“十四五”职业教育国家规划教材

“十三五”江苏省高等学校重点教材

高等职业教育通信技术专业系列教材

数据通信与网络技术

（第二版）

主编　王文轩　汤昕怡　胡　峰

南京大学出版社

图书在版编目(CIP)数据

数据通信与网络技术 / 王文轩，汤昕怡，胡峰主编
. — 2 版. — 南京 ：南京大学出版社，2021.6
ISBN 978 - 7 - 305 - 24088 - 1

Ⅰ. ①数… Ⅱ. ①王… ②汤… ③胡… Ⅲ. ①数据通信—教材②计算机网络—教材 Ⅳ. ①TN919②TP393

中国版本图书馆 CIP 数据核字(2020)第 257461 号

出版发行 南京大学出版社
社 址 南京市汉口路 22 号 邮 编 210093
出 版 人 金鑫荣

书 名 数据通信与网络技术
主 编 王文轩 汤昕怡 胡 峰
责任编辑 吴 华 编辑热线 025 - 83596997

照 排 南京开卷文化传媒有限公司
印 刷 南京人民印刷厂有限责任公司
开 本 787×1092 1/16 印张 14.25 字数 329 千
版 次 2021 年 6 月第 2 版 2021 年 6 月第 1 次印刷
ISBN 978 - 7 - 305 - 24088 - 1
定 价 39.80 元

网 址：http://www.njupco.com
官方微博：http://weibo.com/njupco
微信服务号：njuyuexue
销售咨询热线：(025)83594756

☞ 扫码教师可免费
申请教学资源

前　言
Foreword

习近平总书记指出，信息化和经济全球化相互促进，互联网已经融入社会生活方方面面，深刻改变了人们的生产和生活方式。互联网与传统行业深入融合发展，涌现出互联网金融、交通、医疗、地图等数字经济新业态。

互联网上的服务，均是依托互联网高速生成、传送、处理信息功能而进行，这是表面的现象。透过现象看本质，互联网服务的载体是电信网的数据服务。数据服务，表现为“流量”，是与话音、短信息并列的基础电信业务。

当今的电信网与经济社会的各行各业深度融合，涌现出大量新业务、新业态，支撑经济社会高质量发展，本质是利用数据通信技术改造和提升了传统行业。一是数据通信以强大的数据传输能力，支撑传统行业数字化、网络化和智能化改造，促进传统行业转型升级、提质增效。二是数据通信以信息传送、发送、接收基本功能为载体，与传统行业深度融合，让传统行业可以网络化达成交易、提供服务，实现高效联结生产要素，迭代优化业务模式，深刻重塑行业架构。三是数据通信让距离不再成为问题，使广大人民群众可以本地化、便捷化、优质化享受各行各业发展成果。试想一下，当强劲算力和数据下沉到园区、车联网等终端，却发现园区网络根本带不动，甚至可能被“冲垮”，那所谓的“新基建”自然也就成为空谈。

互联互通的网络如何为千行万业输送养分，沿着这条线索攀爬，或许才能更清晰地判断出一个健康茁壮的智能社会，到底需要怎样的基础设施？在全球疫情与经济形势大背景下，多种技术资源的价值发挥，都必须依赖于企业数据通信能力的迭代。

一方面，5G＋AI 推动的业务多元化创新，也让网络数据传输从传统的简单数据，转变为语音通话、视频会议、即时通信、实时计算等诸多应用，不仅要求大带宽与实时性，而且对网络承载复杂异构数据的能力与可靠性也提出了挑战；另一方面，VPN 网关、流控网关、安全网关等多种产品的串形部署，使总部与分支的网络出口结构变得越来越复杂，既增加了安全风险，也让网关设备变得难以管理，增大了 IT 运维人员的工作难度。

总的来说，要让千行百业都能从“新基建”的水利设施中得到滋养，IP 网络的技术更

新，对网络流量的整体规划和质量、电信级的可靠性，以及全面互联的安全性，起到了至为关键的作用。

因此，在不久的将来，全国将有大量的企事业单位、高校急需一大批数据通信知识扎实、网络技术全面的人员，负责新型园区网络的部署、运维和管理工作。而高等院校相关专业也迫切需要一本全面介绍基于新型园区网的数据通信和网络技术的教材，其内容要随着技术革新、业务融合进行更新。为此，本书编者在长期从事一线科研和教学工作的基础上，与行业领军企业的专家合作完成相关课程的开发，在大量工程项目和产品培训中积累素材，整理为本书。

本书以“京华大学校园网络建设一期工程”的智慧校园网络为案例，贯彻全书始终，分解为四部分工作任务，包括 15 个子任务。本书内容特别适合于大中专院校的通信、物联网、人工智能和云计算等专业学生，以及所有从事网络运维管理、网络设计施工等人员。

本书授课时长建议为 64 学时，教学内容包含以理论内容为主的工作任务一和以实践操作为主的工作任务二、三、四。工作任务一立足于网络基础理论知识，内容为网络规划设计；工作任务二为局部组网与配置操作，聚焦分层体系的第二层（数据链路层或网络接口层）技术；工作任务三为网络互联与配置，定位于分层体系的第三层（网络层）技术；工作任务四涉及网络安全和其他常见应用技术。通过四部分任务的学习，学习者可以完成多区域分布、园区级网络的基本搭建，提供业务的网络支撑平台。

本书的总项目需求分析、工作任务一、工作任务三由王文轩编写，工作任务二由汤昕怡编写，工作任务四由胡峰编写。孙婷婷高工提供华为设备资料，肖明坤高工提供现网案例资源，汤昕怡负责审阅全书工作，王文轩负责统稿校正工作。

在本书编写和出版过程中，南京信息职业技术学院网络与通信学院各位教师提出了不少有益的建议，中通服咨询设计研究院有限公司提供了非常宝贵的技术文献资料，浙江华为通信技术有限公司对编写组教师提供了技术培训和业务咨询，南京大学出版社也给予了很多的支持，对此我们表示衷心的感谢！

由于成书时间紧迫和编者水平有限，书中不妥和疏漏之处在所难免，真诚地希望本书的读者能给予指正并将对本书的意见反馈给我们。

编写组

2021 年 3 月

目　录
Contents

工作任务二　局部组网与配置

工作任务三 网络互联与配置

工作任务四 网络安全与应用技术

项目需求分析

项目背景

随着学校信息化应用不断推广，师生要求尽可能方便、快速、流畅地访问校园信息平台、在线视频课程等的信息化资源，建立校园网络已经成为学校的一项基础建设工作。校园网络是利用网络设备、通信介质和适宜的网络技术与协议，以及各类系统管理软件和应用软件，将校园内计算机和各种终端设备有机地集成在一起，并用于教学、科研、学校管理、信息资源共享和远程教育等方面工作的计算机网络系统。

校园网建成后，将现代的网络引入教学各个环节，从而可以引发教学方法、教学手段、教学工具的重大革新，对提高教学质量，推动我国教育现代化的发展起着不可估量的作用。校园网络又为学校的管理者和老师提供了获取资源、协同工作的有效途径，所以校园网不仅会是学校提高管理水平、工作效率，改善教学质量的有力手段，而且是解决信息时代教育问题的基本工具。因此，我们将为现代校园网络打造一个集数据传输和备份、多媒体应用、语音传输、OA 应用和 Internet 访问等于一体的高可靠、高性能的宽带多媒体校园网。

项目名称

京华大学校园网络建设一期工程

总体目标

建设学院千兆校园网，完成一个整体规划、分步实施、充分考虑现有设备与实际资金情况的方案，建立网络中心和主干网，然后建立学校的信息管理网络、教学网络、资源网络和各应用子系统，并进行教学楼、办公楼、实训楼和图书馆的结构化布线，将网络扩展到整个校园以及位于不同地点的分校区，实现学校整体网络的全部功能，最后可通过路由器与 Internet 接入，整个项目计划投资总额在 200 万元左右。项目使用 GPON 全光网设计，高质量通信需求有保障，光路可扩展性强，十年内无需替换。所有机房光纤入户，并且通过新增汇聚设备，使机房网络管理更加便捷，且机房内网数据传输不占用校园网资源。目标要求如下：

