

# 不断演进的园区

基于 EVPN/VXLAN 的企业网络

## 挑战

传统园区网络太过专有和僵化，无法满足大型企业中的端点需求。这些网络必须足够灵活，才能支持物联网设备，并在园区内部和跨园区的每层提供一致的安全性。

## 解决方案

瞻博网络不断演进的园区解决方案基于“VXLAN 与 EVPN 叠加”控制平面，提供了构建和互连多个园区、数据中心和公有云并且可扩展的高效方法。

## 优势

- 基于控制平面的 L2/L3 信息交换
- 高效的主机移动性
- 非专有解决方案
- 可在所有网络层实现扩展
- 更快速的融合
- 灵活且安全的架构

全球企业网络采用云和基于云的应用程序提升竞争力、降低 IT 成本，并为用户提供随时随地访问资源和数据的权限。这种趋势在很大程度上由广泛使用移动设备、社交媒体和协作工具以及越来越多的物联网 (IoT) 设备推动，显著影响了企业园区网络。日益增多的网络端点以及快速发展的业务需求驱动了对高度可扩展网络的需求。这些网络不仅简单、可扩展且可编程，而且采用园区与数据中心都通用的基于标准的架构构建。

## 挑战

大多数园区网络基于传统 2 层以太网型架构，不需要生成树协议。虽然这些架构在中小型园区中运作良好（服务限于单一网络且满足传统园区需求），但它们太过僵化而无法满足大型企业的可扩展性需求。

基于云的应用程序支持全新业务模式，提供更高的业务敏捷性，且支持采用统一通信、视频及其他延迟敏感型应用程序等关键技术。物联网设备使用范围的广泛增加也意味着人们期望这些相同的网络能够得到快速扩展，而又不增加复杂性和资源。由于许多物联网设备的网络功能有限，因此它们需要建筑物或园区之间的 L2 邻接。传统上，通过使用数据平面泛洪和学习扩展这些区域之间的 VLAN 来解决此问题。但是，这种方法效率低下且难于管理。

安全性不再仅仅是外围问题，它也面临独特的挑战。现代企业希望将安全嵌入到网络架构中 — 不仅仅嵌入在园区内部，而且嵌入在整个组织扩展的分段和策略中，包括数据中心。

## 瞻博网络不断演进的园区解决方案

瞻博网络基于 EVPN/VXLAN 的园区架构使用虚拟可扩展 LAN (VXLAN) 和以太网 VPN (EVPN) 等技术将叠加网络与底层分离。通过让网络管理员在不同的 L3 网络中创建逻辑 L2 网络，满足了现代企业网络的需求。

VXLAN 是一种封装/隧道协议，不会更改以太网协议的泛洪和学习行为，而是使用 MP-BGP 允许网络在控制平面中同时处理 L2 媒体访问控制 (MAC) 和 L3 IP 信息。VXLAN 通过将合并的 MAC 和 IP 信息集用于提供决策来优化路由和交换，而允许 BGP 传输 L2 MAC 和 L3 IP 信息的扩展 EVPN 解决泛洪和学习问题。

基于标准的 EVPN 解决方案在作为园区控制平面协议运行时具有以下优势。

- 更高的网络效率:
  - 使用控制平面 MAC 学习减少未知的单播泛洪
  - 通过在控制平面中启用 MAC 到 IP 绑定来减少地址解析协议 (ARP) 泛洪
  - 通过多个核心交换机 (VXLAN 平均信息量) 支持多路径流量
  - 支持主动/主动双宿主机接入层交换机的多路径流量
- 快速的融合:
  - 在其中一个双宿主接入交换机的链路失败时启用更快速的再融合
  - 在端点移动时支持更快速的再融合
- 可扩展性:
  - 提供可扩展的基于 BGP 的控制平面
  - 允许根据需要无缝扩展核心、分布和接入层
  - 支持随着业务需求的增长无缝扩展园区
- 灵活性:
  - 与 L3 和 L2 VPN 轻松集成
  - 提供允许应用细粒度策略的基于 BGP 的控制平面
- 非专有:
  - 使用基于标准的协议支持多供应商核心、分布和接入层

借助叠加，可以将端点放置在网络中的任何位置且仍然连接到同一逻辑 L2 网络，从而将虚拟拓扑与物理拓扑分离。借助 EVPN 控制平面，企业可以随着自身的发展轻松地增加更多核心、分布和接入层设备 — 无需重新设计网络或执行叉车式升级。

基于 EVPN/VXLAN 的架构可让您跨园区部署一组支持 L2 和 L3 VPN 的通用策略和服务。使用 3 层基于 IP 的底层与 EVPN/VXLAN 叠加，园区网络运营商可以部署比传统 L2 基于以太网的架构更大型的网络。

在不断演进的园区架构（参见图 1）中，核心和分布层构成一个包含 EVPN/VXLAN 叠加的 L3 结构。理想情况下，底层通过使用具有核心和分布交换机的 L3 Clos 模式部署，接入层交换机多宿主到分布层。

