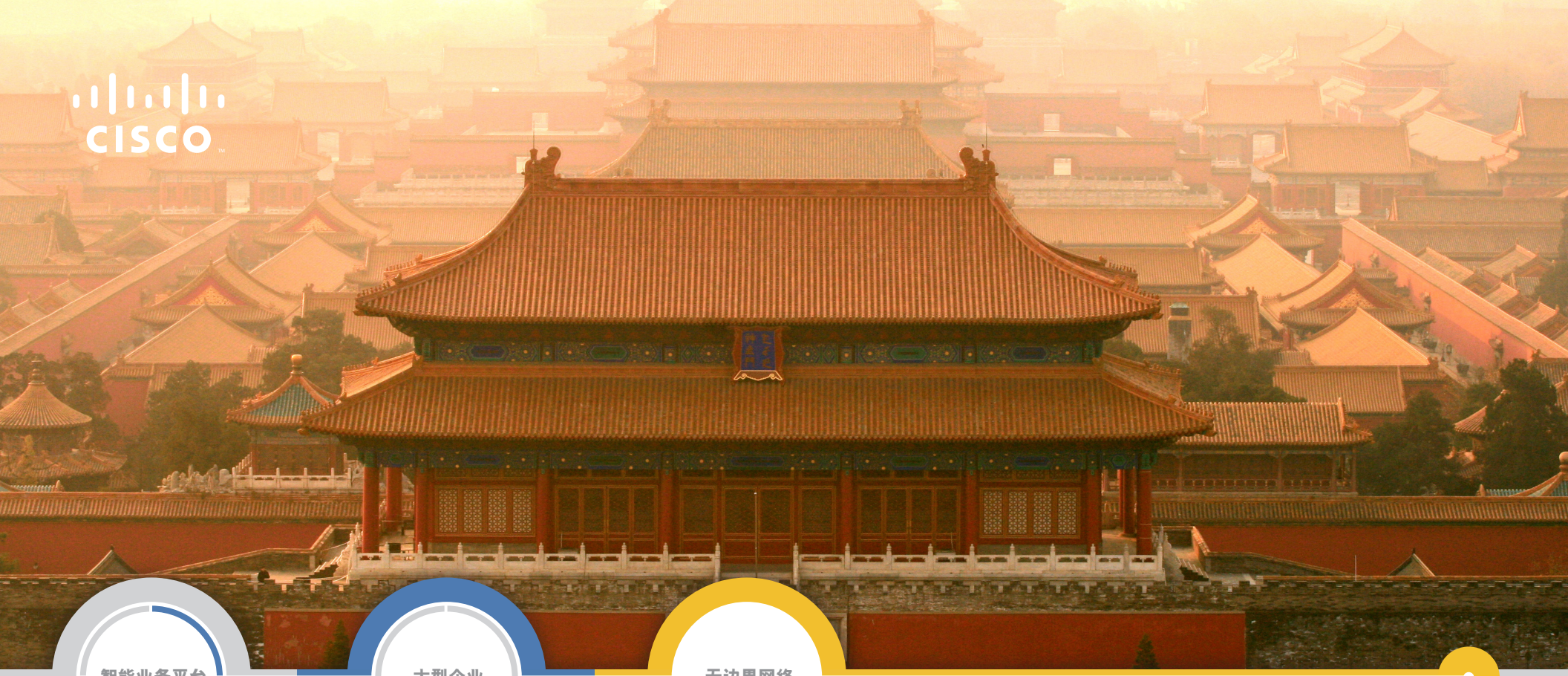
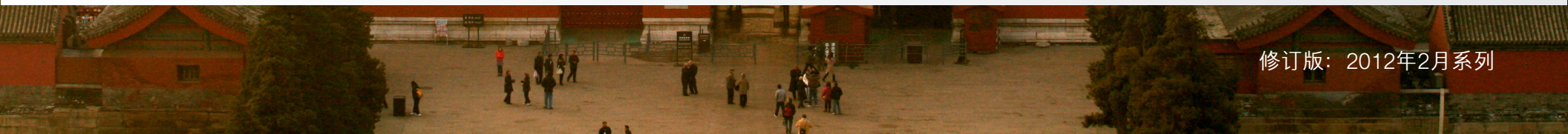



# VPN远程站点部署指南

智能业务平台



修订版：2012年2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人员：

- 需要实施解决方案时的标准规范的系统工程师
- 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指南作为工程师之间技术交流、项目实施经验分享的统一指导文件，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。

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“2011年8月系列”。

您可以在以下网址查看最新的IBA指南系列：

客户访问：http://www.cisco.com/go/cn/iba

合作伙伴访问：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

如需要了解更多有关思科IBA智能业务平台的信息，请访问

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

如需要注册快速报价工具（QPT），请访问

http://www.cisco.com/go/qpt

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 ..... 1
关于IBA ..... 1
关于本指南 ..... 1

简介 ..... 2
设计目标 ..... 2
易于部署、灵活性和可扩展性 ..... 2

架构概述 ..... 5
广域网设计 ..... 5
IP组播 ..... 11
服务质量 ..... 11
广域网优化 ..... 12

部署广域网 ..... 14
整体广域网架构设计目标 ..... 14

部署动态多点虚拟专用网（DMVPN）WAN ..... 16
业务概述 ..... 16
技术概述 ..... 16
部署详情 ..... 22
DMVPN中枢路由器配置 ..... 22
防火墙和DMZ交换机配置 ..... 31
远程站点DMVPN分支路由器配置 ..... 37
在DMVPN分支路由器上启用DMVPN备份 ..... 50
远程站点DMVPN分支路由器配置 ..... 55

部署WAN远程站点分布层 ..... 66
远程站点DMVPN分支路由器分布层 ..... 66
远程站点第二台路由器分布层 ..... 68
远程站点WAN分布层交换机配置 ..... 70

部署WAN服务质量 ..... 74
QoS配置 ..... 74

借助WAAS部署应用优化 ..... 78
业务概述 ..... 78
技术概述 ..... 78
WAAS/WAE配置 ..... 82

附录A：大型企业VPN远程站点部署产品列表 ..... 99

附录B：技术特性补充 ..... 101
用于DMVPN的Front Door vREF (FVRF) ..... 101

附录C：变更 ..... 103

本手册中的所有设计、规格、陈述、信息和建议（统称为“设计”）均按“原样”提供，可能包含错误信息。思科及其供应商不提供任何保证，包括但不限于适销性、适合特定用途和非侵权保证，或与交易过程、使用或贸易惯例相关的保证。在任何情况下，思科及其供应商对任何间接的、特殊的、继发的或偶然性的损害均不承担责任，包括但不限于由于使用或未能使用本手册所造成的利润损失或数据丢失或损害，即使思科或其供应商已被告知存在此类损害的可能性。这些设计如有更改，恕不另行通知。用户对于这些设计的使用负有全部责任。这些设计不属于思科、供应商或合作伙伴的技术建议或其它专业建议。用户在采用这些设计之前应咨询他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

文中使用的任何互联网协议（IP）地址均非真实地址。文中的任何举例、命令显示输出和图示仅供说明之用。在图示中使用任何真实IP 地址均属无意和巧合。

© 2012 思科系统公司。保留所有权利。

# 本IBA指南的内容

## 关于IBA

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，确保能够实现无缝协作。IBA采用的组件式方法简化了在采用多种技术时通常需要进行的系统集成工作，使您可以随意选择能够满足企业需求的解决方案，而不必担心技术复杂性方面的问题。

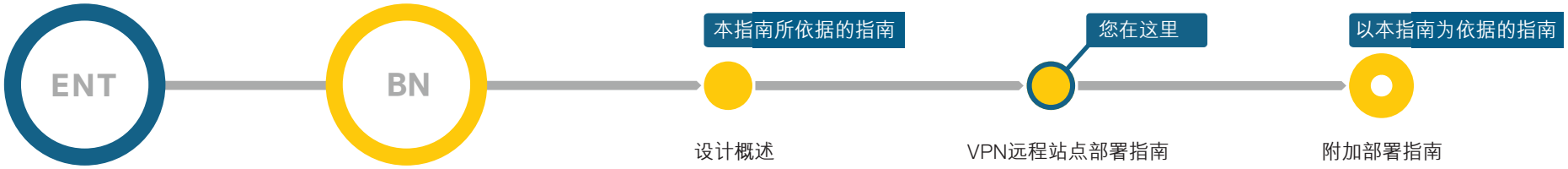
了解更多信息，请参阅《思科IBA使用入门》文档：
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

## 关于本指南

此附加部署指南包含以下章节：

- 业务概述——您的企业所面临的挑战。业务决策者可通过本章内容来了解介绍的解决方案与其企业运营的相关性。
- 技术概述——思科如何应对上述挑战。技术决策者可以利用此章节的内容了解解决方案的工作原理。
- 部署详情——解决方案的具体实施步骤介绍。系统工程师可以在这些步骤的指导下快速可靠地配置和启用解决方案。

本指南假定您已经阅读了本指南所依据的指南，如成功部署路线图中所示。




## 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——即上面路线图中本指南左侧的所有指南。所有以本指南为依据的指南都在右侧。

如需要了解更多有关思科IBA智能业务平台的信息，请访问：
http://www.cisco.com/go/cn/iba
如需要注册快速报价工具（QPT），请访问：
http://www.cisco.com/go/qpt

# 简介

面向大型企业的思科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2,000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。

基础架构在一份设计指南中进行了介绍，另几份部署和配置指南对基础架构的以下三部分进行了介绍：局域网、广域网和互联网边缘。

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远程站点部署指南》为配套配置文件中的主用/备用宽带或互联网传输提供了配置和部署指南
- 《广域网部署指南》十分灵活，提供了用于多协议标签交换（MPLS）传输，以及备用宽带或互联网传输的配置和部署指南。
- 《二层广域网部署指南》为VPLS或城域以太网传输以及备用宽带或互联网传输提供了配置和部署指南。

## 相关内容

本设计指南将向您介绍整个思科IBA智能业务平台设计，并对选择具体产品时需要考虑的要求做了阐述。

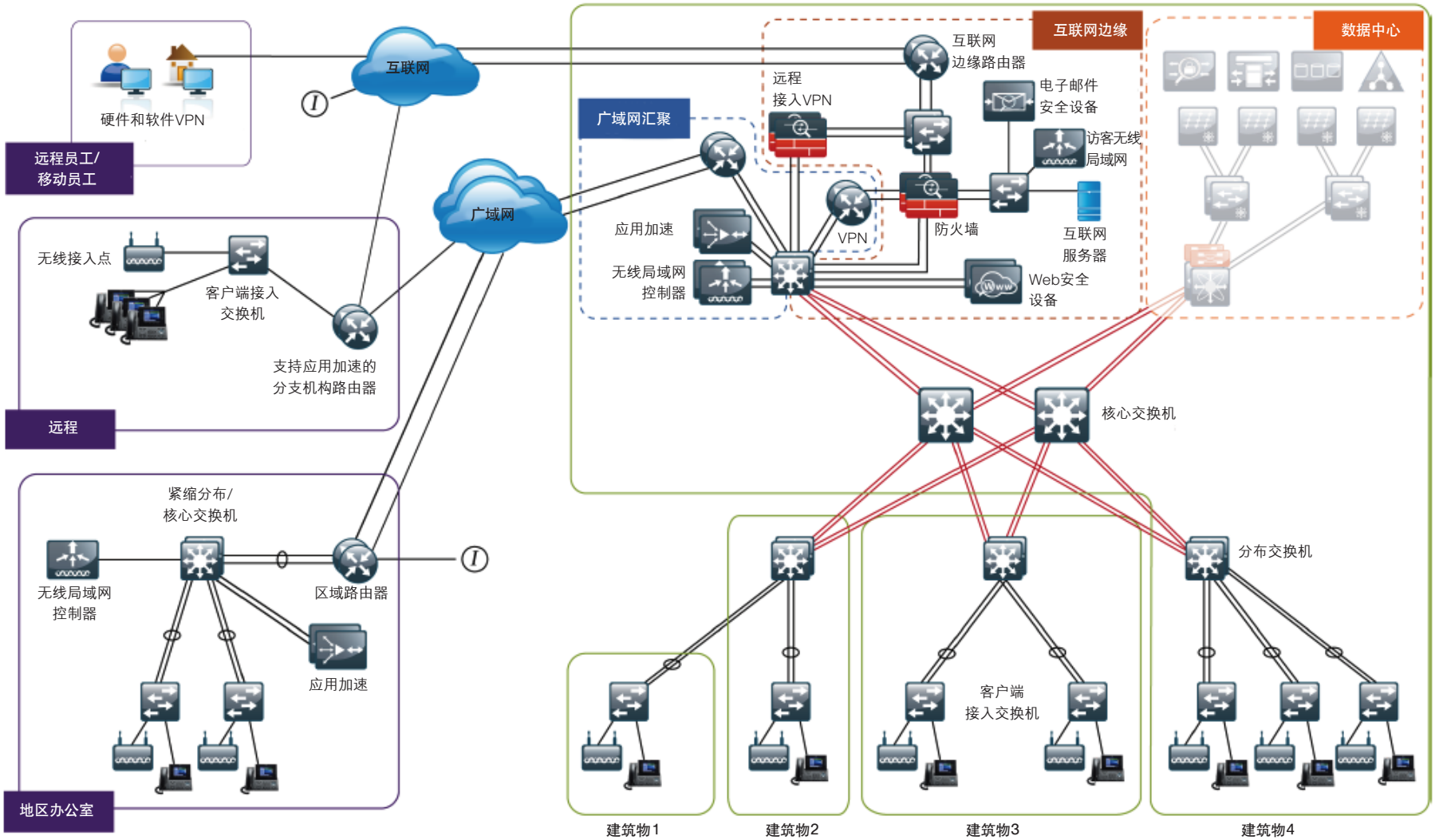
局域网部署指南介绍了有线和无线网络接入，旨在为较大规模的园区级局域网和较小的远程站点局域网提供无所不在的联网功能。此外，为提供强大的通信环境，还包括永续性、安全性和可扩展性。服务质量（QoS）也集成在本指南中，以确保基础架构能够支持大量应用，包括在单一网络上与数据应用共存的、对丢弃敏感的低延迟多媒体应用。该指南还提供了一个访客和合作伙伴接入解决方案，该解决方案和员工网络使用相同的无线基础设施，但不能访问内部保密信息。

《互联网边缘部署指南》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。互联网服务提供商的连接和路由方案，与服务器负载均衡相结合，为设计提供了永续性。本指南的“电子邮件安全”章节用于保护电子邮件免遭垃圾邮件和恶意软件的影响。“Web安全”章节提供可接受的使用控制和监控功能，并向您介绍了如何管理因客户端浏览互联网而带来的日益严重的风险。远程接入VPN设计能够为远程工作人员和移动用户提供安全的远程网络接入。所有这些部分都采用独立章节介绍，但又能相互配合，提供一个安全的互联网边缘解决方案。

## 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在2000到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：

图1. 面向大型企业的无边界网络概述



## 易于部署、灵活性和可扩展性

拥有2000到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的复杂性这两个因素。

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保持可用非常关键。

网络安全性也是本架构的一个重要组件。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，就能随时添加这些高级技术。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就得以简化了。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，能够通过VPN提供软电话，以及传统的硬电话或桌面电话

# 架构概述

《面向大型企业的思科IBA智能业务平台——无边界网络VPN远程站点部署指南》介绍了一种出色设计，能够为多个远程站点局域网带来高度可用、安全且优化的连接。

广域网是网络基础设施，在相隔距离甚远的远程站点之间提供了基于IP的互连。

本文介绍了如何部署网络基础架构和服务，以支持：

- 为25到500个远程站点提供广域网连接
- 部署主要和辅助链路，提供冗余拓扑选项以实现永续性
- 通过加密实现数据保护
- 广域网优化和应用加速
- 为所有远程站点提供有线和无线局域网接入

## 广域网设计

这一设计主要侧重于针对主要和辅助链路支持使用以下常用的广域网传输方法：

- 互联网VPN（主要）
- 互联网VPN（辅助）

在较高级别，广域网是一个IP网络，这一传输方式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服务提供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。

## 使用互联网作为广域网传输方法

互联网从本质上而言是一个由多个互连的服务提供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。虽然采用的是“尽力而为（best effort）”方案，互联网是在无法使用其他传输方式时作为主要传输的一种明智选择。使用互联网作为替代的传输方式，可以提供额外的弹性。

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。远程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，对于远程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，来作为主要广域网传输或备用广域网传输方法（到主要VPN站点间连接）。

## 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，并支持使用简单的星型配置和免接触中枢部署模式来添加远程站点，使之成为了理想的互联网传输加密解决方案。此外，DMVPN也支持能够动态分配IP地址的分支路由器（spoke router）。

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。在本文中这些mGRE隧道有时也称作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均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。端接VPN流量的广域网边缘路由器被称作VPN中枢路由器。所有广域网边缘路由器均连接到分布层。

本指南中讨论的唯一WAN传输方式是传统的互联网接入。单运营商或双运营商互联网接入链路连接至VPN中枢路由器或VPN中枢路由器对。它们使用相似的连接和配置方法。

本部署指南中介绍了两种广域网汇聚设计：DMVPN 100和DMVPN 500。这两种设计的主要区别在于DMVPN 500使用两个互联网服务提供商。其他区别包括架构的总体规模，以及为支持该设计选用的不同平台的功能。

在这两种广域网汇聚设计中，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。

两种设计都使用了双VPN中枢路由器。下表对不同设计模式进行了对比。

**表1.** 广域网汇聚设计

| 模式 | 广域网链路 | 边缘路由器 | 传输方法1 | 传输方法2 |
|---|---|---|---|---|
| DMVPN 100 | 一个 | 一个 | 互联网VPN | |
| DMVPN 500 | 两个 | 两个 | 互联网VPN | 互联网VPN |

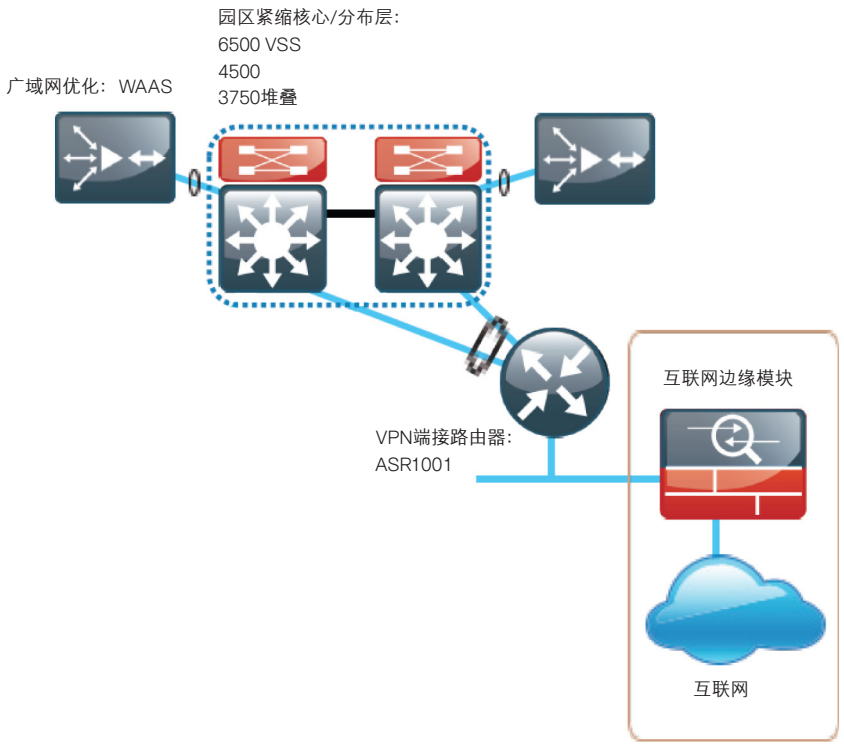
每一种设计的特征如下：

## DMVPN 100设计

- 拥有高达100 Mbps的汇聚带宽
- 支持最多100个远程站点
- 使用单个互联网链路

DMVPN 100设计如下图所示。

**图2.** DMVPN 100设计

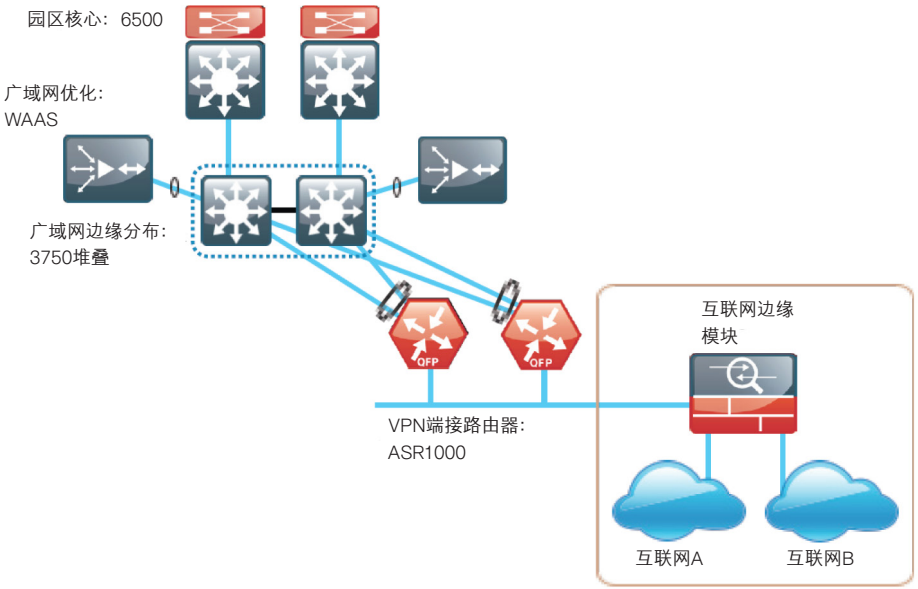



## DMVPN 500设计

- 拥有高达1Gbps的汇聚带宽
- 支持最多500个远程站点
- 使用双互联网链路

DMVPN 500设计如下图所示。

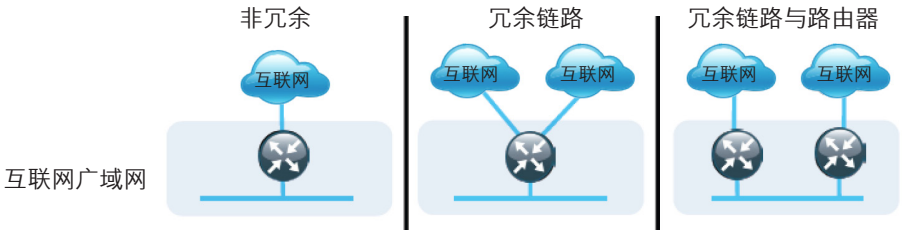
图3. DMVPN 500设计




## 广域网远程站点设计

本指南介绍了多种广域网远程站点设计。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4. 广域网远程站点设计




远程站点设计包含单个或两个广域网边缘路由器。在本指南中，所有远程站点路由器都是VPN分支路由器。

大多数远程站点均采用单个路由器广域网边缘进行设计；然而，某些远程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程站点类型。

表2. 广域网远程站点传输方案

| 广域网远程站点路由器 | 广域网传输方法 | 主要传输方法 | 辅助传输方法 |
|---|---|---|---|
| 一个 | 一个 | 互联网 | - |
| 一个 | 两个 | 互联网 | 互联网 |
| 两个 | 两个 | 互联网 | 互联网 |

网络设计的模块化特性使您能创建出可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程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/局域网互联

广域网的主要作用是互联主要站点和远程站点局域网。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，以及远程站点局域网如何连接到远程站点广域网设备。有关设计中局域网组件的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》。

在远程站点中，局域网拓扑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程站点路由器。本指南中测试和介绍的不同方案如下表所示。

表3. 广域网远程站点局域网方案

| 广域网远程站点路由器 | 广域网传输方法 | 局域网拓扑 |
|---|---|---|
| 一个 | 一个 | 仅接入层<br>分布层/接入层 |
| 一个 | 两个 | 仅接入层<br>分布层/接入层 |
| 两个 | 两个 | 仅接入层<br>分布层/接入层 |

