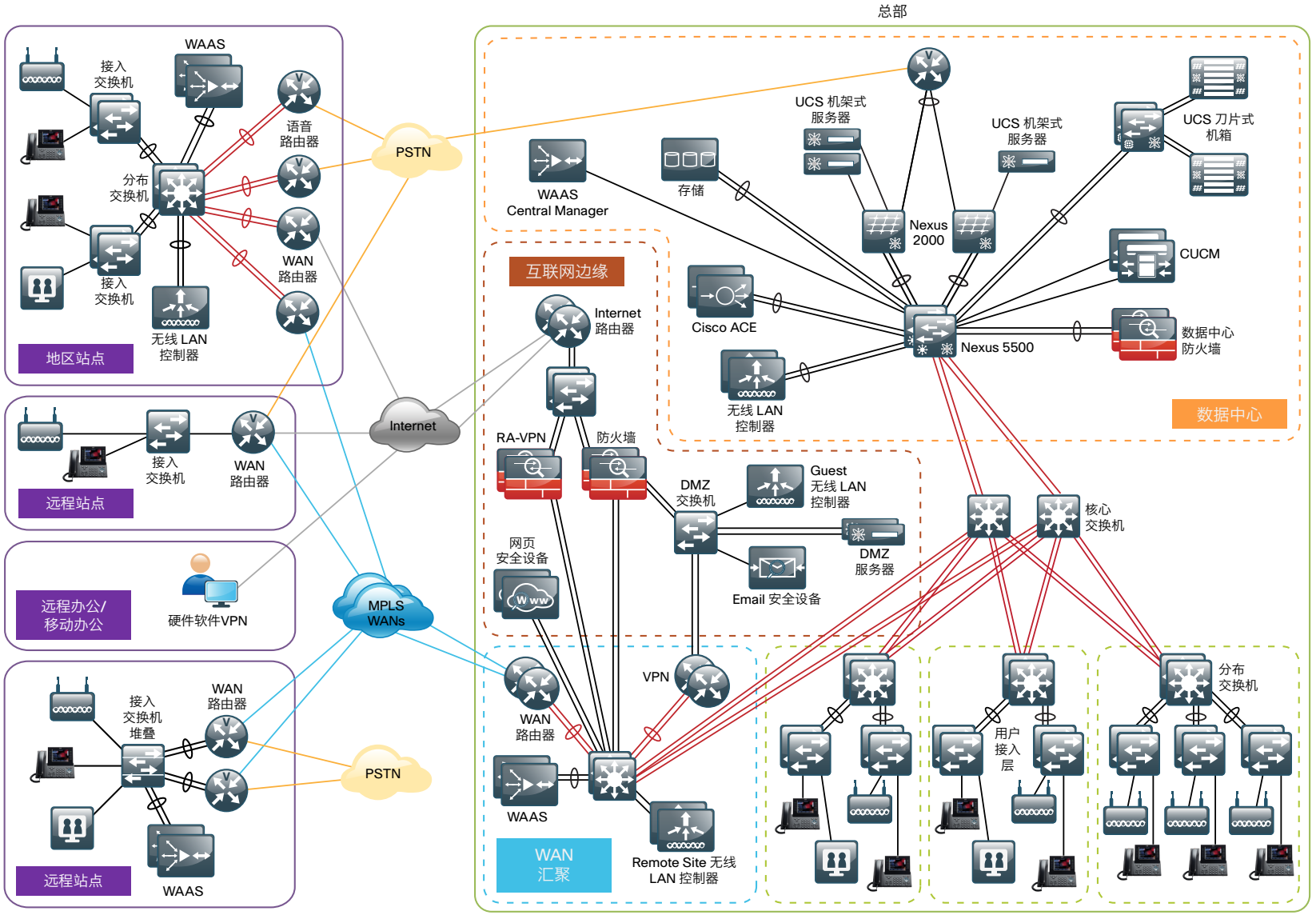
灵活性、可扩展性、永续性和安全性都是可以支持未来先进技术的网络特性。本架构的模块化设计意味着，当企业作好了部署准备时，就能随时添加这些先进技术。此外，因为本架构中的产品和配置从部署之初就能够随时支持协作，所以协作等先进技术的部署得以简化。例如：

- 接入交换机为电话部署提供了以太网供电（PoE），无需本地电源插座。
- 整个网络预先配置了支持高质量语音的QoS。
- 为支持高效的语音和广播视频交付，在网络中配置了组播。

- 为利用无线局域网发送语音的设备预配置了无线网络，可通过802.11 Wi-Fi（即支持移动办公的技术）在所有地点提供IP语音服务

互联网边缘已准备就绪，能够提供基于VPN的软电话，以及传统的硬电话或桌面电话。

图 1 - 面向企业网组织机构的无边界网络概览



架构概述

思科IBA智能业务平台—《无边界网络VPN广域网部署指南》为多个远端站点局域网提供了一个支持高度可用、安全和优化的连接的设计。

广域网是网络基础设施，在相距甚远的远端站点之间提供了IP互联。

本文介绍了如何部署网络基础架构和服务，以支持：

- 为至500个远端站点提供VPN广域网连接
- 部署主要和辅助链路，提供冗余拓扑选项以实现永续性
- 通过加密保护数据私密性
- 为所有远端站点提供有线局域网接入

广域网设计

这一设计主要侧重于为主用和备用链路支持使用以下常用的广域网传输方法：

- Internet VPN（主用）
- Internet VPN（备用）

在较高级别，广域网是一个IP网络，该传输方法可轻松集成到设计之中。所选择的架构会指定一个主要的广域网汇聚站点，类似于传统星型设计中的中枢站点。该站点直接连接到特定电信运营商的广域网传输连接和高速连接。此外，该站点还可以利用网络设备扩展能力来提供卓越性能与冗余能力。主要的广域网汇聚站点与数据中心、以及主要的园区或局域网共存。

本指南同样覆盖了Internet VPN传输的使用方法，为MPLS广域网提供一个冗余的拓扑选项。它包括：配置在《MPLS广域网部署指南》或配置在《二层广域网部署指南》的二层广域网永续性。

使用互联网作为广域网传输方式

互联网从本质上而言就是一个由多个互连的电信运营商组成的大型公共广域网。互联网能够在不同位置之间提供可靠的高性能连接，但无法为这些连接提供明确的保证。互联网采用的是“尽力而为（best effort）”方案。在无法使用主要传输方法进行连接的情况下，互联网不失为一种明智的选择。通过使用互联网作为交替传输方法提供额外的永续性。

互联网连接通常在有关互联网边缘、尤其是主要站点的讨论中进行介绍。远端站点路由器通常也具备互联网连接，但无法基于互联网提供同样范围的服务。出于安全和其他原因的考虑，远端站点的互联网接入往往通过主要站点进行路由。

广域网可使用互联网提供VPN站点间连接，作为主用广域网传输和备用广域网传输方案（到主用VPN站点到站点连接）。

动态多点VPN

动态多点VPN（DMVPN）为构建可扩展的站点间VPN提供了一种出色的解决方案，能够支持多种应用。DMVPN常被用于支持基于公共或私有IP网络的加密站点间连接，并可部署在本部署指南中介绍的所有广域网路由器之上。

DMVPN支持按需全网状连接，并可使用简单的星型配置和零接触中枢部署模式来添加远端站点，由此成为了理想的互联网传输加密解决方案。此外，DMVPN还可支持拥有动态分配的IP地址的分支路由器。

DMVPN使用多点通用路由封装（mGRE）隧道来互连中枢路由器和所有分支路由器。在这种情形下这些mGRE隧道有时也被称作DMVPN云。这一技术组合支持单播、组播和广播IP，并支持在隧道中运行路由协议。

以太网广域网

上文提及的广域网传输方法使用以太网作为标准介质类型。以太网正在成为许多市场中主要的运营商传输方法，因此在测试架构中将以太网作为主要介质非常必要。然而，虽然未明确指出，本指南中的许多内容同样也适用于非以太网介质，如T1/E1、DS-3和OC-3等。

广域网汇聚设计

广域网汇聚（中枢）设计包含两种场景，分别是一个或两个广域网边缘路由器。当广域网边缘路由器用于连接到运营商或服务提供商时，它们通常被称作客户边缘（CE）路由器。结束VPN流量的广域网边缘路由器被称作VPN中枢（hub）路由器。所有广域网边缘路由器均连接到分布层。

当主用传输是MPLS VPN、二层广域网或互联网时，广域网传输方法包括使用传输或备用传输作为传统的互联网访问。该文档仅包括互联网传输的使用方法。单一或双承载互联网访问链路分别连接到VPN 中心路由器节点或VPN中枢路由器组。我们可为它们使用相似的连接和配置方法。

本部署指南介绍了多点广域网汇聚设计模型。只有DMVPN设计模型使用Internet VPN作为传输。双DMVPN设计模型使Internet VPN，使用两个互联

网服务提供商作为主用和备用传输。另外，DMVPN备用设计模型使用Internet VPN作为备用，连接到现存的主用MPLS广域网或二层广域网传输。

主用设计与DMVPN备用设计不同，主要区别在于：其VPN中枢路由器是否部署在现存的MPLS CE路由器上，它将归类到DMVPN备份共享中讨论；或VPN中枢是否部署在专用的VPN中枢路由器上，它将归类到DMVPN专用备份中讨论。

每个设计模型展示了局域网到盒式核心/分布层或专用的广域网分布层的连接。从广域网汇聚观点来看，这两种方法在功能上没有区别。

在所有的广域网汇聚设计中，诸如IP路由汇总等任务在分布层执行。网络中还有其他多种支持广域网边缘服务的设备，这些设备也应连接到分布层。

下表对不同设计模式进行了对比。

表 1 - 只使用VPN传输的设计模型

模型	远端站点	广域网链路	DMVPN中枢	传输1	传输2
单DMVPN	至100	单	单	Internet VPN	
双DMVPN	至 500	双	双	Internet VPN	Internet VPN

表 2 - 使用VPN传输作为备份的设计模型

模型	远端站点	广域网链路	DMVPN中枢	传输1（现存）	传输2（现存）	传输3（现存）	备份传输
DMVPN备份共享	至100	双	单（与MPLS CE共享）	MPLS VPN A			Internet VPN
DMVPN备份专用	至 500	多重	单	MPLS VPN A	MPLS VPN B	城域以太/VPLS	Internet VPN

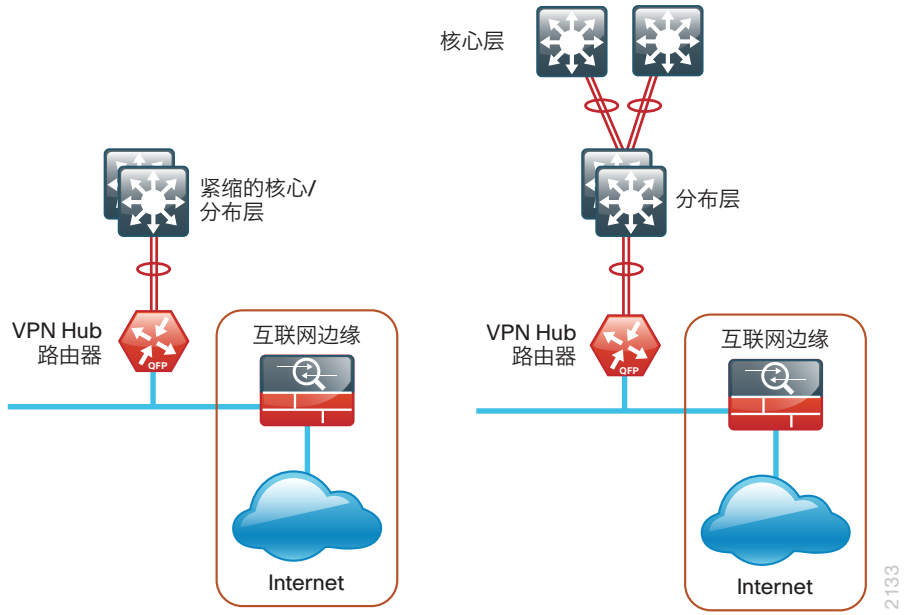
每一种设计的特征如下：

单DMVPN设计模型

- 支持至100远端站点
- 使用单个互联网链路

单DMVPN的设计如下图所示。

图 2 - 单DMVPN设计模型

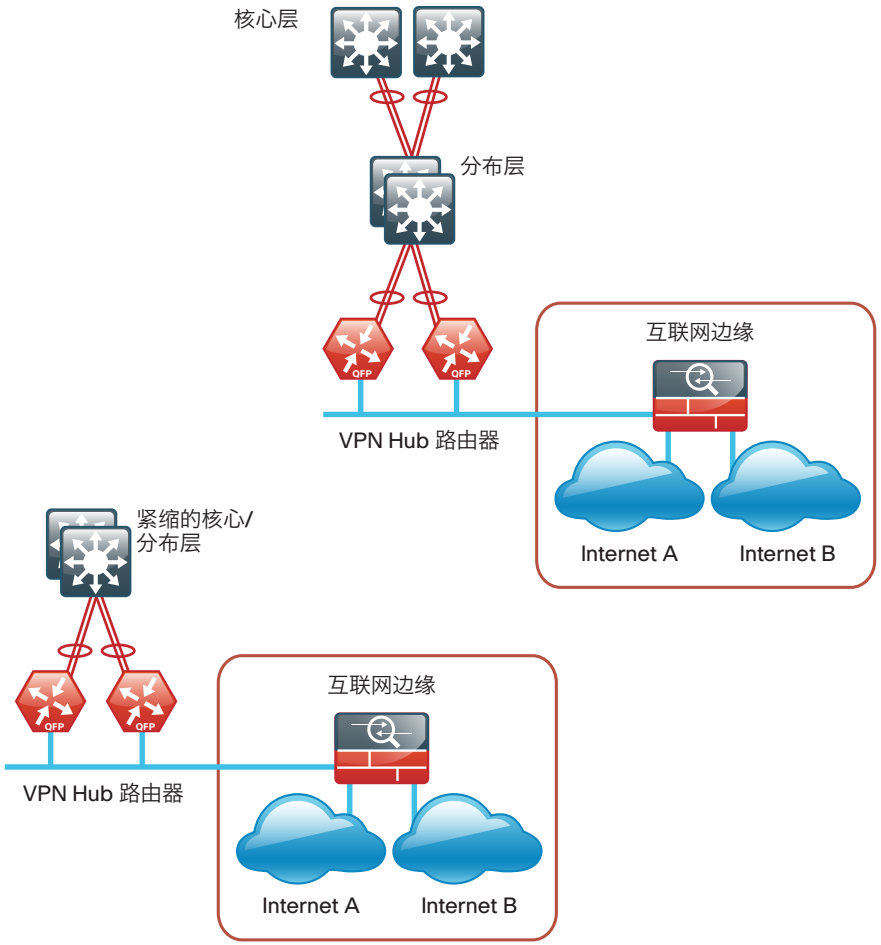


双DMVPN设计模型

- 支持至500远端站点
- 使用双互联网链路
- 通常使用专用的广域网分布层

双DMVPN的设计如下图所示。

图 3 - 双DMVPN设计模型



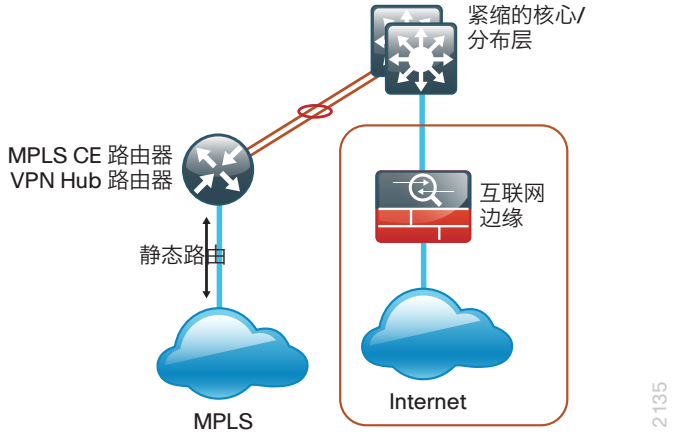
在单DMVPN和双DMVPN设计模型中，DMVPN中枢路由器连接到互联网，会间接的穿越互联网边缘的防火墙分军事区（DMZ）接口。如需了解去往互联网连接的更详细信息，请参阅《防火墙和IPS部署指南》。需要注意的是，VPN中枢路由器连接至防火墙DMZ接口，而不是直接连接至互联网服务提供商路由器。

DMVPN备份共享设计模型

- 支持至50远端用户
- 为MPLS CE和VPN中枢使用相同的路由器
- 拥有单一的MPLS VPN载体
- 以静态路由的方式使用MPLS VPN承载
- 使用单一的互联网链路

DMVPN备份共享设计如下图所示。

图 4 - DMVPN备份共享设计模型



在DMVPN备份共享设计模型中，DMVPN中枢路由器也是MPLS CE路由器；它已经连接至分布层或核心交换机。去往互联网的连接已经由互联网边缘的防火墙接口建立连接，对于该设计模型来说不需要DMZ。如需了解去往互联网连接的更详细信息，请参阅《防火墙和IPS部署指南》。

DMVPN备份专用设计模型

- 支持至500远端站点
- 拥有单或双MPLS VPN载体或单二层广域网。
- 以BGP路由的方式使用MPLS VPN承载，或在二层广域网上使用EIGRP路由。
- 使用单互联网链路

不同场景的DMVPN专用设计如下图所示。

图 5 - 用于MPLS广域网的DMVPN备份专用设计模型

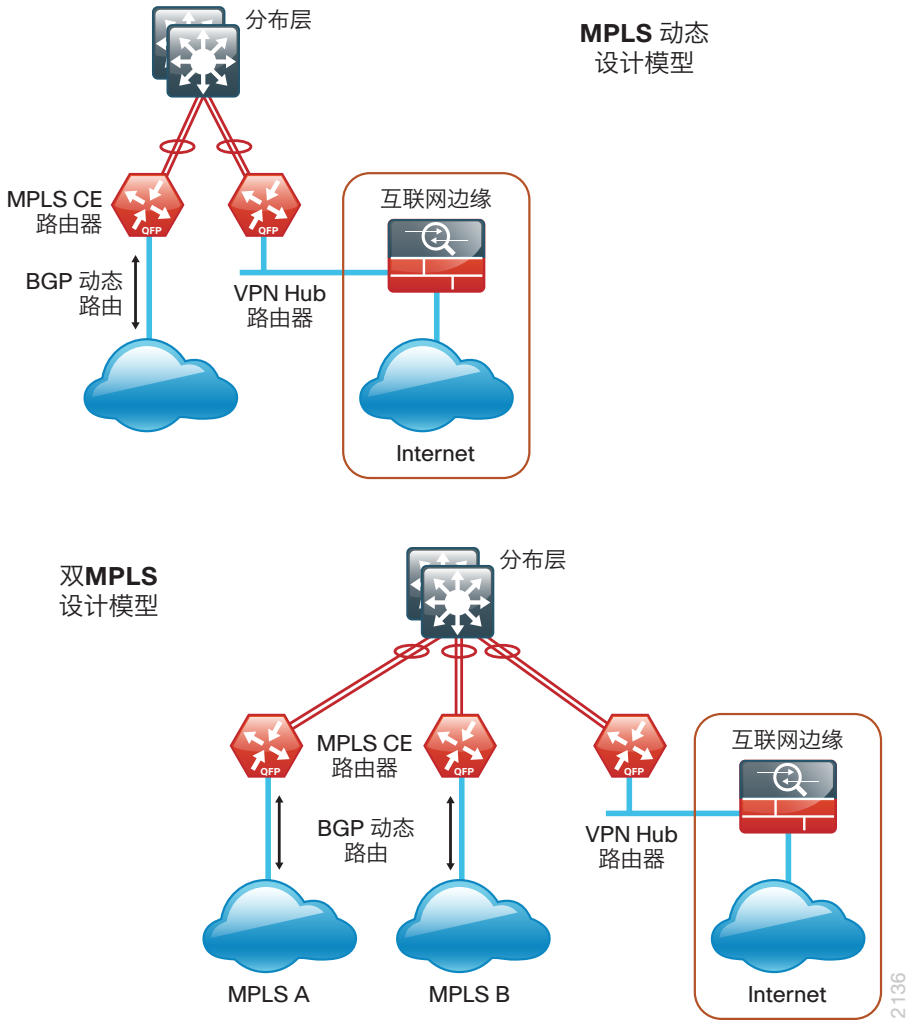
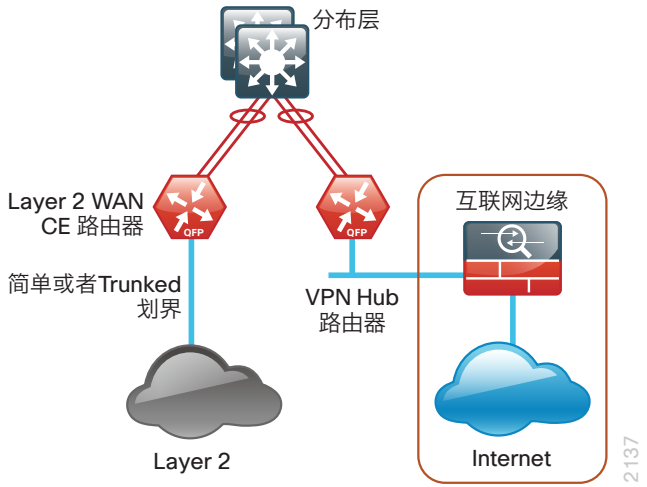


图 6 - 用于二层广域网主用设备的DMVPN备份专用设计模型

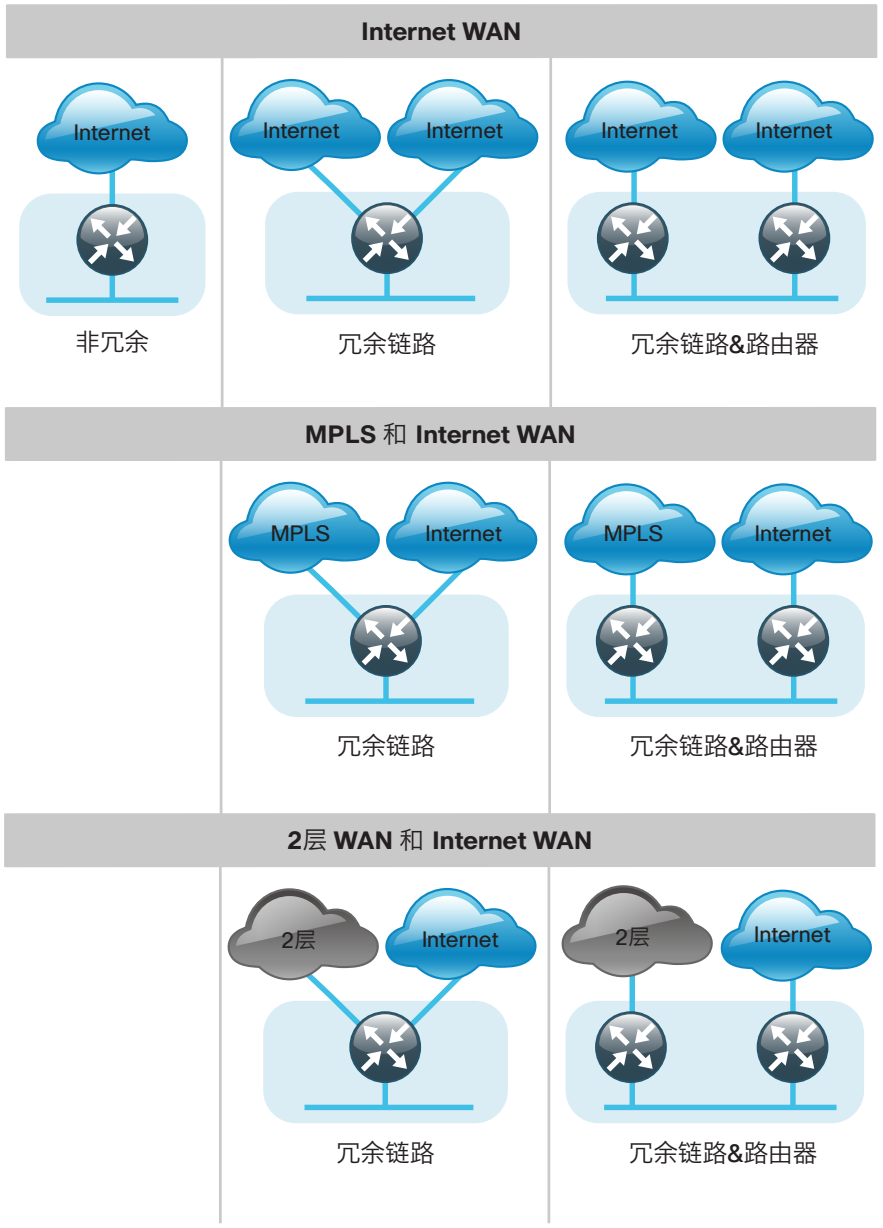


在DMVPN备份专用设计模型中，DMVPN中枢路由器连接到互联网，会间接的穿越互联网边缘的防火墙分军事区（DMZ）接口。如需了解去往互联网连接的更详细信息，请参阅《防火墙和IPS部署指南》。需要注意的是，VPN中枢路由器连接至防火墙DMZ接口，而不是直接连接至互联网服务提供商路由器。

WAN远端站点设计

本指南介绍了多种广域网远端站点设计。这些设计构建于多种广域网传输组合之上，反映了站点具体的服务等级和冗余要求。

图 7 - 广域网远端站点设计



远端站点设计包含单个或两个广域网边缘路由器。这些路由器可以是CE路由器（对于MPLS或二层广域网来说）或VPN分支路由器。在某些情况中，单个广域网边缘路由器可以同时执行CE路由器和VPN分支路由器的功能。

大多数远端站点均采用单个路由器广域网边缘进行设计；然而，某些远端站点类型则要求使用双路由器广域网边缘。适用双路由器的站点包括有着大量用户的地区办事处或远程园区；以及有着关键业务需求，需要增加冗余能力以消除单点故障的站点。

总体的广域网设计方法以主要的广域网汇聚设计站点设计为基础，该设计能够支持所有与下表中所列的不同链路组合对应的远端站点类型。

表 3 - 广域网远端站点传输选项

广域网远端站点路由器	广域网传输方法	主用传输	备用传输
单个	单个	互联网	-
单个	两个	互联网	互联网
两个	两个	互联网	互联网
单个	两个	MPLS VPN	互联网
两个	两个	MPLS VPN	互联网
单个	两个	城域以太网/VPLS	互联网
两个	两个	城域以太网/VPLS	互联网

该网络设计的模块化特性使您可以创建在网络中进行复制的设计元素。

两种广域网汇聚设计和所有广域网远端站点设计均为总体设计中的标准构建模块。复制单个构建模块的能力为扩展网络提供了一种简便快捷的方法，同时也支持采用一致的部署方案。

广域网/局域网互连

广域网的主要作用是互连主要站点和远端站点局域网。本指南中有关局域网的探讨仅限于广域网汇聚站点局域网如何连接到广域网汇聚设备，以及远端站点局域网如何连接到远端站点广域网设备。关于设计中的局域网组件的详细信息在《*局域网部署指南*》中进行阐述。

在远端站点中，局域网拓扑结构取决于站点要连接的用户数量和所处的地理位置。大型站点可能要求使用分布层来支持多个接入层交换机。其他站点可能仅要

求使用一个接入层交换机来直接连接广域网远端站点路由器。本指南中测试和介绍的不同方案如下表所示。

表 4 - 广域网远端站点局域网选项

广域网远端站点路由器	广域网传输方法	局域网拓扑
单	单	仅接入层 分布层/接入层
单	单	仅接入层 分布层/接入层
双	双	仅接入层 分布层/接入层

广域网远端站点—局域网拓扑

为了保持一致性和模块化特性，所有广域网远端站点均使用了下表中显示的相同VLAN分配方案。本部署指南所采用的实践适用于任意具有单个接入交换机的位置，并且这一模式也可以通过添加分布层扩展至更多的接入间（access closet）。

表 5 - 广域网远端站点—VLAN分配

VLAN	用途	二层接入	三层分布/接入
VLAN 64	数据1	是	-
VLAN 69	语音 1	是	-
VLAN99	传输	是 （仅双路由器）	是 （仅双路由器）
VLAN50	路由器连接 (1)	-	是
VLAN54	路由器连接 (2)	-	是

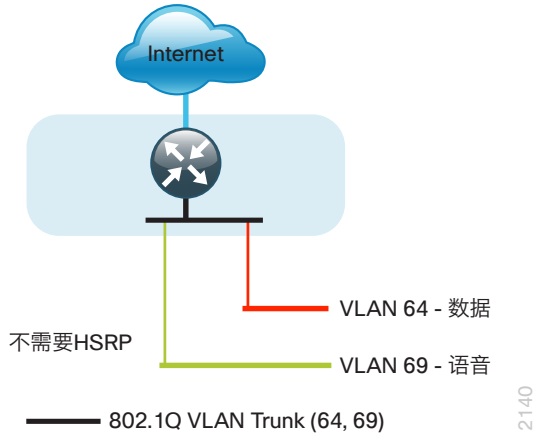
二层接入层

不需要额外分布层路由设备的广域网远端站点被视为扁平结构，或者从局域网的角度，被视为无路由二层站点。所有三层服务均通过相连的广域网路由器来提供。通过使用多个VLAN，接入交换机能够支持诸如数据和语音（等服务。下图中的设计显示了一个标准的VLAN分配方案。这种设计的优势非常明显：在这一配置中，无论有多少个站点，所有接入交换机均可以采用相同的配置。

接入交换机及其配置在本指南中不做介绍。《局域网部署指南》提供了关于各种接入交换平台的配置详细信息。

IP子网基于每个VLAN进行分配。尽管需要的IP地址数量少于254个，这一设计仅使用255.255.255.0子网掩码来为接入层分配子网。（这一模式可根据其他IP地址方案进行调整。）路由器和接入交换机之间的连接必须针对与路由器子接口相连的802.1Q VLAN进行配置。这些子接口分别与交换机上的VLAN相对应。各个路由器子接口用作每个IP子网和VLAN组合的IP缺省网关。

图 8 - 广域网远端站点——扁平型二层局域网（单路由器）



类似的局域网设计可以扩展为下图中所示的双路由器边缘。这种设计变更会增加一定的复杂性。首先需要运行路由协议。您需要在路由器之间配置增强型内部网关协议（EIGRP）。为了保持与主要站点局域网的一致性，应使用EIGRP进程100。

由于现在每个子网有两个路由器，必须实施第一跳冗余协议（FHRP）。在此设计中，思科选择了热备用路由器协议（HSRP）作为FHRP。HSRP能够支持第一跳IP路由器实现透明的故障切换。通过为配置了缺省网关IP地址的IP主机提供第一跳路由冗余能力，HSRP可带来高度的网络可用性。HSRP用于包含一组路由器的环境中，用来选择活动路由器和备用路由器。当局域网上有多个路由器时，活动路由器用于路由数据包；备用路由器用于在活动路由器发生故障或达到预定的条件时接管活动路由器的工作。

图 9 - 广域网远端站点——扁平型二层局域网 (双路由器)

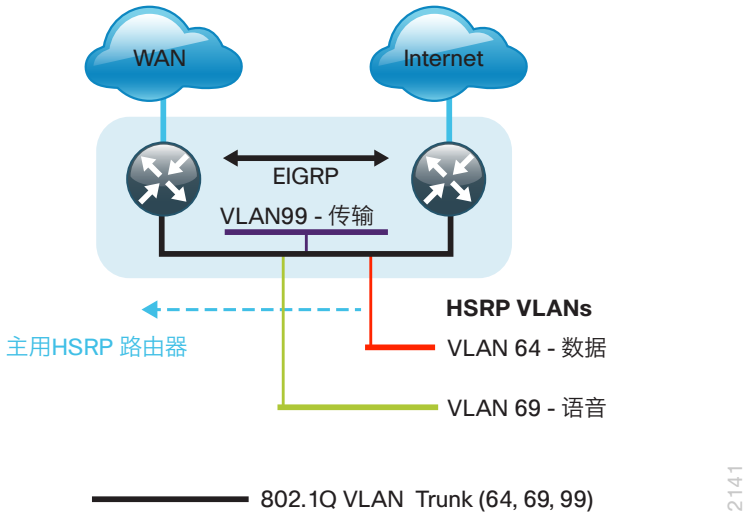
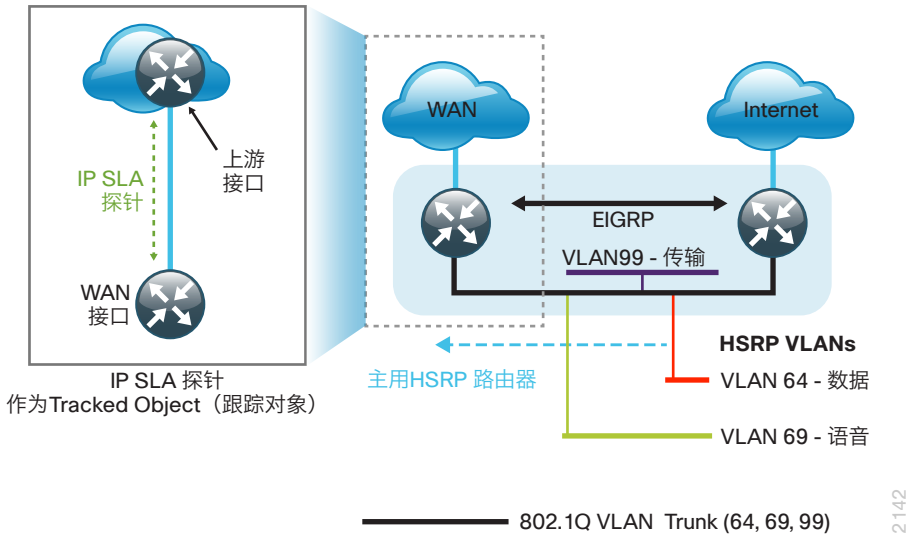


