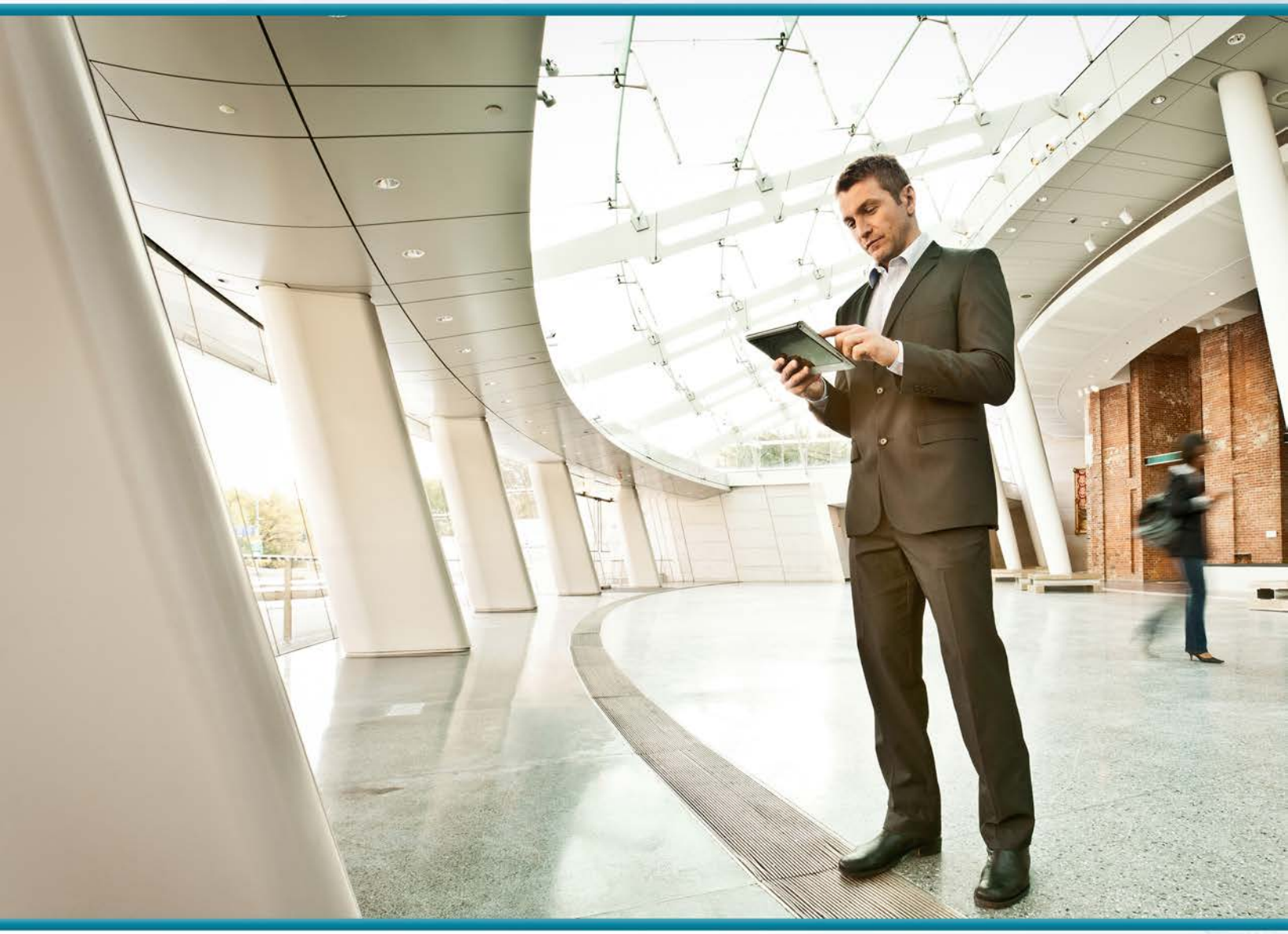


# 智能广域网

## 技术设计指南摘要

2015 年 1 月

CISCO VALIDATED DESIGN

# 简介

思科智能广域网 (IWAN) 解决方案为以下具有以下目标的组织提供设计和实施指导：使用与传输方式无关的设计 (TID)、智能路径控制、应用优化来部署广域网 (WAN)；保护分支机构之间的加密通信，同时减少广域网的运行成本。IWAN 充分利用具成本效益的传输服务以增加带宽容量，而不要求降低协作或基于云的应用的性能、可靠性和安全性。

# 技术使用案例

组织要求使用广域网来提供足够的性能和可靠性，从而让远程站点的用户能够高效地支持业务。虽然远程站点工作人员使用的大多数应用和服务都集中于某个位置，但广域网设计还必须为处于任何位置的员工提供常用资源访问体验。