## 广域网远程站点——局域网拓扑

为了保持一致性和模块化特性，所有广域网远程站点均使用了相同的VLAN分配方案，如下表所示。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4. 广域网远程站点——VLAN分配

| VLAN | 使用 | 二层接入 | 三层分布/接入 |
|---|---|---|---|
| VLAN 100 | 数据（主要） | 未使用 | 是 |
| VLAN 65 | 无线数据 | 是 | 是 |
| VLAN 70 | 无线语音 | 是 | 是 |
| VLAN 64 | 数据1 | 是 | 是 |
| VLAN 69 | 语音1 | 是 | 是 |
| 未分配 | 数据2 | 未使用 | 是 |
| 未分配 | 语音2 | 未使用 | 是 |
| VLAN99 | 传输 | 是（仅双路由器） | 是（仅双路由器） |
| VLAN50 | 路由器链路（1） | 未使用 | 是 |
| VLAN54 | 路由器链路（2） | 未使用 | 是（仅双路由器） |

## 二层接入

不需要额外分布层路由设备的广域网远程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（有线和无线）和语音（有线和无线）等服务。下图中的设计示出了一个标准的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。如需了解有关不同接入交换平台的详细配置信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》。

IP子网基于每个VLAN单独进行分配。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配置802.1Q VLAN中继，且路由器上的子接口映射到交换机上的对应的VLAN。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5. 广域网远程站点——扁平型二层局域网（单路由器）

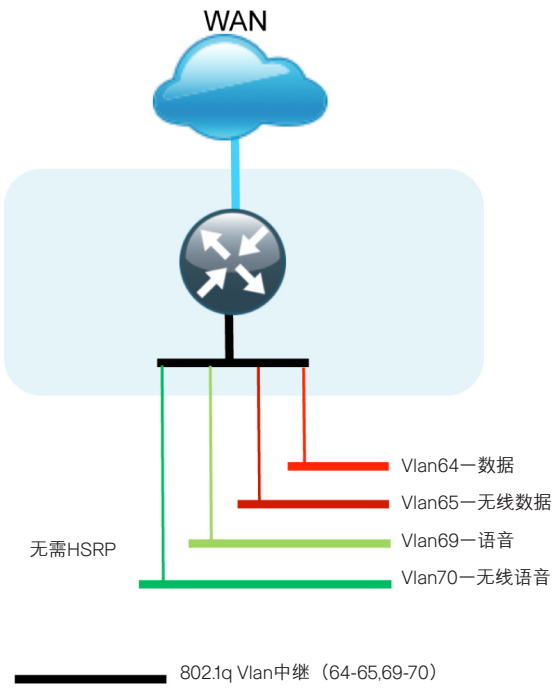
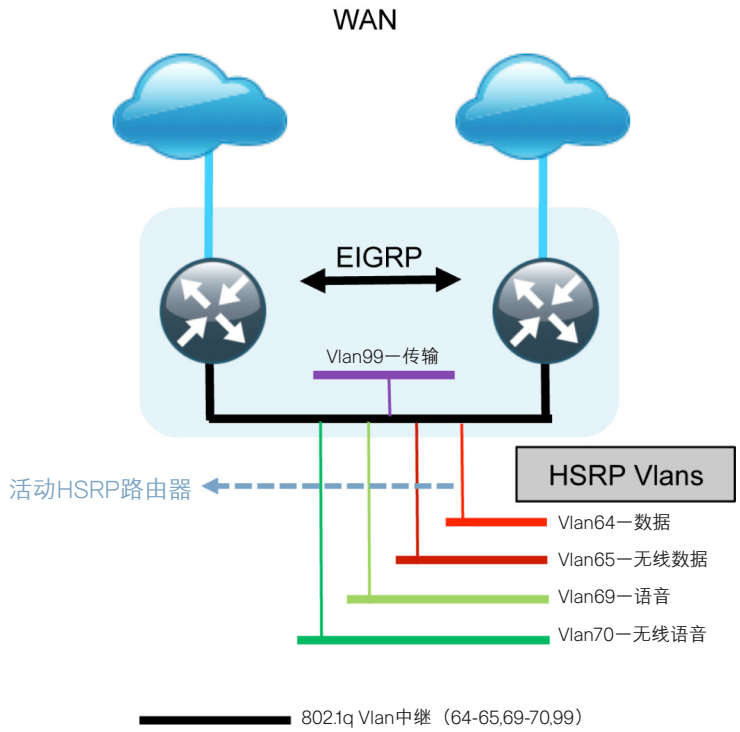



图6. 广域网远程站点——扁平型二层局域网（双路由器）




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。您应在路由器间配置增强型内部网关路由协议（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。

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、IP route reachability、IP service-level agreement (SLA) reachability，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，并发送给远程响应装置。响应装置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。此类路由器将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，我们前后使用了EOT与IP SLA。

为了缩短在发生主要DMVPN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DMVPN分支路由器发送至DMVPN中枢路由器，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。

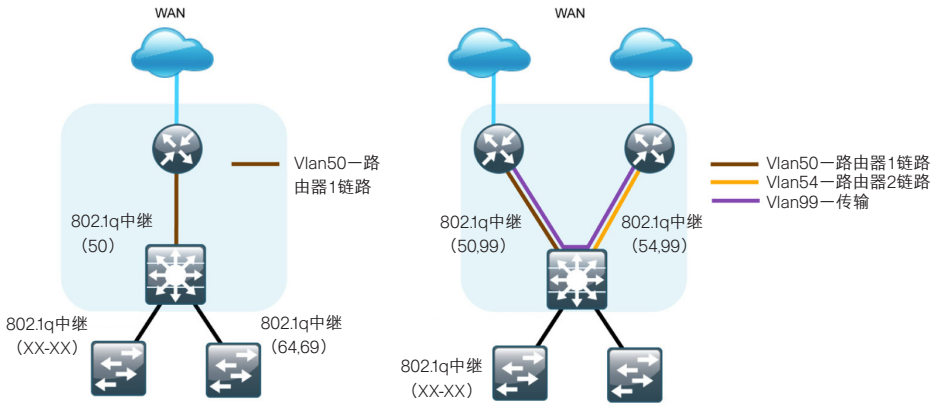
双路由器设计还提供了在特定情形下进行正确的路由所需的一个额外组件。在这些情况中，来自远程站点主机的流量可能被发送至通过备用广域网传输方案才能到达的目的地（例如：与仅使用DMVPN2的远程站点进行通信的双DMVPN远程站点）。之后，主要广域网传输路由器会通过相同的数据接口将流量发送至备用广域网传输路由器，由后者将该流量转发至正确的目的地。这一过程被称作“发夹”。

避免通过相同接口发送流量的正确方法是，在路由器间引入一个额外的链路，并将该链路设定为传输网络（Vlan 99）。传输网络不连接主机而仅用于路由器之间的通信。路由协议在分配给传输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中继配置能够轻松支持额外的子接口。

## 分布层与接入层

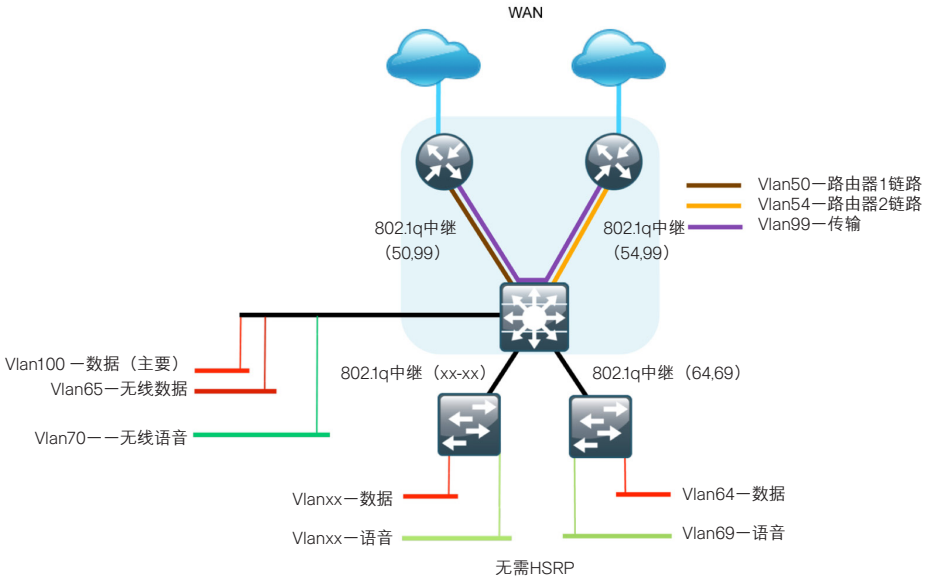
大型远程站点可能要求类似于小型园区局域网的局域网环境，其中包含有分布层和接入层。这一拓扑能够很好地支持单个或双路由器广域网边缘。要实施这一设计，路由器应通过EtherChannel链路连接到分布层交换机。这些EtherChannel链路被配置为802.1Q VLAN中继，这使在路由点对点链路中允许路由器和分布层交换机间运行EIGRP路由协议，且在双路由器设计中为两台广域网路由器之间提供直接的传输网络。

图7. 广域网远程站点——连接到分布层




分布层交换机以VLAN中继方式连接到接入交换机，处理所有接入层路由。当设计包含分布层时，无需使用HSRP。下图显示了一个完整的分布层与接入层设计。

图8. 广域网远程站点——分布层与接入层（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，然后将其从单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是一种控制平面功能，应置于网络的核心位置，或者与IP组播源通过三层交换机或路由器相连的临近的位置。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实施策略。该策略在稀疏模式协议独立组播协议（PIM SM）网络中提供了负载均衡与冗余能力。两个RP均衡源注册的负载，并能够互为彼此的热备用路由器。

从广域网的角度而言，这一策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程序机制，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。

但实际上，网络影响着所有流量，因此必须了解最终用户需求和提供的服务。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。

在该架构内，有线和无线连接选项提供了先进的分类、优先级划分、排队和拥塞机制，作为实现综合QoS的一部分，可确保网络资源得到最佳利用。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是本架构中使用的网络基础设施设备的一项重要功能。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，以保护流量正常和异常情况下网络的功能和可管理性。

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期间或在日后以最少的工作量和最小的系统影响，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5. QoS服务类别映射

| 服务类别 | 每跳行为(PHB) | 差分服务代码（DSCP） | IP优先(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, 34 | 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 |

## 广域网优化

思科广域应用服务（WAAS）是一款完善的广域网优化解决方案，能够通过广域网加快应用程序运行速度，向远程办事处提供视频，以及在本地托管远程站点IT服务。思科WAAS支持集中管理应用程序并使用数据中心内的存储，同时提供如同局域网般的应用程序性能。

WAAS能够对广域网上传输的应用程序和数据进行加速，优化带宽、支持云计算、并在本地托管远程站点IT服务，而所有这些优势均与行业领先的网络相集成。思科WAAS支持IT组织集中管理应用程序和存储，同时保持远程站点用户和移动用户的生产效率。

WAAS集中进行管理，要求在数据中心实地部署一个或多个Cisco WAAS Central Manager设备。所有这些设备均可通过Web界面进行访问。

用于优化广域网流量的设计要求在广域网汇聚站点和广域网远程站点均部署思科广域应用引擎（WAE）设备或模块。WAE运行WAAS软件，后者可提供广域网优化服务。此设计要求在每个位置部署一个或多个WAE设备。通过在一个站点放置多台设备，将可以实现出色的永续性。思科WAAS解决方案能够作为TCP代理与网络中的其他服务透明集成，并能够向最终用户提供广域网优化优势，而无需在广域网中创建优化隧道。

低带宽远程站点可以使用思科路由器上的Cisco IOS软件内嵌的WAAS Express（WAASx）功能。WAASx包括WAAS的几个基本功能，但不包括针对诸如CIFS和HTTP等的应用优化器（Application Optimizers）。

广域网优化解决方案与广域网路由器紧密集成，通过路由器控制采用WAAS优化的流量拦截和重导向工作。这一设计将在现有网段中部署WAE设备，从而无需对网络做出重大变动。

成功部署WAAS要求以下要素：

- 拦截广域网中往返的特定流量的方法
- 将选择的流量导向WAE设备以进行合理优化的能力
- WAE在优化后将优化的流量重新引入网络的能力

路由器使用Web缓存通信协议（WCCP）来拦截从局域网进入路由器的流量（来自客户端或数据中心），或从广域网进入路由器的流量（来自远程WAE）。作为WCCP重导向的一部分，流量将通过通用路由封装(GRE)隧道被转发至选定的WAE。

一个位置的多个WAE设备可作为集群运行。执行WCCP重导向的路由器负责在集群内的各个WAE设备间进行负载均衡。WAAS高可用性通过称作N+1模式的方式实现。这一名称意味着如果需要N个等效设备来提供所需性能，将同时需要一个额外的设备来提供冗余能力。

需要重新加入到网络中的流量使用协商返回WCCP GRE隧道输出方法来返回到发起路由器。这种方法为推荐方法，因为它允许将WAE设备放置在与WCCP路由器相距一个或多个路由跳数远的位置。该方法能够带来多项优势，将在本文后面的章节中进行详细介绍。

成功部署WAAS Express要求以下要素：

- 满足正确硬件要求的路由器，尤其是升级到最大的DRAM
- 用以支持WAAS Express的相应的特性许可

WAAS Express路由器不要求任何流量重导向和重新引入，因此不需要WCCP。该特性目前不支持多个活动链路，因此它仅在本设计中用于采用单一WAN传输方式的远程站点。

**备注**

# 部署广域网

## 整体广域网架构设计目标

### 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

在广域网远程站点，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作为主要或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，一个缺省路由将被通告给广域网远程站点。

## 局域网接入

所有远程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项故障情况，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、双链路类远程站点必须能够在任一广域网传输出现问题时继续正常运行。
- 双路由器、双链路类远程站点必须能够在任一边缘路由器或广域网传输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，以及远程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上的一个站点；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

双广域网传输方案的使用专门针对以活动/备用模式工作进行了调整。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DMVPN 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。

DMVPN主要+ DMVPN辅助双连接站点:

- 连接到同一DMVPN上的一个站点；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）

所有远程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程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的服务提供商时，广域网边缘QoS分类与处理方法必须与服务提供商的产品保持一致，以确保实现一致的端到端QoS流量处理方法。

## 应用优化

大多数从广域网汇聚站点到任意远程站点的业务应用流量，或从某一远程站点到任意其他远程站点的流量，应进行优化。

应用优化过程应对最终用户保持透明。应用优化设计应包含高可用性组件，以作为广域网设计的其他高可用性组件的补充。

## 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各种网络基础设施服务。这些参数如下表所列。

表6. 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 |
| 身份验证控制系统（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（DMVPN）WAN

## 业务概述

企业要求广域网能够为远程站点用户提供卓越的性能和出色的可靠性，以高效支持业务的开展。尽管远程站点员工使用的大多数应用和服务均位于中央位置，但广域网设计必须要为处于任意位置的员工带来相同的资源访问体验。

对于使用广域网传输方案来支持远程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足以为远程站点提供主要网络传输方案。此外，它们还能提供一种可选的传输方案，您可将其作为另一主要IP VPN的弹性备份。一个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。

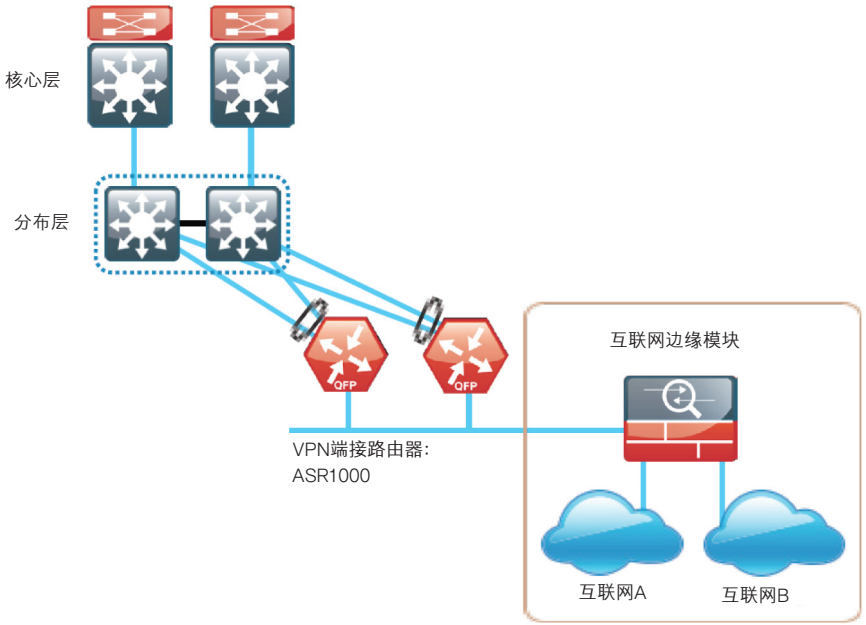
## 技术概述

### DMVPN 500设计

DMVPN 500设计可支持多达500个远程站点，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。这一设计使用Cisco ASR1002汇聚多业务路由器作为DMVPN中枢路由器。DMVPN 500设计使用了双互联网服务提供商和双DMVPN中枢路由器，如下图所示。

DMVPN VPN路由器通过包含在互联网边缘中的防火墙隔离区（DMZ）接口间接与互联网相连。如需了解有关主要站点互联网连接的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络互联网边缘部署指南》。VPN中枢路由器连接至防火墙DMZ接口，而非直接连接到互联网服务提供商路由器。

**图9.** DMVPN 500设计

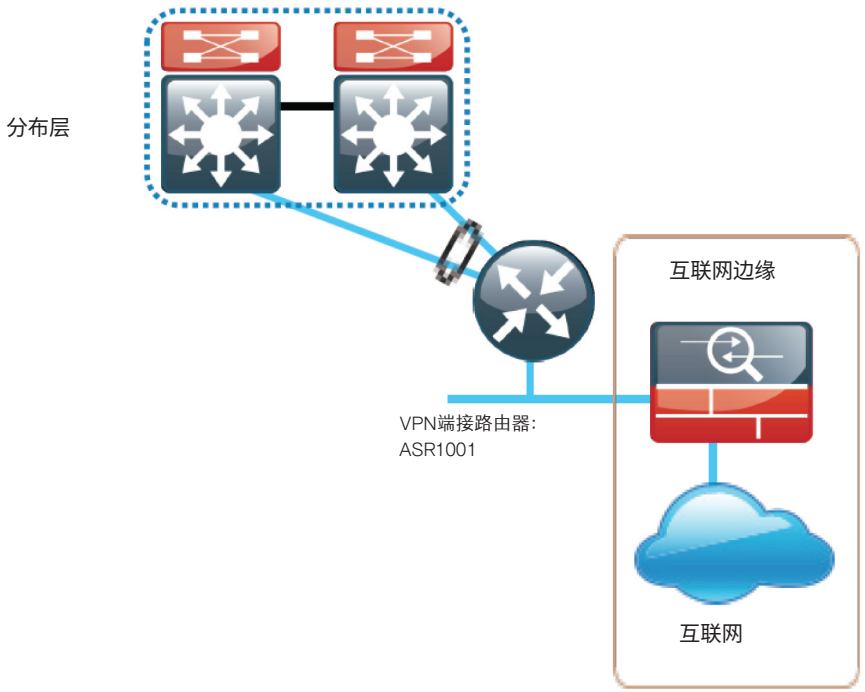



Cisco ASR1000系列汇聚多业务路由器是一款下一代、模块化集成业务思科路由平台。它们专为广域网汇聚而设计，具备出色的灵活性，能够支持广泛的4到16 Mpps数据包转发能力和2.5到20 Gbps系统带宽，并可进一步扩展。Cisco ASR 1000系列在硬件和软件方面均实现了全面的模块化。该款路由器具备真正的运营商级路由产品的全部要素，能够出色地支持企业和服务提供商网络。

## DMVPN 100设计

DMVPN 100设计可支持多达100个远程站点，广域网汇聚总带宽最高可达100 Mbps。DMVPN 100从本质上而言是DMVPN 500设计的一个小型版本，仅支持一个互联网服务提供商。这一版本用于提供有限的扩展能力。如果预计带宽或站点数量会进一步增长，则应考虑使用DMVPN 500设计。使用大型设计可避免由于设备升级导致的不必要的停机问题。此设计使用Cisco ASR1001汇聚多业务路由器作为DMVPN中枢路由器。DMVPN 100设计使用了单个互联网服务提供商和单个DMVPN中枢路由器，如下图所示。

**图10.** DMVPN 100设计




## 远程站点——DMVPN分支路由器选择

实际的广域网远程站点路由平台仍未确定，因为规格与站点的带宽要求、以及对于服务模块插槽使用的潜在要求紧密相关。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。

在选择广域网远程站点路由器时，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，以及支持拓扑所需特性集的相应思科IOS软件映像。思科测试了五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7.** 广域网远程站点集成多业务路由器方案

| | 1941[1] | 2911 | 2921 | 3925 | 3945 |
|---|---|---|---|---|---|
| 包含服务的以太网广域网[2] | 25 Mbps | 35 Mbps | 50 Mbps | 100 Mbps | 150 Mbps |
| 板载GE端口 | 2 | 3 | 3 | 3 | 3 |
| 服务模块插槽[3] | 0 | 1 | 1 | 2 | 4 |
| 冗余电源选项 | 无 | 无 | 无 | 有 | 有 |

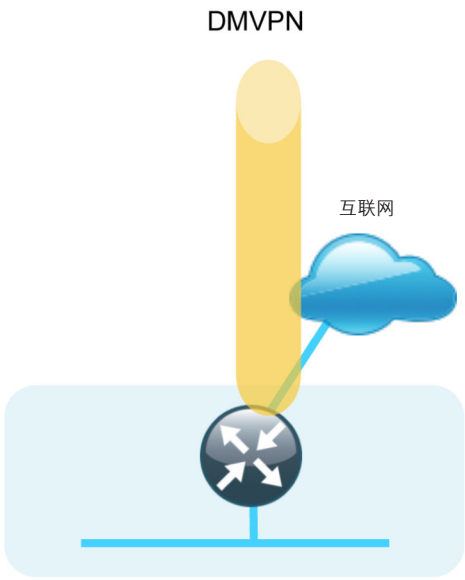
注：

1. 对于单路由器单链路远程站点，建议使用1941。
2. 性能数值为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. 一些服务模块为双宽模块。

广域网远程站点的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程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远程站点是适用于任意远程站点的最基本的构建模块。此设计可用于DMVPN分支路由器与接入层直接相连的情况，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，可在广域网汇聚站点使用静态路由和在远程站点使用静态缺省路由全盘处理。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。在动态路由中，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程站点添加或修改IP网络的工作。

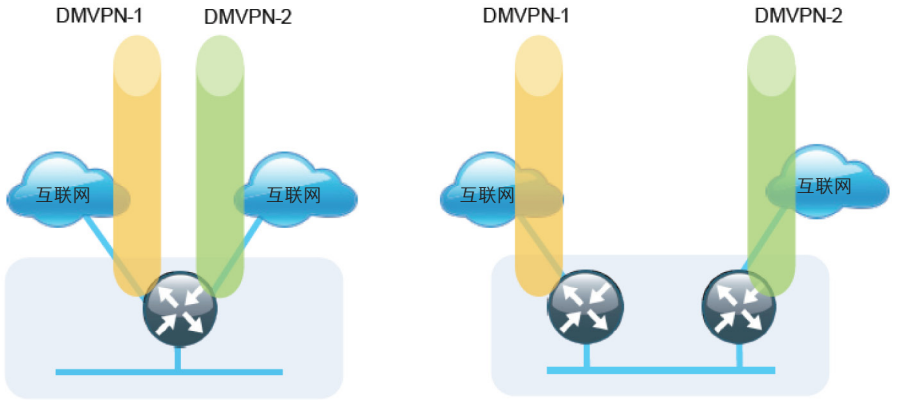
图11. DMVPN远程站点（单链路 — 单路由器）




DMVPN连接可用作主要广域网传输方案，或者用作另一DMVPN广域网传输方案的备用选择。DMVPN单链路设计可添加到现有的DMVPN广域网设计中，通过连接到相同的路由器或其他路由器提供更高的永续性。通过添加额外链路，您可以为远程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，将强制使用动态路由。路由协议将进行相应调节，以确保流量表现达到预期。

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12. DMVPN + DMVPN远程站点（双链路方案）




