数据中心网络应用蓝图

思科服务导向网络架构的主要基础

大型分支机构

大型分支机构使用两台集成多业务路由器，为提高冗余性，每台路由器与不同的WAN链路相连。在第三层设备上使用双栈IPv6-IPv4服务。利用集成式IOS防火墙和入侵防御提高边缘安全性。利用集成式呼叫管理提供远程语音功能。当IPv6流量有可能进/出分支机构时，可以考虑使用IPv6防火墙策略、过滤和DHCP前缀委派。利用集成式广域引擎执行文件高速缓存、本地视频广播和静态内容服务。

在大型分支机构的LAN/SAN设计中，服务器、存储和客户端连接与小型数据中心小型园区相似。可以使用第三层交换机提供分支机构级LAN服务，并为需要的所有接入层交换机提供连接。可以根据分支机构的不同功能要求部署多个VLAN，例如LAN设计中的服务器群、销售点、语音、视频、数据、无线和管理。

考虑使用存储网络的设计和可用的存储连接方式：FC、iSCSI和NAS。应根据延迟和事务处理速率要求规划从分支机构到总部的数据复制过程。可通过QoS分类使不同类型的流量能够满足不同应用的数据丢失和延迟要求。

外部网

将专用外部网作为IPSEC和SSL VPN的高度可扩展的安全终端，以支持业务合作伙伴连接。可以为面向特定合作伙伴的应用环境而采用内部网服务器群设计最佳实践，但同时要考虑它们特殊的安全和扩展要求。

互联网边缘

在企业网边缘执行分布式拒绝服务（DDoS）攻击防御。部署Guard和Anomaly Detector，检测和阻挡高容量攻击流量，并将可疑流量转至防欺骗和防攻击动态过滤器，执行相应的防护处理。使用自适应安全设备同时在企业网边缘执行防火墙、VPN和入侵防御功能。应在边缘路由器上使用双栈IPv6-IPv4，并考虑执行IPv6防火墙和过滤功能。

将全球站点选择器部署在DMZ中，以防止DNS流量穿过边缘安全边界。可以按照内部网服务器群中使用的最佳实践来设计面向互联网的服务器群。但要根据目标用户群的规模确定可扩展性和安全要求。为机制和数字签名验证等XML过滤使用ACN应用网关，并为原有应用的消息格式提供事务处理完整性和安全性。

互联网

合作伙伴

电信运营商1

电信运营商2

VPN

备用互联网边缘和外部网

为高度集中的集成边缘网络使用精简互联网边缘和外部网设计。边缘服务是通过防火墙、内容交换、SSL和VPN模块等服务模块，以及Guard XT和用于执行DDoS防护的Anomaly Detector等设备的嵌入式智能特性提供的。其它边缘功能包括站点选择器和内容高速缓存，以及由集成多业务设备提供的事件关联引擎和流量监控。可以在第三层设备中使用双栈IPv4-IPv6服务，需支持IPv6防火墙策略和IPv6过滤功能。

远程机构

家庭办公室

可以将家庭办公室作为企业网的延伸。基本服务包括对应用以及数据、语音和视频的访问。可使用VPN保证远程员工环境的安全性，因而需要执行公司的安全策略。还可以将无线接入作为企业网的延伸，这种方式安全而可靠。

支持策略QoS，提供语音、数据和视频流量的服务水平。可以通过双栈IPv6-IPv4路由器支持IPv6远程设备，IPv6流量的安全策略应包含IPv6过滤和相应的防火墙。

小型机构

可以为企业多分支机构环境采用集成多业务设计。服务包括语音、视频、安全和无线。语音服务包括IP电话、本地呼叫处理、本地语音留言以及到PSTN的VoIP网关。安全服务包括集成式防火墙、入侵防御、IPSec和准入控制。小型机构通过VPN与总部相连。应确保QoS分类和执行，以便为不同的流量类型提供适当的服务级别。应该为要求多个接收者同时接收相同流量的应用配置组播功能。可利用双栈IPv4-IPv6路由器支持IPv6流量。路由器应支持IPv6防火墙规则和过滤功能。

园区网络

园区核心

园区核心提供企业网主要区域之间的连接，包括数据中心、外部网和互联网边缘、园区、广域网（WAN）和城域网（MAN）。可使用全网格园区核心提供不同网段之间的高速冗余第三层连接。应在所有第三层设备和桌面服务中使用双栈IPv6-IPv4。