基于运营商的 MPLS 服务对于专门使用该服务来实现远程站点广域网连接的组织而言，并不总是可用的或具成本效益的。有多种广域网传输产品（包括 MPLS VPN、互联网、蜂窝网 [3G/LTE]，以及运营商以太网）可同时用来创建一个强大的、安全的，并具成本效益的广域网。基于互联网的 IP VPN 提供具有吸引力的带宽定价，可以增加优质 MPLS 产品或在某些场景下更换 MPLS。一个灵活的网络架构应包括所有常用的广域网传输产品作为选项，而不会显著增加整体设计的复杂性。

虽然互联网 IP VPN 网络提出了一个具有吸引力的高效的广域网连接方案，但在任何时候，一个组织通过公共网络发送数据时都存在该数据将受到损坏的风险数据。丢包或损坏可能导致监管违规，可能呈现负面的公众形象，这两种后果都可能会对组织的财务方面造成重大影响。保护通过互联网等公共网络的数据传输要求适当的加密技术以企业信息。

## 使用案例：保护站点间的广域网通信

本指南帮助组织通过私有 (MPLS VPN) 和公共（互联网）IP 网络高效、安全地连接远程站点。

本设计指南能帮助您实现以下网络功能：

- 安全的加密通信解决方案通过使用动态多点 VPN (DMVPN) IPsec 隧道重叠配置可在多达 2000 个位置实施
- 多宿主主用 - 主用连接解决方案通过在远程站点使用单或双路由器可实现恢复力并高效使用所有广域网带宽
- 支持在核心的网络枢纽站点上执行 IP 组播和复制
- 可与执行了网络地址转换 (NAT) 的公共互联网网络进行兼容性

# 思科智能广域网概述

随着全球化的到来，广域网已经成为处于世界任何一个角落的远程办事处和客户之间进行沟通的主要渠道。此外，随着数据中心的整合，应用正迁移到集中的数据中心和云。现在，广域网发挥着更重要的作用，因为企业的生存依赖于网络的可用性和性能。

到现在为止，使用可预测的性能获得可靠的连接性的唯一方法是利用采用 MPLS 或租用线路服务的私有广域网。然而，基于运营商的 MPLS 和租用线路服务对于要使用这两者进行广域网传输，以便支持远程站点连接日益增长的带宽需求的组织而言价格昂贵，而且并不总是具成本效益。组织正在寻找各种方法来降低运营预算，同时提供远程站点所需的足够的网络传输。

随着带宽需求的增加，互联网已成为一个更加稳定的平台，而且性价比非常有吸引力。然而，企业主要在自己的较小型站点部署“使用互联网作为广域网”，或者因其具有风险将之作为备份路径。现在，借助思科 IWAN，您可在所有的分支机构实现这个具成本效益的、性能有所提升的机会。

思科 IWAN 使组织能够通过任何连接提供无与伦比的体验。借助思科 IWAN，IT 组织可以通过使用更便宜的广域网传输方案为分支机构连接提供更多的带宽，而不会影响性能、安全性或可靠性。借助 IWAN 解决方案，流量基于应用的服务级别协议 (SLA)、终端类型和网络条件动态路由，以提供最佳的质量体验。通过使用 IWAN 实现的节省不仅可用于支付基础设施升级，还可释放业务创新所需的资源。

*图 1 - 思科 IWAN 解决方案组件*


## 与传输方式无关

使用 DMVPN，IWAN 为通过任何运营商的服务产品（包括 MPLS、宽带和蜂窝网 3G/4G/LTE）的简单的多宿主提供功能更重要的是，该设计使用单一路由控制平面和面向提供商的最小的对等，简化了路由设计，使组织可以轻松混搭，同时更改提供商和传输方案建议。使用两个或多个广域网传输提供商，以便最大限度地提升网络可用性 (99.999%)。此外，思科 DMVPN 解决方案提供业界认可，并经过美国政府 FIPS 140-2 认证的 IPsec 解决方案，用于实现数据隐私和完整性保护，以及自动化站点间 IP 安全性 (IPsec) 隧道。这些隧道可以使用预共享密钥或具有非军事区 (DMZ) 证书授权的公共密钥基础设施进行设置，以注册并授权在路由器之间使用密钥。

### 智能路径控制

思科性能路由 (PfR) 提高应用交付速度和广域网效率。PfR 通过查看应用类型、性能、策略和路径状态来动态控制数据包的转发。PfR 持续监控抖动、丢包和延迟等网络性能，然后基于应用策略，选择性能最佳的路径来转发关键应用。思科 PfR 可以智能平衡负载流量，以便高效地利用所有可用的广域网带宽。IWAN 智能路径控制是基于互联网传输提供企业级广域网的关键。

### 应用优化

思科应用可视性与可控性 (AVC) 和思科宽域应用服务 (WAAS) 基于广域网提供应用性能可视性与优化。由于 HTTP（端口 80）等众所周知的端口不断重复使用，应用变得越来越不透明，因此应用静态端口类别已无法满足需求。思科 AVC 提供应用感知，对流量执行深度数据包检测，以确定和监控应用的性能。思科 AVC 使 IT 能够确定网络中通过的流量、为业务关键型服务调整网络，并解决网络问题随着网络上应用可视性的提高，可以支持更好的 QoS 和 PfR 策略，以帮助确保关键应用在网络中传输时享有适当的优先级。思科 WAAS 可提供特定应用加速功能，在改进响应时间的同时降低对广域网带宽的要求。