## 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。

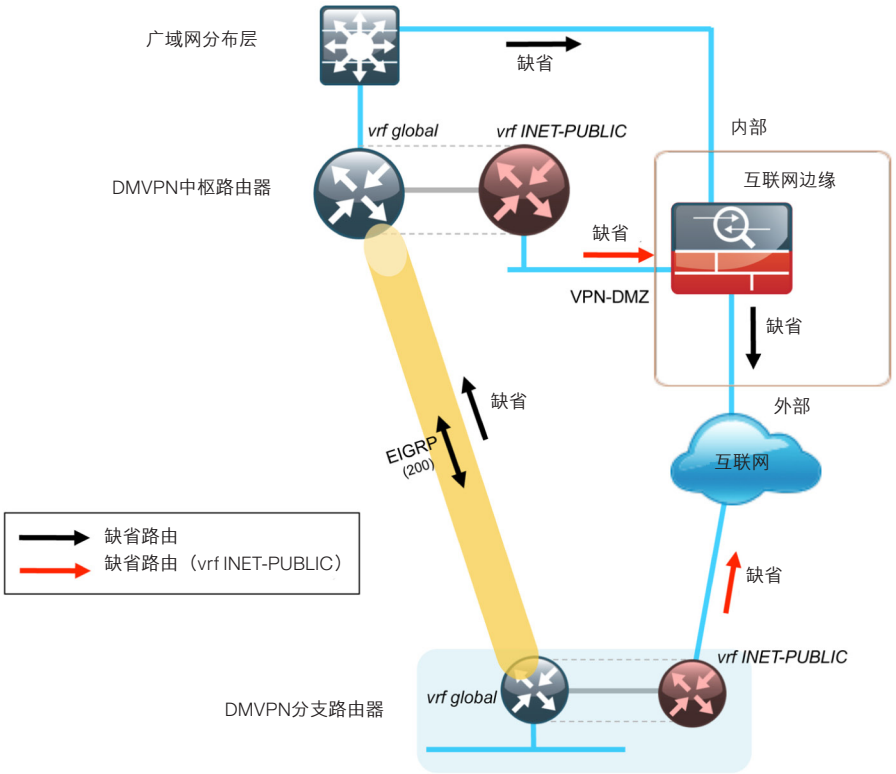
您可以通过为每一个VRF建立不同的路由表将VRF部署在网络设备中，这些路由表也被称作转发信息库(FIB)。或者，网络设备可能会配置不同的虚拟路由器，其中每一个都有各自的FIB，相同设备上的任意其他虚拟路由器无法对其进行访问。

最简单的VFR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。

这一广域网远程站点设计中使用的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程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 13.** Front door vREF (FVRF)



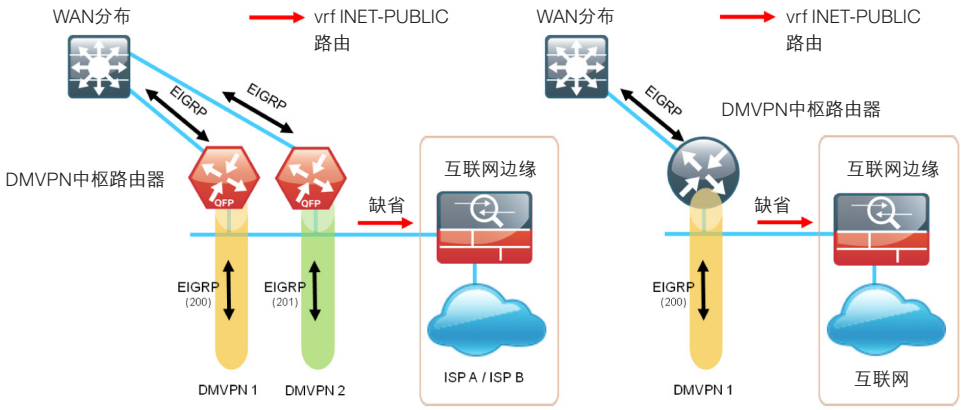

## 设计详情

DMVPN中枢路由器连接至分布层和DMZ中的弹性交换设备。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），其余用于DMVPN（EIGRP-200，EIGRP-201）。使用独立的EIGRP进程的主要原因是确保在部署其他IBA WAN设计时，与WAN汇聚站点路由选择过程的兼容性。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 14.** DMVPN 500/100设计——路由详细信息



## EIGRP

思科采用增强型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，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程站点。EIGRP-200和EIGRP-201被用于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8.** 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，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。考虑到其他潜在的开销，思科建议您采用1400字节MTU配置隧道接口。

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，这些动态方法并不奏效，通常是因为安全设备会过滤掉必要的探测流量。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。在这一解决方案中，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。

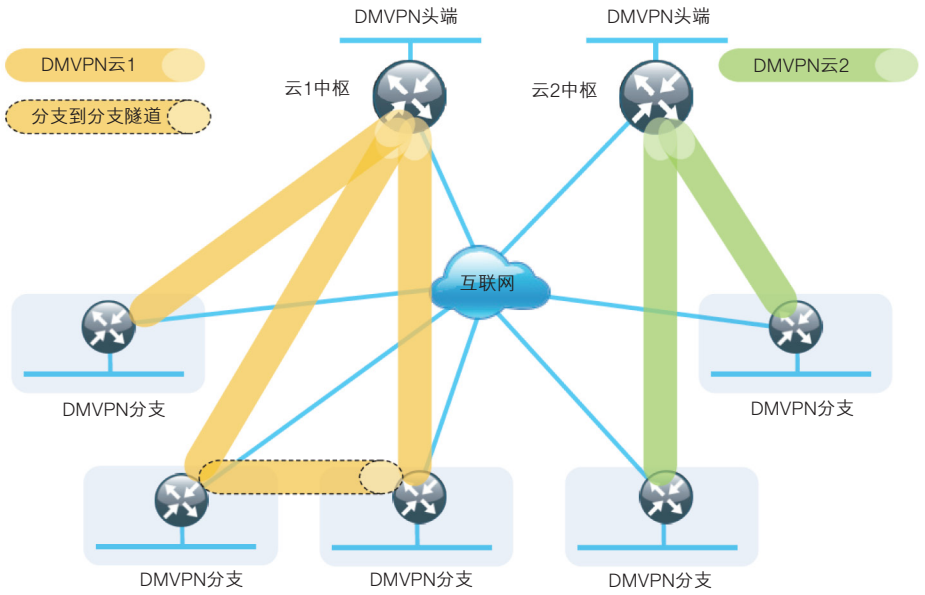
在本设计指南中，单链路用例使用互联网/DMVPN作为主要的WAN传输方案，要求使用DMVPN单云、单中枢（hub）设计。双链路用例要求DMVPN双云设计，每个云采用单中枢路由器。DMVPN路由器使用支持IP单播、IP组播和广播流量的隧道接口，包括使用动态路由协议。在初始星型隧道激活后，可以创建动态分支到分支隧道，以满足站点间IP流量传输的需要。

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-1918 IP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）持活时距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15. 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，通常借助互联网提供商提供的DHCP实现。分支路由器可以充分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。这一配置对于确保路由器正常工作至关重要，因为每一台分支路由器都会在其配置中嵌入这些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。

表9. 部署中使用的通用网络服务示例

| 服务 | 地址 |
|---|---|
| 主机名: | VPN-ASR1002-1 |
| 路由器回环IP地址: | 10.4.32.243/32 |
| 路由器端口通道IP地址: | 10.4.32.18/30 |

## 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

此流程假设已根据《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》的指导配置了分布层交换机。其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。

局域网分布层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至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。

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。

```
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-protocol lacp
  channel-group 3 mode active
  logging event link-status
  logging event trunk-status
  logging event bundle-status
  no shutdown
```

步骤3：配置连接到局域网核心层的接口，以汇总广域网网络范围。

```
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
```

步骤4：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
```

## 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-ASR1000-1
```

步骤2：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)提供了设备身份验证和数据加密功能。

通过使用SSH和HTTPS协议，能对局域网设备进行安全的管理。这两个协议均进行了加密，可提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

```
cdp run
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

启用简单网络管理协议(SNMP)后，能够通过网络管理系统（NMS）对网络基础设施设备进行管理。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3**：配置安全用户身份验证。

启用身份验证、授权与记账（AAA）来支持访问控制。所有针对网络基础设施设备的管理访问（SSH和HTTPS）均受到AAA的控制。

**读者提示**

本架构中使用的AAA服务器是思科ACS。如需了解有关ACS配置的更多信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络网络设备身份验证与授权部署指南》。

TACACS+是在基础设施设备上向AAA服务器验证管理登录所采用的主要协议。此外，系统还在每个网络基础设施设备上定义了一个本地AAA用户数据库，用于在中央TACACS+服务器不可用时，提供备用身份认证源。

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

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
```

**步骤5**：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。从分布层交换机向网络其余部分汇总的IP地址块中分配回环地址。

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

ip pim sparse-mode命令将在该流程中做进一步介绍。

将SNMP和SSH进程绑定到回环接口地址，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6**：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7**：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 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 mode active
  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-channel 3
```

## 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描述符（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，以便可以任意选择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
```

**读者提示**

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中枢路由器通过Cisco ASA5500自适应安全设备建立连接，并使用了专为VPN端接路由器创建和配置的DMZ接口。

**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。

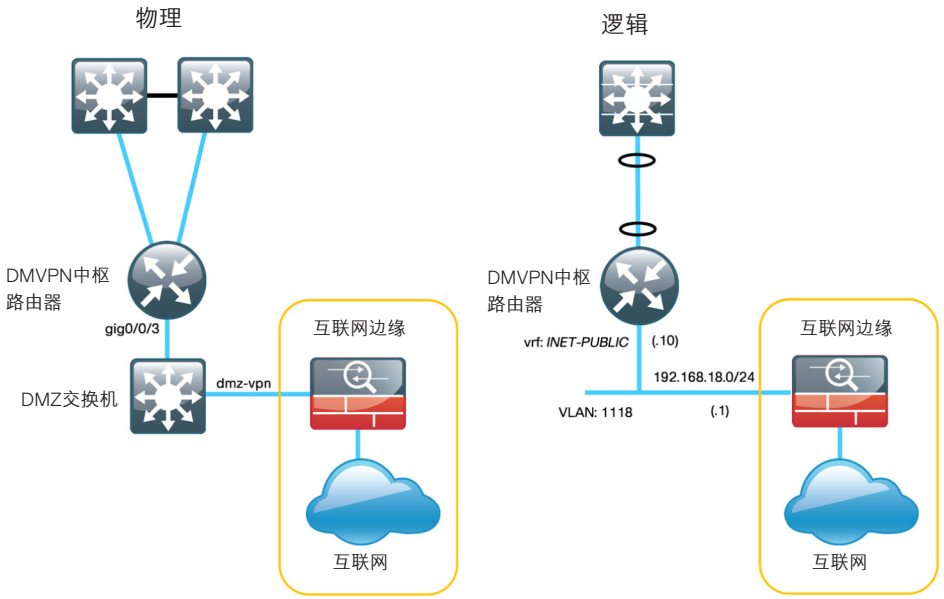
```
interface GigabitEthernet0/0/3
 ip vrf forwarding INET-PUBLIC
 ip address 192.168.18.10 255.255.255.0
 no shutdown
```

**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16. DMZ连接的物理视图与逻辑视图




## 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）进行身份验证
- 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）身份验证算法的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10.** 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，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。使用您用于连接至互联网的的同一源接口。将tunnel vrf命令设置成之前为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 GigabitEthernet0/0/3
 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和身份验证密钥。NHRP缓存保持时间应设置为600秒。

EIGRP（在以下程序中配置）依赖于组播传输方案，并需要NHRP来自动向组播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。

```
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。

**读者提示**

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，但是针对您首先需要配置的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命令所覆盖。

EIGRP问候间隔增加至20秒，EIGRP保持时间增加至60秒，以支持单个DMVPN云中的多达500个远程站点。

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

## 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程站点中获知的路由，能够在广域网分布层交换机上显示为EIGRP外部路由。如果您仅使用一个进程，远程站点路由将在广域网分布层交换机上显示为EIGRP内部路由。任意MPLS VPN获知的路由适于使用这一方法。

**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 0.0.1.255
 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。

此设计使用相互路由重分布。来自EIGRP-200进程的DMVPN路由重分布到EIGRP-100中，而其他从EIGRP-100获知的路由则重分布到EIGRP-200中。由于路由协议相同，因此无需缺省度量值。

当使用这种相互路由重分布时，严密控制不同路由协议间共享路由信息的方式非常重要；否则可能会出现路由翻动问题，即特定路由在设备路由表中重复进行安装和撤销。正确的路由控制可确保路由表的稳定性。

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11.** 针对DMVPN中枢路由器的路由标签信息

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

本例中包含参考设计中的所有WAN路由来源。根据您网络的实际设计，您可能需要使用更多的标签。

