# 思科业务就绪园区解决方案

## 思科园区虚拟专用网解决方案

企业的不断扩张引发了对于前所未有的网络灵活性和安全性的要求。怎样在不中断现有基础设施的情况下满足这些要求？

## 今天的企业园区网络

从以太网交换面世以来，园区 LAN 的设计已经经历了巨大的发展变化。很多技术改进和丰富的实际经验共同构建了今天的网络设计理念。

随着园区 LAN 的扩建，企业迫切需要对网络进行划分——按照用户、地点或者职能。最初，虚拟 LAN（VLAN）和生成树协议为将 LAN 划分为多个虚拟网络提供了一种有效的机制，可以满足企业对于划分多个使用共同基础设施的群组的需求。但是，这个解决方案很难扩展。

随着能够执行路由任务的多层交换机的出现，可扩展性和可用性变成了比将网络划分为多个虚拟实体更加重要的设计标准。因此，今天的园区 LAN 是一个汇集了交换式和路由式平台的服务的网络，可以实现最佳的模块性、可扩展性和高可用性。

以前的园区设计方案都没有为区分网络中的流量提供一种便捷的方法，因而无法为园区中的封闭用户群组提供一个安全的、独立的环境。

思科园区虚拟专用网（VPN）解决方案一方面保留了当今园区设计的优点，另一方面又通过在现有的 LAN 上叠加 VPN 机制，添加了将网络划分为多个安全虚拟网络的功能和优势。与此同时，这个解决方案还解决了分布式地部署服务和安全策略的问题。通过集中管理共享服务和应用安全策略，可以大幅度地降低维护园区的不同群组共享的安全策略和服务所需要的资本和运营开支。

## 挑战

在所有企业中都存在拥有不同需求的用户群组。这些群组之间的很多差异都转变成了不同的网络需求。在有些企业中，不同群组的需求只是略微有所不同。但是在其他一些企业中，这些需求的差异如此之大，以至于不同的群组需要被 IT 视为完全不同的客户。在区别对待不同群组时，IT 部门需要：

- 在群组之间确保完全的保密性
- 为每个群组提供独立的路由域和地址空间
- 为每个群组部署不同的计费机制
- 为每个群组执行不同的安全策略
- 有效地管理和扩展所有上述能力

保持这些群组的独立性和安全性是 IT 部门面临的一个艰巨的挑战，尤其是伴随着无线网络和用户移动的出现。

设想一下不同企业的不同网络需求。一个极端是这样一些企业：尽管他们希望划分用户群组，但是这并不是他们的首要任务。这种企业的流量划分问题看起来可以方便地通过选择适当的布线和防火墙位置解决。例如，这些公司可能希望来宾只能从特定区域（包括大厅或者来宾会议室）访问网络，以便利用防火墙将他们与网络其他部分隔开。这种做法可以有效地区分来宾和员工。但是，在需要将用户进一步区分为来宾、承包商、工程师、管理层、薪酬人员时，这种区别方式就会变得有些复

杂。在遇到这种情况时，防火墙的物理位置就无法以可扩展的方式解决这个问题。

另外一个极端是一些拥有很多用户群组的企业。机场和大学都是这种机构的典型例子，它们在一个共同的园区 LAN 中有很多不同的（常常是互相竞争的）客户。

机场（与其他企业一样）在他们的 LAN 上开展所有的内部业务。所有这些业务——包括行李领取、安全、空中客流控制、地面客流控制、维护、财务等——都需要访问 LAN。另外，机场还为每家使用该机场的航空公司建立了单独的物理网络。设想一下为每家航空公司建立的全网状连接的光纤网络。这不仅非常昂贵，而且很难维护。另外，如果需要在机场内部转移某个航空公司的位置，这种方式提供的灵活性极为有限。但是，全球大多数机场都采用了这种方式。使用这种独立网络的目的是保护每家航空公司的私密和安全。在这些网络中，光纤只铺设到特定的地点，因此机场的某些特定区域只供固定的航空公司使用。

同样，大学也拥有很多需要保持独立的设施。他们还拥有大量由私人资金赞助的研究小组。在很多情况下，资助机构要求项目网络必须与学校网络的其他部分隔离，但是仍然可以访问大学的所有网络资源。如果大学必须部署多个包含专用防火墙和路由设备的独立物理网络，无疑需要投入大量的资金。

园区 VPN 可以为企业节约大量资本和运营开支的另外一个例子是商务中心。商务中心需要在一个物理区域——相当于一个园区——中为不同的公司提供办公空间。这些公司向商务中心租用物理空间，以及网络基础设施和语音、视频、监控和寻呼服务。在某些情况下，他们甚至还可以租用服务器群。

由于数据中心前端需要足够的智能，所以为每个客户部署一个专用数据中心可能会非常昂贵。很多客户可能只需要一个服务器群，这使得为每个客户部署一个专用数据中心变得更加没有必要。

### 传统的划分机制

过去，可以用于划分园区 LAN 的机制包括 VLAN 和分布式访问控制列表（ACL）。这两种解决方案都存在自己的可扩展性限制和管理问题。它们只能实现有限的划分，而且不能为不同的内部客户提供完全私有的、独立的网络。

### 使用 VLAN

对于一个很小的园区，IT 可能愿意为其建立一个相对较大的生成树域。在这种情况下，VLAN 可以实现端到端的跨越，而且用户群组可以直接与 VLAN 关联，以实现隔离。但是，实践证明，这种解决方案在达到一定范围之后就将很难扩展。

