IWAN和PfRv3简介

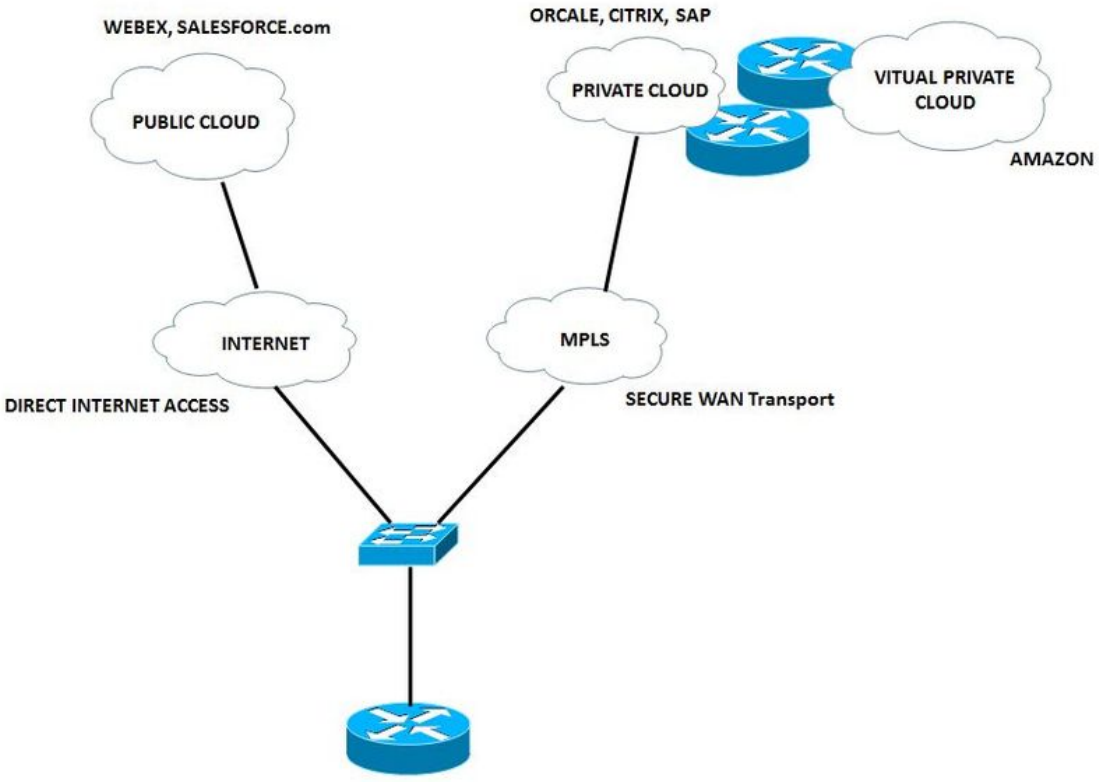
目录

简介

本文档介绍思科智能广域网(IWAN)和思科性能路由(PfR)。

IWAN

思科IWAN是一种增强协作和云应用性能的系统，同时也降低了广域网的运营成本。IWAN解决方案为希望部署独立于传输的广域网的组织提供设计和实施指南，该广域网具有智能路径控制、应用优化以及到互联网和分支机构位置的安全连接，同时降低广域网的运营成本。IWAN充分利用优质广域网和经济高效的互联网服务来增加带宽容量，而不会损害协作或基于云的应用的性能、可靠性或安全性。组织可以使用IWAN来将互联网用作广域网传输，以及直接访问公共云应用。



