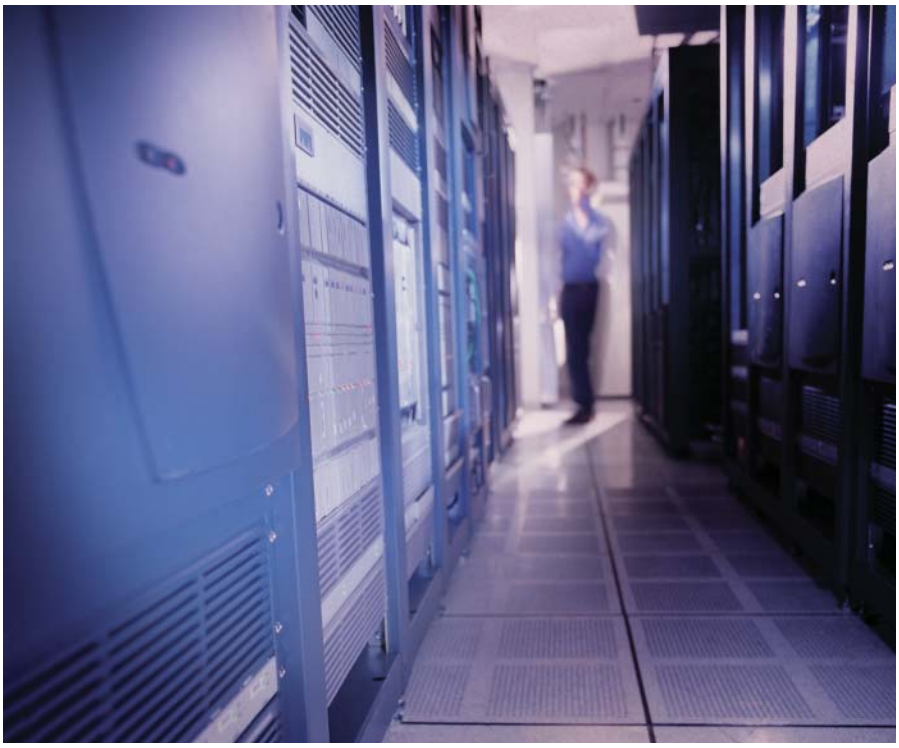
不断发展的数据中心

专题报告：新趋势影响数据中心网络架构



作者：
MAURICIO ARREGOCES
认证工程师
CCIE No. 3285

思科系统公司工程部经理，主要负责网络设计和构建工作。他持有计算机科学专业的学士和硕士学位，针对数据中心网络撰写过大量文章并发表过大量演讲。他的联系方式是：marregoc@cisco.com。

企业制订业务目标来控制运营成本并提高业务灵活性，而数据中心使用的高新技术为满足这些业务目标提供了新方式。部署高新技术将帮助企业数据中心实现快速发展。

本文将讨论新趋势对数据中心网络架构的影响以及可能影响下一代数据中心的架构变化。

新趋势

控制运营成本使许多企业都将服务器、应用、存储甚至是数据中心等不同技术领域整合在一起。此外，通过提高分布式环境中的永续性以实现应用和数据安全、业务连续性和服务器集群等要求促成了其他趋势的形成。例如，合并和收购可帮助企业在不同市场中实现快速增长，在完成合并或收购后，企业需要共享应用并合并网络，同时控制接入、验证、路由和安全策略。网络分段和虚拟化技术简化了合并流程。某些趋势源自增长和扩展，需要进行容量规划以处理供电、冷却、布线、空气流通及网络和计算增长等环境问题。

