IWAN和PfRv3简介

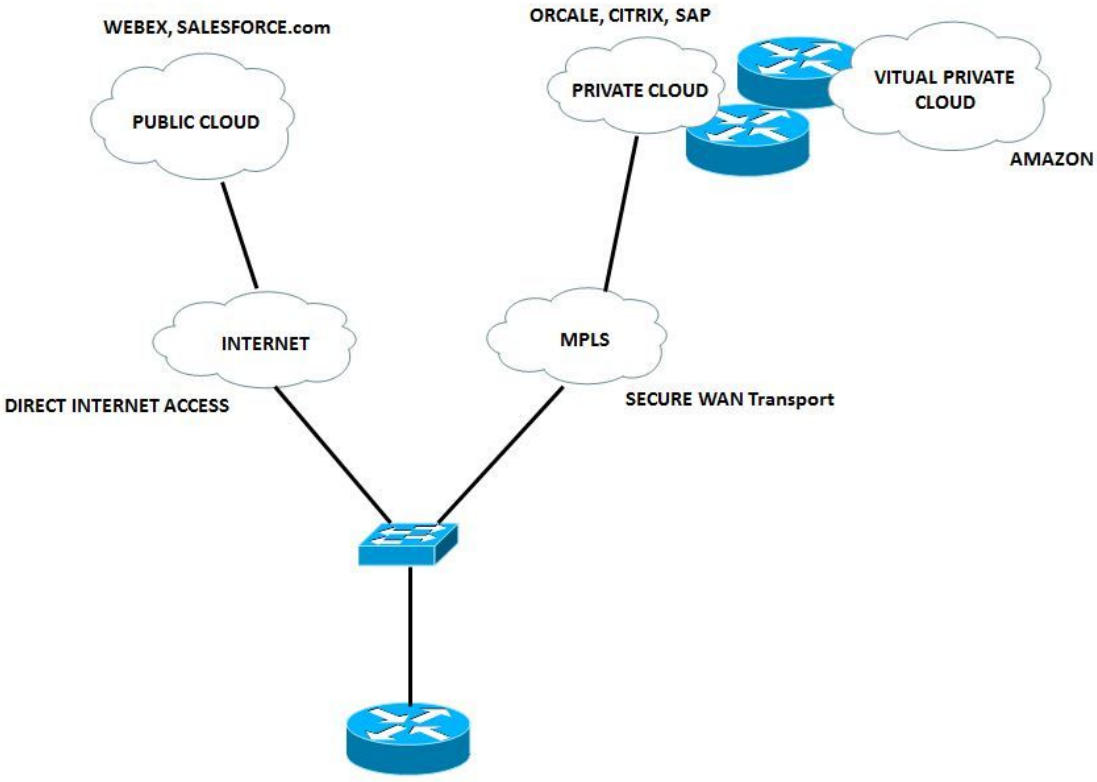
Contents

Introduction

本文描述Cisco智能广域网(IWAN)和Cisco性能路由(PfR)。

IWAN

Cisco IWAN是提高协作和网云应用程序性能的系统，虽然减少广域网的运作成本。查找配置传输与智能路由控制、应用程序最优化和安全连接的独立广域网到互联网和分支机构位置的组织的IWAN解决方案提供设计和实施指导，当减少广域网时的运作成本。IWAN利用高级版广域网和有效网络服务的增加带宽容量，不用在性能、协作或基于网云的应用程序可靠性或者安全的一妥协。组织能使用IWAN为了有效利用互联网作为广域网传输，以及为直接访问到公共网云应用程序。