### 安全连接

安全连接保护企业通信并将用户流量直接卸载到互联网强大的 IPsec 加密、基于区域的防火墙和严格的访问控制都用来保护通过公共互联网的广域网。将远程站点用户直接路由到互联网提高了公共云应用的性能，同时降低了通过广域网的流量。思科云网络安全 (CWS) 服务提供了一个基于云的网络代理，以便集中管理并保护访问互联网的用户流量。

# 设计概述

“*Cisco Intelligent WAN Design Guide*”（*思科智能广域网设计指南*）提供的设计支持面向多个远程站点局域网 (LAN) 的高可用的、安全的优化连接。

### 与传输方式无关的广域网设计

与传输方式无关的设计通过使用所有广域网传输方案（包括 MPLS、互联网和蜂窝网 [3G/4G]）的 IPsec VPN 重叠来简化广域网部署单个的 VPN 重叠降低路由和安全的复杂性，并在选择提供商和传输方案方面提供灵活性。思科 DMVPN 提供 IWAN IPsec 重叠。

DMVPN 使用多点通用路由封装 (mGRE) 隧道来互连网络枢纽和所有分支路由器。在这种情况下，这些 mGRE 隧道有时也被称为 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。

#### 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运营商组成的大型公共 IP 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任何明确的保证。虽然采用的是“尽力而为”方案，但在某些情况下，互联网是增加优质 MPLS VPN 传输，或作为主要广域网传输的一种明智选择。IWAN 架构利用两个或多个提供商获取恢复力和应用可用性。提供商路径的多样性为 PfR 提供了围绕供应商性能波动进行路由的基础。

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。

本设计指南同时使用 MPLS 和互联网实现 VPN 站点间连接。

### 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，并可部署在本设计指南中介绍的所有广域网路由器之上。

DMVPN 支持基于任何运营商传输的按需全网状连接，并支持使用简单的中心辐射型配置，成为了安全的重叠广域网解决方案。此外，DMVPN 也支持能够动态分配 IP 地址的分支路由器。

DMVPN 使用多点通用路由封装 (mGRE) 隧道来互连网络枢纽和所有分支路由器。在这种情况下，这些 mGRE 隧道有时也被称为 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

上文提及的广域网传输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

本指南介绍了两种 IWAN 设计模式。

第一种设计模式是 IWAN 混合模式，它使用与互联网 VPN 搭配的 MPLS 作为广域网传输方式。在这种设计模式中，MPLS 广域网可以为关键应用所需的关键服务类别提供更多的带宽，并为这些应用提供 SLA 保证。第二种设计模式是 IWAN 双互联网模式，它使用一对互联网运营商，以便进一步降低成本，同时保持较高水平的广域网恢复力。第三种设计模式是 IWAN 双 MPLS 模式，不会在本指南中介绍。

*图 2 - 思科 IWAN 设计模式*

适用于两种设计模式的 IWAN 广域网汇聚（网络枢纽）设计包含两个广域网边缘路由器。

当广域网汇聚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 流量的广域网汇聚路由器被称作 *VPN 网络枢纽路由器*。在采用 IWAN 的情景中，MPLS CE 路由器也用作 VPN 网络枢纽路由器。不管采用哪种设计模式，广域网汇聚路由器都始终连接到一对分布层交换机。

