

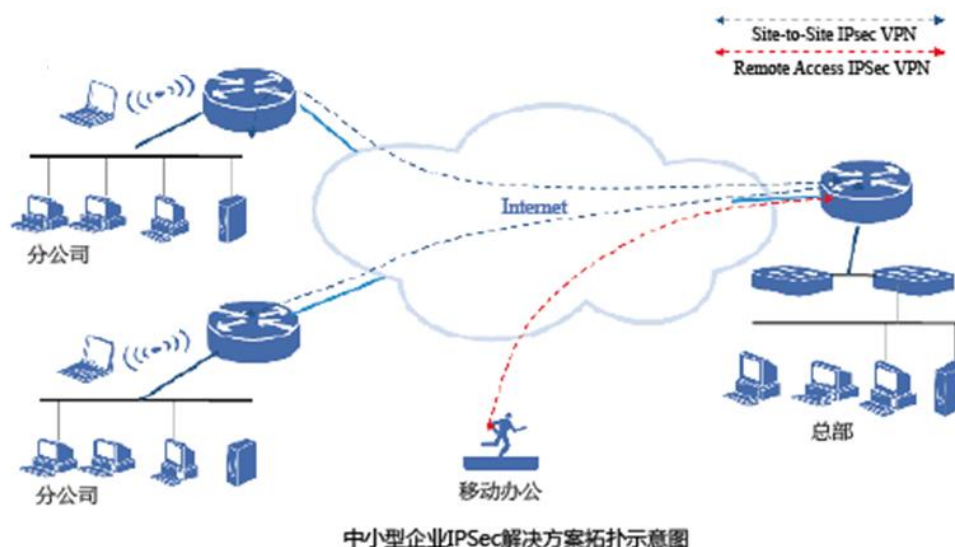
企业面向 LAN 应用和 WAN 设备联网的智能组网——SD-WAN 3.0

随着企业发展壮大，分支的增加不可避免。当分支越来越多，如何进行多分支组网互联就成为了急需解决的问题。

企业多分支的组网，简单来说，就是企业的多个分支通过虚拟专用网络技术，以 Internet 网络为基础，进行私有网络互联。今天咱们就以某制造业企业为例，了解一下多分支组网技术的演进。