R1将更希望语音和视频流量采用最佳路径，其可用两条链路中的延迟、抖动和/或丢失相对较少。其他流量进行负载均衡以最大化带宽。

如果当前路径降级(多协议标签交换(MPLS))，然后选择直接互联网接入(DIA)链路，则会重新路由语音和视频。

您可以通过 IWAN：

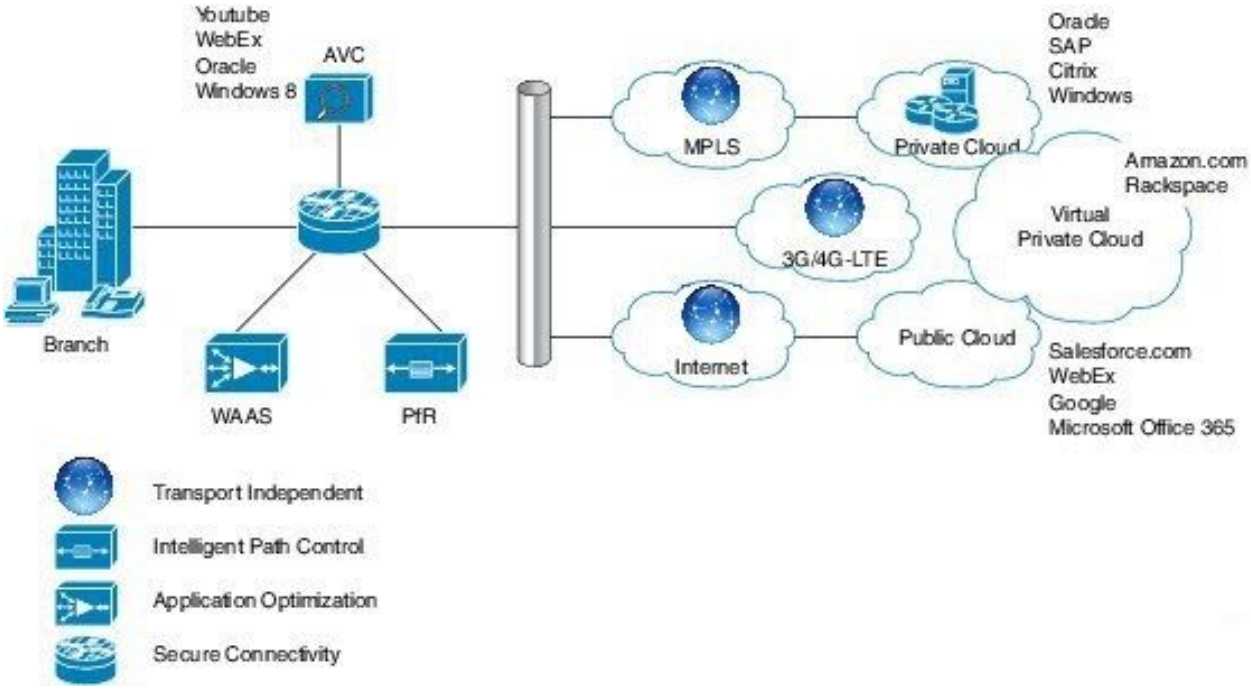
- 以较低成本的INTERNET模式连接，以获取不太重要的数据。
- 允许WAN使用应用优化、智能缓存和高度安全的DIA。

到目前为止，获得具有可预测性能的可靠连接的唯一方法是利用使用MPLS或租用线路服务的专用广域网。但是，基于运营商的MPLS和租用线路服务可能非常昂贵，而且对于组织来说，使用广域网传输来支持对远程站点连接不断增长的带宽需求并非总是具成本效益的。组织在为远程站点充分提供网络传输的同时寻找降低运营预算的方法。

IWAN使组织能够通过任何连接提供不打折扣的体验。借助思科IWAN，IT组织可以通过更便宜的广域网传输选项为分支机构连接提供更多带宽，而不会影响性能、安全性或可靠性。采用 IWAN 解决方案时，可以根据应用的服务级别协议 (SLA)、终端类型和网络条件来动态路由流量，从而提供最佳的质量体验。

借助 IWAN，您可以快速部署带宽密集型应用，例如视频、虚拟桌面基础设施 (VDI) 和访客 Wi-Fi 服务。无论您喜欢哪种传输模式，无论是MPLS、互联网、蜂窝还是混合广域网接入模式，都无关紧要。