```
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
```

## 流程

防火墙和DMZ交换机配置

1. 配置DMZ交换机
2. 配置隔离区接口
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

此程序假设已根据《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》的指导配置了交换机。其中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汇聚路由器的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 GigabitEthernet1/0/24
 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汇聚路由器的接口。

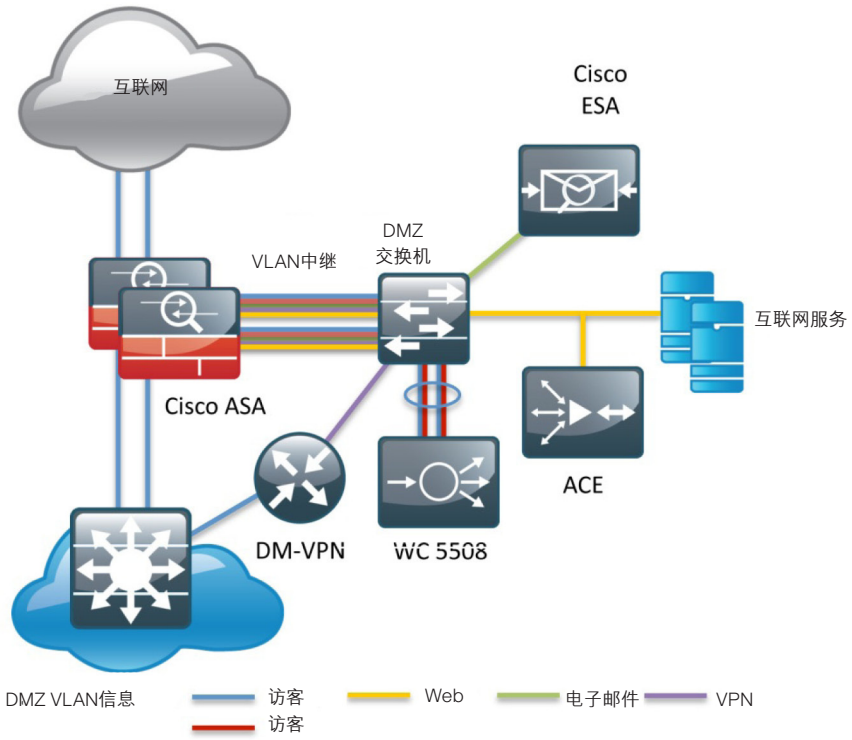
```
interface GigabitEthernet1/0/7
 description VPN-ASR1000-1 Gig0/3
!
interface GigabitEthernet2/0/7
 description VPN-ASR1000-2 Gig0/3
!
interface range GigabitEthernet1/0/7, GigabitEthernet2/0/7
 switchport access vlan 1118
 switchport host
 macro apply EgressQoS
 logging event link-status
 no shutdown
```

## 程序2　配置隔离区接口

防火墙的隔离区(DMZ)是严格限制流量进出网络其它部分的网络区域。企业将网络服务放置在DMZ中，以便通过互联网进行访问。除非情况特殊，通常不允许这些服务器与内部网络建立连接。

DMZ网络通过VLAN中继连接到ASA的千兆以太网接口，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。中继将ASA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IP地址，用于管理交换机。

**图17.** DMZ VLAN拓扑和服务



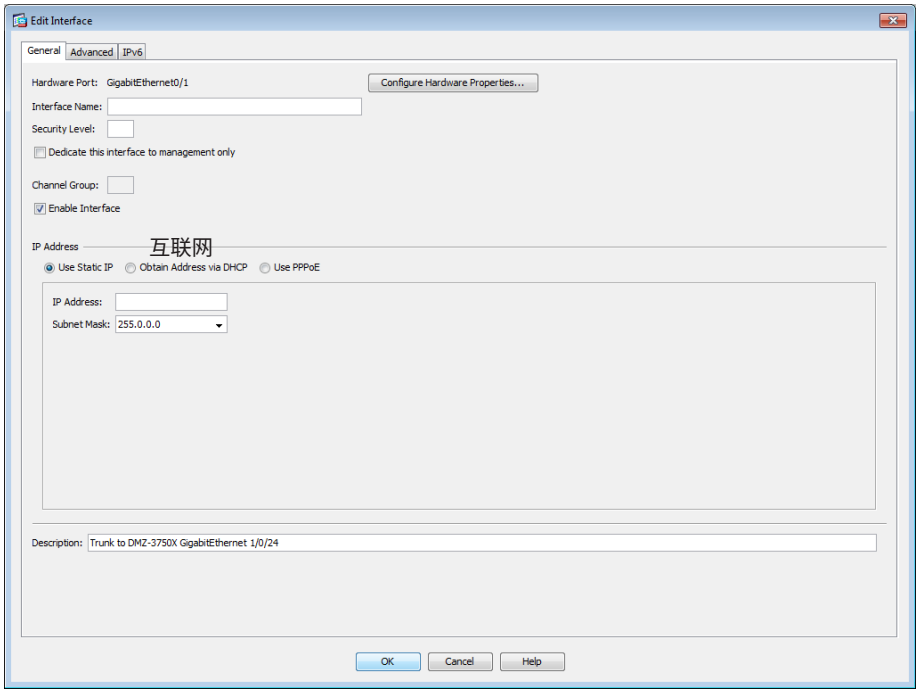

**技术提示**

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，点击连接到DMZ交换机的接口。（例如：GigabitEthernet0/1)

**步骤2**：点击Edit（编辑）。

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




**步骤4**：在Interface（接口）窗格，点击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)

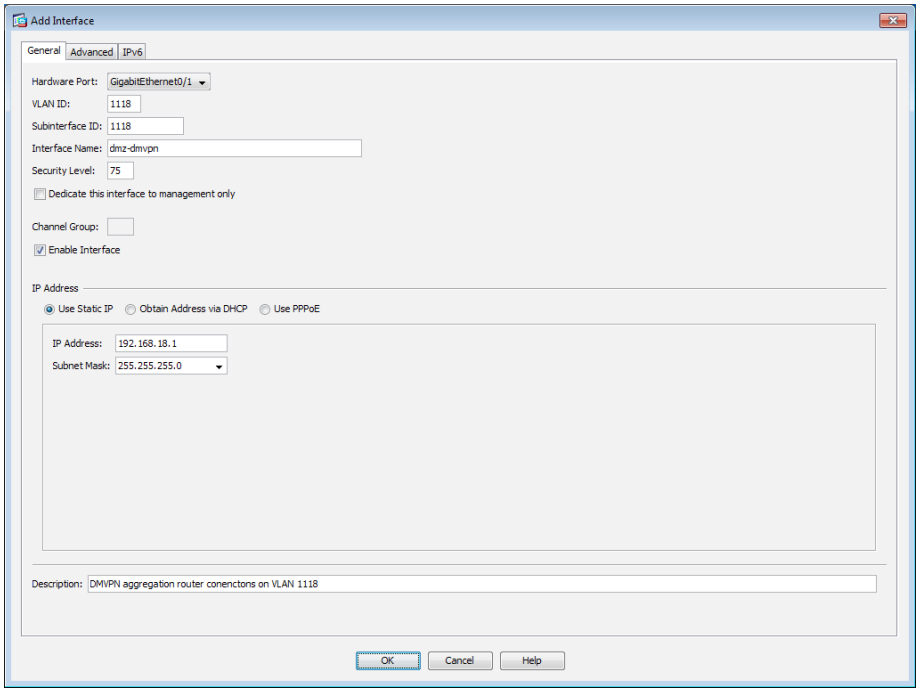
步骤8：输入一个Interface Name（接口名称）。（例如：dmz-dmvpn)

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），然后点击OK。（例如：255.255.255.0)

步骤12：点击Apply（应用）。

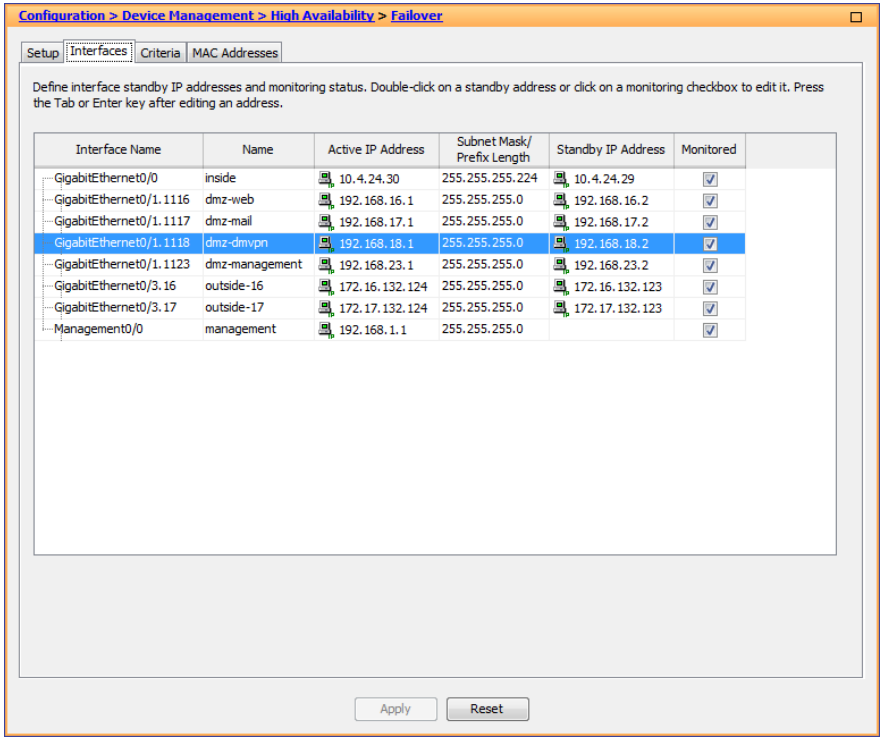



步骤13：在Configuration（配置） > Device Management（设备管理） > High Availability（高可用性）>点击Failover（故障切换）。

步骤14：在Interfaces（接口）选项卡上，针对在步骤4中创建的接口，在Standby IP address（备用IP地址）栏中，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：点击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汇聚路由器的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汇聚路由器DMZ地址 | DMVPN汇聚路由器公共地址（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）>点击Network Objects/ Groups（网络对象/组）。

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

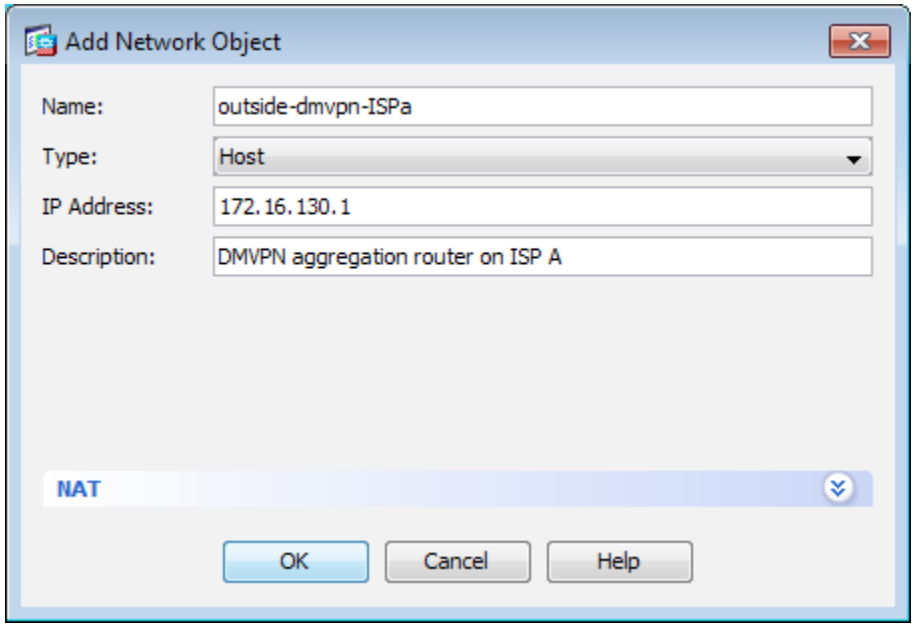
**步骤2**：点击Add（添加）> Network Object（网络对象）。

**步骤3**：在Add Network Object（添加网络对象）对话框上，在Name（名称）框中，为DMVPN汇聚路由器的公共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汇聚路由器的公共IP地址，然后点击OK。（例如：172.16.130.1)

**步骤6**：点击Apply（应用）。




接下来，你可以为DMVPN汇聚路由器的专用DMZ地址添加一个网络对象。

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

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

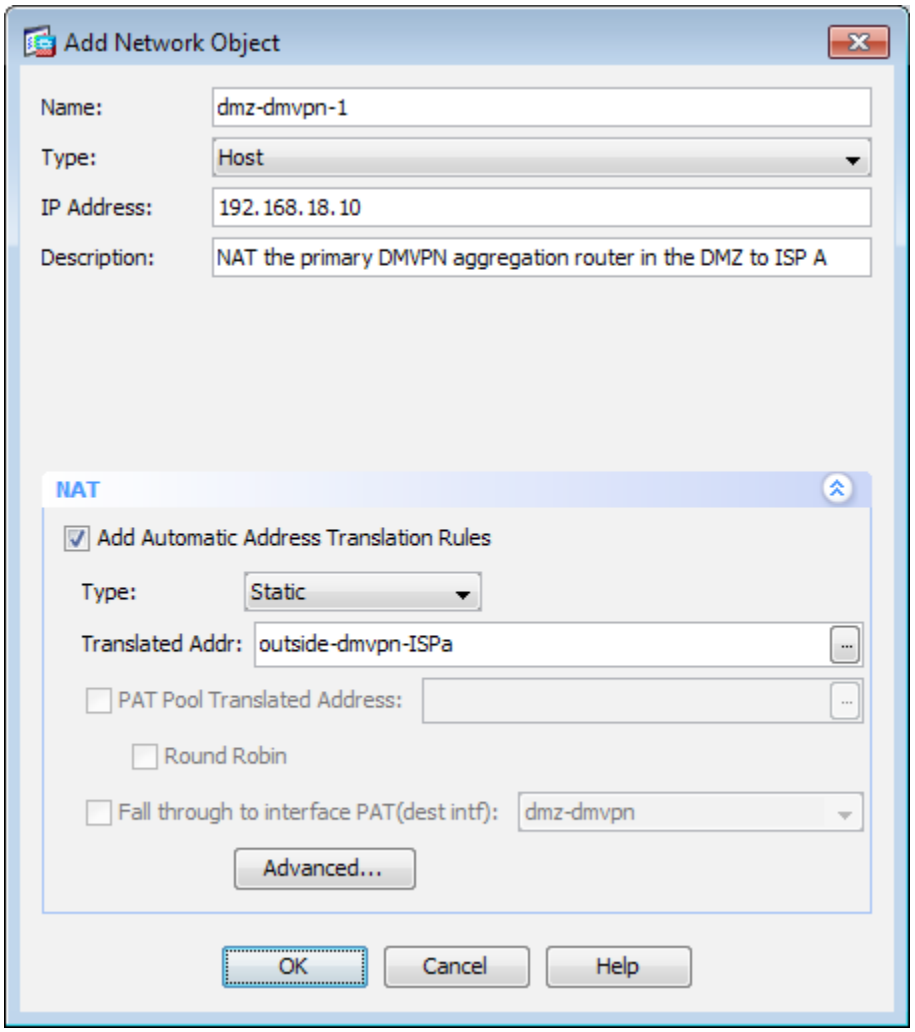
**步骤9**：在Type（类型）列表中，选择Host（主机）。

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

**步骤11**：点击两个向下箭头。NAT窗格会展开。

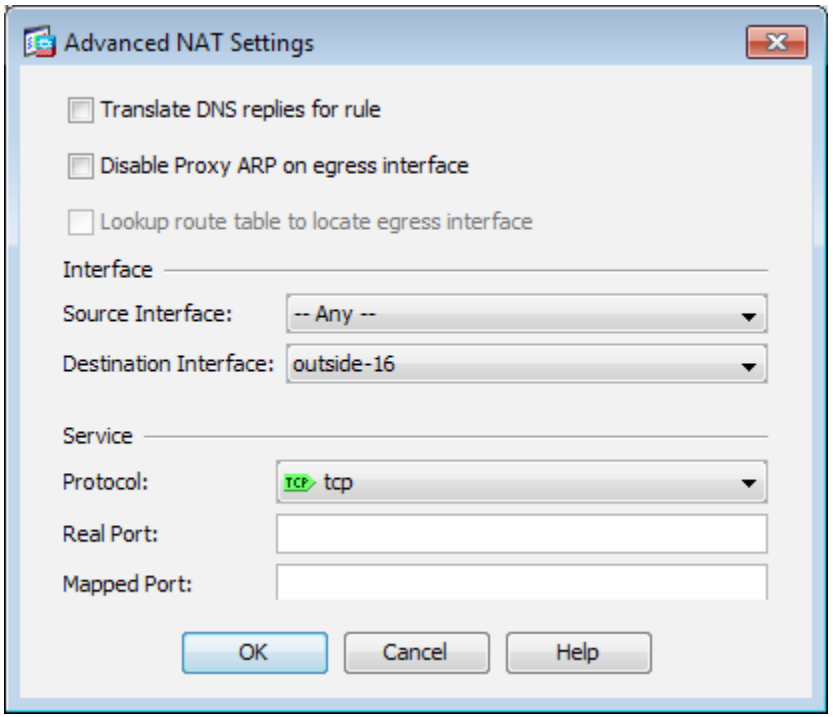
**步骤12**：选择Add Automatic Address Translation Rules（添加自动地址转换规则）。

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。




步骤14：点击Advanced（高级）。

步骤15：在Destination Interface（目的地接口）列表中，选择主用互联网连接的接口名称，然后点击OK。（例如：outside-16)




步骤16：点击OK（确定）。

步骤17：点击Apply（应用）。

步骤18：针对永续DMVPN汇聚路由器，重复这一流程。

## 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。过滤器仅允许DMVPN相关的流量到达DMVPN汇聚路由器。

表12.所需的DMVPN协议（汇聚路由器）

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

表13.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**：点击规则，拒绝流量从DMZ流向其他网络。

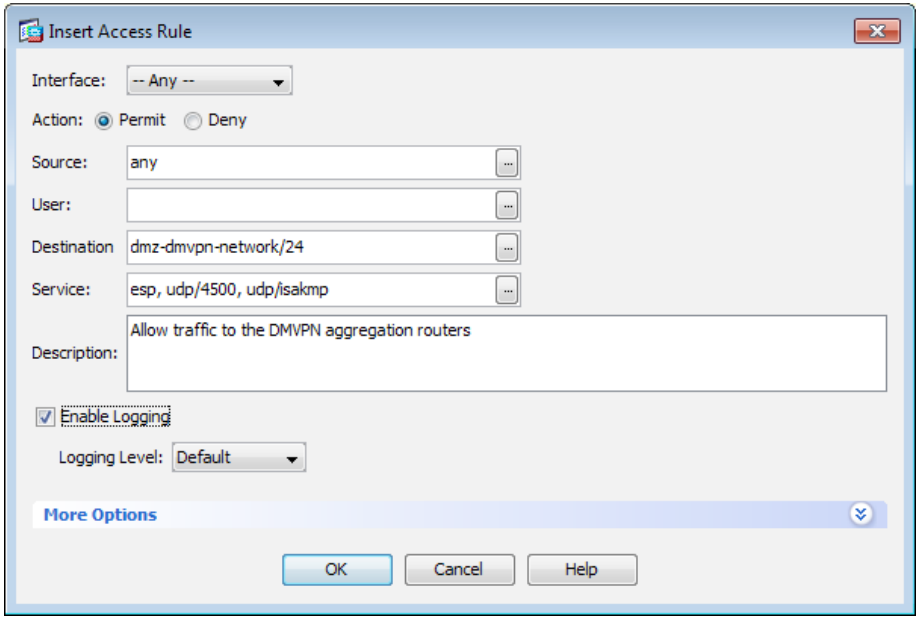
接下来，您必须在您选择的规则之上插入一个新的规则。

**步骤3**：点击Add（添加）> Insert（插入）。

你必须支持DMVPN远程路由器与DMZ中的DMVPN汇聚路由器进行通信。

**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，然后点击OK。



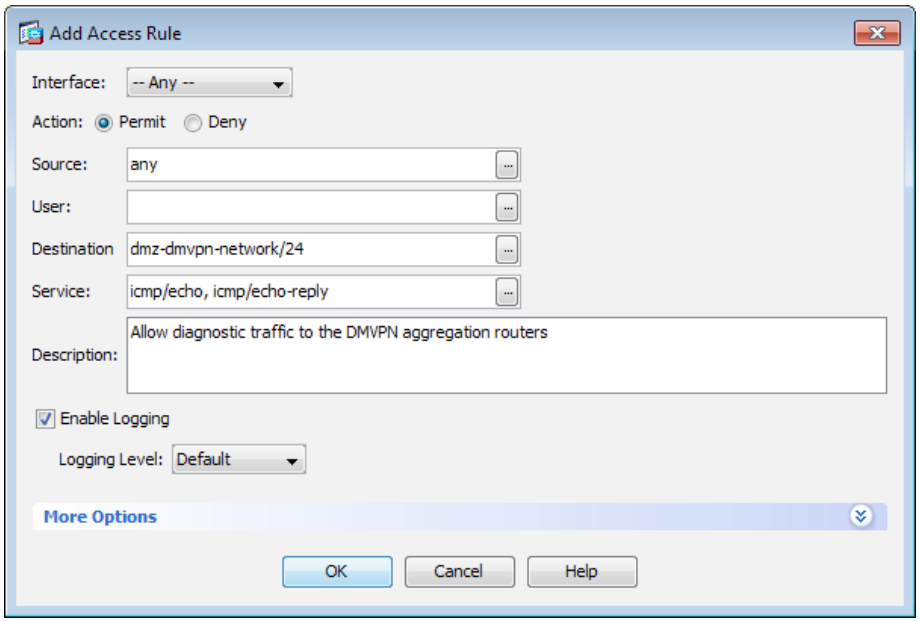

接下来，您必须插入一个新规则，以允许诊断流量到达DMVPN汇聚路由器。

**步骤6**：点击Add（添加）> Insert（插入）。

你必须支持DMVPN远程路由器与DMZ中的DMVPN汇聚路由器进行通信。

**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，然后点击OK。




**步骤9**：点击Apply（应用）。

## 流程

远程站点DMVPN分支路由器配置

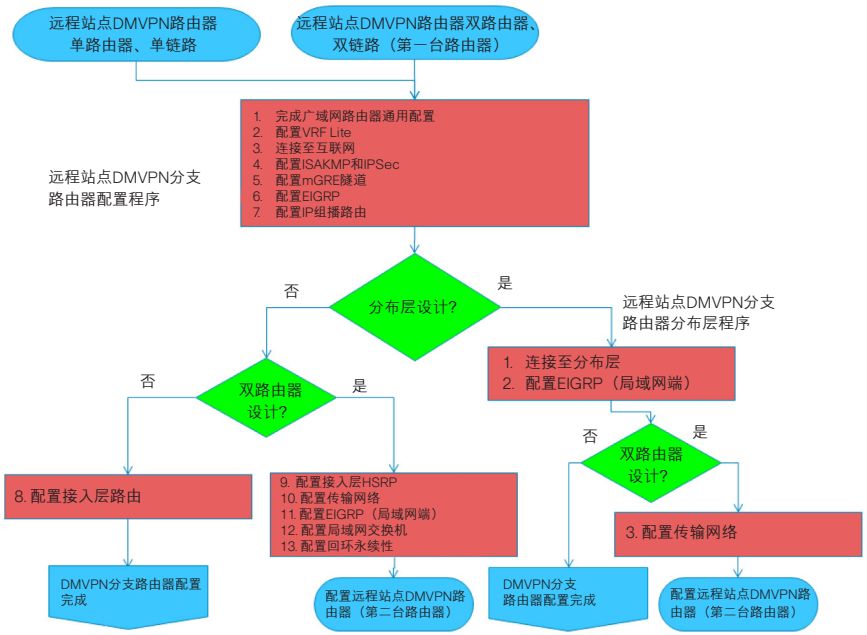
1. 完成广域网路由器通用配置
2. 配置VRF Lite
3. 连接至互联网
4. 配置ISAKMP和IPsec
5. 配置mGRE隧道
6. 配置EIGRP
7. 配置IP组播路由
8. 配置接入层路由
9. 配置接入层HSRP
10. 配置传输网络
11. 配置EIGRP（局域网端）
12. 配置局域网交换机
13. 配置回环永续性

这组程序用于为DMVPN远程站点（单路由器、单链路）配置DMVPN分支路由器，已经包含了所有必需的程序。

在配置DMVPN + DMVPN远程站点时，您也应该使用这组程序。当您配置双路由器、双链路设计的第一台路由器时，请使用这些程序。

下面的流程图详细介绍了如何配置远程站点DMVPN分支路由器。

图18. 远程站点DMVPN分支路由器配置流程图




## 程序1 完成广域网路由器通用配置

在本设计中，有些特性和服务在所有广域网远程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)提供了设备身份验证和数据加密功能。
通过使用SSH和HTTPS协议，能对局域网设备进行安全的管理。这两个协议均进行了加密，可提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

启用简单网络管理协议(SNMP)后，能够通过网络管理系统（NMS）对网络基础设施设备进行管理。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3**：配置安全用户身份验证。

启用身份验证、授权与记账（AAA）来支持访问控制。所有针对网络基础设施设备的管理访问（SSH和HTTPS）均受到AAA的控制。

**读者提示**

本架构中使用的AAA服务器是思科ACS。如需了解有关配置ACS的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络网络设备身份验证与授权部署指南》。

TACACS+是在基础设施设备上向AAA服务器验证管理登录所采用的主要协议。此外，系统还在每个网络基础设施设备上定义了一个本地AAA用户数据库，用于在中央TACACS+服务器不可用时，提供备用身份认证源。

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

您应将您的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
```

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
```

**步骤5**：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。从分布层交换机向网络其余部分汇总的IP地址块中分配回环地址。

```
interface Loopback0
  ip address [ip address] 255.255.255.255
  ip pim sparse-mode
```

ip pim sparse-mode命令将在该流程中做进一步介绍。

将SNMP和SSH进程绑定到回环接口地址，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6**：配置IP组播路由。

IP组播允许基础设施（即路由器和交换机）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——基于稀疏模式组播操作，思科使用autorp提供了一种简单但可扩展的方法，来构建具备高永续性的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，以便可以任意选择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
```

### 读者提示

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 连接至互联网

采用DMVPN的远程站点可以使用静态或者动态分配的IP地址。思科使用DHCP分配的外部地址测试了设计，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。这种设计提供了出色的安全性。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-PUBLIC
 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14. 所需的DMVPN协议

| 名称 | 协议 | 用途 |
|---|---|---|
| non500-isakmp | UDP 4500 | 基于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15. 可选协议——DMVPN分支路由器

| 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, 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PSK（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）
- 使用PSK进行身份验证
- Diffie-Hellman组：2

启用DPD，每30秒间隔发送一次持活时距，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-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）身份验证算法的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，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。源接口应与用于连接互联网的接口相同。tunnel vrf命令应设置成之前为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 GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC
 tunnel protection ipsec profile DMVPN-PROFILE
```

**步骤3**：配置NHRP。

DMVPN中枢路由器为面向所有分支的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。

NHS所使用的值为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。本设计方案使用了下表中所示的值。

**表16.** DMVPN隧道参数

| DMVPN云 | 隧道IP地址 | 隧道编号 | NHRP网络ID |
|---|---|---|---|
| 主用 | 10.4.34.1/23 | 10 | 101 |
| 备用 | 10.4.36.1/23 | 11 | 102 |

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份验证密钥。NHRP缓存保持时间应设置为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选项允许您改写现有的缓存条目。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。

您将在下面的程序中配置EIGRP，但首先您需要针对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个远程站点。

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

远程站点局域网必须进行通告。远程站点的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

在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存根路由，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
 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，并在所有三层接口上启用该模式，包括DMVPN隧道接口。

不要在互联网接口上启用PIM，因为这一接口不得用于请求组播流量。

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

**步骤2**：为DMVPN隧道启用PIM非广播多点接入模式

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NBMA问题，您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。

```
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。您可以将通过分支路由器的DR优先级设置为0来避免这种情况。

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

## 程序8 配置接入层路由

在接入层设计中，远程站点使用紧缩路由（collapsed routing），并通过802.1Q中继接口连接至局域网接入层。VLAN编号仅在本地有意义。接入交换机仅限用于二层。

**步骤1**：启用物理接口

```
interface GigabitEthernet [number]
 no ip address
 no shutdown
```

**步骤2**：创建子接口和分配VLAN标签。

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

**步骤3**：为每一个子接口配置IP设置

这一设计使用了IP地址惯例，缺省网关路由器分配到的IP地址和IP掩码组合为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来到达中央DHCP服务器。

如果远程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  GigabitEthernet [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [LAN network 1] [LAN network 1 netmask]
 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 10.5.12.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.5.10.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.13.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.11.1 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim sparse-mode
```

**步骤4**：在局域网交换机上配置中继。

使用802.1Q中继来连接此上游设备，允许该设备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监听和地址解析协议(ARP)检测设置为可信。

```
default interface GigabitEthernet [number]
!
interface GigabitEthernet [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,65,69,70
  switchport mode trunk
  macro apply EgressQoS
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

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

以下程序（程序9至程序13）仅适用于双路由器设计。

## 程序9　配置接入层HSRP

### 仅适用于双路由器设计

您需要配置HSRP来支持使用虚拟IP（VIP）作为缺省网关，在两台路由器之间共享。HSRP活动路由器是与主要运营商相连的路由器，HSRP备用路由器是连接到辅助运营商或备用链路的路由器。配置HSRP活动路由器，其备用优先级高于HSRP备用路由器。

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17. 广域网远程站点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 |

分配的IP地址将取代在前一程序中配置的地址，因此缺省网关IP地址将在拥有一台或两台路由器的各个位置保持一致。

双路由器接入层设计需要进行一些修改，以支持弹性组播。PIM DR应位于HSRP活动路由器之上。指定路由器（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，并不要求您使用相同的值。

此程序应针对所有数据或语音子接口重复进行。

```
interface GigabitEthernet [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 1 ip [LAN network 1 gateway address]
 standby 1 priority 110
 standby 1 preempt
```

**示例**

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.12.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.12.1
 standby 1 priority 110
 standby 1 preempt
!
interface GigabitEthernet0/2.65
 description WirelessData
```

```
 encapsulation dot1Q 65
 ip address 10.5.10.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.10.1
 standby 1 priority 110
 standby 1 preempt
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.13.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.13.1
 standby 1 priority 110
 standby 1 preempt
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.11.2 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.11.1
 standby 1 priority 110
 standby 1 preempt
```

## 程序10 配置传输网络

### 仅适用于双路由器设计

两台路由器之间需要配置传输网络。该网络用于支持路由器间通信，并避免“发夹”问题。传输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 GigabitEthernet0/2 [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 10.5.8.1 255.255.255.252
 ip pim sparse-mode
```

## 程序11 配置EIGRP（局域网端）

### 仅适用于双路由器设计

您必须在两台路由器之间配置路由协议。这可以确保HSRP活动路由器获得所有广域网远程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。除了传输网络子接口外，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接口的广域网接口。

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

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

这一步骤仅应在DMVPN分支路由器上完成。

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，因此无需缺省度量值。

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

## 程序12 配置局域网交换机

**步骤1**：局域网交换机上的中继配置

使用802.1Q中继连接此上游设备，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监听和ARP检测被设置为可信。

```
default interface GigabitEthernet [number]
!
interface GigabitEthernet [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,65,69,70,99
  switchport mode trunk
  macro apply EgressQoS
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

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

## 程序13　配置回环永续性

### 仅适用于双路由器设计

远程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。

如果广域网协议是EIGRP

**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
```

**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 [as]
redistribute eigrp 100 route-map LOOPBACK-ONLY
eigrp stub connected summary redistributed
```

如果广域网是BGP

**步骤3**：配置BGP来通告邻接路由器的回环网络

```
router bgp 65511
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
```

## 流程

在DMVPN分支路由器上启用DMVPN备份

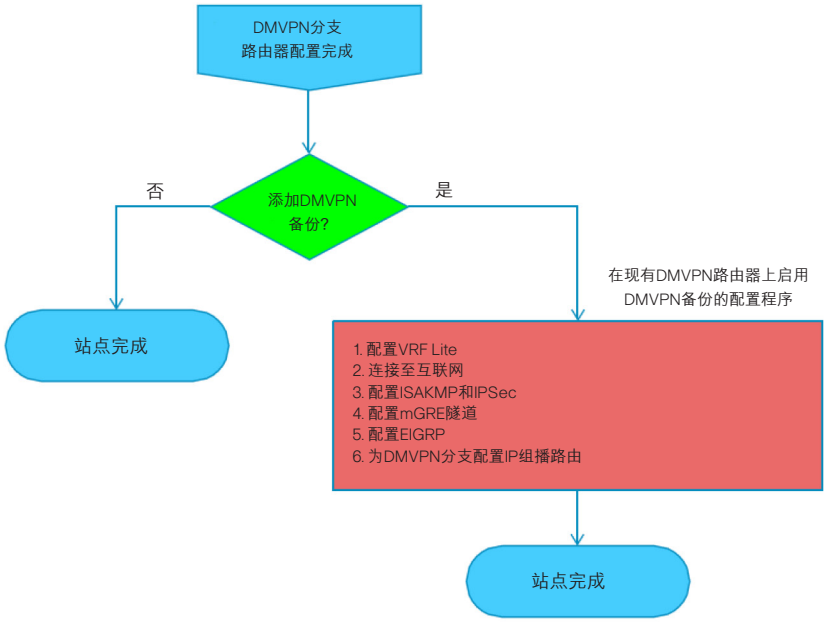
1. 配置VRF Lite
2. 连接至互联网
3. 配置ISAKMP和IPsec
4. 配置mGRE隧道
5. 配置EIGRP
6. 配置IP组播路由

这组程序包括了为DMVPN + DMVPN远程站点（单路由器、双链路）配置DMVPN分支路由器所需的额外步骤。

以下程序假定已经完成了为DMVPN广域网远程站点（单路由器、单链路）配置DMVPN分支路由器的工作。此处仅包含了向正在运行的DMVPN分支路由器添加DMVPN备份的额外程序。

下面的流程图详细介绍了如何在现有的远程站点DMVPN分支路由器上添加DMVPN备份。

图19. 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Front Door VRF。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，以便可以任意选择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-PUBLIC2
 rd 65512:2
```

### 读者提示

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　连接至互联网

采用DMVPN的远程站点可以使用静态或者动态分配的IP地址。思科使用DHCP分配的外部地址测试了设计，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。这种设计提供了出色的安全性。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-PUBLIC2
 ip address dhcp
 no cdp enable
 no shutdown
```

**步骤2**：配置并应用访问列表。

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18.** 所需的DMVPN协议

| 名称 | 协议 | 用途 |
|---|---|---|
| non500-isakmp | UDP 4500 | 基于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19.** 可选协议—DMVPN分支路由器

| 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, 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-KEYRING2 vrf INET-PUBLIC2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
```

**步骤2**：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3**：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，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。使用您用于连接互联网的同一源接口。将tunnel vrf命令设置成之前为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 GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel vrf INET-PUBLIC2
 tunnel protection ipsec profile DMVPN-PROFILE2
```

**步骤3**：配置NHRP。

DMVPN中枢路由器为面向所有分支的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。

NHS所使用的值为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。本设计方案使用了下表中所示的值。

表20. DMVPN隧道参数

| DMVPN云 | 隧道IP地址 | 隧道编号 | NHRP网络ID |
|---|---|---|---|
| 主用 | 10.4.34.1/23 | 10 | 101 |
| 备用 | 10.4.36.1/23 | 11 | 121 |

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份验证密钥。NHRP缓存保持时间应设置为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选项允许您改写现有的缓存条目。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。

您将在下面的程序中配置EIGRP，但首先您需要针对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个远程站点。

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

远程站点局域网必须进行通告。远程站点的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。如果汇总内的任意网络出现在路由表中，汇总将被通告给DMVPN中枢，从而提供了一种永续性衡量机制。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5　配置EIGRP

在DMVPN分支路由器上运行一个额外的EIGRP-201进程，来支持第二个DMVPN云。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存根路由，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
 passive-interface default
 no passive-interface Tunnel11
 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，并在所有三层接口上启用该模式，包括DMVPN隧道接口。

不要在互联网接口上启用PIM，因为这一接口不得用于请求组播流量。

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

**步骤2**：为DMVPN隧道启用PIM 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NBMA问题，您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。