- 网络具有传递语音、图形、图像等多种信息功能，具备性能优越的资源共享功能；

- 校园网中各终端间具有快速交换功能；
- 中心系统交换机采用虚拟网技术，具备对网络用户分类控制的功能；
- 对网络资源的访问提供完善的权限控制；
- 网络具有防止及便于捕杀病毒的功能，以保证网络使用安全；
- 校园网与 Internet 相连后具有“防火墙”过滤功能，以防止网络黑客入侵网络系统；
- 可对接入因特网的各网络用户进行权限控制。

实施要求

- 采用三层结构的分层模型，分别是核心层、接入层、分布层。这样的分层模型可以提供一个模块化的框架，使网络设计更加灵活，也让该校园网络的实施和排错更加轻松。
- 实施 VLAN 技术，实现多个网段的划分和隔离，并能灵活改变配置，使校园网在逻辑上的业务网和管理网分开，以适应教学办公环境的调整和变化，即实现移动教学办公的需求。
- 学校网络系统要确保整个计算机网络系统的可靠性、安全性，具有一定的冗余、容错能力，确保信息处理安全保密。
- 学校信息网络系统要保证实用和技术先进，便于非计算机专业人员使用。
- 提高网络节点设备交换机高性能，能够使接入层接入更多的终端设备。
- 提高网络系统的扩展能力来满足学校未来业务发展的需要。
- 提高网络主干带宽，采用主干网万兆设计，千兆到桌面以保证其高流量。
- 实现远程通信能力，借助电话网等通信手段，以最低的通信成本，方便地实现远程互联，跨越地域限制。
- 提高校园服务器集群的可靠性、冗余性，从而保证系统的安全性和数据的安全性。

设计原则

为保证网络系统建设的质量，系统的网络设计和硬件配置应遵循性价比高、扩展性强、可靠性和安全性好、易于维护的原则并具有一定的先进性。一个好的校园网系统应具有较高的吞吐能力和处理能力，网络各层均不存在阻塞状况，所以设计主要包括以下几个原则：

- 稳定性和可靠性

由于校园对整个网络系统运行的稳定性有一定要求，这就要求网络具有较高的可靠性，因此，分别在核心层和分布层均采用双备份和双线路的设计理念，实现冗余的架构，从而保证整个网络系统稳定、可靠地运行。

- 高带宽

为了支持数据、话音、视像多媒体的传输能力，所以对网络的性能要求比较高，要采用先进的网络技术，以适应大量数据和多媒体信息的传输，既要满足目前的业务需求，又要充分考虑未来的发展，为此应选用高带宽的先进技术。

● 可管理性

校园网大部分用户是学生机和教学用的服务设备，出于管理和安全方面的角度考虑，学生用户上网的带宽是应当受相应的管理和限制，避免其对学校相关信息的破坏。

● 先进性

以先进、成熟的网络通信技术进行组网，支持数据、语音和视频图像等多媒体的应用，采用交换技术代替传统的路由的技术，要注意选择性能价格比较好的技术、硬件和软件组网，保证系统的基础环境十年不落后。

● 可扩展性

考虑到教学规模将不断地扩大，对网络的提高扩展性要求比较高，并要求其能随着技术的发展不断升级。按照每年至少增长 30％用户的数据增长量，保证 2 年内的增长所需，所以校园网的易扩展性是必须仔细考虑的。然而，易扩展不仅仅指设备端口的扩展，还指网络结构的易扩展性和网络协议的易扩展性，因此，无论是选择第三层网络路由协议，还是规划第二层虚拟网的划分，都应注意其扩展能力。

● 安全性

校园网络系统应具有良好的安全性，保证数据的安全及网络使用的安全。由于该校园网络连接校园内部所有用户，安全管理十分重要。应支持 VLAN 的划分，并能在 VLAN 之间进行第三层交换时进行有效的安全控制，以保证系统的安全性，而且，采用防火墙等手段有效控制和防御网络病毒的攻击，以实现整个校园网络系统的安全可靠性。网络数据环境的安全运行十分关键，必须保证这些系统不会遭到来自网络的非法访问和恶意破坏。网络安全系统应当保证内网机密信息在存储与传输时能够保密。允许外部用户访问公共 WEB 或 FTP 服务器上的数据，但是不允许访问内部数据，如教务网等一些敏感性的数据。

区域划分

区域名	区域 ID	区域实体
骨干核心区	0 区域	三层交换机
办公行政区	1 区域	办公大楼
实验教学区	2 区域	教学楼，图书馆，实验楼，教师宿舍
学生后勤区	3 区域	体育馆，食堂，学生宿舍
内服务器区	4 区域	服务器
Internet 区	5 区域	Internet 网络

工作任务一

网络规划设计

任务描述

随着学校信息化应用不断建设，师生要求尽可能方便、快速、流畅地访问校园信息化、在线视频课程等的信息化资源，现有的校园部分区域无线网络已无法满足师生需求，故学校顺应时代发展，适时开启校园网改造建设，提升学校师生的无线网络感知，同时创新网络价值，推动学校信息化的整体发展。学校需要部署包含办公、教学、师生宿舍、图书馆在内的较为完善、高速的有线、无线网络，为学校的信息化应用起到基础设施的作用。

校园网的建设应当在设计阶段就做好规划，将师生教学、行政管理、教育应用、信息交流等功能考虑在内，定好规划分阶段逐步完善。首先要分析本项目的总体建设目标，可具体分解为：

（1）通过本项目建设，使用 GPON 全光网设计，高质量通信需求有保障，光路可扩展性强，十年内无需替换；所有机房光纤入户，并且通过新增汇聚设备，使机房网络管理更加便捷。

（2）通过无线网的部署与建设，实现办公楼、教学楼、宿舍和食堂等区域 WiFi 的无缝高速覆盖。办公区域有线、无线全千兆接入，提升用户体验，满足智慧校园建设基本要求；高质量高性能无线设备满足各种大流量并发的教学应用和办公需求。

（3）通过合理的网络规划设计，实现位于不同地点的校区之间的互联互通，实现校园网内部稳定、高速、安全的访问，能够支持五年内的网络高速访问和网络扩容需求。

有线网络与无线网络的建设目标是：建设一个高可用、高安全、高稳定、易使用、易管理、易扩展的校园有线网络与无线网络，实现无线网络的无缝、高速覆盖，为网络资源的充分利用和共享提供强有力的保障，为学校的全面信息化奠定坚实的基础。网络基础设施完善，基本形成覆盖全校的高速网络。在网络规模、技术水平、性能、稳定性和安全性方面，达到一流校园网络水平，为学校各类应用系统和公共资源服务提供一个高速、安全、可靠的基础平台。

知识技能

知识运用要求

- 掌握网络分类和拓扑结构。
- 了解网络性能指标和常见网络设备情况。

- 掌握 OSI 参考模型结构。
- 了解 TCP/IP 协议体系结构。
- 了解 IP 协议基本概念。
- 掌握 IP 地址和子网掩码计算。
- 了解园区网络的分类和构成。

技能操作要求

- 使用 Wireshark 软件完成数据的抓取、分析等操作。
- 掌握小型网络 IP 参数规划方法。
- 了解园区网络设计过程和要点。
- 了解网络规划设计的步骤和文档撰写。

1.1　网络组建基础

需求分析

网络已成为当今世界不可缺少的一部分，它使地球成为信息网络村，不受时间和空间的限制，不但能够让你随时和他人互动，还能够实现资源的共享，实现数据信息的快速传递。因此，总结网络最主要的三个用途就是：数据通信、资源共享、分布处理。数据通信是网络最基本的功能，网络为分布在不同地域的用户提供了强有力的通信手段，用户可以通过网络进行信息传送、消息发布及生产活动等等。利用这一特点，可实现将分散在不同地区的单位或部门用终端联系起来，进行统一调配、控制和管理。

要想建设和管理好网络，提供基础网络服务，就要学习和掌握开放式的网络体系结构，使不同软硬件环境、不同网络协议的网络可以互连，真正达到资源共享；同时网络要向高性能发展，追求高速、高可靠和高安全性，提供多媒体、智能化、综合性服务。

知识学习

1.1.1　网络分类与拓扑结构

微课：网络分类与拓扑结构

分析网络技术一定要了解两个方面的基本概念：网络的类型和基本拓扑结构。下面分别对这两个方面进行介绍：

一、网络分类

自诞生至今，出现过很多类型的网络，可以从不同的角度进行分类。

1. 按网络的交换方式分类

(1) 电路交换；

(2) 分组交换。

提示

还有一类交换方式称为报文交换，也属于“存储-转发”方式，分组交换是对报文交换的一种改进。报文交换是基于语义，所以传送的报文需要是一个语义整体，由于报文大小不一致，无法有效利用网络流量和适应于多任务。