图 10 - 广域网远端站点—IP SLA探针来验证上游设备可达性



增强的对象跟踪 (EOT) 技术为不同路由器和交换特性提供了一种一致的方法，来根据其他进程中可用的信息对象有条件地修改其工作方式。可以跟踪的对象包括interface line protocol (接口线路协议)、IP route reachability (IP路由可达性) 和IP服务等级协议 (SLA) 可达性，以及其他几个对象。

IP SLA特性能够支持路由器生成综合网络流量，并发送给远程响应设备。响应设备可以是能够响应互联网控制消息协议 (ICMP) echo (ping) 请求的通用IP终端设备，或是运行IP SLA响应装置进程的思科路由器。它们能够响应诸如抖动探测等更复杂的流量。IP SLA的使用使得路由器能够确定到某一目的地的端到端可达性，以及往返延时。更复杂的探测类型也可支持计算路径中的丢包和抖动情况。在这一设计中，我们结合使用了IP SLA与EOT。

为了缩短在主用广域网发生故障后的收敛时间，HSRP能够通过使用EOT和IP SLA监控下一跳IP邻接设备的可达性。这一组合使得路由器能够在上游邻接设备变得无响应时放弃其HSRP活动路由器角色，从而提高网络永续性。

HSRP被设定为在拥有最高广域网传输优先级的路由器上激活。IP SLA探测的EOT技术与HSRP结合使用，以便当广域网传输方案发生故障时，拥有较低 (备用) 广域网传输优先级的备用HSRP路由器能够成为活动HSRP路由器。IP SLA探测从远端站点主用广域网路由器被发送至上游邻居 (MPLS PE，二层广域网CE或DMVPN中枢 (DMVPN hub))，以确保下一跳路由器的可达性。这比只监控广域网接口的状态更为有效。

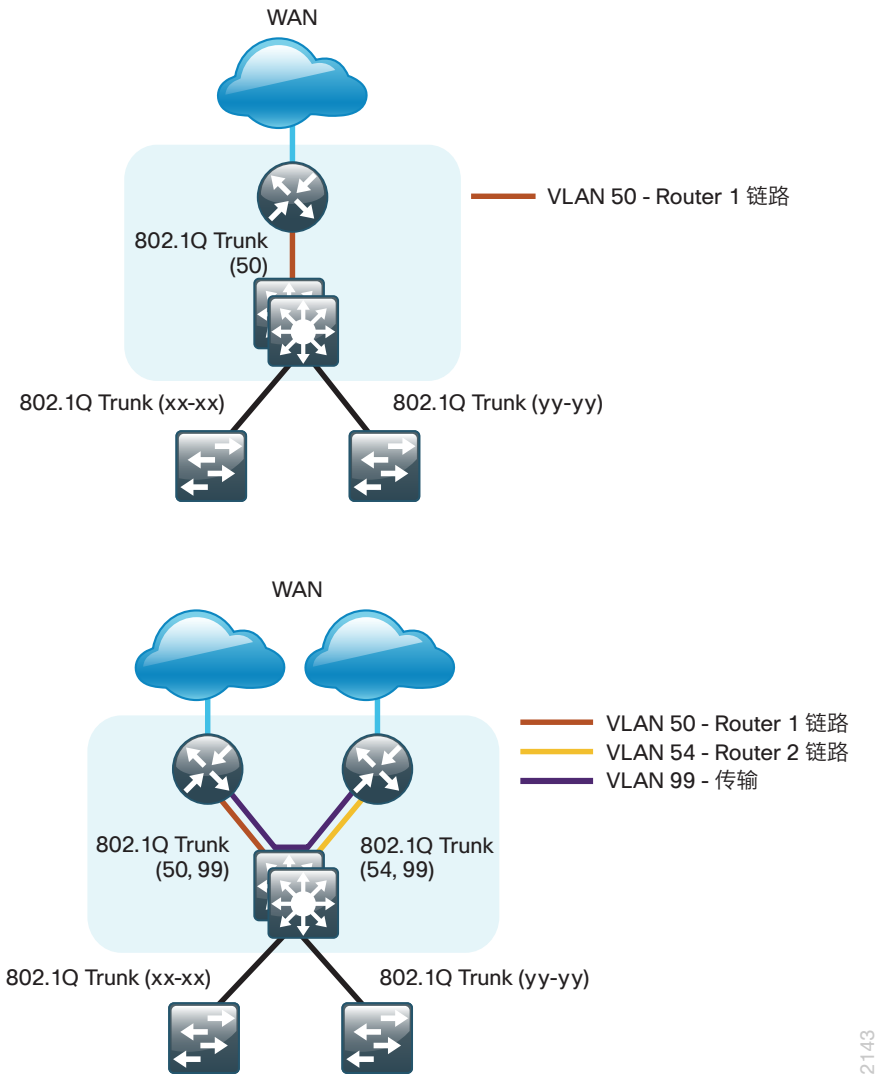
双路由器设计还提供了在特定情形下进行正确的路由所需的一个额外组件。在这些情形中，来自远端站点主机的流量可能被发送至通过备用广域网传输方案才能到达的目的地 (例如：双MPLS + DMVPN远端站点与单DMVPN2远端站点进行通信)。之后，主要广域网传输路由器会通过相同的数据接口将流量发送至备用广域网传输路由器，由后者将该流量转发至正确的目的地。这一过程被称作“发夹”。

避免通过相同接口发送流量的正确方法为，在路由器间引入一个额外的链路，并将该链路设定为过境网络 (Vlan 99)。过境网络没有与之相连的主机，仅用于支持路由器之间的通信。路由协议在分配给过境网络的路由器子接口间运行。这一设计变更不需要额外的路由器接口，因为802.1Q VLAN中继 (trunk) 配置能够轻松支持额外的子接口。

分布层与接入层

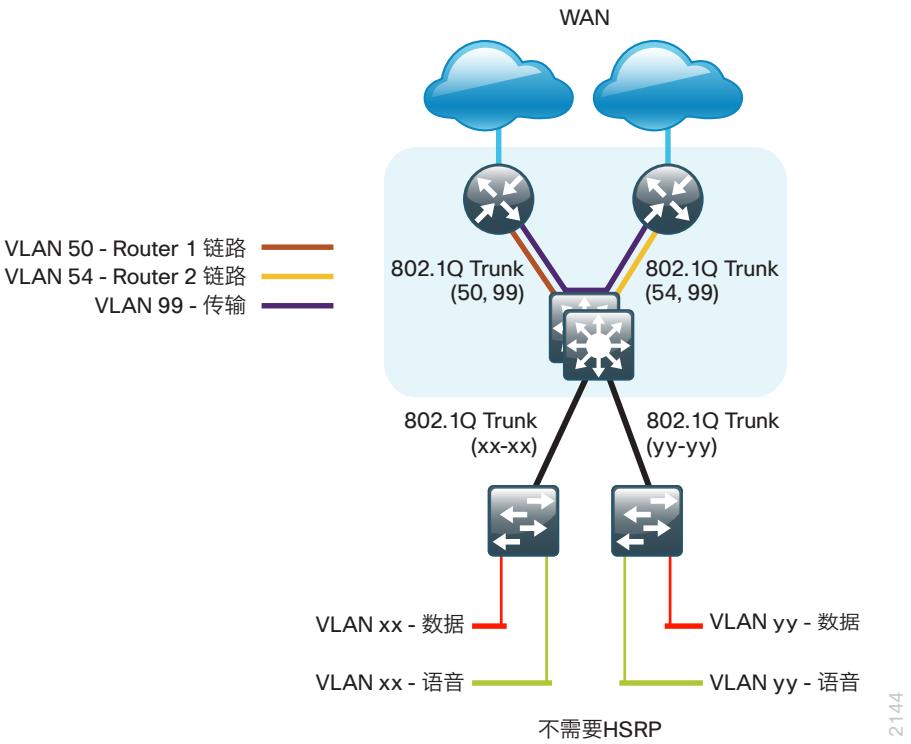
大型远端站点可能要求类似于小型园区局域网的局域网环境，其中包含有分布层和接入层。这一拓扑能够很好地支持单路由器或双路由器广域网边缘。要实施这一设计，路由器应通过EtherChannel链路连接到分布层交换机。这些EtherChannel链路被配置为802.1Q 中继，能够支持路由点对点链路和双路由器设计。其中路由点对点链路可支持在分布层交换机上进行EIGRP路由；而双路由器设计能够提供一个过境网络，支持在广域网路由器之间直接进行通信。

图 11 - 广域网远端站点—到分布层的连接



分布层交换机负责通过连接到接入交换机的VLAN，处理所有接入层路由。当设计包含分布层时，无需使用HSRP。下图显示了完整的分布层与接入层设计。

图 12 - 广域网远端站点—分布层和接入层 (双路由器)



IP组播

IP组播允许基础设施 (路由器和交换机) 复制单个IP数据流, 然后将其从一个源设备发送到多个接收设备。IP组播要比多个单独的单播数据流或四处传播的广播数据流更为高效。IP电话等待音乐 (MOH) 和IP视频广播数据流就是IP组播应用的两个实例。

为了接收特定的IP组播数据流, 终端主机必须通过向其本地组播路由器发送互联网群组管理协议 (IGMP) 消息, 加入组播组。在传统的IP组播设计中, 本地路由器会询问网络中充当汇聚点 (RP) 的另一个路由器, 将接收设备映射到活动源设备上, 以便它们能够加入其数据流。

RP是一种控制平面操作, 应被置于网络的核心, 或者邻近一对三层交换机或路由器上的IP组播源的位置。如果接入层是二层, 并提供了到IP组播汇聚点的连接, IP组播路由将从分布层开始。在没有核心层的设计方案中, 分布层会承担起汇聚点的功能。

这种设计可全面支持单一的IP组播全局部署。它采用了Anycast RP实施战略。该战略在稀疏模式独立组播协议 (PIM SM) 网络中提供了负载分享与冗余能力。两个RP分享源注册的负载, 并能够互为彼此的热备份路由器。

从广域网的角度而言, 这一战略的优势在于广域网中的所有IP路由设备均使用基于Anycast RP的相同配置。IP PIM SM在所有接口上均可用, 包括回环接口、VLAN和子接口。

服务质量

大多数用户均将网络视作一种传输效用机制, 可将数据以尽可能快的速度从A点移动到B点。许多人将这一过程简单归结为 “速度和馈进 (speeds and feeds) ”。虽然IP网络确实在默认情况下以尽力而为 (Best Effort) 的模式转发流量, 但这一路由类型仅适用于能够根据延迟、抖动和丢包等变量进行适当调整的应用程序。然而, 网络的设计决定了它需要支持多种服务, 包括实时语音和视频, 以及数据流量。此处的区别在于实时应用程序要求数据包在规定的丢失、延迟和抖动参数内送达。

事实上, 网络影响着所有通信流量, 因此必须了解最终用户要求和提供的服务。即使在无限带宽环境中, 时间敏感型应用也会受到抖动、延迟和丢包现象的影响。服务质量 (QoS) 支持多种用户服务和应用程序在同一网络中共存。

该架构支持有线和无线连接选项, 采用先进的分类、优先级划分、队列和拥塞机制, 作为实现综合QoS的一部分, 确保网络资源的最佳利用。这一功能支持对应用程序进行区别处理, 以确保每一个应用程序均能够享有适当的网络资源, 从而保护用户体验, 并保证关键业务应用程序的持续运行。

QoS是本架构中所用网络基础设施设备的一个重要功能。QoS可支持多种用户服务和应用程序, 包括实时语音、高质量视频和延迟敏感型数据等在同一网络中共存。为了使网络提供可预测、可衡量、且有保证的服务, 就必须要对带宽、延迟、抖动和丢包参数进行管理。即使您当前的应用程序不需要QoS, 您也可以将QoS用于管理和网络协议, 在正常和流量拥塞的情况下保证网络功能和可管理性。

本设计的目标是提供足够的服务类别, 以支持您在初始部署中, 或者在日后以最少的工程工作和最小的系统影响, 向网络中添加语音、互动视频、关键数据应用程序和管理流量。

本设计中应用了下表中的QoS分类。此表仅作为参考之用。

表 6 - QoS服务类别映射

服务类别	逐跳行为（PHB）	差分服务代码点 (DSCP)	IP优先级（IPP）	服务类别（CoS）
网络层	三层	三层	三层	二层
网络控制	CS6	48	6	6
电话	EF	46	5	5
信令	CS3	24	3	3
多媒体会议	AF41, 42, 43	34, 36, 38	4	4
实时交互	CS4	32	4	4
多媒体流	AF31, 32, 33	26, 28, 30	3	3
广播视频	CS5	40	4	4
低延迟数据	AF21, 22, 23	18, 20, 22	2	2
运营、管理和维护 (OAM)	CS2	16	2	2
批量数据	AF11, 12, 13	10, 12, 14	1	1
Scavenger (清道夫)	CS1	8	1	1
缺省“尽力而为”(Best Effort)	DF	0	0	0

部署广域网

广域网架构整体设计目标

IP路由

这一设计要实现以下IP路由目标:

- 为从主要广域网汇聚站点到所有远程地点提供最佳路由连接
- 避免广域网路由拓扑变更影响到网络中的其他部分
- 当存在多个路径时, 确保实现活动/备用对称路由, 以简化故障排除工作, 避免超额配置IP电话呼叫准入控制 (CAC) 限度
- 通过主要广域网汇聚站点, 提供站点间远程路由 (星型模式)
- 当支持运营商服务时, 提供最佳的直接站点间远程路由 (分支到分支模式)
- 支持来自主要广域网汇聚站点的IP组播

在广域网远端站点, 没有用于浏览网页和使用云服务的本地互联网接入服务。这一模式被称作集中互联网模式。值得注意的是, 采用互联网/DMVPN作为备用传输方案的站点, 将能够潜在地提供本地互联网能力; 然而, 在本设计中, 只有到其他DMVPN站点的加密流量才可以使用互联网链路。在集中互联网模式中, 除了来自数据中心和园区的内部路由外, 缺省路由也将被通告给广域网远端站点。

局域网接入

所有远端站点均支持有线和无线局域网接入。

高可用性

网络必须能够容忍单一故障情况, 包括主要广域网汇聚站点中的任意单个广域网传输链路或任意单个网络设备的故障。

- 单路由器、双链路类远端站点必须能够在任一广域网传输方案出现问题时继续正常运行。
- 双路由器、双链路类远端站点必须能够在任一边缘路由器或广域网传输方案出现问题时继续正常运行。

路径选择偏好

根据所使用的广域网传输方案, 以及远端站点是否使用了双广域网传输方案, 流量可以多种方式进行传输。

单一广域网传输方案的路由功能如下描述。

DMVPN连接的站点:

- 连接到同一DMVPN上的站点; 在DMVPN中实现最佳路由 (只有最初的流量被发送至DMVPN中枢, 然后经由分支-分支隧道 (spoke-spoke tunnel) 绕行穿过 (cut-through)) 。
- 连接到任意其他站点; 路由通过主要站点进行。

双广域网传输方案的使用专门针对在活动/备用模式中工作进行了调整。这一配置类型提供了对称路由, 流量沿着同一路径进行双向传输。对称路由可简化故障排除工作, 因为双向流量始终沿着相同的链路进行传输。

该设计假定其中一个MPLS VPN WAN传输方式被指定为主要的传输方式, 并且在大多数情况下是首选路径。

MPLS VPN (主用) + MPLS VPN (备用) 双连接站点:

- 连接到同一MPLS VPN上的站点; 在MPLS VPN中实现最佳路由 (流量未发送至主要站点) 。
- 连接到任意其他站点; 路由通过主要站点进行。

MPLS VPN + DMVPN双连接站点:

- 连接到同一MPLS VPN上的站点; 在MPLS VPN中实现最佳路由 (流量未发送至主要站点) 。
- 连接到任意DMVPN单一连接的站点; 在DMVPN内实现最佳路由 (只有初始流量被发送至DMVPN中枢, 之后通过分支到分支隧道进行直通传输) 。
- 连接到任意其他站点; 路由通过主要站点进行。

二层广域网 (主用) + DMVPN (备用) 双连接站点:

- 连接到二层广域网 (相同VLAN) 的站点; 在二层广域网中实现最佳路由 (流量未发送至主要站点) 。
- 连接到任意DMVPN单一连接的站点; 在DMVPN内实现最佳路由 (只有初始流量被发送至DMVPN中枢, 之后通过分支到分支隧道进行直通传输) 。
- 连接到任意其他站点; 路由通过主要站点进行。

数据机密性 (加密)

所有远端站点流量在通过互联网等公共IP网络进行传输时必须加密。

加密技术的使用应避免对远端站点应用程序的性能或可用性造成影响，并应对最终用户保持透明。

服务质量 (QoS)

网络必须确保业务应用程序能够在网络拥塞期间在广域网上正常运行。流量必须进行分类和排队，广域网连接必须能够调整，以便在连接的能力范围内工作。当广域网设计使用了提供有QoS的电信运营商的产品时，广域网边缘QoS分类与处理方法必须与电信运营商的产品保持一致，以确保实现一致的端到端QoS流量处理方法。

设计参数

本部署指南使用了特定标准设计参数，并参考了在广域网中不存在的多种网络基础设施服务。这些参数如下表所列。

表 7 - 通用设计参数

网络服务	IP地址
域名	cisco.local
活动目录、DNS服务器、DHCP服务器	10.4.48.10
身份认证控制系统 (ACS)	10.4.48.15
网络时间协议 (NTP) 服务器	10.4.48.17

备注

部署动态多点虚拟专用网络（DMVPN）广域网

业务概述

企业要求广域网能够为远端站点用户提供卓越的性能和出色的可靠性，以有效支持业务的开展。尽管远端站点员工使用的大多数应用和服务均位于集中部署的位置，但广域网设计必须要为处于任意位置的员工提供相同的资源访问体验。

对于使用广域网传输方案来支持远端站点连接的企业而言，基于运营商的MPLS服务并不总是可用或者经济高效。基于互联网的IP VPN为远端网络充分提供了主用网络传输。此外，他们同样可提供一种可选的传输方案，您可以将其作为另一个主用IP VPN的永续性备用方案，灵活的网络架构应在不会显著增加整体设计复杂性的情况下，将互联网VPN包含在传输方案中。

虽然互联网IP VPN网络为建立有效的广域网连接提供了一种富有吸引力的选择，但企业在任何时候通过公共网络发送数据，都会面临数据泄露的风险。数据丢失或损坏可能导致违反法律规定，损害公共形象，而这些都会对企业造成严重的财务影响。通过互联网等公共网络进行安全的数据传输要求进行充分的加密，来保护业务信息。

技术概述

DMVPN中枢路由器

DMVPN设计可支持多达500个远端站点，广域网汇聚总带宽最高可达1.0 Gbps。其中最关键的设备为负责可靠IP转发和QoS的广域网路由器。所需带宽量用于广域网汇聚站点中所使用的路由器模型；为了提供到所有远端站点的连接，通过DMVPN云的数量选择实施单路由器或双路由器。

Cisco ASR 1000系列汇聚多业务路由器是一款下一代、模块化集成业务思科路由平台。它们专为广域网汇聚而设计，具备出色的灵活性，能够支持广泛的3到16 mpps（每秒一百万数据包）数据包转发能力和2.5到40-Gbps系统带宽，并可进一步扩展。

Cisco ASR 1000系列在硬件和软件方面均实现了全面的模块化。该款路由器具备真正的运营商级路由产品的全部要素，能够出色地支持企业和电信运营商网络。

本设计使用如下路由器作为DMVPN中枢路由器：

- Cisco ASR 1002汇聚服务路由器，配有一个嵌入式服务处理器5（ESP5）
- Cisco ASR 1001 聚服务路由器，配有一个固定的2.5 Gbps 嵌入式服务处理器
- Cisco 3945 集成服务路由器
- Cisco 3925 集成服务路由器

所有的设计模型可以使用表格 8中所列任意的DMVPN中枢服务器搭建。您应考虑如下：路由器的转发性能为启用大多数服务的以太广域网部署所使用。路由器符合建议的设计模式，和远端站点的数量。

表 8 - DMVPN中枢路由器选项

选项	Cisco 3925	Cisco 3945	ASR 1001	ASR 1002
包含服务的以太广域网	100 Mbps	150 Mbps	250 Mbps	500 Mbps
软件冗余选项	无	无	是	是
冗余电力供应	可选	可选	默认	默认
支持的设计模型	所有	所有	所有	所有
建议的设计模型	DMVPN 备份共享	DMVPN 备份共享	单 DMVPN DMVPN 备份专用	双 DMVPN DMVPN 备份专用
建议的远端站点数量	25	50	100	250

远端站点—DMVPN分支路由器选择

由于平台规格与站点的带宽要求、以及潜在的服务模块插槽使用要求紧密相关，所以实际的广域网远端站点路由平台仍未确定。模块化设计方法的优势之一，便是能够采用各种可能的路由器选择来实施这一解决方案。

在选择广域网远端站点路由器时，有多种因素需要考虑。其中对于初始部署至关

重要的是，要能够处理预期的流量数量和类型。您还需要确保拥有足够的接口和模块插槽，以及可支持拓扑所需特性集的相应思科IOS软件映像。思科测试了多种集成多业务路由器型号在用作DMVPN分支路由器时的表现，预期性能如下表所示。

表 9 - 广域网远端站点的思科集成服务路由器选项

Option	1941	2911	2921	2951	3925	3945
包含服务的以太网广域网2	25 Mbps	35 Mbps	50 Mbps	75 Mbps	100 Mbps	150 Mbps
板载GE端口3	2	3	3	3	3	3
服务模块插槽4	0	1	1	2	2	4
冗余电源选项	否	否	否	No	是	是

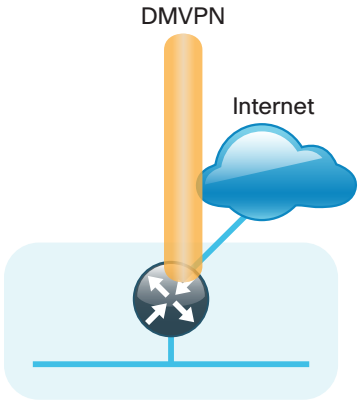
注：

1. 我们推荐在单路由器 (single-router) 、单链路 (single-link) 的远端站点使用Cisco 1941集成服务路由器。
2. 性能数值是路由器在配置了大量服务、且CPU利用率低于75%时传输IMIX流量得出的保守数字。
3. 当使用port-channel连接接入层或分布层时，单路由器、双链路的远端站点需要4个路由器接口。为提供额外的面向广域网 (WAN-facing) 接口，添加EHWIC-1GE-SFP-CU到Cisco 2900 and 3900系列集成服务路由器。
4. 一些服务模块有两倍宽。

广域网远端站点的DMVPN分支路由器通过路由器接口直接与互联网相连。更多有关连接至互联网的远端站点路由器的安全配置信息，将在本指南后部分进行讨论。单链路DMVPN远端站点是适用于任意远端站点的最基本的构建模块。此设计用于DMVPN分支路由器直接连接到接入层的情况，或者通过将DMVPN分支路由器与分布层直接连接，来支持更复杂的局域网拓扑。

IP路由非常简单，通过在广域网汇聚站点使用静态路由以及远端站点使用静态缺省路由直接全盘处理。然而，采用动态路由配置这一类型的站点能够带来巨大的价值。当使用动态路由时，由于任意变更均能够立即反映到网络的其余部分，因此它能够显著简化在远端站点添加或修改IP网络的工作。

图 13 - DMVPN远端站点 (单链路—单路由器)

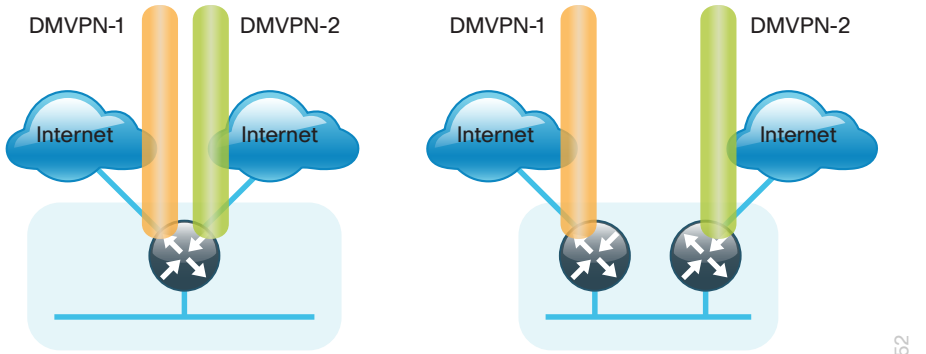


单DMVPN设计

DMVPN连接可用作主要广域网传输方案，或者用作另一个DMVPN广域网传输方案的备用选择。DMVPN备份链路可添加到现有的DMVPN单链路设计中，以提供更高的永续性连接到相同的路由器或其他路由器。通过添加额外链路，您可以为远端站点带来第一级别的高可用性。路由器能够自动检测主要链路故障，并将流量重路由至辅助路径。当存在多条路径时，必须强制运行动态路由。路由协议根据预期的流量情况进行调节。

双路由器、双链路设计可进一步改进站点的高可用性级别。这种设计能够允许在主要路由器出现故障时，辅助路由器通过备用路径重新路由流量。

图 14 - DMVPN + DMVPN远端站点 (双链路选项)



双DMVPN设计

DMVPN连接同样可替换现有的MPLS广域网或二层广域网传输。通过连接相同路由器或附加路由器，您可添加DMVPN备份链路到MPLS广域网或二层广域网单链路设计中，以提供额外的永续性。DMVPN双链路选项的相同永续性优势在于，应用MPLS + DMVPN 和二层+ DMVPN选项。单路由器和双路由器选项分别展示在图 15和图 16中。

图 15 - MPLS + DMVPN和二层广域网 + DMVPN远端站点（单路由器，双链路）

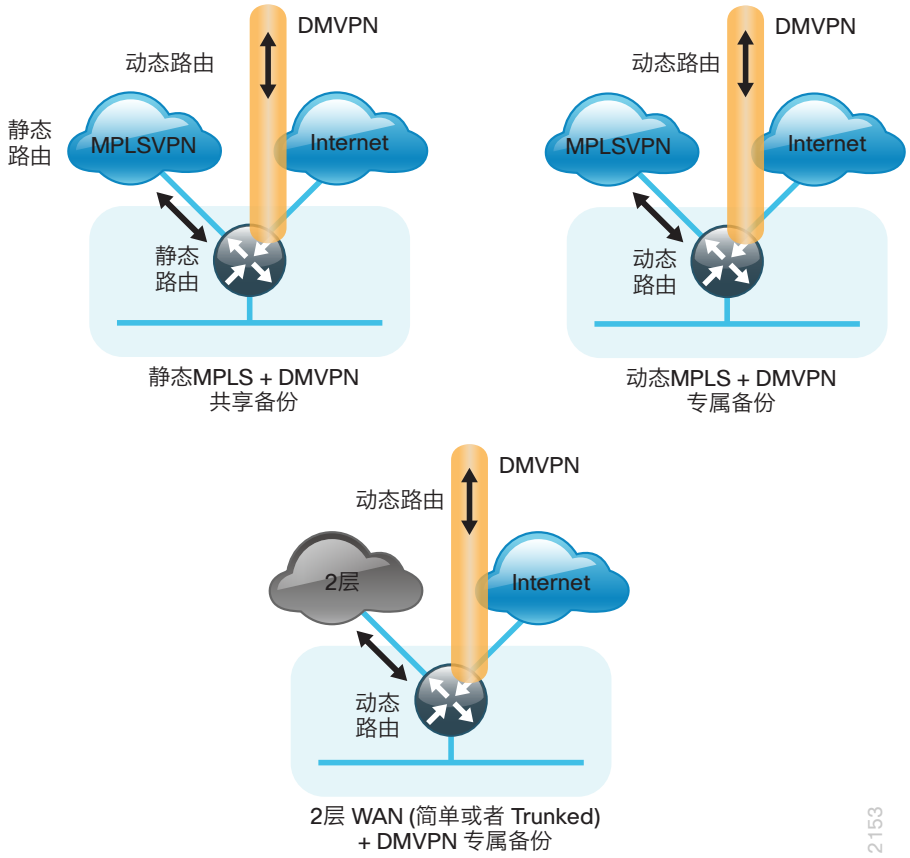
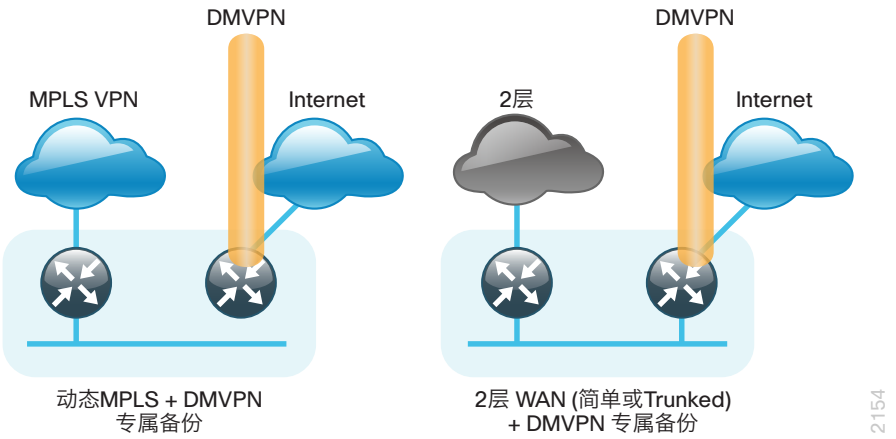


图 16 - MPLS + DMVPN和二层广域网 + DMVPN远端站点（双路由器，双链路）



VRF和Front Door VRF

虚拟路由转发（VRF）是一种在计算机网络中使用的技术，能够支持路由表的多个实例同时在同一台路由器上共存。由于路由实例彼此独立，因此您可以使用相同或重叠的IP地址，而不会在相互间产生冲突。在MPLS环境中，VRF还通常被定义为VPN路由转发。

您可以通过为每一个VRF建立不同的路由表将VRF部署在网络设备中，这些路由表也被称作转发信息库（FIB）。或者，网络设备可能会配置不同的虚拟路由器，其中每一个都有各自的FIB，相同设备上的任意其他虚拟路由器无法对其进行访问。

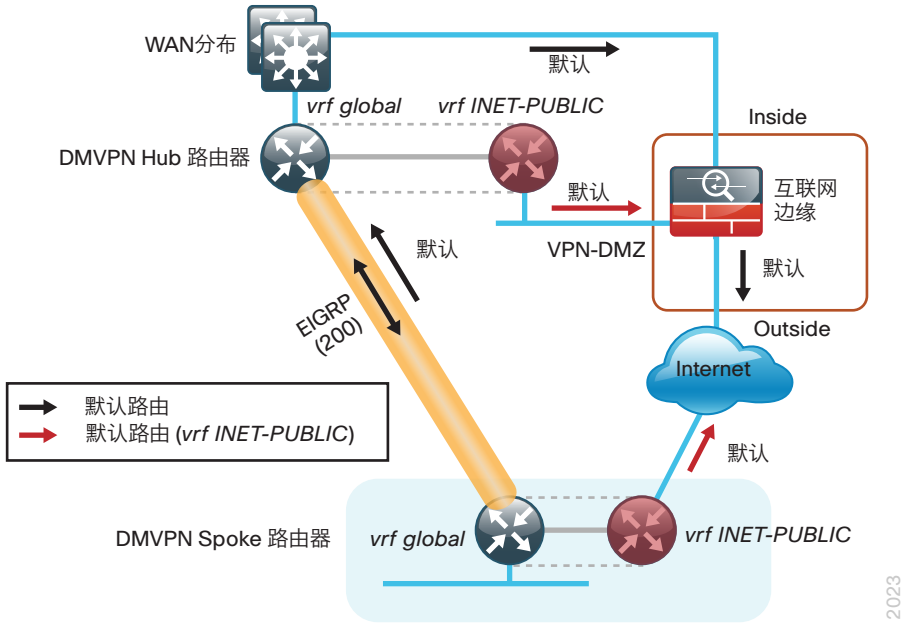
最简单的VRF部署形式为VRF Lite。在这一部署中，网络中的每一台路由器在对等的基础上参与虚拟路由环境。VRF Lite配置仅适用于本地环境。

这一广域网远端站点设计中使用的IP路由策略不允许直接使用互联网浏览网页或进行其他用途；任意访问互联网的远端站点主机必须通过主要站点的互联网边缘进行此类活动。终端主机要求具备面向所有互联网目的地的缺省路由，该路由必须强制流量经过主要或辅助广域网传输DMVPN隧道。这一要求与更为常见的VPN分支路由器要求存在冲突。后者要求采用面向互联网的缺省路由来建立VPN隧道。