每种设计模式都显示拥有局域网连接，或者连接到紧缩核心/分布层，或者连接到专用广域网分布层。从广域网汇聚的角度，这两种方法在功能方面没有差异。

在所有广域网汇聚设计中，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。

每种设计的特点在下面的章节中加以讨论。

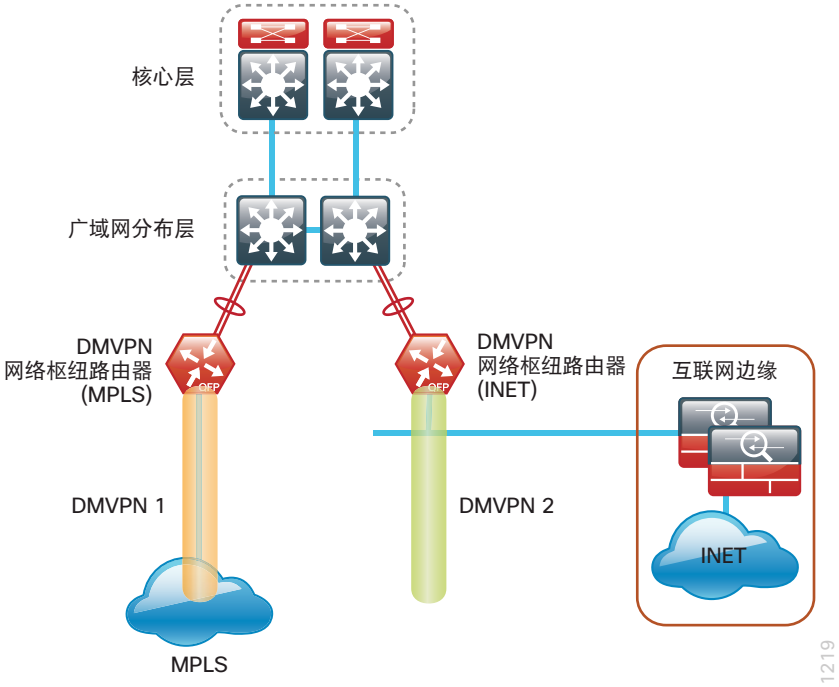
### IWAN 混合设计模式

IWAN 混合设计模式：

- 拥有单个 MPLS VPN 运营商。
- 使用单个互联网运营商。
- 在 MPLS 和互联网链路上都使用前门虚拟路由和转发 (FVRF)，在 FVRF 内使用静态默认路由。

  FVRF 提供从提供商出分离出来的控制平面，以及内部和外部网络之间的额外安全层。

*图 3 - 广域网汇聚：IWAN 混合设计模式*



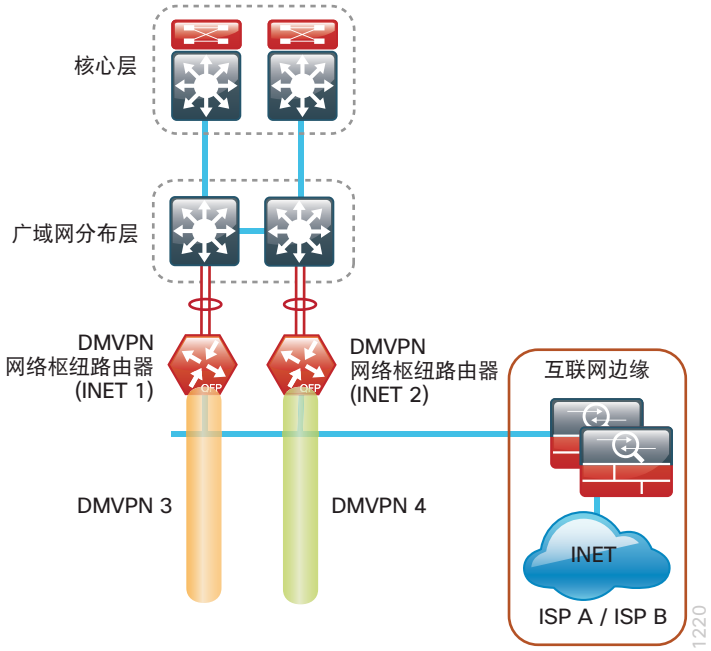
在 IWAN 混合和 IWAN 双互联网这两种设计模式中，DMVPN 网络枢纽路由器都通过互联网边缘中包含的防火墙 DMZ 接口间接连接到互联网。有关连接到互联网的详细信息，请参阅“Firewall and IPS Technology Design Guide（防火墙和 IPS 技术设计指南）”。VPN 网络枢纽路由器被连接到防火墙 DMZ 接口，而不是直接与互联网运营商路由器连接。当 VPN 网络枢纽路由器连接到 MPLS 运营商时，通常不使用防火墙连接。

## IWAN 双互联网设计模式

IWAN 双互联网设计模式：

- 使用两个互联网运营商。
- 在这两种互联网链路上都使用前门 VRF (FVRF)，在 FVRF 内使用静态默认路由。

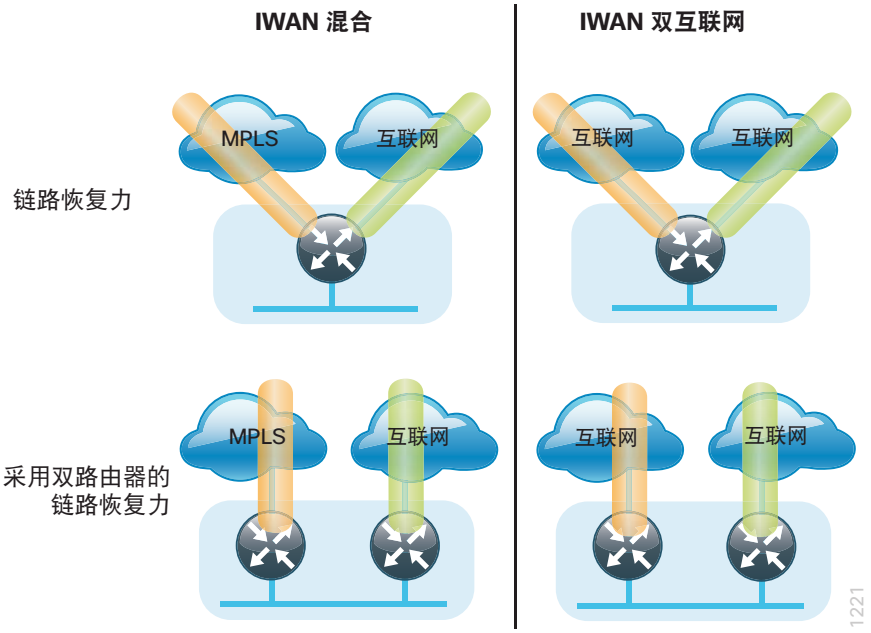
*图 4 - 广域网汇聚：IWAN 双互联网设计模式*



## 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。这些设计构建于各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 5 - 广域网远程站点设计方案*




