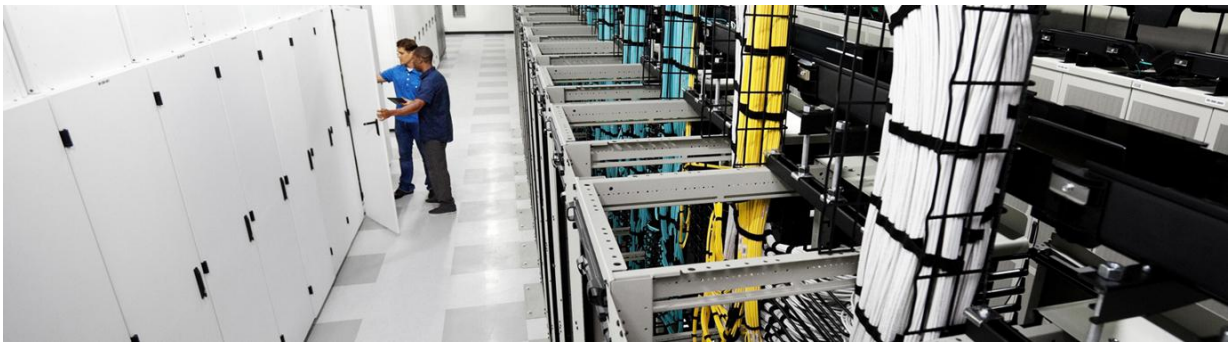
以应用为中心的基础设施的原理



概述

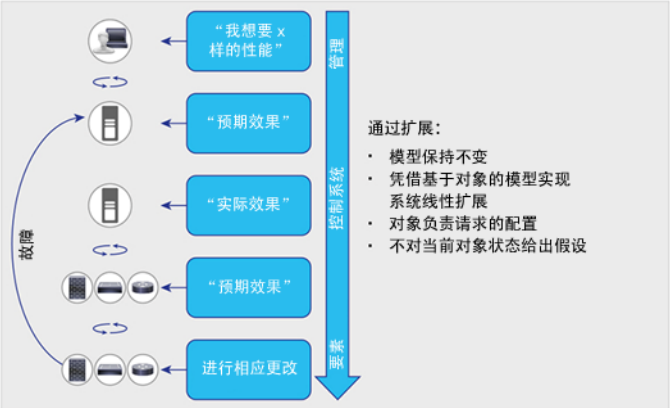
以应用为中心的基础设施 (ACI) 的一大创新就是引入了一个高度抽象的界面，可用来表示应用组件之间的连接，以及管理这种连接的更高级别的策略。该模型采用简单设计，应用开发人员使用方便，同时可以提高自动化程度和安全性。

ACI 策略理论

ACI 策略模型是一种基于承诺理论的对象导向模型。承诺理论基于可扩展的智能对象控制，而不是那种自上而下的管理系统的传统命令式模型。在这个系统中，中央管理器必须知道底层对象的配置命令及其当前状态。

相反，承诺理论依赖于底层对象来处理由控制系统自身引发的配置状态变化作为“理想的状态变化”。然后，对象作出响应，将异常或故障传递回控制系统。这种方法减少了控制系统的负担和复杂性，并可实现更大规模的扩展。该系统通过允许底层对象从其他底层对象和较低级别对象请求状态变化的方法来进一步扩展（图 1）。

图 1. 适用于大规模系统控制的承诺理论方法



在这一理论模型下，ACI 将应用作为关注重点，构建了适合应用部署的对象模型。从传统意义上来说，应用会受到网络功能的限制，也会受到用于防止结构误用的实施策略的限制。寻址、VLAN 和安全等概念已经紧密联系在一起，限制了应用的扩展和移动性。由于应用正处于重新设计阶段以便满足移动性和 Web 扩展的要求，这种传统的方法阻碍了快速一致的部署。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

ACI 策略模型并未对底层网络的结构作出任何规定。然而，承诺理论却决定其需要具备一定的优势元素，称之为 iLeaf，来管理到各种设备的连接。

对象模型

顶层的 ACI 对象模型建立在单租户或多租户组的基础上，允许网络基础设施管理和数据流分离。租户可用于客户、业务单位或群组，具体情况视组织需求而定。例如，企业可能为整个组织使用一个租户，云提供商可能让使用一个或多个租户的客户代表他们的组织。

可以将租户进一步划分为不同情景，具体情景直接与虚拟路由与转发 (VRF) 实例或独立的 IP 空间有关。每个租户都可以拥有一个或多个情景，具体数量取决于该用户的业务需求。情景提供了一种方法来进一步分离特定租户的组织要求和转发要求。由于情景使用单独的转发实例，因此 IP 寻址可以在适用于多租户的独立情景中复制。