整合趋势

现在，整合无疑是影响全球数据中心的最常见的趋势。主要业务驱动因素包括：成本控制、运营效率和有效利用资源等。图 1 显示了数据中心的技术整合流程。

数据中心整合

数据中心整合指减少分布式服务器集群的数量，将服务器重新安排到现有或全新设施中。这些整合后的数据中心相互连接，其运营、支持和设计的最佳业务实践均实现标准化。整合的目标包括：减少需要管理的位置、集中计算基础设施（服务器和应用）以及利用现有数据中心设施投资，如图 1 所示。从网络的角度看，整合将使大幅度增加环境中运行的服务器和应用数量，因此需要更高的端口密度，使用更多的基于网络的服务并提高可用性，以满足更高要求。这些变化将影响超额配置率、总吞吐量、可扩展性及高可用性目标。

服务器整合

服务器整合指减少需要支持的服务器硬件平台和操作系统数量以及应用环境标准化（web和中间件层）。减少需要支持的服务器硬件平台数量将帮助企业缩短恢复时间、缓解备件库存问题、降低对工作人员的技能需求、减轻维护工作的复杂性。服务器硬件的标准化包括选择BUS/NIC 技术（例如，在 PCI、PCI-X 或 PCIExpress 之间进行选择，以及从 10/100、10/100/1000 和万兆以太网中选择服务器连接等）及选择单寻的或多寻的等。网络整合包括：服务器与接入层之间、接入层与汇聚层之间以及汇聚层与核心层之间的重新访问超额配置率；多寻的所需的端口密度；网卡（NIC）组合类型等。使用 PCI-Express 和千兆以太网的超额配置率大不相同，因为使用千兆以太网将增加平均突发率、双寻的需要两倍数量的接口、并使不同接入交换机之间形成第二层邻接。

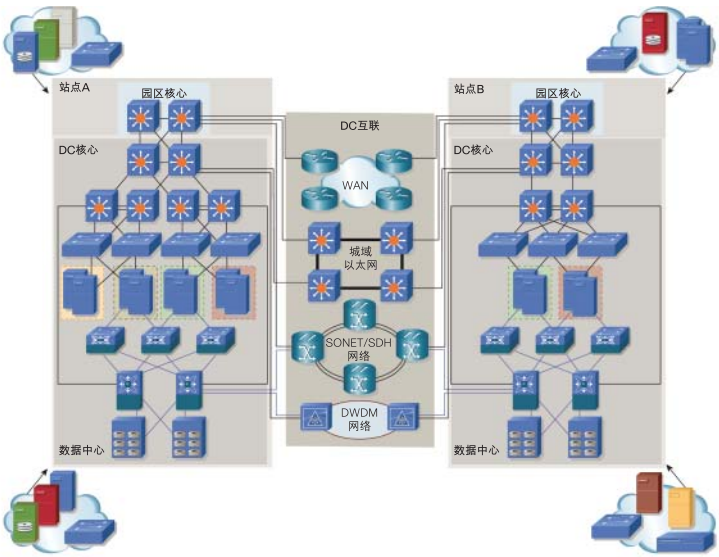
刀片服务器集成

刀片服务器技术提供每机架更高的计算、内存和 I/O 容量，同时减少所需线缆（网络、键盘、视频、鼠标或KVM）。刀片服务器集成中与网络相关的部分包括I/O和网络矩阵选择。I/O选项包括直通技术和集成的网络矩阵。直通技术将服务器与网络直接连接，而集成的网络矩阵则是连接服务器的机箱内的一系列冗余交换机。在直通环境中，服务器需要外部线缆连接。当使用集成的网络矩阵时，选项包括以太网、光纤通道和 Infiniband，每个服务器都被预连接到安装交换机的插槽中。集成交换机提供多条上行链路来连接现有的数据中心基础设施。