远程站点设计包含单或双广域网边缘路由器。在本指南中，所有远程站点路由器都是主要站点网络枢纽的 DMVPN 分支路由器。

大多数远程站点均采用单路由器广域网边缘设计；然而，某些远程站点类型则要求使用双路由器广域网边缘设计。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位置，或者有着业务关键型需求、要求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 1 - 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 | 两个 | MPLS VPN | 互联网 |
| 两个 | 两个 | MPLS VPN | 互联网 |
| 一个 | 两个 | 互联网 | 互联网 |
| 两个 | 两个 | 互联网 | 互联网 |

本设计指南还介绍如何为单路由器远程站点添加 LTE 备用 DMVPN。

*表 2 - 采用 LTE 备用的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 | 第三级传输方法 |
|---|---|---|---|---|
| 一个 | 两个，采用备用 | MPLS VPN | 互联网 | 4G LTE |
| 一个 | 两个，采用备用 | 互联网 | 互联网 | 4G LTE |

IWAN 网络设计的模块化特性使您能够创建出可在整个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块。复制单个构建块的能力为网络扩展提供了一种简便的方法，同时也支持采用一致的部署方案。

### 广域网/局域网互连

广域网的主要作用是互连主要站点和远程站点局域网。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“Campus Wired LAN Technology Design Guide”（园区有线局域网技术设计指南）。

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 | 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。本设计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轻松地扩展至更多的接入间。

*表 4 - 广域网远程站点：VLAN 分配*

| VLAN | 用途 | 第 2 层接入 | 第 3 层分布/接入 |
|---|---|---|---|
| VLAN 64 | 数据 1 | 是 | — |
| VLAN 69 | 语音 1 | 是 | — |
| VLAN 99 | 传输 | 是<br>（仅限双路由器） | 是<br>（仅限双路由器） |
| VLAN 50 | 路由器链路 (1) | — | 是 |
| VLAN 54 | 路由器链路 (2) | — | 是<br>（仅限双路由器） |

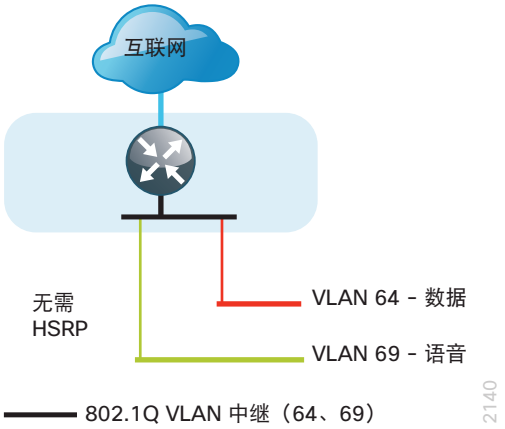
### 第 2 层接入

不需要额外的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，被视为无路由第 2 层站点。所有第 3 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数据和语音等服务。下图中的设计展示的是标准化 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“Campus Wired LAN Technology Design Guide”（园区有线局域网技术设计指南）。

IP 子网基于每个 VLAN 单独进行分配。这一设计仅为接入层分配网络掩码为 255.255.255.0 的子网，即使需要的 IP 地址数量少于 254 个。（这一模式可根据需要调整为其他 IP 地址方案。）路由器和接入交换机之间的连接必须配置 802.1Q VLAN 中继，并且路由器上的子接口要映射到交换机上对应的 VLAN。各个路由器子接口用作每个 IP 子网和 VLAN 组合的 IP 默认网关。

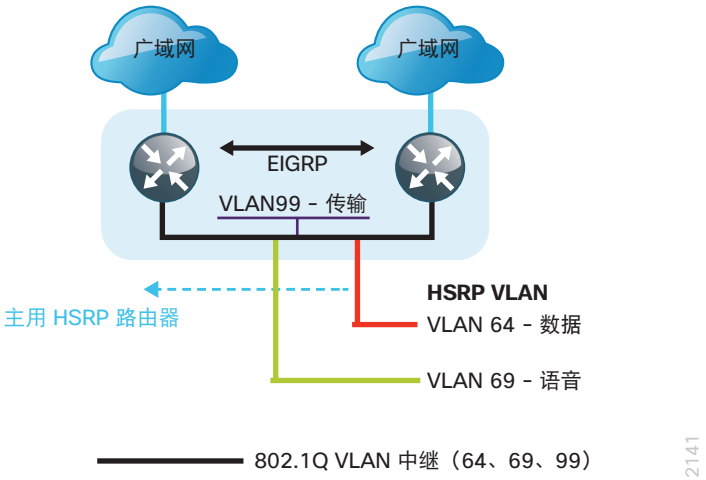
*图 6 - 采用扁平型第 2 层局域网的广域网远程站点（单路由器）*



类似的局域网设计可以扩展为下图中所示的双路由器边缘。这种设计变更会增加一定的复杂性。首先需要运行路由协议。您应在路由器间配置增强型内部网关路由协议 (EIGRP)。