端到端 VLAN 不能有效扩展的主要原因是它们需要依靠生成树协议避免出现拓扑环路。生成树协议所基于的原则是：跟踪整个网络的拓扑从而建立单个树。如果发生故障或者拓扑发生变化，生成树协议就需要将这种变化反映到整个网络之中。因此，这会产生与网络规模成比例的收敛延时。如果超出一定的网络规模，所产生的延时可能会让人无法接受。

端到端 VLAN 不能扩展的另外一个原因是单个广播域（VLAN）的创建会不可避免地形成一个统一的故障域。换句话说，VLAN 中发生的单个故障会影响整个 VLAN。当 VLAN 为端到端跨越时，就无法控制故障的影响范围，因而会波及整个网络。

生成树协议的诊断和管理需要全面的文档和深入的网络知识。当 STP 只限于网络的一小部分（例如一个配线间）时，这是一个可以实现的目标。但是，如果将生成树域扩展到一个大型网络，它就会变得非常难以维护和诊断。

### 使用 ACL

对于一个需要用现有的 ACL 机制保护供某个特定群组使用的网络资源的 IT 部门，群组用户必须位于特定的子网中，因而与明确的网络设备关联。如果满足这些条件（即用户不具备移动性），那么网络管理员的任务就是在适当的网络设备上添加适当的 ACL。但是，如果您将这种方式扩展到多个用户群组，结果就是会有数量难以控制的 ACL 散布在整个园区中。

随着用户在园区中的移动性的增强，这种方式的可扩展性问题变得更加明显。因为 ACL 需要依靠地址识别用户，所以必须要在整个园区中为每个群组创建子网，再在每个分布层交换机为每个群组创建不同的 ACL。为每个群组创建一个子网并不是问题，因为路由协议可以做到有效的扩展，但是为了保护群组安全而对 ACL 进行的部署和维护工作可能会非常费时。

利用 ACL 划分用户群组不仅相当繁琐，而且不能提供用户群组所需得的自治能力。某些用户群组可能需要选择他们自己的 IP 寻址机制（可能会与网络中的其他网络重叠）。另外一些用户群组可能需要在他们自己的专用防火墙上控制他们的安全策略。与此同时，企业可能需要在每个 VPN 的基础上，根据它的业务模式部署计费和记帐机制，还可能需要能够在不同的 VPN 之间共享集中资源（例如防火墙设备、服务器群集、WAN 和互联网接入）。

### 正确的解决方案

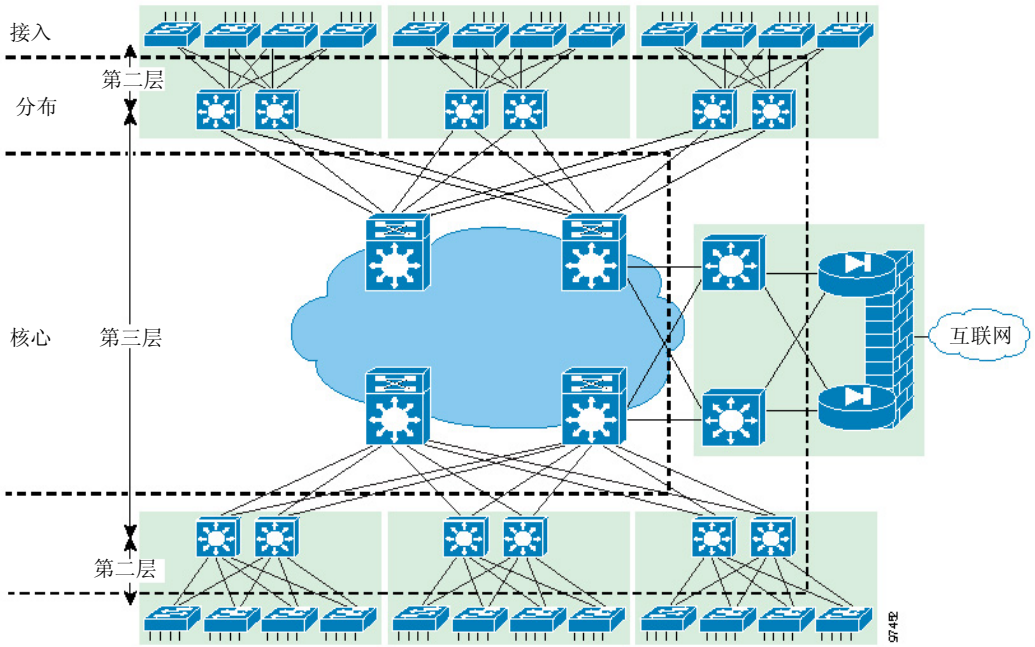
要保持用户群组的完全独立和集中管理服务、安全策略，以及保存现有园区设计的高可用性和可扩展性，需要使用一个可扩展的解决方案。这样的解决方案可以通过在园区 LAN 的路由式基础设施上建立基于多协议标签交换（MPLS）的第三层 VPN 实现。

## 思科园区 VPN 解决方案

典型的园区网络设计会在网络边缘（接入层）使用多种交换技术（第二层），在网络核心（分布层和核心层）使用路由技术（第三层）。因此，可以在网络接入层利用 VLAN 实现网络划分，并在网络核心（第三层）利用基于 MPLS 的第三层 VPN 划分路由域，从而实现可扩展的端到端网络划分。