如果园区接入层使用了第二层设备，应将主分布交换机设置成主默认网关和STP根，并将冗余分布交换机设置为备用默认网关和备用根。将HSRP和RPVST+作为主默认网关和STP协议。

大楼Y

如果需要高吞吐率，可在基础设施内使用10GbE（在分布交换机之间以及接入和分布交换机之间）。如果多台接入交换机不需要共享VLAN，而且对融合的要求不高，可以使用第三层接入交换机。

大楼X

广域网

PSTN

主站点

备用站点

将WAN作为通往内部网服务器群的用户流量的主要路径。通过使用DNS和HI控制，可以独立公布应用的精确度，以及分布式应用环境的状态。应该为语音、数据和视频流量实施适当的QoS分类。要求在所有第三层设备中使用双栈IPv6-IPv4。

备用园区网络

园区核心

将分布层的无线控制器与接入层的无线接入点集成在一起。使用分布交换机之间的以太网通道技术提供冗余性和可扩展性。使用双回路接入交换机与分布层相连，以便通过提供备用路径而提高冗余性。可以考虑在接入层、分布层和核心层的第三层和/或第二层设备中使用双栈IPv4-IPv6服务。

大楼Z

备用数据中心

将备用数据中心作为备份中心，提供关键事务处理层应用的热备份系统（提供接近零RPO和RTO）和冗余非事务处理层应用的备份系统（提供12-24小时范围的RPO和RTO）。

备用数据中心设计是主数据中心的近似翻版，用于支持备用关键应用环境。当主数据中心出现故障时，备用数据中心能够迅速接管主数据中心的工作，恢复关键应用的正常运行。

将在同一VLAN中提供相似功能的服务器分组。以便实行协调一致、可管理的安全、SSL、负载均衡和监控策略。除利用双回路连接关键服务器与各接入交换机外，还应该在可用接入交换机之间进行交错主物理连接。

使用PortChannel和中继干线将多条交换机间物理链路（ISL）汇聚成一条逻辑链路。使用VSAN技术在一个物理网络中划分多个SAN，整合独立SAN和SAN交换阵列。如果设计目标允许超额配置，可使用核心一边缘技术连接多台工作组阵列交换机。

使用存储虚拟化技术进一步提高有效存储利用率和实现存储阵列集中管理。不同阵列可形成一个虚拟存储池，并以虚拟磁盘的形式服务于应用。

城域网（MAN）互联

城域以太网

使用高速（10GE）城域光网络在分布式园区和数据中心环境之间提供基于分组的透明LAN服务。

除在城域或长途环境中分布式位置之间传输语音、视频以及其它IP流量外，还可以使用SONET/SDH传输网络传送FCIP流量。可以考虑使用RPR/802.17技术为分布位置间建立高度可用的城域网核心。

使用DWDM/SONET/SDH/以太网传输网络支持高速低延迟应用，例如分布式磁盘子系统之间的同步数据复制。通用传输网络可同时支持多种协议，例如FC、GE和ESCON。

如果想使高可用性服务器群实现更高冗余性，可以将高可用性集群内的一部分服务器分配给数据中心。分配给分布式数据中心的高可用性集群称为地理集群或延伸集群。通常需要分布式节点之间具有第二层邻接。邻接指同一个VLAN（IP子网）和VSAN必须跨越分布式数据中心之间的共享传输基础设施。高可用性集群就能够跨越相距很远的多个数据中心设施。

公共VLAN

集群VLAN

阵列C

阵列D

传输网络支持延伸集群内节点之间的多通信流。可利用多个VLAN将集群内部流量与客户端流量分开。利用多个SAN阵列交换机为扩展SAN提供路径冗余。使用主机上的多路径以及SAN阵列导向器之间的I/R发挥冗余阵列优势。使用写加速来提高数据复制过程的性能。还可以利用加密保护数据传输，并利用压缩提高数据传输速度。

大型主数据中心

精简多层设计

使用内容交换机扩展服务器群。使用虚拟防火墙隔离应用环境。使用AON优化应用响应全性和通信服务，并提供对实时事务处理的可视性。将来自不同流量源的数据相互关联，并利用MARS检测安全异常。