R1将更喜欢语音和视频数据流相对采取有较少延迟、抖动和损失的最佳路径在可用两条的链路中的它。其他数据流是被均衡的负荷为了最大化带宽。

重路由语音和视频，如果当前路径降低(多协议标签交换(MPLS))直接互联网访问(DIA)链路然后被选择。

IWAN允许您对：

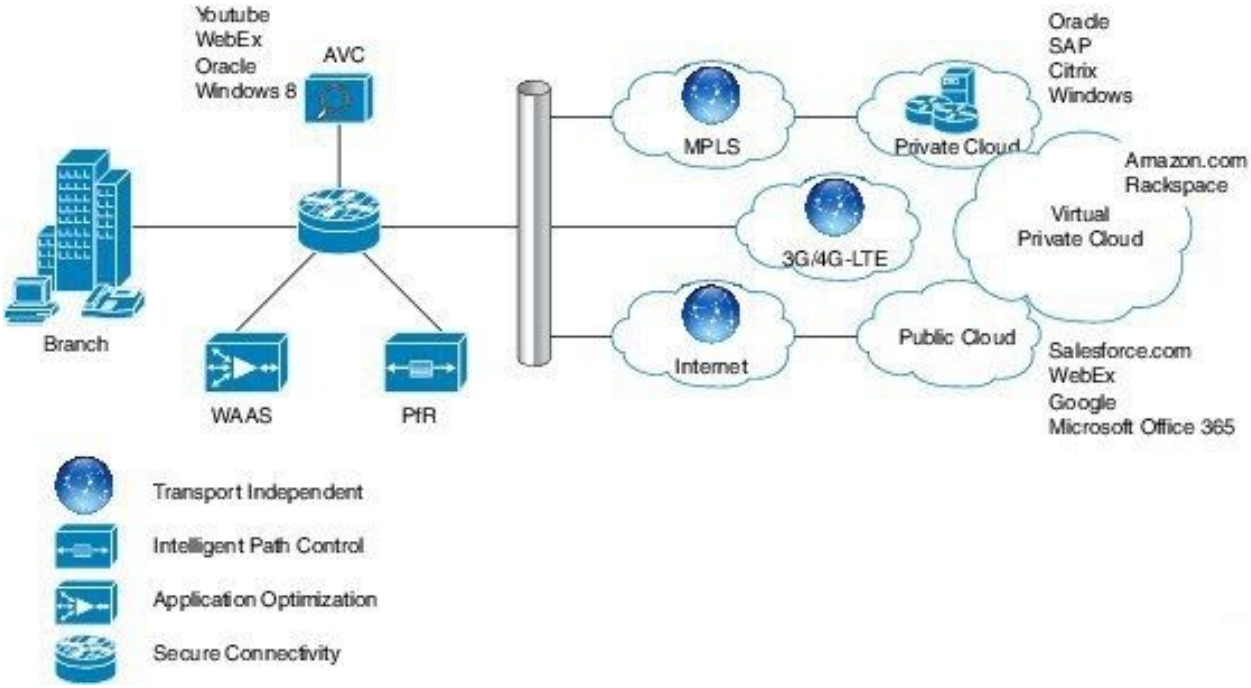
- 连接到一个更加便宜的模式作为较少重的数据的互联网。
- 允许广域网使用应用程序最优化，智能缓存和高度巩固DIA。

到目前为止，确立与可预测的性能的可靠的连通性的唯一方法是利用专用的广域网使用MPLS或一条租用线路服务。然而，舰载的MPLS和租用线路服务可以是消耗大的并且总是不是有效为了组织能使用广域网传输支持远程站点连接的生长带宽需求。组织寻找方式降低他们的营业预算，当足够提供网络传输为远程站点时。

IWAN能提供在所有连接的一个没有暴露的经验的enable (event)组织。使用Cisco IWAN， IT组织能提供更多带宽给他们的与较低花费的广域网传输选项的分支机构连接，无需影响性能、安全或者可靠性。用IWAN解决方案，数据流根据应用程序服务级别协议，终端类型和网络状况动态地被路由提供最佳的质量经验。

使用IWAN，您能迅速转出带宽密集型应用，例如视频、虚拟桌面基础设施(VDI)和客户Wi-Fi服务。并且传输型号您更喜欢，是否MPLS，互联网，蜂窝电话或者一个混合的WAN接入型号的不重要。

