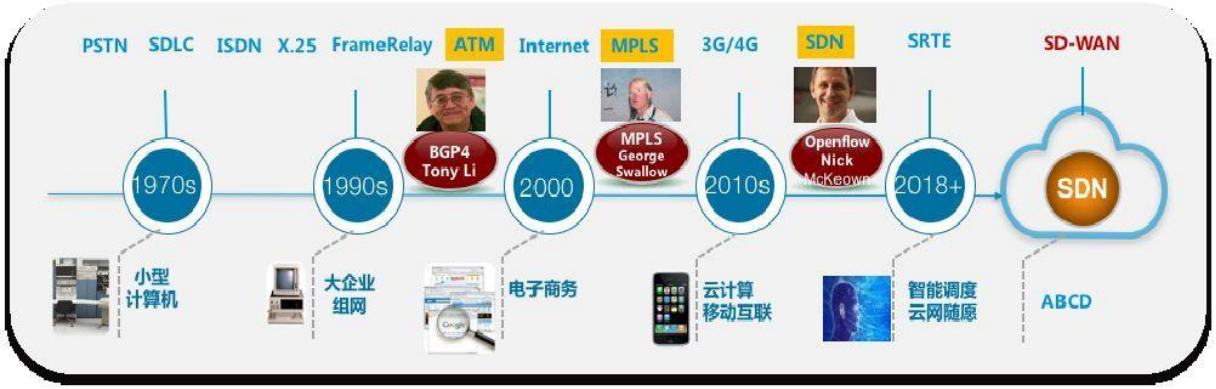
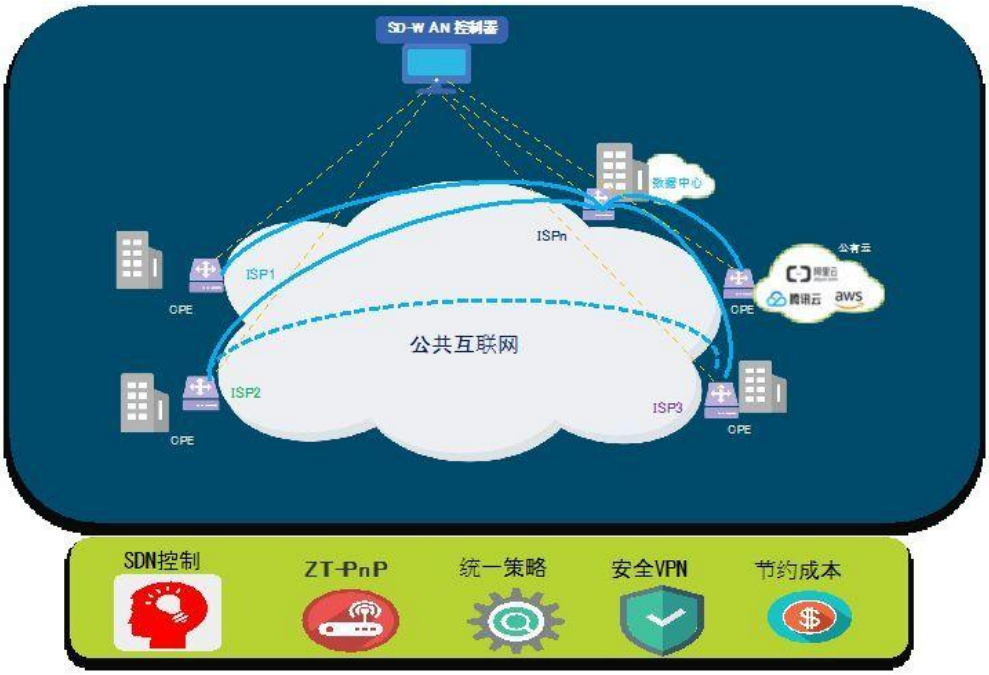
四类 SD-WAN 技术架构解析