可以在汇聚层交换机上整合提供应用和安全服务（服务模块或设备）。保证接入层设计（无论第二层或第三层）能提供可以预测的确定性行为，并允许服务器群扩充到期望的节点数。可结合使用VLAN与应用实例，以及安全服务为每个应用提供独立的运行环境。

利用VSAN技术在共享物理基础设施上建立独立SAN。使用两台不同的SAN交换机提供高可用的SAN环境。使用端口通道技术来提高路径冗余性和实现快速链路故障恢复。使用FSPF在冗余路径上提供等成本负载均衡。使用存储虚拟化将各种物理存储阵列放入同一个池中，而屏蔽各自的物理细节（阵列、转数、LUN等）。

数据中心核心

使用一个数据中心核心层支持多个汇聚模块。如果每个模块的服务器数量超过了模块的容量，可使用多个汇聚模块。将数据中心核心交换机与园区核心交换机相连，以便延伸到企业网的其余部分。可以在核心和汇聚交换机之间使用10Gb以太网链路。应该在数据中心的所有第三层设备中使用IPv6-IPv4双栈，并考虑服务器群要求，以保证IPv6流量符合防火墙和过滤策略。

扩展多层设计

设备或服务模块最好从汇聚层提供的应用服务，覆盖接入层上连接的所有服务器和业务。

将主汇聚交换机作为主默认网关和STP根。将冗余汇聚交换机作为备用默认网关和备用根。使用HSRP和RPVST+作为主默认网关和STP协议。

成对部署接入层交换机，以支持服务器双回路。在接入和汇聚交换机之间使用中继干线。每条中继干线上都支持所有接入层VLAN，以便提高服务器群的灵活性和可扩展性。

使用防火墙控制服务器各层之间的流量路径，并隔离不同的应用环境。使用内容交换机监视和控制服务器和应用的状况，并在客户端和服务器群之间，以及各服务器/应用层之间，均衡流量负载。

直接通过EtherChannel连接应用和后端网段中使用的接入交换机。使用VLAN按功能或应用类型划分服务器组。

使用VSAN技术将相互独立的阵列组合成共享基础设施，但专用阵列服务、安全性和稳定性保持不变。利用光纤通道主机总线适配器（HBA）部署与SAN交换机双回路连接的主机。

使用双阵列交换机拓扑最大程度地提高SAN环境的冗余性。建议使用通用管理VSAN，以便用阵列管理器监控整个网络环境。

刀片服务器组合

可以考虑各种可用的刀片服务器组网选项：以太网、光纤通道和Infiniband以及连接方式：集成式交换机或直通式模块。当使用集成式以太网交换时，设置一半刀片服务器的激活链路连接到交换机一而另外一半连接到交换机二。每台以太网交换机通过双回路GE通道与第三层交换机相连。可使用PrVST+加快STP收敛。使用链路状态跟踪来检测上行链路故障，并允许备用NIC在发生故障时接管任务。

如果使用直通式模块，可利用双回路把服务器与接入/边缘层交换机相连。直通式模块不但可以使光纤通道环境避免互操作问题，还允许访问高级SAN交换阵列特性。

如果使用集成式Infiniband交换机，其可以与服务器阵列交换机相连，还可以在需要这种连接时支当以太网的网关。应该将网关交换机与汇聚交换机相连，以便连接问网络。

高密度以太网集群

高密度以太网集群包含多台服务器，能够同时操作，完成复杂的计算任务。有些任务需要一定程度的并行处理，而另一些任务则需要单纯的CPU处理能力。大型以太网集群的常见应用包括大型搜索引擎站点和大型Web服务器群。图中显示的分层设计为总共1536台服务器使用了“位于机架顶部”的1RU接入交换机。

拓扑细节：
- 8台核心交换机。通过为每台交换机配置台的10GE链路与每个汇聚模块相连
- 4个汇聚模块，每个模块2台三层交换机，为接入层交换机提供10GE连接
- 每个汇聚模块连接8台接入交换机。每台接入交换机通过10GE链路与两台汇聚交换机相连
- 每台接入层交换机支持48个10/100/1000端口和2条10GE上行链路