此图概述了IWAN解决方案的组件。性能路由是此计划的重要支柱：



IWAN的四个组件是：

- **安全灵活的传输独立设计** — 动态多点VPN(DMVPN)IWAN通过任何运营商服务产品（包括MPLS、宽带和蜂窝3G/4G/LTE）提供轻松多宿主的功能。 技术：DMVPN/IPsec 重叠设计

- **智能路径控制 —** 借助Cisco PfR，此组件可提高应用交付和广域网效率。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 可以帮助业务应用防止广域网性能波动，同时根据应用策略在性能最佳的路径上智能平衡流量负载。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。Cisco PfR包括连接到宽带服务的边界路由器和路由器上Cisco IOS®软件支持的主控制器应用。边界路由器收集

流量和路径信息并将其发送到主控制器，主控制器检测并实施服务策略以匹配应用要求。Cisco PfR可以选择出口广域网路径，以便根据电路成本智能地对流量进行负载均衡，从而降低公司的整体通信费用。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。 技术：PfRPfR 已发展为称为 PfRv3 的主要新版本。

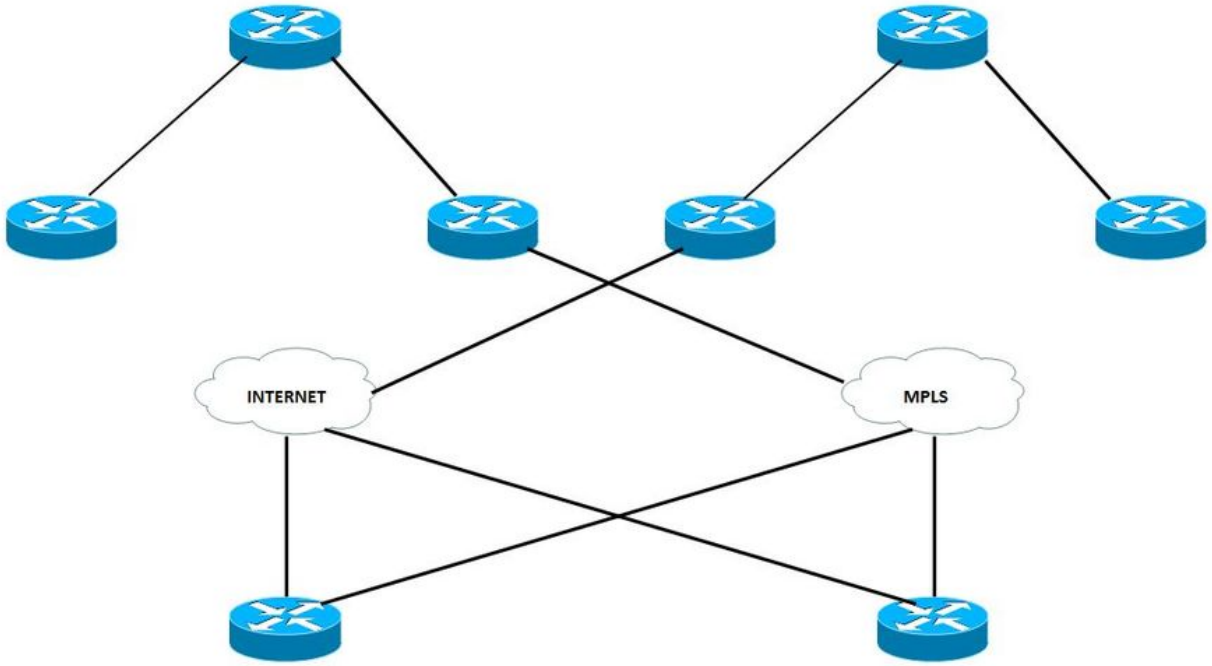
- **应用优化 —** 思科应用可视性与可控性(AVC)和思科广域应用服务(WAAS)可在广域网上提供应用性能可视性和优化。由于 HTTP（端口 80）等公认端口不断重复使用，应用变得越来越不透明，因此应用的静态端口分类已无法满足需求。思科 AVC 提供应用感知，对流量执行深度数据包检测，以确定和监控应用的性能。它通过基于网络的应用识别 2 (NBAR2)、NetFlow、服务质量 (QoS)、性能监控、Medianet 等 AVC 技术提供应用级（第 7 层）可视性与可控性。 技术：应用可视性与可控性 (AVC)、WAAS 和 Akamai Connect