存储整合

存储整合可通过集中来简化存储容量管理工作并提高存储容量利用率。通过从直接连接存储磁盘（DASD）移植到存储阵列，您将能够提高存储资源利用率并从集中的存储阵列对存储资源进行更好的管理。现在支持高光纤通道端口密度和逻辑SAN分区（通过虚拟SAN）的存储局域网（SAN）矩阵技术，允许您进一步集中存储资源并整合孤立的存储孤岛，同时减少单独的存储矩阵数量。网络整合的目标是：为服务器连接提高边缘层的光纤通道端口密度；为存储阵列和磁带子系统连接提高核心层的光纤通道端口密度。其他的考虑因素还包括：提供高水平的冗余和性能以保持合理的超额配置水平。

图 1 整合数据中心资源可减少分布式服务器集群的数量并将服务器重新放置到现有或全新设施中。



多层应用集成

多层应用集成的目标是移植到基于 web 的应用中。在此，演示（web）、应用（中间件）和数据库功能明确分离，从物理上由不同的服务器提供。应用集成的目标还包括：使用 web 服务、中间件环境标准化以及支持服务导向架构（SOA）等。基于网络的服务允许扩展、保护并使用信息，并可缓存静态和动态内容以及网络文件的系统文件等。您可将这些基于网络的功能逐层、逐应用、逐多层应用组地运用到物理或逻辑应用层中。虚拟化功能使基于网络的服务能够提供灵活性，允许底层硬件支持逻辑实例的单独使用。

数据和应用安全

数据和应用安全在数据中心及企业网络的其余位置进行管理。数据中心安全指服务器集群中的信息的完整性、保密性和可访问性，可通过消除攻击对服务器、应用、存储以及支持它们的网络基础设施的影响得以实现。

服务器和应用安全

服务器和应用安全包括：分割服务器群的应用层、拒绝服务（DoS）攻击和分布式 DoS（DDoS）攻击防御、入侵检测与防御、防御蠕虫攻击等。为了满足这些要求，基于网络的服务使用运行在服务器上的

代理来保护应用环境和服务设备，来监控并分析流量，包括关联多个设备提供的信息以减少误报现象等。基于网络的服务涉及到入侵检测 / 防御产品、DoS 攻击防御产品、防火墙、流量分析和关联引擎等。

数据安全

数据安全指保护存储阵列中的信息（与连接到IP还是SAN云无关）以及保存在服务器中的信息（DASD）。两个主要目标是通过防止篡改和信息盗用来维护数据的完整性。如果数据保存在 IP 网络中（NAS 头端或 DASD），则使用与服务器和应用安全相同的保护机制。如果信息保存在连接 SAN 的存储阵列中，则安全保护机制由网络基础设施以分区、设备认证和基于端口的安全等形式提供。如果数据保存在SAN中但却是通过 IP 传输的（FCIP 或 iSCSI），如数据复制或远程备份等，则应采用加密和虚拟专用网（VPN）等安全措施，以便在数据传输时对其分段（隔离）和加密。

基础设施安全

基础设施安全用于保护支持流量在服务器群间传输的网络设备和链路。网络设备保护包括一些基本的机制，例如路由器验证、用于防止控制平面饱和的限速器、通过过滤掉不良流量来避免链路饱和的 DoS/DDoS 攻击防御设备等。您可通过控制平面监管、定制限速器、路由器验证和端口安全等多个特性，以及解决专用 VLAN 等终端安全问题的其他特性来强化网络基础设施。

虚拟化和分区趋势

虚拟化和分区将影响数据中心环境和 WAN、园区、分支机构环境及互联网边缘等其他网络位置。虚拟化和分区为基于用户角色或功能来控制网络设备和数据等资源的环境提供了所需功能。用户接入在接入点得到控制并贯彻在整个网络中。网络设备提供的功能需要单一物理单元提供的多个逻辑实例（虚拟），以便在不同的应用环境或由不同的用户群同时使用。数据访问的控制由网络元素实例根据应用环境的特定限制条件进行控制。图 2 显示了通过独立路径向服务器群传输的用户流量，在此，虚拟防火墙和虚拟负载均衡器等负责控制应用访问，可能运行在虚拟服务器上。通过服务的逻辑实例，利用 VLAN、VSAN 及防火墙和负载均衡器策略，可对不同应用环境进行分区。