此图概述IWAN解决方案的组件。性能路由是此主动性一根关键柱子：



IWAN四个组件是：

- **巩固和灵活的独立传输设计-**动态多点VPN (DMVPN) IWAN为在提供所有的承载业务的容易的多归属提供功能，包括MPLS、宽带和蜂窝电话3G/4G/LTE。 技术：DMVPN/IPsec重叠设计
- **智能路由控制-**使用Cisco PfR，此组件改进应用程序发运和广域网效率。动态PfR控制数据信息包转发决定通过查看应用类型、性能、策略和路径状态。PfR保护商业应用免受动摇的广域网性能，当在根据应用程序策略时的最执行好的路径的智能负载平衡数据流。PfR监控网络性能-抖动，信息包丢失，延迟-并且使决策转送在根据应用程序策略的最执行好的路径的重要应用。Cisco PfR包括连接到宽带业务的边界路由器和在路由器的Cisco IOS软件支持的一个主令控制器应用程序。边界路由器收集数据流和路径信息并且发送它到主令控制器，发现并且强制执行

服务策略匹配应用程序需求。Cisco PfR能选择出口广域网路径智能负载平衡根据电路费用的数据流为了减少公司的整体通信费用。IWAN智能路由控制是键对提供在互联网传输的一企业级广域网。 技术：PfR。PfR演变对称为PfRv3的一主要新版本。

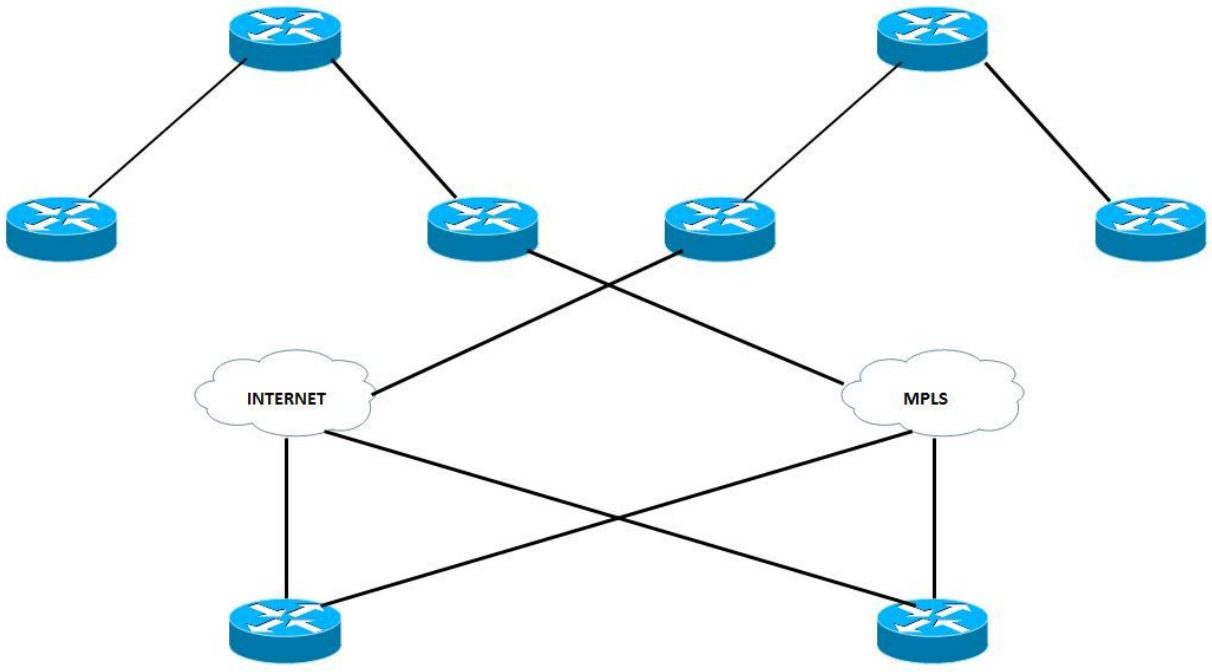
- **应用程序最优化-** Cisco应用公开性和控制(AVC)和Cisco广域应用服务(WAAS)提供应用程序性能公开性和最优化在广域网。当应用程序成为越来越不透明由于增加众所周知的端口重新使用例如HTTP (端口80)，应用程序的静态端口分类不再是满足的。Cisco AVC提供应用程序感知数据流的深度信息包检验识别和监控应用程序性能。公开性和控制在应用级(第7)层通过AVC技术提供例如基于网络的应用程序识别2 (NBAR2)， Netflow，服务质量(QoS)，性能监控，Medianet和更。 技术：应用程序公开性和控制(AVC)， WAAS， Akamai连接