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，思科选择了热待机路由器协议 (HSRP) 作为 FHRP。HSRP 能够支持第一跳 IP 路由器实现透明故障切换。通过为配置了默认网关 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，用来选择主用路由器和备用路由器。当局域网上有多个路由器时，主用路由器用于转发数据包；备用路由器用于在主用路由器发生故障或在达到预定的条件时接管主用路由器的工作。

*图 7 - 采用扁平型第 2 层局域网的广域网远程站点（双路由器）*




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接口线路协议、IP 路由的可达性、IP SLA 的可达性，以及其他几个对象。

为了缩短在发生主广域网故障后的收敛时间，HSRP 能够监控 DMVPN 隧道接口的线路协议状态。该功能使得路由器能够在其 DMVPN 网络枢纽变成无响应时放弃其 HSRP 主用路由器角色，并提供额外的网络恢复力。

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。DMVPN 隧道的 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 路由器能够成为主用 HSRP 路由器。

双路由器设计还提供了在特定情况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，在路由器之间引入一个额外的链路，并将其指定为传输网络 (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之间。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，其中包含有包括分布层与接入层。这一拓扑能够很好地支持单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，这使在路由点到点链路中允许路由器和分布交换机之间运行 EIGRP 路由协议，且在双路由器设计中允许为两个广域网路由器之间通过直接的传输网络。

*图 8 - IWAN 单路由器远程站点：连接到分布层*

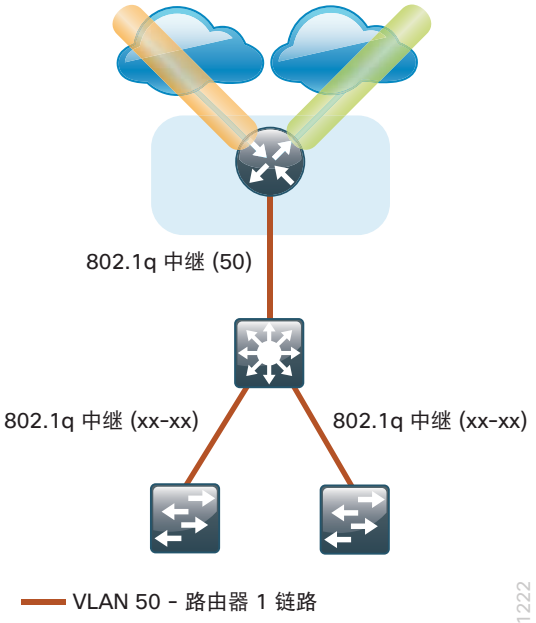
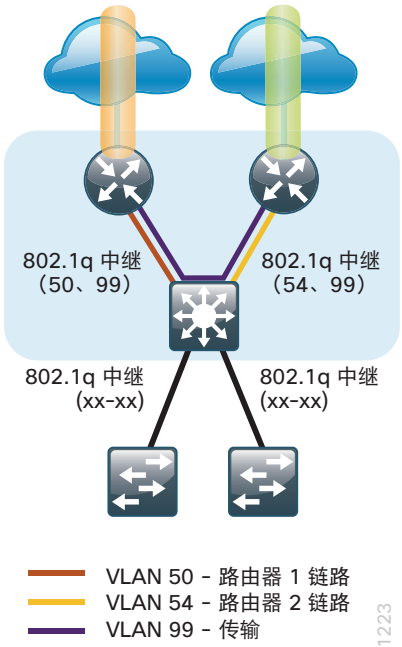
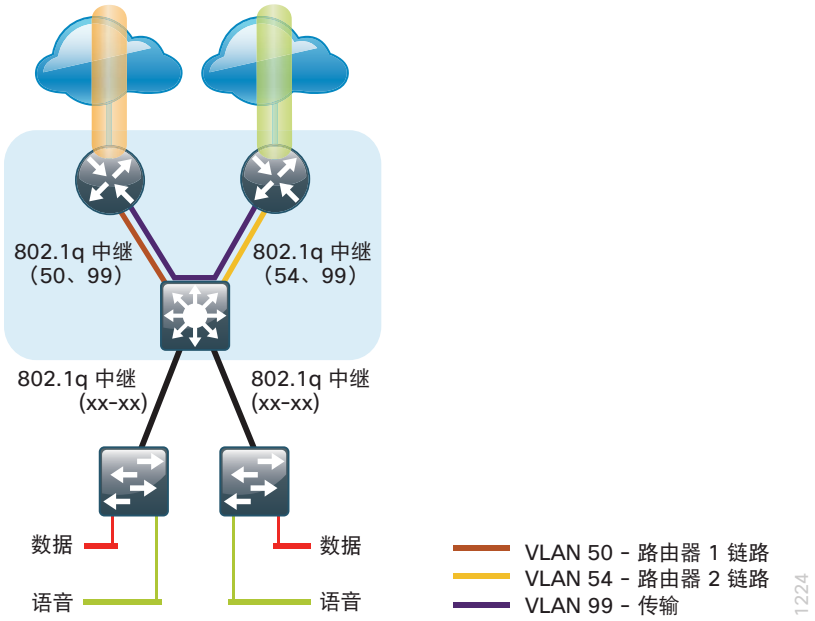