本文假定已经存在一个可扩展的网络设计——包括一个路由式园区核心和分布层（如图 1 所示）。

**图 1**
可扩展园区设计

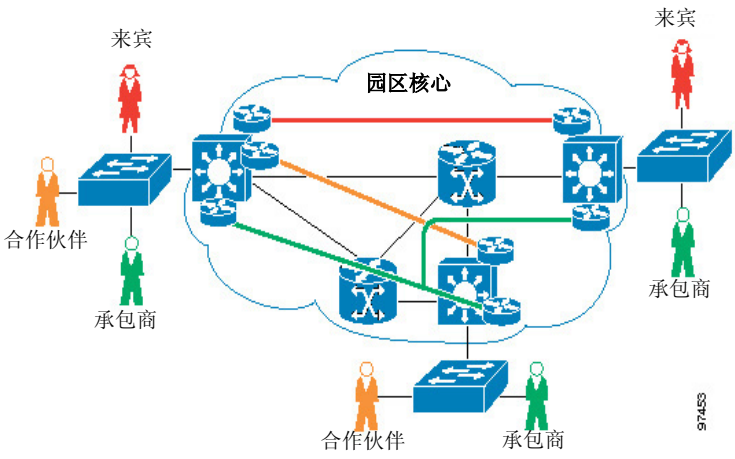



作为现有园区设计的一部分，VLAN 部署在网络边缘。它可以映射到重叠于园区的路由部分之上的第三层 VPN。通过这种方式，既可以保留层次化园区部署的所有优点，又可以在园区 LAN 中实现端到端的、可扩展的网络划分和集中管理的安全和服务。

每个 VPN 都在每个路由器上具有自己的路由表和路由进程，所有流量都在根据 MPLS 或者 802.1Q 标签进行转发时保持独立。该解决方案可以被视为多个独立的物理网络的重叠。但是，每个网络都是一个 VPN，而不是一个物理网络。

图 2 显示了独立的虚拟网络如何重叠到现有的园区 LAN 上，为合作伙伴、承包商和来宾提供独立的 VPN。

**图 2**
利用 VPN 划分网络



每个 VPN 都在端接 VPN 隧道的交换机上拥有一个独立的虚拟路由进程。它被称为虚拟路由转发（VRF）。值得注意的是上图中的承包商 VPN，它显示了 BGP/MPLS VPN 的任意－任意连接特性。必须牢记的是，这些隧道并不是点对点线路，而是可以提供任意－任意连接的点对群体连接。这种点对群体方式可以克服其他点对点 VPN 机制所共有的辐射形拓扑的复杂性问题。

还记得机场所面临的挑战吗？利用思科园区 VPN 解决方案，所有航空公司的流量都可以通过一个机场园区 LAN 进行安全的传输－－不仅提供航空公司所需要的隐私和安全性，而且让航空公司可以灵活地、毫不费力地将他们的业务转移到机场中的任何候机室。

这可以显著地降低机场的成本。物理布线将得到大幅度简化，而机场现在可以灵活地让任何航空公司使用任何登机口，从而缩短资源的闲置时间并提高生产率－－同时最大限度地降低运营成本。

至于大学，利用思科园区 VPN 解决方案，不同的研究小组和教师们可以被分配到共享式园区基础设施上的不同 VPN。这使得不同的研究小组可以在互相隔离的网络中开展工作。另外，思科园区 VPN 解决方案还可以让 VPN 在某个可选的中央地点端接，即进出 VPN 的通信可以由单个防火墙设备控制。该设备可以为每个 VPN 提供功能齐全的、彼此独立的虚拟防火墙。

这可以为大学带来很多好处－－从降低基础设施成本、加强可扩展性到提高可管理性。

利用思科园区 VPN 解决方案，商务中心可以在使用共享式基础设施的同时，确保保每个客户的私密性和安全性。在这种情况下，共享式基础设施不仅包括线缆、路由器、交换机和网络设备（例如防火墙），还包括可以通过园区 VPN 划分的服务区群集，从而让企业可以利用一个统一划分的数据中心为多个内部客户提供服务。这种方式可以利用和共享现有的数据中心设备，例如 SSL 端接引擎和负载平衡器。

## 为企业带来的好处

思科园区 VPN 解决方案的很多优势来自于网络划分和服务集中。

### 将园区 LAN 划分为 VPN

这些网络是完全独立的，使用自己的寻址机制和策略。利用第三层 VPN 机制划分 LAN 的优势包括：

- 私密性保护
- 子网透明度
- 用户移动性
- 针对每个 VPN 执行流量策略（监管、整形）
- 针对每个 VPN 进行计费

### 服务的集中化

服务的集中化可以大幅度简化和加强安全策略的实施。通过为每个 VPN 提供单个接入点，集中的防火墙和入侵检测设备可以由多个 VPN 共享。不同 VPN 都需要使用的其他一些服务也可以共享，从而显著降低提供这些服务的资本和运营开支。

可以集中化的服务包括：

- 安全策略执行（ACL 和防火墙通道）
- 流量监控、记帐和计费
- 共享的互联网和 WAN 接入
- 共享的数据中心
- 地点集成

## 私密性保护

通过将园区分为多个独立的 VPN，每个群组可以保护自己的私密性。第三层 VPN 解决方案可以为每个 VPN 建立独立的路由域。因此，不同群组的路由控制信息是彼此隔离的。由于路由信息在不同 VPN 之间的分发会受到严格的限制，不同群组的数据不会发生意外泄漏。

通过第三层 MPLS VPN 实现的网络划分和安全等级可以与通过基于电路的网络（例如 ATM 和帧中继）所建立的服务供应商环境相提并论。在 LAN 中，网络划分和 VPN 间安全的等级与通过 VLAN 实现的等级相当。

如前所述，一种可以让企业从工作组之间的这种私密性保护中获益的情况是他们需要为员工、承包商和来宾提供独立的网络。承包商和来宾需要与员工共享网络基础设施，但是不得访问员工所使用的内部流量或资源。同样，来宾不得访问承包商流量，反之亦然。因此，所有不同的群组都需要在共享同一个物理网络的同时，保护他们的私密性。最终用户的体验应当是在使用完全独立的物理网络，这些网络可能被安全地互联，也可能没有。