多缺省路由难题可通过在路由器上使用VRF来解决。路由器可以拥有多个在逻辑上相隔离的路由表。从转发平面的角度来看，这种隔离与虚拟路由器类似。全局VRF用于响应传统的路由表，其他VRF分别被指定名称和路由描述符（RD）

。路由器上的部分特性能够感知VRF，包括静态路由和路由协议、接口转发与IPSec隧道等。这组特性与DMVPN结合使用，可允许为DMVPN中枢路由器和DMVPN分支路由器使用多个缺省路由。该特性组合被称作Front Door vREF（FVRF），因为VRF面向互联网，而路由器内部接口和mGRE隧道均保留在全局VRF中。更多有关FVRF的技术详情，请参阅技术特性补充附录。

图 17 - Front door VRF (FVRF)



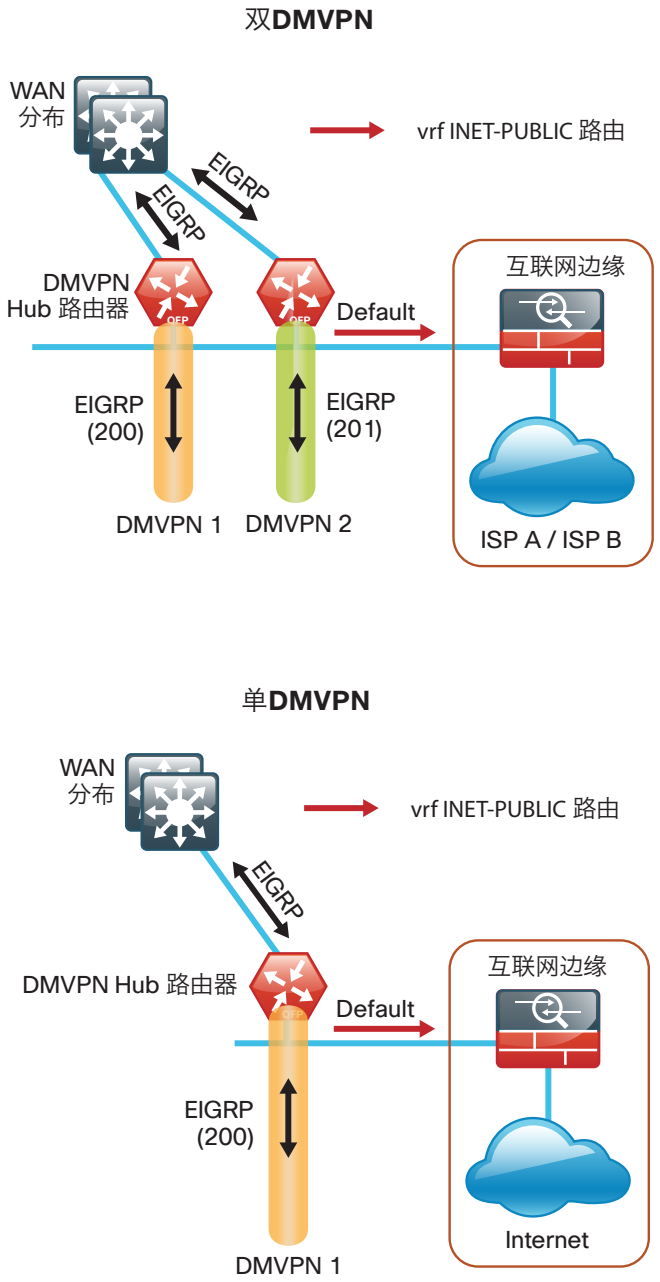
设计详情

DMVPN中枢路由器连接至分布层和DMZ中的永续性交换设备。DMVPN路由器使用由两个端口捆绑组成的EtherChannel连接。这种设计可带来出色的永续性与更高的转发性能。更高的转发性能可通过增加EtherChannel中的物理链路数量实现。

DMVPN中枢路由器必须具备足够的IP路由信息，以提供端到端可达性。维护这种路由信息通常需要路由协议，EIGRP便可用于这一用途。此设计中使用了多个独立的EIGRP进程，一个用于局域网上的内部路由（EIGRP-100），多个用于DMVPN（EIGRP-200，EIGRP-201）。使用独立EIGRP进程的主要原因在于，当部署其他的IBA智能业务平台广域网设计时，确保广域网汇聚站点的路由选择进程的兼容性。这一方法确保了DMVPN获知的路由在重发布至在园区局域网上使用的EIGRP-100进程后，显示为EIGRP外部路由。

在广域网汇聚站点，您必须将DMVPN路由器连接至分布层和提供有互联网连接的DMZ-VPN。DMVPN中枢路由器使用FVRF，并拥有静态缺省路由，其中INET-PUBLIC VRF指向防火墙DMZ接口。

图 18 - 双DMVPN和单DMVPN设计—路由详情

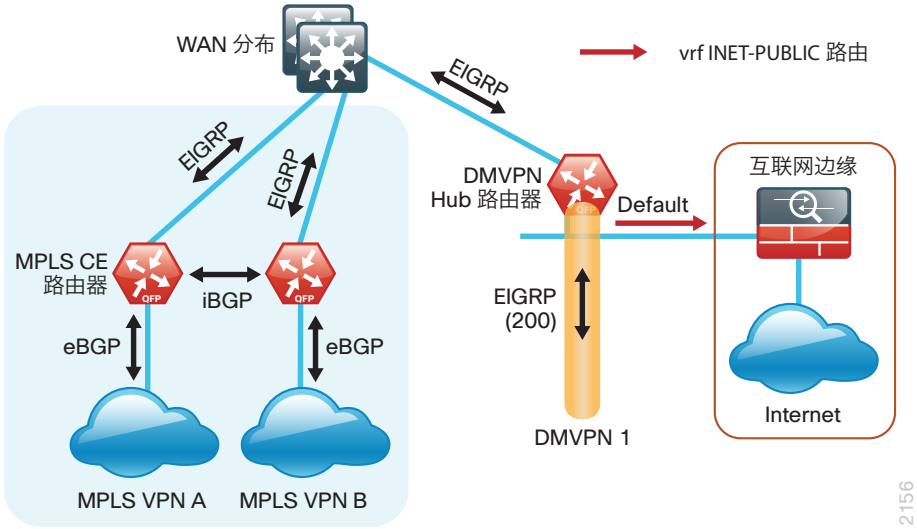


DMVPN备份专用设计模型本质上是单DMVPN或双DMVPN设计模型与任意的如下来自《MPLS广域网部署指南》和《二层广域网部署指南》中已部署设计模型的整合。

- MPLS动态
- 双MPLS
- 二层广域网简单划分
- 二层广域网中继划分

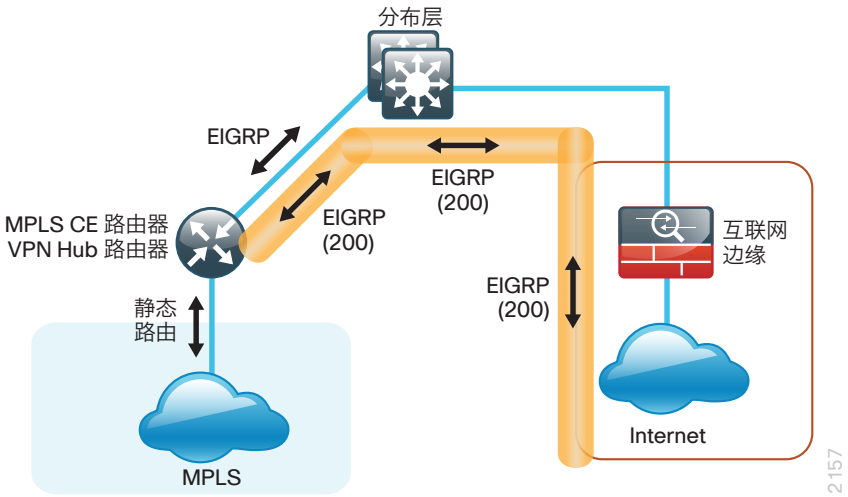
下图展示了DMVPN备份专用设计模型的路由明细案例。

图 19 - DMVPN备份专用设计—路由明细



DMVPN共享备用设计不需要额外的硬件。现有的MPLS静态设计来自《MPLS广域网部署指南》，它包括了广域网汇聚MPLS CE路由器和互联网访问。主要不同在于VPN连接和所需的为VPN备用链路所运行的路由协议。在这些设计中中，MPLS广域网连接沿用了静态路由。这些设计的路由明细如下图所示。

图 20 - DMVPN共享备份设计—路由明细



EIGRP

思科选择增强型IGRP (EIGRP) 作为主要的路由协议，因为它易于配置，不需要大量的规划工作，拥有灵活的汇总和过滤功能，并且可扩展至大型网络。随着网络的扩大，路由表中的IP前缀或路由的数量也将会相应增加。您应该在存在逻辑边界的链路上进行IP汇总，如分布层到广域网或核心层的链路。通过执行IP汇总，您可以减少运行大型路由表所需的带宽、处理器和内存数量，同时降低当发生链路故障时所需的收敛时间。

在这一设计中，EIGRP进程100是主要的EIGRP进程，被称作EIGRP-100。

EIGRP-100用于在广域网汇聚站点中，以连接主要站点局域网分布层，同时也可用于采用两个广域网路由器或分布层局域网拓扑的广域网远端站点。EIGRP-200和EIGRP-201用于DMVPN隧道。

加密

加密旨在通过当数据在网络中传输时对IP数据包进行加密，来保护数据机密性、完整性和真实性。

经过加密的有效载荷之后使用新的报头（或多个报头）进行封装，并在网络中传输。额外的报头会给总体数据包长度带来一定的开销。下表列出了根据各种IPsec和GRE组合所需的额外报头，与加密相关的数据包开销。

表 10 - 与IPsec和 GRE相关的开销

封装	开销
仅GRE	24字节
IPsec（传输模式）	36字节
IPsec（隧道模式）	52字节
IPsec（传输模式）+ GRE	60字节
IPsec（隧道模式）+ GRE	76字节

IP网络中的每个链路都有一个最大传输单元(MTU)，通常MTU为1500字节。超过1500字节的IP数据包在通过这些链路传输时，必须进行分片处理。我们不推荐进行分片，这会影响网络性能。为避免分片，原始数据包与开销的总大小必须等于或小于1500字节，这意味着发送方必须削减原始数据包大小。结合其他潜在的开销，思科建议隧道接口使用1400字节MTU进行配置。

有一些动态方法可帮助网络客户端设备探测到路径MTU，从而使得它们能够削减所传输的数据包的大小。然而，在许多情况下，由于安全设备通常会过滤掉必要的探测流量，这些动态方法并不奏效。探测路径MTU失败之后，就要求采用一种能够可靠地通知网络设备相应数据包大小的方法。解决方案就是在广域网路由器上执行**ip tcp adjust mss [size]**命令。该命令能够改变终端主机报告的TCP最大分段大小(MSS)值。

MSS定义了在单一TCP/IP数据报中，主机愿意接收的最大数据量。MSS值仅在TCP SYN片段中以TCP报头的形式发送。TCP连接的每一端向另一端报告其MSS值。发送主机需要限制单个TCP片段中的数据大小，使其小于或等于接收主机报告的MSS。

IP和TCP报头总计会占用40字节的开销，因此网络客户端通常报告的MSS值为1460。这一设计采用了基于1400字节MTU的加密隧道，因此终端设备使用的MSS应配置为1360，以最大限度降低分片处理的影响。在此解决方案中，您在所有面向广域网的路由器接口上实施**ip tcp adjust mss 1360**命令。

DMVPN

此解决方案使用互联网作为广域网传输方案。出于数据安全性和机密性的考虑，任何通过互联网传输的站点间流量都必须进行加密。有多种技术可用于进行加密，但从性能、规模、应用程序支持和部署简易性方面综合考虑，DMVPN是最佳的方法。

在本设计指南中，单链路用例采用互联网/DMVPN作为主用WAN传输方案，要

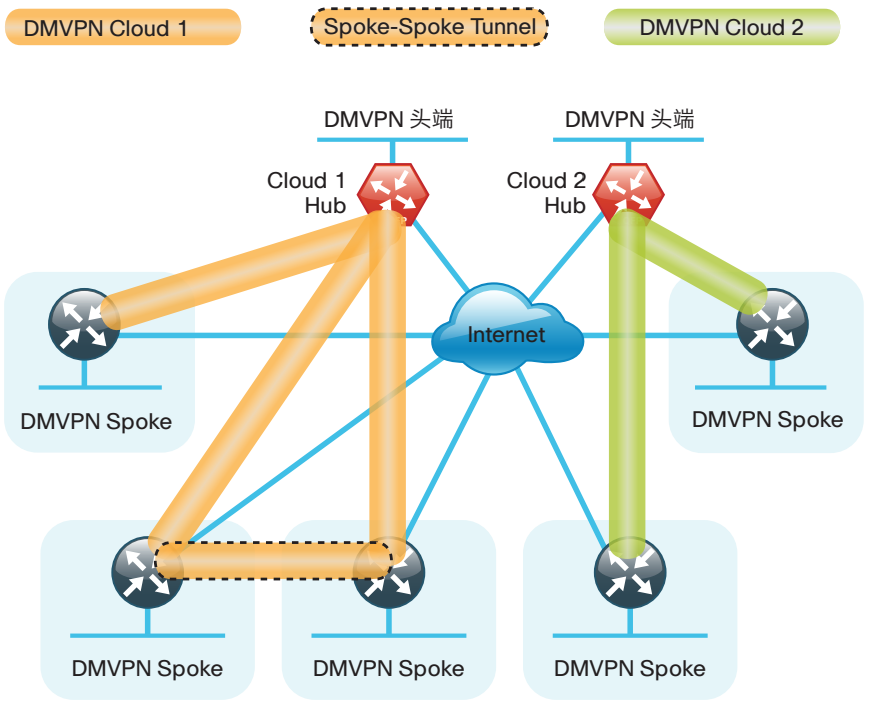
求使用DMVPN单云、单中枢 (hub) 设计。双链路用例要求使用DMVPN双云设计，每处都有一个中枢路由器。DMVPN路由器使用支持IP单播、IP组播和广播流量的隧道接口，包括使用动态路由协议。在初始星型隧道激活后，可以创建动态分支到分支隧道，以满足站点间IP流量传输的需要。

分支路由器建立动态分支到分支隧道和正确解析其他分支路由器所需的信息，通过下一跳解析协议 (NHRP) 提供。分支到分支隧道允许在不同地点间以最佳方式路由流量，而无需通过中枢路由器进行间接转发。空闲的分支到分支隧道会在一段时间闲置后停止连接。

DMVPN中枢路由器和互联网之间通常会部署防火墙。在许多情况下，防火墙可以提供网络地址转换 (NAT) 功能，将内部RFC-1918IP地址 (如10.4.128.33) 转变为互联网可路由的IP地址。DMVPN解决方案能够很好地支持NAT，但要求使用IPsec传输模式，以在静态NAT下支持DMVPN中枢路由器。

DMVPN要求使用互联网安全关联与密钥管理协议 (ISAKMP) 持活间隔来进行对等体状态检测 (DPD)，这对于推动快速重新收敛，以及支持分支路由器注册流程在DMVPN中枢路由器重新加载时正确执行至关重要。这一设计能够支持分支路由器检测出是否有加密对等体出现故障，以及与该对等体的ISAKMP会话是否失效，之后它将能够支持创建一个新的会话。如果没有DPD，IPsec安全关联 (SA) 必须设定超时时间 (缺省为60分钟)。当路由器无法重新协商一个新的SA时，新ISAKMP会话将被发起。最长等待时间约为60分钟。

图 21 - DMVPN双云



DMVPN解决方案的一个关键优势就在于，分支路由器可以使用动态分配的地址，这通常借助互联网提供商提供的DHCP实现。分支路由器可以利用互联网缺省路由来到达中枢路由器和其他分支路由器地址。

DMVPN中枢路由器在面向公共网络的接口上采用了静态IP地址。这一配置对于确保正常工作至关重要，因为每一台分支路由器都会在其配置中嵌入这一IP地址。

部署详情

本部分中的程序步骤为某些设置提供了示例。您所使用的实际设置和值取决于您当前的网络配置。本流程用于双DMVPN设计 (对每个DMVPN中枢路由器重复)，并同样用于DMVPN专用设计和DMVPN专用备份设计。

表 11 - 使用在部署案例中的参数

主机名	Loopback IP地址	Port Channel IP地址
VPN-ASR1002-1	10.4.32.243/32	10.4.32.18/30
VPN-ASR1002-2	10.4.32.244/32	10.4.32.22/30

流程

DMVPN中枢路由器配置

1、配置分布层交换机

2、配置广域网汇聚平台

3、配置到局域网的连接

4、配置VRF Lite

5、连接至互联网DMZ

6、配置ISAKMP和IPsec

7、配置mGRE隧道

8、配置EIGRP

程序 1 配置分布层交换机

读者提示

此流程假设分布层交换机已经按照《局域网部署指南》中的指导进行配置。本指南中仅包括支持将广域网汇聚路由器集成到部署中所需的程序。

局域网分布交换机是通往企业主要园区和数据中心的路径。一个三层端口通道接口连接分布层交换机和广域网汇聚路由器，内部路由协议在该接口上进行对等通信。

技术提示

作为一种最佳实践，请尽可能在链路两端使用相同的通道编号。

步骤 1: 配置三层端口通道接口并分配IP地址。

```
interface Port-channel3
 description VPN-ASR1002-1
 no switchport
 ip address 10.4.32.17 255.255.255.252
 ip pim sparse-mode
 logging event link-status
 carrier-delay msec 0
 no shutdown
```

步骤 2: 配置EtherChannel成员接口。

使用**channel-group**命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。port-channel和channel-group的编号必须匹配。并非所有的路由器平台都支持链路汇聚控制协议（LACP）并与交换机协商，

因此EtherChannel需静态配置。

此外，同时在出口配置QoS的宏命令，保证流量的优先级。

```
interface GigabitEthernet1/0/3
 description VPN-ASR1002-1 Gig0/0/0
!
interface GigabitEthernet2/0/3
 description VPN-ASR1002-1 Gig0/0/1
!
interface range GigabitEthernet1/0/3, GigabitEthernet2/0/3
  no switchport
  macro apply EgressQoS
  carrier-delay msec 0
  channel-group 3 mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

步骤 3: 允许路由协议在端口通道上形成邻居关系。

```
router eigrp 100
  no passive-interface Port-channel3
```

步骤 4: 这是从广域网分布层到核心侧汇总IP路由的最佳实践。配置连接到局域网核心层的接口，以汇总（summarize）广域网网络范围。

```
interface range TenGigabitEthernet1/1/1,
TenGigabitEthernet2/1/1
 ip summary-address eigrp 100 10.4.32.0 255.255.248.0
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

程序 2　配置广域网汇聚平台

在本设计中，有些特性和服务在所有广域网汇聚路由器间是相同的。这些系统设置能够简化并保护解决方案的管理。

步骤 1: 配置设备主机名

配置设备主机名称，以便轻松识别设备。

```
hostname VPN-ASR1002-1
```

步骤 2: 配置本地登录和密码。

本地的登录帐号和密码提供基本的设备访问身份认证来观察平台操作。通过使能密码获得访问设备配置模式。通过使能密码加密，可防止通过查看配置文件获取到在用的纯文本密码。

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

默认情况下，https访问交换机需使用使能密码做身份认证。

步骤 3: (可选)配置集中式用户身份认证。

随着网络规模的数量的扩大和设备维护的增加，维护每台设备上的本地用户帐号已成为较大的操作负荷。一个集中的身份认证、授权和审计（AAA）服务器可减少每台设备的操作任务，并提供用户访问审计日志，日志内容涵盖安全合规和根因分析。为访问控制启用AAA时，所有的访问网络基础设施（SSH和HTTPS）的管理都将通过AAA控制。

读者提示

本架构中使用AAA服务器是思科身份认证控制系统（ACS）。如需了解有关这ACS相关配置的详细信息，请参阅思科IBA智能业务平台《利用ACS部署设备管理指南》

TACACS+是用于验证基础架构设备上对AAA服务器管理登录主要的协议。此外，系统还针对每个网络基础设施设备定义了一个本地AAA用户数据库，用于在集中部署的TACACS+服务器不可用时，提供备用身份认证源。

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
```

```
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

步骤 4: 配置设备管理协议。

安全HTTP (HTTPS)和安全外壳(SSH)是HTTP和Telnet协议的安全替代品。它们使用安全套接字层(SSL)和传输层安全(TLS)提供了设备身份认证和数据加密功能。

SSH和HTTPS协议可实现对LAN设备的安全管理。这两个协议都进行加密，提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

通过在vty line下指定**transport preferred none**命令，从而避免错误连接尝试的提示显示在CLI窗口中。如果没有此命令，一旦ip name-server查找不可达，可能会发生因输错命令产生的长时间超时延迟。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

当启用同步记录未请求信息和调试报告时，在显示或打印交互式CLI输出结果后，控制台日志信息将在控制台上显示。借助这一命令，您可以在启用调试流程时，继续在设备控制台上输入信息。

```
line con 0
 logging synchronous
```

简单网络管理协议(SNMP)用于支持使用网络管理系统(NMS)管理网络基础设施设备。SNMPv2c针对只读和读写团体字符串(community string)进行了配置。

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

步骤 5: (可选)网络运营支撑聚焦于您可通过使用访问控制列表限制网络中可访问的设备来增强网络安全。在这个例子中，只有在10.4.48.0/24网段内的设备可以通过SSH或SNMP访问它。

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

技术提示

如果您在VTY接口上配置了一个access-list配置，当使用ssh登录时，您可能会失去从一台路由器到下一台的这种逐跳方式的排错能力。

步骤 6: 配置同步时钟。

网络时间协议(NTP)用于同步网络设备。NTP网络通常从权威时间源，如与时间服务器相连的无线电时钟或原子钟那里获取时间信息。然后NTP在企业网络中分发此信息。

您应将网络设备设定为与网络中的本地NTP服务器保持同步。本地NTP服务器通常会参考来自外部来源的更准确的时钟信息。通过对控制台消息、日志和调试报告进行配置，在输出时添加时间戳，您可以实现对网络中事件的交叉参考。

```
ntp server 10.4.48.17
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

步骤 7: 配置带内管理接口

回环接口是一个逻辑接口，只要设备通电且IP接口能接入网络，它就始终可连接。基于此功能，回环地址是带内管理交换机的最佳方法。三层进程和功能也捆绑于此回环接口，以确保进程永续性。

回环地址通常是一个带32位地址掩码的主机地址。从一个不属于任何其他内部

网络汇总范围的独特网络范围中分配回环地址。

```
interface Loopback 0
  ip address 10.4.32.243 255.255.255.255
  ip pim sparse-mode
```

ip pim sparse-mode命令将在该程序中做进一步介绍。

为SNMP, SSH, PIM, TACACS+ 和NTP绑定设备进程到回环接口地址，以实现最高永续性：

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

步骤 8: 配置IP单播路由

EIGRP面向局域网分布层或核心层进行配置。在这一设计中，端口通道接口和回环接口必须为EIGRP接口。回环接口可能仍然是被动接口。网络范围必须在单个网络声明或多个网络声明中包含这两个接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。

```
router eigrp 100
  network 10.4.0.0 0.1.255.255
  no auto-summary
  passive-interface default
  eigrp router-id 10.4.32.243
```

步骤 9: 配置IP组播路由。

IP 组播允许基础设施（路由器和交换机）复制单个IP数据流，然后将其从一个源设备发送到多个接收设备。与多个独立单播流或传播至所有地点的广播流相比，使用IP组播更为高效。IP电话MOH和IP视频广播数据流就是IP组播应用的两个实例。

为了接收特定的IP组播数据流，终端主机必须通过向其本地组播路由器发送IGMP消息，加入组播组。在传统的IP组播设计中，本地路由器会询问网络中充当RP的另一个路由器，将接收设备映射到活动源设备上，以便它们能够加入其数据流。

在此设计中，在稀疏模式组播基础上，思科使用任意播RP提供了一种简单但便于扩展的方法，能够支持高永续性RP环境。

在全局配置模式下，在平台上启用IP组播路由。

```
ip multicast-routing
```

Cisco ASR1000系列路由器需要**distributed**关键字。

```
ip multicast-routing distributed
```

必须配置每个三层交换机和路由器，以便利用autorp来发现IP组播RP。使用**ip pim autorp listener**命令，来支持跨稀疏模式链路的发现。这一配置支持在未来对IP组播环境进行扩展和控制，并可根据网络需求与设计进行变更。

```
ip pim autorp listener
```

网络中所有的三层接口均必须启用，以支持稀疏模式组播操作。

```
ip pim sparse-mode
```

程序 3 配置到局域网的连接

到邻接分布层的任何链路都应当是三层链路或三层以太通道(EtherChannel)。

步骤 1: 配置三层接口。

```
interface Port-channel3
  ip address 10.4.32.18 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

步骤 2: 配置EtherChannel成员接口。

使用channel-group命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。

```
interface GigabitEthernet0/0/0
 description WAN-D3750X Gig1/0/3
!
interface GigabitEthernet0/0/1
 description WAN-D3750X Gig2/0/3
!
interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  channel-group 3
  cdp enable
  no shutdown
```

步骤 3: 配置EIGRP接口

允许EIGRP在接口上形成邻居关系，以建立对等邻接性和交换路由表。

```
router eigrp 100
  no passive-interface Port-channel3
```

程序 4 配置VRF Lite

创建面向互联网的VRF，以支持面向DMVPN的FVRF。VRF名称可随意设定，但最好选择一个能够描述VRF的名称。要使VRF发挥作用，还必须配置相关的路由标识(RD)。RD配置也会创建路由和转发表，并将RD与VRF实例关联起来。

此设计使用了VRF Lite，从而可以任意选择RD值。当以类似的方式使用VRF时，最佳实践是在多个设备间使用相同的VRF/RD组合。然而，这一惯例并不要求严格遵循。

```
ip vrf INET-PUBLIC
 rd 65512:1
```

技术提示

命令参考:

RD或者与ASN相关（由一个ASN和一个任意数字组成），或者与IP地址相关（由一个IP地址和一个任意数字组成）。

您可以采用以下格式输入RD:

16位自治系统号码:您的32位数字

例如，65512:1。

32位IP地址：您的16位数字

例如，192.168.122.15:1。

程序 5 连接至互联网DMZ

DMVPN中枢路由器需要一个到互联网的连接。在这一设计中，DMVPN中枢路由器使用专为VPN端接路由器创建和配置的DMZ接口，通过Cisco ASA5500自适应安全设备进行连接。

步骤 1: 启用接口、选择VRF和分配IP地址

您用于DMVPN中枢路由器上面向互联网的接口的IP地址必须是互联网可路由的地址。这一任务可通过两种方法完成:

- 直接为路由器分配一个可路由的IP地址
- 直接为路由器分配一个不可路由的RFC-1918地址，使用Cisco ASA5500上的静态NAT将路由器IP地址转换为可路由的IP地址。

这一设计假定在Cisco ASA5500上为DMVPN中枢路由器配置了静态NAT。

DMVPN设计使用了FVRF，因此这一接口必须放置在上一程序配置的VRF中。

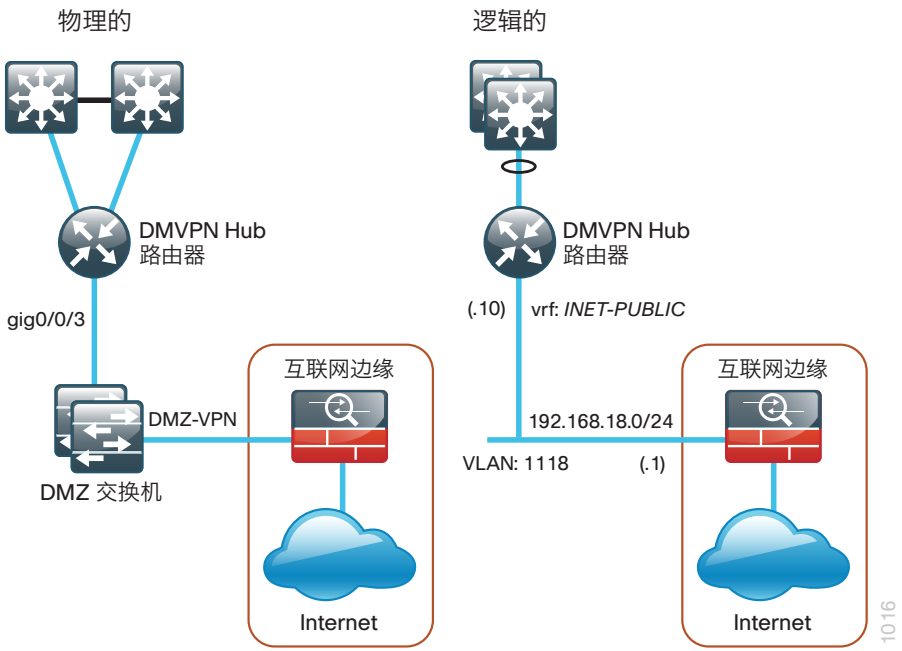
```
interface GigabitEthernet0/0/3
 ip vrf forwarding INET-PUBLIC
 ip address 192.168.18.10 255.255.255.0
 no shutdown
```

步骤 2: 配置VRF特定的缺省路由

为FVRF创建的VRF必须有其自己的到互联网的缺省路由。这一缺省路由指向ASA5500 DMZ接口IP地址。

```
ip route vrf INET-PUBLIC 0.0.0.0 0.0.0.0 192.168.18.1
```

图 22 - DMZ连接的物理和逻辑视图



程序 6　配置ISAKMP和IPsec

步骤 1: 配置crypto keyring。

crypto keyring针对特定VRF中可到达的IP源，定义了一个预共享密钥（或密码）。如应用于任意IP源，该密钥是一个通配预共享密钥。通配密钥使用0.0.0.0 0.0.0.0网络/掩码组合进行配置。

```
crypto keyring DMVPN-KEYRING vrf INET-PUBLIC
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

步骤 2: 配置ISAKMP策略。

面向DMVPN的ISAKMP策略采用如下规则：

- 基于256位密钥的高级加密标准（AES）
- 安全哈希标准（SHA）
- 使用预共享密钥(PSK)进行身份认证
- Diffie-Hellman组：　2

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
```

步骤 3: 创建ISAKMP配置文件

ISAKMP配置文件将身份地址、VRF和crypto keyring关联起来。VRF内的通配地址标注为0.0.0.0。

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC
   keyring DMVPN-KEYRING
   match identity address 0.0.0.0 INET-PUBLIC
```

步骤 4: 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合，应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

面向DMVPN的IPsec转换集采用如下规则：

- 采用256位AES加密算法的ESP
- 采用SHA（HMAC变体）身份认证算法的ESP

由于DMVPN中枢路由器在NAT设备后端，IPsec转换必须针对传输模式进行配置。

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
 mode transport
```

步骤 5: 创建IPSec配置文件

IPsec配置文件将ISAKMP配置文件和IPsec转换集关联起来。

```
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC
```

程序 7　配置mGRE隧道

表 12 - DMVPN隧道参数

DMVPN云	隧道IP地址	EIGRP AS	NHRP网络ID
主用	10.4.34.1/23	200	101
备用	10.4.36.1/23	201	102

步骤 1: 配置基本接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定，但最好从10或更大的数字开始编号，这是因为这一设计中部署的其他特性也可能需要使用隧道，它们可能在缺省情况下选择了较小的数字。

带宽设置应与相应的主要或辅助运营商的互联网带宽相匹配。

将IP MTU配置为1400，将ip tcp adjust-mss配置为1360。二者之间有40字节的差异，这一差异与IP和TCP报头的总长度对应。

```
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

步骤 2: 配置隧道。

DMVPN使用多点GRE (mGRE)隧道。这一隧道类型仅需要一个源接口。请使用您用于连接互联网的同一源接口。将**tunnel vrf**命令设置到之前为FVRF定义的VRF上。

在这一接口上启用加密要求采用在上一程序中配置的IPsec配置文件。

```
interface Tunnel10
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC
 tunnel protection ipsec profile DMVPN-PROFILE
```

步骤 3: 配置NHRP。

DMVPN中枢路由器充当着所有分支路由器的NHRP服务器的角色。NHRP供远程路由器使用，来为mGRE隧道连接的对等体确定隧道目的地。

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份认证密钥。NHRP缓存保持时间应被设置为600秒。

EIGRP（在以下程序中配置）依赖于组播传输方案，并需要NHRP自动向组播NHRP映射中添加路由器。

ip nhrp redirect命令允许DMVPN中枢路由器告知分支路由器存在到目的地网络的更佳路径。DMVPN分支到分支直接通信可能需要这一功能。

```
interface Tunnel10
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
```

步骤 4: 为DMVPN隧道启用PIM非广播多点接入(NBMA)模式。

分支到分支DMVPN网络带来了一种独特的挑战，因为分支路由器彼此间不能直接交换信息，即使它们处于相同的逻辑网络中也不行。无法直接交换信息可能会导致在运行IP组播时发生问题。

为了解决这一问题，需要采用一种单独跟踪每个远程PIM邻接设备加入信息的方法。PIM NBMA模式下的路由器会假定，每一个远程PIM邻接设备均已通过点对点链路连接至路由器。

技术提示

不要在互联网DMZ接口上启用PIM，这一接口不得用于请求组播流量。