Clos 模式提供的架构可启用核心、分布和接入层的确定性延迟和横向扩展。您可以使用 OSPF 之类的内部网关协议 (IGP) 作为底层，或使用外部 BGP (EBGP) 作为底层路由协议。此解决方案将内部 BGP (IBGP) 叠加设计与路由反射配合使用，其中给定性能优化型数据中心 (POD) 内的分布设备将端点信息上游作为 EVPN 路由分享给作为路由反射器的核心设备。核心设备再将路由下游反射给其他分布设备。通过使用路由反射器，无需全网状 BGP 连接，且可利用所有分布层交换机中的一致配置简化分布层的配置。

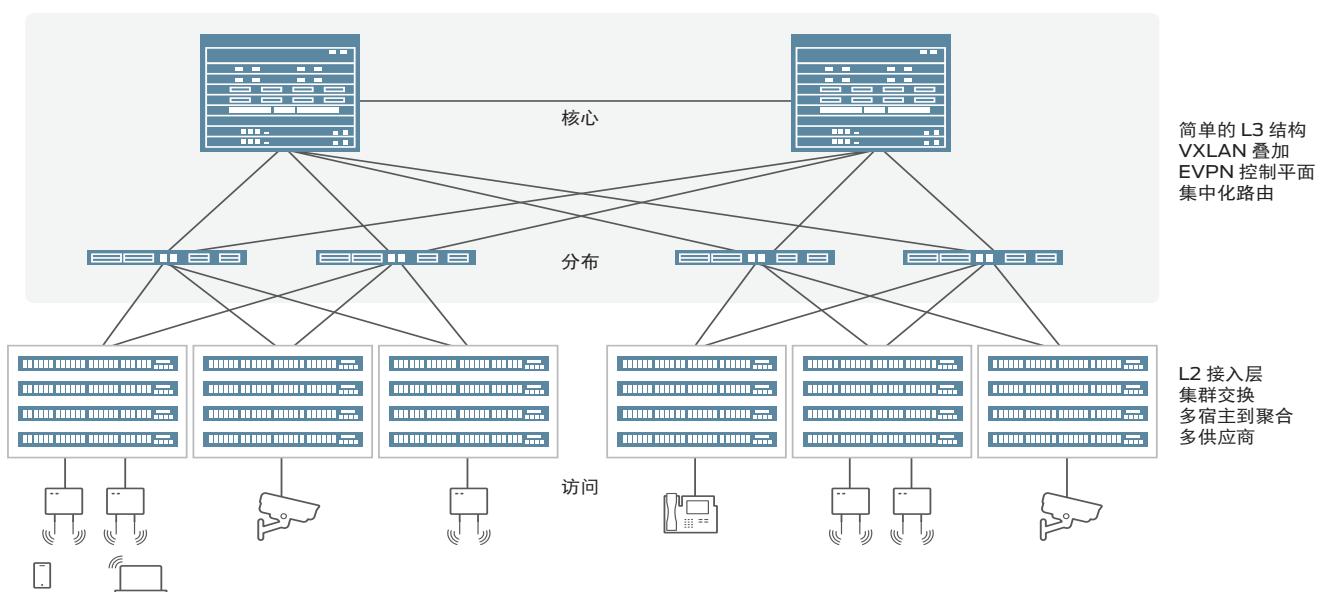


图 1：不断演进的园区高级架构

接入层交换机不属于 EVPN/VXLAN 交换矩阵，接入层交换机通常部署在集群交换配置中，此配置最多允许 10 个互连平台作为单个逻辑设备运行。这个仅为 L2 的接入层会将端点映射到 VLAN，使用从接入层到分布层的多宿主上行链路在中继端口（直到分布层）中承载 VLAN。此解决方案与供应商无关，允许企业使用现有的接入层基础架构并升级到瞻博网络或任何其他供应商的接入层交换机。

VLAN 会映射到分布层的 VXLAN，而用于 VXLAN 的 L3 集成式路由和桥接 (IRB) 或交换机虚拟接口 (SVI) 位于具有任播网关地址的核心交换机上。灵活且安全的配置选项意味着可以将 IRB 放置在通用路由实例中，或在需要分段时放在单独的路由实例中。路由实例与虚拟路由和转发 (VRF) 类似，可根据多租户和/或安全性将网络分段。根据企业安全策略，在 VRF 间通信的路由实例之间可能会泄露一些路由，也可能通过实施高级安全防火墙和网络分段强制 VRF 间流量。

与其他瞻博网络架构一样，不断演进的园区架构不会强制客户投资新设备；用于其他瞻博网络架构的相同设备可以用于不断演进的园区部署，如下所示。

- 核心层：
  - EX9204/EX9208/EX9214 以太网交换机
  - EX9251/EX9253 以太网交换机
- 分布层：
  - EX4600 以太网交换机
  - QFX5110 交换机
- 接入层：
  - EX4300/EX3400/EX2300 以太网交换机
  - EX4200/EX3300/EX2200 以太网交换机
  - 集群交换技术
  - 非瞻博网络接入层交换机