## 子网透明度

如前所述，每个 VPN 都建有一个独立的路由域。这提供了为任何指定 VPN 使用任何 IP 地址空间的灵活性——无论它是否与其他 VPN 的地址空间重叠或者冲突。因此，每个群组可以按照 RFC 1918 的规定，独立地使用私有 IP 地址。

这种灵活性在很多情况下都很有用。例如，当需要将某个已经分配了地址的、被收购的公司网络合并到共享 LAN 中时，可以将该网络作为一个独立的 VPN 加入基础设施。这使得被收购的网络可以在不与其他 VPN 发生冲突的情况下保留它的原始地址空间。同样，这种灵活性对于那些拥有经常需要独立管理自己的地址空间的工程或者开发群组的企业具有重要的意义。

## 用户移动性

由于基于 MPLS 的园区 VPN 具有很高的可用性，可以在每个配线间支持每个 VPN。事实上，从管理的角度来说，这种方式更加适合在园区 LAN 中部署 VPN。

因为所有 VPN 都可以随处可用，所以用户可以一边在园区中移动，一边使用他们的 VPN 中规定的权力和策略。无所不在的 VPN 让用户可以始终处于他们的原始 VPN 中——无论他们身在何地。

将用户分配到园区中的某个 VPN 相当于将用户所连接的端口分配到与该 VPN 有关的接入 VLAN。可以根据用户的身份（利用 802.1x 身份验证）或者他们的设备 MAC 地址（利用 VLAN 管理策略服务器[VMPS]或者思科安全用户注册工具[URT]）将用户分配到某个指定的 VPN（VLAN）。尽管这种 VPN 分配不是动态的，但是它很简便，只需要将相关的接入端口分配到适当的 VLAN。

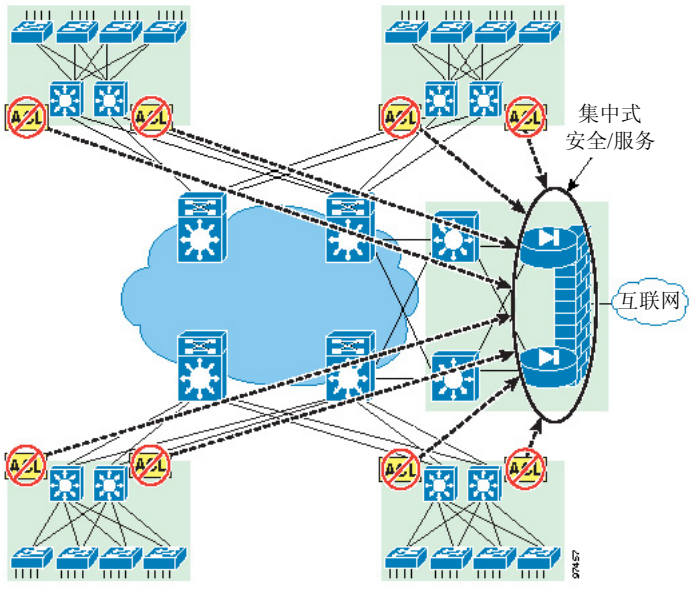
再设想一下航空公司的例子。园区 VPN 的使用让不同的航空公司可以共用登记柜台和登机口。这种被称为“共用用户终端设备”的理念可以让航空公司的员工和操作人员在机场中移动办公，从而提高机场空间的利用效率。另外，每个航空公司的跑道操作人员可以通过无线技术连接网络。这些用户需要在往返于跑道之间时始终位于他们特定的 VPN 中。跑道操作人员的移动要求更为复杂，因为它需要使用无线漫游机制，这在目前意味着要使用扁平式第二层网络。目前，这个问题可以通过使用第二层环和生成树加以解决。将来，第二层 VPN 机制——例如虚拟专用 VPN 服务（VPLS）——可以利用现有的、支持 MPLS 的基础设施，提供一个更加便于扩展的第二层 VPN 解决方案。

无线漫游所导致的问题是暂时性的。移动 IP 无线客户端和接入点很快将可以在第三层提供漫游功能。但是，园区中还有很多需要第二层连接的应用。对于这些应用，MPLS VPN 可以通过为大部分 IP 流量使用第三层 VPN 和为其他流量使用第二层 VPN，提供一个全面的解决方案。这两种 VPN 可以同时使用，提供本文所介绍的所有优势。

## 集中式安全

如前所述，除非专门设置了一个针对某个 VPN 的出/入路由，否则流量无法进入或者离开该 VPN。这使得网络工程师可以控制 VPN 的接入点的位置和数量。它还可以大幅度减少网络工程师必须维护的 ACL 的数量，因为 ACL 只需要位于出/入点（如图 3 所示）。当这些出/入点位于某个集中地点时，该集中地点就可以被用作安全策略的集中实施点，以及 VPN 之间的中转区和对共享资源（例如服务器群、WAN 或互联网）的接入点。

**图 3**
集中式安全



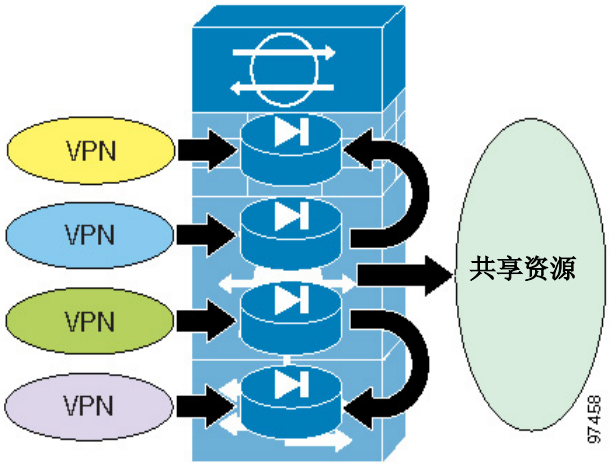

在一个中央地点实施安全策略可以减少需要维护的 ACL 的数量和长度，从而简化管理。过去需要被分发到整个园区的 ACL 现在可以变得更短，并且只需要在中央地点部署。