```
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
```

## 流程

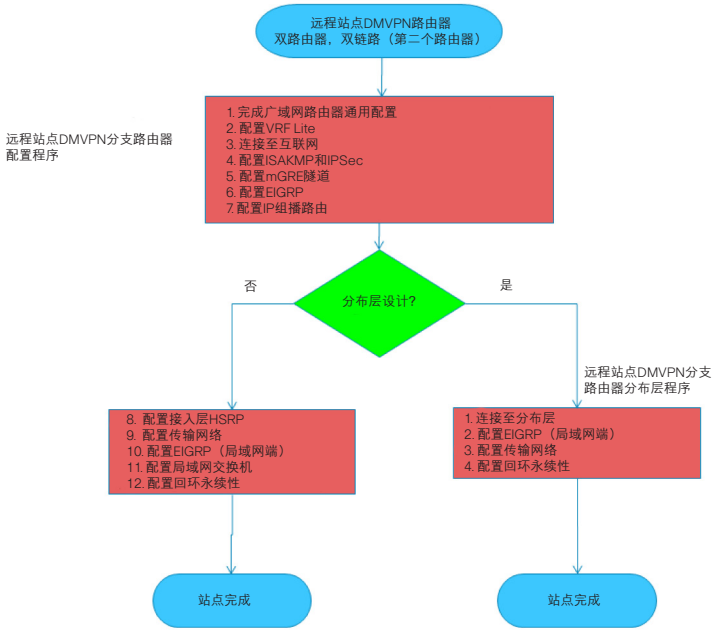
远程站点DMVPN分支路由器配置

1. 完成广域网路由器通用配置
2. 配置VRF Lite
3. 连接至互联网
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. 配置接入层HSRP
9. 配置传输网络
10. 配置EIGRP（局域网端）
11. 配置局域网交换机
12. 配置回环永续性

当您配置DMVPN + DMVPN远程站点时，请使用这组程序。当您配置双路由器、双链路设计的第二台路由器时，可以使用这些程序。

下面的流程图详细介绍了如何配置远程站点DMVPN分支路由器

图20. 远程站点DMVPN分支路由器配置流程图




## 程序1　完成广域网路由器通用配置

在本设计中，有些特性和服务在所有广域网远程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)提供了设备身份验证和数据加密功能。

通过使用SSH和HTTPS协议，您可以实现对局域网设备的安全管理。这两个协议均进行了加密，可提供信息保密性，而不安全协议Telnet和HTTP则被关闭。

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
  transport input ssh
```

启用简单网络管理协议(SNMP)后，能够通过网络管理系统（NMS）对网络基础设施设备进行管理。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3：配置安全用户身份验证。

启用身份验证、授权与记账（AAA）来支持访问控制。所有针对网络基础设施设备的管理访问（SSH和HTTPS）均受到AAA的控制。

**读者提示**

本架构中使用的AAA服务器是思科身份验证控制系统。如需了解有关配置ACS的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络网络设备身份验证与授权部署指南》。

TACACS+是在基础设施设备上向AAA服务器验证管理登录所采用的主要协议。此外，系统还在每个网络基础设施设备上定义了一个本地AAA用户数据库，用于在中央TACACS+服务器不可用时，提供备用身份认证源。

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

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
```

步骤5：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。从分布层交换机向网络其余部分汇总的IP地址块中分配回环地址。

```
interface Loopback0
  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。

将SNMP和SSH进程绑定到回环接口地址，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6**：配置IP组播路由。

IP组播允许基础设施（即路由器和交换机）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电话等待音乐(MOH)和IP视频广播流是两个IP组播应用的范例。

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——基于稀疏模式组播操作，思科使用autorp提供了一种简单但可扩展的方法，来构建具备高永续性的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
```

您必须启用网络中的所有三层接口，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，您还必须配置相关的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，以便可以任意选择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
```

### 读者提示

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 连接至互联网

采用DMVPN的远程站点可以使用静态或者动态分配的IP地址。我们使用DHCP分配的外部地址测试了设计，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。这种设计提供了出色的安全性。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-PUBLIC
 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21.** 所需的DMVPN协议

| 名称 | 协议 | 用途 |
|---|---|---|
| non500-isakmp | UDP 4500 | 基于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
```

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22.** 可选协议—DMVPN分支路由器

| 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, 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PSK（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）
- 使用PSK进行身份验证
- Diffie-Hellman组：2

启用DPD，每30秒间隔发送一次持活时距，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-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）身份验证算法的ESP

由于DMVPN中枢路由器在NAT设备后端，您必须针对传输模式配置IPsec转换。

```
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5　配置mGRE隧道

**步骤1**：配置基本接口设置

您可以在配置隧道接口的过程中创建它们。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。

IP MTU应配置为1400，ip tcp adjust-mss应配置为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。源接口应与您用于连接互联网的接口相同。您应将tunnel vrf命令设置成之前为FVRF定义的VRF。

要在这一接口上启用加密，您必须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-PUBLIC
 tunnel protection ipsec profile DMVPN-PROFILE
```

**步骤3**：配置NHRP。

DMVPN中枢路由器为面向所有分支的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。

关于NHS值，请使用DMVPN中枢路由器的mGRE隧道地址。映射条目必须设定为在Cisco ASA 5500上配置的DMVPN中枢的外部NAT值。本设计方案使用了下表中所示的值。

**表23.** DMVPN隧道参数

| DMVPN云 | 隧道IP地址 | 隧道编号 | NHRP网络ID |
|---|---|---|---|
| 主用 | 10.4.34.1/23 | 10 | 101 |
| 备用 | 10.4.36.1/23 | 11 | 102 |

NHRP要求DMVPN云内的所有设备均使用相同的网络ID和身份验证密钥。您应将NHRP缓存保持时间设置为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选项允许您改写现有的缓存条目。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 10.4.36.1 172.17.130.1
 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。

您将在下面的程序中配置EIGRP，但首先您需要针对mGRE隧道接口配置一些具体的要求。

将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个远程站点。

```
interface Tunnel10
 ip hello-interval eigrp 201 20
 ip hold-time eigrp 201 60
```

您必须通告远程站点局域网。远程站点的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。如果汇总内的任意网络出现在路由表中，汇总将被通告给DMVPN中枢，从而提供了一种永续性衡量机制。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

在DMVPN分支路由器上运行一个额外的EIGRP-201进程来支持第二个DMVPN云。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存根路由，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
 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。

思科建议您使用稀疏模式来支持IP组播接口工作模式，并在所有三层接口上启用该模式，包括DMVPN隧道接口。

不要在互联网接口上启用PIM，因为这一接口不得用于请求组播流量。

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

**步骤2**：为DMVPN隧道启用PIM 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NBMA问题，您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。

```
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。您可以通过将分支路由器的DR优先级设置为0来避免这种情况。

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

## 程序8 配置接入层HSRP

您需要配置HSRP来支持使用VIP作为缺省网关，在两台路由器之间共享。HSRP活动路由器是与主要运营商相连的路由器，HSRP备用路由器是连接到辅助运营商或备用链路的路由器。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24. 广域网远程站点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 |

双路由器接入层设计需要进行一些修改，以支持弹性组播。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程序。

```
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 1 ip [LAN network 1 gateway address]
 standby 1 priority 105
 standby 1 preempt
```

**示例**

```
interface GigabitEthernet0/2
 no ip address
 no shutdown
!
interface GigabitEthernet0/2.64
 description Data
 encapsulation dot1Q 64
 ip address 10.5.12.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.12.1
 standby 1 priority 105
 standby 1 preempt
!
interface GigabitEthernet0/2.65
 description WirelessData
 encapsulation dot1Q 65
 ip address 10.5.10.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 110
 ip pim sparse-mode
 standby 1 ip 10.5.10.1
 standby 1 priority 105
```

```
 standby 1 preempt
!
interface GigabitEthernet0/2.69
 description Voice
 encapsulation dot1Q 69
 ip address 10.5.13.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby 1 ip 10.5.13.1
 standby 1 priority 105
 standby 1 preempt
!
interface GigabitEthernet0/2.70
 description WirelessVoice
 encapsulation dot1Q 70
 ip address 10.5.11.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby 1 ip 10.5.11.1
 standby 1 priority 105
 standby 1 preempt
```

## 程序9 配置传输网络

两台路由器之间需要配置传输网络。该网络用于支持路由器间通信，并避免“发夹”问题。传输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 GigabitEthernet0/2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.48.2 255.255.255.252
 ip pim sparse-mode
```

## 程序10 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程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。除了传输网络子接口外，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接口的广域网接口。

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface GigabitEthernet0/2.99
 eigrp router-id [IP address of Loopback0]
 no auto-summary
```

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

这一步骤仅应在DMVPN分支路由器上完成。

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。

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

## 程序11 配置局域网交换机

**步骤1**：在局域网交换机上配置中继。

使用802.1Q中继来连接此上游设备，允许该设备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监听和ARP检测被设置为可信。

```
vlan 99
!
default interface GigabitEthernet [number]
!
interface GigabitEthernet [number]
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 64,65,69,70,99
  switchport mode trunk
  macro apply EgressQoS
  ip arp inspection trust
  ip dhcp snooping trust
  logging event link-status
  no shutdown
```

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

## 程序12 配置回环永续性

### 仅适用于双路由器设计

远程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。

#### 选项1.广域网协议是EIGRP

**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
```

**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 [as]
redistribute eigrp 100 route-map LOOPBACK-ONLY
eigrp stub connected summary redistributed
```

#### 选项2. 广域网协议是BGP

**步骤1**：配置BGP来通告邻接路由器的回环网络

```
router bgp 65511
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
```

# 部署WAN远程站点分布层

使用这组程序来为DMVPN远程站点（单路由器、单链路）配置DMVPN分支路由器，并且已经包含了连接至分布层所必需的全部程序。

此外，这组程序也可用于配置DMVPN + DMVPN远程站点。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。

## 流程

远程站点DMVPN分支路由器分布层

1. 将路由器连接至分布层
2. 配置EIGRP（局域网端）
3. 配置传输网络

## 程序1 将路由器连接至分布层

二层端口通道接口连接到广域网分布交换机。

这种连接允许必要时在EtherChannel上包括多个VLAN。

以下配置用于在路由器和交换机之间创建一个EtherChannel链路，并设定两个通道组成员。

**步骤1**：配置端口通道接口。

创建端口通道接口。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。

```
interface Port-channel [number]
 no ip address
```

**步骤2**：配置端口通道子接口并分配IP地址。

在您启用物理接口后，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-channel [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [IP address] [netmask]
```

**步骤3**：以管理员身份启用端口通道组成员并指定相应的通道组。

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，因此您应以静态方式配置EtherChannel。

```
interface [interface type] [number]
 no ip address
 channel-group [number]
 no shutdown
```

示例

```
interface Port-channel1
 no ip address
interface Port-channel1.50
 encapsulation dot1Q 50
 ip address 10.5.0.1 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 no ip address
 channel-group 1
 no shutdown
!
interface GigabitEthernet0/2
 no ip address
 channel-group 1
 no shutdown
```

## 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 [as number]
 network [network] [inverse mask]
 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
 redistribute eigrp 200
 passive-interface default
 no passive-interface Port-channel2.54
 eigrp router-id 10.5.0.254
 no auto-summary
```

## 程序3　配置传输网络

### 仅适用于双路由器设计

在两台路由器之间配置传输网络。您可以使用这一网络来支持路由器间通信，并避免“发夹”问题。传输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。

传输网络必须是非被动EIGRP接口。

这一网络未连接终端站，因此不需要HSRP和DHCP。

```
interface Port-channel1.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.0.9 255.255.255.252
 ip pim sparse-mode

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

## 流程

远程站点第二台路由器分布层

1. 将分支路由器连接至分布层
2. 配置EIGRP（局域网端）
3. 配置传输网络
4. 配置回环永续性

使用这组程序配置DMVPN + DMVPN远程站点。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。

## 程序1　将分支路由器连接至分布层

二层端口通道接口连接到广域网分布交换机。这种连接允许必要时在EtherChannel上包括多个VLAN。

以下配置用于在路由器和交换机之间创建一个EtherChannel链路，并设定两个通道组成员。

**步骤1**：配置端口通道接口。

创建端口通道接口。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。

```
interface Port-channel [number]
 no ip address
```

**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上的VLAN。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-channel [number].[sub-interface number]
 encapsulation dot1Q [dot1q VLAN tag]
 ip address [IP address] [netmask]
```

**步骤3**：启用端口通道组成员并指定相应的通道组。

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

```
interface [interface type] [number]
 no ip address
 channel-group [number]
 no shutdown
```

**示例**

```
interface Port-channel2
 no ip address

interface Port-channel2.54
 encapsulation dot1Q 54
 ip address 10.5.0.5 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 no ip address
 channel-group 2
 no shutdown
!
interface GigabitEthernet0/2
 no ip address
 channel-group 2
 no shutdown
```

## 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 [as number]
 network [network] [inverse mask]
 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
 redistribute eigrp 201
 passive-interface default
 no passive-interface Port-channel2.54
 eigrp router-id 10.5.0.253
 no auto-summary
```

## 程序3 配置传输网络

### 仅适用于双路由器设计

在两台路由器之间配置传输网络。您可以使用这一网络来支持路由器间通信，并避免“发夹”问题。传输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。

传输网络必须是非被动EIGRP接口。

这一网络未连接终端站，因此不需要HSRP和DHCP。

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

### 示例

```
interface Port-channel2.99
 description Transit Net
 encapsulation dot1Q 99
 ip address 10.5.0.10 255.255.255.252
 ip pim sparse-mode
router eigrp 100
 no passive-interface Port-channel2.99
```

## 程序4　配置回环永续性

### 仅适用于双路由器设计

远程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。

#### 选项1. 广域网协议是EIGRP

**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
```

**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 [as]
redistribute eigrp 100 route-map LOOPBACK-ONLY
eigrp stub connected summary redistributed
```

#### 选项2. 广域网协议是BGP

**步骤1**：配置BGP来通告邻接路由器的回环网络。

```
router bgp 65511
 network 10.5.12.0 mask 255.255.255.0
 network 10.5.13.0 mask 255.255.255.0
```

## 流程

远程站点WAN分布层交换机配置

1. 完成交换机通用配置
2. 连接至WAN路由器
3. 配置EIGRP
4. 配置传输网络VLAN

## 程序1　完成交换机通用配置

本指南假定已经配置了分布层交换机，因此仅包含了完成交换机与广域网边缘路由器连接所需的程序。如需了解有关分布层交换机配置的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》。

## 程序2　连接至WAN路由器

端口通道接口连接至单WAN路由器或双WAN路由器，这些连接是二层端口通道。以下配置用于在交换机和路由器之间创建一个EtherChannel链路，并设定两个通道组（channel-group）成员。必要时，请对其他的WAN路由器重复该程序。

**步骤1**：为交换机上的路由器链路创建VLAN，创建VLAN接口并分配IP地址。

为路由器链路创建点对点VLAN。

```
vlan [VLAN number]
```

为点对点链路创建VLAN接口并分配IP地址。

```
interface Vlan [VLAN number]
 ip address [IP address] [netmask]
 no shutdown
```

**步骤2**：配置端口通道接口，并针对802.1q VLAN中继进行配置。

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。

```
interface Port-channel [number]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [VLAN number]
 switchport mode trunk
```

**步骤3**：以管理员身份启用端口通道组成员并指定相应的通道组。针对802.1 VLAN中继进行配置。

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，因此您应以静态方式配置EtherChannel。

```
interface [interface type] [number]
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan [VLAN number]
 switchport mode trunk
 channel-group [number] mode on
 no shutdown
```

**示例**

```
vlan 50
!
interface Port-channel1
 description DMVPN spoke router
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 description DMVPN spoke router port 1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet2/0/1
 description DMVPN spoke router port 2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
 channel-group 1 mode on
 no shutdown
!
interface Vlan50
 ip address 10.5.0.2 255.255.255.252
 no shutdown
```

## 程序3 配置EIGRP

为网络将使用的IP地址空间启用EIGRP。如果您的网络需要，可以输入多个网络声明。禁用IP网络的自动汇总功能，并将所有路由链路缺省设置为被动属性。EIGRP路由器ID使用Loopback 0 IP地址，以确保最高永续性。

单一逻辑分布层设计使用状态切换和不间断转发功能，以便在管理引擎数据或控制平面发生故障时实现亚秒级故障切换。这一功能减少了在切换到冗余逻辑设备时的丢包现象，并能够在数据平面与邻近节点无通信时保持数据包流向。在基于堆叠的分布层方法中，仍存在单个逻辑控制点，堆叠中的主控制平面可以在发生故障时切换到堆叠中的其他成员，从而带来秒级或亚秒级永续性。当分布平台的管理引擎或主交换机从活动管理引擎切换到热备用管理引擎时，将继续在硬件中交换IP数据流。然而，管理引擎需要时间在控制平面和EIGRP路由邻接设备之间重建双向对等关系，避免对等路由器由于丢失通信而破坏邻接关系，后者可能会导致流量重路由和中断。为了给管理引擎提供恢复时间，路由协议使用了不间断转发（NSF）设置，以等待两台管理引擎对等交换机进行恢复。邻接路由器如果具备能够识别NSF对等体的IOS版本，我们就可以说它能够感知NSF。这一设计中使用的所有平台均具备NSF感知能力，能够支持正在使用的路由协议。

您必须配置分布层交换机，为正在使用的协议启用NSF功能，以便当它需要切换到对等邻接设备的热备用管理引擎时能够告知对等体，从而有时间重建到该节点的EIGRP协议。在这一网络中无需对缺省的NSF计时器进行调节。具备NSF感知能力的对等路由器无需进行配置。

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

**示例**

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Vlan50
 eigrp router-id 10.5.0.252
 no auto-summary
 nsf
```

## 程序4 配置传输网络VLAN

### 仅适用于双路由器设计

您需要在两台路由器之间配置传输网络，而路由器之间不需要物理链路。可以使用传输VLAN进行代替。分布层在两个现有的二层EtherChannel上扩展了VLAN。分布层不参与传输网络上的任何路由，因此传输VLAN无需VLAN接口。

**步骤1**：在交换机上创建传输VLAN。

创建传输VLAN。

```
vlan [VLAN number]
```

**步骤2**：将传输VLAN添加到现有端口通道中继接口和通道组成员。

```
interface Port-channel [number]
 switchport trunk allowed vlan add [VLAN number]
!
interface [interface type] [number]
 switchport trunk allowed vlan add [VLAN number]
```

示例

```
vlan 99
!
interface Port-channel1
 switchport trunk allowed vlan add 99
 !
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan add 99
 !
interface GigabitEthernet2/0/1
 switchport trunk allowed vlan add 99
```

备注

# 部署WAN服务质量

## 流程

QoS配置

1. 创建QoS映射表对流量进行分类
2. 将ISAKMP流量添加到网络关键（Network-Critical）服务类别
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WAN QoS策略应用于物理接口

配置WAN-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映射表对流量进行分类

这一程序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。您可以使用以下两种形式的match命令：match dscp和match protocol。

使用下列步骤来配置所需的WAN类别映射表（class-map）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WAN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25. 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（如Telnet、Citrix和Oracle瘦客户端） | af31, cs3 | 15 | 基于DSCP |
| DATA（数据） | 数据 | af21 | 19 | 基于DSCP |
| SCAVENGER（清道夫） | 清道夫 | af11, cs1 | 5 | - |
| NETWORK-CRITICAL（网络关键） | 路由协议以及运营、管理和维护（OAM）流量 | cs6, cs2 | 3 | - |
| Default（默认） | 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中所示的缺省类别内了。

## 程序2 将ISAKMP流量添加到网络关键（Network-Critical）服务类别

对于使用DMVPN的WAN连接，您需要确保ISAKMP流量在WAN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。

该程序仅对WAN-汇聚DMVPN中枢路由器或WAN远程站点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

这一程序适用于所有广域网路由器。

WAN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”（best effort）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26中的每个类别重复步骤2-6，包括缺省类别。

**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**

虽然这些带宽分配符合基本要求，但考虑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。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。

这一程序适用于所有广域网路由器。您可以多次重复这一程序，以支持具有多个连接到不同接口的WAN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WAN QoS策略应用于物理接口