```
interface Tunnel10
 ip pim sparse-mode
 ip pim nbma-mode
```

步骤 5: 配置EIGRP。

您在下面的的程序 8中配置EIGRP, 但是针对您需要首先配置的mGRE隧道接口有一些具体的要求。

分支到分支DMVPN网络带来了一种独特的挑战, 因为分支路由器彼此间不能直接交换信息, 即使它们处于相同的逻辑网络中也不行。这一限制要求DMVPN中枢路由器通告来自同一网络上其他分支的路由。这些路由的通告通常会被水平分割 (split horizon) 所阻止, 并被no ip split-horizon eigrp命令所越过。

EIGRP问候间隔增加到20秒, EIGRP保持时间增加到60秒, 以便在一个DMVPN云上支持多达500个远端站点。

```
interface Tunnel10
 ip hello-interval eigrp [EIGRP AS] 20
 ip hold-time eigrp [EIGRP AS] 60
 no ip split-horizon eigrp [EIGRP AS]
```

程序 8 配置EIGRP

您在DMVPN中枢路由器上使用两个EIGRP进程。增加一个进程主要是为了确保从广域网远端站点中获知的路由, 能够在广域网分布层交换机上显示为EIGRP外部路由。如果您仅使用了一个进程, 远端站点路由将在广域网分布层交换机上显示为EIGRP内部路由。任何MPLS VPN获知的路由都适于使用这一方法。

步骤 1: 为DMVPN启用额外的EIGRP进程。

为DMVPN mGRE接口配置EIGRP。来自其他EIGRP进程的路由被重分布。由于路由协议相同, 因此无需缺省metric (度量值) 。

隧道接口是唯一的EIGRP接口, 您需要明确列出其网络范围。

```
router eigrp [EIGRP AS]
 network 10.4.34.0 0.0.1.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.4.32.243
 no auto-summary
```

步骤 2: 标记与重分布路由。

本设计使用相互的路由重分发。EIGRP-200/EIGRP201上的DMVPN路由被重分发到EIGRP-100上, 从EIGRP-100上学习到的路由也被重分发到EIGRP-200/EIGRP201上。因为使用相同的路由协议, 无需使用缺省权值 (default metrics) 。

当采用了这一共同路由重分布时, 密切控制路由信息如何在不同路由协议间共享十分重要。否则, 将有可能遭遇路由翻动——某些路由会从设备路由表中重复安装和撤销。正确的路由控制保障了路由表的稳定。

在广域网汇聚路由器上使用的入站发布列表用于限制哪些路由能够被安装到路由表中。这些路由器被配置成只接受非起源于MPLS和DMVPN广域网的路由。要完成这一任务, DMVPN中枢路由器在路由重分布过程中必须对DMVPN获知的广域网路由进行明确标记。所用的具体路由标记如下表所示。

表 13 - DMVPN中枢路由器的路由标记信息

标记	路由来源	标记方法	动作
65401	MPLS A	隐含	接受
65402	MPLS B	隐含	接受
300	二层广域网	显式	接受
65512	DMVPN中枢路由器	显式	标记

本例中包含了参考设计中的所有广域网路由来源。根据您网络的实际设计, 您可能需要使用更多标记。

```
router eigrp 100
 redistribute eigrp [EIGRP AS] route-map SET-ROUTE-TAG-DMVPN
!
router eigrp [EIGRP AS]
 redistribute eigrp 100
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65512
```

流程

防火墙和DMZ交换机配置

1、配置DMZ交换机

2、配置防火墙DMZ接口

3、配置网络地址转换

4、配置安全策略

程序 1 配置DMZ交换机

读者提示

此程序假设层交换机已经按照《局域网部署指南》中的指导进行了配置。仅包括支持将防火墙集成到部署中所需的程序。

步骤 1: 针对包含DMVPN中枢路由器的VLAN，将DMZ交换机设定为生成树根。

```
vlan 1118
spanning-tree vlan 1118 root primary
```

步骤 2: 将连接到设备的接口配置为中继。

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1118
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

步骤 3: 配置连接到DMVPN中枢路由器的接口。如果有必要，重复该步骤。

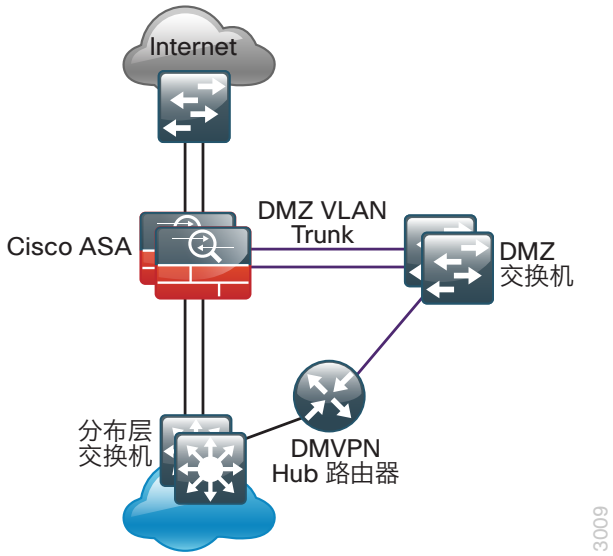
```
interface GigabitEthernet1/0/7
 description VPN-ASR1002-1 Gig0/0/3
 switchport access vlan 1118
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

程序 2 配置防火墙DMZ接口

防火墙的隔离区(DMZ)是网络的一个区域，这个区域与其它网络区域之间的流量往来受到严格限制。企业可将网络服务放在DMZ，使其向互联网开放。除非在特殊情况下，这些服务器通常不能向‘内部’网络发起连接请求。

DMZ网络通过VLAN中继和appliance的千兆以太网接口连接到appliance，以便在必须增加新的VLAN来连接更多DMZ时实现最大的灵活性。中继(trunk)将appliance连接到一个3750X接入交换机堆叠，以提供永续性。Cisco ASA上的每个DMZ VLAN接口都将获得一个IP地址，作为每个VLAN子网的默认网关。DMZ交换机只提供二层交换功能；DMZ交换机的VLAN接口未分配IP地址，只有一个VLAN接口带有一个IP地址，用于对交换机进行管理。

图 23 - DMZ VLAN拓扑和服务



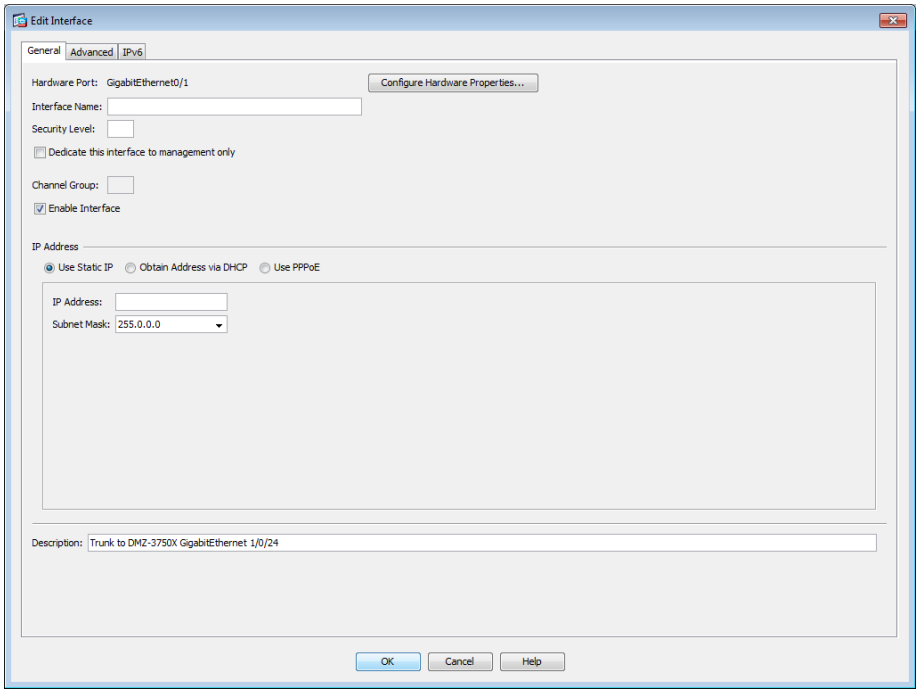
技术提示

通过将DMZ连接设置为一个VLAN中继，您将获得最大的灵活性。

步骤 1: 在**Configuration (配置) > Device Setup (设备设置) > Interfaces (接口)** 中，单击连接到DMZ交换机的接口。(例如: GigabitEthernet0/1)

步骤 2: 单击**Edit (编辑)** 。

步骤 3: 选择**Enable Interface (启用接口)**，然后单击**OK**。



步骤 4: 在Interface (接口) 窗格中，单击**Add (添加) > Interface (接口)** 。

步骤 5: 在**Hardware Port (硬件端口)** 列表中，选择步骤 1中配置的接口。(例如: GigabitEthernet0/1)

步骤 6: 在**VLAN ID**框中，输入DMZ VLAN的VLAN号。(例如: 1118)

步骤 7: 在**Subinterface ID (子接口ID)** 框中，输入DMZ VLAN的VLAN号。(例如: 1118)

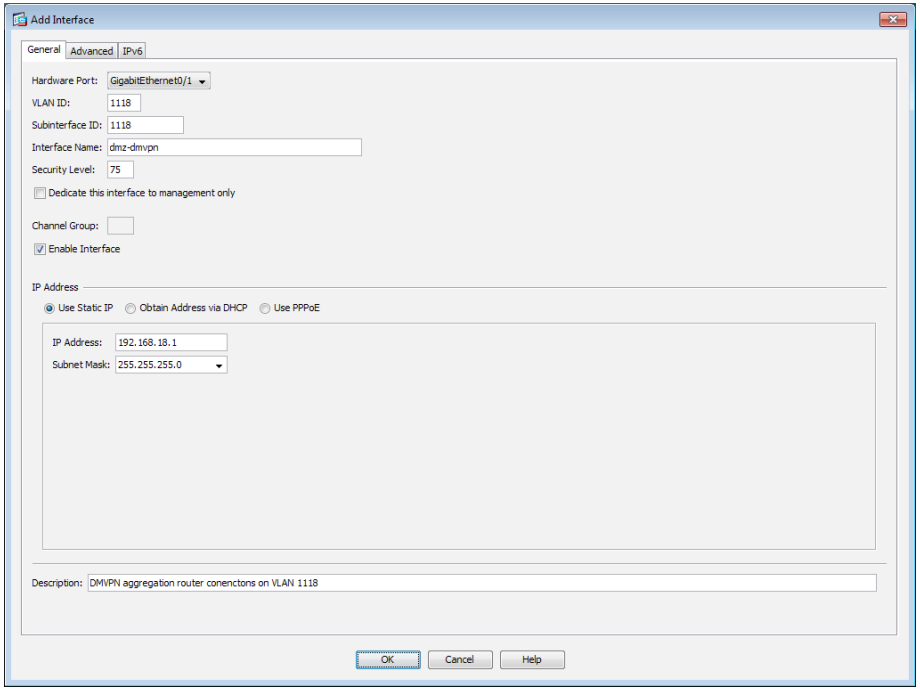
步骤 8: 输入一个**接口名称**。(例如: dmz-dmvpn)

步骤 9: 在**Security Level (安全级别)** 框中，输入值75。

步骤 10: 输入接口**IP Address (IP地址)** 。(例如: 192.168.18.1)

步骤 11: 输入接口**Subnet Mask (子网掩码)**，然后单击**OK**。(例如: 255.255.255.0)

步骤 12: 单击**Apply (应用)**

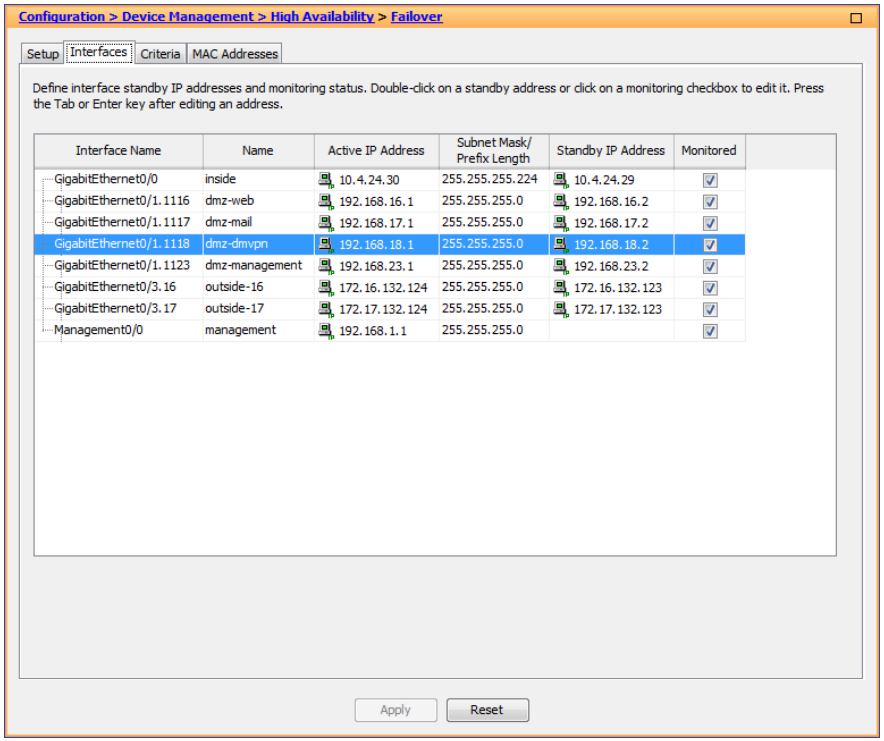


步骤 13: 在**Configuration (配置) > Device Management (设备管理) > High Availability (高可用性)** 中，单击**Failover (故障切换)**。

步骤 14: 在**Interfaces (接口)** 选项卡上，对于在步骤 4中创建的接口，在**Standby IP address (备用IP地址)** 列中输入备用设备的IP地址。(例如: 192.168.18.2)

步骤 15: 选择**Monitored (受监视)**。

步骤 16: 单击**Apply (应用)**。



程序 3 配置网络地址转换

DMZ网络使用的专用网(RFC 1918)地址无法在互联网上路由，因此防火墙必须将DMVPN中枢路由器的DMZ地址转换为外部公共地址。

下表中以示例方式列出了与DMZ地址相对应的公共IP地址。

DMVPN中枢路由器DMZ地址	DMVPN中枢路由器公共地址 (NAT转换后外部可路由的地址)
192.168.18.10	172.16.130.1 (ISP-A)
192.168.18.11	172.17.130.1 (ISP-B)

步骤 1: 在**Configuration (配置) > Firewall (防火墙) > Objects (对象)** 中，单击**Network Objects/Groups (网络对象/组)**。

首先，在主要互联网连接上，为DMVPN中枢路由器的公共地址添加一个网络对

象。

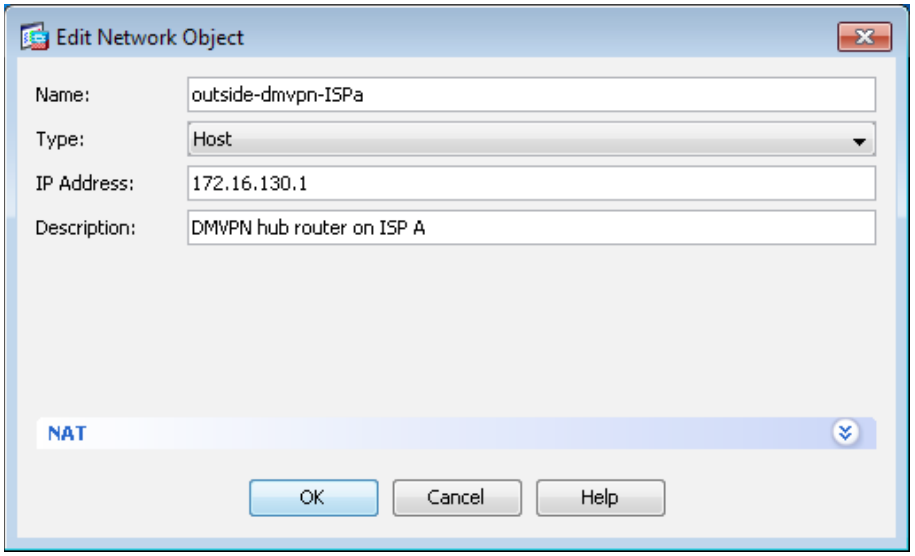
步骤 2: 单击**Add (添加) > Network Object (网络对象)**。

步骤 3: 在Add Network Object (添加网络对象) 对话框上, 在**Name box** (名称框) 中, 为DMVPN中枢路由器的公共IP地址输入一个描述。(例如: outside-dmvpn-ISPa)

步骤 4: 在**Type (类型)** 列表中, 选择**Host (主机)**。

步骤 5: 在**IP Address (IP地址)** 框中, 输入DMVPN中枢路由器的公共IP地址, 然后单击**OK**。(例如: 172.16.130.1)

步骤 6: 单击**Apply (应用)**。



接下来, 您可以为DMVPN中枢路由器的专用DMZ地址添加一个网络对象。

步骤 7: 单击**Add (添加) > Network Object (网络对象)**。

步骤 8: 在**Add Network Object (添加网络对象)** 对话框中, 在**Name box (名称框)** 中, 为DMVPN中枢路由器的专用DMZ IP地址输入一个描述。(例如: dmz-dmvpn-1)

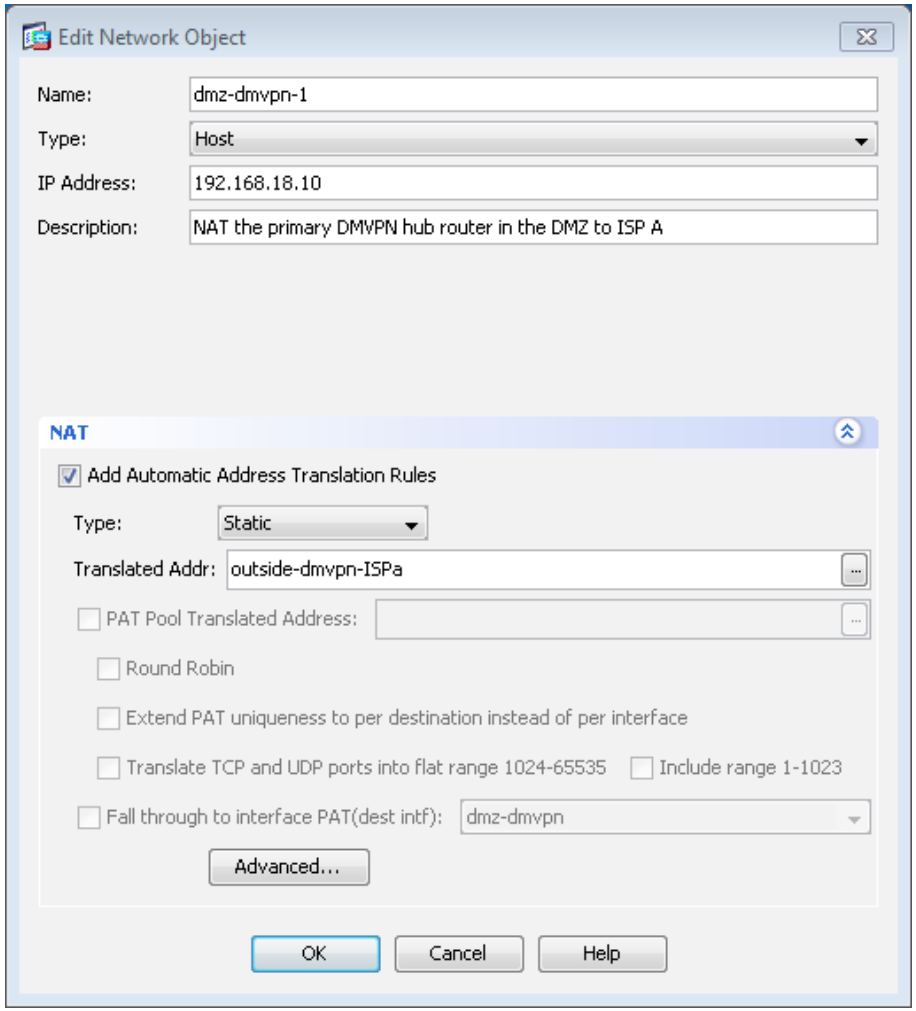
步骤 9: 在**Type (类型)** 列表中, 选择**Host (主机)**。

步骤 10: 在**IP Address (IP地址)** 框中, 输入路由器的DMZ IP地址。(例如: 192.168.18.10)

步骤 11: 单击双向下箭头。NAT窗格会展开。

步骤 12: 选择**Add Automatic Address Translation Rules (添加自动地址转换规则)**。

步骤 13: 在**Translated Addr (转换的地址)** 列表中, 选择在步骤 2中创建的网络对象, 然后单击OK。



步骤 14: 为永续的DMVPN中枢路由器重复该过程。

程序 4 配置安全策略

DMVPN DMZ提供了一个额外的保护层，以减少某些类型的DMVPN路由器配置错误的可能性。这些路由器用于将业务网络与互联网相连通。一个过滤器仅允许DMVPN相关的流量到达DMVPN中枢路由器。

表 14 - 要求的DMVPN协议（汇聚路由器）

名称	协议	用途
non500-isakmp	UDP 4500	经由NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

表 15 - 可选协议—DMVPN汇聚路由器

名称	协议	用途
icmp echo	ICMP Type 0, Code 0	允许远程ping
icmp echo-reply	ICMP Type 8, Code 0	允许ping回复（根据我们的请求）
icmp ttl-exceeded	ICMP Type 11, Code 0	允许跟踪路由回复（根据我们的请求）
icmp port-unreachable	ICMP Type 3, Code 3	允许跟踪路由回复（根据我们的请求）
UDP high ports	UDP > 1023	允许远程跟踪路由

步骤 1: 转至**Configuration（配置） > Firewall（防火墙）> Access Rules（访问规则）**。

步骤 2: 在Global rules(全局规则)内展开Global rules（全球规则），单击拒绝从DMZ到其他网络的流量。

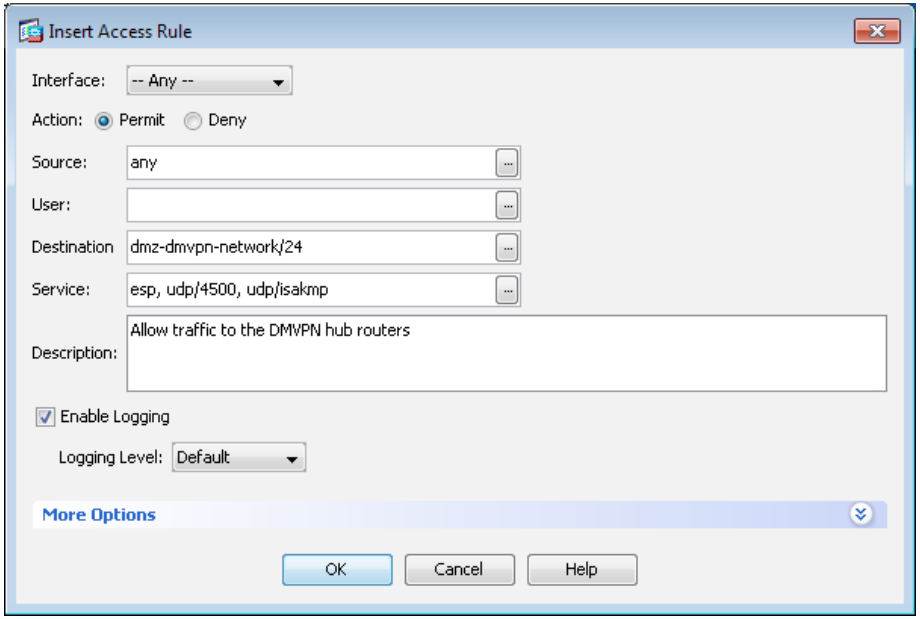
接下来，您必须在您选择的规则之上插入一个新的规则。

步骤 3: 单击Add **（添加）> Insert（插入）**。.

您必须启用DMVPN远端路由器，以便与DMZ中的DMVPN中枢路由器进行通信。

步骤 4: 在**Destination（目的地）**列表中，选择程序 3中创建的网络对象组。（例如：dmz-dmvpn-network/24）

步骤 5: 在**Service（服务）**列表框中，输入**esp， udp/4500， udp/isakmp**，然后单击**OK**。



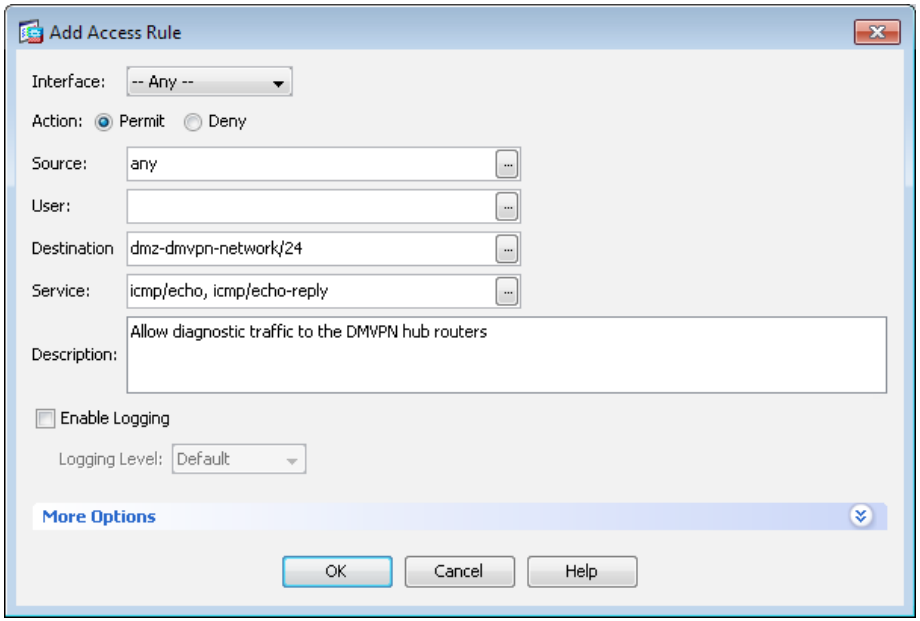
接下来，您必须插入一个新规则，以允许诊断流量到达DMVPN中枢路由器。

步骤 6: 单击**Add（添加）> Insert（插入）**。

您必须启用DMVPN远端路由器，以便发送诊断到DMZ中的DMVPN汇聚路由器。

步骤 7: 在**Destination（目的地）**列表中，选择为DMVPN DMZ自动创建的网络对象。（例如：dmz-dmvpn-network/24）

步骤 8: 在**Service (服务)** 列表框中, 输入**icmp/echo， icmp/echo-reply**, 然后单击OK



步骤 9: 单击**Apply (应用)** 。

流程

添加DMVPN中枢到现存的广域网汇聚路由器

1、配置ISAKMP and IPsec

2、配置mGRE隧道

3、配置EIGRP

4、在防火墙桑配置NAT

5、在防火墙上配置安全策略

VPN备份在更小规模部署中可使用现存的MPLS广域网路由器作为DMVPN中枢路由器。该流程假设MPLS广域网路由器已经配置，且使用静态路由作为MPLS承载。本流程用于DMVPN共享备份设计。

技术提示

本流程不需要FVRF。

程序 1 配置ISAKMP and IPsec

步骤 1: 配置crypto keyring。

crypto keyring针对特定VRF中可到达的IP源，定义了一个预共享密钥 (或密码) 。如应用于任意IP源，该密钥是一个通配预共享密钥。通配密钥使用0.0.0.0 0.0.0.0网络/掩码组合进行配置。

```
crypto keyring DMVPN-KEYRING
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

步骤 2: 配置ISAKMP策略。

面向DMVPN的ISAKMP策略采用如下规则:

- 基于256位密钥的高级加密标准 (AES)
- 安全哈希标准 (SHA)
- 使用预共享密钥(PSK)进行身份认证
- Diffie-Hellman组: 2

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
```

步骤 3: 创建ISAKMP配置文件

ISAKMP配置文件将身份地址、VRF和crypto keyring关联起来。VRF内的通配地址标注为0.0.0.0。

```
crypto isakmp profile ISAKMP-PROFILE
   keyring DMVPN-KEYRING
   match identity address 0.0.0.0
```

步骤 4: 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合, 应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

面向DMVPN的IPsec转换集采用如下规则:

- 采用256位AES加密算法的ESP
- 采用SHA (HMAC变体) 身份认证算法的ESP

由于DMVPN中枢路由器在NAT设备后端, IPsec转换必须针对传输模式进行配置。

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
 mode transport
```

步骤 5: 创建IPSec配置文件

IPsec配置文件将ISAKMP配置文件和IPsec转换集关联起来。

```
crypto ipsec profile DMVPN-PROFILE
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile ISAKMP-PROFILE
```

程序 2 配置mGRE隧道

表 16 - DMVPN隧道参数

DMVPN云	隧道IP地址	EIGRP AS	NHRP网络ID
主用	10.4.34.1/24	200	101

步骤 1: 配置基本的接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定, 但最好从10或更大的数字开始编号, 这是因为这一设计中部署的其他特性也可能需要使用隧道, 它们可能在缺省情况下选择了较小的数字。

带宽设置应与相应的主要或辅助运营商的互联网带宽相匹配。

将IP MTU配置为1400, 将ip tcp adjust-mss配置为1360。二者之间有40字节的差异, 这一差异与IP和TCP报头的总长度对应。

```
interface Tunnel10
 bandwidth 10000
 ip address 10.4.34.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

步骤 2: 配置隧道。

DMVPN使用多点GRE (mGRE)隧道。这一隧道类型仅需要一个源接口。请使用您用于连接互联网的同一源接口。

在这一接口上启用加密要求采用在上一程序中配置的IPsec配置文件。

```
interface Tunnel10
 tunnel source Port-Channel32
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN-PROFILE
```

步骤 3: 配置NHRP。

DMVPN中枢路由器充当着所有分支路由器的NHRP服务器的角色。NHRP供远程路由器使用, 来为mGRE隧道连接的对等体确定隧道目的地。

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份认证密钥。NHRP缓存保持时间应被设置为600秒。

EIGRP（在以下程序中配置）依赖于组播传输方案，并需要NHRP自动向组播NHRP映射中添加路由器。

ip nhrp redirect命令允许DMVPN中枢路由器告知分支路由器存在到目的地网络的更佳路径。DMVPN分支到分支直接通信可能需要这一功能。

```
interface Tunnel10
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp redirect
```

步骤 4: 为DMVPN隧道开启PIM非广播多路访问（NBMA）模式。

分支到分支DMVPN网络带来了一种独特的挑战，因为分支路由器彼此间不能直接交换信息，即使它们处于相同的逻辑网络中也不行。无法直接交换信息可能会导致在运行IP组播时发生问题。

为了解决这一问题，需要采用一种单独跟踪每个远程PIM邻接设备加入信息的方法。PIM NBMA模式下的路由器会假定，每一个远程PIM邻接设备均已通过点对点链路连接至路由器。

技术提示

不要在互联网DMZ接口上启用PIM，这一接口不得用于请求组播流量。

```
interface Tunnel10
 ip pim sparse-mode
 ip pim nbma-mode
```

步骤 5: 配置EIGRP。

您在下面的的程序 3中配置EIGRP，但是针对您需要首先配置的mGRE隧道接口有一些具体的要求。

分支到分支DMVPN网络带来了一种独特的挑战，因为分支路由器彼此间不能直接交换信息，即使它们处于相同的逻辑网络中也不行。这一限制要求DMVPN中枢路由器通告来自同一网络上其他分支的路由。这些路由的通告通常会被水平分割（split horizon）所阻止，并被**no ip split-horizon eigrp**命令所越过。

EIGRP问候间隔增加到20秒，EIGRP保持时间增加到60秒，以便在一个DMVPN云上支持多达500个远端站点。

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
 no ip split-horizon eigrp 200
```

程序 3 配置EIGRP

您在DMVPN中枢路由器上使用两个EIGRP进程。增加一个进程主要是为了确保从广域网远端站点中获知的路由，能够在广域网分布层交换机上显示为EIGRP外部路由。如果您仅使用了一个进程，远端站点路由将在广域网分布层交换机上显示为EIGRP内部路由。任何MPLS VPN获知的路由都适于使用这一方法。

步骤 1: 为DMVPN启用额外的EIGRP进程。

为DMVPN mGRE接口配置EIGRP-200。来自其他EIGRP进程的路由被重分布。由于路由协议相同，因此无需缺省metric（度量值）。

隧道接口是唯一的EIGRP接口，您需要明确列出其网络范围。