集中实施安全策略还可以实现安全设备——例如防火墙和入侵检测系统（IDS）——的共享。下一代防火墙（例如针对 Catalyst 6500 系列交换机的思科防火墙服务模块）同时在一个设备上提供数百个虚拟防火墙。这些虚拟防火墙可以支持 VPN，能够为每个 VPN 分配一个专用的虚拟防火墙。通

过使用支持 VPN 的虚拟防火墙，每个群组可以在自己的虚拟防火墙上执行自己的策略，同时企业只需要拥有和维护一台防火墙设备。

还记得那个需要为每个研究小组提供一个私有网络的大学的例子吗？为每个小组提供独立的防火墙服务可能会非常昂贵，尤其是在需要以分散的方式执行安全策略的情况下。通过集中实施安全策略（如图 4 所示），大学可以在一个防火墙设备上（或者由两个防火墙组成的冗余阵列）使用多个虚拟防火墙，从而一方面为所有教师和研究小组提供服务，一方面保持他们之间的独立性。

**图 4**
共享资源




## 地点集成

安全和对共享服务的访问的集中管理也可以简化新办公地点在网络中的集成。企业可以在不影响其他办公地点，也不需要重新配置整个集中安全 ACL 的情况下，方便地添加新的办公地点。这对于那些正在迅速扩建，需要不中断其他地点（包括中央服务地点）的业务或者配置的情况下集成或者移除地点的园区尤为有用。

## 共享服务

因为 VPN 在某个中央地点端接，而且它们的所有流量都需要流经防火墙，所以企业可以保护进入每个 VPN 的所有通信流量的安全性。通过防火墙的网络地址解析（NAT）功能，VPN 可以与某个共享服务区域进行安全的通信。

共享服务区域可以提供任何共享资源——从服务器群到互联网接入。这个区域还可以被用作 VPN 间通信的中转区域。

利用 Cisco Catalyst 系列交换机上的虚拟防火墙、流量整形器和监管器，可以对所有进出 VPN 的流量实施安全控制，例如针对每个 VPN 的流量整形和速率限制。这有助于精确地控制对于共享资源的访问权限，例如互联网或者 WAN 连接，让企业可以在 VPN 需要访问这些资源时，为不同的 VPN 分配不同的服务等级。

与此同时，企业可以为 VPN 和共享服务区域之间的流量保存基于每个 VPN 的记帐信息。如有必要，这些信息可以被用于管理或者计费。

## 共享数据中心

企业中的很多群组可能需要专用的服务器群，但是这些服务器群的规模往往很小。因此，不同的群组并不需要一个包含成百上千台服务器的大型数据中心，而是需要一个专用的小型数据中心。部署多个小型数据中心并不经济，上文已经介绍了利用 ACL 划分共用数据中心的弊端。园区 VPN 的使用让网络工程师可以划分数据中心和为不同的群组提供专用的服务器资源，同时使用一个共享的数据中心基础设施。数据中心可以通过 VLAN 进行划分。这些 VLAN 会被映射到分布层上相应的第三层 VPN。

## 记帐和计费

根据企业所采用的服务模式，需要确定一种基于客户对于特定资源的使用情况的计费机制。Cisco NetFlow Collector 让企业可以准确地对网络流量记帐。这些信息可以被用于计费。与安全和共享服务一样，记帐也应当集中管理。

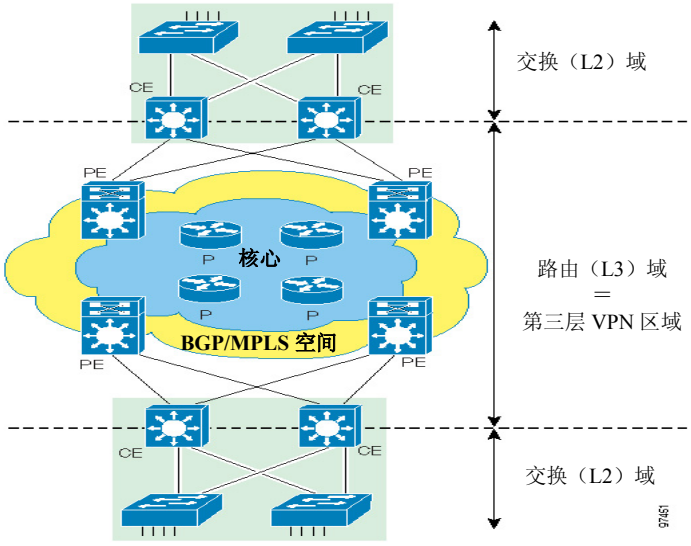
存在记帐和计费需求的企业包括机场和商务中心。商务中心需要为多个租户提供共享园区网络。商务中心服务的一部分是一个数据中心基础设施，其中通常包括 IP 电话和互联网接入服务。这些服务的使用必须按照每个租户（VPN）的使用情况进行计费。思科 IP 电话解决方案包括了适用于电话的计费机制。在思科所提供的解决方案中，互联网接入服务可以按照 Cisco NetFlow Collector 在共享服务区域搜集到的流量统计数据计费。