要在物理接口上调用整形和排队，您必须应用在之前的程序中配置的父策略。

这一程序适用于所有广域网路由器。您可以多次重复这一程序，以支持具有多个连接到不同接口的WAN连接的设备。

**步骤1**：选择WAN接口。

```
interface [interface type] [number]
```

**步骤2**：应用WAN 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
```

# 借助WAAS部署应用优化

## 业务概述

随着远程工作地点不断增加，网络管理员需要工具来帮助他们确保在远程地点提供可靠的应用性能。最近的趋势是企业远程站点数量不断增加，而且多数新雇佣的员工都位于远程站点。这些趋势与全球扩张、员工吸引和挽留、并购、成本节省以及环境问题等因素密切相关。

与此同时，远程站点通信要求也在不断发展，需要采用协作应用、视频和Web 2.0技术。这些发展也对远程站点和WAN提出了更高的性能要求。

企业进行数据中心整合的趋势也在继续。整合将把多数远程站点资产转移到数据中心内，很大程度上是为了符合监管要求，实现集中化的安全性和对企业数据资产更强有力的控制。

在整合数据中心的同时增加远程站点人数意味着，越来越多的远程站点员工要通过相对较慢的WAN来访问基于LAN的业务应用。随着这些应用日益以多媒体为中心、对延迟的敏感性越来越高，IT和网络人员面临着越来越大的压力，来保持远程应用的响应时间与位于公司数据中心应用服务器本地的用户处于同等水平。这些本地用户享有数Mb的局域网速度，不会像处在广域网连接另一端的同事一样，受到距离导致的延迟的影响。

应用优化可以提升网络性能，同时增强安全性和改善应用交付。Cisco WAN优化是一个架构解决方案，包含一系列工具和技术，它们相互配合，以一种战略性的系统方式，提供一流的WAN优化性能，同时最大限度降低总体拥有成本。

## 技术概述

### WAN汇聚

WAN汇聚站点使用了由两台或多台WAE设备组成的集群，来提供WAAS功能。WAE设备连接至分布层交换机。连接都使用EtherChannel，以提升吞吐率和弹性。WAE连接至在分布交换上配置的WAN服务网络。

WAN 500设计使用了一个WAE-7371设备集群。需要的设备总数量最低为2个（用于实现N+1冗余）。同样，WAN 100设计使用了一个WAE-7341设备集群，需要的设备总数量最少为2个（用于实现N+1冗余）。关于WAE规模确定（sizing）的其他细节在下表中提供。扇出数量与远端对等WAE设备的总数量相对应。

表26. WAN-汇聚WAE选项

| 设备 | 最大优化TCP连接 | 最大推荐WAN链路 [Mbps] | 最大优化吞吐率[Mbps] | 最大核心扇出[对等体] |
|---|---|---|---|---|
| WAVE-574-3GB | 750 | 8 | 100 | 35 |
| WAVE-574-6GB | 1300 | 20 | 150 | 70 |
| WAVE-594-8GB | 750 | 50 | 250 | 50 |
| WAVE-594-12GB | 1300 | 100 | 300 | 100 |
| WAE-674-4GB | 2000 | 45 | 250 | 100 |
| WAE-674-8GB | 6000 | 90 | 350 | 200 |
| WAE-674-8GB-VB | 4000 | 90 | 350 | 200 |
| WAE-694-16GB | 2500 | 200 | 450 | 150 |
| WAE-694-24GB | 6000 | 200 | 500 | 300 |
| WAE-7341 | 12000 | 310 | 1000 | 1400 |
| WAE-7371 | 50000 | 1000 | 2500 | 2800 |
| WAVE-7541 | 18000 | 500 | 1000 | 700 |
| WAVE-7571 | 60000 | 1000 | 2000 | 1400 |
| WAVE-8541 | 150000 | 2000 | 4000 | 2800 |

我们为cisco.com网站的注册用户提供了一个更全面的、互动的WAAS规模确定工具：
http://tools.cisco.com/WAAS/sizing

WCCP是由思科开发的协议。其目的在于透明地截获和重定向从网络设备到WCCP设备的流量，如运行WAAS的WAE（在下面探讨）。

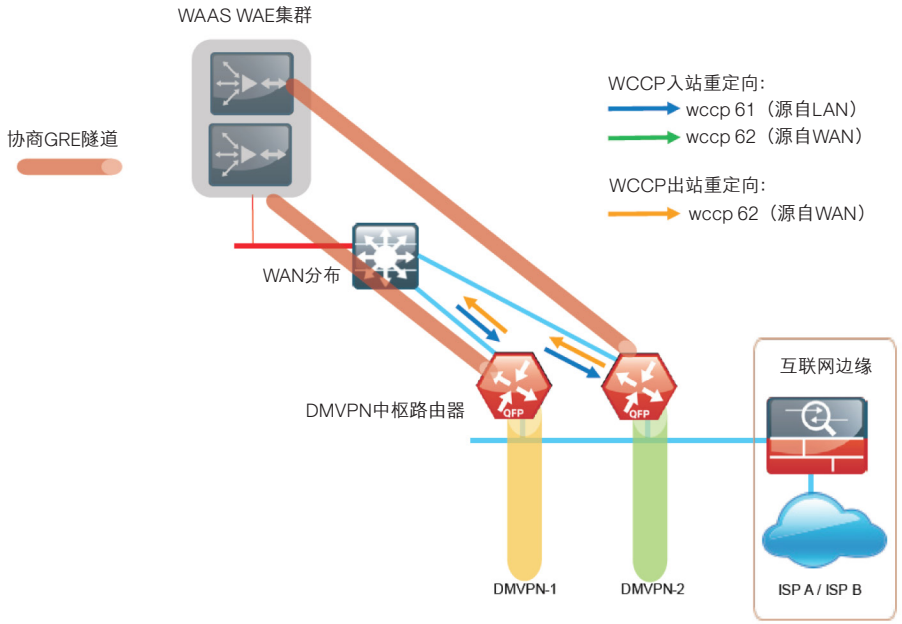
WCCP在DMVPN路由器上启用。WCCP重定向使用服务组61和62来匹配用于重定向的流量。这些服务组必须成对使用：

- 服务组61使用源地址来重定向流量
- 服务组62使用目标地址来重定向流量

这一设计在面向LAN的接口上入站使用了WCCP 61来匹配源自数据中心的未经优化的数据，而数据中心是位于WAN远程站点的客户机目的地。在面向LAN的接口上出站使用了WCCP 62，匹配源自WAN远程站点的优化数据。

从交换机至DMVPN路由器的连接均为路由的点对点链路。这一设计强制使用了从WAE到路由器的协商返回（negotiated-return）GRE隧道。当设计方案使用了GRE协商返回（negotiated return）时，就不需要扩展WAN服务VLAN来将DMVPN路由器包括在内。

图21. WAN汇聚—WAAS拓扑




## 远程站点

远程站点的WAN优化设计根据站点的具体特点会有所不同。单路由器站点使用一个（非冗余）WAE。同样，所有双路由器站点使用双WAE。WAE规模和形式（form factor）的具体情况主要取决于最终用户的数量和WAN链路的带宽。低带宽（< 2 Mbps）单路由器、单链路站点也可以使用路由器内嵌的WAASx功能。

在选择广域网远程站点WAE优化平台时，有多种因素需要考虑。主要考虑因素是WAN链路的带宽。在满足带宽要求之后，需要考虑的下一因素就是并发的、优化的TCP连接的最大数量。关于WAE规模确定（sizing）的其他细节在下表中提供。优化的吞吐率数据与在WAAS成功优化后可用的带宽相对应。

表27. WAN远程站点WAE选项

| 设备 | 最大优化TCP连接 | 最大推荐WAN链路 [Mbps] | 最大优化吞吐率[Mbps] |
|---|---|---|---|
| Cisco1941/WAASx[1] | 150 | 4 | 8 |
| SRE-700-S | 200 | 20 | 200 |
| SRE-700-M | 500 | 20 | 200 |
| SRE-900-S | 200 | 50 | 300 |
| SRE-900-M | 500 | 50 | 300 |
| SRE-900-L | 1000 | 50 | 300 |
| WAVE-274 | 200 | 2 | 90 |
| WAVE-294-4GB | 200 | 10 | 100 |
| WAVE-294-8GB | 500 | 20 | 150 |
| WAVE-474 | 400 | 4 | 90 |
| WAVE-574-3GB | 750 | 8 | 100 |
| WAVE-574-6GB | 1300 | 20 | 150 |
| WAVE-594-8GB | 750 | 50 | 250 |
| WAVE-594-12GB | 1300 | 100 | 300 |
| WAE-674-4GB | 2000 | 45 | 250 |
| WAE-674-8GB | 6000 | 90 | 350 |
| WAE-674-8GB-VB | 4000 | 90 | 350 |
| WAE-694-16GB | 2500 | 200 | 450 |
| WAE-694-24GB | 6000 | 200 | 500 |
| WAE-7341 | 12000 | 310 | 1000 |
| WAE-7371 | 50000 | 1000 | 2500 |
| WAVE-7541 | 18000 | 500 | 1000 |
| WAVE-7571 | 60000 | 1000 | 2000 |
| WAVE-8541 | 150000 | 2000 | 4000 |

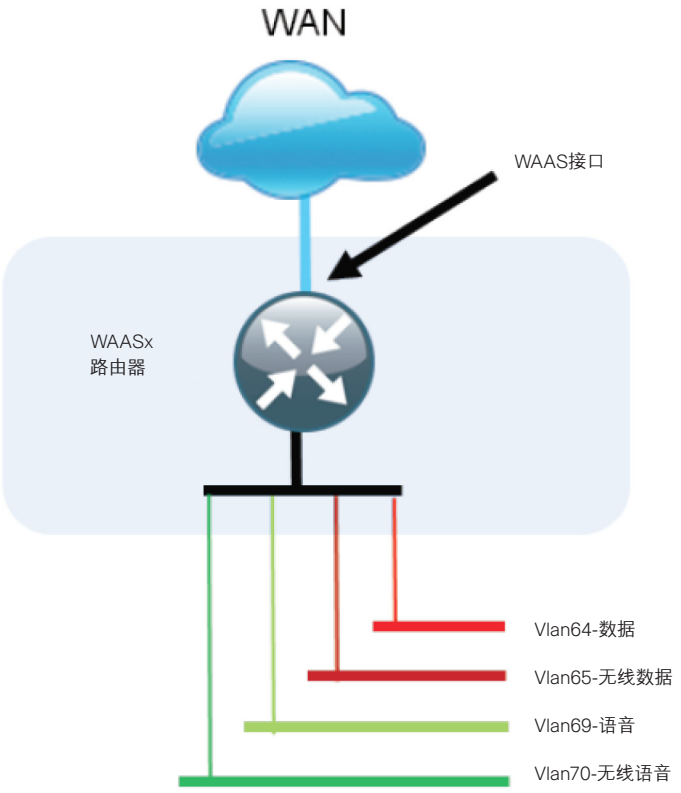
注:

1. 仅限单链路设计

我们为cisco.com网站的注册用户提供了一个更全面的、互动式WAAS规模确定工具:
http://tools.cisco.com/WAAS/sizing

内嵌的路由器WAASx提供了WAE平台WAAS完整功能集的一个子集。当前的WAASx软件版本经济高效、易于部署，可兼容单链路WAN设计。无需更改设计或架构，即可在路由器上启用这项功能。

图22. WAN远程站点——WAASx拓扑



之前讨论的WAE形式（form factor）包括一个路由器服务就绪引擎（SRE），以及一个外部设备。这些不同的组件均运行同样的WAAS软件，在功能上相当。主要的区别在于将这些设备连接到LAN的方法。

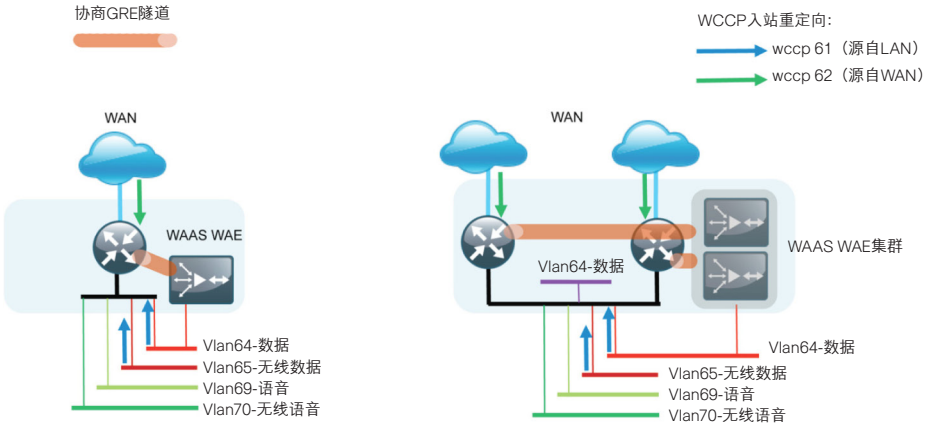
· SRE：一个内部接口（仅连接路由器），一个外部接口
· 设备：两个接口（均为外部）

无论所选的硬件形式如何，将WAE设备连接到LAN的方式都是一致的。所有的WAE连接均利用外部接口实现。这种方法的优势是没有必要去创建一个专门的网络，来专门连接WAE设备，而SRE和外部设备可以使用同样的设计。除了用于设备配置的初始引导（initial bootstrapping）之外， SRE的内部接口不用于这种设计。

对于这种解决方案，您必须从每个SRE模块连接一根外部以太网线缆。

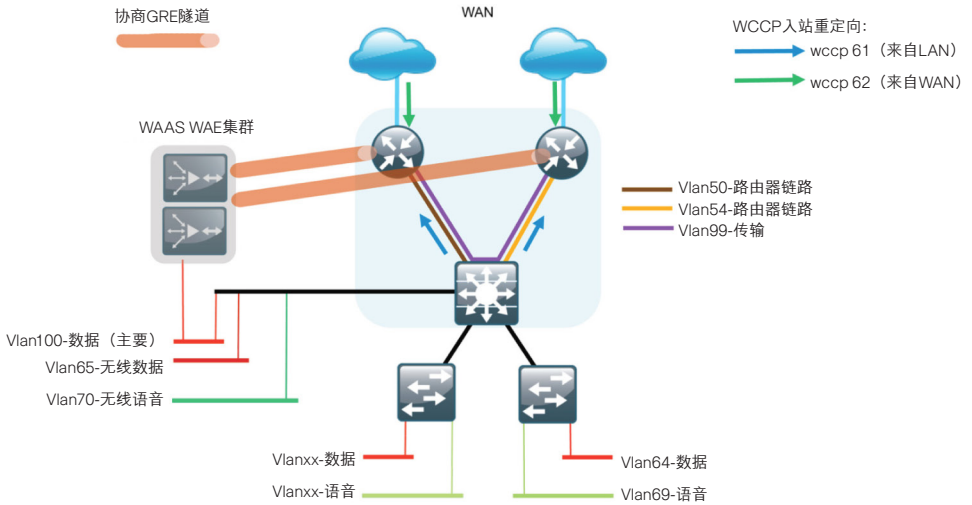
在所有扁平型二层设计中，您应将WAE设备连接至接入层交换机的数据VLAN。

**图23.** WAN远程站点—WAAS拓扑（接入层连接）




当部署采用分布层设计时，WAE设备应连接到分布层交换机上的主要数据VLAN。

**图24.** WAN远程站点—WAAS拓扑（分布层连接）




请尽可能通过这两个接口利用EtherChannel连接WAE设备，以实现高水平的性能和永续性。

在WAN路由器上启用WCCP版本2，以将流量重定向至WAAS设备。

WCCP重定向使用服务组61和62来匹配用于重定向的流量。这些服务组必须成对使用：

· 服务组61使用源地址来重定向流量
· 服务组62使用目标地址来重定向流量

此设计在面向LAN的VLAN子接口上入站使用了WCCP 61来匹配源自客户机、去往数据中心（或其他远程站点）的未经优化的数据。在所有情况下，WCCP 62在面向WAN的接口上入站使用，来匹配源自数据中心（或其他远程站点）的经优化的数据。

由于WAE连接到数据VLAN，本设计要求使用从WAE到路由器的协商返回（negotiated-return）GRE隧道。当使用GRE协商返回（negotiated return）时，您无需专门在路由器上创建一个新网络来连接WAE。

以下步骤概述了配置一个基本的WAAS环境所需的操作。

## 流程

WAAS/WAE配置

1. 安装vWAAS虚拟机
2. 配置WAAS中央管理器
3. 配置用于WAE设备的交换机
4. 配置WAE设备
5. 配置WAE SRE设备
6. 为WAE设备配置远程交换机
7. 在路由器上配置WCCPv2
8. 为WAASx配置中央管理器
9. 配置WAAS Express路由器

## 程序1 安装vWAAS虚拟机

此程序为可选程序，仅在您采用虚拟WAAS (vWAAS)时需要。

vWAAS以开放虚拟设备(OVA)的形式提供。OVA预装有磁盘、内存、CPU、NIC和其它与虚拟机相关的配置参数。这是行业标准，许多虚拟设备都以这种形式提供。每种vWAAS型号采用不同的OVA文件。

**技术提示**

目前OVA文件仅以DVD媒体格式提供，www.cisco.com上不提供下载。

**步骤1**：借助VMWare vSphere客户端部署OVF模板。

在配置vWAAS前，您必须首先采用vSphere在VMware ESX/ESXi服务器上安装vWAAS OVA。

**步骤2**：采用VMware控制台配置设备。

配置vWAAS中央管理器和vWAAS应用加速器设备的程序和步骤，与用于配置WAE设备和SRE设备的步骤和程序相同。选择下列适当的程序，完成vWAAS配置。

## 程序2 配置WAAS中央管理器

使用Cisco WAVE-574设备在主要位置提供中央管理器功能，为WAAS网络提供图形化管理、配置和报告功能。此设备位于服务器群中，这是因为它不直接处在WAN优化的转发路径中，但却提供管理和监控服务。中央管理器的初始配置需要终端设备访问控制台端口，以获得基本配置选项和IP地址分配。对于所有WAE设备，工厂缺省用户名是admin，工厂缺省密码是default。

您可以通过输入setup命令，从命令行启动初始设置工具。

**步骤1**：运行setup。

```
    Parameter                 Default Value
 1. Device Mode               Application Accelerator
 2. Interception Method       WCCP
 3. Time Zone                 UTC 0 0
 4. Management Interface      GigabitEthernet 1/0
 5.     Autosense                Enabled
 6.     DHCP                     Enabled
ESC Quit ? Help ———————————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

步骤2：配置为中央管理器。

```
1. Application Accelerator
2. Central Manager
Select device mode [1]: 2
```

步骤3：配置时区。

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

步骤4：配置管理接口、IP地址和缺省网关。

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 1/0           dhcp
  2. GigabitEthernet 2/0           dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.48.100/24
Enter Default Gateway IP Address [Not configured]: 10.4.48.1
```

步骤5：配置DNS、主机和NTP设置。

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAAS-WCM-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

步骤6：选择适当的许可。

```
The product supports the following licenses:
1. Enterprise
Enter the license(s) you purchased [1]: 1
```

步骤7：验证配置设置和开始重新加载。

```
    Parameter                 Configured Value
 1. Device Mode               Central Manager
 2. Time Zone                 PST -8 0
 3. Management Interface      GigabitEthernet 1/0
 4.     Autosense                Enabled
 5.     DHCP                     Disabled
 6.     IP Address               10.4.48.100
 7. IP Network Mask           255.255.255.0
 8. IP Default Gateway        10.4.48.1
 9. DNS IP Address            10.4.48.10
10. Domain Name(s)            cisco.local
11. Host Name                 WAAS-WCM-1
12. NTP Server Address        10.4.48.17
13. License                   Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
————————————

Press 'y' to select configuration, 'd' to toggle defaults
display, <1-13> to change specific parameter [y]: y
Apply WAAS Configuration: Device Mode changed in SETUP; New
configuration takes effect after a reload. If applicable,
registration with CM, CM IP address, WAAS WCCP configuration
etc, are applied after the reboot. Initiate system reload?
<y/n> [n] y
Are you sure? <y/n> [n]: y
```

步骤8：重启之后，登录到WAAS中央管理器并启用SSH。

要启用SSH，您需要生成RSA密钥并启用sshd服务。

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

**步骤9**：禁用telnet。

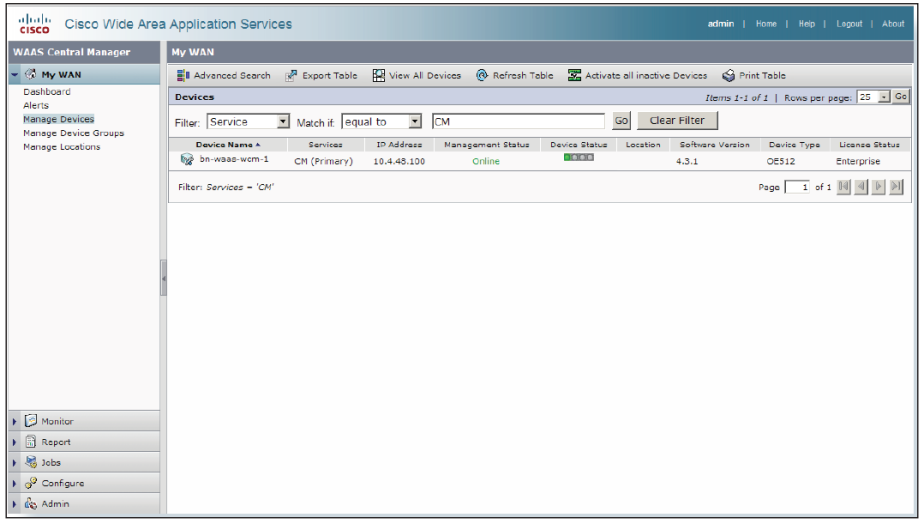
```
no telnet enable
```

**步骤10**：通过web接口访问WAAS中央管理器。

重新加载完成后，现在中央管理器设备应启动运行，并可以通过在Web浏览器中输入在设置工具步骤6中分配的IP地址来进行访问，或者如果它已在DNS中进行了配置，则输入相关主机名进行访问。指定安全HTTP和端口号8443来访问中央管理器，例如https://10.4.48.100:8443。使用缺省用户名admin和密码default进行登录。

**步骤11**：点击My WAN（我的广域网） -> Manage Devices（管理设备）。Central Manager（中央管理器）作为唯一的托管设备出现在My WAN（我的广域网）窗口中。

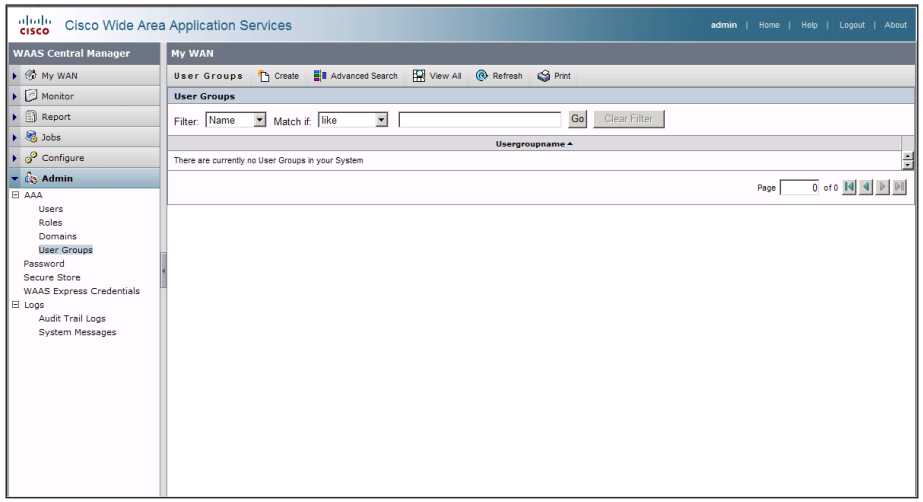
图25. WAAS中央管理器—初始托管设备列表



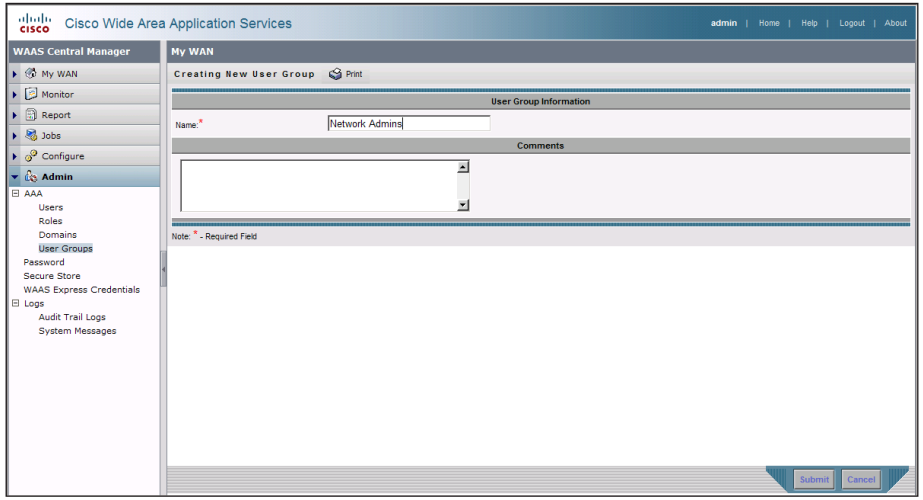

**步骤12**：配置Network-Admins（网络管理员）用户组

Central Manager（中央管理器）的web接口需要分配有适当角色的用户组，来授权源自外部AAA数据库的用户。在下面的步骤中启用AAA之前必须先完成这一设置，并且只能采用web接口来执行。

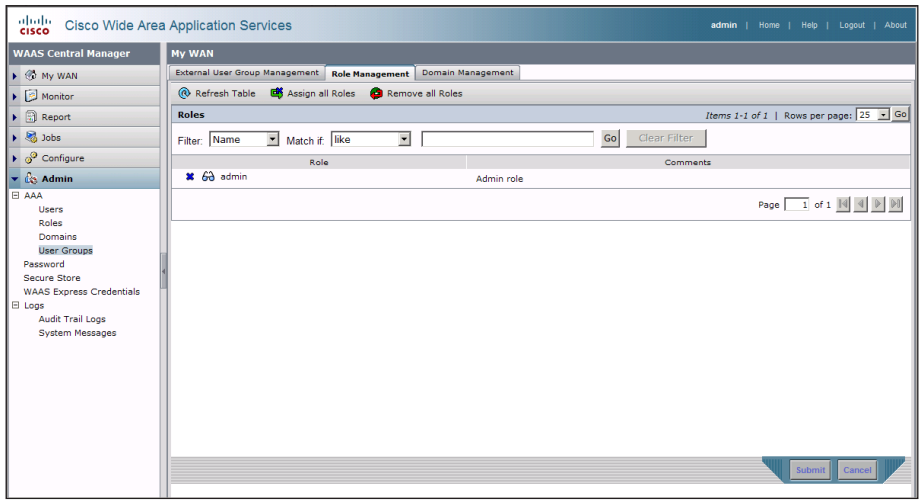
在Admin（管理员）> AAA > 中点击User Groups（用户组）。



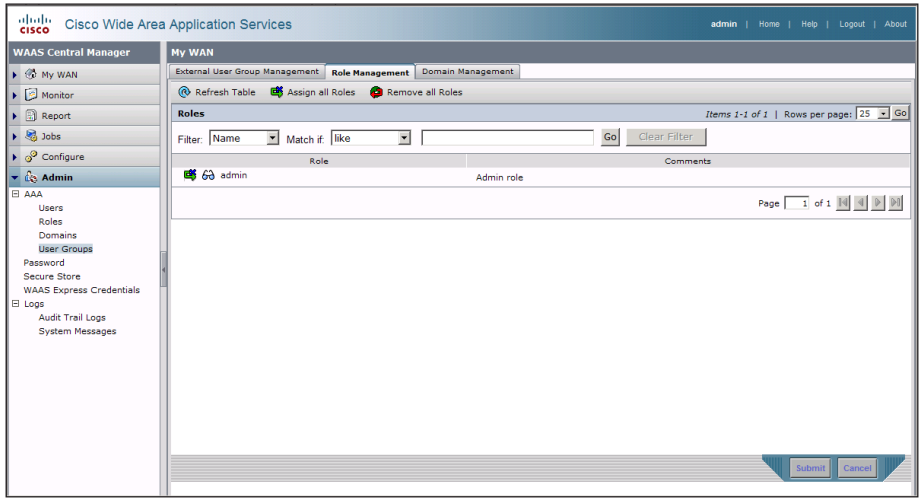

点击Create（创建），然后在Name（名称）字段中输入一个名称。这一名称必须与AAA服务器上所用的组名称完全匹配（区分大小写）。例如，此部署中采用的是”Network Admins”（网络管理员）。



在您创建了组之后，点击Role Management（角色管理）选项卡，然后点击X分配角色。




在您正确地分配角色后，该图标旁边会出现一个大的绿色复选标记。




**步骤13**：配置安全用户身份验证。

启用AAA身份验证来支持访问控制。AAA控制所有对于WAAS/WAE设备的管理访问(SSH和HTTPS)。

在设置期间已在WAAS/WAE上创建了本地管理员用户。这一用户帐户能够在中央TACACS+服务器不可用或是贵企业没有TACACS+服务器的情况下管理设备。

**技术提示**

此处所显示的AAA配置详情仅适用于WAAS设备。若要成功进行用户授权，还需要在AAA服务器上进行额外的配置。只有完成《面向大型企业的思科IBA智能业务平台——无边界网络网络设备身份验证与授权部署指南》中的相关步骤时，才能够继续配置安全用户身份验证。

以下设置可将TACACS+配置为用户身份验证（登录）和用户授权（配置）的主要方法。

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

**步骤14**：在您完成配置更改后，保存配置。