```
router eigrp 200
 network 10.4.34.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.4.32.254
 no auto-summary
```

步骤 2: 标记与重分布路由。

本设计使用相互的路由重分发。EIGRP-200上的DMVPN路由被重分发到EIGRP-100上，从EIGRP-100上学习到的路由也被重分发到EIGRP-200上。因为使用相同的路由协议，无需使用缺省权值（default metrics）。

当采用了这一共同路由重分布时，密切控制路由信息如何在不同路由协议间共享十分重要。否则，将有可能遭遇路由翻动—某些路由会从设备路由表中重复安装

和撤销。正确的路由控制保障了路由表的稳定。

在广域网汇聚路由器上使用的入站发布列表用于限制哪些路由能够被安装到路由表中。这些路由器被配置成只接受非起源于MPLS和DMVPN广域网的路由。要完成这一任务，DMVPN中枢路由器在路由重分布过程中必须对DMVPN获知的广域网路由进行明确标记。

本例中包含了参考设计中的所有广域网路由来源。根据您网络的实际设计，您可能需要使用更多标记。

```
router eigrp 100
 redistribute eigrp 200 route-map SET-ROUTE-TAG-DMVPN
!
router eigrp 200
 redistribute eigrp 100
!
route-map SET-ROUTE-TAG-DMVPN permit 10
 match interface Tunnel10
 set tag 65512
```

程序 4　在防火墙桑配置NAT

读者提示

本程序假设防火墙已参考如下指导《防火墙和IPS部署指南》做过配置。本程序还包括了需要允许VPN协议穿越防火墙，该操作仅在本程序使用。

DMVPN中枢路由器连接至网络核心，并位于互联网边缘防火墙的后面。互联网边缘ASA必须转发所有去往路由器私有IP地址的入向VPN流量，并在ASA的出向到入向（outside-to-inside）访问策略中容纳VPN流量。

内部网络使用的专用网(RFC 1918)地址无法在互联网上路由，因此防火墙必须将DMVPN中枢路由器的面向核心/分布的地址转换为外部公共地址。

下表中以示例方式列出了与内部地址相对应的公共IP地址。

DMVPN中枢路由器内部地址	DMVPN中枢路由器公共地址（NAT转换后外部可路由的地址）
10.4.32.2	172.16.130.1

步骤 2: 在**Configuration（配置） > Firewall（防火墙） > Objects（对象）**中，单击**Network Objects/Groups（网络对象/组）**。

首先，在主要互联网连接上，为DMVPN中枢路由器的公共地址添加一个网络对象。

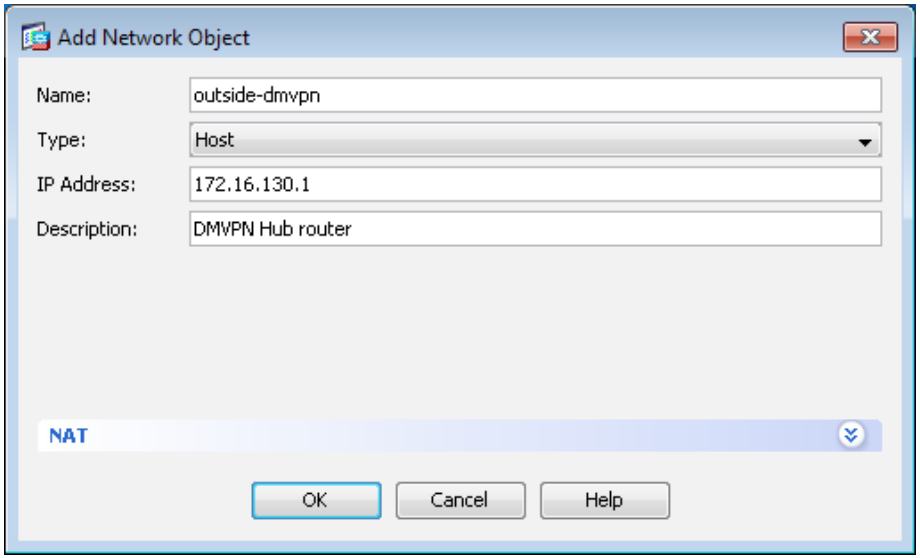
步骤 3: 单击**Add（添加）> Network Object（网络对象）**。

步骤 4: 在Add Network Object（添加网络对象）对话框上，在**Name box**（名称框）中，为DMVPN中枢路由器的公共IP地址输入一个描述。（例如：outside-dmvpn）

步骤 5: 在**Type（类型）**列表中，选择**Host（主机）**。

步骤 6: 在**IP Address（IP地址）**框中，输入DMVPN中枢路由器的公共IP地址，然后单击**OK**。（例如：172.16.130.1）

步骤 7: 单击**Apply (应用)**。



接下来, 您可以为DMVPN中枢路由器的私有内部地址添加一个网络对象。

步骤 8: 单击**Add (添加) > Network Object (网络对象)**。

步骤 9: 在**Add Network Object (添加网络对象)** 对话框中, 在**Name box (名称框)** 中, 为DMVPN中枢路由器的私有内部IP地址输入一个描述。(例如: internal-dmvpn-1)

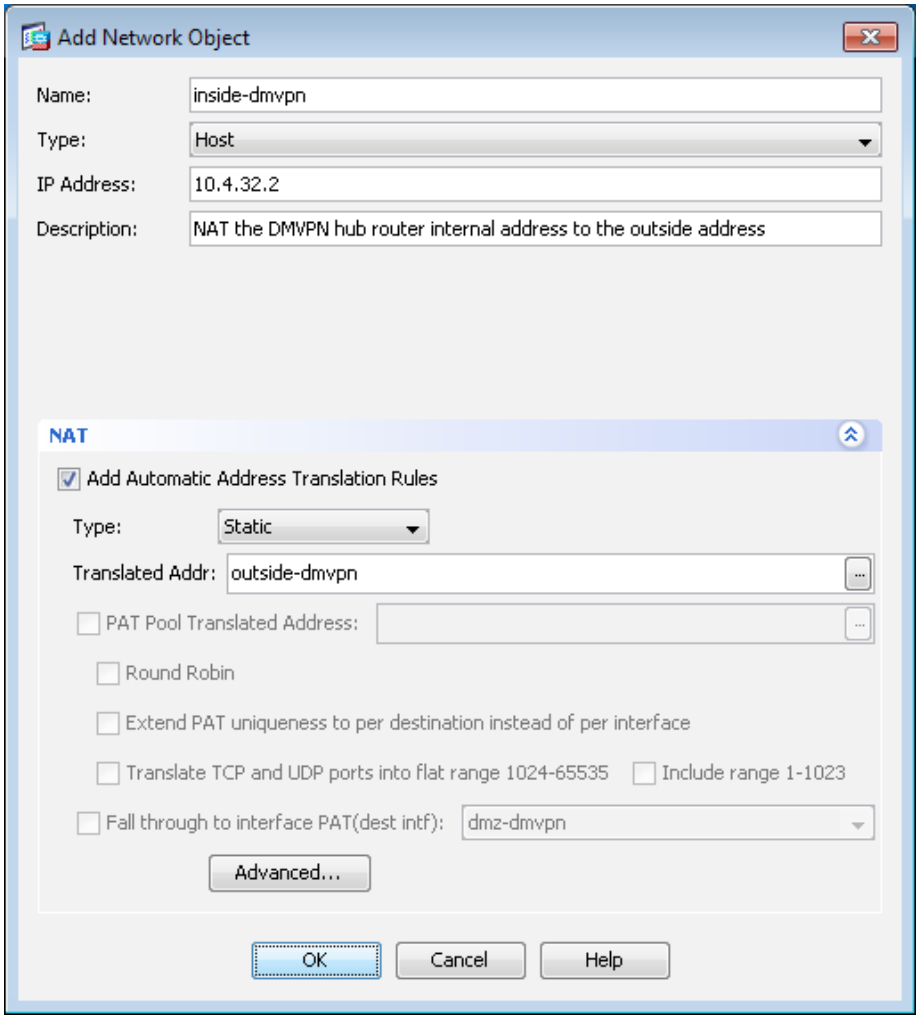
步骤 10: 在**Type (类型)** 列表中, 选择**Host (主机)**。

步骤 11: 在**IP Address (IP地址)** 框中, 输入路由器的私有内部IP地址。(例如: 10.4.32.2)

步骤 12: 单击双向下箭头。NAT窗格会展开。

步骤 13: 选择**Add Automatic Address Translation Rules (添加自动地址转换规则)**。

步骤 14: 在**Translated Addr (转换的地址)** 列表中, 选择在步骤 2中创建的网络对象, 然后单击**OK**。



步骤 15: 单击**Apply (应用)**。

程序 5 在防火墙上配置安全策略

一个过滤器仅允许DMVPN相关的流量到达DMVPN中枢路由器。

表 17 - 要求的DMVPN协议 (汇聚路由器)

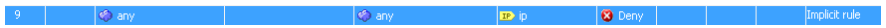
名称	协议	用途
non500-isakmp	UDP 4500	经由NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec

表 18 - 可选协议—DMVPN汇聚路由器

名称	协议	用途
icmp echo	ICMP Type 0, Code 0	允许远程ping
icmp echo-reply	ICMP Type 8, Code 0	允许ping回复 (根据我们的请求)
icmp ttl-exceeded	ICMP Type 11, Code 0	允许跟踪路由回复 (根据我们的请求)
icmp port-unreachable	ICMP Type 3, Code 3	允许跟踪路由回复 (根据我们的请求)
UDP high ports	UDP > 1023	允许远程跟踪路由

步骤 1: 转至**Configuration (配置) > Firewall (防火墙) > Access Rules (访问规则)**。

步骤 2: 在Global rules(全局规则)内展开Global rules (全球规则), 单击拒绝从任意到任意的流量。



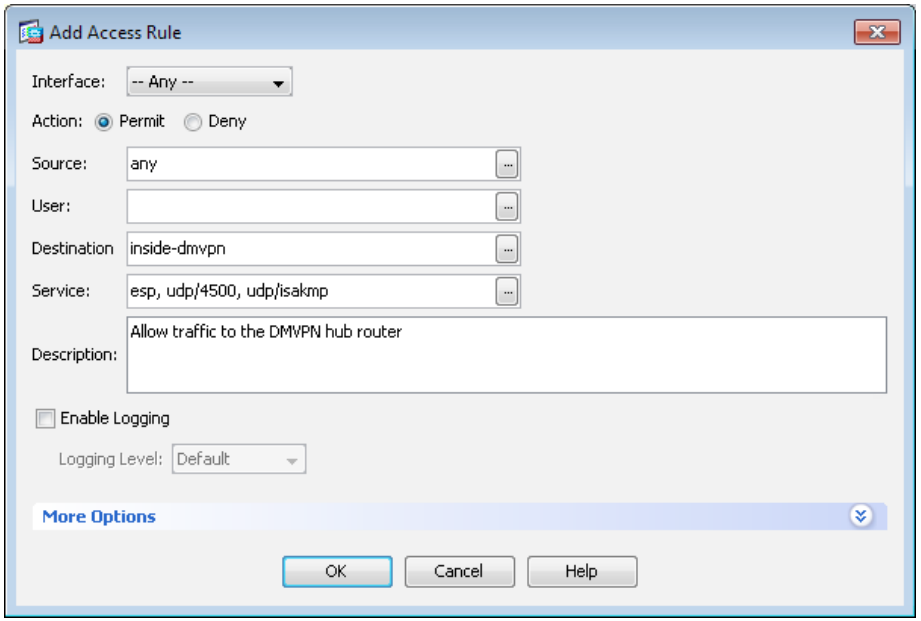
接下来, 您必须在您选择的规则之上插入一个新的规则。

步骤 3: 单击Add **(添加) > Add Access Rule (添加访问规则)**。

您必须启用DMVPN远端路由器, 以便与内部网络中的DMVPN中枢路由器进行通信。

步骤 4: 在**Destination (目的地)** 列表中, 选择程序 4中创建的网络对象组。(例如: inside-dmvpn)

步骤 5: 在**Service (服务)** 列表框中, 输入**esp, udp/4500, udp/isakmp**, 然后单击**OK**。



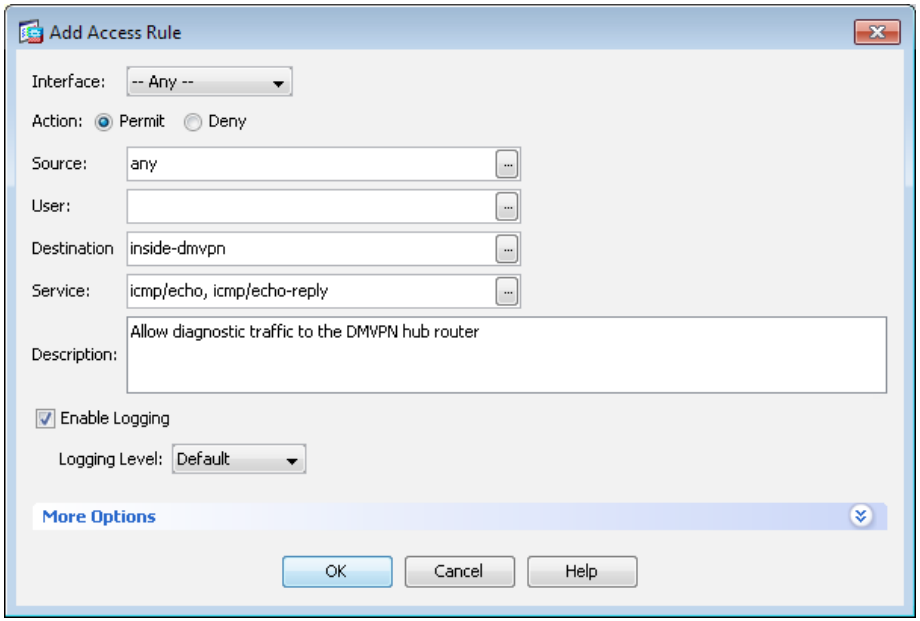
接下来, 您必须插入一个新规则, 以允许诊断流量到达DMVPN中枢路由器。

步骤 6: 单击**Add (添加) > Add Access Rule (添加访问规则)**。

步骤 7: 您必须启用DMVPN远端路由器, 以便发送诊断到DMVPN汇聚路由器。

步骤 8: 在**Destination (目的地)** 列表中, 选择创建在程序 4中的host network object (主机网络对象)。(例如: inside-dmvpn)

步骤 9: 在**Service (服务)** 列表框中, 输入**icmp/echo, icmp/echo-reply**, 然后单击**OK**。



步骤 10: 单击**Apply (应用)**。

流程

远端站点DMVPN分支路由器配置

1、配置广域网远端路由器

2、配置VRF Lite

3、连接到Internet

4、配置ISAKMP和IPsec

5、配置mGRE隧道

6、配置EIGRP

7、配置IP组播路由

8、连接路由器至接入层交换机

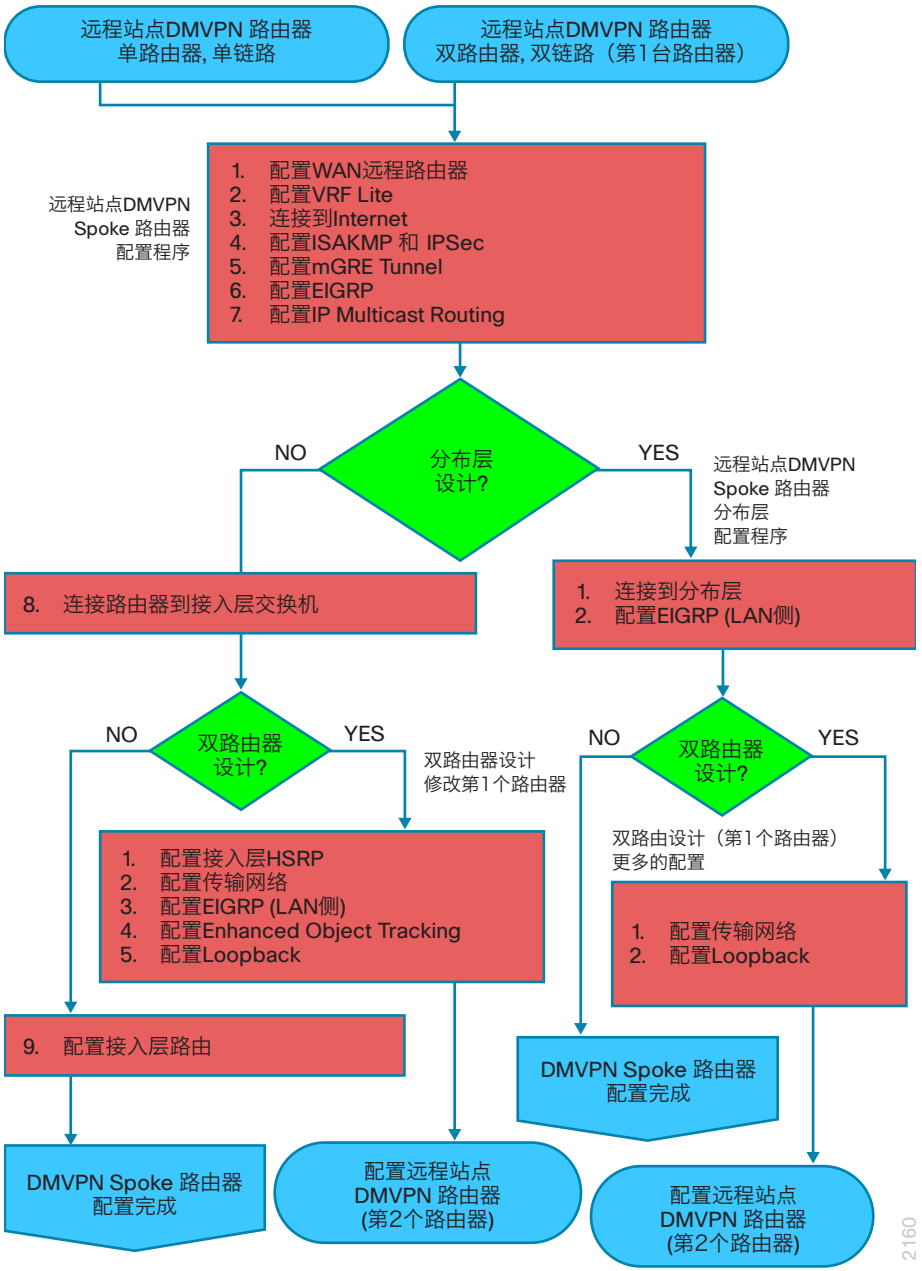
9、配置接入层接口

本套程序详述了DMVPN分支路由器、DMVPN远端站点 (单路由器, 单链路) 的配置, 并包含了所有必须的过程。

在您配置一个DMVPN + DMVPN远端站点时, 您应同样使用这组程序。当您配置双路由器、双链路设计的第一台路由器时, 可以使用这些程序。

下面的流程图详细介绍了如何配置远端站点DMVPN分支路由器。

图 24 - 远端DMVPN分支路由器配置流程图



程序 1 配置广域网远端路由器

在本设计中, 有些特性和服务在所有广域网远端站点路由器间是相同的。这些系统设置能够简化并保护解决方案的管理。

步骤 1: 配置设备主机名称, 以便轻松识别设备。

```
hostname [hostname]
```

步骤 2: 配置本地登录和密码。

本地的登录帐号和密码提供基本的设备访问身份认证来观察平台操作。通过使能密码获得访问设备配置模式。通过使能密码加密, 可防止通过查看配置文件获取到在用的纯文本密码。

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

默认情况下, https访问交换机需使用使能密码做身份认证。

步骤 3: (可选)配置集中式用户身份认证。

随着网络规模的数量的扩大和设备维护的增加, 维护每台设备上的本地用户帐号已成为较大的操作负荷。一个集中的身份认证、授权和审计（AAA）服务器可减少每台设备的操作任务, 并提供用户访问审计日志, 日志内容涵盖安全合规和根因分析。为访问控制启用AAA时, 所有的访问网络基础设施（SSH和HTTPS）的管理都将通过AAA控制。

读者提示

本架构中使用AAA服务器是思科身份认证控制系统（ACS）。如需了解有关这ACS相关配置的详细信息, 请参阅思科IBA智能业务平台《利用ACS部署设备管理指南》。

TACACS+是用于验证基础架构设备上对AAA服务器管理登录主要的协议。此外，系统还针对步骤 2中的每个网络基础设施设备定义了一个本地AAA用户数据库，用于在集中部署的TACACS+服务器不可用时，提供备用身份认证源。

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

步骤 4: 配置设备管理协议。

安全HTTP (HTTPS)和安全外壳(SSH)是HTTP和Telnet协议的安全替代品。它们使用安全套接字层(SSL)和传输层安全(TLS)提供了设备身份认证和数据加密功能。

SSH和HTTPS协议可实现对LAN设备的安全管理。这两个协议都进行加密，提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

通过在vty line下指定transport preferred none命令，从而避免错误连接尝试的提示显示在CLI窗口中。如果没有此命令，一旦ip name-server查找不可达，可能会发生因输错命令产生的长时间超时延迟。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

当启用同步记录未请求信息和调试报告时，在显示或打印交互式CLI输出结果后，控制台日志信息将在控制台上显示。借助这一命令，您可以在启用调试流程时，继续在设备控制台上输入信息。

```
line con 0
 logging synchronous
```

简单网络管理协议(SNMP)用于支持使用网络管理系统(NMS)管理网络基础设施设备。SNMPv2c针对只读和读写团体字符串(community string)进行了配置。

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

步骤 5: (可选)网络运营支撑聚焦于您可通过使用访问控制列表限制网络中可访问的设备来增强网络安全。在这个例子中，只有在10.4.48.0/24网段内的设备可以通过SSH或SNMP访问它。

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

技术提示

如果您在VTY接口上配置了一个access-list配置，当使用ssh登录时，您可能会失去从一台路由器到下一台的这种逐跳方式的排错能力。

步骤 6: 配置同步时钟。

网络时间协议(NTP)用于同步网络设备。NTP网络通常从权威时间源，如与时间服务器相连的无线电时钟或原子钟那里获取时间信息。然后NTP在企业网络中分发此信息。

您应将网络设备设定为与网络中的本地NTP服务器保持同步。本地NTP服务器通常会参考来自外部来源的更准确的时钟信息。通过对控制台消息、日志和调试报告进行配置，在输出时添加时间戳，您可以实现对网络中事件的交叉参考。

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
```

```
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

步骤 7: 配置带内管理接口

回环接口是一个逻辑接口，只要设备通电且IP接口能接入网络，它就始终可连接。基于此功能，回环地址是带内管理交换机的最佳方法。三层进程和功能也捆绑于此回环接口，以确保进程永续性。

回环地址通常是一个带32位地址掩码的主机地址。从一个不属于任何其他内部网络汇总范围的独特网络范围中分配回环地址。

```
interface Loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

ip pim sparse-mode命令将在下一步中介绍。

为SNMP， SSH， PIM， TACACS+ 和NTP绑定设备进程到回环接口地址，以实现最高永续性：

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

步骤 8: 配置IP组播路由。

IP 组播允许基础设施（路由器和交换机）复制单个IP数据流，然后将其从一个源设备发送到多个接收设备。与多个独立单播流或传播至所有地点的广播流相比，使用IP组播更为高效。IP电话MOH和IP视频广播数据流就是IP组播应用的两个实例。

为了接收特定的IP组播数据流，终端主机必须通过向其本地组播路由器发送IGMP消息，加入组播组。在传统的IP组播设计中，本地路由器会询问网络中充当RP的另一个路由器，将接收设备映射到活动源设备上，以便它们能够加入其数据流。

在此设计中，在稀疏模式组播基础上，所使用的任意播RP（Auto RP）提供了一种简单但便于扩展的方法，能够支持高永续性RP环境。

在全局配置模式下，在平台上启用IP组播路由。

```
ip multicast-routing
```

必须配置每个三层交换机和路由器，以便利用autorp来发现IP组播RP。使用**ip pim autorp listener**命令，来支持跨稀疏模式链路的发现。这一配置支持在未来对IP组播环境进行扩展和控制，并可根据网络需求与设计进行变更。

```
ip pim autorp listener
```

网络中所有的三层接口均必须启用，以支持稀疏模式组播操作。

```
ip pim sparse-mode
```

程序 2　配置 VRF Lite

创建面向互联网的VRF，以支持面向DMVPN的FVRF。VRF名称可随意设定，但最好选择一个能够描述VRF的名称。要使VRF发挥作用，还必须配置相关的路由标识(RD)。RD配置也会创建路由和转发表，并将RD与VRF实例关联起来。

此设计使用了VRF Lite，从而可以任意选择RD值。当以类似的方式使用VRF时，最佳实践是在多个设备间使用相同的VRF/RD组合。然而，这一惯例并不要求严格遵循。

```
ip vrf INET-PUBLIC1
 rd 65512:1
```

技术提示

命令参考：

RD或者与ASN相关（由一个ASN和一个任意数字组成），或者与IP地址相关（由一个IP地址和一个任意数字组成）。

您可以采用以下格式输入RD：

16位自治系统号码:您的32位数字

例如，65512:1。

32位IP地址：您的16位数字

例如，192.168.122.15:1。

程序 3　连接至Internet

采用DMVPN的远端站点可以使用静态或者动态分配的IP地址。思科使用DHCP分配的外部地址对设计进行了测试，同时它还提供了动态配置的缺省路由。

DMVPN分支路由器直接连接至互联网，无需单独的防火墙。这一连接通过两种方式保证安全性。由于互联网接口位于独立的VRF中，除了来自DMVPN隧道的流量外，没有流量可以接入全局VRF。这种设计提供了自身固有的安全性。此外，IP访问列表仅允许传输加密隧道所需的流量，以及DHCP和进行故障排除所需要的各种ICMP协议。

步骤 1： 启用接口、选择VRF并启用DHCP。

DMVPN设计使用了FVRF，因此这一接口必须放置在上一程序配置的VRF中。

```
interface GigabitEthernet0/0
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 no cdp enable
 no shutdown
```

不要在接口启用PIM，因为该接口没有组播流量的需求。

步骤 2： 配置和应用访问列表。

IP访问列表必须许可下表中指定的协议。访问列表应用于广域网接口的入站方向，因此将对目的地为路由器的流量进行过滤。

表 19 - 需要的DMVPN协议

名称	协议	用途
non500-isakmp	UDP 4500	经由NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

访问列表示例：

```
interface GigabitEthernet0/0
 ip access-group ACL-INET-PUBLIC in
ip access-list extended ACL-INET-PUBLIC
    permit udp any any eq non500-isakmp
    permit udp any any eq isakmp
    permit esp any any
    permit udp any any eq bootpc
```

下表中所列的其他协议可以协助进行故障排除，但并非DMVPN正常运行所必需的协议。

表 20 - DMVPN分支路由器的可选协议

名称	协议	用途
icmp echo	ICMP Type 0, Code 0	允许远程ping
icmp echo-reply	ICMP Type 8, Code 0	允许ping回复（根据我们的请求）
icmp ttl-exceeded	ICMP Type 11, Code 0	允许跟踪路由回复（根据我们的请求）
icmp port-unreachable	ICMP Type 3, Code 3	允许跟踪路由回复（根据我们的请求）
UDP high ports	UDP > 1023, TTL=1	允许远程跟踪路由

其他可添加到访问列表中以支持ping的可选条目如下所示：

```
    permit icmp any any echo
    permit icmp any any echo-reply
```

其他可添加到访问列表中，以支持跟踪路由的可选条目如下所示：

```
    permit icmp any any ttl-exceeded       ! for traceroute
(sourced)
    permit icmp any any port-unreachable   ! for traceroute
(sourced)
    permit udp any any gt 1023 ttl eq 1    ! for traceroute
(destination)
```

程序 4　配置ISAKMP和IPsec

步骤 1： 配置crypto keyring。

crypto keyring针对特定VRF中可到达的IP源，定义了一个预共享密钥（或密码）。如应用于任意IP源，该密钥是一个通配预共享密钥。通配密钥使用0.0.0.0 0.0.0.0网络/掩码组合进行配置。

```
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

步骤 2: 配置ISAKMP策略和对等体状态检测。

面向DMVPN的ISAKMP策略采用如下规则:

- 基于256位密钥的高级加密标准 (AES)
- 安全哈希标准 (SHA)
- 通过PSK进行身份认证
- Diffie-Hellman组: 2

启用DPD, 每30秒间隔发送一次持活信息, 重试间隔为5秒, 这被认为是检测故障中枢路由器的一个合理设置。

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
```

步骤 3: 创建ISAKMP配置文件。

ISAKMP配置文件将身份地址、VRF和crypto keyring关联起来。VRF内的通配地址标注为0.0.0.0。

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
```

步骤 4: 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合, 应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

面向DMVPN的IPsec转换集采用如下规则:

- 采用256位AES加密算法的ESP
- 采用SHA (HMAC变体) 身份认证算法的ESP

由于DMVPN中枢路由器在NAT设备后端, IPsec转换必须针对传输模式进行配置。

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
 mode transport
```

步骤 5: 创建IPsec配置文件。

IPsec配置文件将ISAKMP配置文件和IPsec转换集关联起来。

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

程序 5 配置mGRE隧道

步骤 1: 配置基本接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定, 但最好从10或更大的数字开始编号, 这是因为这一设计中部署的其他特性也可能需要使用隧道, 它们可能在缺省情况下选择了较小的数字。

带宽设置应与互联网带宽相匹配。

将IP MTU配置为1400, 将**ip tcp adjust-mss**配置为1360。二者之间有40字节的差异, 这一差异与IP和TCP报头的总长度对应。

```
interface Tunnel10
 bandwidth [bandwidth (kbps)]
 ip address [IP address] [netmask]
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

步骤 2: 配置隧道。

DMVPN使用多点GRE (mGRE) 隧道。这一隧道类型仅需要一个源接口。源接口应与在 中使用的、连接至互联网的接口相同。将**tunnel vrf**命令设置到之前为FVRF定义的VRF上。

在这一接口上启用加密要求采用在上一程序中配置的IPsec配置文件。

```
interface Tunnel10
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
```

```
tunnel protection ipsec profile DMVPN-PROFILE1
```

步骤 3: 配置NHRP。

DMVPN中枢路由器是面向所有分支的NHRP服务器。NHRP供远程路由器使用，来为mGRE隧道连接的对等体确定隧道目的地。

分支路由器要求几个额外的配置声明，以便为DMVPN中枢路由器mGRE隧道IP地址定义NHRP服务器（NHS）和NHRP映射声明。EIGRP（在下面的程序 6中配置）依赖于组播传输方案。分支路由器要求使用NHRP静态组播映射。

您用于NHS的值是DMVPN中枢路由器的mGRE隧道地址。映射条目必须设定为在Cisco ASA5500上配置的DMVPN中枢的外部NAT值。本设计方案使用了表格 21中所示的值。

表 21 - DMVPN隧道参数

DMVPN云	VRF	DMVPN 中枢公共IP地址（真实的）	DMVPN 中枢公共IP地址（NAT后可路由外部的）	隧道IP地址（NHS）	隧道号码	NHRP网络ID
主用	INET-PUBLIC1	192.168.18.10	172.16.130.1	10.4.34.1	10	101

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份认证密钥。NHRP缓存保持时间应被设置为600秒。

这一设计可支持通过DHCP接收外部IP地址的DMVPN分支路由器。这些路由器可能在重新加载后会获得不同的IP地址。当路由器尝试在NHRP服务器中注册时，可能会与缓存中已有的条目重复而被拒绝。**registration no-unique**选项允许您覆盖现有的缓存条目。这一特性仅在NHRP客户端（DMVPN分支路由器）上需要。

ip nhrp redirect命令允许DMVPN中枢路由器告知分支路由器存在到目标网络的更佳路径。DMVPN分支到分支直接通信可能需要这一功能。当建立了分支到分支隧道后，DMVPN分支路由器还可使用快捷交换（shortcut switching）。

```
interface Tunnel10
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

步骤 4: 配置EIGRP。

在下面的程序中配置EIGRP，但您需要首先针对mGRE隧道接口配置一些具体的要求。

EIGRP问候间隔增加到20秒，EIGRP保持时间增加到60秒，以便在一个DMVPN云上支持多达500个远端站点。

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
```

远端站点局域网必须被通告。远端站点的IP分配经过专门设计，旨在确保正在使用的所有网络均能够在单个汇聚路由中进行汇总。如下配置的汇总地址可以禁止更多特定的路由。如果该汇总结果中的任何网络出现在路由表中，汇总结果将被通告给DMVPN中枢，从而提供了一种永续性措施。如果各个局域网不能进行汇总，那么EIGRP将继续通告特定的路由。

```
interface Tunnel10
 ip summary-address eigrp 200 [summary network] [summary mask]
```

程序 6 配置EIGRP

DMVPN分支路由器上运行单个EIGRP进程。路由器上的所有接口均为EIGRP接口，但只有DMVPN隧道接口采用非被动设置。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。所有DMVPN分支路由器应运行EIGRP末梢（stub）路由，以提高网络稳定性和降低资源消耗。

```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
```

```
eigrp router-id [IP address of Loopback0]
eigrp stub connected summary
no auto-summary
```

程序 7　配置IP组播路由

此程序包含了当为已启用了IP组播的路由器添加DMVPN备份功能时，完成IP组播配置所需的额外步骤。

步骤 1: 在DMVPN隧道接口上配置PIM

使用稀疏模式来支持IP组播接口工作模式。