高可用性服务器集群

高可用性服务器集群包含有多台支持业务永续或灾难恢复特性的关键业务应用服务器。这些应用包括数据库、过滤器、邮件服务器或文件服务器。一个应用集群内的节点通过集群机制互联，有两个节点时使用单播，多于两个节点时使用组播。各节点相互备份，并使用“心跳”确定节点状态。其它服务器集群共享支持高可用性集群的网络基础设施。可以使用更多VLAN和VSAN连接集群操作需要的其它NIC和HBA。由于应用数据必须向集群中的所有节点提供，因而必须共享磁盘，即磁盘不能被某个节点独享。共享磁盘或磁盘阵列还可以通过IP（iSCSI或NAS）、光纤通道（SAN）或共享SCSI访问。可用于连接数据中心LAN和SAN的传输技术包括裸光纤、DWDM、CWDM、SONET、城域以太网、EoMPLS、L2TPv3等。

4992节点以太网集群

- 每个机架组一个模块化机箱
- 8个汇聚模块——16台接入交换机
- 每个汇聚模块16条10GE下行链路
- 每台接入交换机8条10GE上行链路
- 在汇聚和接入交换机内部署第三层设备
- 8路等成本多路径ECMP
- 每台接入交换机312个GE端口
- 3.9:1超额配置率
- 每台接入交换机80Gbps容量

当需群需要与现有IP网络环境连接时，将需要核心层。模块化接入层交换机能够为机架组提供接入功能。设计的目标是减少集群中任意两个节点之间的跳数。

288节点Infiniband集群

为专门执行计算任务的服务器集群使用无阻塞设计。在为节动态/接入层和连接的每个HCA提供的无阻塞设计中，都有一条与汇聚层交换机相连的上行链路。

拓扑细节：

边缘：
- 24台交换机——每台24个端口
- 每台交换机连接12台服务器
- 通过12条上行链路与汇聚层相连

汇聚层：
- 12台交换机——每台24个端口
- 一条或多条上行链路连接到每台核心交换机

核心：
- 核心交换机数量取决于IP网络的连接需求

高可用性服务器集群

高可用性群中的节点利用现有网络基础设施与多个网络接接在一起。可使用专用网络提供“心跳”，使用公共网络执行集群间通信和客户端接入，分布式数据中心内的节点可能应位于需要第二层邻接的子网内。

VLAN X 公共网络

VLAN Y 专用网络

VSAN P

VSAN Q

高性能Infiniband集群

可以为经常执行大量计算任务，并需要低延迟、高吞吐率的应用使用Infiniband交换矩阵。为满足集群内要求，可以在边缘和汇聚层之间，以及汇聚、核心和以太网阵列之间，选择适当的超额配置率。在每两个HCA与边缘交换机相连的2:1模块拓扑中，有一条连接到汇聚层交换机的上行链路。核心交换机提供与以太网阵列的连接。可以使用Vframe来管理服务器阵列交换机的I/O虚拟化功能。

1024台服务器的拓扑细节：

边缘：
- 96台交换机——每台24个端口——每台交换机连接12台服务器
- 通过12条上行链路与汇聚层相连

汇聚层：
- 6台交换机——每台96个端口
- 4条下行链路——每台边缘交换机一条

核心：
- 交换机数量因网络连接需求的不同而不同

服务器群 VSAN

网络运行中心（NOC）

使用一个NOC VLAN支持关键管理工具，并将管理流量与客户端/服务器流量隔离开。使用NTP、SSH-2、SNMPv3、CDP和Radius/TACACS+作为基础管理协议。利用CiscoWorks LMS管理网络基础设施并监控IPv4-IPv6流量；利用思科安全管理器（CSM）控制、配置和部署防火墙、VPN和IPS安全策略；利用性能查看管理器（PVM）测量端到端应用性能；利用CS-MARS管理系统将流量关联起来，执行异常流量检测；利用网络规划解决方案（NPS）建立网络拓扑模型，用于进行故障分析，并依据设备配置、路由表、NAM和Netflow数据执行其它离线分析；利用MDS阵列管理器管理存储网络；利用Netflow和网络分析模块（NAM）执行容量规划和流量分析。

NOC VLAN/VSAN

网络规划 CS-MARS MDS阵列管理器 安全管理器 性能查看管理器 CiscoWorks LMS