```
copy running-config startup-config
```

## 程序3 配置用于WAE设备的交换机

WAN分布交换机是实际连接位于WAN-汇聚站点的设备（如支持WAN优化的WAE设备）的相应位置。该类型设备需要一种具有弹性的连接，但不需要路由协议。这种连接可以使用二层EtherChannel链路。

本指南假定已经配置了分布层交换机，只有完成交换机与WAE设备连接所需的程序包括在内。有关分布层交换机配置的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》。

您必须为具有相似连接需求的这种及其他设备创建一个VLAN和SVI。该VLAN被称为WAN服务网络。

**步骤1**：创建VLAN和SVI。

```
vlan [VLAN number]
 name [VLAN name]
interface Vlan [VLAN number]
 ip address [IP address] [netmask]
 no shutdown
```

**步骤2**：为设备配置二层EtherChannel链路，并将它们与VLAN相关联。

```
interface Port-channel [number]
  switchport access vlan [VLAN number]
interface [type] [number]
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
!
```

**示例**

```
vlan 350
 name WAN_Service_Net-10.4.32.128

interface Port-channel7
 description bn-wae-1 EtherChannel
 switchport access vlan 350

interface GigabitEthernet1/0/2
 description bn-wae-1 port 1
 switchport access vlan 350
 channel-group 7 mode on
 no shutdown
!
interface GigabitEthernet2/0/2
 description bn-wae-1 port 2
 switchport access vlan 350
 channel-group 7 mode on
 no shutdown
!
interface Vlan350
 ip address 10.4.32.129 255.255.255.192
 no shutdown
```

## 程序4 配置WAE设备

一个Cisco WAE-7341设备集群部署在WAN汇聚站点，为通过广域网往返远程站点的WAAS流量提供头端端接。您须将这些设备直接连接到WAN分布层交换机，利用GRE-协商返回（negotiated return）来与WCCP路由器进行通信。

您也可以将WAE设备独立地或者作为WAE集群的一部分部署在WAN远程站点。您应采用这一程序来配置WAN远程站点WAE设备。您可以使用与您在WAAS中央管理器初始配置中所使用的相同设置工具来设置WAE设备。这些设备仅要求通过其控制台端口进行基本的设置来分配初始设定；在您完成此设置之后，您可以通过WAAS中央管理器控制台来执行WAAS网络的所有管理工作。

WAE应用加速器的初始配置需要终端设备访问控制台端口，以获得基本配置选项和IP地址分配。对于所有WAE设备，工厂缺省用户名是admin，工厂缺省密码是default。

应用加速器WAE的设置工具配置步骤类似于中央管理器的设置，但在第二步选择“application-accelerator”（应用加速器）作为设备模式后，步骤开始不同。选择此模式后，设置脚本就更改为允许您在现有中央管理器中注册WAE，并将流量截获方法定义为WCCP。

**步骤1**：运行setup。

您可以通过输入setup命令，从命令行启动初始设置工具。

```
    Parameter                Default Value
 1. Device Mode              Application Accelerator
 2. Interception Method      WCCP
 3. Time Zone                UTC 0 0
 4. Management Interface     GigabitEthernet 1/0
 5. Autosense                Enabled
 6.     DHCP                    Enabled
ESC Quit ? Help ———————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
6> to change specific default [y]: n
```

**步骤2**：配置为应用加速器。

```
1. Application Accelerator
2. Central Manager
Select device mode [1]: 1
```

**步骤3**：配置截获方法。

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

**步骤4**：配置时区。

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

**步骤5**：配置管理接口、IP地址和默认网关。

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 1/0           dhcp
  2. GigabitEthernet 2/0           dhcp
Select Management Interface [1]: 1
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X(optional mask bits)> [Not configured]:
10.4.32.161/26
Enter Default Gateway IP Address [Not configured]: 10.4.32.129
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.48.100
```

**步骤6**：配置DNS、主机和NTP设置。

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): WAE7341-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

**步骤7**：配置WCCP路由器列表。

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.4.32.243 10.4.32.244
```

**步骤8**：选择适当的许可。

```
The product supports the following licenses:
1. Transport
2. Enterprise
3. Enterprise & Video
4. Enterprise & Virtual-Blade
5. Enterprise, Video & Virtual-Blade
Enter the license(s) you purchased [2]: 2
```

步骤9：验证配置设置。

```
      Parameter                 Configured Value
   2. Interception Method       WCCP
   3. Time Zone                 PST -8 0
   4. Management Interface      GigabitEthernet 1/0
   5.     Autosense                Enabled
   6.     DHCP                     Disabled
   7.     IP Address               10.4.32.161
   8.     IP Network Mask          255.255.255.192
   9. IP Default Gateway        10.4.32.129
  10. CM IP Address             10.4.48.100
  11. DNS IP Address            10.4.48.10
  12. Domain Name(s)            cisco.local
  13. Host Name                 WAE7341-1
  14. NTP Server Address        10.4.48.17
  15. WCCP Router List          10.4.32.243 10.4.32.244
  10.4.32.243
  16. License                   Enterprise
  ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
  ————————

  Press 'y' to select configuration, <F2> to see all
  configuration, 'd' to toggle defaults display, <1-16> to
  change specific parameter [y]: y
  Applying WAAS configuration on WAE ...
  May take a few seconds to complete ...
```

如果到WAE的交换机连接被配置为端口通道，此程序将会失败，因为WAE设置脚本不支持端口通道。如果是这样，在WAAS中央管理器中的注册将在步骤11中手动完成。

步骤10：（可选）为WAE配置端口通道连接，连接到分布层交换机堆叠。

这是一个可选步骤，仅在利用端口通道连接WAE实现弹性连接时需要。

```
interface GigabitEthernet 1/0
 no ip address 10.4.32.161 255.255.255.192
 exit
!
primary-interface PortChannel 1
!
interface PortChannel 1
 ip address 10.4.32.161 255.255.255.192
 exit
!
interface GigabitEthernet 1/0
 channel-group 1
 exit
interface GigabitEthernet 2/0
 channel-group 1
 exit
```

步骤11：（可选）完成在WAAS中央管理器中的注册。

在配置了端口通道之后，WAE就可以到达WAAS中央管理器。运行cms enable命令来强制进行手动注册。

这是一个可选步骤，仅在步骤9的初始连接尝试注册失败时才需要。

```
cms enable
Registering WAAS Application Engine...
Sending  device registration request to Central Manager with
address 10.4.48.100
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-
config startup-config'.
Otherwise management service will not be started on reload and
node will be shown 'offline' in WAAS Central Manager UI.
management services enabled
```

有一些额外的非缺省设置在WAE设备上启用，来完成配置。这些设置在步骤12至14中进行配置。

**步骤12**：配置GRE协商返回（negotiated return）。

所有WAE设备对其各自的WCCP路由器使用GRE-协商返回（negotiated return）：

```
egress-method negotiated-return intercept-method wccp
```

**步骤13**：配置WCCP路由器列表。

设置脚本根据提供的信息生成一个路由器列表。要查看设备配置，请输入以下命令：

```
WAE7341-1# show running-config | include wccp router-list
wccp router-list 8 10.4.32.243 10.4.32.244 10.4.32.244
```

路由器列表8专门用于在缺省网关路由器上配置的WCCP。此设计使用了GRE-协商返回（negotiated return）和路由器回环（loopback）地址，因此我们需要创建一个新的路由器列表，并删除路由器列表8。

在此设计中所有WAE配置均使用路由器列表1。

```
no wccp router-list 8 10.4.32.243 10.4.32.244
wccp router-list 1 10.4.32.243 10.4.32.244
```

该设计在路由器和WAE之间使用了认证。

ASR1000系列路由器必须使用WCCP掩码分配模式，以便WCCP正常运行。

如有任何WCCP路由器是Cisco ASR1000系列路由器，那么请将hash-source-ip的默认设置更改为mask-assign。这种更改在WAE上进行，而不是在路由器上。

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 1
password c1sco123 mask-assign
```

所有其他路由器可使用缺省设置：

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 1
password c1sco123
```

**步骤14**：启用SSH。

要启用SSH，您必须生成RSA密钥并启用sshd服务：

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

**步骤15**：禁用telnet。

```
no telnet enable
```

**步骤16**：配置安全用户身份验证。

启用AAA身份验证来支持访问控制。AAA控制所有对于WAAS/WAE设备的管理访问(SSH和HTTPS)。

在设置期间已在WAAS/WAE上创建了本地管理员用户。这一用户帐户能够在中央TACACS+服务器不可用或是贵企业没有TACACS+服务器的情况下管理设备。

以下设置可将TACACS+配置为用户身份验证（登录）和用户授权（配置）的主要方法。

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

**步骤17**：保存配置。

在您通过控制台进行配置更改后，保存配置。

```
copy running-config startup-config
```

## 程序5 配置WAE SRE设备

对于本设计中的远程站点WAAS设备，您可以使用多种WAE设备或SRE型号，具体取决于性能要求。

您可以将SRE模块直接插入远程站点路由器中相应的模块插槽内，配置方式与WAE设备略有不同。如果您使用的是WAE设备，那么您可以采用远程站点编址参数，按照WAN-汇聚WAE设备系列程序进行操作。

虽然远程站点路由器可以利用路由器背板潜在地与SRE直接进行通信，但此设计使用了模块上的外部接口，以便无论选择了何种WAE设备，都可以实施一致的设计。SM接口必须启用，而且分配了任意的（仅在本地有意义）IP地址，以便通过控制台会话从主机路由器进行访问。

在接入或分布交换机上，您必须将外部接口连接到数据网络，由此这种配置才能正常工作。

**步骤1**：在主机路由器上配置控制台访问和SRE IP地址。

要允许控制台访问SRE模块，您必须在主机路由器上输入以下命令。

```
interface SM1/0
 ip address 1.1.1.1 255.255.255.252
 service-module external ip address 10.5.52.8 255.255.255.0
 service-module ip default-gateway 10.5.52.1
 no shutdown
```

**技术提示**

在此设计中，分配到SM/0的IP地址（1.1.1.1）可以任意设定，并且仅在主机路由器本地有意义。

**步骤2**：（可选）为SRE设备配置AAA豁免。

如果已在路由器上启用了AAA，系统将提示您进行路由器登录和WAAS登录；这将会使您感到困惑。禁用初始的路由器认证需要创建AAA方法，然后可利用该方法在与SRE相关的路由器上进行具体的线路配置。

创建AAA登录方法：

```
aaa authentication login MODULE none
```

确定将哪个线路编码分配给SRE。下面的输出示例展示的为线路67。

```
Br203-2921-1# show run | begin line con 0
line con 0
 logging synchronous
line aux 0
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
 flowcontrol software
line vty 0 4
 password 7 04585A150C2E1D1C5A
 transport input ssh
```

通过创建访问列表，限制对于SRE控制台的访问。访问列表编号可随意设定，但IP地址必须与分配给SM接口的地址相匹配。

```
access-list 67 permit 1.1.1.1
```

将创建好的方法分配给相应的线路：

```
line 67
 login authentication MODULE
 access-class 67 in
 transport output none
```

步骤3：利用来自主机路由器的会话连接至WAE控制台。

在分配了IP地址并启用接口之后，在WAE上打开会话并运行设置脚本成为可能。对于所有WAE设备，工厂缺省用户名是admin，工厂缺省密码是default。

如果您在路由器上使用的是安全用户身份验证，并且没有创建AAA豁免，那么您在登录WAE控制台会话之前，必须首先凭借有效的路由器登录凭证进行认证。

```
Br203-2921-1# service-module sm 1/0 session
```

步骤4：运行setup。

您可以通过输入setup命令，从命令行启动初始设置工具。

```
    Parameter                 Default Value
    Device Mode               Application Accelerator
 1. Interception Method       WCCP
 2. Time Zone                 UTC 0 0
 3. Management Interface      GigabitEthernet 1/0
(internal)
        Autosense                Disabled
        DHCP                     Disabled
ESC Quit ? Help ————————————— WAAS Default Configuration
————————————

Press 'y' to select above defaults, 'n' to configure all, <1-
3> to changespecific default [y]: n
```

步骤5：配置截获方法。

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

步骤6：配置时区。

```
Enter Time Zone <Time Zone Hours(-23 to 23) Minutes(0-59)>
[UTC 0 0]: PST -8 0
```

步骤7：配置管理接口、IP地址和默认网关。

此设计使用外部接口作为管理接口。

```
No.      Interface Name      IP Address    Network Mask
  1. GigabitEthernet 1/0      unassigned      unassigned
(internal)
  2. GigabitEthernet 2/0            dhcp
(external)
Select Management Interface [1]: 2
Enable Autosense for Management Interface? (y/n)[y]: y
Enable DHCP for Management Interface? (y/n)[y]: n
```

**技术提示**

您可能会收到以下警告。由于IP地址配置之前已经提供，该警告可以忽略。

*** You have chosen to disable DHCP! Any network configuration learnt from DHCPserver will be unlearnt! SETUP will indicate failure as the managementinterface cannot be brought up - Please make sure WAE Management Interface IPaddress and Default Gateway are configured from the Router; Press ENTER to continue:

步骤8：配置中央管理器地址

```
Enter Central Manager IP Address (WARNING: An invalid entry
will cause SETUP to take a long time when applying WAAS
configuration) [None]: 10.4.48.100
```

步骤9：配置DNS、主机和NTP设置。

```
Enter Domain Name Server IP Address [Not configured]:
10.4.48.10
Enter Domain Name(s) (Not configured): cisco.local
Enter Host Name (None): Br203-WAE-SRE700-1
Enter NTP Server IP Address [None]: 10.4.48.17
```

步骤10：配置WCCP路由器列表。

```
Enter WCCP Router (max 4) IP Address list (ip1 ip2 ...) []:
10.5.48.253 10.5.48.254
```

步骤11：选择适当的许可。

```
1. Transport
2. Enterprise
3. Enterprise & Video
Enter the license(s) you purchased [2]: 2
```

步骤12：验证配置设置。

```
      Parameter                 Configured Value
 1. Interception Method         WCCP
 2. Time Zone                   PST -8 0
 3. Management Interface        GigabitEthernet 2/0
(external)
 4.     Autosense                  Enabled
 5.     DHCP                       Disabled
        IP Address                 10.5.52.8
        IP Network Mask            255.255.255.0
    IP Default Gateway          10.5.52.1
 6. CM IP Address               10.4.48.100
 7. DNS IP Address              10.4.48.10
 8. Domain Name(s)              cisco.local
 9. Host Name                   Br203-WAE-SRE700-1
10. NTP Server Address          10.4.48.17
11. WCCP Router List            10.5.48.253 10.5.48.254
12. License                     Enterprise
ESC Quit ? Help ! CLI ———————— WAAS Final Configuration
————————

Press 'y' to select configuration, <F2> to see all
configuration, 'd' to toggle defaults display, <1-12> to
change specific parameter [y]: y
                Router WCCP configuration
First WCCP router IP in the WCCP router list seems to be an
external address; WCCP configuration on external routers is
not allowed through SETUP. Please press ENTER to apply WAAS
configuration on WAE ...
Applying WAAS configuration on WAE ...
May take a few seconds to complete ...
WAAS configuration applied successfully!!
Saved configuration to memory.
Press ENTER to continue ...
```

您将收到包含了建议的路由器WCCP配置模板的提示。该路由器配置在随后的程序中均有包括，因此您不需要保留这些信息。

步骤13：配置GRE协商返回（negotiated return）。

所有WAE设备对其各自的WCCP路由器使用GRE-协商返回（negotiated return）：

```
egress-method negotiated-return intercept-method wccp
```

步骤14：配置WCCP路由器列表。

设置脚本根据提供的信息生成一个路由器列表。要查看设备配置，请输入以下命令：

```
Br203-WAE-SRE700-1# show running-config | include wccp router-
list
wccp router-list 8 10.5.48.253 10.5.48.254
```

路由器列表8专门用于在缺省网关路由器上配置的WCCP。此设计使用了GRE-协商返回（negotiated return）和路由器回环地址，因此我们需要创建一个新的路由器列表，并删除路由器列表8。

在此设计中所有WAE配置均使用路由器列表1。

```
no wccp router-list 8 10.5.48.253 10.5.48.254
wccp router-list 1 10.5.48.253 10.5.48.254
```

此设计在路由器和WAE之间使用了认证。

```
wccp tcp-promiscuous service-pair 61 62 router-list-num 1
password c1sco123
```

步骤15：启用SSH。

启用SSH需要生成RSA密钥并启用sshd服务。

```
ssh-key-generate key-length 2048
sshd version 2
sshd enable
```

**步骤16**：禁用telnet。

```
no telnet enable
```

**步骤17**：配置安全用户身份验证。

启用AAA身份验证来支持访问控制。AAA控制所有对于WAAS/WAE设备的管理访问(SSH和HTTPS)。

在设置期间已在WAAS/WAE上创建了本地管理员用户。这一用户帐户能够在中央TACACS+服务器不可用或是贵企业没有TACACS+服务器的情况下管理设备。

以下设置可将TACACS+配置为用户身份验证（登录）和用户授权（配置）的主要方法。

```
tacacs key SecretKey
tacacs password ascii
tacacs host 10.4.48.15 primary
!
authentication login local enable secondary
authentication login tacacs enable primary
authentication configuration local enable secondary
authentication configuration tacacs enable primary
authentication fail-over server-unreachable
```

**步骤18**：保存配置。

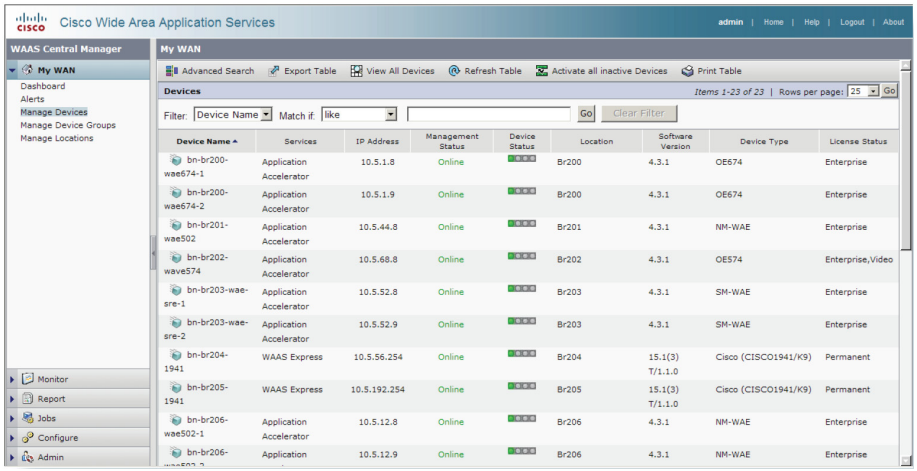
在您完成配置更改后，保存配置。

```
copy running-config startup-config
```

当WAE在网络上变为活动状态之后，每个WAE都将在WAAS中央管理器中进行注册。您可以通过在各个WAE上使用show cms info命令，或者通过WCM的web界面，来验证这一注册。

当配置完成后，通过输入转义字符串Ctrl-Shift-6 x，您可以将会话返回至主机路由器的命令行。

**图26.** WAAS中央管理器—安装的托管设备列表




## 程序6　为WAE设备配置远程交换机

如果您使用的是远程站点分布交换机设计，该分布交换机将是实际连接WAE设备的位置。该类型设备需要一种具有弹性的连接，但不需要路由协议。这种连接可以使用二层EtherChannel链路。

本指南假定已经配置了分布层交换机，只有完成交换机与WAE设备连接所需的程序包括在内。有关分布层交换机配置的详细信息，请参阅《面向大型企业的思科IBA智能业务平台——无边界网络局域网部署指南》。

这种设计将WAE设备置于数据（主要）VLAN之上。这需要创建一个VLAN和相应的SVI（如果没有的话）。

**步骤1**：创建VLAN和SVI（如果必要的话）。

```
vlan [VLAN number]
 name [VLAN name]
interface Vlan [VLAN number]
 ip address [IP address] [netmask]
 no shutdown
```

步骤2：为设备配置二层EtherChannel链路，并将它们与VLAN相关联。

```
interface Port-channel [number]
  switchport access vlan [VLAN number]
!
interface [type] [number]
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
!
interface [type] [number]
 switchport access vlan [VLAN number]
 channel-group [number] mode on
 no shutdown
```

示例

```
vlan 100
 name Data
interface Port-channel7
 description bn-wae-1 EtherChannel
 switchport access vlan 100
!
interface GigabitEthernet1/0/3
 description bn-wae-1 port 1
 switchport access vlan 100
 channel-group 7 mode on
 no shutdown
!
interface GigabitEthernet2/0/3
 description bn-wae-1 port 2
 switchport access vlan 100
 channel-group 7 mode on
 no shutdown
!
interface Vlan100
 ip address 10.5.1.1 255.255.255.0
 no shutdown
```

## 程序7 在路由器上配置WCCPv2

在此设计中，WCCP将流向广域网的网络流量导向WAAS系统，进行优化。这种方法实现了简洁的部署，只增加了极少的布线工作，它需要WAN汇聚和远程站点路由器都针对WCCP进行配置。

步骤1：配置全局WCCP参数，并启用服务61和62。

您必须为针对WAAS的WCCP重定向启用服务61和62。这些服务应当使用WCCP版本2。作为一种最佳实践，可以使用重定向列表，从WCCP重定向中免除某些关键的流量类型。

为了防止未经授权的WAE设备加入WAAS集群，您应当配置一个组列表和密码。

```
ip wccp version 2
ip wccp 61 redirect-list [redirect ACL] group-list [group ACL]
password [password]
ip wccp 62 redirect-list [redirect ACL] group-list [group ACL]
password [password]
ip access-list standard [group ACL]
 permit [WAAS cluster member IP]
 permit [WAAS cluster member IP]
ip access-list extended [redirect ACL]
 deny   tcp [src IP address] [dest IP address] any eq [TCP
port]
 deny   tcp [src IP address] [dest IP address] any eq [TCP
port]
  <additional lines as necessary>
 deny   tcp [src IP address] [dest IP address] any eq [TCP
port]
 permit tcp any any
```

步骤2：在LAN和WAN接口上配置WCCP重定向。

选项1. 针对DMVPN中枢路由器。

必须确定在哪些接口截获往返广域网的流量。

借助服务61在LAN接口的入站方向截获来自局域网的流量。

interfaces. interface [interface type] [number]

```
ip wccp 61 redirect in
```

DMVPN中枢路由器要求在LAN接口的出站方向上使用WCCP 62，以支持分支到分支隧道的动态创建。

借助服务62在LAN接口的出口方向上截获来自广域网的流量。

```
interface [interface type] [number]
 ip wccp 62 redirect out
```

示例——选项1

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
!
interface Port-channel3
 ip wccp 61 redirect in
 ip wccp 62 redirect out
!
ip access-list standard BN-WAE
 permit 10.4.32.161
 permit 10.4.32.162

ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
```

选项2：针对除DMVPN中枢路由器外的所有WAAS路由器。

必须确定在哪些接口截获往返广域网的流量。

借助服务61在所有LAN接口的入站方向上截获来自局域网的流量。没有必要在语音接口和语音VLAN上配置WCCP截获。

```
interface [interface type] [number]
 ip wccp 61 redirect in
```

借助服务62在所有WAN接口的入站方向上截获来自广域网的流量，包括DMVPN隧道接口（但非其底层的物理接口）。

```
interface [interface type] [number]
 ip wccp 62 redirect in
```