2018，客观讲 SD-WAN 技术在中国市场才开始真正起步，曾有人深情而浪漫地把它描述为“当 SDN 遇见 WAN”。 坦率地说，从网络技术发展的历史长河来讲，以前也不是缺乏 SDN 这样的想象力和尝试，早期的 ATM 技术 （MPOA/LANE）就是一个典型尝试，但是有两个致命的问题导致 ATM/MPOA 昙花一现。其中的两个技术原因：一方面是 ATM 信元技术过于复杂导致成本过高 ，另一方面是转发层面过分依赖控制层面导致性能的屏障和可靠性下降。当然我认为另一个原因更关键，是业务应用驱动力不足，当时没有类似今天”云计算和互联网应用”之轰轰烈烈的颠覆性业务 ,导致技术上实现的难度和其可能带来的效益和风险完全不成比例。



回到今天的技术话题，我们对国内外 SD-WAN 的厂商做过粗略统计和分析， 国内 2018 年 20+家发展到到 2022 将近 100+原生技术和产品厂家都在做 SD-WAN，尽管在 2014 年的 ONUG 的会议上定义了 SD-WAN 新术语但事实上由于 SD-WAN 没有一个事实的标准衡量，导致每家的技术差别很大，实现功能千差万别。百花齐放也许是件好事，但为了让大家在谈 SD-WAN 技术架构时能尽量有个一致理解，在报告中我们分析和梳理了市场上主流 SD-WAN 技术和设计思路，将 SD-WAN 技术大致分成四种技术架构：**叠加架构、云端架构、整合架构和原生架构。**

第一类架构：叠加网络结构（On-Prem-Overlay），这是最基本的 SD-WAN 架构，初期 SD-WAN 的典型架构，适合中小企业小规模快速组网。如图所示：



简单介绍一下这种架构：

不论是传统硬件厂商、V**厂商或新型的 SD-WAN 公司，设计一套 SD-WAN 控制器，部署在云端或总部，基于互联网统一管理分支机构的 CPE 设备并组网：

在本地分支机构部署 SD-WAN 的 CPE，云端部署 SD-WAN 控制器，与每个分支机构 CPE 互联，CPE 之间利用互联网和 V**技术实现安全连接。（底层技术有用 GRE+IPSEC，也有用 VLXAN，P2P 隧道技术，UID 区块链技术等等）

满足企业分支基于互联网灵活部署和组网

实现 SDN 控制和统一策略、ZT-PNP 自动部署，即插即用

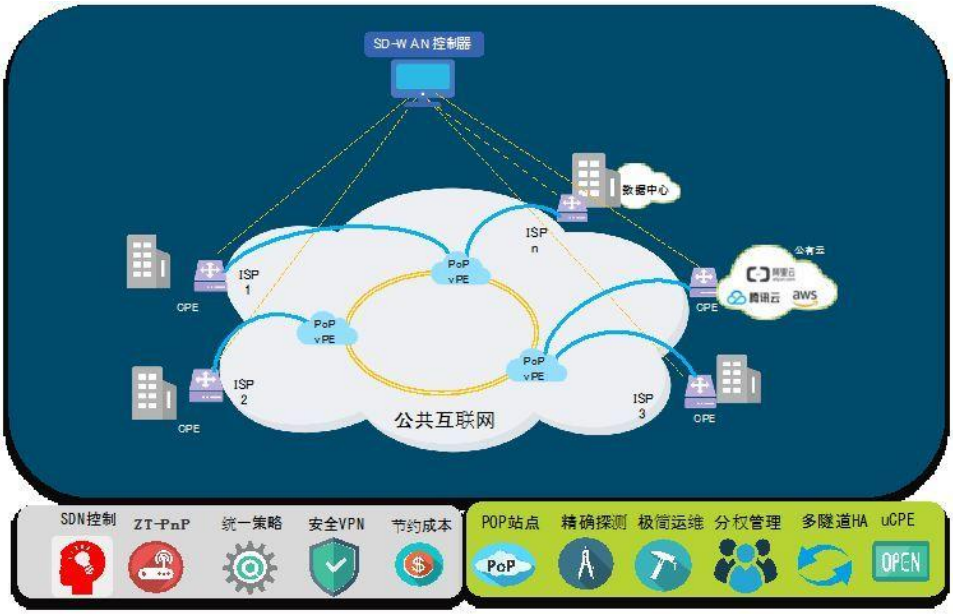
组网模式 推荐 Hub-Spoke 或小规模 Full-Mesh

架构点评：

适合中小规模企业分支机构互联，由于分支机构需要直接建立隧道，不适合大规模扩展，如果客户有 Full-Mesh 的需求，这种架构就是一个灾难。

这种架构主要解决的是自动部署和 V**互联问题。在中国，需要考虑南北运营商互联的瓶颈问题，跨南北运营商互联时网络性能完全不可控。

第二类架构：基于 POP 云端网络架构（On-POP-Overlay 架构），这个是云商和服务商最喜欢的 SD-WAN 架构，也是 SD-WAN 大规模分支部署的推荐架构。如下图所示：