在情景中，该模型提供了一系列定义应用的对象。这些对象是终端 (EP) 和终端组 (EPG) 以及用于定义它们之间关系的策略（图 2）。请注意，这个案例中的策略不仅仅是一组访问控制列表 (ACL)，也包括入站和出站过滤器、流量质量设置、标记规则和重定向规则的集合。

图 2. 逻辑对象模型

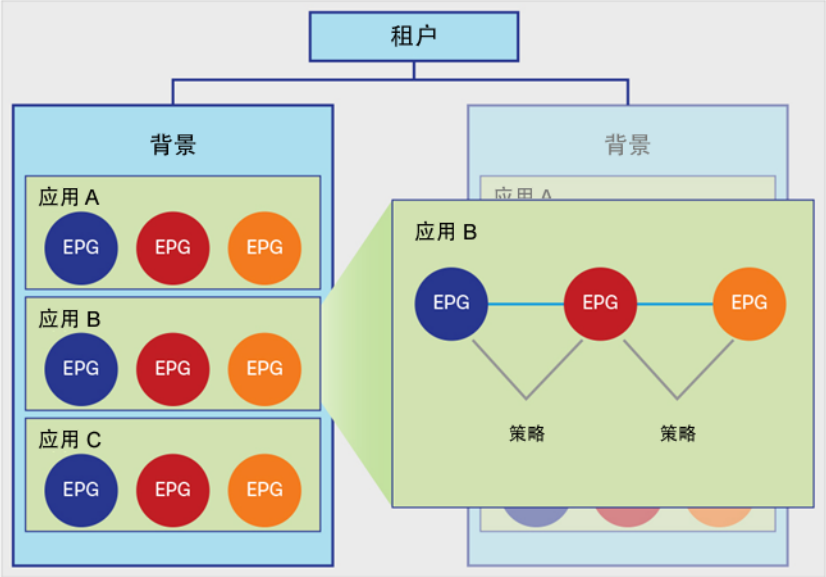


图 2 显示一个租户具备两个情景，并显示了组成这两个情景的各个应用。图中所示的 EPG 是构成应用层或其他逻辑应用组的终端组。例如，图右侧展开显示的应用 B，可能包括 Web 层（蓝色）、应用层（红色）和数据库层（橙色）。EPG 以及定义其交互操作的策略的结合体是 ACI 模型中的应用网络配置文件。

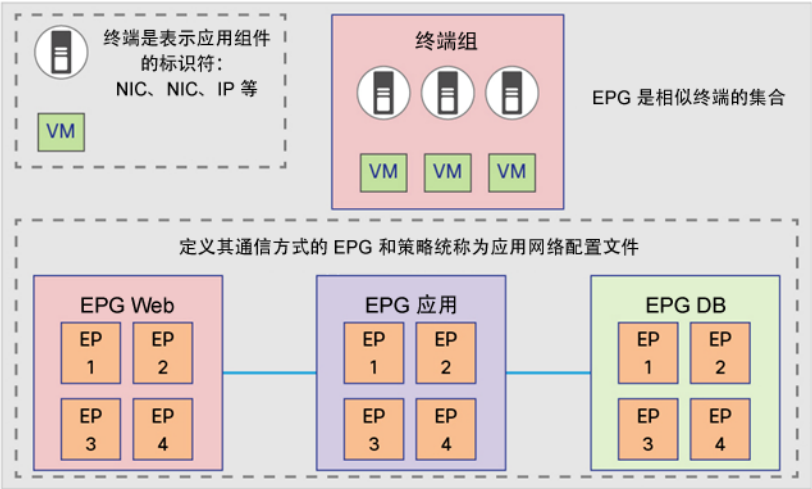
终端组

EPG 是代表应用层或服务集的相似终端的集合。它们提供了需要相似策略的对象的逻辑分组。例如，EPG 可能是构成应用的 Web 层的一组组件。终端可使用网络接口卡 (NIC)、虚拟 NIC (vNIC)、IP 地址或域名系统 (DNS) 名称来进行定义，其扩展性可支持未来的应用组件识别方法。

EPG 也用于表示外部网络、网络服务、安全设备和网络存储等实体。EPG 是提供相似功能的一个或多个终端的集合。它们是具备各种使用选项的逻辑分组，具体情况取决于所使用的应用部署模型（图 3）。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 3. 终端组的关系



EPG 设计灵活，可根据客户可选的一个或多个部署模型进行定制。然后，EPG 将用于定义应用策略的元素。在网络交换矩阵中，在 EPG 之间应用策略来定义 EPG 相互通信的方式。未来，这种方法未来可扩展以支持 EPG 内部的策略应用。