- **安全连接 —** 它可保护WAN并将用户流量直接卸载到Internet。强大的 IPsec 加密、基于区域的防火墙和严格的访问列表都用来保护通过公共互联网的广域网。将分支机构用户直接路由到互联网可提高公共云应用的性能，同时降低通过广域网的流量。思科云网络安全 (CWS) 服务提供基于云的网络代理，以便集中管理并保护访问互联网的用户流量。 技术：思科 IOS 防火墙/IPS、云网络安全 (CWS)

为什么使用DMVPN

IWAN 使用的规范化设计基于 DMVPN，是一种与传输方式无关的混合设计。DMVPN 可以跨 MPLS 和互联网传输部署。这种方法使用包括两种传输方式的单个路由域，显著简化了路由。DMVPN路由器使用支持IP单播以及IP组播和广播流量（包括使用动态路由协议）的隧道接口。在初始的分支到中心隧道处于活动状态后，可以在站点间 IP 流量流需要时创建动态的分支间隧道。

与传输方式无关的设计的基础是每个运营商一个 DMVPN 云。本指南使用两个提供商，一个被视为主(MPLS)，另一个被视为辅助（互联网）。 分支机构站点连接到两个 DMVPN 云，且两个隧道均已建立。



如图所示，每台分支路由器都连接到两个提供商，一个是主MPLS，另一个是辅助INTERNET。

根据流量类型，每个提供商都用于发送流量。例如，优先级较高的数据可以通过MPLS发送出去，优先级较低的数据可以通过互联网路由。这使其更具成本效益，并释放可用资源，以用于更具创新性的业务目的。

传输独立设计（双DMVPN）

设计摘要

本设计提供双活广域网路径，充分利用 DMVPN 提供一致的 IPsec 重叠。MPLS 和互联网连接可以端接到一台路由器上，也可以端接到两台不同路由器上以提供额外的恢复能力。同样的设计可以在MPLS、Internet或3G/4G传输上使用，这使设计独立于传输。

建议每个运营商使用一个 DMVPN 中心 (PfRv3 BR) 并在该中心上传输。这样，路由配置就会简单得多。

DMVPN 需要使用互联网密钥管理协议版本 2 (IKEv2) 保持连接间隔进行失效对等体检测 (DPD)。这对于 DMVPN 中心重新加载时促进快速重新收敛和分支注册功能正常运作至关重要。此设计让分支能够发现加密对等体已发生故障，并且该对等体的 IKEv2 会话已经过期，从而允许创建新的会话。如果没有 DPD，IPsec SA 就必须超时（默认为 60 分钟），并且当路由器无法重新协商新 SA 时发起新的 IKEv2 会话。最长等待时间约为 60 分钟。

DMVPN 阶段摘要

DMVPN有多个阶段，总结如下：

DMVPN 第 1 阶段基于中心与分支功能。

- 中心上的配置更精简且更少
- 支持动态寻址的 CPE (NAT)
- 支持路由协议和组播
- 辐条不需要完整的路由表，可在集线器上总结

DMVPN第2阶段在集线器上没有汇总。

每个分支都有每个分支目的前缀的下一跳（分支地址）。

PfR具有所有信息，可通过动态PBR和正确的下一跳信息来实施路径。

DMVPN 第 3 阶段允许进行路由汇总：

- 执行父路由查找时，只有通往中心的路由可用。
- NHRP 动态安装快捷隧道，并因此填充 RIB/CEF。
- PfR 仍有中心的下一跳信息，但当前无法知悉下一跳更改。

PfRv3支持所有DMVPN阶段。

有关DMVPN的详细信息，请参[阅Cisco IOS DMVPN概述]。