简单介绍一下这种架构：

这种架构利用云端或运营商的 POP 节点来终结 CPE，设计部署时会选择在各地的多个机房部署多线 POP 节点，分支机构需要首先探测和选择最佳的 POP 节点并建立连接。在 POP 中部署 vPE 或网关设备，CPE 与之 POP 节点的建立 V**隧道，在 POP 层解决跨运营商互通提升互联品质， POP 之间构建专线骨干网确保 SD-WAN 远程传输业务品质。

架构点评：

由于采用 POP 思路，大大简化隧道的数量 ，非常适合大规模 SD-WAN 部署

统一策略，极简运维，即插即用

组网模式可以是 Full-Mesh 或 Hub-Spoke

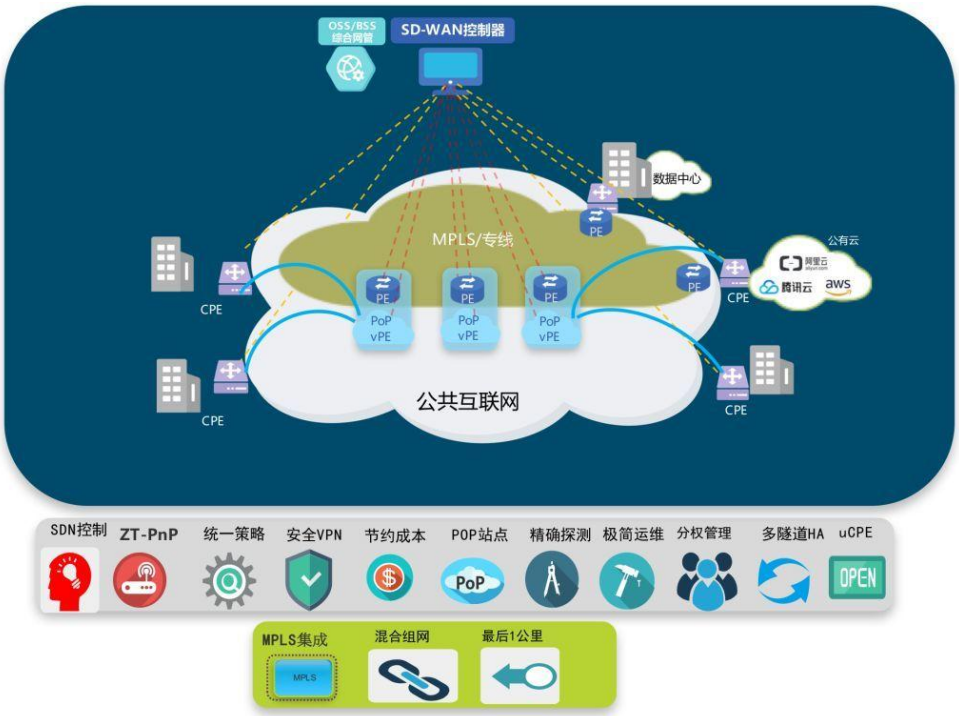
解决南北运营商 Internet 瓶颈的问题，提升基于互联网组网 SLA 服务质量

推荐采用基于 Linux 或 OpenWRT 的 CPE 盒子，通用的 uCPE 不再被厂商锁定。万联物云自主技术可以为合作伙伴提供定制化的 OEM/ODM 边缘 SD-WAN 网关设备和 POP 设备。