虚拟化

虚拟化技术涉及到服务器和应用环境、防火墙和负载均衡器等基于网络的服务、以及路由器和交换机等基础设施组件的广泛功能。服务器和应用虚拟化指通过独立于这些资源所运行的硬件平台的方法来使用它们的逻辑实例。从本质上说，应用服务（操作系统和应用软件）是服务器中的逻辑实例，可根据需要轻松移植到任何可用的服务器中。实现这个目标需要预先存在的应用服务镜像并且可能需要I/O功能与服务器平台分离，以便轻松使用逻辑实例。

目前市场上存在两类主要的服务器虚拟化技术。一类是将单一物理服务器分成多个逻辑实体，或者虚拟服务器，每个逻辑实体都运行自己的操作系统和应用环境。另一类是将多个服务器从逻辑上组合成一台，作为运行单一操作系统的一个服务器，在此，您可通过添加或拆除服务器来提高或降低 CPU 容量，从而简化多种软件和硬件配置的管理工作。

基于网络的服务虚拟化适用于多用户组环境，可将各组彼此隔离，并在多层应用环境中将每个层次或整个多层环境彼此隔离。在单一应用环境中，每个层次都有自己的安全和可扩展性要求，而这些要求需要在不同的应用环境中得到满足。基于网络的功能通过逻辑实例单独应用到每个层次和每个应用环境中。通过虚拟化，可定义并应用基于网络的功能的逻辑实例，称为虚拟环境。虚拟环境的例子包括从一组冗余防火墙应用到四个不同应用环境的虚拟防火墙，在此，每个虚拟环境针对每个应用环境单独配置。防

火墙功能是虚拟的，但总策略却是集中的，而具体策略实例则单独管理。

基础设施虚拟化提供了使用VLAN和VSAN等基础设施功能的灵活性，以便从逻辑上划分计算资源组。根据需要将这些资源组的逻辑划分通过网络拓扑进行扩展，组间的边界仍然适用。其他基础设施虚拟服务包括虚拟路由器和交换机等。在虚拟路由中，相同物理交换机中的路由实例为每个应用环境单独提供路由功能并从路由器群集中到企业网络中。在虚拟交换中，两个物理交换机被视为一个设备，从而简化了代码维护与配置管理工作，但更重要的是，通过支持跨越不同物理交换机的端口通道和状态来提供物理冗余。

