第1部分

项目背景

了解目标客户的基本情况、业务发展需求和建设需求，是科学设计云计算解决方案的基础。

第 1 章

本书教学项目介绍

1.1 项目概述

目标客户是一家专注于软件开发和信息技术服务的全球性公司(简称 M 公司)。业务范围涵盖多个领域,包括但不限于企业级应用、移动应用、网站开发、数据分析以及网络安全。M 公司总部设在 A 城市。因业务发展需求,M 公司计划在 B 城市设立一个研发中心,主要业务为公司自有软件研发和 B 市本地的软件外包业务,后期计划将公司主要数据中心迁移至 B 市,届时 B 市数据中心将成为公司主要的数据中心,为全球用户提供服务。

B 市研发中心计划容纳 300 人,包含行政部门、市场部门、四个项目组、一个数据中心,其中一个项目组为涉密开发,保密级别为“机密”。

数据中心向用户提供线上业务管理服务,同时为内部员工提供多种企业应用和文件管理、测试等服务。在第一期建设中预计部署 20 台服务器,后期随着业务的不断增加,会逐步加大 B 市数据中心的建设规模。

1.2 建设需求

M 公司希望将 B 市研发中心建设成公司核心研发中心之一,以后 B 市分公司也将成为公司主要的数据服务中心,要求分公司 IT 基础架构简约、合理,并具备可扩展性。初期建设不要太多的冗余性设计,满足当前基本需求即可,但是方案要具备无限扩展的可能性,不能存在因基础架构导致整体方案无法升级和扩容的问题。

B 市研发中心因为承接了部分涉密开发,因此在数据中心建设方面不考虑托管运营商机房或租赁公有云服务,计划在公司内部自建数据中心机房,因为软件开发行业特性,经常需要频繁部署和更新多种操作系统及软件开发环境,因此公司部分技术人员建议数据中心采用云计算解决方案,但是也存在另一种顾虑是担心云计算解决方案会极大限制应用硬件

资源的使用，造成整体性能下降并导致生产力明显下降。同时云计算解决方案会导致数据高密度部署，数据的可靠性和安全性无法得到保障。

但是从别的途径了解到云计算解决方案目前在行业内的普及率较高，因此希望方案中能明确云计算解决方案在数据中心建设中的优势及缺陷，为公司的最终决策提供参考依据。

作为科技类公司，对于网络和数据的重视度极高，因此要求整体应用及网络安全可靠，网络可靠性方面，单次故障恢复时间不得超过一小时；数据方面保证少量硬件损坏不会导致数据丢失，应用和开发数据至少每日一次备份。

对于涉密项目要做到绝对的数据安全，尽可能做到涉密项目的网络物理隔离，如无法实现物理隔离，也应通过技术手段实现访问隔离。

对外业务服务器，根据实际需求要满足高并发、高负载、高可靠性的基本要求，同时还应具备一定的应对特殊高并发事件的能力。

第2部分

网络架构

网络架构是数字化解决方案中的重要组成部分，它支撑着各种应用和服务的正常运行。优秀的网络架构可以应对企业对于数字化技术变革的各种需求，而不合理的网络架构会让企业维护人员投入大量时间解决各种琐碎的小故障。

第 2 章

网络基础架构设计

通过对本章的学习，学生可以掌握关于企业网络基础架构的设计思路和标准，了解不同的网络拓扑结构的优缺点和对应的关键技术，为后期企业网络的不断升级扩展打下坚实的基础。

“新基建”政策的推出，强调了数字化、网络化、智能化等新兴技术的应用和发展。网络基础架构设计技能，可以服务“新基建”的建设，为数字化转型提供强大的技术支持。

2.1 建设需求

2.1.1 客户需求

网络基础架构是所有信息技术的根本，所有企业级应用及公司业务的交流都需要通过基础架构来进行承载，后期业务扩展也受限于基础架构的总体容量，其合理性直接决定着整个数字化解决方案后期的发展空间。

B 市研发中心一期规划为 300 名员工，后期随着业务增长将会扩大规模，具体发展计划目前尚未确定，在基础架构设计中需要保证结构合理，为后期业务增长预留一定的扩展空间。

作为科技类公司，几乎所有业务交流都需要基于数字化方案完成，M 公司计划在 B 市建设数据中心，90％的业务数据在 B 市本地进行交流和存储，因此其对内部网络性能和可靠性要求极高。