```
interface Tunnel10
 ip pim sparse-mode
```

步骤 2: 为DMVPN隧道启用PIM 无广播多路访问 (NBMA) 模式。

分支到分支DMVPN网络带来了一种独特的挑战，因为分支路由器彼此间不能直接交换信息，即使它们处于相同的逻辑网络中也不行。无法直接交换信息可能会导致在运行IP组播时发生问题。

要解决NBMA问题，您需要采用单独跟踪每个远程PIM邻接设备加入信息的方法。PIM NBMA模式下的路由器会假定，每一个远程PIM邻接设备均已通过点对点链路连接至路由器。

```
interface Tunnel10
 ip pim nbma-mode
```

步骤 3: 为DMVPN分支路由器配置DR优先级

在DMVPN云中正确运行组播要求中枢路由器承担起PIM指定路由器 (DR) 的角色。分支路由器永远不应成为DR。为避免出现此情况，您可以将分支路由器的DR优先级设置为0。

```
interface Tunnel10
 ip pim dr-priority 0
```

程序 8　连接路由器至接入层交换机

读者提示

为完成更详细的接入层配置，请参考《局域网部署指南》。该指南仅包含了完成接入层配置的额外步骤。

如果您使用远端分布层，请跳转到本指南“部署广域网远端站点分布层”章节。

二层EtherChannel能够以最具永续性的方式，将CE路由器互联到接入层。如果接入层设备是单独的固定配置交换机，将在路由器和交换机间使用简单的二层中继。

在接入层设计中，远端站点使用紧缩路由，并将802.1Q中继接口连接到局域网接入层。

Option 1. 从路由器到接入层交换机的二层EtherChannel

步骤 1: 在路由器上配置port-channel接口。

```
interface Port-channel1
 description EtherChannel link to RS232-A2960S
 no shutdown
```

步骤 2: 在路由器上配置EtherChannel成员接口。

使用channel-group命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。并非所有的路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet0/1
 description RS232-A2960S Gig1/0/24
!
interface GigabitEthernet0/2
 description RS232-A2960S Gig2/0/24
```

```
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

步骤 3: 在接入层交换机上配置EtherChannel成员接口。

将路由器EtherChannel上行链路连接到接入层堆叠交换机。或在使用Cisco Catalyst 4507R+E分布层的情况下，连接至单独的冗余模块，以实现更高的永续性。

在配置逻辑端口通道接口前，先配置属于二层EtherChannel成员的物理接口。按此顺序进行配置能够尽量减少所需操作和错误，因为大多数输入端口通道接口的命令会复制到它的成员接口，无需人工复制。

将两个或多个物理接口配置为EtherChannel成员。此外，采用在平台配置程序中定义的出口QoS宏，以确保正确地划分流量优先级。

并非所有的联网路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet1/0/24
 description Link to RS232-2911-1 Gig0/1
interface GigabitEthernet2/0/24
 description Link to RS232-2911-1 Gig0/2
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport
 macro apply EgressQoS
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤 4: 在分布层交换机上配置EtherChannel中继。

采用802.1Q中继，从而使路由器能够为接入层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于接入层交换机上处于活动状态的VLAN。当采用EtherChannel时，接口类型为端口通道，编码必须与步骤 3中配置的通道组相匹配。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface Port-channel1
 description EtherChannel link to RS232-2911-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

Catalyst 2960-S和4500不需要**switchport trunk encapsulation dot1q**命令。

Option 2. 从路由器到接入交换机的二层中继

步骤 1: 在路由器上启用物理接口。

```
interface GigabitEthernet0/2
 description RS231-A2960S Gig1/0/24
 no ip address
 no shutdown
```

步骤 2: 在接入层交换机上配置中继。

采用802.1Q中继连接，从而使路由器能够为接入层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于接入层交换机上处于活动状态的VLAN。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface  GigabitEthernet1/0/24
 description Link to RS231-2911 Gig0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
 no shutdown
```

Catalyst 2960-S和4500不需要switchport trunk encapsulation dot1q

命令。

程序 9　配置接入层接口

步骤 1: 创建子接口和分配VLAN标记。

在启用物理接口后，相应的数据或语音子接口可以映射到局域网交换机的VLAN上。子接口编号不需要与802.1Q标记保持一致，但保持一致可以简化整体配置。配置的子接口部分将在所有数据或语音VLAN上重复进行。

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
```

步骤 2: 为每一个子接口配置IP设置

这一设计使用了IP编址惯例，缺省网关路由器分配到的IP地址和IP掩码组合是**N.N.N.1 255.255.255.0**，其中N.N.N是IP网络，1是IP主机。

在这一设计中，所有使用DHCP进行终端站IP分配的路由器局域网接口，必须使用IP helper来到达集中部署的DHCP服务器。

如果远端站点路由器是双路由器设计中的第一台路由器，则需要在接入层配置HSRP。这要求在每个子接口上使用修改的IP配置。

```
interface [type][number].[sub-interface number]
 ip address [LAN network 1] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

示例 - 二层EtherChannel

```
interface Port-channel1
 no ip address
 no shutdown
 !
 interface Port-channel1.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.212.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Port-channel1.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.213.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

示例

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.192.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.193.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

流程

在远端路由器上启用DMVPN

1、配置VRF Lite

2、连接至Internet

3、配置ISAKMP和IPsec

4、配置mGRE隧道

5、配置EIGRP

6、配置IP组播路由

7、VPN与静态路由的控制使用

为如下拓扑中任意场景只用本套程序： DMVPN + DMVPN远端站点，MPLS + DMVPN远端站点，或二层WAN + DMVPN远端站点。

本套程序包括了添加DMVPN备份链路到远端站点路由器的必要附加步骤，如下的配置方法中介绍了备份链路和主用链路的使用方法。

在本指南中：

- 远端DMVPN分支路由器配置

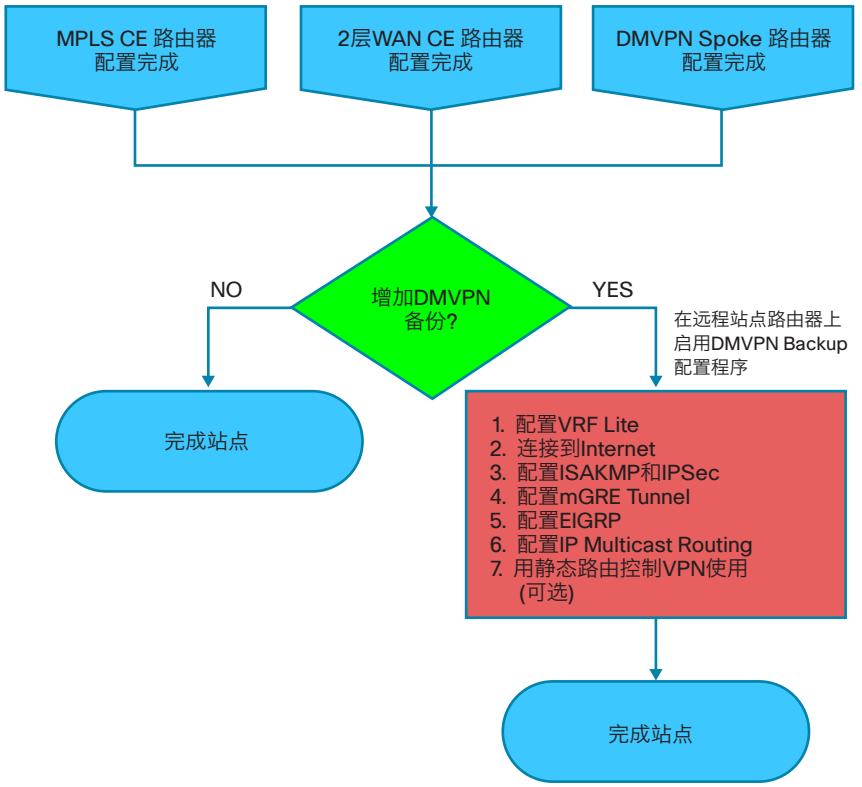
或如下其他指南：

- 《MPLS部署指南》—远端站点MPLS CE路由器配置
- 《二层广域网部署指南》—远端站点二层广域网CE路由器配置

本指南仅包括添加DMVPN备份到当前正在运行的远端路由器的额外程序。

如下流程图提供了详细的有关在现存的远端站点路由器如何添加DMVPN备份的示例。

图 25 - 添加DMVPN备份配置流程图



程序 1 配置VRF Lite

创建面向互联网的VRF，以支持面向DMVPN的FVRF。VRF名称可随意设定，但最好选择一个能够描述VRF的名称。要使VRF发挥作用，还必须配置相关的RD。RD配置也会创建路由和转发表，并将RD与VRF实例关联起来。

此设计使用了VRF Lite，从而可以任意选择RD值。当以类似的方式使用VRF时，最佳实践是在多个设备间使用相同的VRF/RD组合。然而，这一惯例并不要求严格遵循。

当添加DMVPN备份到已配置的DMVPN中枢路由器时，使用下表中新的VRF和其他已关联参数。

表 22 - 双DMVPN的VRF参数

参数	主用DMVPN云	备用DMVPN云
vrf	INET-PUBLIC1	INET-PUBLIC2
rd	65512:1	65512:2
crypto keyring	DMVPN-KEYRING1	DMVPN-KEYRING2
crypto isakmp profile	FVRF-ISAKMP-INET-PUBLIC1	FVRF-ISAKMP-INET-PUBLIC2
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2

```
ip vrf INET-PUBLIC1
 rd 65512:1
```

技术提示

命令参考:

RD或者与ASN相关（由一个ASN和一个任意数字组成），或者与IP地址相关（由一个IP地址和一个任意数字组成）。

您可以采用以下格式输入RD:

16位自治系统号码:您的32位数字

例如，65512:1。

32位IP地址：您的16位数字

例如，192.168.122.15:1。

程序 2 连接至Internet

使用DMVPN的远端站点可使用静态或动态分配IP地址。我们测试了用于DHCP分配外部地址的设计，它同样提供了动态的默认路由配置。

DMVPN分支路由器直接连接至互联网，无需单独的防火墙。这一连接通过两种方式保证安全性。由于互联网接口位于独立的VRF中，除了来自DMVPN隧道的流量外，没有流量可以接入全局VRF。这种设计提供了自身固有的安全性。此外，IP访问列表仅允许传输加密隧道所需的流量，以及DHCP和进行故障排除所需要的各种ICMP协议。

步骤 1: 启用接口、选择VRF并启用DHCP

DMVPN设计使用了FVRF，因此这一接口必须放置在上一程序配置的VRF中。

```
interface GigabitEthernet0/1
 ip vrf forwarding INET-PUBLIC1
 ip address dhcp
 no cdp enable
 no shutdown
```

步骤 2: 配置和应用访问列表。

IP访问列表必须许可下表中指定的协议。访问列表应用于广域网接口的入站方向，因此将对目的地为路由器的流量进行过滤。

表 23 - 需要的DMVPN协议

名称	协议	用途
non500-isakmp	UDP 4500	经由NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

访问列表示例:

```
interface GigabitEthernet0/1
 ip access-group ACL-INET-PUBLIC in
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
```

下表中所列的其他协议可以协助进行故障排除，但并非DMVPN正常运行所必需的协议。

表 24 - DMVPN分支路由器的可选协议

名称	协议	用途
icmp echo	ICMP Type 0, Code 0	允许远程ping
icmp echo-reply	ICMP Type 8, Code 0	允许ping回复（根据我们的请求）
icmp ttl-exceeded	ICMP Type 11, Code 0	允许跟踪路由回复（根据我们的请求）
icmp port-unreachable	ICMP Type 3, Code 3	允许跟踪路由回复（根据我们的请求）
UDP high ports	UDP > 1023, TTL=1	允许远程跟踪路由

其他可添加到访问列表中以支持ping的可选条目如下所示：

```
permit icmp any any echo
permit icmp any any echo-reply
```

其他可添加到访问列表中，以支持跟踪路由的可选条目如下所示：

```
permit icmp any any ttl-exceeded        ! for traceroute
(sourced)
permit icmp any any port-unreachable    ! for traceroute
(sourced)
permit udp any any gt 1023 ttl eq 1     ! for traceroute
(destination)
```

程序 3　配置ISAKMP和IPsec

步骤 1: 配置crypto keyring。

crypto keyring针对特定VRF中可到达的IP源，定义了一个预共享密钥（PSK）（或密码）。如应用于任意IP源，该密钥是一个通配PSK。通配密钥使用0.0.0.0 0.0.0.0网络/掩码组合进行配置。

```
crypto keyring DMVPN-KEYRING1 vrf INET-PUBLIC1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

步骤 2: 配置ISAKMP策略和对等体状态检测。

面向DMVPN的ISAKMP策略采用如下规则：

- 基于256位密钥的高级加密标准（AES）
- 安全哈希标准（SHA）
- 通过PSK进行身份认证
- Diffie-Hellman组： 2

启用DPD，每30秒间隔发送一次持活信息，重试间隔为5秒，这被认为是检测故障中枢路由器的一个合理设置。

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
```

步骤 3: 创建ISAKMP配置文件。

ISAKMP配置文件将身份地址、VRF和crypto keyring关联起来。VRF内的通配地址标注为0.0.0.0。

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC1
   keyring DMVPN-KEYRING1
   match identity address 0.0.0.0 INET-PUBLIC1
```

步骤 4: 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合，应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

面向DMVPN的IPsec转换集采用如下规则：

- 采用256位AES加密算法的ESP
- 采用SHA（HMAC变体）身份认证算法的ESP

由于DMVPN中枢路由器在NAT设备后端，IPsec转换必须针对传输模式进行配置。

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
 mode transport
```

步骤 5: 创建IPsec配置文件。

IPsec配置文件将ISAKMP配置文件和IPsec转换集关联起来。

```
crypto ipsec profile DMVPN-PROFILE1
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC1
```

程序 4　配置mGRE隧道

步骤 1: 配置基本接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定，但最好从10或更大的数字开始编号，这是因为这一设计中部署的其他特性也可能需要使用隧道，它们可能在缺省情况下选择了较小的数字。

带宽设置应与互联网带宽相匹配。

将IP MTU配置为1400，将**ip tcp adjust-mss**配置为1360。二者之间有40字节的差异，这一差异与IP和TCP报头的总长度对应。

```
interface Tunnel10
 bandwidth [bandwidth (kbps)]
 ip address [IP address] [netmask]
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

步骤 2: 配置隧道。

DMVPN使用多点GRE（mGRE）隧道。这一隧道类型仅需要一个源接口。源接口应与在 中使用的、连接至互联网的接口相同。**tunnel vrf**命令应设置为之前为FVRF定义的VRF。

在这一接口上启用加密要求采用在上一程序中配置的IPsec配置文件。

```
interface Tunnel10
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC1
 tunnel protection ipsec profile DMVPN-PROFILE1
```

步骤 3: 配置NHRP。

DMVPN中枢路由器是面向所有分支的NHRP服务器。NHRP供远程路由器使用，来为mGRE隧道连接的对等体确定隧道目的地。

分支路由器要求几个额外的配置声明，以便为DMVPN中枢路由器mGRE隧道IP地址定义NHRP服务器（NHS）和NHRP映射声明。EIGRP（在下面的程序 5中配置）依赖于组播传输方案。分支路由器要求使用NHRP静态组播映射。

您用于NHS的值是DMVPN中枢路由器的mGRE隧道地址。映射条目必须设定为在Cisco ASA5500上配置的DMVPN中枢的外部NAT值。本设计方案使用了表格 25中所示的值。

表 25 - DMVPN隧道参数

DMVPN云	VRF	DMVPN 中枢公共IP地址 (真实的)	DMVPN 中枢公共IP地址 (NAT后可路由外部的)	隧道IP地址 (NHS)	隧道号码	NHRP网络ID
主用	INET-PUBLIC1	192.168.18.10	172.16.130.1	10.4.34.1	10	101
备用	INET-PUBLIC2	192.168.18.11	172.17.130.1	10.4.36.1	11	102

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份认证密钥。NHRP缓存保持时间应被设置为600秒。

这一设计可支持通过DHCP接收外部IP地址的DMVPN分支路由器。这些路由器可能在重新加载后会获得不同的IP地址。当路由器尝试在NHRP服务器中注册时，可能会与缓存中已有的条目重复而被拒绝。**registration no-unique**选项允许您覆盖现有的缓存条目。这一特性仅在NHRP客户端（DMVPN分支路由器）上需要。

ip nhrp redirect命令允许DMVPN中枢路由器告知分支路由器存在到目标网络的更佳路径。DMVPN分支到分支直接通信可能需要这一功能。当建立了分支到分支隧道后，DMVPN分支路由器还可使用快捷交换（shortcut switching）。

```
interface Tunnel10
 ip nhrp authentication cisco123
 ip nhrp map 10.4.34.1 172.16.130.1
 ip nhrp map multicast 172.16.130.1
 ip nhrp network-id 101
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.34.1
 ip nhrp registration no-unique
```

```
ip nhrp shortcut
ip nhrp redirect
```

步骤 4: 配置EIGRP。

在下面的程序中配置EIGRP, 但您需要首先针对mGRE隧道接口配置一些具体的要求。

EIGRP问候间隔增加到20秒, EIGRP保持时间增加到60秒, 以便在一个DMVPN云上支持多达500个远端站点。

```
interface Tunnel10
 ip hello-interval eigrp 200 20
 ip hold-time eigrp 200 60
```

远端站点局域网必须被通告。远端站点的IP分配经过专门设计, 旨在确保正在使用的所有网络均能够在单个汇聚路由中进行汇总。如下配置的汇总地址可以禁止更多特定的路由。如果该汇总结果中的任何网络出现在路由表中, 汇总结果将被通告给DMVPN中枢, 从而提供了一种永续性措施。如果各个局域网不能进行汇总, 那么EIGRP将继续通告特定的路由。

```
interface Tunnel10
 ip summary-address eigrp 200 [summary network] [summary mask]
```

程序 5 配置EIGRP

DMVPN分支路由器上运行单个EIGRP-200进程。路由器上的所有接口均为EIGRP接口, 但只有DMVPN隧道接口采用非被动设置。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。所有DMVPN分支路由器应运行EIGRP末梢 (stub) 路由, 以提高网络稳定性和降低资源消耗。

```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

程序 6 配置IP组播路由

此程序包含了当为已启用了IP组播的路由器添加DMVPN备份功能时, 完成IP组播配置所需的额外步骤。

步骤 1: 在DMVPN隧道接口上配置PIM

使用稀疏模式来支持IP组播接口工作模式。

```
interface Tunnel10
 ip pim sparse-mode
```

步骤 2: 为DMVPN隧道启用PIM 无广播多路访问 (NBMA) 模式。

分支到分支DMVPN网络带来了一种独特的挑战, 因为分支路由器彼此间不能直接交换信息, 即使它们处于相同的逻辑网络中也不行。无法直接交换信息可能会导致在运行IP组播时发生问题。

要解决NBMA问题, 您需要采用单独跟踪每个远程PIM邻接设备加入信息的方法。PIM NBMA模式下的路由器会假定, 每一个远程PIM邻接设备均已通过点对点链路连接至路由器。

```
interface Tunnel10
 ip pim nbma-mode
```

步骤 3: 为DMVPN分支路由器配置DR优先级

在DMVPN云中正确运行组播要求中枢路由器承担起PIM指定路由器 (DR) 的角色。分支路由器永远不应成为DR。为避免出现此情况, 您可以将分支路由器的DR优先级设置为0。

```
interface Tunnel10
 ip pim dr-priority 0
```

程序 7 VPN与静态路由的控制使用

本程序为可选, 仅以MPLS广域网的静态路由方式使用。

对于双链路设计 (单路由器, 双链路), 当添加VPN备用和服务提供商已使用的静态路由时, 本程序用于控制VPN的使用。MPLS VPN是主用的广域网传输, 且当操作时, 隧道接口将保持关闭。

远端路由器可使用IP SLA特性发送回应探测 (echo probe) 到站点的MPLS PE路由器上，且如果PE路由器不可达，那么路由器会使用嵌入式时间管理（Embedded Event Manager 简称EEM) 动态的启用隧道接口。

步骤 1: 启用IP SLA探测 (probe) 。

使用标准ICMP echo (ping) 探测，并以15秒的间隔来发送它们。响应必须在1000毫秒时间内收到。如果将MPLS PE路由器作为探测目的地，则目的地地址将与已配置的静态路由下一条地址相同。使用MPLS广域网金额口作为测探源接口。

```
ip sla [probe number]
 icmp-echo [probe destination IP address] source-interface
[interface]
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule [probe number] life forever start-time now
```

步骤 2: 配置嵌入式对象跟踪 (Enhanced Object Tracking 简称EOT)

本步骤将IP SLA测探状态与EEM脚本监控的对象联系在了一起。

```
track [object number] ip sla [probe number] reachability
```

步骤 3: 配置EEM脚本语言以启用或关闭隧道接口。

事件跟踪EEM脚本会监控对象的状态并为特定状态运行路由器IOS命令。这也是生成syslog信息以提供关于EEM状态信息的最佳实践。

```
event manager applet [EEM script name]
 event track [object number] state [tracked object state]
 action [sequence 1]  cli command "[command 1]"
 action [sequence 2]  cli command "[command 2]"
 action [sequence 3]  cli command "[command 3]"
 action [sequence …]  cli command "[command …]"
 action [sequence N] syslog msg "[syslog message test]"
```

示例:

```
track 60 ip sla 200 reachability
ip sla 200
 icmp-echo 192.168.6.142 source-interface GigabitEthernet0/0
 threshold 1000
 frequency 15
ip sla schedule 200 life forever start-time now
```

EEM脚本在MPLS链路失效链路上启用隧道接口:

```
event manager applet ACTIVATE-VPN
 event track 60 state down
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface tunnel10"
 action 4  cli command "no shutdown"
 action 5  cli command "end"
 action 99 syslog msg "Primary Link Down - Activating VPN
interface"
```

EEM脚本在MPLS恢复链路上关闭隧道接口:

```
event manager applet DEACTIVATE-VPN
 event track 60 state up
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface tunnel10"
 action 4  cli command "shutdown"
 action 5  cli command "end"
 action 99 syslog msg "Primary Link Restored - Deactivating
VPN interface"
```

流程

为双路由器设计改变Router 1

1、配置接入层HSRP

2、配置过境 (Transit) 网络

3、配置EIGRP (局域网端)

4、启用增强的对象跟踪 (Object Tracking)

5、配置环回 (Loopback) 永续性

当第一台路由器已使用如下之一的方法配置时，将需要使用本步骤。

在此指南中:

- 远端DMVPN中枢路由器配置

或这些其他指南:

- 《MPLS部署指南》 - 远端站点MPLS CE路由器配置
- 《二层广域网部署指南》 - 远端站点二层广域网CE路由器配置

程序 1 配置接入层HSRP

您需要配置HSRP以启用虚拟IP (VIP) 作为在两台路由器之间的共享默认网关的功能。HSRP主用 (active) 路由器连接到主用载体，HSRP备用 (standby) 路由器连接到备用载体或备用链路。使用standby priority配置主用HSRP路由器，其优先级需要高于HSRP备用路由器。

拥有较高备用优先级 (standby priority) 的路由器被用作HSRP活动路由器。抢占 (preempt) 选项可以让拥有较高优先级的路由器成为HSRP活动路由器，而无需等到环境中没有HSRP活动路由器时才转变状态。针对路由器配置的相关HSRP参数如下表所示。

表 26 - 广域网远端站点HSRp参数 (双路由器)

路由器	HSRP角色	虚拟IP地址 (VIP)	实际IP地址	HSRP优先级	PIM DR优先级
主用	活动	.1	.2	110	110
备用	备用	.1	.3	105	105

在先前的程序中，已分配的IP地址覆盖了这些配置，因此默认路由IP地址在穿越单或双路由器时需保持一致。

双路由器接入层设计需要进行一些修改，以支持永续性组播。PIM DR应位于HSRP活动路由器之上。DR通常基于最高的IP地址选出，而与HSRP配置无关。在这一设计中，HSRP活动路由器的实际IP地址低于HSRP备用路由器，因此需要对PIM配置进行修改。可以通过明确设置路由器上面向局域网的子接口的DR优先级，来对PIM DR选择施加影响。

技术提示

上表中显示的HSRP优先级和PIM DR优先级有着相同的值，而您可不必要求这些值必须保持相同。

针对所有数据或语音子接口重复进行此程序。

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 110
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

示例 - 二层链路

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.212.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.212.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.213.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.213.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

程序 2　配置过境 (Transit) 网络

在两台路由器间配置过境网络。您使用该网络进行路由器间通信，并避免“发夹”问题。过境网络应在已被用于数据或语音服务的路由器接口上使用一个额外的子接口。

这一网络未连接终端站，因此不需要HSRP和DHCP。

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [transit net address] [transit net netmask]
 ip pim sparse-mode
```

示例

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.208.1 255.255.255.252
 ip pim sparse-mode
```

步骤 1: 添加过境网络VLAN到接入层交换机。

如果VLAN在接入层交换机上不存在，现在配置它。

```
vlan 99
 name Transit-net
```

步骤 2: 添加过境网络到现有的接入层中继。

```
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan add 99
```

程序 3　配置EIGRP (局域网端)

两台路由器之间必须配置路由协议。这可以确保HSRP活动路由器获得所有广域网远端站点的全部可达性信息。

步骤 1: 启用EIGRP-100.

配置面向接入层的EIGRP-100。在这一设计中，所有面向局域网的接口和回环接口均必须为EIGRP接口。除了过境网络子接口外，所有接口均必须设置为被动。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。不包括作为EIGRP-100接口的DMVPN mGRE接口。

```
router eigrp 100
 network [network] [inverse mask]
 passive-interface default
 no passive-interface [Transit interface]
 eigrp router-id [IP address of Loopback0]
```

```
no auto-summary
```

步骤 2: 将广域网路由协议重分布至EIGRP-100中。

远端站点路由器使用BGP为MPLS连接或使用EIGRP为二层广域网或DMVPN连接。使用中的面向广域网侧路由协议需要重分布到EIGRP-100中。

EIGRP-200或EIGRP-300已配置在DMVPN或二层广域网部署中，且路由器从这些EIGRP进程已被重分布。由于路由协议相同，不需要定义缺省metric参数。

```
router eigrp 100
 redistribute eigrp 200
```

BGP已配置在MPLS的部署中。BGP路由使用缺省metric参数重分布进EIGRP。默认来说，只有带宽和延时参数可用于metric计算。

```
router eigrp 100
 default-metric [bandwidth] [delay] 255 1 1500
 redistribute bgp 65511
```

示例: EIGRP重分布到EIGRP

```
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.253.232
 no auto-summary
```

示例: BGP重分布到EIGRP

```
router eigrp 100
 default-metric 100000 100 255 1 1500
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.252.206
 no auto-summary
```

程序 4 启用增强的对象跟踪 (Object Tracking)

除非路由器被重新加载或出现故障，否则HSRP活动路由器将始终用作活动路由器。将HSRP路由器保持用作活动路由器可能会导致意外的行为。如果主用广域网传输发生故障，HSRP活动路由器将通过到HSRP备用路由器的过境网络获得一条备用路径，并通过该备用路径转发流量。这是次优路由 (sub-optimal routing)，您可以使用EOT来解决它。

HSRP活动路由器 (主用MPLS CE，二层广域网CE或主用DMVPN分支) 可使用IP SLA特性向其上行邻居路由器发送echo探测；如果路由器不可到达，则HSRP活动路由器将会降低自己的HSRP优先级，以便HSRP备用路由器能够取得优先权，成为HSRP活动路由器。

此程序仅适用于连接到主要传输方案的路由器。

步骤 1: 启用IP SLA探测。

使用标准ICMP echo (ping) 探测，并以15秒的间隔来发送它们。响应必须在1000毫秒时间内收到。如果将MPLS PE路由器作为探测目的地，则目的地地址将与BGP邻接设备地址相同。如果使用广域网层CE路由器作为探测目的地，目的地址既是使用简单边界 (simple demarcation) 的CE路由器地址，又是使用中继边界 (trunked demarcation) 的子接口CE路由器地址。如果使用DMVPN中枢路由器作为探测目的地，则目的地址是mGRE隧道地址。

```
ip sla 100
 icmp-echo [probe destination IP address] source-interface
[WAN interface]
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
```

步骤 2: 配置EOT。

跟踪对象基于IP SLA探测创建。被跟踪的对象即代表着探测到达与否。如果探测成功，跟踪对象的状态为Up；如果失败，跟踪对象的状态为Down。

```
track 50 ip sla 100 reachability
```

步骤 3: 连接HSRP与跟踪对象。

所有数据或语音子接口均应启用HSRP跟踪。

HSRP可以监控跟踪对象的状态。如果状态为Down，HSRP优先级将根据配置的优先级进行降低。当优先级降低到一定程度，HSRP备用路由器将取得优先权。

```
interface [interface type] [number].[sub-interface number]
 standby 1 track 50 decrement 10
```

示例

```
ip sla 100
 icmp-echo 192.168.3.10 source-interface GigabitEthernet0/0
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now
!
track 50 ip sla 100 reachability
!
!
interface GigabitEthernet0/2.64
 standby 1 track 50 decrement 10
!
interface GigabitEthernet0/2.69
 standby 1 track 50 decrement 10
```

程序 5　配置环回（Loopback）永续性

远端站点路由器通过回环接口配置带内管理。要确保双路由器设计中的回环接口可达性，须将邻接路由器的回环重分布至广域网路由协议中。程序的改变依靠所使用的广域网路由协议。

Option 1. 配有BGP的MPLS CE路由器

步骤 1: 配置BGP通告临界路由器的回环IP地址。

```
router bgp 65511
 network 10.255.253.203 mask 255.255.255.255
```

Option 2. 配有EIGRP的DMVPN中枢路由器或二层广域网CE路由器

步骤 1: 配置一个访问列表来限制重分布仅包含邻接路由器的回环IP地址。

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

示例

```
ip access-list standard R2-LOOPBACK
 permit 10.255.253.211
!
route-map LOOPBACK-ONLY permit 10
 match ip address R2-LOOPBACK
```

步骤 2: 配置EIGRP来重分布邻接路由器的回环IP地址。必须对EIGRP存根（stub）路由进行调整，以允许重分布的路由。

DMVPN分支路由器示例

```
router eigrp 200
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

二层广域网CE路由器示例

```
router eigrp 300
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

流程

远端站点DMVPN中枢路由器配置(Router 2)

1、配置广域网远端路由器

2、配置VRF Lite

3、连接至Internet

4、配置ISAKMP和IPsec

5、配置mGRE隧道

6、配置EIGRP

7、配置IP组播路由

8、连接路由器至接入层交换机

9、配置接入层接口

10、配置接入层HSRP

11、配置过境网络

12、配置EIGRP (局域网端)

13、配置回环永续性

当您为如下任意拓扑配置双路由器、双链路设计的第二台路由器时, 使用本套程序: DMVPN + DMVPN远端站点， MPLS + DMVPN远端站点, 或二层WAN + DMVPN远端站点。

本套程序包括了第二台路由器作为DMVPN中枢路由器必要的额外配置步骤, 在此之前请确保第一台路由器已使用远端DMVPN中枢路由器配置方法进行了配置。

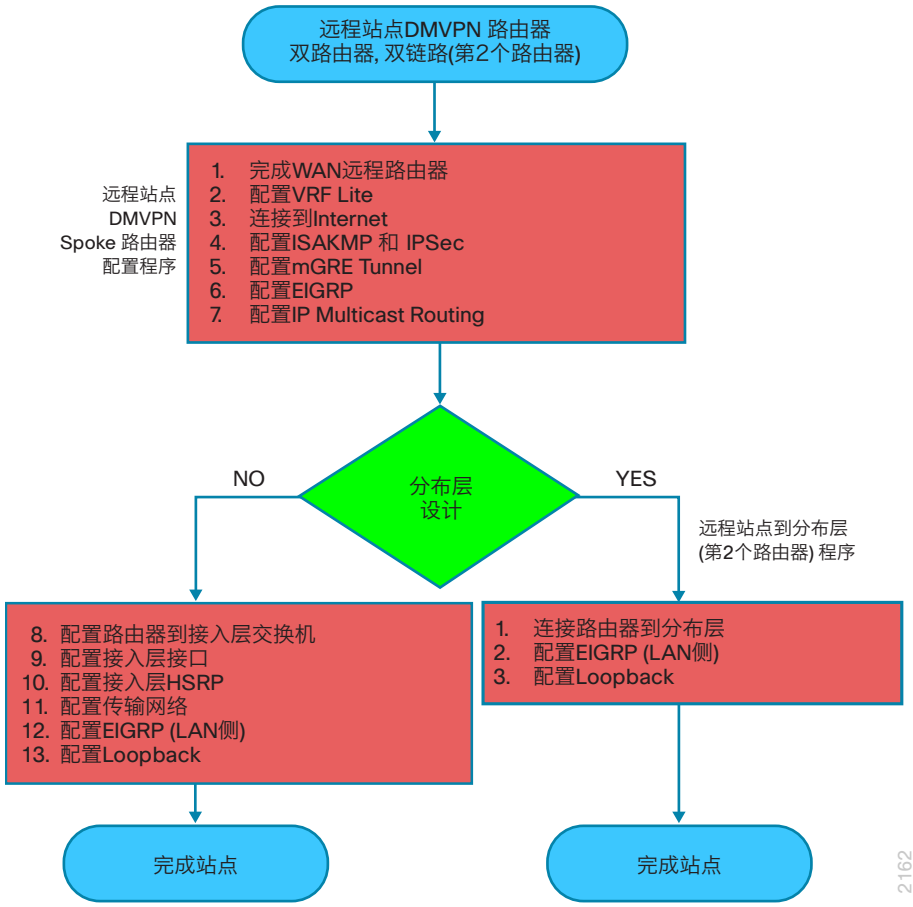
作为一种选择, 如果第一台路由器已根据如下程序之一的不同IBA指南做了配置:

- 《MPLS部署指南》—远端站点MPLS CE路由器配置
- 《二层广域网部署指南》—远端站点二层广域网CE路由器配置

那么前面的步骤, Rouer1修改为双路由器设计, 同样必须完成。

如下流程图提供了详细的有关如何完成远端站点DMVPN中枢路由器配置的示例。

图 26 - 远端DMVPN中枢路由器配置流程图



程序 1　配置广域网远端路由器

在本设计中，有些特性和服务在所有广域网远端站点路由器间是相同的。这些系统设置能够简化并保护解决方案的管理。

步骤 1: 配置设备主机名称，以便轻松识别设备。