以下是一些 EPG 用例：

- 由传统网络 VLAN 定义的 EPG：将所有终端连接到位于 EPG 的指定 VLAN
- 由虚拟可扩展 LAN (VXLAN) 定义的 EPG：同 VLAN，使用 VXLAN 时除外
- 映射到 VMware 端口组的 EPG
- 由 IP 或子网定义的 EPG：例如，172.168.10.10 或 172.168.10
- 由 DNS 名称或范围定义的 EPG：例如，example.foo.com 或 *.web.foo.com

EPG 的使用具有灵活性和可扩展性。该模型旨在提供一种工具来构建可映射到实际环境中的部署模型的应用网络模型。终端的定义也具有可扩展性，能够为今后的产品改进和行业要求提供支持。

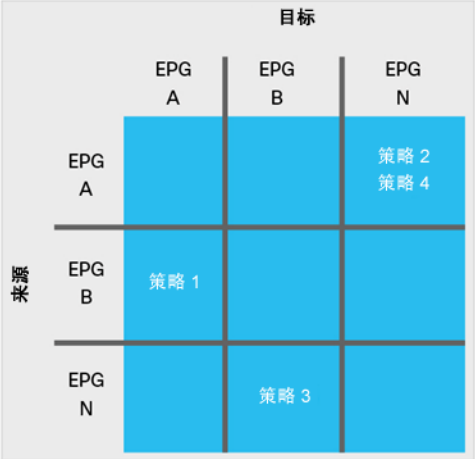
EPG 模型提供了大量的管理优势。它提供了一个具有统一策略的对象，面向更高级别的自动化和协调工具。该工具无需在单个终端上运行即可修改策略。此外，它还有助于确保同组中所有终端的一致性，而不考虑终端在网络中的位置。

策略实施

可将 EPG 和策略之间的关系看作一个矩阵。该矩阵具有一个坐标轴，表示源 EPG (sEPG) 和其他目标 EPG (dEPG)。一个或多个策略将被放置在适当的 sEPG 和 dEPG 轴的交叉点上。该矩阵在大多数情况下呈稀疏分布状态，这是因为许多 EPG 无需相互通信（图 4）。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 4. 策略实施矩阵



可按服务质量 (QoS)、访问控制、服务插入等过滤器对策略进行划分。过滤器是两个 EPG 之间策略的具体规则。过滤器包括入站和出站规则：允许、拒绝、重定向、记录、复制和标记。策略允许在定义中使用通配符函数（图 5）。策略实施通常采用最具体匹配优先的方法。

图 5. 通配符实施规则

sEPG	dEPG	应用	备注
完全限定	完全限定	完全限定	完全限定（S、D、A）规则
完全限定	完全限定	*	(S, D, *) 规则
完全限定	*	完全限定	(S, *, A) 规则
*	完全限定	完全限定	(*, D, A) 规则
完全限定	*	*	(S, *, *) 规则
*	完全限定	*	(*, D, *) 规则
*	*	完全限定	(*, *, A) 规则
*	*	*	默认（例如，隐式拒绝）

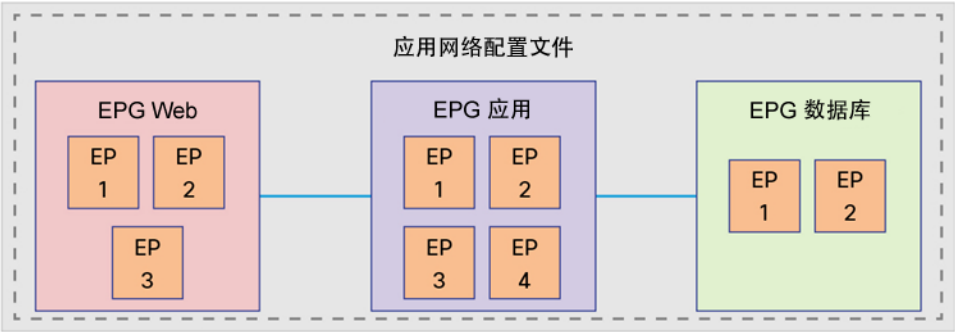
应用网络配置文件

应用网络配置文件是 EPG 及其连接以及定义这些连接的策略的集合。应用网络配置文件是应用及其在网络交换矩阵中的相互依存关系的逻辑表示。

应用网络配置文件旨在以符合应用设计和部署方式的逻辑方式建模。策略和连接的配置与实施由系统处理，而非由管理员手动处理。图 6 显示了访问配置文件的示例。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 6. 应用网络配置文件