电路交换方式能为任一个入网的数据通信用户提供一条临时、专用的物理信道(电路)。这条物理信道是由通路上各节点内部在空间(布线接续)或时间(时隙互换)上完成信道接续而构成的，这为信源的 DTE 与信宿的 DTE 之间建立一条信道。在信息传输期间，该信道仅为一对 DTE 用户所占用，通信结束后才释放该信道。

实现电路交换的主要设备是具有电路交换功能的交换机，它由电路交换部分和控制部分组成。电路交换部分实现主、被叫用户的连接，构成数据传输信道；控制部分的主要功能是根据主叫用户的选线信号控制交换网络完成接续。

电路交换技术的优缺点及其特点：

(1) 优点：数据传输可靠、迅速，数据不会丢失且保持原来的序列。

(2) 缺点：在某些情况下，电路空闲时的信道容易被浪费，在短时间数据传输时电路建立和拆除所用的时间得不偿失。因此，它适用于系统间要求高质量的大量数据传输的情况。

(3) 特点：在数据传送开始之前必须先设置一条专用的通路。在线路释放之前，该通路由一对用户完全占用。对于突发式的通信，电路交换效率不高。

虽然电路交换接续快、网络时延小，但是其线路利用率低，不利于实现不同类型、不同速率的数据终端设备之间的相互通信，而报文交换信息传输时延又太大，不满足许多数据通信系统的交互性的要求。分组交换技术能够较好地解决这些矛盾。

分组交换也称为包交换，它是将用户传送的数据分成一定长度的包(分组)。在每个包(分组)的前面加一个首部(报头)，其中的地址标志指明该分组发往何处，然后由分组交换机根据每个分组的地址标志，将它们转发至目的地，这一过程称为分组交换，进行分组交换的通信网称为分组交换网。

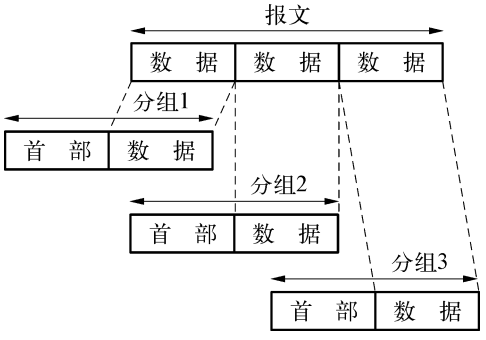


图 1-1 分组的形成

在发送端，先把较长的报文划分成较短的、固定长度的数据段。每一个数据段前面添加上报头构成分组，如图 1-1 所示。分组交换网依次把各分组发送到接收端，接收端收到分组后剥去报头重新组装成报文。

2. 按网络的作用范围分类

按照网络作用的地理范围或者网络规模进行分类，可分为局域网、城域网和广域网三

种。这三种网络可以很好地反映出不同类型的技术特征，采用不同的传输技术，形成了不同的网络服务功能。从网络层次上看，城域网是广域网和局域网的桥接区，如图1－2所示。

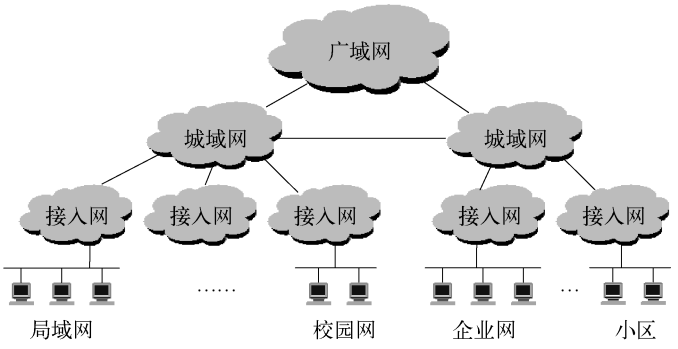


图 1－2　局域网、城域网和广域网之间的关系

(1) 局域网

局域网(LAN)是最常见的、应用最多的一种网络，大到各行各业的企业内部网络，小到千家万户的家庭网络都属于局域网，我们常说的校园网通常也是一种局域网。局域网是将一个比较小的区域内的各种通信设备互连在一起组成的网络。LAN 具有如下特点：

① 私有所属。LAN 属于个人或单位自建，如企业局域网通常只为本单位员工提供服务，其用途是完全私用，采用专门分配私有地址。关于局域网的工作原理和设备操作将在工作任务二中介绍。

② 覆盖范围小。LAN 中计算机网络设备分布的地理范围较小，一般在 10 m～10 km之间。但范围会有很大的差异，跨度比较大，可以是家庭的居住范围，可以是公司的楼层，也可以是校园的不同建筑物。

③ 结构简单，布线容易。LAN 属于个人或单位私有，网络结构相对较为简单，不用太多、太复杂的网络设备和结构就可以满足自身的网络业务需求。目前大多数 LAN 的传输介质采用比较廉价的双绞线布线，一些大公司或高校的核心网络也会采用光缆。无论选择哪种介质，因为分布范围比较小，所以布线方式较为简单，容易实现。

④ 网络速率高。目前以以太网(Ethernet)为代表的局域网技术发展迅速，最高速率已经达到了 100 Gbps，相对广域网和互联网有很大的优势，这为企业网内部大量、高速、集中性的应用提供了保证。

⑤ 误码率低。局域网的距离短，结构简单，线缆提供的带宽大，因此，通信系统的误码率比较低，一般在 10^{-11}～10^{-8}之间。

现在经常说的以太网(Ethernet)和 WLAN，便是两种应用非常广泛的局域网技术。以太网技术使用的数据被称为以太网帧(Frame)。

(2) 城域网

城域网(MAN)作用范围在局域网和下面介绍的广域网之间，通常是 10～100 km，例如作用范围是一个城市，可跨越几个街区或整个城市。城域网可以为一个或几个单位所

拥有，也可以是一种公用设施，用来将多个局域网互连。城域网要支持多种业务、多个网络协议和多级数据传输速率，在城域网内部或城域网之间要有高速链路相连接。如图1-3所示，MAN包含IP城域网与IP RAN/STN两张网络，设备分立、业务分离、管理分散。

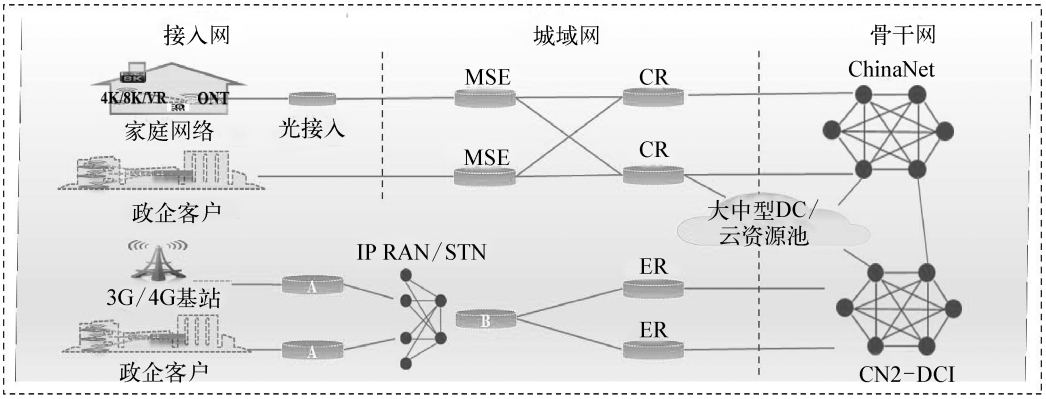


图1-3　城域网组网架构、组网方式

两种网络的性能与配置比较见表1-1所示：

表1-1　两种城域网的性能与配置比较

网络类型	承载流量	业务接入控制点	承载业务	设备类型		网管系统
IP城域网	约200 T，利用率42%，扩容门限城域内65%，城域出口80%	MSE	公众业务为主政企业务为辅	CR、MSE	网络功能与设备紧耦合	城域网管、PON网管、ITMS等
IP RAN网络	约20 T，利用率低于20%，网络轻载设计	移动业务全省集中	移动业务为主政企业务为辅	A、B、ER		IP RAN网管