- **安全连接-**它保护广域网并且卸载用户数据流直接地到互联网。严格的IPSec加密、基于区域的防火墙和严格的访问列表用于保护在公共互联网的广域网。路由分组用户直接地对互联网改进公共网云应用程序性能，当减少在广域网时的数据流。Cisco Cloud Web安全(CWS)服务提供一个基于网云的Web代理在中央管理和访问互联网的安全用户数据流。 技术：Cisco IOS Firewall/IPS， Cloud Web安全(CWS)

为什么使用DMVPN

IWAN以根据DMVPN的一个混合的传输独立设计使用一个规定的设计。DMVPN在MPLS和互联网传输间配置。这非常地简化路由通过使用包含两传输的单个路由域。DMVPN路由器使用支持IP单播以及IP组播和广播数据流，包括使用动态路由协议的隧道接口。在最初的spoke-to-hub隧道是活跃的后，创建动态spoke-to-spoke隧道是可能的，当站点到站点IP通信流要求它时。

传输独立设计根据每个供应商一DMVPN网云。在此指南两使用供应商，一个人被认为主要的(MPLS)，并且一个人认为第二(互联网)。分支机构站点被连接到两DMVPN网云，并且两条隧道是UP。



如图表所显示，每个分支机构路由器被连接到两个供应商，一个是主要的MPLS，并且其他是附属

的互联网。

从属于流量类型，其中每一个供应商用于发送数据流。例如，是更加高优先级的数据可以通过MPLS和数据被派出以一点优先级可以在互联网路由。这使更加有效并且释放可用资源可以为更加创新的营业目的使用。

传输独立设计(双重DMVPN)

设计汇总

设计提供利用DMVPN的一致IPsec重叠的主动-主动广域网路径。MPLS和互联网连接在单个路由器在另外的弹性的两个独立路由器可以被终止或者被终止。同一个设计可以在MPLS、互联网或者3G/4G传输使用，使设计独立传输。

推荐使用一台DMVPN在集线器的集线器(PfRv3增殖比)每个供应商和传输。它做路由配置更加容易。

DMVPN为对端死机检测(DPD)要求使用互联网密钥管理协议版本2 (IKEv2)保活间隔，是重要实现快速的再收敛和分支注册的能正常运行，万一DMVPN集线器被重新载入。此设计的enable (event)讲话发现加密对等体发生了故障，并且与该对等体的IKEv2会话是过时的，然后允许新的被创建。没有DPD， IPsec SA必须计时(默认值是60分钟)和，当路由器不能重新协商新的SA时，起动一次新的IKEv2会话。最长等待时间是大约60分钟。

DMVPN阶段汇总

DMVPN有被总结这里的多个阶段：

DMVPN阶段1根据星型网功能。

- 在集线器的被简单化的和更小的配置
- 技术支持动态地寻址CPE (NAT)
- 路由协议和组播的技术支持
- Spoke在集线器不需要充分的路由表，能总结

DMVPN第2阶段没有在集线器的汇总。

每分支有下个跳跃(分支地址)每分支目的地前缀的。

PfR有强制执行所有的信息有动态PBR和正确的下个跳越信息的路径。

DMVPN phase3允许路由概要：

- 当父母路由查找执行，只有路由到集线器是可用的。
- NHRP动态地安装快捷方式隧道并且填充RIB/CEF。
- PfR仍然有集线器下个跳越信息并且对下个跳越更改当前是没有察觉的。

PfRv3支持所有DMVPN阶段。

欲知关于DMVPN的详情，请参阅Cisco IOS DMVPN概述。