*图 9 - IWAN 双路由器远程站点：连接到分布层*



分布交换机以 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 10 - IWAN 双路由器远程站点：分布层与接入层*




## 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器。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，终端主机必须加入组播组，方法是向其本地组播路由器发送互联网群组管理协议 (IGMP) 消息。在传统的 IP 组播设计中，本地路由器会询问网络中充当交汇点 (RP) 的另一个路由器。RP 将接收器映射到主用源设备上，这样，终端主机就可以加入其数据流。

RP 是一种控制平面功能，应置于网络的核心位置，或者与 IP 组播源通过一对第 3 层交换机或路由器相连的临近的位置。如果接入层是第 2 层，并提供了到 IP 组播 RP 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 RP 的功能。

这种设计可全面支持单一的 IP 组播全局部署，采用 Anycast RP 实施策略。该策略在稀疏模式独立组播协议 (PIM SM) 网络中提供了负载平衡与冗余能力。两个 RP 分担源注册的负载，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，包括环回接口、VLAN 接口和子接口。

## 服务质量

大多数用户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。许多人将这一过程归结为“速度和馈进”。虽然 IP 网络在默认情况下以尽力而为的模式转发流量，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。然而，网络的设计决定了它需要多种服务，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要求数据包在规定的延迟、抖动和丢包参数内送达。

但实际上，网络影响着所有流量，因此必须了解终端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在同一网络中共存。

在该架构内，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进行区别处理，以确保每个应用均能够享有适当的网络资源，从而保护用户体验，并保证业务关键型应用的持续运行。

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，包括实时语音、高质量视频和延迟敏感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，就必须对带宽、延迟、抖动和丢包参数进行管理。

可根据接口速度、可用队列和设备功能，将服务类别分组为常见的 12 种。这 12 种类别的处理方式可以根据您的组织的政策进行调整。思科建议以精细方式对您的流量进行标记，这样更容易在网络中的不同位置做出适当的队列决定。本设计的目的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小的系统影响和最少的工作量，支持网络中的语音、视频、关键数据应用、批量数据应用和管理流量。

下表中列出的 12 种映射通过使用企业中的 8 级的模式和运营商网络中的 6 级模式应用于整个设计。

*表 5 - QoS 服务类别映射*

| 服务类别 | 每跳行为 (PHB) | 差分服务代码点 (DSCP) | 应用示例 |
|---|---|---|---|
| 网络控制 | CS6 | 48 | EIGRP、OSPF、BGP、HSRP、IKE |
| VoIP 电话 | EF | 46 | 思科 IP 电话（G.71 、G.729） |
| 呼叫信令 | CS3 | 24 | SCCP、SIP、H.323 |
| 多媒体会议 | AF4 | 34、36、38 | 思科网真、Jabber、UC 视频、WebEx |
| 实时交互 | CS4 | 32 | 思科网真（以前的） |
| 多媒体流 | AF3 | 26、28、30 | 思科数字媒体系统 (VoD) |
| 广播视频 | CS5 | 40 | 思科 IP 视频监控/思科企业 TV |
| 事务数据 | AF2 | 18、20、22 | ERP 应用、CRM 应用、数据库应用 |
| 运营、管理和维护 (OAM) | CS2 | 16 | SNMP、SSH、Syslog |
| 批量数据 | AF1 | 10、12、14 | 邮件、FTP、备份应用、内容发布 |
| 默认“尽力而为” | DF | 0 | 默认分类 |
| Scavenger | CS1 | 8 | YouTube、iTunes、BitTorent、Xbox Live |

### 适用于 DMVPN 的 Per-Tunnel QoS

适用于 DMVPN 的 Per-Tunnel QoS 功能允许基于每条隧道（分支）在 DMVPN 网络枢纽上配置 QoS 策略。该功能让您能够在 DMVPN 中心辐射型隧道的出口方向在隧道实例（基于每个终端或每个分支）上应用。QoS 策略通过隧道实例上的 QoS 策略，您能够让隧道流量适用于单个分支（父策略），并对隧道内的流量类别进行区分，从而以适当的方法进行处理（计划生育政策）。

通过简化的配置，阻止网络枢纽站点发送超过任何单个远程站点可以处理的流量。这样可以确保高带宽网络枢纽站点的数量少于带宽更低的远程站点的数量。

## 智能路径控制

利用 PfR 进行智能路径控制，可提高应用交付和广域网的效率。PfR 使用策略通过查看应用类型、性能和路径状态来动态控制数据包的转发。PfR 持续监控抖动、丢包和延迟等网络性能，然后基于应用策略，选择性能最佳的路径来转发关键应用。PfR 使用高级负载平衡技术，可以平均分配流量，以便保持相对均等的链路利用率水平，即使各条链路的带宽能力有所差异。