(3) 广域网

广域网(WAN)是规模最大的一种计算机网络，分布的地理范围非常广，如一个或多个城市，多个国家甚至遍布全球。WAN是互联网的核心部分，由不同ISP组建，其任务是通过长距离发送主机的数据。广域网的主要内容将在工作任务三中讨论。

二、网络拓扑结构

网络的拓扑结构是指一个网络的通信链路和节点构成的几何布局图。在选择拓扑结构时，要根据不同设备承担的角色、各节点设备工作性能要求、安装/维护/升级的难易程度、通信介质故障时受影响的情况等各方面进行考虑。

根据实际应用需要，网络可根据需要连成多种拓扑结构，典型的拓扑结构有6种：总线型、环型、星型、树型、网状和全网状，如图1-4所示。从拓扑结构来看，网络内部的主机、终端、交换机都可以称为节点。

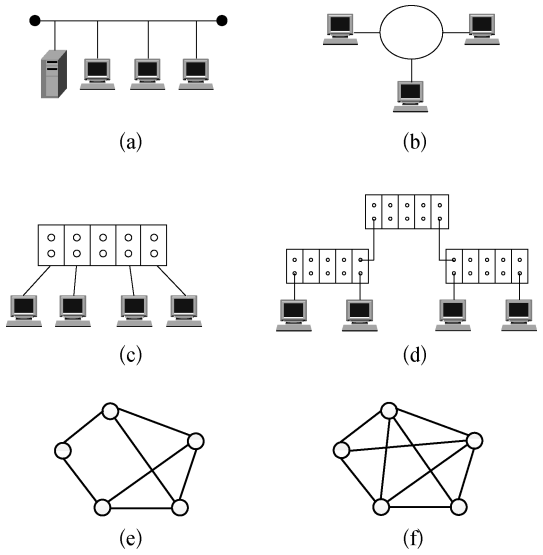


图 1－4　几种典型的网络拓扑结构

1. 总线型拓扑结构

总线结构通常采用广播式信道，即网上的一个节点（主机）发信时，其他节点均能接收总线上的信息，如图 1－4(a)所示。

这种结构具有费用低、数据端用户入网灵活、站点或某个端用户失效不影响其他站点或端用户通信的优点。缺点是一次仅一个端用户能发送数据，其他端用户必须等待到获得发送权；媒体访问获取机制较复杂，维护难，分支节点故障查找难。尽管有上述一些缺点，但由于布线要求简单，扩充容易，端用户失效、增删不影响全网工作，所以是 LAN 技术中使用最普遍的一种。

2. 环型拓扑结构

环型结构采用点到点通信，即一个网络节点将信号沿一定方向传送到下一个网络节点，在环内依次高速传输，如图 1－4(b)所示。为了可靠运行，也常使用双环结构。

环型拓扑结构的优点：由于两个结点间只有唯一的通路，因此，大大简化了路径选择的控制；网络中所需的电缆短，不需要接线盒，价格便宜；扩充方便，增减结点容易。缺点是如果环的某一点断开，则环上所有端点间的通信便会终止；为保证环的正常工作，需要较复杂的环维护处理，环结点的加入和撤出过程都比较复杂。

3. 星型拓扑结构

如图 1－4(c)所示，星型结构中有一个中心节点，执行数据交换网络控制功能。这种结构易于实现故障隔离和定位，但它存在瓶颈问题，一旦中心节点出现故障，将导致网络失效。因此，为了增强网络可靠性，应采用容错系统，设立热备用中心节点。

星型拓扑结构是目前应用最广、实用性最好的一种拓扑结构，主要因为它容易实现网络的扩展，现在大量应用于以太局域网中。

4. 树型拓扑结构

树型结构的连接方法像树一样从顶部开始向下逐步分层分叉，有时也称其为层型结

构，如图 1－4(d)所示。这种结构中执行网络控制功能的节点常处于树的顶点，在树枝上很容易增加节点，扩大网络，但同样存在瓶颈问题。

5. 网状/全网状拓扑结构

网状结构的特点是节点的用户数据可以选择多条路由通过网络，网络的可靠性高，但网络结构协议复杂，如图 1－4(e)所示。目前大多数复杂交换网都采用这种结构。当网络节点为交换中心时，常将交换中心互连成全连通网，如图 1－4(f)所示。

1.1.2 网络的性能指标

各种网络系统都有各自的技术性能指标，互不相同。衡量任何网络性能的优劣都是以有效性和可靠性为基础的，数据通信系统也不例外，它也有表示有效性和可靠性的指标。

一、有效性指标

1. 码元传输速率 R_B

数字通信系统通常传输的是以 0、1 表示的脉冲序列，每一个表示 0 或 1 的脉冲称为一个码元。图 1－5 所示为二进制与四进制码元。

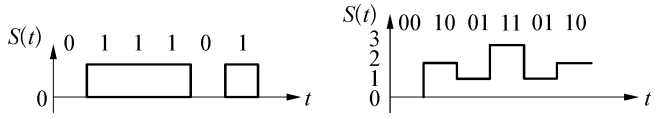


图 1－5 二进制码元与四进制码元比较

码元传输速率 R_B 也称为波特率、传码率，是指在单位时间内传输的码元数，单位为波特(Baud)，常用符号“B”表示。这里的码元可以是二进制的，也可以是多进制的。

$$R_B = 1/T_b \tag{1-1}$$

其中，T_b 为信号码元持续时间(时间长度、码元周期)，单位为秒(s)。在图 1－5 中，虽然进制数不同，但 T_b 相同，因此，码元传输速率 R_B 相同。

2. 信息传输速率 R_b

信息传输速率 R_b 简称传信率，又称比特率，是每秒传输二进制码元的个数或比特数。单位为比特每秒(bit/s、bps 或 b/s)，也使用千比特每秒(kb/s)、兆比特每秒(Mb/s)或吉比特每秒(Gb/s)。传码率 R_B 和传信率 R_b 的关系如下：

$$R_b = R_B \log_b M \tag{1-2}$$

3. 频带利用率 η

数据信号的传输需要一定的频带。两个数据传输系统的传信率相同，它们的通信效率也可能不同。衡量数据传输系统有效性的指标是单位频带内的传输速率，即频带利用率 η。

$$\eta = R_B/B \text{ 或 } \eta = R_b/B \tag{1-3}$$

其中，B 是带宽值。在相同传码率下，多进制比二进制的传信率高，频带利用率高，这

就是信道传输采用多进制的原因之一。

二、可靠性指标

由于数据信号在传输过程中不可避免地会受到噪声干扰，信道的不理想也会带来信号的畸变，当噪声干扰和信号畸变达到一定程度时就可能导致接收的差错。衡量数字通信系统可靠性的指标是差错率，常用误码率 P_e 和误信率 P_b 表示。

$$P_e = \frac{\text{接收差错码元数}}{\text{发送总码元数}} \tag{1-4}$$

$$P_b = \frac{\text{接收差错比特数}}{\text{发送总比特数}} \tag{1-5}$$

差错率是一个统计平均值，因此，在测量或统计时，总的比特（码元）数要达到一定的数量，否则得出的结果将失去意义。

差错率的大小取决于信道的特性、质量及系统噪声等因素，不同的通信系统对差错率的要求不同。差错率越低，数字通信系统的可靠性就越高，质量越好。

三、带宽指标

“带宽”（bandwidth）本来是指信号具有的频带宽度，单位是赫、千赫、兆赫、吉赫（Hz、kHz、MHz、GHz）。现在“带宽”是数字信道所能传送的“最高数据率”的同义语，单位是比特每秒（b/s）。正是因为带宽代表数字信号的发送速率，因此，带宽有时也称为吞吐量（throughput）。

吞吐量表示在单位时间内通过某个网络（或信道、接口）的数据量。吞吐量更经常地用于对现实世界中的网络的一种测量，以便知道实际上到底有多少数据量能够通过网络。吞吐量受网络的带宽或网络的额定速率的限制，常用每秒发送的比特数（或字节数、帧数）来表示。