创建应用网络配置文件需要以下常规步骤：

1. 创建 EPG（如前所述）。
2. 使用以下规则创建定义连接的策略：
   - 允许
   - 拒绝
   - 记录
   - 标记
   - 重定向
   - 复制
3. 使用称为“合同”的策略结构创建 EPG 之间的连接点。

合同

合同定义了入站和出站允许、拒绝、QoS 规则和重定向等策略。合同允许在 EPG 彼此通信时采取简单和复杂两种方式，具体情况取决于环境要求。虽然合同是在 EPG 之间实施，但利用提供商-消费者关系可将合同与 EPG 相联系。基本上，一个 EPG 提供合同，而另一个 EPG 使用该合同。

提供商-消费者模型可用于若干目的。该方式提供了将“屏蔽”或“隔膜”连接到应用层的自然方式，决定了该层与应用的其他部分进行交互的方式。例如，Web 服务器可能提供 HTTP 和 HTTPS，因此该 Web 服务器可以包括在仅支持这些服务的合同中。此外，该合同的提供商-消费者模型通过允许简单一致的策略更新到单个策略对象而不是更新到合同可能代表的多个链接来增强安全性。此外，合同允许策略一次定义后多次重用，可提供简便性（图 7）。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

图 7. 合同

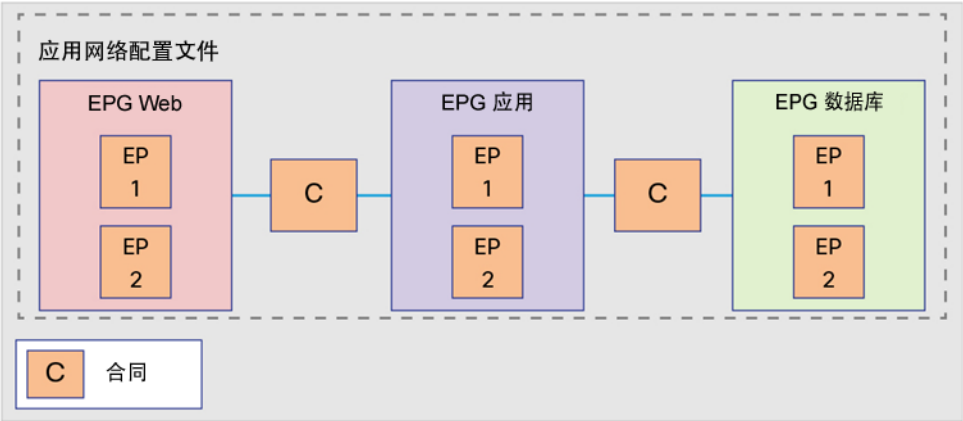
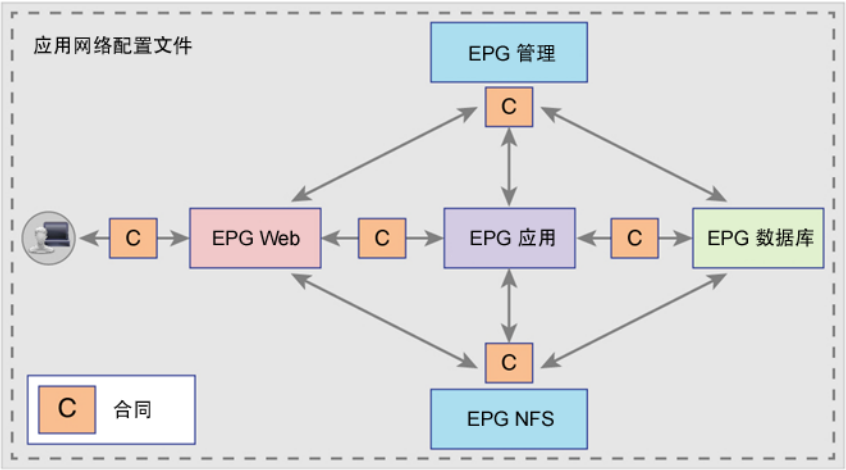


图 8 显示了由 EPG 连接定义的三个 Web 应用层与定义其通信的合同之间的关系。这些部分共同构成了应用网络配置文件。合同还为通常与多个 EPG 通信的服务提供了可重用性和策略一致性。

图 8. 完整的应用网络配置文件



总结

本文档仅介绍了 ACI 策略模型：讨论 ACI 的概念以及如何使用其策略模型。该模型还包括许多其他的结构和对象，为简单起见未在此处一一介绍。

更多详情

请访问 http://www.cisco.com/go/aci。

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1110R)

美国印刷

C11-729906-00 11/13

© 2013 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。