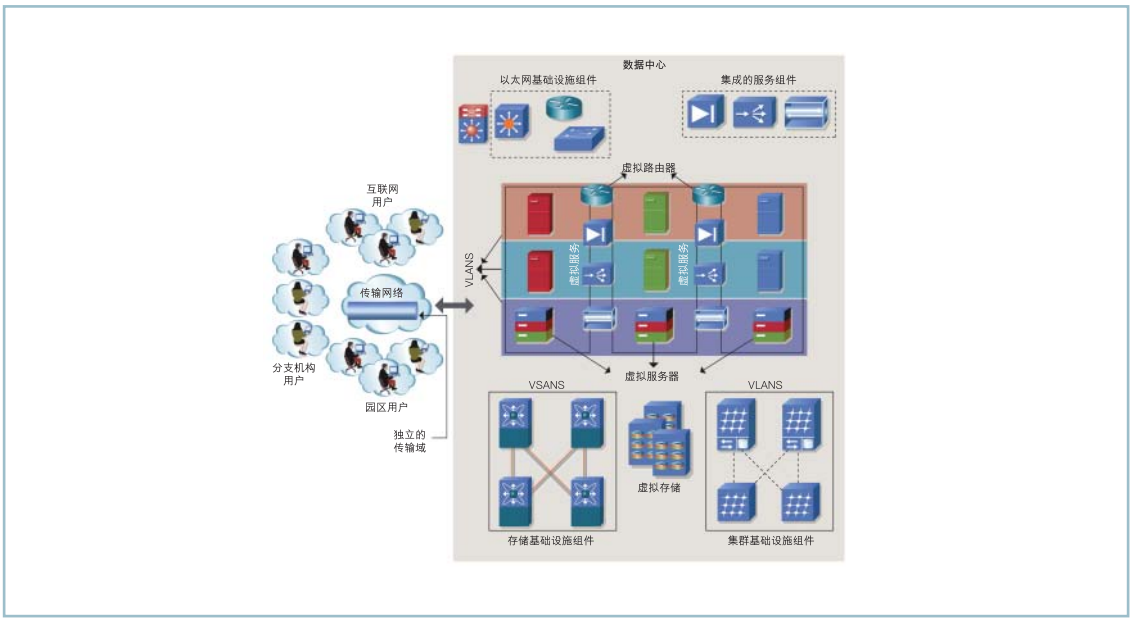
分区

分区是网络趋势，在此，技术有助于用户组的逻辑划分以及支持用户组对应用环境的接入。当您在设计分区环境时，应考虑用户接入控制、安全的传输技术和分区的应用环境等三个领域。用户接入控制（同时针对内外部用户）首先在接入点执行，通常是分支机构、园区和互联网边缘。在这些接入点中，您应对用户进行验证和授权，获得许可后，根据相关策略将用户放置到所属的小组中。在网络环境中，允许向访问应用环境的用户提供逻辑上的独立路径，从而形成分区的环境。分区的逻辑路径为通过终止在流量目的地附近的共享基础设施来传输客户流量提供了安全媒体。如果流量的目的地是服务器群，则应在数据中心入口处执行接入控制。

分区技术对于合并及收购非常有用，在这种环境下，公司必须合并网络、共享物理数据中心空间、并在客户与应用之间传输网络。

提供分区服务的网络需要在整个网络中使用多项技术，其中某些技术依赖于虚拟化功能。在接入点，执行机制使用 IEEE 802.1X 以及验证、授权和记帐（AAA）来控制用户接入、组分配和组策略。客户流量的传输使用 GRE 或 L2TPv3 隧道、MPLS VPN 或 VRF Lite 等技术，通过共享基础设施上的多条独立路径提供安全的传输。在数据中心，传输路径到应用环境传输的映射使用虚拟路由器、虚拟防火墙和任何其他的预定义虚拟服务完成。

图 2 虚拟化和分区技术使您能够在单一物理基础设施上创建多个拓扑，从而优化网络和服务器资源的利用率。



业务连续性

业务连续性方案用于防止业务运营的中断。在世界的许多国家，这个要求都已演变成一种政府制度，针对于不同行业，以防发生经济动荡。为了实现最高级别的可用性，企业需要对主要的数据中心设施和分布式数据中心环境实现冗余。网络设计必须考虑构建一个永续主数据中心以及使用多个数据中心：用于同步复制的近距离备用数据中心、用于异步复制的远程数据中心、采用主用 - 主用模式的多个数据中心。传统的业务连续性领域包括 SAN 扩展以及分布式数据中心之间的数据复制。其他功能还包括：选择距离用户最近的应用实例（名为站点选择）、为存储之间、客户端与服务器之间以及服务器之间的流量传输选择传输方法等。在服务器到服务器的环境中，传输还包括支持服务器集群间的第二层邻接，名为延伸集群。

物理数据中心环境

导致物理环境变化的原因包括：整合数据中心、服务器、应用和存储；提供业务连续性；以及应用环境为了提高性能、响应速度和可扩展性而进行的自然发展等。涉及到的主要环境问题包括供电、冷却、布线以及占地和机架空间等。企业常需要根据每机架的服务器密度及相关供电、冷却和布线要求的变化来重新考虑设计方案。数据中心规划还应考虑到冷却装置、电源、每机架单元的计算容量、以及机架空间（每机架所需的最大端口数量）的合理增长。