四、时延指标

时延（delay）是指一个报文或分组从一个网络的一端传送到另一端所需的时间，是衡量网络性能的重要参数。一般时延由以下三个部分组成：

1. 发送时延

也称为传输时延。发送时延是结点在发送数据时使数据块从结点进入到传输媒体所需要的时间，也就是从数据块的第一个比特开始发送算起，到最后一个比特发送结束所需的时间。该值的计算公式是：

$$\text{发送时延} = \frac{\text{数据块长度}}{\text{信道带宽}} \tag{1-6}$$

信道带宽就是数据在信道上的发送速率，也称为数据在信道上的传输速率。

2. 传播时延

传播时延是电磁波在信道中传播一定的距离而花费的时间，传播时延的计算公式：

$$传播时延=\frac{信道长度}{电磁波在信道上的传播速率} \tag{1-7}$$

电磁波在自由空间的传播速率是光速，即 3.0×10^5 km/s。电磁波在网络传输媒体中的传播速率比在自由空间要略低一些：在铜线电缆中的传播速率约为 2.5×10^5 km/s，在光纤中的传播速率约为 2.0×10^5 km/s。

从以上讨论中可以得到，信号传输时延（发送时延）和电磁波传播时延是两个完全不同的概念，因此，不能将这两个时延概念弄混。

3. 处理时延

数据在交换结点缓存队列中排队要经历一定的时延，因此，也称为排队时延。处理时延的长短往往取决于网络中的通信量。当网络通信量很大时，会发生队列溢出使分组丢失。

端到端的总时延就是以上三种时延之和，如图 1-6 所示：

$$总时延=发送时延+传播时延+处理时延 \tag{1-8}$$

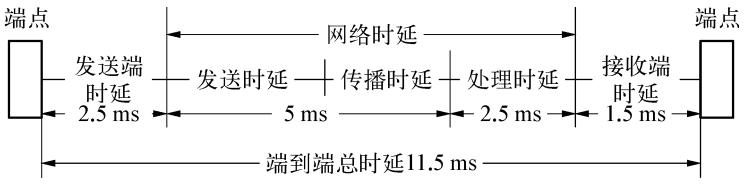


图 1-6　网络总时延的组成

5G 网络是由特定业务场景的驱动而诞生的，比如无人驾驶和远程医疗等均需要网络端到端时延达到一个很低的水平。5G 时代的传输专线必须具备低时延的特性，URLLC 业务端到端时延小于 1 ms，eMBB 业务端到端时延小于 10 ms。目前我国的 4G 传输专线端到端理想时延是 10 ms 左右，端到端典型时延是 50～100 ms 之间，这意味着 5G 传输专线的端到端时延将缩短为 4G 的 1/10，这对底层的承载网络提出了前所未有的挑战。于是，5G 传输专线低时延特性的研究工作实属重中之重。

提示

经常听到的诸如“在高速链路（或高带宽链路）上，比特流传输速度更快”和“光纤信道的传输速率高”之类的说法都是错误的。

通常所说的“光纤的带宽大，速率高”是指向光纤信道发送数据的速率很高，发送的数据块从第一个比特到最后一个比特的时间很短，即光纤介质的发送时延（传输时延）很小。但光纤信道的传播时延实际上比铜线的传播时延略高一点，经过测量得知，光在光纤中的传播速率和电磁波在铜线（如 6 类线）中的传播速率分别为 20.5 万公里每秒和 23.1 万公里每秒。

1.1.3　网络常见设备

一、以太网卡

网络接口卡(NIC)通常也简称为“网卡”,它是计算机、交换机、路由器等网络设备与外部网络世界相连的关键部件。特定的网卡服务于特定的网络,如以太网、令牌环、FDDI或无线局域网。本书所提及的网卡一般是指以太网接口卡,简称以太网卡或以太卡。

一般来说,终端至少会安装一个 NIC,网络设备(如路由器)会有多个 NIC。每个 NIC 都有一个全网唯一的地址用于被识别,在以太网中该地址称为 MAC 地址。MAC 地址也叫作网卡地址、硬件地址或物理地址,因为它通常是由网卡生产厂家烧入网卡的 EPROM,这是传输数据时真正标识发出和接收数据的主机的地址。MAC 地址由 48 比特(6 字节)的数字组成,0～23 位是由厂家自己分配,24～47 位叫作组织唯一标志符,是识别 LAN 节点的表示。其中第 46 位是全局地址标志位,第 47 位是组播地址标志位。

终端和局域网通过 NIC 的通信过程见图 1－7,可以总结得出 NIC 需要完成的具体工作任务有以下几点:

① 对数据链路层的数据帧进行封装和解封装;

② 实现终端内部的并行通信到局域网线路上的串行通信的转换;

③ 实现以太网访问控制方法;

④ 实现信道编码与信道译码。

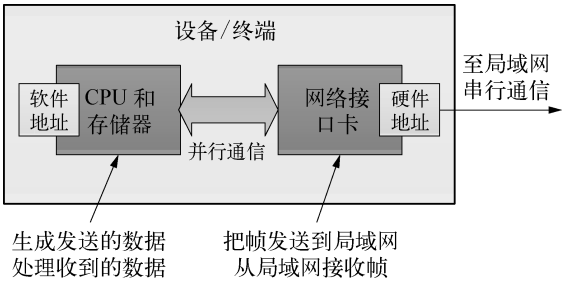


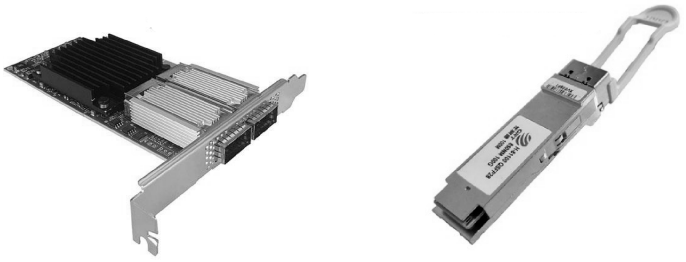
图 1－7　NIC 通信过程示意图

在 1990 年代和 2000 年代初期,网卡一般用于计算机上,直到后来才慢慢被用在服务器和工作站上,在此期间因为无线技术的成熟化以及无线网络的普及化,无线网卡也逐渐被广泛应用在计算机上,不过由于连接的可靠性,有线网卡在无需移动的网络设备中仍然是主导。近年来,行业也一直不断地推出新的网卡,以满足不同的以太网需求,如百兆网卡、千兆网卡、万兆网卡以及 25G 网卡等。

数据中心正以前所未有的速度扩展,推动了服务器与交换机之间连接趋于更高带宽的发展。如今,数据中心正从 10G 向 100G 升级,其中 25G 网卡作为连接 25G 服务器与 100G 交换机的中间设备已然成了主流。但考虑到数据中心的带宽增长迅速及数据中心硬件升级周期为两年,以太网发展速度会比预期的要快。随着数据中心趋于 400G 发展,服务器与交换机之间的连接将趋于 100G 发展,100G 网卡将在下一代数据中心中扮演着

不可或缺的角色，目前 Intel、Mellanox 等供应商已相继推出了 100G 网卡。

由于市场对 100G 网卡的需求增长将推动其他网络设备的需求，如用于 100G 服务器上的 100G 光模块。如今市面上大多数光模块供应商可提供 CXP/CFP/CFP4/QSFP28 不同封装的 100G 光模块。



(a)　　(b)

图 1－8　(a) 100G 网卡，(b) 100G QSFP28 光模块

提示

现如今随着 5G 网络的正式商用，运营商需要更高的带宽实现大流量数据的应用，为 100G 网卡的应用铺平了道路，此时网络部署时所需的 100G 光模块和 400G 网络交换机也成了必不可少的网络设备之一。相信在 5G 网络时代，100G 网卡将逐渐普及，并将引领光通信市场持续增长。

二、以太网交换机

目前除了以太网交换机外，其他类型的交换机已被市场机制所淘汰，因此，以太网交换机与局域网交换机几乎成了同一个概念，本书中的交换机都是指以太网交换机。

如图 1－9 所示，交换机会对通过传输介质进入其端口的每一个帧都进行转发操作，操作可分为 3 种：泛洪(Flooding)、转发(Forwarding)、丢弃(Discarding)。