```
hostname [hostname]
```

步骤 2: 配置本地登录和密码。

本地的登录帐号和密码提供基本的设备访问身份认证来观察平台操作。通过使能密码获得访问设备配置模式。通过使能密码加密，可防止通过查看配置文件获取到在用的纯文本密码。

```
username admin password c1sco123
enable secret c1sco123
service password-encryption
aaa new-model
```

步骤 3: 默认情况下，https访问交换机需使用使能密码做身份认证。

步骤 4: （可选）配置集中式用户身份认证。

随着网络及需要维护设备数量的增长，在每个设备上的本地用户的维护成本也在相应增加。一个集中的AAA服务，为每台设备减少日常操作的同时，也提供偶尔关于用户访问安全合规性和根源分析的审计日志。当为访问控制启用AAA，所有的网络基础设施设备的管理访问（SSH和HTTPS）都由AAA控制。

读者提示

在此架构中使用AAA服务器是Cisco ACS。如需更多关于Cisco ACS 相关配置详情，请参考《使用ACS的思科设备管理部署指南》。

TACACS+是在设备上用于验证管理登录到AAA服务器的主要协议。在每个网络设备上一个本地AAA用户数据库同样在步骤 2中被定义，它提供了备用身份认证源，以防集中TACACS+服务不可用的情况。

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

步骤 5: 配置设备管理协议。

安全HTTP (HTTPS)和安全外壳(SSH)是HTTP和Telnet协议的安全替代品。它们使用安全套接字层(SSL)和传输层安全(TLS)提供了设备身份认证和数据加密功能。

SSH和HTTPS协议可实现对LAN设备的安全管理。这两个协议都进行加密，提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

通过在vty line下指定transport preferred none命令，从而避免错误连接尝试的提示显示在CLI窗口中。如果没有此命令，一旦ip name-server查找不可达，可能会发生因输错命令产生的长时间超时延迟。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

当启用同步记录未请求信息和调试报告时，在显示或打印交互式CLI输出结果后，控制台日志信息将在控制台上显示。借助这一命令，您可以在启用调试流程时，继续在设备控制台上输入信息。

```
line con 0
 logging synchronous
```

简单网络管理协议(SNMP)用于支持使用网络管理系统(NMS)管理网络基础设

施设备。SNMPv2c针对只读和读写团体字符串(community string)进行了配置。

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

步骤 6: (可选)网络运营支撑聚焦于您可通过使用访问控制列表限制网络中可访问的设备来增强网络安全。在这个例子中，只有在10.4.48.0/24网段内的设备可以通过SSH或SNMP访问它。

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

技术提示

如果您在VTY接口上配置了一个access-list配置，当使用ssh登录时，您可能会失去从一台路由器到下一台的这种逐跳方式的排错能力。

步骤 7: 配置同步时钟。

网络时间协议(NTP)用于同步网络设备。NTP网络通常从权威时间源，如与时间服务器相连的无线电时钟或原子钟那里获取时间信息。然后NTP在企业网络中分发此信息。

您应将网络设备设定为与网络中的本地NTP服务器保持同步。本地NTP服务器通常会参考来自外部来源的更准确的时钟信息。通过对控制台消息、日志和调试报告进行配置，在输出时添加时间戳，您可以实现对网络中事件的交叉参考。

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

步骤 8: 配置带内管理接口

回环接口是一个逻辑接口，只要设备通电且IP接口能接入网络，它就始终可连接。基于此功能，回环地址是带内管理交换机的最佳方法。三层进程和功能也捆绑于此回环接口，以确保进程永续性。

回环地址通常是一个带32位地址掩码的主机地址。从一个不属于任何其他内部网络汇总范围的独特网络范围中分配回环地址。

```
interface Loopback 0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

ip pim sparse-mode命令将在该程序中做进一步介绍。

为SNMP， SSH， PIM， TACACS+ 和NTP绑定设备进程到回环接口地址，以实现最高永续性：

```
snmp-server trap-source Loopback0
ip ssh source-interface Loopback0
ip pim register-source Loopback0
ip tacacs source-interface Loopback0
ntp source Loopback0
```

步骤 9: 配置IP组播路由。

IP 组播允许基础设施（路由器和交换机）复制单个IP数据流，然后将其从一个源设备发送到多个接收设备。与多个独立单播流或传播至所有地点的广播流相比，使用IP组播更为高效。IP电话MOH和IP视频广播数据流就是IP组播应用的两个实例。

为了接收特定的IP组播数据流，终端主机必须通过向其本地组播路由器发送IGMP消息，加入组播组。在传统的IP组播设计中，本地路由器会询问网络中充当RP的另一个路由器，将接收设备映射到活动源设备上，以便它们能够加入其数据流。

在此设计中，在稀疏模式组播基础上，思科使用任意播RP提供了一种简单但便于扩展的方法，能够支持高永续性RP环境。

在全局配置模式下，在平台上启用IP组播路由。

```
ip multicast-routing
```

必须配置每个三层交换机和路由器，以便利用autorp来发现IP组播RP。使用**ip pim autorp listener**命令，来支持跨稀疏模式链路的发现。这一配置支持在未来对IP组播环境进行扩展和控制，并可根据网络需求与设计进行变更。

```
ip pim autorp listener
```

网络中所有的三层接口均必须启用，以支持稀疏模式组播操作。

```
ip pim sparse-mode
```

程序 2　配置VRF Lite

创建面向互联网的VRF，以支持面向DMVPN的FVRF。VRF名称可随意设定，但最好选择一个能够描述VRF的名称。要使VRF发挥作用，还必须配置相关的路由标识(RD)。RD配置也会创建路由和转发表，并将RD与VRF实例关联起来。

此设计使用了VRF Lite，从而可以任意选择RD值。当以类似的方式使用VRF时，最佳实践是在多个设备间使用相同的VRF/RD组合。然而，这一惯例并不要求严格遵循。

当您在备用DMVPN云上配置DMVPN链路时，使用下表中新的VRF和其他已关联参数。

表 27 - 双DMVPN的VRF参数

参数	主用DMVPN云	备用DMVPN云
vrf	INET-PUBLIC1	INET-PUBLIC2
rd	65512:1	65512:2
tunnel number	10	11
crypto keyring	DMVPN-KEYRING1	DMVPN-KEYRING2
crypto isakmp profile	FVRF-ISAKMP-INET-PUBLIC1	FVRF-ISAKMP-INET-PUBLIC2
crypto ipsec profile	DMVPN-PROFILE1	DMVPN-PROFILE2

```
ip vrf INET-PUBLIC2
 rd 65512:2
```

技术提示

斜线或前缀/长度表示法较短，也较易阅读；在此例中，使用前24位作为子网掩码，因此前缀/长度写作“/24”。在本文后面部分，除非需要点分十进制掩码来进行更多概念性说明，否则都采用网络前缀/长度表示法。

程序 3　连接至Internet

使用DMVPN的远端站点可使用静态或动态分配IP地址。我们测试了用于DHCP分配外部地址的设计，它同样提供了动态的默认路由配置。

DMVPN分支路由器直接连接至互联网，无需单独的防火墙。这一连接通过两种方式保证安全性。由于互联网接口位于独立的VRF中，除了来自DMVPN隧道的流量外，没有流量可以接入全局VRF。这种设计提供了自身固有的安全性。此外，IP访问列表仅允许传输加密隧道所需的流量，以及DHCP和进行故障排除所需要的各种ICMP协议。

步骤 1: 启用接口、选择VRF并启用DHCP

DMVPN设计使用了FVRF，因此这一接口必须放置在上一程序配置的VRF中。

```
interface GigabitEthernet0/0
 ip vrf forwarding INET-PUBLIC2
 ip address dhcp
 no cdp enable
 no shutdown
```

不要在本接口上启用PIM，因为没有来自本接口的组播流量需求。

步骤 2: 配置和应用访问列表。

IP访问列表必须许可下表中指定的协议。访问列表应用于广域网接口的入站方向，因此将对目的地为路由器的流量进行过滤。

表 28 - 需要的DMVPN协议

名称	协议	用途
non500-isakmp	UDP 4500	经由NAT-T的IPsec
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

访问列表示例:

```
interface GigabitEthernet0/0
 ip access-group ACL-INET-PUBLIC in
ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
```

下表中所列的其他协议可以协助进行故障排除, 但并非DMVPN正常运行所必需的协议。

表 29 - DMVPN分支路由器的可选协议

名称	协议	用途
icmp echo	ICMP Type 0, Code 0	允许远程ping
icmp echo-reply	ICMP Type 8, Code 0	允许ping回复 (根据我们的请求)
icmp ttl-exceeded	ICMP Type 11, Code 0	允许跟踪路由回复 (根据我们的请求)
icmp port-unreachable	ICMP Type 3, Code 3	允许跟踪路由回复 (根据我们的请求)
UDP high ports	UDP > 1023, TTL=1	允许远程跟踪路由

其他可添加到访问列表中以支持ping的可选条目如下所示:

```
permit icmp any any echo
permit icmp any any echo-reply
```

其他可添加到访问列表中, 以支持跟踪路由的可选条目如下所示:

```
 permit icmp any any ttl-exceeded       ! for traceroute
(sourced)
 permit icmp any any port-unreachable   ! for traceroute
(sourced)
 permit udp any any gt 1023 ttl eq 1    ! for traceroute
(destination)
```

程序 4 配置ISAKMP和IPsec

步骤 1: 配置crypto keyring。

crypto keyring针对特定VRF中可到达的IP源, 定义了一个预共享密钥 (或密码) 。如应用于任意IP源, 该密钥是一个通配预共享密钥。通配密钥使用0.0.0.0 0.0.0.0网络/掩码组合进行配置。.

```
crypto keyring DMVPN-KEYRING2 vrf INET-PUBLIC2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

步骤 2: 配置ISAKMP策略和对等体状态检测 (DPD) 。

面向DMVPN的ISAKMP策略采用如下规则:

- 基于256位密钥的高级加密标准 (AES)
- 安全哈希标准 (SHA)
- 通过PSK进行身份认证
- Diffie-Hellman组: 2

启用DPD, 每30秒间隔发送一次持活信息, 重试间隔为5秒, 这被认为是检测故障中枢路由器的一个合理设置。

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
```

步骤 3: 创建ISAKMP配置文件。

ISAKMP配置文件将身份地址、VRF和crypto keyring关联起来。VRF内的通配地址标注为0.0.0.0。

```
crypto isakmp profile FVRF-ISAKMP-INET-PUBLIC2
   keyring DMVPN-KEYRING2
   match identity address 0.0.0.0 INET-PUBLIC2
```

步骤 4: 定义IPsec转换集。

转换集是一个可接受的安全协议、算法和其他设置的组合，应用于IPsec保护流量。对等体同意在保护特定的数据流时使用特定的转换集。

面向DMVPN的IPsec转换集采用如下规则：

- 采用256位AES加密算法的ESP
- 采用SHA（HMAC变体）身份认证算法的ESP

由于DMVPN中枢路由器在NAT设备后端，IPsec转换必须针对传输模式进行配置。

```
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256
esp-sha-hmac
 mode transport
```

步骤 5: 创建IPsec配置文件。.

IPsec配置文件将ISAKMP配置文件和IPsec转换集关联起来。

```
crypto ipsec profile DMVPN-PROFILE2
 set transform-set AES256/SHA/TRANSPORT
 set isakmp-profile FVRF-ISAKMP-INET-PUBLIC2
```

程序 5 配置mGRE隧道

步骤 1: 配置基本接口设置。

隧道接口在配置的过程中创建。隧道编号可随意设定，但最好从10或更大的数字开始编号，这是因为这一设计中部署的其他特性也可能需要使用隧道，它们可能在缺省情况下选择了较小的数字。

带宽设置应与互联网带宽相匹配。

将IP MTU配置为1400，将**ip tcp adjust-mss**配置为1360。二者之间有40字节的差异，这一差异与IP和TCP报头的总长度对应。

```
interface Tunnel11
 bandwidth [bandwidth (kbps)]
 ip address [IP address] [netmask]
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

步骤 2: 配置隧道。

DMVPN使用多点GRE（mGRE）隧道。这一隧道类型仅需要一个源接口。源接口应与在 中使用的、连接至互联网的接口相同。**tunnel vrf**命令应设置为之前为FVRF定义的VRF。

在这一接口上启用加密要求采用在上一程序中配置的IPsec配置文件。

```
interface Tunnel11
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC2
 tunnel protection ipsec profile DMVPN-PROFILE2
```

步骤 3: 配置NHRP。

DMVPN中枢路由器是面向所有分支的NHRP服务器。NHRP供远程路由器使用，来为mGRE隧道连接的对等体确定隧道目的地。

分支路由器要求几个额外的配置声明，以便为DMVPN中枢路由器mGRE隧道IP地址定义NHRP服务器（NHS）和NHRP映射声明。EIGRP（在下面的程序 6中配置）依赖于组播传输方案。分支路由器要求使用NHRP静态组播映射。

您用于NHS的值是DMVPN中枢路由器的mGRE隧道地址。映射条目必须设定为在Cisco ASA5500上配置的DMVPN中枢的外部NAT值。本设计方案使用了表格 30中所示的值。

表 30 - DMVPN隧道参数

DMVPN云	VRF	DMVPN 中枢公共IP地址(真实的)	DMVPN 中枢公共IP地址(NAT后可路由外部的)	隧道IP地址(NHS)	隧道号码	NHRP网络ID
主用	INET-PUBLIC1	172.16.130.1	10.4.34.1/23	10	101	200
备用	INET-PUBLIC2	172.17.130.1	10.4.36.1/23	11	102	201

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份认证密钥。NHRP缓存保持时间应被设置为600秒。

这一设计可支持通过DHCP接收外部IP地址的DMVPN分支路由器。这些路由器可能在重新加载后会获得不同的IP地址。当路由器尝试在NHRP服务器中注册时，可能会与缓存中已有的条目重复而被拒绝。**registration no-unique**选项允许您覆盖现有的缓存条目。这一特性仅在NHRP客户端（DMVPN分支路由器）上需要。

ip nhrp redirect命令允许DMVPN中枢路由器告知分支路由器存在到目标网络的更佳路径。DMVPN分支到分支直接通信可能需要这一功能。当建立了分支到分支隧道后，DMVPN分支路由器还可使用快捷交换（shortcut switching）。

```
interface Tunnel11
 ip nhrp authentication cisco123
 ip nhrp map 10.4.36.1 172.17.130.1
 ip nhrp map multicast 172.17.130.1
 ip nhrp network-id 102
 ip nhrp holdtime 600
 ip nhrp nhs 10.4.36.1
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
```

步骤 4： 配置EIGRP。

在下面的程序中配置EIGRP，但您需要首先针对mGRE隧道接口配置一些具体的要求。

EIGRP问候间隔增加到20秒，EIGRP保持时间增加到60秒，以便在一个DMVPN云上支持多达500个远端站点。

```
interface Tunnel11
 ip hello-interval eigrp 201 20
 ip hold-time eigrp 201 60
```

远端站点局域网必须被通告。远端站点的IP分配经过专门设计，旨在确保正在使用的所有网络均能够在单个汇聚路由中进行汇总。如下配置的汇总地址可以禁止更多特定的路由。如果该汇总结果中的任何网络出现在路由表中，汇总结果将被通告给DMVPN中枢，从而提供了一种永续性措施。如果各个局域网不能进行汇总，那么EIGRP将继续通告特定的路由。

```
interface Tunnel11
 ip summary-address eigrp 201 [summary network] [summary mask]
```

程序 6　配置EIGRP

DMVPN分支路由器上运行单个EIGRP进程(200或201)。路由器上的所有接口均为EIGRP接口，但只有DMVPN隧道接口采用非被动设置。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。所有DMVPN分支路由器应运行EIGRP末梢（stub）路由，以提高网络稳定性和降低资源消耗。

```
router eigrp 201
 network 10.4.36.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel11
 eigrp router-id [IP address of Loopback0]
 eigrp stub connected summary
 no auto-summary
```

程序 7　配置IP组播路由

此程序包含了当为已启用了IP组播的路由器添加DMVPN备份功能时，完成IP组播配置所需的额外步骤。

步骤 1： 在DMVPN隧道接口上配置PIM

使用稀疏模式来支持IP组播接口工作模式。

```
interface Tunnel11
 ip pim sparse-mode
```

步骤 2： 为DMVPN隧道启用PIM 无广播多路访问（NBMA）模式。

分支到分支DMVPN网络带来了一种独特的挑战，因为分支路由器彼此间不能直接交换信息，即使它们处于相同的逻辑网络中也不行。无法直接交换信息可能会导致在运行IP组播时发生问题。

要解决NBMA问题，您需要采用单独跟踪每个远程PIM邻接设备加入信息的方

法。PIM NBMA模式下的路由器会假定，每一个远程PIM邻接设备均已通过点对点链路连接至路由器。

```
interface Tunnel11
 ip pim nbma-mode
```

步骤 3: 为DMVPN分支路由器配置DR优先级。

在DMVPN云中正确运行组播要求中枢路由器承担起PIM指定路由器（DR）的角色。分支路由器永远不应成为DR。为避免出现此情况，您可以将分支路由器的DR优先级设置为0。

```
interface Tunnel11
 ip pim dr-priority 0
```

程序 8 连接路由器至接入层交换机

读者提示

为完成更详细的接入层配置，请参考《局域网部署指南》。该指南仅包了完成接入层配置的额外步骤。

如果您使用远端分布层，请跳转到本指南“部署广域网远端站点分布层”章节。

二层EtherChannel能够以最具永续性的方式，将CE路由器互联到接入层。如果接入层设备是单独的固定配置交换机，将在路由器和交换机间使用简单的二层中继。

在接入层设计中，远端站点使用紧缩路由，并将802.1Q中继接口连接到局域网接入层。

Option 1. 从路由器到接入层交换机的二层EtherChannel

步骤 1: 在路由器上配置port-channel接口。

```
interface Port-channel2
 description EtherChannel link to RS232-A2960S
 no shutdown
```

步骤 2: 在路由器上配置EtherChannel成员接口。

使用channel-group命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。并非所有的路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet0/1
 description RS232-A2960S Gig1/0/23
!
interface GigabitEthernet0/2
 description RS232-A2960S Gig2/0/23
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

步骤 3: 在接入层交换机上配置EtherChannel成员接口。

将路由器EtherChannel上行链路连接到接入层堆叠交换机。或在使用Cisco Catalyst 4507R+E分布层的情况下，连接至单独的冗余模块，以实现更高的永续性。

在配置逻辑端口通道接口前，先配置属于二层EtherChannel成员的物理接口。按此顺序进行配置能够尽量减少所需操作和错误，因为大多数输入端口通道接口的命令会复制到它的成员接口，无需人工复制。

将两个或多个物理接口配置为EtherChannel成员。此外，采用在平台配置程序中定义的出口QoS宏，以确保正确地划分流量优先级。

并非所有的联网路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet1/0/23
 description Link to RS232-2911-2 Gig0/1
interface GigabitEthernet2/0/23
 description Link to RS232-2911-2 Gig0/2
!
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
 switchport
 macro apply EgressQoS
 channel-group 2 mode on
```

```
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤 4: 在分布层交换机上配置EtherChannel中继。

采用802.1Q中继，从而使路由器能够为接入层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于接入层交换机上处于活动状态的VLAN。当采用EtherChannel时，接口类型为端口通道，编码必须与步骤 3中配置的通道组相匹配。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface Port-channel2
 description EtherChannel link to RS232-2911-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69,99
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

Catalyst 2960-S和4500不需要**switchport trunk encapsulation dot1q**命令。

Option 2. 从路由器到接入交换机的二层中继

步骤 1: 在路由器上启用物理接口。

```
interface GigabitEthernet0/2
 description RS232-A2960S Gig1/0/23
 no ip address
 no shutdown
```

步骤 2: 在接入层交换机上配置中继。

采用802.1Q中继连接，从而使路由器能够为接入层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于接入层交换机上处于活动状态的VLAN。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface  GigabitEthernet1/0/23
 description Link to RS232-2911-2 Gig0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 64,69,99
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
 no shutdown
```

Catalyst 2960-S和4500不需要**switchport trunk encapsulation dot1q**命令。

程序 9 配置接入层接口

步骤 1: 创建子接口并分配VLAN标记。

在物理接口或者端口通道被启用后，您可以将相应的数据或语音子接口映射到局域网交换机的VLAN上。子接口编号不需要与802.1Q标签保持一致，但保持一致可以简化整体配置。配置的子接口部分将在所有数据或语音VLAN上重复进行。

```
interface [type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
```

步骤 2: 为每一个子接口配置IP设置。

这一设计使用了IP编址惯例，缺省网关路由器分配到的IP地址和IP掩码组合是N.N.N.1 255.255.255.0，其中N.N.N是IP网络，1是IP主机。

在这一设计中，所有使用DHCP进行终端站IP分配的路由器局域网接口，必须使用IP helper来到达集中部署的DHCP服务器。

本远端站点DMVPN分支路由器是双路由器设计中的第二台路由器，并且需要在接入层配置HSRP。这要求按照下面的程序配置实际接口的IP分配。

```
interface  [type][number].[sub-interface number]
 description [usage]
 encapsulation dot1Q [dot1q VLAN tag]
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

示例——二层EtherChannel

```
interface Port-channel2
 no ip address
 no shutdown
 !
 hold-queue 150 in
!
interface Port-channel2.64
 description Data
 encapsulation dot1Q 64
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface Port-channel2.69
 description Voice
 encapsulation dot1Q 69
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

示例 - 二层链接 (Link)

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

程序 10　配置接入层HSRP

您配置HSRP来启用您用作缺省网关 (在两台路由器之间共享) 的VIP。HSRP活动路由器是与主要运营商相连的路由器，HSRP备用路由器是连接至备用运营商或者备用链接的路由器。配置HSRP备用路由器，其备用优先级低于HSRP活动路由器。

拥有较高备用优先级的路由器被用作HSRP活动路由器。抢占 (preempt) 选项可以让拥有较高优先级的路由器成为HSRP活动路由器，而无需等到环境中没有HSRP活动路由器时才转变状态。针对路由器配置的相关HSRP参数如下表所示。

表 31 - 广域网远端站点HSRP参数 (双路由器)

路由器	HSRP 角色	虚拟IP地址 (VIP)	实际IP地址	HSRP优先级	PIM DR优先级
主用	活动	.1	.2	110	110
备用	待机	.1	.3	105	105

双路由器接入层设计需要进行一些修改，以支持永续性组播。PIM DR应位于HSRP活动路由器之上。DR通常基于最高的IP地址选出，而与HSRP配置无关。在这一设计中，HSRP活动路由器的实际IP地址低于HSRP备用路由器，因此需要对PIM配置进行修改。可以通过明确设置路由器上面向局域网的子接口的DR优先级，来对PIM DR选择施加影响。

技术提示

上表中显示的HSRP优先级和PIM DR优先级有着相同的值，然而，并无规定要求这些值必须保持相同。

针对所有数据或语音子接口重复进行此流程。

```
interface [interface type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1 address] [LAN network 1 netmask]
```

```
 ip helper-address 10.4.48.10
 ip pim sparse-mode
 ip pim dr-priority 105
 standby version 2
 standby 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

示例 - 二层EtherChannel

```
interface PortChannel2
 no ip address
 no shutdown
!
interface PortChannel2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.212.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.212.1
 standby 1 priority 105
 standby 1 preempt
 standby authentication md5 key-string c1sco123
!
interface PortChannel2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.213.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.13.1
 standby 1 priority 105
 standby 1 preempt
 standby authentication md5 key-string c1sco123
```

示例 - 二层链接 (Link)

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.212.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.212.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.213.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.13.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

程序 11　配置过境网络

两台路由器之间需要配置过境网络。该网络用于支持路由器间通信，并避免“发夹”问题。过境网络应在已被用于数据或语音服务的路由器接口上使用一个额外

的子接口。

这一网络未连接终端站，因此不需要HSRP和DHCP。

```
interface [interface type][number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [transit net address] [transit net netmask]
```

示例

```
interface GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.208.2 255.255.255.252
```

程序 12　配置EIGRP（局域网端）

两台路由器之间必须配置路由协议。这可以确保HSRP活动路由器获得所有广域网远端站点的全部可达性信息

步骤 1： 启用EIGRP-100。

您配置面向接入层的EIGRP-100。在这一设计中，所有面向局域网的接口和回环接口均必须为EIGRP接口。除了过境网络子接口外，所有接口均必须设置为被动。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。勿将DMVPN MGRE接口用作EIGRP接口。

```
router eigrp 100
 network [network] [inverse mask]
 passive-interface default
 no passive-interface [Transit interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

步骤 2： 将EIGRP-201（DMVPN）重分布至EIGRP-100中。

EIGRP-201已经针对DMVPN mGRE接口进行了配置。来自此EIGRP进程的路由被重分布。由于路由协议相同，因此无需缺省度量值（metric ）。

```
router eigrp 100
 redistribute eigrp 201
```

示例

```
router eigrp 100
 network 10.4.0.0 0.1.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 201
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id 10.255.254.232
 no auto-summary
```

程序 13　配置回环永续性

远端站点路由器通过回环接口配置带内管理。要确保双路由器设计中的回环接口可达性，须将邻接路由器的回环重分布至广域网路由协议EIGRP-201（DMVPN）中。

步骤 1： 配置一个访问列表来限制重分布仅包含邻接路由器的回环IP地址。

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

示例

```
ip access-list standard R1-LOOPBACK
 permit 10.255.253.232
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

步骤 2： 配置EIGRP来重分布邻接路由器的回环IP地址。必须对EIGRP存根（stub）路由进行调整，以允许重分布的路由。

```
router eigrp 201
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

部署广域网远端站点分布层

流程

远端站点路由器至分布层

1、连接路由器至分布层

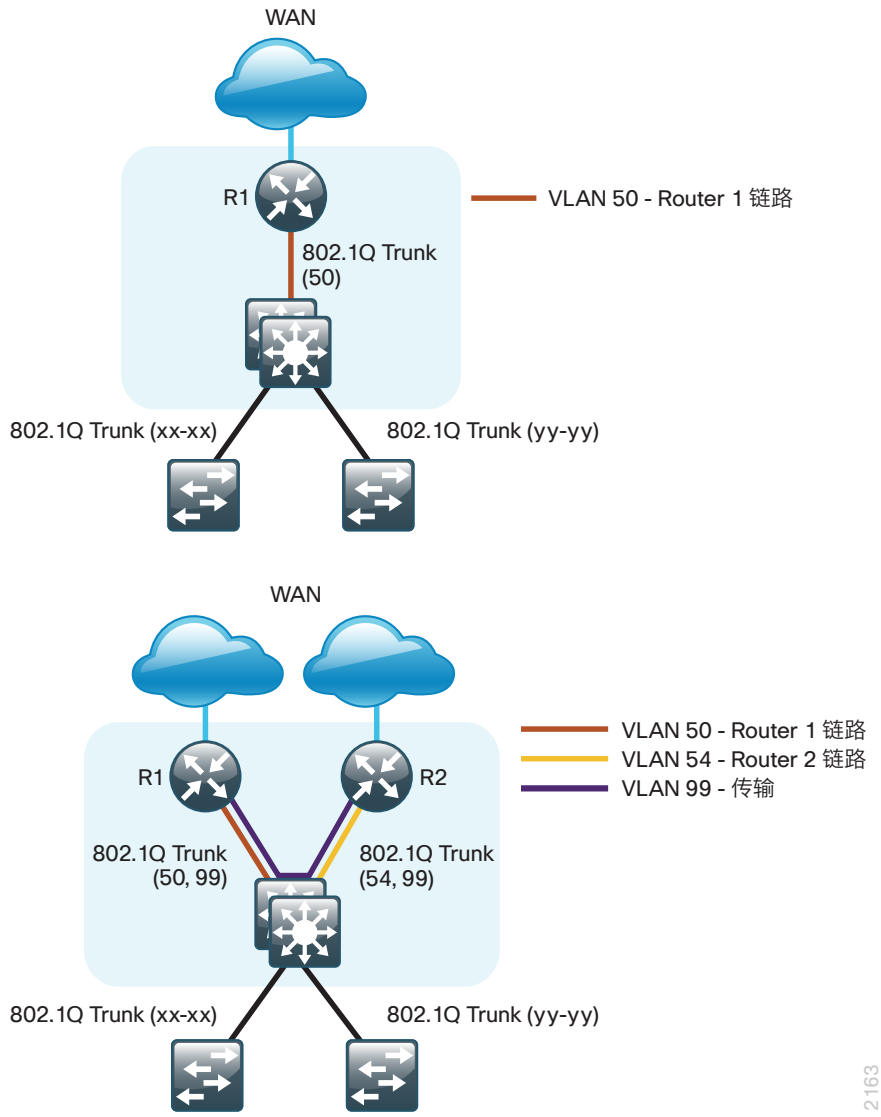
2、配置EIGRP（局域网端）

使用本组程序来为DMVPN远端站点（单路由器、单链路）配置DMVPN分支路由器，内容包括连接到分布层所需的全部流程。

也可以针对DMVPN + DMVPN远端站点使用本组流程。在单路由器、双链路设计中，可使用这些程序来将分布层连接至双角色MPLS CE和DMVPN分支路由器。当您将分布层连接至双路由器、双链路设计的第一台路由器时，请使用这些程序。

分布层和远端站点选项如下图所示。

图 27 - 广域网远端站点 - 连接至分布层



程序 1　连接路由器至分布层

读者提示

请参考《局域网部署指南》以完成分布层配置详情。本指南仅包含完成分布层配置的其它步骤。

在多数永续方法可能的情况下，二层EtherChannel用于CE路由器与分布层的相互连接。这种连接允许必要时在EtherChannel上包括多个VLAN。

步骤 1: 在路由器上配置port-channel（端口通道）接口。

```
interface Port-channel1
 description EtherChannel link to RS232-D3750X
 no shutdown
```

步骤 2: 配置port channel（端口通道）子接口并分配IP地址。

在您启用了接口后，请将相应的子接口映射到分布层交换机的VLAN上。子接口编号不需要与802.1Q标签保持一致，但保持一致可以简化整体配置。

路由器上配置的子接口与分布层交换机上VLAN接口相对应。流量在设备间进行路由，而VLAN充当点对点链路。

```
interface Port-channel1.50
 description R1 routed link to distribution layer
 encapsulation dot1Q 50
 ip address 10.5.208.1 255.255.255.252
 ip pim sparse-mode
```

步骤 3: 在路由器上配置EtherChannel成员接口。

使用channel-group命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。并非所有的路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet0/1
 description RS232-D3750X Gig1/0/1
!
interface GigabitEthernet0/2
 description RS232-D3750X Gig2/0/1
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 1
  no shutdown
```

步骤 4: 在分布层交换机上配置VLAN。

如果分布层交换机上没有现成的VLAN，请立即进行配置。

```
vlan 50
 name R1-link
```

步骤 5: 在分布层交换机上配置三层。.

针对新添加的VLAN，配置VLAN接口，即交换机虚拟接口(SVI)。SVI用于分布层和广域网路由器之间的点对点IP路由。.