安全性方面，M 公司自身对研发成果存在一定的保密需求，同时还承接部分保密级别较高的外包项目，此类项目中，客户要求基础设施物理隔离。

初步规划的需求如下。

（1）设立一个行政部门，非研发及市场部职员均在同一个办公区，该办公区不少于 30 台工作站。

（2）设立一个市场部门，该部门需要至少有 40 台工作站。

（3）建设一个数据中心机房，在机房内部署多项 IT 服务为员工提供公司应用系统服

务，其中项目研发的测试及应用服务器均存放到数据中心机房。

（4）部署三个普通项目室，每个项目室容纳不少于 40 台工作站。

（5）部署两个大型会议室，九个小型会议室。

（6）部署一个涉密项目室，容纳不少于 50 台工作站，保密级别为“机密”。

（7）部署一个公共区域，设立 50 台高性能计算机，用于项目研发人员休息娱乐。

（8）总部和分支机构采用一条专线进行连接。

2.1.2 需求分析

网络基础架构的设计一般取决于用户的网络规模，规模的判定取决于物理空间分布，如房间、部门、大楼、园区等。

根据用户描述分析，可以得出以下几点。

（1）用户需要进行划分的空间包括：一个行政办公室、一个市场部办公室、一个公共区域、两个大型会议室、九个小型会议室、三个普通项目室、一个涉密项目室、一个数据中心机房等。

（2）数据中心机房为本地和互联网用户提供服务，还需通过专线访问总部，因此数据中心务必保证高可靠性和高安全性，避免受到来自内外网的各种网络攻击。

（3）行政部、市场部、其他办公室为独立部门，需要保证不同部门之间的独立性，另外考虑多个部门人数太多，在同一个局域网中可能会存在大量广播包，导致网络性能下降，因此不同部门之间需要一定的隔离。

（4）娱乐区域的主要功能是娱乐，对业务要求并不高，这部分计算机的安全性并不能得到有力的保证，所以这部分计算机需要与办公网络尽量隔离，满足基本业务的情况下只需要保证访问互联网即可。

（5）会议室有着大量的业务交流，因此其网络应该独立，避免被监听。

（6）每一个项目室应该是独立的网络，只需要能访问数据中心即可，其他网络都不能访问项目室网络。

（7）网络中所有终端数量不到 400 个，多个部门需要构建独立的局域网，同时还应保证各部门都可访问数据中心及互联网。

2.2 层级化网络模型

现代网络设计普遍采用了层级化网络模型。层级化网络模型将网络划分为三层，每一层都定义了特定的功能，通过各层功能的配合，可以构建一个功能完善的 IP 网，如图 2-1 所示。

（1）接入层：提供丰富的端口，负责接入工作组用户，使用户获得网络服务。接入层还可以对用户实施接入控制策略。

（2）汇聚层：通过大量的链路连接接入层设备，将接入层数据汇集起来。同时，这一层依据复杂控制策略对数据、信息等实施控制。其典型行为包括路由聚合和访问控制等。

（3）核心层：网络的骨干层，主要负责对来自汇聚层的数据进行尽可能快速的交换。

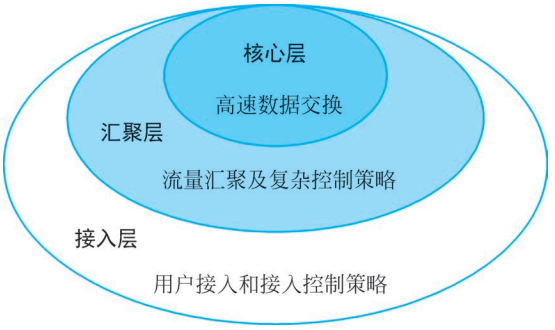

图 2-1　企业网层级化网络模型

理论上，即使目前最大规模的网络，其网络设计也不超过三个层次。小型或者中型网络设计可以根据情况合并某些层次的功能，将网络层次减少到一至二层。

2.2.1　接入层

接入层处于三层网络模型的最底层，负责接入终端用户。接入层为用户提供网络的访问接口，是整个网络的对外可见部分，也是用户与网络的连接场所。因此，接入层应具有种类丰富的大量端口，提供强大的接入能力。接入安全性也是一个必须考虑的因素。

一方面，如果接入层设备或链路出现故障，只会对设备接入的用户造成影响，影响范围较小；另一方面，接入层设备和连接数量相对较多，用户设备数量也比较多，不便于一一实现设备和链路冗余。因此，通常不考虑接入层设备和链路的冗余性。当然，如果接入层设备接入了重要用户或服务器，可以采用链路或设备冗余来提高可靠性。