示例——选项2

```
ip wccp version 2
ip wccp 61 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
ip wccp 62 redirect-list WAAS-REDIRECT-LIST group-list BN-WAE
password c1sco123
!
interface Port-channel1
 ip wccp 61 redirect in
!
interface Tunnel10
 ip wccp 62 redirect in

ip access-list standard BN-WAE
 permit 10.4.32.161
 permit 10.4.32.162

ip access-list extended WAAS-REDIRECT-LIST
 remark WAAS WCCP Redirect List
 deny   tcp any any eq 22
 deny   tcp any eq 22 any
 deny   tcp any eq telnet any
 deny   tcp any any eq telnet
 deny   tcp any eq bgp any
 deny   tcp any any eq bgp
 deny   tcp any any eq 123
 deny   tcp any eq 123 any
 permit tcp any any
```

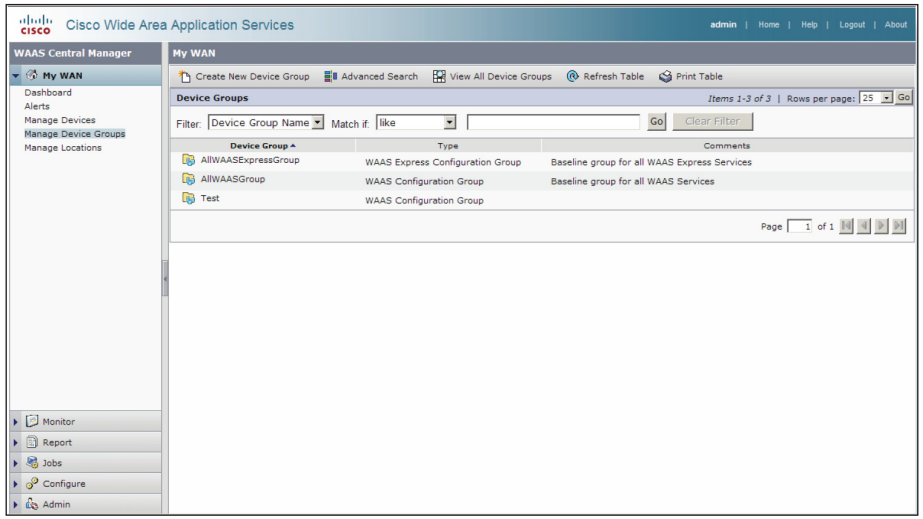
## 程序8　为WAASx配置中央管理器

与WAE设备类似，您可以使用WAAS中央管理器来集中管理WAASx路由器。您必须设定一个用户名和密码，以用于WCM访问WAASx路由器执行监控和管理任务。这些通信采用HTTPS加以保护，而HTTPS需要使用数字证书。

**步骤1**：为WAAS Express路由器设置证书

在WAAS中央管理web接口上（https://10.4.48.100:8443），为WAASx路由器配置登录和密码证书。您可以通过编辑设备组AllWAASExpressGroup来完成这项操作。从WAAS Central Manager（WAAS中央管理器）主页面，点击左侧的My Wan（我的广域网）-> Manage Device Groups（管理设备组）。

**图27.** WAAS中央管理器——托管设备组




点击AllWAASExpressGroup，选择设备组，然后点击Admin（管理员）选项卡（与AllWAASExpressGroup设备组相关联）

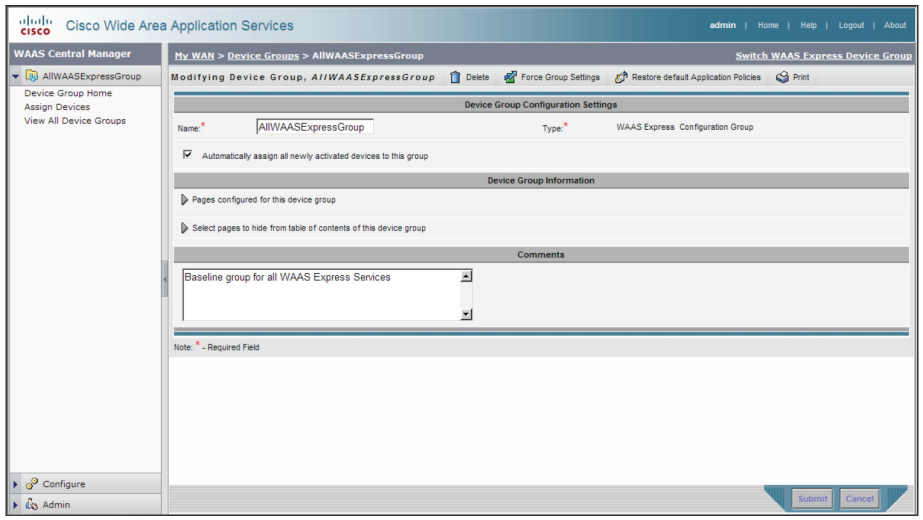
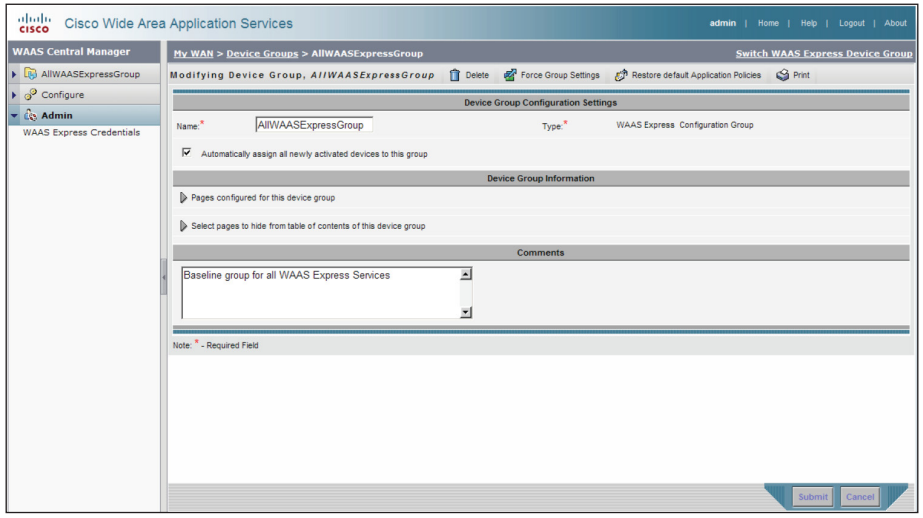
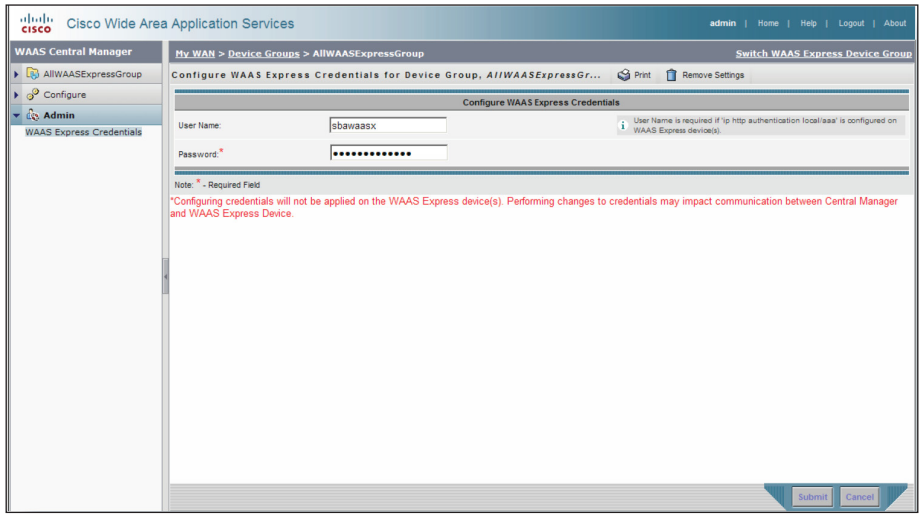



**图28.** WAAS中央管理器—AllWAASExpressGroup



点击WAAS Express Credentials（WAAS Express证书）。

图29. WAAS中央管理器—WAASx credentials




输入适当的用户名和密码（您也计划在WAASx路由器或中央AAA服务器上配置）。示例使用了用户名sbawaasx和密码c1sco123

**步骤2**：从WCM导出可信的数字证书

在WCM和路由器之间进行安全的通信，需要您为每个WAASx路由器安装来自WCM的数字证书。该证书能够以保密增强邮件（PEM）Base64格式导出。此命令可以通过设备命令行界面执行。

```
WAAS-WCM-1#show crypto certificate-detail admin | begin BEGIN
...skipping
-----BEGIN CERTIFICATE-----
<certificate data deleted>
-----END CERTIFICATE-----
```

鉴于所有WAASx路由器都需要这一证书，请复制粘贴此证书并将其保存到安全的文件中。

## 程序9　配置WAAS Express路由器

要打开内嵌的WAN优化功能，您必须在路由器的WAN接口上启用WAAS优化。WAASx也可以通过WAE设备所使用的同一WAAS中央管理器进行集中管理。路由器必须进行适当的配置，以便与WCM安全地通信。

请注意，WAASx是一项经特别许可的特性。必须将这一许可证安装在具有充足DRAM的路由器上，以支持WAASx功能。

WAASx路由器必须采用最大的DRAM进行配置

WCCP重定向不能用于实施WAASx。因为所有流量优化都是在路由器上进行，因此无需将流量重定向至外部设备。

**步骤1**：在WAN接口上启用WAAS。

WAASx只需一个命令即可启用。

在采用mGRE隧道的远程站点DMVPN分支路由器上。

```
interface Tunnel10
 waas enable
```

步骤2：配置自签名信任点和生成数字证书。

在WAASx路由器上，配置永久的自签名信任点并注册。即使您已经拥有了一个从之前已启用的HTTPS自动生成的自签名信任点，这一步骤也必不可少。请确保路由器上已经配置好的主机名和域名符合subject-alt-name字段。

```
crypto pki trustpoint SELF-SIGNED-TRUSTPOINT
 enrollment selfsigned
 subject-alt-name Br205-1941.cisco.local
 revocation-check none
 rsakeypair SELF-SIGNED-RSAKEYPAIR 2048
 exit
crypto pki enroll SELF-SIGNED-TRUSTPOINT
The router has already generated a Self Signed Certificate for
trustpoint TP-self-signed-xxxxxx.
If you continue the existing trustpoint and Self Signed
Certificate will be deleted.
Do you want to continue generating a new Self Signed
Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/
no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

步骤3：配置HTTPS客户端和服务器

配置WAASx路由器，以便将回环接口用作任意HTTP客户端通信的源接口。

```
ip http client source-interface Loopback0
```

启用HTTPS安全服务器。

```
ip http secure-server
ip http secure-trustpoint SELF-SIGNED-TRUSTPOINT
```

步骤4：创建信任点并导入WAAS中央管理器证书。

```
crypto pki trustpoint BN-WAAS-WCM
 revocation-check none
 enrollment terminal pem
 exit
crypto pki authenticate BN-WAAS-WCM
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

现在，从上一程序生成的WAAS中央管理器中粘贴PEM证书。

```
-----BEGIN CERTIFICATE-----
<certificate data omitted>
-----END CERTIFICATE-----
Certificate has the following attributes:
 Fingerprint MD5: 2EA6FF8F 38ABC32F 25168396 1A587F17
Fingerprint SHA1: 8DAB6185 7B95FC4C 34FDACDC A8F2B1A4 8074709B
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

步骤5：在WAAS中央管理器中注册WAASx路由器。

在正确生成并安装数字证书后，您可以在WCM中注册路由器。

```
waas cm-register https://10.4.48.100:8443/wcm/register
```

路由器将在WCM上显示为托管设备。

# 附录A: 大型企业VPN远程站点部署产品列表

| 功能区域 | 产品 | 产品编号 | 软件版本 |
|---|---|---|---|
| WAN 500设计 | | | |
| WAN汇聚 | ASR1002 | ASR1002-5G-VPN/K9<br>ASR1002-PWR-AC | IOS-XE 15.1(3)S0a |
| WAN汇聚: WAAS中央管理器 | WAVE-594 WAAS设备 | WAVE-594-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| WAN汇聚: WAAS应用加速器 | WAE-7571-K9 WAAS设备 | WAE-7571-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| WAN 100设计 | | | |
| WAN汇聚: | ASR1001 | ASR1001-2.5G-VPNK9<br>ASR1001-PWR-AC | IOS-XE 15.1(3)S0a |
| WAN汇聚: WAAS中央管理器 | WAVE-594 WAAS设备 | WAVE-594-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| WAN汇聚: WAAS应用加速器 | WAE-7541-K9 WAAS设备 | WAE-7541-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| WAN远程站点路由器 | | | |
| WAN远程站点路由器 | Cisco1941 | C1941-WAASX-SEC/K9<br>SL-19-DATA-K9 | 15.1(4)M2 |
| WAN远程站点路由器 | Cisco2911 | C2911-VSEC/K9<br>SL-29-DATA-K9 | 15.1(4)M2 |
| WAN远程站点路由器 | Cisco2921 | C2921-VSEC/K9<br>SL-29-DATA-K9 | 15.1(4)M2 |
| WAN远程站点路由器 | Cisco3925 | C3925-VSEC/K9<br>SL-39-DATA-K9 | 15.1(4)M2 |

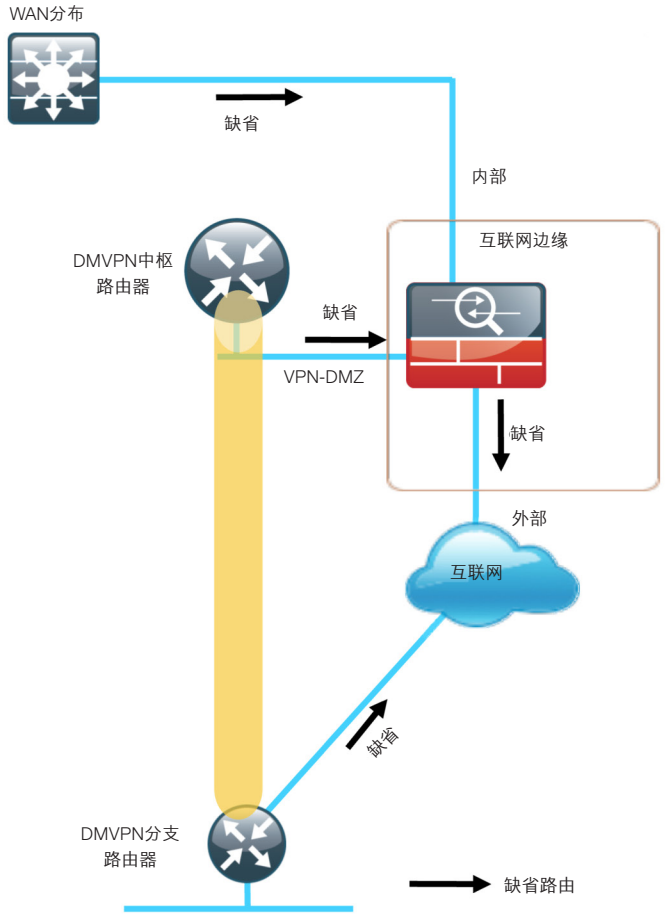
| 功能区域 | 产品 | 产品编号 | 软件版本 |
| --- | --- | --- | --- |
| WAN远程站点路由器 | Cisco3945 | C3945-VSEC/K9<br>SL-39-DATA-K9 | 15.1(4)M2 |
| WAN远程站点WAAS | | | |
| 应用加速器 | SM-SRE-700-K9 | SM-SRE-700-K9<br>WAAS-ENT-SM | 4.4.1 (WAAS-UNIVERSAL-K9) |
| 应用加速器 | SM-SRE-900-K9 | SM-SRE-900-K9<br>WAAS-ENT-SM | 4.4.1 (WAAS-UNIVERSAL-K9) |
| 应用加速器 | WAVE-294 | WAVE-294-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| 应用加速器 | WAVE-594 | WAVE-594-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |
| 应用加速器 | WAVE-694 | WAVE-694-K9<br>WAAS-ENT-APL | 4.4.1 (WAAS-UNIVERSAL-K9) |

# 附录B: 技术特性补充

## 用于DMVPN的Front Door vREF (FVRF)

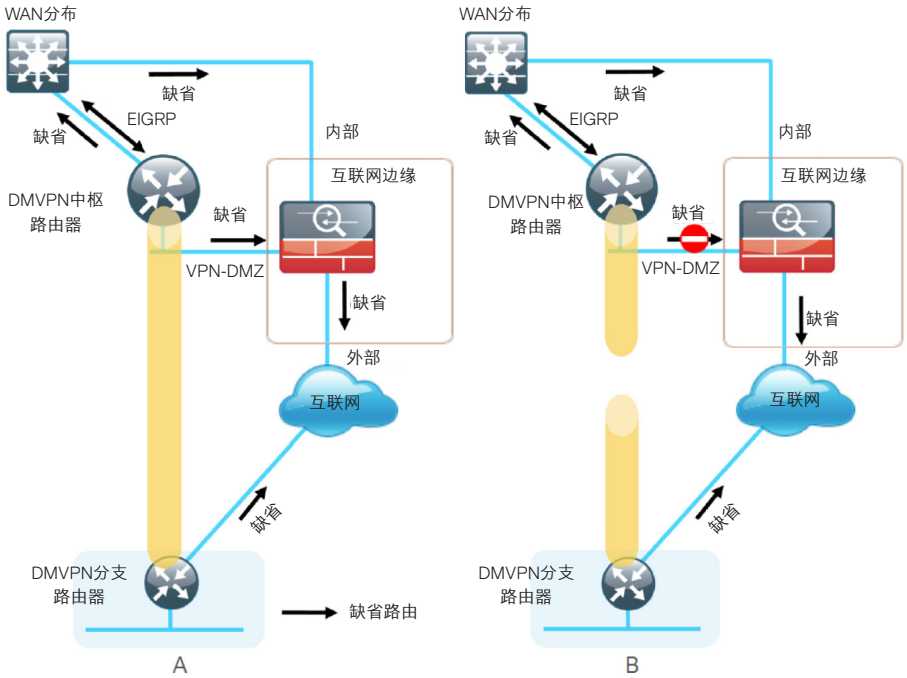
建立IPsec隧道要求加密路由器之间具备可达性。当您使用互联网时，路由器使用缺省路由来联系其对等设备。

图30. 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），那么您必须要向VPN中枢路由器通告缺省路由。要了解详情，请参见下图的A部分。

图31. 缺省路由注入之前/之后的IPsec隧道



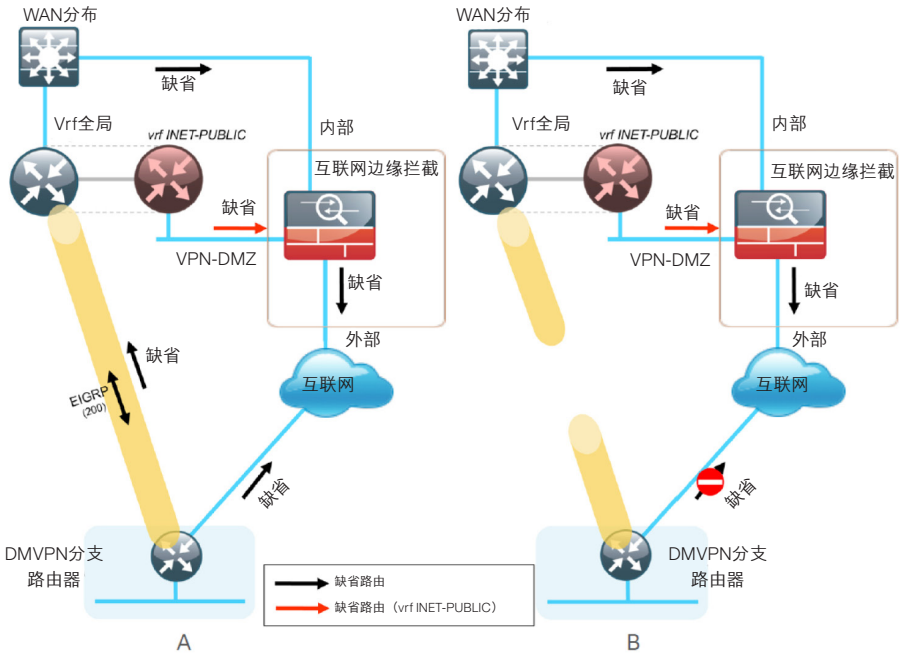

向中枢路由器（目前具有缺省路由）通告缺省路由会带来问题。该路由需要更佳的管理距离来成为活动缺省路由，然后取代支持对等IPsec隧道连接的缺省路由。这一路由通告将破坏上面图31 B部分中所示的隧道。

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。如下面图32的A部分所示。

**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32. 支持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。由于远程站点策略需要为最终用户提供中央互联网访问能力，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，隧道连接中断，如上图的B部分中所示。

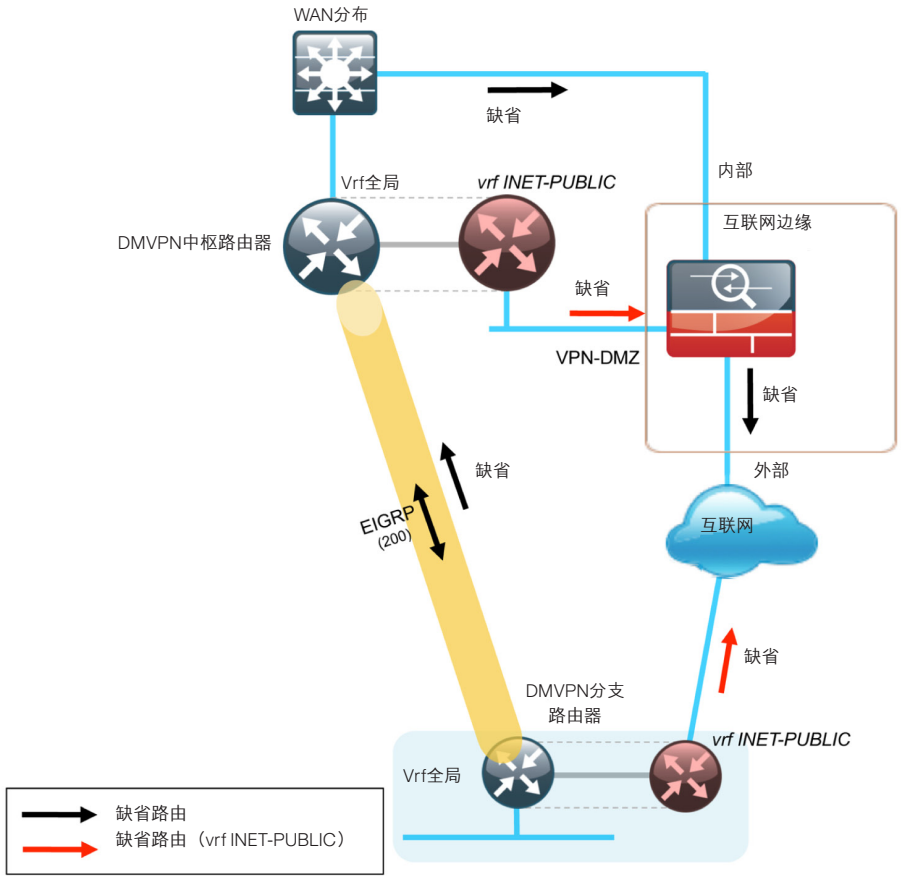
此配置要求在远程站点路由器上也使用F-VRF。

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隧道进行缺省路由
- 对于采用多种WAN传输方法的站点，能够使用动态缺省路由
- 能够采用DMVPN构建分支到分支隧道，最终用户流量通过VPN隧道进行缺省路由

在WAN汇聚站点和WAN远程站点都使用了F-VRF的最终设计如下图所示。

图33. FVRF一最终配置



# 附录C：变更

本附录总结了相比先前的思科IBA智能业务平台，本指南所做的变更。

- 针对IP组播，我们启用了思科自动RP，以简化部署。
- 对于远程站点路由器回环接口，我们建议使用一个不在网络任何其他部分汇总范围内的IP地址范围。
- 对于AAA，我们更新了命令的语法。
- 对于广域网汇聚平台选项，我们删除了Cisco 3945E集成多业务路由器。
- 对于应用加速平台选项，我们删除了之前的生成设备。

**备注**

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

B-0000160-1 1/12