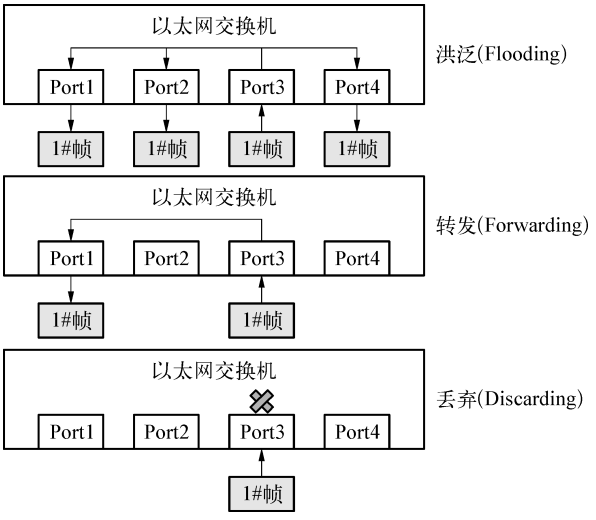


图 1－9　交换机对帧的三种转发操作

① 泛洪：交换机把从某一端口进来的帧通过所有其他的端口转发出去（“其他端口”是指除了这个帧进入交换机的那个端口以外的所有端口）。泛洪操作是一种点到多点的转发行为。

② 转发：交换机把从某一端口进来的帧通过另一个端口转发出去。这里的转发操作是一种点到点的转发行为。

③ 丢弃：交换机把从某一端口进来的帧直接丢弃。丢弃操作其实就是不进行转发。

如果按照工作模式分，以太网交换机可以分为直通、存储转发和碎片隔离三种类型。

① 直通：直通方式的以太网交换机是在各端口间纵横交叉的线路矩阵电话交换机。其基本原理是它在输入端口检测到一个数据帧时，只接受并检查该帧的帧首，获取帧的目的 MAC 地址，通过查找转发表找到对应端口，在输入和输出交叉处接通，把数据直通到相应的端口，实现交换功能。

由于不需要存储，延迟非常小、交换速度快，这是它的优点。它的缺点是因为没有保存完整的数据帧，故无法检测错误，并且只能连接速率相同的端口，容易丢包。

② 存储转发：存储转发方式是数据通信领域内应用最为广泛的方式。它把输入端口的数据帧先存储，然后进行 CRC（循环冗余码校验）检错，检错通过后才取出目的 MAC 地址，查找转发表从对应端口输出。

存储转发方式由于存在数据处理而时延大，但能够对数据帧进行差错检测，有效地改善网络性能。尤其是它可以支持不同速度的端口间的转换，保持高速端口与低速端口间的协同工作。

③ 碎片隔离：这是介于前两者之间的一种解决方案。它检查数据帧的长度是否小于 64 字节，如果小于 64 字节，说明是无效帧应该丢弃；如果大于 64 字节，则转发该帧。这种方式不提供数据校验，它的速度介于前两者之间。

提示

交换机其实有二层交换机、三层交换机和四层交换机几种类型。这里我们简单比较一下常用的二层和三层交换机的区别：

二层交换机发展比较成熟，可以识别 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中，常用于小型局域网或网段之间相连。

三层交换机具有部分路由器功能，最重要的目的是加快大型局域网内部的数据交换，能够做到“一次路由，多次转发”。对于数据包转发等规律性的过程由硬件高速实现，而如路由信息更新、路由表维护、路由计算、路由确定等功能由软件实现。三层交换技术就是“二层交换＋三层转发”。在校园网、城域网中，骨干网、城域网骨干、汇聚层都有三层交换机的用武之地，尤其是核心骨干网一定要用三层交换机。

三、中大型路由器

在园区网、地区网乃至整个互联网的研究领域中，路由器技术始终处于核心地位，其

发展历程和方向成为整个互联网研究的一个缩影。由于未来网络仍然使用 IP 协议来进行路由(或基于该路由技术的某些改进),路由器将扮演着重要的角色。

路由器的核心作用是实现网络互连,在不同网络之间转发数据单元。为实现在不同网络间转发数据单元的功能,路由器必须具备以下条件。首先,路由器上多个三层接口要连接在不同的网络上,每个三层接口连接到一个逻辑网段。这里面所说的三层接口可以是物理接口,也可以是各种逻辑接口或子接口。在实际组网中确实存在只有一个接口的情况,这种方式我们称之为单臂路由,单臂路由应用很少。其次,路由器必须具有存储、转发、寻径功能。

下面将路由器需要具备的主要功能解释如下:

① 路由功能(寻径功能):包括路由表的建立、维护和查找。

② 交换功能:路由器的交换功能与以太网交换机执行的交换功能不同,路由器的交换功能是指在网络之间转发分组数据的过程,涉及从接收接口收到数据帧,解封装,对数据包做相应处理,根据目的网络查找路由表,决定转发接口。

③ 隔离广播、指定访问规则:路由器阻止广播的通过,并且可以设置访问控制列表(ACL)对流量进行控制。

④ 子网间的速率匹配:路由器有多个接口,不同接口具有不同的速率,路由器需要利用缓存及流控协议进行速率适配。

对于不同规模的网络,路由器作用的侧重点有所不同:

在骨干网上,路由器的主要作用是路由选择。骨干网上的路由器,必须知道到达所有下层网络的路径。这需要维护庞大的路由表,并对连接状态的变化做出尽可能迅速的反应。路由器的故障将会导致严重的信息传输问题。

在地区网中,路由器的主要作用是网络连接和路由选择,即连接下层各个基层网络单位——园区网,同时,负责下层网络之间的数据转发。

在园区网内部,路由器的主要作用是分隔子网。早期的互联网基层单位是局域网,其中所有主机处于同一个逻辑网络中。随着网络规模的不断扩大,局域网演变成以高速骨干和路由器连接的多个子网所组成的园区网。在其中,各个子网在逻辑上独立,而路由器就是唯一能够分隔它们的设备,它负责子网间的报文转发和广播隔离,在边界上的路由器则负责与上层网络的连接。

任务布置

● 通信的概念大家并不陌生,在人类社会的发展过程中,通信就一直存在。对于生活在信息时代的我们,通信的必要性和重要性是不言而喻的。

通信系统的基本组成有哪些部分?请用图画描述通信系统的一般架构。

● 网络技术是计算机技术和数据通信技术结合而成的。数据通信是依照一定的通信协议,利用数据传输技术在两个终端之间传递数据信息的一种通信方式和通信业务,是继电报、电话之后的第三种通信业务。

经过多年的发展,数据通信网络的典型组网模型被归纳为三种,请简单叙述。

● 在网络通信中，传输媒体是能够被用于从一点到另一点传播信号的任何物质，例如，光纤、电缆、水和空气等。我们一般会将传输媒体按照是否具有传输导向性分为导向性介质和非导向性介质，即有线介质和无线介质。

常用的传输媒体有哪几种？各有何特点？各自用途是什么？光缆具有怎样的物理结构、传输特性和抗干扰性？

1.2　网络协议架构

需求分析

数据通信系统中非常关键的一个部分是网络协议，所谓协议，就是为了使网络中的不同设备能进行数据通信而预先制定的一整套通信各方相互了解和共同遵守的格式和约定，是一系列规则和约定的规范性描述。协议定义了网络设备之间如何进行信息交换，是网络通信的基础。只有遵从相同的协议，网络设备之间才能够通信。如果一台设备不支持用于网络互联的协议，它就无法与其他设备进行通信。

以电话为例，必须首先规定好信号的传输方式、什么信号表示发起呼叫、什么信号表示呼叫结束、出了错误怎么办、怎样表示呼叫人的号码等，这种预先规定好的格式及约定就是协议。

协议分为两类：一类是各网络设备厂商自己定义的协议，称为私有协议；另一类是专门的标准机构定义的协议，称为开放式协议。私有协议只有厂商自己的设备支持，无法和其他厂商的设备互通，所以在平时应用中，各厂商会尽量遵循开放式协议，但单一、巨大的协议会加大网络设计难度，同时也不利于分析及查找问题。因此，网络模型中引入分层的概念。分层模型是一种用于开发网络的设计方法，将通信问题划分为几个小的问题（层次），每个问题对应一个层次。

知识学习

1.2.1　网络协议和标准化组织

在全球的互联网活动中，存在着各种各样的组织，其中有许多组织扮演着重要角色，对全球网络的互联互通、正常运行和迅速发展起着关键的重要作用，缺乏国际标准将会使技术的发展处于比较混乱的状态。这里我们简要介绍几个组织机构，后面会分别学习到它们的标准：