在这个架构中，各个厂商还有各自独特的技术特性（以万联物云 SD-WAN 技术为例），增加了几个非常有特色的增强功能：

- POP 动态和精准探测功能： POP 站点的信息由控制器发布，CPE 盒子可以根据各自租户的策略动态选择或者人工指定 POP 站点，另一方面 探测算法可以由系统管理员调整。
- POP 站点的多租户支持：POP 站点支持基于租户的的管理和安全隔离，大大节省资源管理和扩展能力。
- 多隧道机制：任何一个 CPE 可以实时建立两个 V**隧道到不同的 POP 点，这样保证任何一个 POP 点或 Internet 质量出现问题 业务可以无缝切换到另一个隧道。同时所有的 POP 站点都是 Active/Active 和动态流量分担状态。
- 还有一非常有特色的功能分级分权管理，如管理员、服务商、合作伙伴和最终租户等。这样可以发展 SD-WAN 服务生态系统打下一个的基础。

第三类架构：整合网络架构（Integrated SD-WAN 架构），这个是 MPLS 服务商最喜欢的 SD-WAN 架构，也是实践中许多客户需要的混合组网架构。如下图所示：



简单介绍一下这种架构：

各个 POP 节点的 vPE 或 GW 通过与运营商 MPLS 网 PE 直联，通过 OptionA 或 别的方式对接，将 SD-WAN 汇聚上来的流量转发到运营商的 MPLS 骨干网中以确保障其 SLA。在这种架构中，运营商可以把

MPLS V**的 PE 和租户 V**集成到 SD-WAN 系统中，真正实现为客户提供全国范围内集 MPLS V**、IPSEC V**、SD-WAN 等多种应用的 WAN 解决方案。国外将这种能力也称之为“混合架构”能力。这种架构能有效提高网络性能和混合组网能力，特别是各种高服务级别的实时流量，而且可方便实现骨干网与主要云运营商对接。

架构点评：

该架构结构兼顾传统 MPLS 客户情况，真正实现为客户提供全国范围内集 MPLS V**、IPSEC V**、SD-WAN 等多种应用的 WAN 解决方案

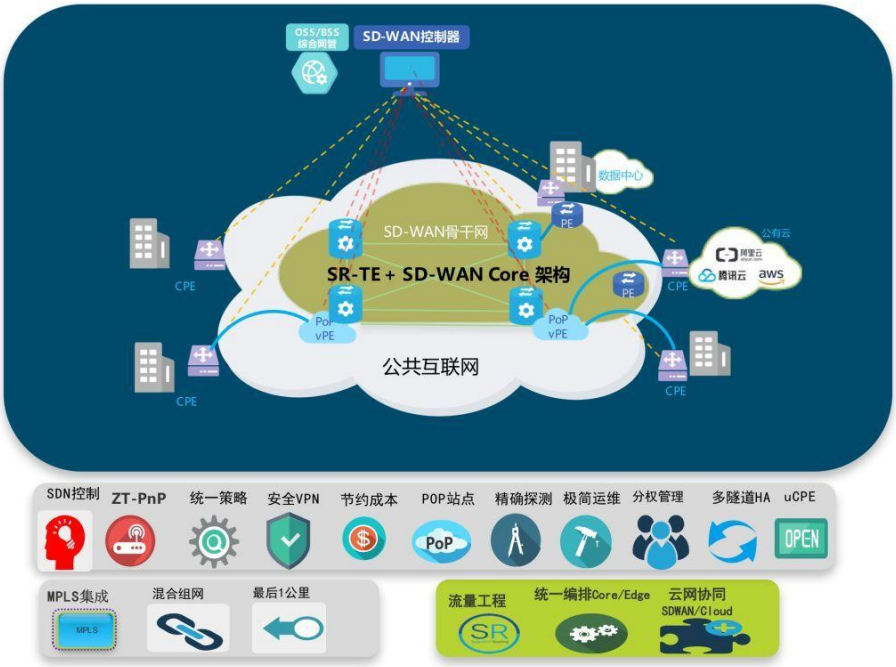
解决运营商最后一公里的难题

由于实现了 MPLS 租户 V**与 SD-WAN 的租户 V**打通，也有称之为“混合架构”能力，非常适合实现骨干网、SD-WAN 与主要云运营商对接，开展云联网业务