## 部署选项

图 5 显示了构成 MPLS VPN 网络的各个组件。

**图 5**

MPLS VPN 网络的组件




供应商边缘（PE）路由器可以从客户边缘（CE）路由器接收路由，并通过一个 MPLS 骨干网将它们发送到其他 PE 路由器。位于网络中间的是供应商（P）路由器或者标签交换路由器（LSR），它可以部署一项纯第三层 MPLS 传输服务。

只有 PE 路由器需要 VPN 信息，它们可以在不同的 PE 路由器之间划分。PE 路由器只需要获得与它们有直接连接的 VPN 的路由信息。骨干网中的 P 路由器并不支持 VPN，因此可以提供更高的可扩

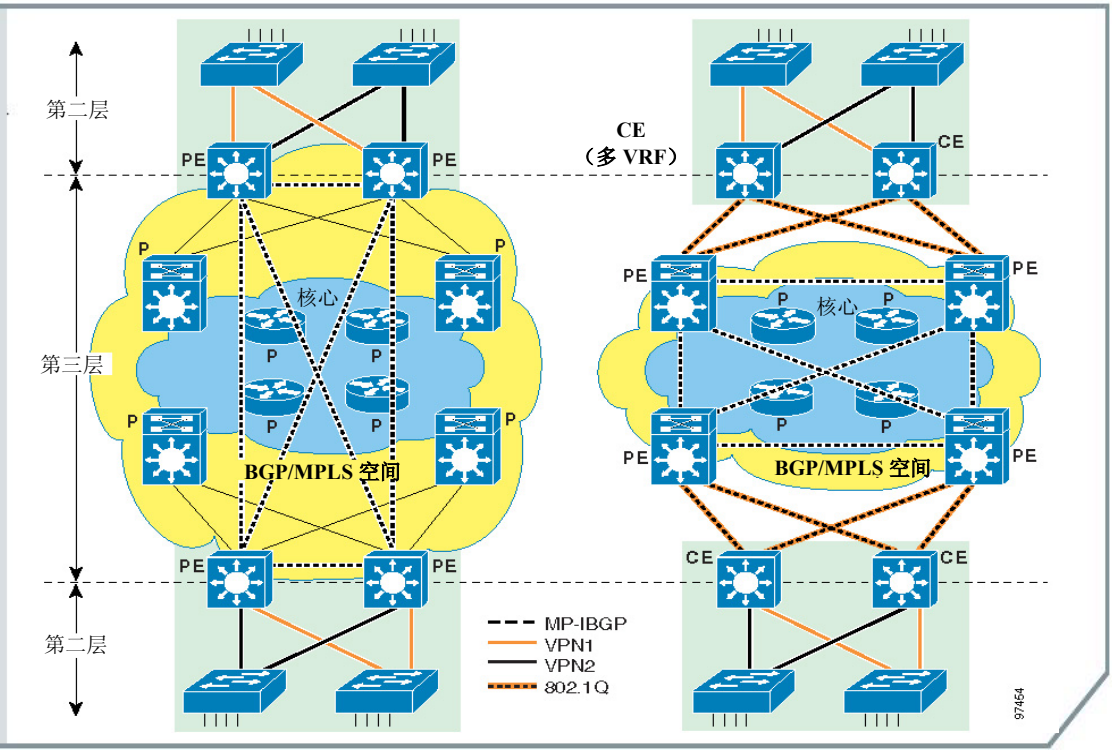
展性，因为它们不需要传输 VPN 路由。这可以防止 P 路由器中的路由表为保存 VPN 状态信息而出现没有必要的增长。

图 5 显示了构成 MPLS VPN 网络的组件：

- **客户边缘**（CE）－－一台位于网络边缘的路由器，可以将第三层 VPN 空间拓展到路由域边缘。CE 路由器不许支持 VPN。
- **供应商边缘**（PE）－－端接 BGP/MPLS VPN 隧道的路由器，标记着 BGP/MPLS VPN 空间的边缘。大部分针对 VPN 的配置和处理都发生在 PE 路由器。
- **供应商**（P）－－任何在 BGP/MPLS VPN 空间内部转发分组的路由器。
- **路由**（L3）**域**－－园区 LAN 中的第三层部分。路由域通常从分布交换机开始，包括网络核心。
- **交换**（L2）**域**－－园区 LAN 中的第二层部分。交换域通常出现在接入层。配线间交换机在这里连接到分布层。它可以通过 VLAN 进行划分。
- **BGP/MPLS 域**－－在路由域的这个部分，可以按照 RFC 2547 的规定，通过 BGP 和 MPLS 机制部署第三层 VPN。这可以覆盖整个路由域，或者只包含核心。
- **第三层 VPN 空间**－－经过划分的路由域。对于园区 VPN，这个空间会覆盖整个路由域。划分可以通过多种第三层 VPN 机制（例如 BGP/MPLS VPN 和/或 Multi-VRF VPN 扩展）的组合而实现。
- **园区 VPN**－－覆盖交换和路由域的端到端网段。这包括 VLAN 和第三层 VPN，以及两者之间的映射。