```
interface Vlan50
 ip address 10.5.208.2 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

步骤 6: 在分布层交换机上配置EtherChannel成员接口。

将路由器EtherChannel上行链路连接到分布层交换机或堆叠中的各个交换机。在使用Cisco Catalyst 4507R+E分布层的情况下，连接至单独的冗余模块，以实现更高的永续性。

在配置逻辑端口通道接口前，先配置属于二层EtherChannel成员的物理接口。按此顺序进行配置能够尽量减少所需操作和错误，因为大多数输入端口通道接口的命令会复制到它的成员接口，无需人工复制。

将两个或多个物理接口配置为EtherChannel成员。建议按照二的倍数添加物理接口。此外，采用在平台配置程序中定义的出口QoS宏，以确保正确地划分流量优先级。

并非所有的联网路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet1/0/1
```

```
 description Link to RS232-2911-1 Gig0/1
interface GigabitEthernet2/0/1
 description Link to RS232-2911-1 Gig0/2
!
interface range GigabitEthernet1/0/1, GigabitEthernet2/0/1
 switchport
 macro apply EgressQoS
 channel-group 1 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤 7: 在分布层交换机上配置EtherChannel中继。

采用802.1Q中继，从而使路由器能够为分布层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于分布层交换机上处于活动状态的VLAN。当采用EtherChannel时，接口类型为端口通道，编码必须与步骤 3中配置的通道组相匹配。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface Port-channel1
 description EtherChannel link to RS232-2911-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

Catalyst 4500不需要**switchport trunk encapsulation dot1q**命令。

程序 2 配置EIGRP（局域网端）

您必须在路由器和分布层之间配置一个路由协议。

步骤 1: 启用EIGRP-100。

配置面向分布层的EIGRP-100。在这一设计中，所有面向分布层的子接口和回环接口均必须为EIGRP接口。所有其他接口应当被设定为被动。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface [interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

步骤 2: 将EIGRP-200 （DMVPN-1）重分布至EIGRP-100中。

EIGRP-200已经针对DMVPN mGRE接口进行了配置。来自此EIGRP进程的路由被重分布。由于路由协议相同，因此无需缺省metric（度量值）。

```
router eigrp [as number]
 redistribute eigrp [as number (DMVPN)]
```

示例

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface Port-channel1.50
 eigrp router-id 10.255.253.232
 no auto-summary
```

流程

为双路由器 (Router 1) 设计的额外配置

1、配置过境网络

2、配置环回永续性

本流程需要在第一台路由器配置后，使用下列流程中任意一种配置。

This process is required when the first router has already been configured using one of the following processes.

在本指南中:

- 远端站点路由至分布层

在其它指南中:

- 《MPLS部署指南》—远端站点路由至分布层
- 《二层广域网部署指南》—远端站点路由至分布层

程序 1 配置过境网络

在两台路由器间配置过境网络。您使用该网络进行路由器间通信，并避免“发夹”问题。过境网络应在已经被用于连接分布层的EtherChannel接口上使用一个额外的子接口。

过境网络必须是非被动EIGRP接口。

这一网络未连接终端站，因此不需要HSRP和DHCP。过境网络在分布层交换机上使用二层直通，因此无需SVI。

步骤 1: 在路由器上配置过境网络接口。

```
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.208.9 255.255.255.252
 ip pim sparse-mode
```

步骤 2: 在路由器的过境网络接口上启用EIGRP。

```
router eigrp 100
  no passive-interface Port-channel1.99
```

步骤 3: 在分布层交换机上配置过境网络VLAN。

```
vlan 99
 name Transit-net
```

步骤 4: 将过境网络VLAN添加至现有的分布层交换机EtherChannel中继。

```
interface Port-channel1
 switchport trunk allowed vlan add 99
```

程序 2 配置环回永续性

远端站点路由器通过回环接口配置带内管理。要确保双路由器设计中的回环接口可达性，须将邻接路由器的回环重分布至广域网路由协议EIGRP-200（DMVPN）中。

步骤 1: 配置一个访问列表来限制重分布仅包含邻接路由器的回环IP地址。

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

示例

```
ip access-list standard R2-LOOPBACK
 permit 10.255.254.232
!
route-map LOOPBACK-ONLY permit 10
 match ip address R2-LOOPBACK
```

步骤 2: 配置EIGRP来重分布邻接路由器的回环IP地址。必须对EIGRP存根（stub）路由进行调整，以允许重分布的路由。

```
router eigrp 200
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

流程

远端站点路由器至分布层（Router 2）

1、将路由器连接至分布层

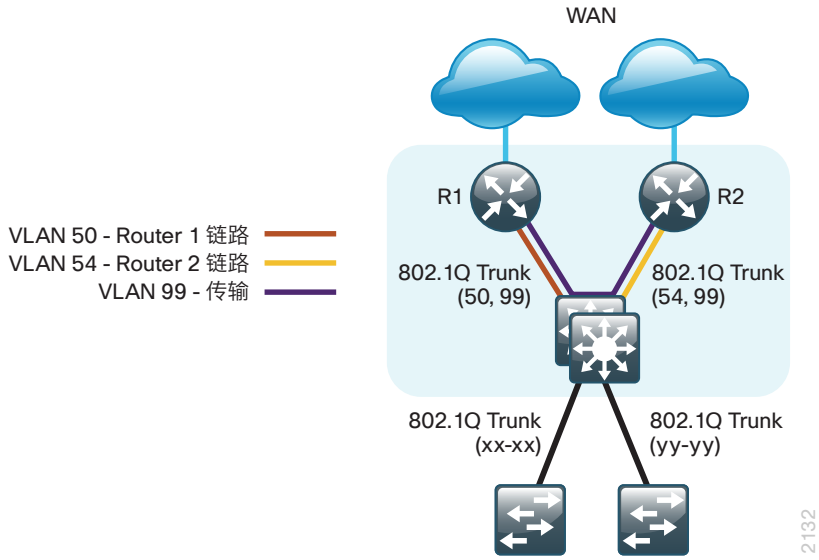
2、配置EIGRP（局域网端）

3、配置回环永续性

针对下列任意拓扑：DMVPN + DMVPN远端站点，MPLS + DMVPN远端站点或二层广域网 + DMVPN远端站点使用本组程序。当配置双路由器、双链路设计的第二台路由器时，可以使用这些程序来连接分布层。这个设计方案在双路由器配置的第二台路由器到局域网分布层交换机之间，采用了一条单独的路由链路。

下图展示了双路由器分布层远端站点选项。

图 28 - 广域网远端站点—连接至分布层



程序 1　将路由器连接至分布层

读者提示

请参阅《局域网部署指南》，了解完整的分布层配置详细信息。本指南仅包括完成分布层配置所需的额外步骤。

二层EtherChannel能够以最具永续性的方式，将CE路由器互联到分布层。这种连接允许必要时在EtherChannel上包括多个VLAN。

步骤 1: 在路由器上配置端口通道接口。

```
interface Port-channel2
 description EtherChannel link to RS232-D3750X
 no shutdown
```

步骤 2: 配置端口通道子接口并分配IP地址。

在您启用了物理接口后，请将相应的子接口映射到分布层交换机的VLAN上。子接口编号不需要与802.1Q标签保持一致，但保持一致可以简化整体配置。

路由器上配置的子接口与分布层交换机上VLAN接口相对应。流量在设备间进行路由，而VLAN充当点对点链路。

```
interface Port-channel2.54
 description R2 routed link to distribution layer
 encapsulation dot1Q 54
 ip address 10.5.208.5 255.255.255.252
 ip pim sparse-mode
```

步骤 3: 在路由器上配置过境网络接口。

```
interface Port-channel2.99
 description Transit net
 encapsulation dot1Q 99
 ip address 10.5.208.10 255.255.255.252
 ip pim sparse-mode
```

步骤 4: 在路由器上配置EtherChannel成员接口。

使用channel-group命令，将物理接口配置为与逻辑端口通道相关联。端口通道和通道组的编号必须匹配。并非所有的路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet0/1
 description RS232-D3750X Gig1/0/2
!
interface GigabitEthernet0/2
 description RS232-D3750X Gig2/0/2
!
interface range GigabitEthernet0/1, GigabitEthernet0/2
  no ip address
  channel-group 2
  no shutdown
```

步骤 5: 在分布层交换机上配置VLAN。

如果分布层交换机上没有现成的VLAN，请立即进行配置。

```
vlan 54
 name R2-link
```

步骤 6: 在分布层交换机上配置三层。

针对新添加的VLAN，配置VLAN接口，即交换机虚拟接口(SVI)。SVI用于分布层和广域网路由器之间的点对点IP路由。

```
interface Vlan54
 ip address 10.5.208.6 255.255.255.252
 ip pim sparse-mode
 no shutdown
```

步骤 7: 在分布层交换机上配置EtherChannel成员接口。

将路由器EtherChannel上行链路连接到分布层交换机或堆叠中的各个交换机。在使用Cisco Catalyst 4507R+E分布层的情况下，连接至单独的冗余模块，以实现更高的永续性。

在配置逻辑端口通道接口前，先配置属于二层EtherChannel成员的物理接口。按此顺序进行配置能够尽量减少所需操作和错误，因为大多数输入端口通道接口的命令会复制到它的成员接口，无需人工复制。

将两个或多个物理接口配置为EtherChannel成员。建议按照二的倍数添加物理接口。此外，采用在平台配置程序中定义的出口QoS宏，以确保正确地划分流量优先级。

并非所有的联网路由器平台均支持链路汇聚控制协议(LACP)与交换机进行协商，因此EtherChannel以静态方式配置。

```
interface GigabitEthernet1/0/2
 description Link to RS232-2911-2 Gig0/1
interface GigabitEthernet2/0/2
 description Link to RS232-2911-2 Gig0/2
!
interface range GigabitEthernet1/0/2, GigabitEthernet2/0/2
 switchport
 macro apply EgressQoS
 channel-group 2 mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
```

步骤 8: 在分布层交换机上配置EtherChannel中继（trunk）。

采用802.1Q中继，从而使路由器能够为分布层交换机上定义的所有VLAN提供三层服务。该中继上所支持的VLAN仅限于分布层交换机上处于活动状态的VLAN。当采用EtherChannel时，接口类型为端口通道，编码必须与步骤 3中配置的通道组相匹配。DHCP侦听和地址解析协议(ARP)检测设置为信任。

```
interface Port-channel2
 description EtherChannel link to RS232-2911-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 54,99
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 ip dhcp snooping trust
 no shutdown
```

Catalyst 4500不需要**switchport trunk encapsulation dot1q**命令。

程序 2 配置EIGRP（局域网端）

您必须在路由器和分布层之间配置一个路由协议。

步骤 1: 启用EIGRP-100。

EIGRP-100面向分布层进行配置。在这一设计中，所有面向分布层的子接口和回环接口均必须为EIGRP接口。所有其他接口应当被设定为被动。网络范围必须在单个网络声明或多个网络声明中包含所有接口IP地址。这一设计采用了将路由器ID指派给回环地址的最佳实践。

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 passive-interface default
 no passive-interface [interface]
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

步骤 2: 将EIGRP-201 （DMVPN-2）重分布至EIGRP-100中。

EIGRP-201已经针对DMVPN mGRE接口进行了配置。来自此EIGRP进程的路由被重分布。由于路由协议相同，因此无需缺省metric（度量值）。

```
router eigrp [as number]
 redistribute eigrp [as number (DMVPN)]
```

示例

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 201
 passive-interface default
 no passive-interface Port-channel2.54
 no passive-interface Port-channel2.99
 eigrp router-id 10.255.254.232
 no auto-summary
```

步骤 3: 启用分布层交换机VLAN接口的EIGRP。

在分布层交换机上已经配置过EIGRP。连接至路由器的VLAN接口必须配置为非被动EIGRP接口。

```
router eigrp 100
 no passive-interface Vlan54
```

程序 3　配置回环永续性

远端站点路由器通过回环接口配置带内管理。要确保双路由器设计中的回环接口可达性，须将邻接路由器的回环重分布至广域网路由协议EIGRP-201（DMVPN）中。

步骤 1: 配置一个访问列表来限制重分布仅包含邻接路由器的回环IP地址。

```
ip access-list standard R[number]-LOOPBACK
 permit [IP Address of Adjacent Router Loopback]
!
route-map LOOPBACK-ONLY permit 10
 match ip address R[number]-LOOPBACK
```

示例

```
ip access-list standard R1-LOOPBACK
 permit 10.255.253.232
!
route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

步骤 2: 配置EIGRP来重分布邻接路由器的回环IP地址。必须对EIGRP存根（stub）路由进行调整，以允许重分布的路由。

```
router eigrp 201
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp stub connected summary redistributed
```

备注

部署广域网服务质量

流程

配置QoS

1、创建QoS映射表来对流量进行分类

2、将ISAKMP流量添加到网络关键 (Network-Critical) 类别

3、定义策略映射表来实施排队策略

4、配置物理接口整形和排队 (S&Q) 策略

5、将广域网QoS策略应用于物理接口

配置广域网边缘QoS，等同于定义流量如何流出网络。关键是分类、标记（marking）和带宽分配要与服务提供商的服务相协调，以确保一致的端到端QoS处理。

程序 1　创建QoS映射表来对流量进行分类

本流程适用于所有广域网路由器。

使用**class-map**命令来定义流量类别和确定与类别名称相关联的流量。类别名称将在配置策略映射表时用到，策略映射表定义了您针对流量类型想要采取的措施。class-map命令设置了匹配逻辑。在这种情况下，匹配任意 (match-any) 关键字表示映射表匹配任何指定的标准。该关键字后跟您想要分配给服务类别的名称。在配置了class-map命令后，您需要定义具体值，如DSCP和协议，来匹配match命令。您使用以下两种形式的**match**命令：**match dscp** 和 **match protocol**。

使用以下步骤来配置所需的广域网类别映射表和匹配标准。

步骤 1： 为DSCP匹配创建类别映射表。

请重复此步骤，为下表中所列的六个广域网服务类别中的每一个分别创建一个类别映射表。

您不需要明确地配置缺省类别。

```
class-map match-any [class-map name]
 match dscp [dcsp value] [optional additional dscp value(s)]
```

表 32 - QoS服务类别

服务类别	流量类型	DSCP 值	带宽%	拥塞避免
VOICE（语音）	语音流量	ef	10 (PQ)	-
INTERACTIVE-VIDEO（交互视频）	交互视频（视频会议）	cs4, af41	23 (PQ)	-
CRITICAL-DATA（关键数据）	高度交互（例如 Telnet, Citrix, Oracle 瘦型客户端）	af31, cs3	15	基于DSCP
DATA（数据）	数据	af21	19	基于DSCP
SCAVENGER（清道夫）	Scavenger（清道夫）	af11, cs1	5	-
NETWORK-CRITICAL（网络关键）	路由协议。运营、管理和维护 (OAM) 流量。	cs6, cs2	3	-
缺省	尽力而为	其他	25	随机

示例

```
class-map match-any VOICE
 match dscp ef
!
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4 af41
!
class-map match-any CRITICAL-DATA
 match dscp af31 cs3
```

```
!
class-map match-any DATA
 match dscp af21
!
class-map match-any SCAVENGER
 match dscp af11 cs1
!
class-map match-any NETWORK-CRITICAL
 match dscp cs6 cs2
```

技术提示

您不需要配置尽力而为 (Best-Effort) 类别。它已经暗含在程序 4 中所示的缺省类别 (class-default) 内了。

程序 2 将ISAKMP流量添加到etwork-Critical类别

对于使用DMVPN的广域网连接，您需要确保ISAKMP流量在广域网中得到正确处理。要对该流量进行分类，需要创建一个访问列表，并将该访问列表名称添加到在程序 1中创建的网络关键 (NETWORK-CRITICAL) 类别映射表中。

此流程仅对广域网汇聚DMVPN中枢路由器或广域网远端站点DMVPN分支路由器来说是必需的。

步骤 1: 创建访问列表。

```
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
```

步骤 2: 将匹配标准添加到现有的网络关键 (NETWORK-CRITICAL) 类别映射表。

```
class-map match-any NETWORK-CRITICAL
 match access-group name ISAKMP
```

程序 3 定义策略映射表来实施排队策略

此程序适用于所有广域网路由器。

广域网策略映射表引用了您在之前的程序中创建的类别名称，并定义了排队行为以及分配给每个类别的最大保证带宽。此规范使用策略映射表完成。然后策略映射表中的每个类别调用一个外出队列，分配一定比例的带宽，并将一个特定的流量类别关联到该队列。一个额外的缺省类别定义了可用于“尽力而为”流量的最低允许带宽。

技术提示

本地路由器策略映射表定义了七个类别，而大多数服务提供商仅提供六个服务类别。定义网络关键 (NETWORK-CRITICAL) 策略映射表，用以确保网络关键流量在通往WAN的出口上得到正确的分类、标记 (marking) 和排队。在流量被传送到服务提供商那里之后，网络关键流量通常被服务提供商重新映射到关键数据类别中。多数提供商都通过在DSCP值cs6和cs2上进行匹配来执行这一再映射。

步骤 1: 创建父策略映射表。

```
policy-map [policy-map-name]
```

针对表格 26中的每个类别重复步骤 2至步骤 6，包括默认类别。

步骤 2: 应用之前创建的类别映射表。

```
class [class-name]
```

步骤 3: （可选）为类别分配最大保证带宽。

```
bandwidth percent [percentage]
```

步骤 4: （可选）为类别定义优先队列。

```
priority percent [percentage]
```

步骤 5: （可选）定义拥塞机制。

```
random-detect [type]
```

示例

```
policy-map WAN
 class VOICE
  priority percent 10
 class INTERACTIVE-VIDEO
  priority percent 23
 class CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class DATA
  bandwidth percent 19
  random-detect dscp-based
 class SCAVENGER
  bandwidth percent 5
 class NETWORK-CRITICAL
  bandwidth percent 3
 class class-default
  bandwidth percent 25
  random-detect
```

技术提示

虽然这些带宽分配提供了一个很好的基准，但考虑您每个类别的实际流量要求，并相应地调整带宽设置仍十分重要。

程序 4　配置物理接口整形和排队 (S&Q) 策略

凭借使用以太网作为接入技术的WAN接口，企业与服务提供商之间的分界点可能不会再有物理接口带宽限制。相反，可以与服务提供商约定指定量的接入带宽。要确保向服务提供商提供的负载不超出协定的速率——超出该速率可能会导致运营商丢弃流量，您需要在物理接口上配置整形 (shaping)。该整形可以借助QoS服务策略来实现。您在外部以太网接口上配置一个QoS服务策略，该父策略包括一个整形器 (shaper)，该整形器随后引用第二个或一个从属 (子) 策略，实现在整形的速率范围内进行排队。这被称为分级式基于类的加权公平队列 (HCBWFQ) 配置。当您配置**shape average**命令时，请确保其值符合您与服务提供商协定的带宽速率。

此流程适用于所有广域网路由器。您可以将这一程序重复执行多次，以支持具有多个连接到不同接口的广域网连接的设备。

步骤 1: 创建父策略映射表。

作为一种最佳实践，请在父策略映射表名称内嵌入接口名称。

```
policy-map [policy-map-name]
```

步骤 2: 配置整形器。

```
class [class-name]
  shape  [average | peak] [bandwidth (kbps)]
```

步骤 3: 应用子服务策略。

```
service-policy [policy-map-name]
```

示例

此示例显示了一个在接口GigabitEthernet0/0上具有20-Mbps链路、在接口GigabitEthernet0/1上具有10-Mbps链路的路由器。

```
policy-map WAN-INTERFACE-G0/0
 class class-default
  shape average 20000000
 service-policy WAN
!
policy-map WAN-INTERFACE-G0/1
 class class-default
  shape average 10000000
 service-policy WAN
```

程序 5　将广域网QoS策略应用于物理接口

要在物理接口上调用整形和排队，您必须应用您在之前的流程中配置的父策略。

此流程适用于所有广域网路由器。您可以将这一程序重复执行多次，以支持具有多个连接到不同接口的广域网连接的设备。

步骤 1: 选择广域网接口。

```
interface [interface type] [number]
```

步骤 2: 应用广域网QoS策略。

该服务策略需要应用于出站方向。

```
service-policy output [policy-map-name]
```

示例

```
interface GigabitEthernet0/0
 service-policy output WAN-INTERFACE-G0/0
!
interface GigabitEthernet0/1
 service-policy output WAN-INTERFACE-G0/1
```

备注

附录 A: 产品列表

WAN汇聚

功能区域	产品描述	产品编号	软件版本
WAN-汇聚路由器	Aggregation Services 1002 Router	ASR1002-5G-VPN/K9	IOS-XE 15.2(2)S Advanced Enterprise
	Aggregation Services 1001 Router	ASR1001-2.5G-VPNK9	
WAN-汇聚路由器	Cisco 3945 Security Bundle w/SEC license PAK	CISCO3945-SEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Security Bundle w/SEC license PAK	CISCO3925-SEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	

WAN远端站点

功能区域	产品描述	产品编号	软件版本
模块化WAN远端站点路由器	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
模块化WAN远端站点路由器	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.1(4)M4 securityk9, datak9
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
模块化WAN远端站点路由器	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	15.1(4)M4 securityk9, datak9
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	

Internet边缘

功能区域	产品描述	产品编号	软件版本
防火墙	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1 IPS 7.1(4) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	6.6.114

Internet边缘LAN

功能区域	产品描述	产品编号	软件版本
DMZ交换机	Cisco Catalyst 3750-X Series Stackable 24 10/100/1000 Ethernet ports	WS-C3750X-24T-S	15.0(1)SE2 IP Base

LAN接入层

功能区域	产品描述	产品编号	软件版本
模块化接入层交换机	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
可堆叠接入层交换机	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

功能区域	产品描述	产品编号	软件版本
独立端口接入层交换机	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
可堆叠接入层交换机	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN分布层

功能区域	产品描述	产品编号	软件版本
模块化分布层虚拟交换机集群	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1 IP services
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/ DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	

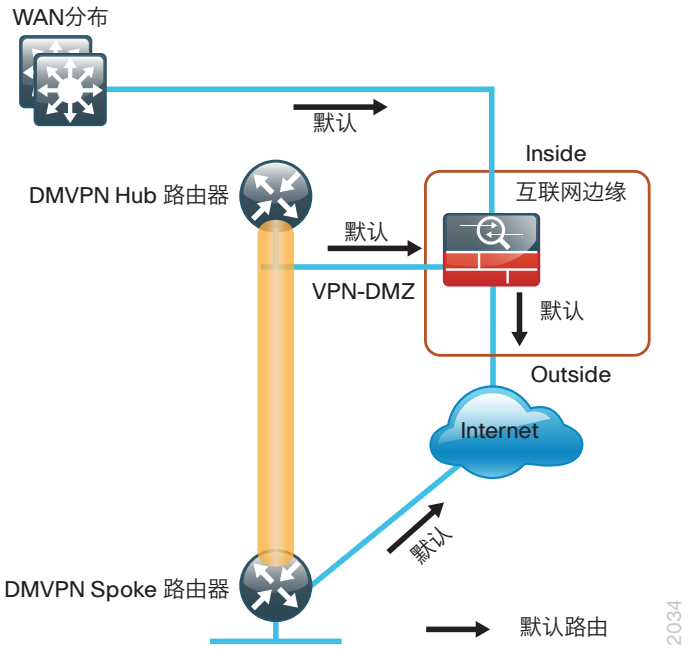
功能区域	产品描述	产品编号	软件版本
模块化分布层交换机	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) Enterprise Services
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
可堆叠分布层交换机	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(1)SE2 IP Services
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

附录B: 技术特性补充

用于DMVPN的Front Door VRF (FVRF)

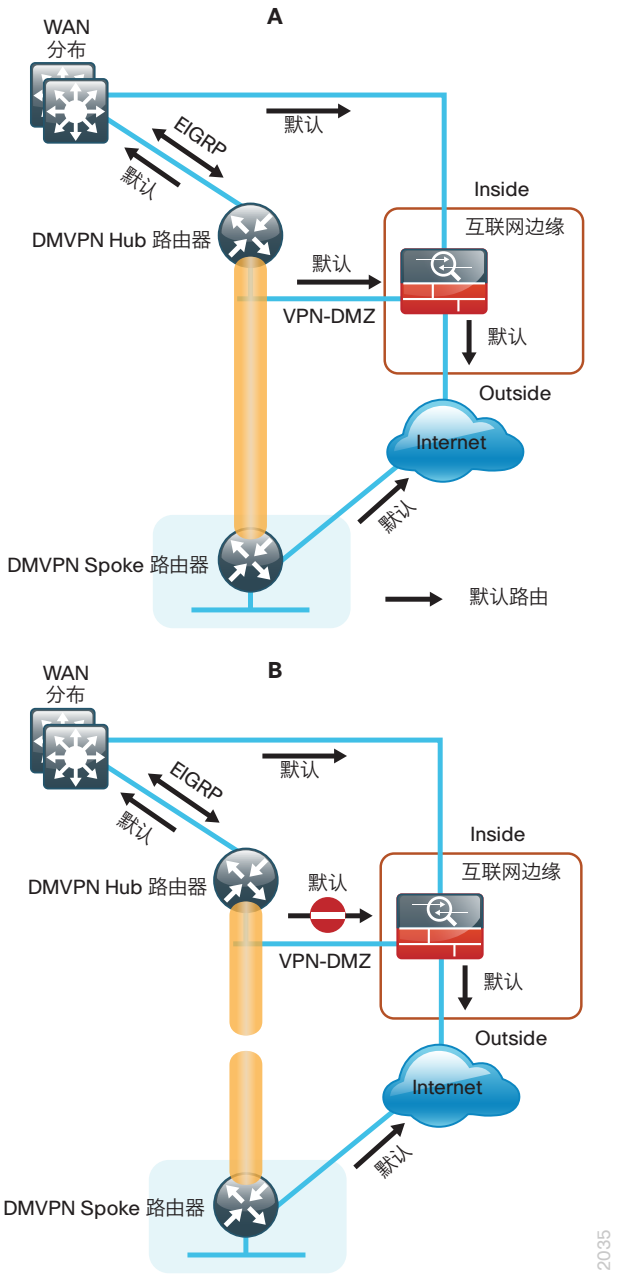
建立IPsec隧道要求加密路由器之间具备可达性。当使用互联网时，路由器使用缺省路由来联系其对等设备。

图 29 - IPsec隧道



如果您需要扩展内部网络（以及可供内部用户使用的同样的缺省路由选项），那么您必须向VPN中枢路由器通告缺省路由。要了解详情，请参见下图中的A部分。

图 30 - 缺省路由注入之前/之后的IPsec隧道



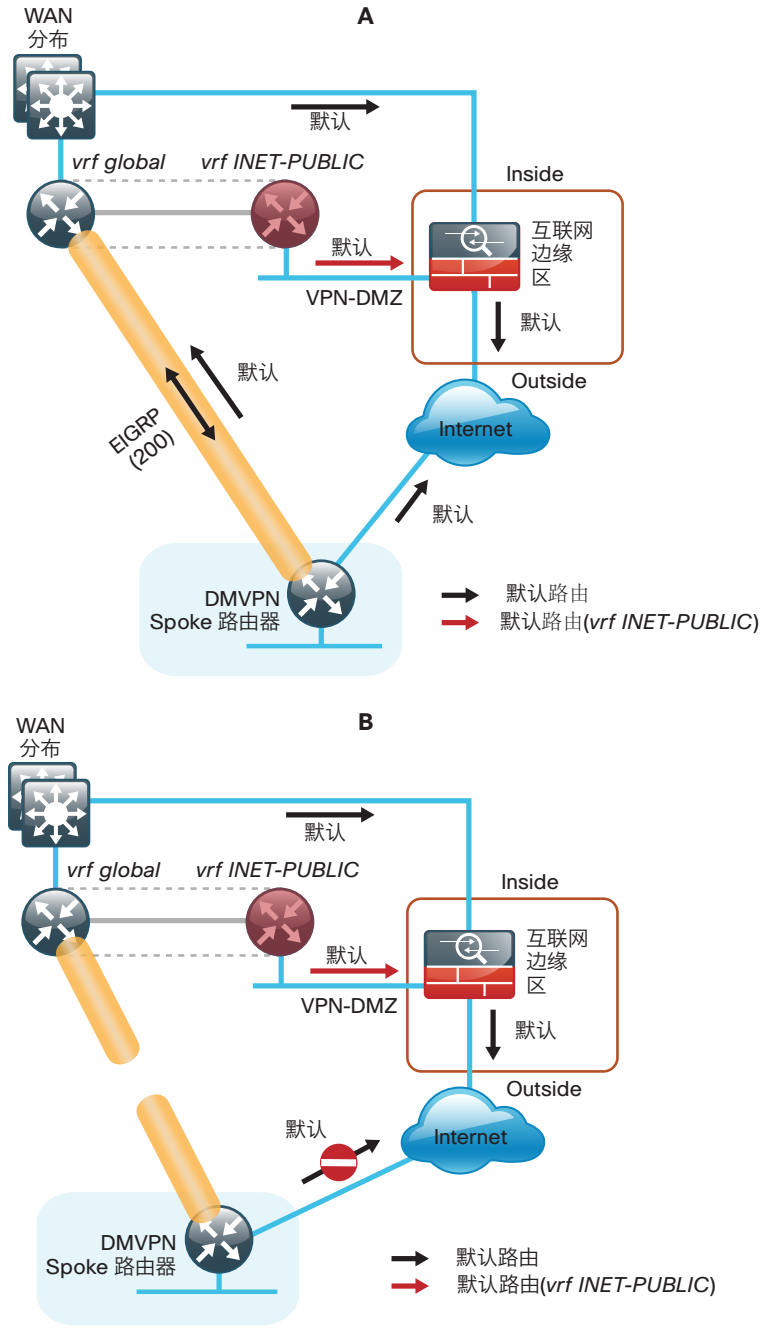
向中枢路由器（目前具有缺省路由）通告缺省路由会带来问题。该路由需要更佳的管理距离来成为活动缺省路由，然后取代支持对等IPsec隧道连接的缺省路由。这一路由通告会打破如上图B部分中所示的隧道。

通过引入外部VRF INET-PUBLIC（红色所示），中枢路由器可以支持多个缺省路由。内部网络留在全局VRF中。这在下图的A部分中示出。

技术提示

中枢路由器上的大多数其他特性不要求VRF感知。

图 31 - 具有FVRF汇聚的 IPsec隧道



这一配置被称为FVRF，因为互联网被包含在VRF中。这一设计的替代方案是内部VRF（IVRF），其中内部网络位于VPN中枢上的VRF中，互联网保留在全局VRF中。本指南未对这种方法进行介绍。

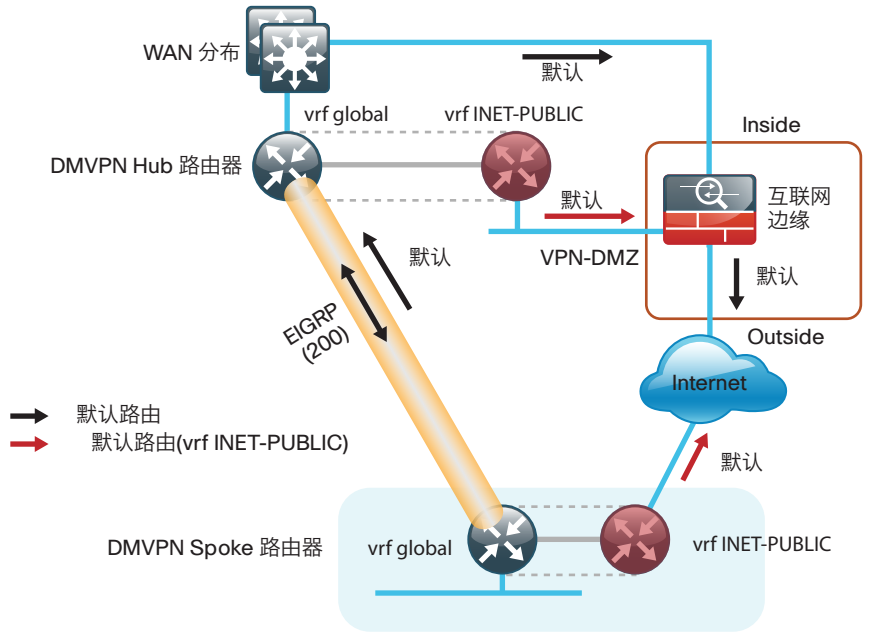
现在，重新建立到远程对等路由器的IPSec隧道已成为可能。由于远端站点策略需要为最终用户提供集中部署的互联网访问能力，缺省路由通过隧道进行通告。这种通告导致在远程路由器上出现相似的缺省路由问题；隧道缺省路由取代互联网指示的缺省路由，隧道连接被打破，如上图B部分中所示。

此配置要求在远端站点路由器上也使用FVRF。采用这一解决方案的主要优势如下：

- 在INET-PUBLIC VRF中简化了缺省路由和静态缺省路由
- 能够支持最终用户流量通过VPN隧道的缺省路由
- 对于采用多种广域网传输方法的站点，能够使用动态缺省路由
- 能够构建DMVPN的分支到分支（spoke-to-spoke）隧道，最终用户流量通过VPN隧道进行缺省路由

在广域网汇聚站点和广域网远端站点都使用了FVRF的最终设计如下图所示。

图 - 32 FVRF——最终配置



附录C: 变更

本附录总结了自先前的Cisco IBA系列到本指南的变更。

- 我们针对设计模型采用了新的命名方式。DMVPN100和DMVPN500变更到单一DMVPN和双DMVPN中。额外的路由器平台为广域网汇聚提供支持。
- 我们介绍了DMVPN专用备份设计模型。该设计模型使用单一DMVPN和双DMVPN, 适用于提供VPN备份到《MPLS广域网部署指南》中的MPLS动态设计模型或《二层广域网部署指南》中的简单分界和中继分界设计模型。
- 我们添加了针对于DMVPN备份共享的设计模型。这种全新的设计模型添加了VPN备份到现存的MPLS CE路由器中, 适用于提供VPN备份到《MPLS广域网部署指南》中的MPLS静态设计模型。我们添加了相关程序以支持本设计模型。
- 我们删除了“部署WAAS的应用优化”章节。在2012年8月系列中, 该章节可在《应用优化部署指南》中找到。

备注

反馈

点击 这里 提供反馈到IBA

美国总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
Singapore

欧洲总部
Cisco Systems International BV Amsterdam,
The Netherlands

思科在全球拥有超过200家办公室。地址，电话号码和传真在思科网站中列出： www.cisco.com/go/offices。