这种架构的加强模式：控制器将 MPLS 服务商 PE 节点统一纳管，这样一旦开通 V**业务时可以实现完全的业务自动化。。

第四类架构：原生 SD-WAN 架构 （Native SD-WAN 架构）

这个是运营商和大型的客户端到端 SD-WAN 架构的目标，实现从接入到骨干网的设备 SDN 统一管理，如下图所示：



简单介绍一下这种架构：

在整合架构的理念上，将 SD-WAN Edge、骨干核心网 PE/vPE 节点统一纳管。 骨干核心网络可以基于路由器组网或者基于商用化交换机组网， 很多新一代的服务商更愿意采用通用商用化交换机搭建的原生态 SD-WAN 骨干网。 不管哪种方式，这种架构将各个 POP 节点的 vPE/网关设备与骨干网系统统一纳管实现完美结合，真正实现端到端的流量 SLA 保障。这是一个比较彻底和原生态的端到端 SD-WAN 架构，可以实时监控和调度全网 SD-WAN 流量和业务，可以端到端保障低延迟、低丢包率和低抖动。

简要点评：

适合重构基础网络资源的运营商和大型客户，可以重构新一代骨干网和实现端到端的流量工程，提供高品质广域网业务。

实现从分支接入到云商、企业 DCI 到云商等高效互联，是整合架构的一种增强架构。

这种架构的加强模式：骨干网基于 SRTE 流量工程 实现流量调度和管理： 流量端到端探测、调度管理，真正实现端到端的流量 SLA 保障。

上面谈到几种的 SD-WAN 技术架构，更多从功能实现和扩展能力不同，并不是代表那个架构一定好于那个（每个人可以有各自的技术流派和追求），不同场景客户有不同选择。除此以外，SD-WAN 还需考虑集

成一定传统网络的功能，如路由协议、安全 ACL、防火墙，QOS，流量识别和加速，分级分权管理，互联网线路和专线组网和统一纳管，还有就是基于客户要求开放北向 API 或定制开发。

下面简要谈谈其中路由协议和 API 定制开发这两点。 有人说 SD-WAN 已经统一管理路由策略了，不需要传统路由支持，其实不对，SD-WAN 除了支持 SDN 本身的策略路由，通常还需要支持传统的 OSPF，BGP，VRRP 和静态路由等，这样 SD-WAN 才可以和已有路由设备可以做到互为备份和混合组网。另外北向 API 或定制开发也是大客户比较关心：运营商客户通常需要 SD-WAN 控制器开放北向接口，与现有的 BSS/OSS 业务系统集成和定制 API ;企业客户在建设 SD-WAN 的过程中 ,由于组网方式、应用需求的不同，也会有一些个性化的定制组网需求。

最后一点，也许是最重要的一点，在设计 SD-WAN 技术架构的时候一定要避免重蹈当年的 ATM 技术架构的覆辙，甚至吸取 Openflow 的 SDN 技术架构的失败教训（至少不推荐大规模部署），我们**物云 SD-WAN 叠加网络在规划设计架构的时候，有三个铁定的原则：第一：SD-WAN 控制器不参与转发面；第二 正常运行阶段控制器即使通讯失联业务不受影响；第三 即使控制器断掉转发面设备有自愈能力。** 简单来说就像我们在开车使用 GPS 导航系统，有了它帮我们实现调度和最优路径选择，但当特殊环境 GPS 信号失联，我们可以用本地地图和人的大脑继续行使到达目的地-尽管难以预测后续的交通拥堵。

最后展望一下 SD-WAN 的未来 ,SD-WAN 将 SDN 的概念和架构引入 WAN 是个既浪漫又务实的话题，如同云计算一样，SDN 通过新型的管理和网络计算模式将分布而有限的物理网络抽象为统一而无限的逻辑网络资源以便更加灵活地使用和调度。今天 SD-WAN 的旅程已经开始，SD-WAN 作为一种新的业务模式带来的价值和意义前景不可估量，企业的上云和多云互联发展必将使 SD-WAN 进入一个新高潮，进而颠覆现有的企业网络组网设计理念。未来的 SDN 以及 SD-WAN 如何和人工智能 AI 和大数据结合-提供精准的智能调度能力以及流量与业务智能关联分析也值得关注，同时未来的一段时间 SD-WAN 将与运营商的 MPLS 融合共存，并为企业网络服务市场带来新的生态环境，除此之外未来的 SDN 的开放性、通用标准和互操作（不被厂商锁定）也将是大势所趋，不忘初心，让我们拭目以待