全新的数据中心网络架构

这些新趋势带来了许多挑战，综合看来，需要搭建一个健壮的数据中心网络架构，能够简化技术的部署。下面的标准对于开发数据中心架构至关重要：选择底层网络基础设施（网络矩阵）、决定数据中心服务、确定分布式环境的目标。

数据中心矩阵

数据中心矩阵是支持服务器群的整体交换基础设施（见图 3）。交换基础设施提供主要功能，帮助实现数据中心设备间更高效的信息交换。信息交换包含以下几类：客户端到服务器、服务器间、服务器到存储、存储间。客户端到服务器的流量属于事务处理应用，用户在此与应用进行互动。服务器间的流量可能是客户端 - 服务器间互动的间接结果（交换状态信息的应用服务器、与数据库服务器交换信息的应用服务器、彼此查询数据库的数据库服务器），也可能是因为服务器需要交换属于单一作业但却被分成多个小型任务的信息（计算分析）。服务器到存储的信息交换由主机组成，这些主机或者接入存储阵列中的目标磁盘，或以传统的区块接入方法接入磁带子系统。对于存储间的信息交换，交换在存储阵列间完成，通常使用数据复制环境中用于同步或异步通信的协议。

连接选项包括以太网和光纤通道以及新兴的 Infiniband 等技术。以太网通过以更低成本提供更高性能而继续发展，为客户端到服务器的应用提供成熟矩阵。光纤通道仍为 SAN 提供连接矩阵，因为它在服务器到存储以及存储间信息交换中可提供关键功能。

Infiniband 用于在服务器集群环境中支持高吞吐量、低延迟、低成本和关键功能。每类矩阵都提供不同的连接选项，每个选项又提供一组服务来支持不同类型的流量及其特定要求。

数据中心服务

以太网矩阵服务主要适用于客户端到服务器的流量以及某些服务器间的事务处理应用流量。这些服务包括安全、应用优化和网络管理。安全服务包括防火墙、入侵检测、IP 安全（IPSec）、SSL VPN、DoS

和 DDoS 防御以及基于网络的基本服务，如广播抑制、ARP 检查和 PVLAN 等。应用优化服务包括服务器负载平衡、SSL 卸载和两类全新服务：文件缓存和消息处理。文件缓存服务在服务器整合中使用，可集中数据中心的文件，同时确保在整合前后为用户提供一致的性能体验。消息处理服务适用于不同应用间的信息交换，力求简化企业应用的集成工作。网络管理服务包括网络元素和配置功能的传统管理，而新趋势则集中于端到端的配置虚拟服务，包括计算资源（服务器和应用）和网络及其服务。其他网络管理功能使用监视特性来创建关联信息，用于安全分析、容量规划和应用优化。

存储网络矩阵也提供虚拟化服务；VSAN将SAN分割成使用相同矩阵的孤岛；存储虚拟化可使多个存储设备看似是单一设备。主要关注数据复制的其他服务可增强分布式存储阵列与矩阵路由服务之间的数据复制流程，允许不同 SAN 上的设备彼此通信（例如，使用远程磁带子系统来对分布式数据中心不同 SAN 上的多个存储阵列备份）。由于还需要以太网和IP云通信，因此，SAN矩阵还提供网关服务以支持iSCSI和FCIP。