传统的 IPsec VPN 组网

某制造业企业发展初期人数较少，分支不多。受限于客观条件，实际采用的是公司总部与分支机构通过点到多点 IPsec VPN 互通，典型组网如下图所示：

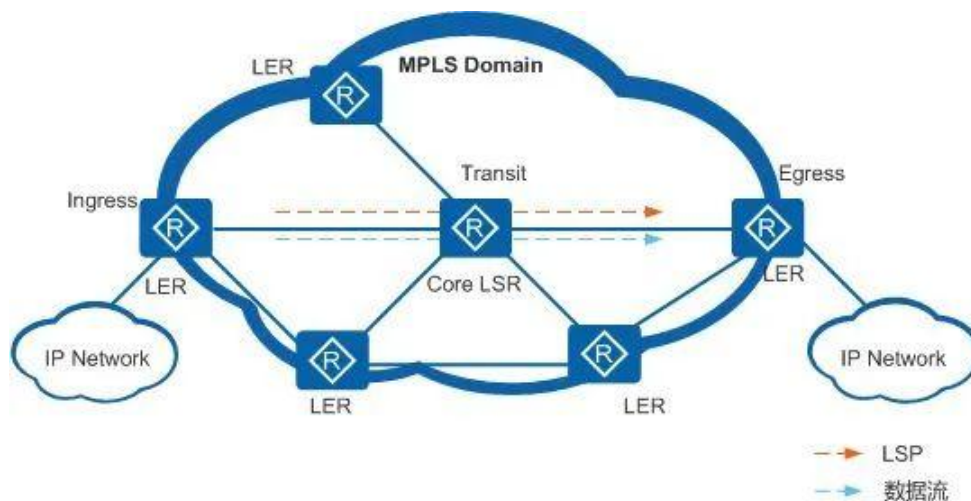


作为上世纪末兴起的 IPsec VPN 技术，它的安全性比较高，但是也存在配置复杂、安装维护困难等缺陷。

当分支较少的时候，还能应付过来，但是分支一旦增多，IPsec VPN 就难以满足需求了。

昂贵的 MPLS VPN 组网

某制造业企业经过发展，公司体量和规模都有较大成长，因此也对网络组网有更高的要求。



此时建构在运营商基础网络之上的 MPLS VPN 似乎是更好的选择。

MPLS 的稳定性较高，接入方便，服务质量更高。但是也存在价格昂贵、开通周期长等缺陷。

SD-WAN 1.0 时代

SD-WAN 1.0 是对传统的 IPsec VPN 组网的延伸，在企业各个站点边缘的 CPE 间建立隧道，企业的组网完全在服务提供商提供的网络之上。

相对于传统 VPN 组网，它带来了几大优势：

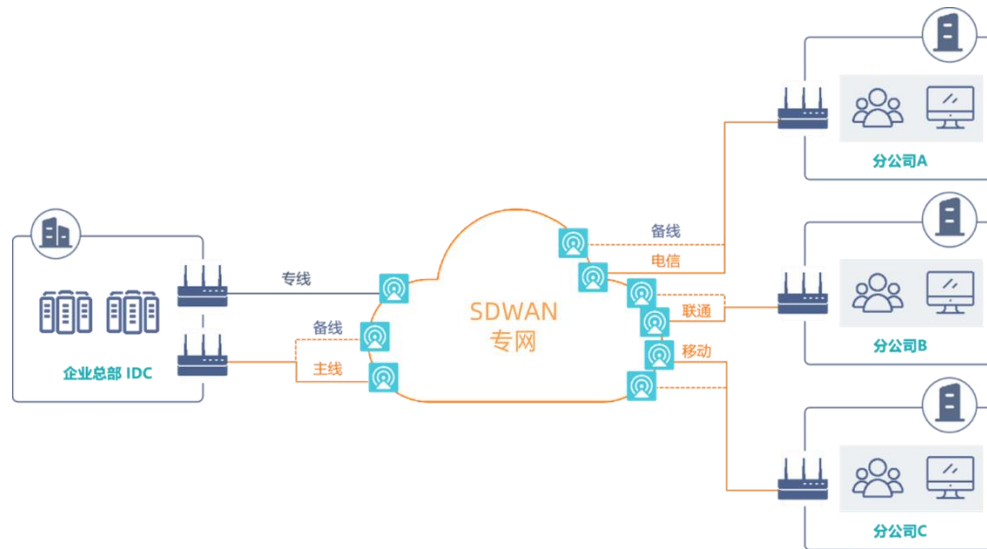
引入了控制器的角色，用于 CPE 的发现与管理，并动态向其下发用于建立隧道的信息，以及组网所需的路由信息，大大地提高了配置效率。

增加了 WAN 链路的监控，优化选路以及链路的故障切换。

上述优势非常明显，但也有明显的不足，所有的链路优化是基于公共网络的，在某些场景下，质量与 MPLS 专线差别明显。因此某制造业企业还在观望。

SD-WAN 2.0 时代

SD-WAN 2.0 的解决思路是，利用已有的网络，集中精力解决最后一公里的接入、优化和管理。具体的实施方案通常是在各个骨干节点建立 POP 点，部署 SD-WAN 网关设备，接入 SD-WAN 专网。



该方案的优势总结如下：

尽可能利用 SD-WAN 专网，提升整体的网络服务质量。

简化了 CPE 之间的隧道建立模式，每个分支节点只需要建立 1 条或 2 条（备份或负载分担）隧道，就能轻松完成 Full-Mesh 组网。

继承了 SD-WAN 1.0 中，控制器对于 CPE 的发现与管理，及隧道与路由策略的动态计算等优势。

继承了 SD-WAN 1.0 中，CPE WAN 链路的监控，优化选路以及链路故障切换等优势。

但该方案也存在明显的不足，就是 POP 点通常只会覆盖一、二线城市，这样，对于某些同城/省组网的时候，其网络质量就不如 SD-WAN 1.0 组网模式。因为同城之间，直接通过公共网络互联，要比经过 POP 点节省了网络路径的开销。

但是相对于传统 IPSec VPN 和 MPLS VPN，SD-WAN2.0 的优势已经非常明显，因此某制造业企业已经考虑采用 SD-WAN 进行多分支组网。

SD-WAN 3.0 时代

万联基于 P2P 协议的对等网络模式提出的 SD-WAN 3.0，继承了 SD-WAN 1.0 和 SD-WAN 2.0 的优势部分，同时解决了两者不足的部分，为企业提供了灵活、最佳的按需组网方式。



该方案的基本思路是，在同省互联，且公共网络的服务质量可以满足的场景下，采用同一运营商城域网下 CPE 与 CPE 之间直接建立隧道的方式，其分支流量不经过 POP 节点。省内直接互访，跨省经过 POP 节点互访，达到了不同场景下的路径最优化。

除此之外，万联网络 SD-WAN 还支持大 2 层组网，传统二层网络能传输的数据万联网络 SD-WAN 都能传输，应用范围更加广泛。

当然某制造业企业并未放弃 MPLS 组网，在一些关键的业务上仍然采用 MPLS 来保障网络质量。在采用了 SD-WAN 3.0 之后，以往大部分网络问题都迎刃而解，极大提升了企业效率。

万联网络专业的企业智能组网产品和方案，致力于为企业提供混合云组网(SD-WAN、MPLS、云互联)，业务云化、数据中心应用 SaaS 化服务延伸、网络接入边界安全服务、行业 IT/CT 一体化解决方案等相关服务，如有相关场景或者疑问的都可以进行咨询。