下面让我们看看用 BGP/MPLS VPN 部署园区 VPN 的两种方式。它们分别符合 RFC 2547 和 IETF 草案 2547bis 的规定。

**图 6**
园区 VPN 部署选项



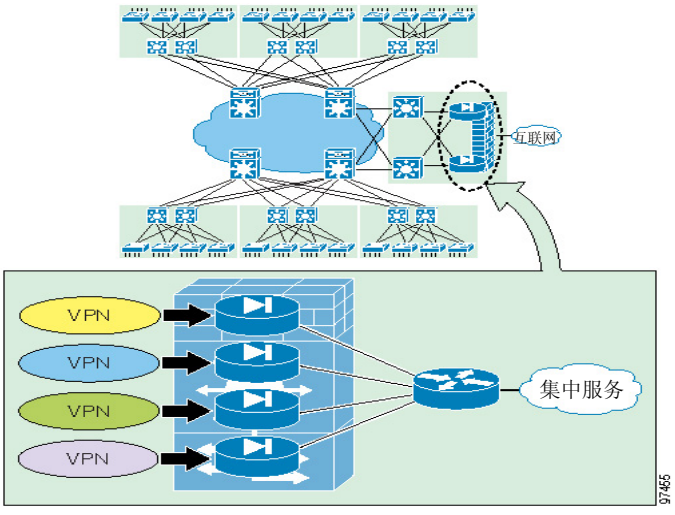
在图 6 左侧的网络中，PE 由分布层交换机担任。在这种情况下，BGP/MPLS VPN 空间会覆盖整个路由域，用一个外部网络云表示。因为该 BGP/MPLS VPN 空间和路由域是相同的，所以不需要将 VPN 扩展到 PE 以外，即不需要使用一台 CE 路由器。VPN 通过 VLAN（红色和黄色）被扩展到路由域以外，进入接入层（第二层）。因此，路由域上的第三层 VPN 第二层域上的 VLAN 的结合可以实现端到端的划分－－一个园区 VPN。

在图 6 右侧的网络中，BGP/MPLS VPN 空间可以被缩减为一跳，因此核心路由器现在可以充当端接 BGP/MPLS VPN 的 PE 路由器。分布层交换机必须充当通过 802.1q 中继与 PE 路由器通信的 CE 路由器，并且支持多个路由表（Multi-VRF CE 或者 VRF-lite），以便将第三层 VPN 扩展到路由域边缘。这种方式需要一种更加复杂的配置，但是在分布层交换机上消除了了对于 MPLS 和 BGP 支持的需求，让企业可以在分布层选择更多的交换机型号。VPN 通过 VLAN 扩展到接入层。

因为网络是独立的，拥有单独的路由表，因此流量无法在没有专门设置某个进入/端接点的情况下离开或者进入 VPN。因此，每个 VPN 所提供的安全等级都可以与单独部署的 VLAN 相当。VPN 的进入/端接点可以在最方便的地方设置。这使得企业可以创建一个中央地点，根据企业的安全策略在不同 VPN 之间共享安全设备服务，并集中控制所有进出外联网和互联网的通信（在必要时甚至包括 VPN 之间的通信）。

集中服务可以通过在与中央服务地点对应的 PE 端接所有 VPN 而部署。每个被端接的 VPN 都被路由到一个（或者冗余的）防火墙设备上的一个虚拟防火墙。流量随后会通过一个中转路由器，在不同的防火墙和共享服务之间路由。如果在不同的 VPN 之间存在重叠的 IP 地址，NAT 可以由虚拟防火墙执行。图 7 显示了集中地点的部署方式。

**图 7**
集中服务的部署



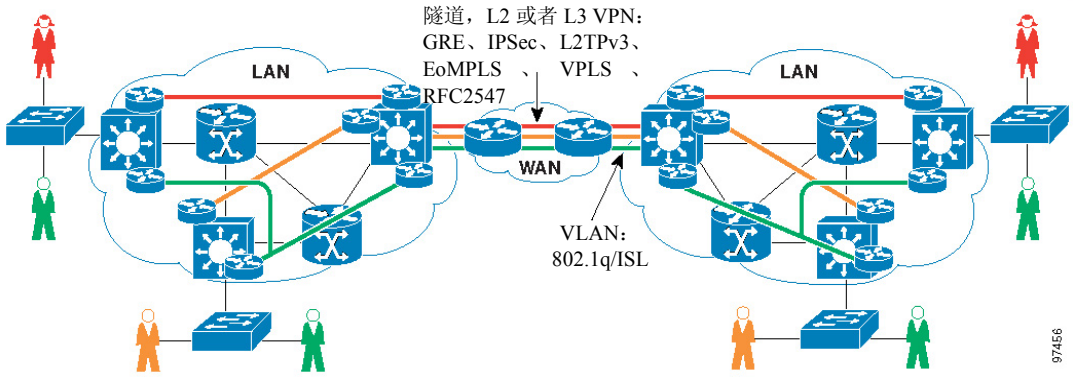

**注意：**现有的其他部署方式涉及到路由目标处理、支持 VRF 的 NAT，以及支持 VRF 的防火墙。无论选择哪种部署方式，流量路由的原理都类似于图 7 中介绍的方式。

在某些情况下，客户可能需要将园区 VPN 拓展到多个地理位置分散的园区。这时，可以在 WAN 上使用多种不同的隧道机制。思科园区 VPN 解决方案可以通过多种点对点和点对群体隧道选项，

在 WAN 上拓展园区 VPN。如图 8 所示，思科园区 VPN 解决方案的架构让企业可以使用任何类型的 WAN 隧道机制（例如 GRE、IPSec、L2TPv3、EoMPLS、VPLS、BGP/MPLG VPN 或者 BGP/GRE VPN）。

**图 8**

WAN 部署




在这种情况下，您可能会自问：“这些难道不都是服务供应商才有的技术吗？”随着企业的不断扩大和他们的网络基础设施的发展，他们的网络需要支持很多不同类型的集成化服务，因而必须提供一个可扩展的、高度可用的网络基础设施。随着越来越多的服务（例如电话、视频、监控、声音系统等）需要依靠企业的网络，服务需求变得越来越严格，针对性也越来越高。企业要想以适当的安全和自定制策略的方式提供这些服务等级，就必须使用一些过去只供服务供应商使用的技术。