（1）ISO（国际标准化组织）：成立于 1947 年 2 月 23 日，是制定全世界工商业国际标准的各国国家标准机构代表的国际标准建立机构，总部设于瑞士日内瓦，成员包括 162 个会员国。该组织自我定义为非政府组织，参加者包括各会员国的国家标准机构和主要公司。ISO

制订了 OSI/RM，成为研究和制订新一代计算机网络标准的基础。各种符合 OSI/RM 与协议标准的远程计算机网络、局部计算机网络与城市地区计算机网络开始广泛应用。

(2) EIA/TIA(美国电子/电信工业协会)：EIA 创建于 1924 年，广泛代表了设计生产电子元件、部件、通信系统和设备的制造商以及工业界、政府和用户的利益。TIA 成员包括为美国和世界各地提供通信和信息技术产品、系统和专业技术服务的大小公司。TIA 与 EIA 有着广泛而密切的联系，EIA/TIA 的布线标准中规定了两种双绞线的线序 568A 与 568B，还制定了其他网络线缆标准，如 RS－232、HSSI 等。

(3) IEEE(电子电气工程师协会)：是一个国际性的电子技术与信息科学工程师的协会，是世界上最大的专业技术组织之一(成员人数)。该组织在太空、计算机、电信、生物医学、电力及消费性电子产品等领域中都是主要的权威。其中比较出名的是 IEEE 802 委员会，它成立于 1980 年 2 月，它的任务是制定局域网的国际标准 802.X，取得了显著的成绩。

(4) IETF(Internet 工程任务组)：成立于 1985 年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定，当前绝大多数国际互联网技术标准出自 IETF。IETF 产生两种文件，一个叫作 Internet Draft，即“互联网草案”，第二个是叫 RFC，叫意见征求书或请求注解文件，只有部分 RFC 文档成为标准。IETF 的实际工作大部分是在其工作组(Working Group)中完成的。这些工作组又根据主题的不同划分到若干个领域(Area)，如路由、传输和网络安全等。

(5) ITU－T(国际电信联盟电信标准部门)：该机构创建于 1993 年，前身是国际电报电话咨询委员会(CCITT)。定义了广域网连接的电信网络的标准，如 X.25、V.24、Frame Relay 等。


微课：OSI 参考模型

1.2.2 OSI 参考模型

OSI/RM 参考模型就是基于 ISO 的建议，简称 OSI 模型。OSI 模型有 7 层，结构如图 1－10 所示。由低层至高层分别是：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。其分层原则为根据不同层次的抽象的分层，每一层都有特定的功能，并且上一层利用下一层所提供的服务。

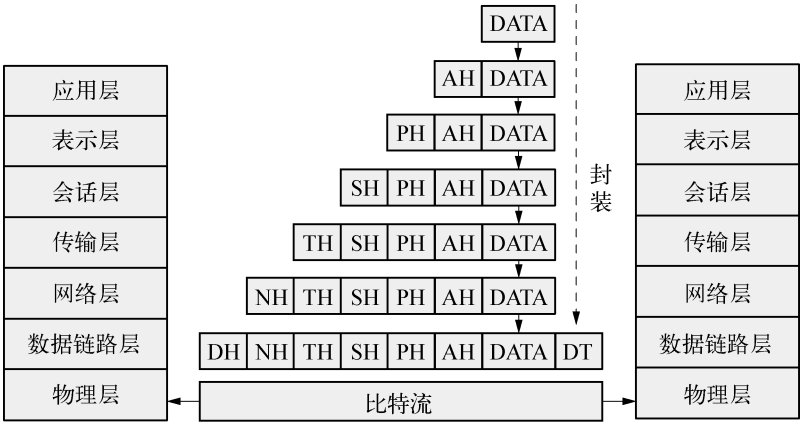


图 1－10　OSI 参考模型中的数据封装过程

应该指出，OSI/RM 只是提供了一个抽象的体系结构，从而根据它研究各项标准，并在这些标准的基础上设计系统。

一、分层功能

(1) 物理层：主要讨论在通信线路上比特流的传输问题。这一层协议描述传输媒质的电气、机械、功能和过程的特性。其典型的设计问题有：信号的发送电平、码元宽度、线路码型、物理连接器插脚的数量、插脚的功能、物理拓扑结构、物理连接的建立和终止、传输方式等。

(2) 数据链路层：主要讨论在数据链路上帧流的传输问题。这一层协议的内容包括：帧的格式，帧的类型，比特填充技术，数据链路的建立和终止信息流量控制，差错控制，向物理层报告一个不可恢复的错误等。这一层协议的目的是保障在相邻的站与节点或节点与节点之间正确地、有次序、有节奏地传输数据帧。

(3) 网络层：主要处理分组在网络中的传输。这一层协议的功能是：路由选择、数据交换，网络连接的建立和终止，一个给定的数据链路上网络连接的复用，根据从数据链路层来的错误报告而进行的错误检测和恢复，分组的排序，信息流的控制等。

(4) 传输层：是第一个端到端的层次，把传输层的地址变换为网络层的地址。主要功能是：运输连接的建立和终止，在网络连接上对运输连接进行多路复用，端-端的次序控制，信息流控制，错误的检测和恢复等。

提示

上面介绍的四层功能可以用邮政通信来类比。传输层相当于用户部门的收发室，它们负责本单位各办公室信件的登记和收发工作，然后交邮局投送，而网络层以下各层的功能相当于邮局，尽管邮局之间有一套规章制度来确保信件正确、安全地投送，但难免在个别情况下会出错，所以收发用户之间可经常核对流水号，如发现信件丢失就向邮局查询。

(5) 会话层：在两台计算机间建立、管理和终止通信来完成对话。在建立会话时核实双方身份是否有权参加会话；确定何方支付通信费用；双方在各种选择功能方面(如全双工还是半双工通信)取得一致；在会话建立以后，需要对进程间的对话进行管理与控制。

(6) 表示层：解决格式和数据表示的差别，从而为应用层提供一个一致的数据格式，如文本压缩、数据加密、字符编码的转换，从而使字符、格式等有差异的设备之间相互通信。

(7) 应用层：与提供网络服务相关，这些服务包括文件传送、打印服务、数据库服务、电子邮件等。

从七层的功能可见，1～3 层主要是完成数据交换和数据传输，称之为网络低层，即通信子网；5～7 层主要是完成信息处理服务的功能，称之为网络高层；低层与高层之间由第 4 层衔接。数据通信网只有物理层、数据链路层和网络层，我们主要研究这三层。

二、数据封装

如图 1－10 所示，在 OSI 参考模型中，当一台主机需要传送用户的数据(DATA)时，数据首先通过应用层的接口进入应用层。在应用层，用户的数据被加上应用层的首部(AH)，形成应用层协议数据单元(PDU)，然后被递交到下一层——表示层。表示层并不“关心”上层——应用层的数据格式，而是把整个应用层递交的数据包看成是一个整体进行封装，即加上表示层的首部(PH)，然后，递交到下层——会话层。

同样，会话层、传输层、网络层、数据链路层也都要分别给上层递交下来的数据加上自己的首部：会话层首部(SH)、传输层首部(TH)、网络层首部(NH)和数据链路层首部(DH)。其中，数据链路层还要加上尾部(DT)，形成最终的一帧数据。

当一帧数据通过物理层传送到目标主机的物理层时，该主机的物理层把它递交到上层——数据链路层。数据链路层负责去掉数据帧的帧头部 DH 和尾部 DT(同时还进行数据校验)。如果数据没有出错，则递交到网络层。同样，网络层、传输层、会话层、表示层、应用层也要做类似的工作。最终，原始数据被递交到目标主机的具体应用程序中。

1.2.3 TCP/IP 协议体系结构


微课：TCP/IP 体系结构

TCP/IP 技术得到了众多厂商的支持，不久就有了很多分散的网络，所有这些单个的 TCP/IP 网络都互联起来称为因特网(Internet)。基于 TCP/IP 协议的因特网已逐步发展成为当今世界上规模最大、拥有用户和资源最多的一个超大型计算机网络，TCP/IP 协议也因此成为事实上的工业标准。IP 网络正逐步成为当代乃至未来计算机网络的主流。