另外，由于接入层是用户与网络的接入点，也是入侵者试图闯入的节点，因此可以在接入层实施安全接入控制策略，以保障网络的安全。例如，通过 802.1X 端口安全技术防止非法用户接入网络，或者采用包过滤技术过滤伪造源地址的数据包，阻止通过伪造地址方式实施的攻击。

接入层还可以实现对数据的分类和标记。接入层直接为用户提供多种多样的服务，在用户数据进入网络时，可以立即控制其流量，进行基于策略的分类，并给以适当的标记。这样网络中的其他设备就可以根据这些标记直接为这些数据提供适当的服务质量(quality of service，QoS)。

2.2.2　汇聚层

汇聚层处于三层网络模型的中间。汇聚层设备是大量接入层设备的集中点，负责汇集来自接入层的数据，并对数据和信息进行基于策略的控制。

汇聚层在位置上处于核心层与接入层的分界。面对大量来自接入层的链路，汇聚层将其数据汇聚在一起，通过少量的高速链路传递给核心层。这样可以减少昂贵的高端设备接口，提高网络转发效率。

如果不采用冗余设计，则某台汇聚层设备或某条汇聚层链路的失效将导致其下面连接的所有接入层设备用户无法访问网络。因此，汇聚层设备的可靠性较为重要。考虑到成本

因素，汇聚层往往采用中端网络设备，并采用冗余链路连接核心层和接入层设备，提高网络可靠性。必要时也可以采用设备冗余的形式提高汇聚层设备的可靠性。

汇聚层还负责实现网络中的大量复杂策略，这些策略包括路由策略、安全策略、QoS 策略等。通过在汇聚层进行适当的地址分配并实行路由聚合，可以减少核心层设备的路由数量，并以汇聚层为模块，对核心层实现网络拓扑变化的隔离。这不但可以提高转发速度，而且可以增强网络的稳定性。在汇聚层配置安全策略，可以实现高效部署和丰富的安全特性。基于接入层设备提供的数据包标记，汇聚层设备可以为数据提供丰富的 QoS。

2.2.3 核心层

核心层处于网络的中心，负责对网络中的大量数据流量进行高速交换转发。网络中各部分之间互相访问的数据流都通过汇聚层设备汇集于核心层，核心层设备以尽可能高的速度对其进行转发。

核心层的性能会影响整个网络的性能，核心层设备或链路一旦发生故障，整个网络就有面临瘫痪的危险。因此，在选择核心层设备时，不仅要求其具有强大的数据交换能力，而且要求其具有很高的可靠性。通常应选择高端网络设备作为核心层设备。这不仅是因为高端网络设备的数据处理能力强，转发速率高，也是因为高端网络设备本身通常具有高可靠性设计。高端网络设备的主要组件通常都采用冗余设计，如采用互为主备的双处理板、双交换网板、双电源等，确保设备不易宕机。而核心层链路多采用高速局域网技术，确保较高的转发速率和效率。

为了确保核心网络的可靠性，可以对核心层设备和链路实现双冗余甚至多冗余，实现网状、环型或部分网状拓扑，即对核心层设备和链路都增加一个以上的备份。一旦主用设备或主用链路出现故障，立即切换到备用设备或备用链路，确保核心层的高可靠性。

由于网络策略对网络性能不可避免会产生影响，因此在核心层不能部署过多或过于复杂的策略。通常，核心层较少采用任何降低核心层设备处理能力或增加数据包交换延迟时间的配置，并尽量避免增加核心层路由器配置的复杂程度，核心层通常只根据汇聚层提供的信息进行数据转发。

核心层对于网络中每个目的地应具备充分的可达性。核心层设备应具有足够的路由信息来转发去往网络中任意目的的数据包。这一要求与加速转发的要求是互相矛盾的，因此应在汇聚层采用适当的路由聚合策略来减少核心层路由表的大小。

2.3 层级化网络模型的优点

（1）网络结构清晰化：网络被分为具有明确功能和特性的三个层次，使原本复杂无序的网络结构显得更加清晰，易于理解和分析。

（2）便于规划和维护：清晰的结构和明确的功能特性定义使网络的规划设计更加合理，管理维护更加方便。

（3）增强网络稳定性：三个层次之间各有分工，彼此相对独立，网络变化和故障的影响范围可以降到最低，网络稳定性大大增强。