## 部署建议

对于思科园区 VPN 解决方案，我们建议的部署方式包括将 BGP/MPLS VPN 扩展到整个第三层域和不使用多 VRF CE 路由器（VRF-lite）。换句话说，如果经济条件允许，部署思科园区 VPN 解决方案的企业应当尝试在他们的整个路由域中部署 BGP/MPLS VPN（RFC 2547）。VRF-lite 应当作为一种移植途径使用。

建议采用这种部署方式的原因主要是一个全面的 BGP/MPLS 部署可以为企业带来的好处（与用 VRF-lite 扩展 VPN 的部署方式相比）：

- **VRF 数量的增加**——一个全面的 BGP/MPLS 部署可以在将一台 Cisco Catalyst 6500 系列 Supervisor Engine 作为 PE 时，支持超过 400 个 VRF。采用 VRF-lite 的部署在分别使用 Catalyst 3550 或者 4500 时，只能处理 7 个 VRF 或者 64 个 VRF。
- **简化的配置和维护**——VRF-lite 的使用需要在 PE-CE 连接上配置和维护 PE-CE 路由协议和 802.1Q 中继。在配置端到端 BGP/MPLS VPN 时并不需要这样做。因此，一个全面的部署可以大幅度简化园区 VPN 的配置和管理。
- **加强组播处理能力**——在一个将 BGP/MPLS VPN 扩展到整个路由域的环境中可以更好地处理组播。利用组播 VPN（MVPN），PE 路由器——例如 Cisco Catalyst 6500 系列 Supervisor Engine 720——可以有效地在不同的 VPN 中处理组播流量。

  目前，人们正在评估通过为 VRF-lite 添加扩展而提供组播支持的灵活性。现在可以采用多种临时性的方法，利用 CE 上的 VRF-lite 在网络中支持组播。但是，这些临时性的方法不属于本文的讨论范围。
- **提高灵活性**——一个全面的 BGP/MPLS VPN 部署可以让网络工程师灵活地部署基于 MPLS 的功能，例如流量/隧道工程和快速重新路由（FRR），而 VRF-lite 无法提供这些功能。

与结合 VRF-lite 的部署相比，在整个路由域中部署 BGP/MPLS VPN 可以带来显著的优势。VRF-lite 的使用让企业可以将一些缺乏 MPLS 功能的较为便宜的产品放在第三层边缘（通常是分布层）。这些产品包括 Cisco Catalyst 3500 和 Cisco Catalyst 4500 交换机。它们可以支持 VRF-lite，但是不具备 MPLS 功能。我们建议在向一个全面的 BGP/MPLS VPN 部署迈进的第一步使用 VRF-lite。全面的 BGP/MPLS VPN 部署可以提供更加全面的功能和优势。另外，可以在需要一个全面的 BGP/MPLS VPN 部署之前，一直使用 VRF-lite 部署。

## 技术和平台

思科园区 VPN 解决方案采用了整个 Cisco Catalyst 交换机系列所提供的多种先进技术。借助 VLAN 的 LAN 划分可以在 Catalyst 系列交换机中端到端地使用，而在分布和核心的路由域中进行的划分可以通过用于 Catalyst 6500 的 Supervisor 720 所支持的 BGP/MPLS VPN 实现。在路由域只覆盖一些小型 Cisco Catalyst 交换机（例如 Catalyst 3550、Catalyst 3750 和 Catalyst 4500 系列）的情况下，可以利用并非基于 MPLS 的、使用 VRF-lite 的点对点 VPN（也被称为 Multi-VRF CE）进行扩展。

在中央地点，安全设备（例如思科防火墙服务模块、思科 IPSec VPN 服务模块和用于 Catalyst 6500 的思科 IDS 模块）可以提供与基础设施集成的服务。这些服务一方面可以由所有 VPN 共享，另一方面又能以虚拟的方式专门用于满足每个 VPN 的特殊需求。多种功能（例如支持虚拟 VRF 的防火墙或者支持 VRF 的 IPSec VPN 加密进程）让一个服务模块可以为多个 VPN 提供独立的服务，从而降低资本开支，为安全管理和 VPN 扩展提供一个集中地点。这种方式不会产生单点故障，因为这些安全设备可以使用高度可用的冗余配置。

Cisco NetFlow Collector 可以为所需的记帐和计费功能提供必要的工具。管理功能由 CiscoWorks 配置工具和/或思科 IP 解决方案中心提供，具体选择哪种方式取决于企业的需求。

整个 Cisco Catalyst 交换机系列可以切入到这个解决方案中的不同层次，从而让网络工程师可以更加充分地发挥智能化基础设施的作用。

## 总结

思科园区 VPN 解决方案有助于改进园区 LAN 和解决当今企业面临的诸多问题。它为实现可扩展的网络划分提供了一个便捷的解决方案。

**思科系统（中国）网络技术有限公司**

**北京**
北京市东城区东长安街 1 号东方广场东方经贸城东一办公楼 19-21 层

邮政编码：100738
电话：(8610) 85155000
传真：(8610) 85181881

**上海**
上海市淮海中路 222 号力宝广场 32-33 层

邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

**广州**
广州市天河北路 233 号中信广场 43 楼

邮政编码：510620
电话：(8620) 85193000
传真：(8620) 38770077

**成都**
成都市顺城大街 308 号冠城广场 23 层

邮政编码：610017
电话：(8628) 86961000
传真：(8628) 86528999

**如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn**



思科系统（中国）网络技术有限公司版权所有。

2005©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS 标识，Cisco Systems, Cisco Systems 标识，Cisco Systems Cisco Press 标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌、名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。



2005 年 3 月翻译