思科 PfR 由连接到各个运营商网络的 DMVPN 重叠网络的边界路由器 (BR) 以及用于执行策略的主控制器 (MC) 应用流程组成。BR 收集流量和路径信息，并将其发送到各个站点的 MC。MC 和 BR 可配置在单独的路由器上或与下图所示相同的路由器上。

*图 11 - 思科性能路由：网络枢纽位置*

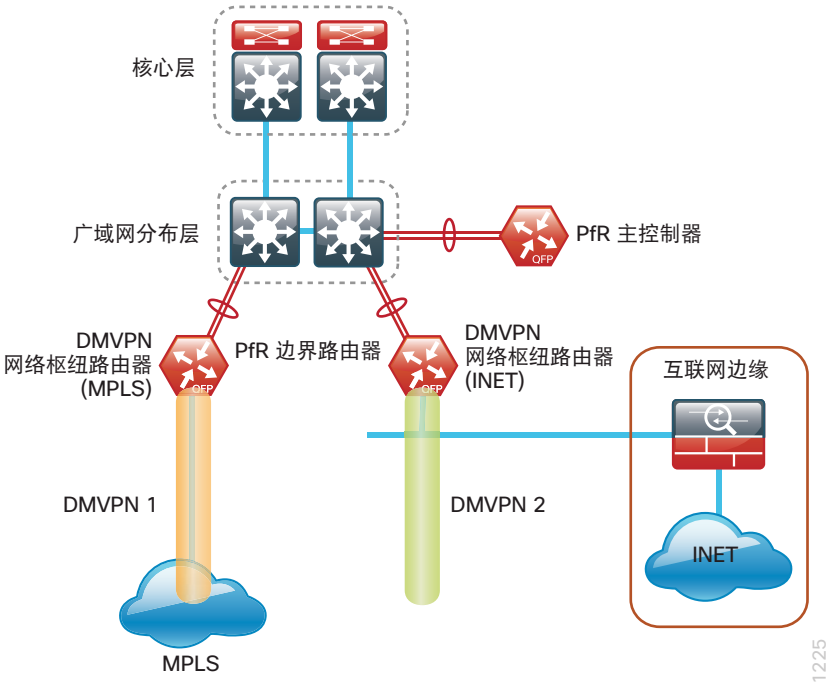
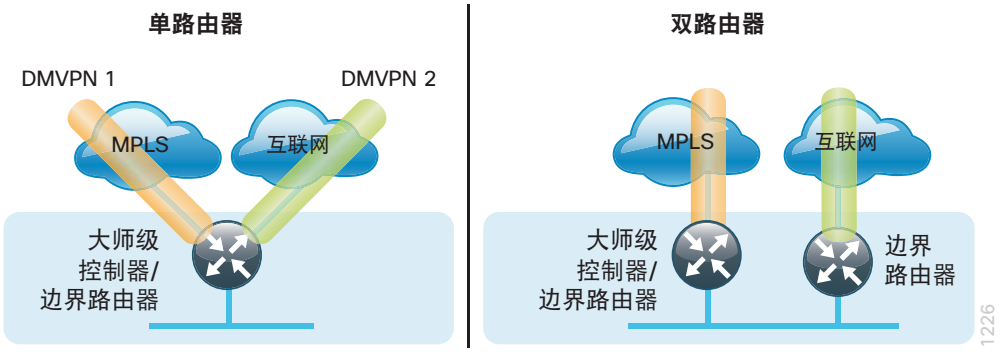


*图 12 - 思科性能路由：远程站点方案*




IWAN 智能路径控制是通过互联网传输提供企业级广域网的关键。

## 获得完整指南

要获得完整的“Cisco Validated Design Guide”（思科验证设计指南），详细了解智能广域网设计以及混合和双互联网广域网的部署详情，请访问 www.cisco.com/go/iwandesignguide


**美洲总部**
Cisco Systems, Inc.
加州圣荷西

**亚太总部**
Cisco Systems (USA) Pte. Ltd.
新加坡

**欧洲总部**
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址、电话和传真。



本手册中所有设计、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，或因交易习惯或贸易惯例而产生的保证。任何情况下，思科或其供应商均不对任何间接性、特殊性、后果性或附带性损害承担责任，包括（但不限于）因使用或未使用这些设计而导致的利润丢包或数据丢包或损坏，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。用户对这些设计的使用负有全部责任。这些设计并不构成思科及其供应商或合作伙伴的技术建议或其他专业建议。用户在采用这些设计之前应询问他们的技术顾问。思科未测试的一些因素可能导致结果有所不同。

本文档中使用的任何 Internet 协议 (IP) 地址都不是有意使用的真实地址。本文档中所含的任何示例、命令显示输出和图形仅供说明之用。说明内容中用到的任何真实 IP 地址都纯属巧合，并非有意使用。

© 2015 Cisco Systems, Inc. 版权所有。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。本文提及的第三方商标均归属其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。