基于 EVPN/VXLAN 的交换矩阵的优势可以扩展至 EVPN 中支持 L2 和 L3 VPN 的各个园区、数据中心和公有云基础架构（参见图 2）。只要园区、数据中心和公有云基础架构具有 IP 连接，VXLAN 就与 WAN 底层无关。可以通过各种 WAN 技术（包括互联网上的私有 MPLS 和 Ipsec）部署 EVPN/VXLAN 叠加。

## 总结 — 企业必须接纳 EVPN 和 VXLAN

基于云的资源日益成为企业 IT 策略的很大一部分。这需要可支持基于云的服务而不影响安全或性能的网络架构。传统网络架构越来越难于满足园区用户对随时随地访问和快速响应的需求。园区网络中日益盛行的物联网设备要求网络灵活，且仍然可以保持架构可扩展、简单、可编程、开放并支持多供应商设备。

瞻博网络的不断演进的园区解决方案基于“VXLAN 与 EVPN 叠加”控制平面，是构建和互连多个园区、数据中心和公有云的高效、可扩展方式。瞻博网络在所有平台上实施强大的 BGP/EVPN（QFX 系列交换机、EX 系列交换机），因此具有得天独厚的优势，通过在当今不断演进的园区和数据中心内部及之间提供经过优化且符合标准的 L2 和 L3 无缝连接，将 EVPN 技术发挥到极致。

## 后续举措

有关更多信息，请联系您的瞻博网络销售代表，或访问 [www.juniper.net](http://www.juniper.net)。

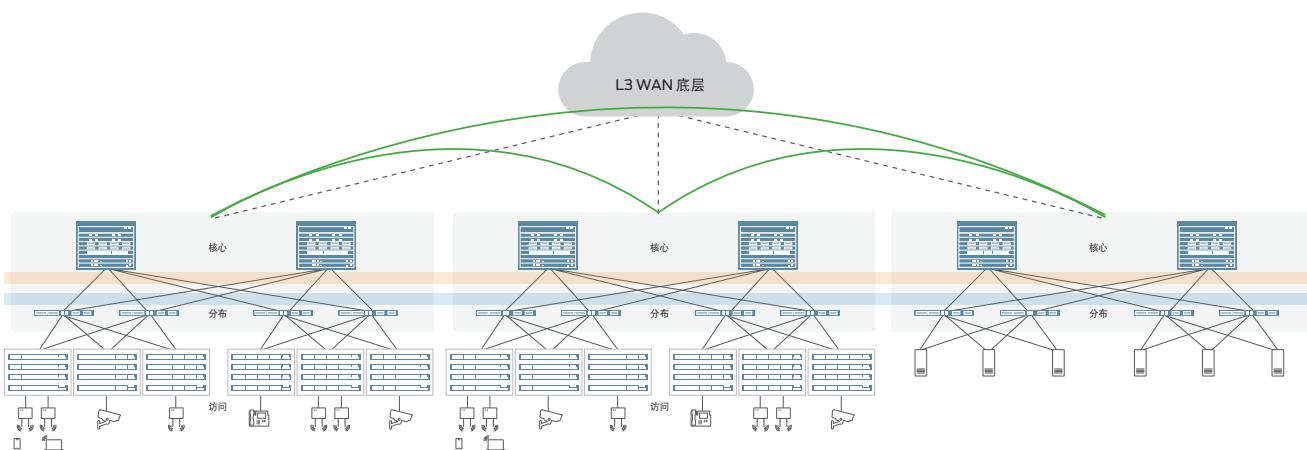


图 2：借助 EVPN/VXLAN 叠加互连多个园区和数据中心

## 关于瞻博网络

瞻博网络将简单性融入到了全球互联的产品、解决方案和服务当中。通过工程创新，我们消除了云时代网络的限制和复杂性，以解决客户和合作伙伴日常工作中面临的最严峻挑战。瞻博网络相信，网络是共享知识和人类进步的资源，而这些能够彻底改变世界。我们致力于想象开创性的方式，来提供自动化、可扩展和安全的网络，并且能随着业务发展的速度而发展。

公司和销售总部  
Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, CA 94089 USA  
电话: 888.JUNIPER (888.586.4737)  
或 +1.408.745.2000  
传真: +1.408.745.2100  
[www.juniper.net](http://www.juniper.net)

APAC 和 EMEA 总部  
Juniper Networks International B.V.  
Boeing Avenue 240  
1119 PZ Schiphol-Rijk  
Amsterdam, The Netherlands  
电话: +31.0.207.125.700  
传真: +31.0.207.125.701

版权所有 2018 Juniper Networks, Inc. 保留所有权利。瞻博网络、瞻博网络徽标、瞻博和 Junos 是 Juniper Networks, Inc. 在美国和其他国家/地区的注册商标。所有其他商标、服务标识、注册商标或注册服务标识均为其各自所有者的资产。瞻博网络对本文档中的任何不准确之处不承担任何责任。瞻博网络保留对本出版物进行变更、修改、转换或以其他方式修订的权利，恕不另行通知。