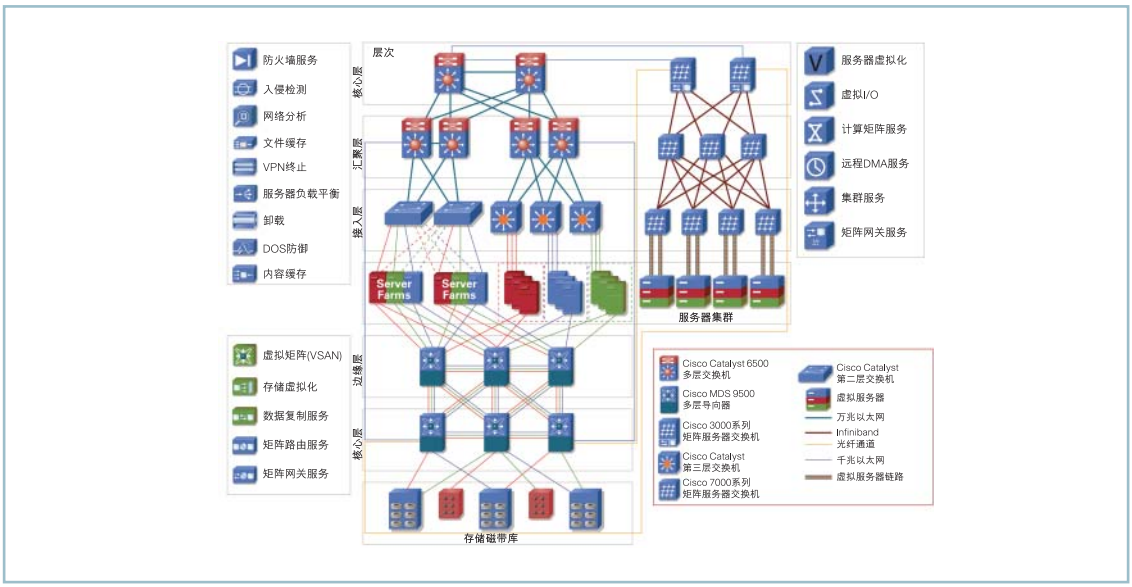
Infiniband网络矩阵为优化服务器集群的运行提供多种服务。Infiniband矩阵可构建超高速、低延迟和超额配置程度低的服务器集群。此外，Infiniband 的其他优势还包括通过远程直接内存接入（RDMA）以及接入 LAN 或 SAN 矩阵等来优化进程间通信。Infiniband矩阵还能使用操作系统、应用和存储的任意组合来无缝配置无磁盘的服务器（利用引导服务），从而提供服务器虚拟化服务。

分布式环境

分布式数据中心环境可帮助实现超越单一站点的高可用性。在主用 - 主用环境中，数据中心之间的连接是关键的，还应考虑到第二层邻接集群的需求。

分布式数据中心的设计标准包括：共包含多少数据中心、哪个数据中心运行着特定应用的有效实例、数据中心之间的传输选项、传输网络上共享的流量类型。其他设计因素包括：站点选择要求、IP 传输基础设施是否还用于数据复制流量、互联网接入点的数量和位置等（在分布式环境中，数据中心包含多个互联网接入点）。

图 3 交换矩阵为客户端到服务器、服务器间、服务器到存储及存储间的连接提供物理媒体（以太网、光纤通道、Infiniband）和服务。



深入阅读

- 思科数据中心设计最佳实践：请访问 cisco.com/go/datacenter
- 思科出版社有关数据中心的书籍：《数据中心基本要素》
  作者：Mauricio Arregoces 和 Maurizio Portolani
  （思科出版社 - ISBN: 1587050234）

北京
北京市朝阳区建国门外
大街2号北京银泰中心
银泰写字楼C座7-12层
邮编：100022
电话：(8610)85155000
传真：(8610)85155960

上海
上海市淮海中路222号
力宝广场32-33层
邮编：200021
电话：(8621)23024000
传真：(8621)23024450

广州
广州市天河区林和西路161号
中泰国际广场A塔34层
邮编：510620
电话：(8620)85193000
传真：(8620)85193008

成都
成都滨江东路 9 号 B 座
香格里拉中心办公楼 12层
邮编：610021
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

欢迎下载电子文档，http://www.cisco.com/web/CN/products/products_netsol/datacenter/index.html
2008 年 10 月印刷