与 OSI 参考模型一样，TCP/IP 协议体系结构也分为不同的层次，每一层负责不同的通信功能。但是，TCP/IP 体系结构简化了层次设计，将原来的七层模型合并为四层协议的体系结构，自顶向下分别是应用层、传输层、网络层和网络接口层，没有 OSI 参考模型的会话层和表示层。应用层包含了 OSI 参考模型所有高层协议。从图 1－11 中可以看出，TCP/IP 协议体系与 OSI 参考模型有清晰的对应关系，覆盖了 OSI 参考模型的所有层次。

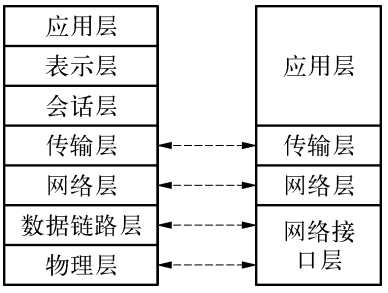


图 1－11　TCP/IP 体系结构与 OSI 参考模型比较

一、TCP/IP 协议族

TCP/IP 协议族是由不同网络层次的不同协议组成的。TCP/IP 协议族中的每层协议如图 1－12 所示。

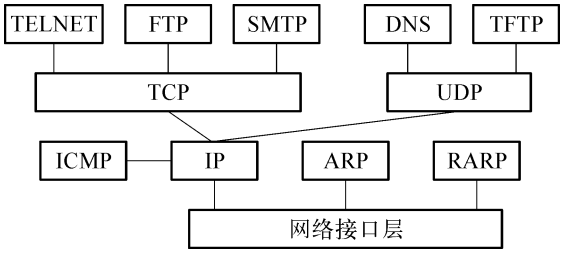


图 1－12　TCP/IP 协议族

网络接口层涉及在通信信道上传输的原始比特流，它实现传输数据所需要的机械、电气、功能性及过程等手段，提供检错、纠错、同步等措施，使之对网络层显现一条无错线路，并且进行流量调控。网络层检查网络拓扑，以决定传输报文的最佳路由，执行数据转发。其关键问题是确定数据包从源端到目的端如何选择路由。网络层的主要协议有 IP(网际协议)、ICMP(互联网控制报文协议)、IGMP(互联网组管理协议)和 ARP(地址解析协议)等。

传输层的基本功能是为两台主机间的应用程序提供端到端的通信。传输层从应用层接收数据，并且在必要的时候把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误。传输层的主要协议有 TCP(传输控制协议)、UDP(用户数据报协议)。

应用层负责处理特定的应用程序细节，显示接收到的信息，把用户的数据发送到低层，为应用软件提供网络接口。应用层包含大量常用的应用程序，例如 HTTP(超文本传输协议)、Telnet(远程登录)、FTP(文件传送协议)等。

二、数据封装

同 OSI 参考模型数据封装过程一样，TCP/IP 协议在报文转发过程中，封装和去封装也发生在各层之间。如图 1－13 所示的封装过程，对等层之间互相交互的数据被称为 PDU(协议数据单元)。

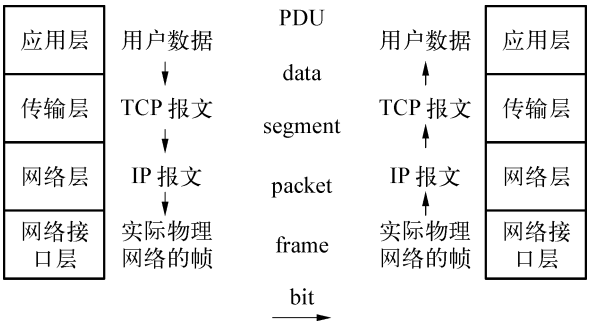


图 1－13　TCP/IP 数据封装过程

PDU 在不同层有不同的名称。如在传输层中，在上层数据中加入 TCP 报头后得到的 PDU 被称为数据段(segment)；数据段被传递到网络层，网络层添加 IP 报头得到的 PDU 被称为数据包(packet)；数据包被传递到网络接口层，封装网络接口层报头得到的 PDU 被称为数据帧(frame)；最后，帧被转换为比特(bit)，通过网络介质传输。后面对传输层和网络层的数据都统一称为报文。

1.2.4 TCP 和 UDP 协议

传输层主要提供两种服务，一种是面向连接的服务，由 TCP 协议实现，是一种可靠的服务；一种是无连接的服务，由 UDP 协议实现，是一种不可靠的服务。

一、TCP 协议

TCP 是一种可靠的、面向连接的字节流服务。源主机在传送数据前需要先和目标主机建立连接，在此连接上，被编号的数据段按序收发。同时，要求对每个数据段进行确认，保证了可靠性。如果在指定的时间内没有收到目标主机对所发数据段的确认，源主机将再次发送该数据段。

TCP 报文分为两部分，前面是报头，后面是数据。其中报头的前 20 个字节格式是固定的，后面是可能的选项，整个报头最多有 60 个字节。TCP 报文格式如图 1－14 所示。

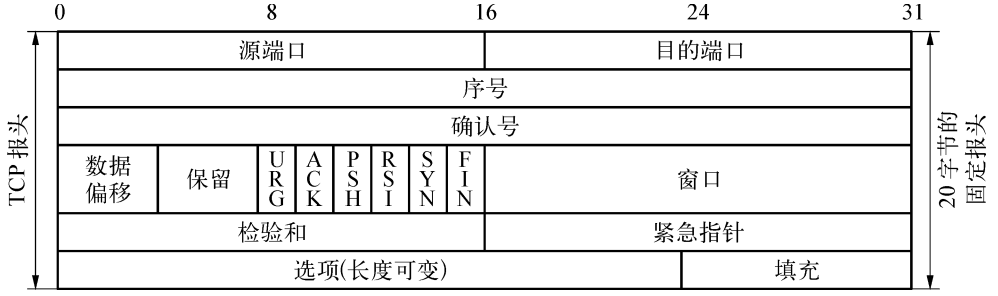


图 1－14　TCP 报文格式

每个 TCP 报文都包含源端口和目的端口的端口号，用于寻找发端和收端的应用进程。端口号加上 IP 报文头部的信息能够唯一确定一个 TCP 连接。序列号则用来标识从 TCP 发端向 TCP 收端发送的数据字节流，它表示在这个报文中的第一个数据字节。窗口大小用于表示接收端期望收到的字节，由于该字段为 16 bit，因而窗口大小最大为 65 535 字节。检验和则是针对整个 TCP 报文以及部分 IP 报文头部的信息进行的报文验证。

TCP 提供的是可靠的面向连接的服务，在传送数据之前，会在收发双方之间建立一条连接通道。TCP 的连接建立过程又称为 TCP 三次握手，如图 1－15 所示：

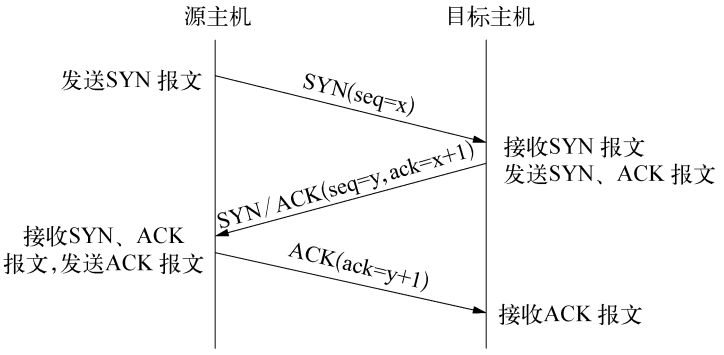


图 1－15　TCP 连接的建立

(1) 源主机向目标主机发起一个建立连接的同步(SYN)请求；

(2) 目标主机在收到这个请求后向源主机回复一个同步、确认(SYN、ACK)应答；

(3) 源主机收到此报文后再向目标主机发送一个确认(ACK)，此时 TCP 连接成功建立。

TCP 会话的三次握手完成。接下来，源主机和目标主机可以互相收发数据。

TCP 的可靠传输还体现在确认技术的应用方面，保证数据流从源设备准确无误地发送到目的设备。以下描述的是确认技术的工作原理。

当目的主机收到源主机发送的数据报时，向源主机发送确认报文，源主机收到确认报文后，继续发送数据报，如此重复。当源主机发送数据报后没有收到确认报文，在一定时间后(计时器结束的时间)，源主机降低数据传输速率，重发数据报。如图 1－16 所示，可分为无差错情况、报文出错、报文丢失、确认报文丢失和确认报文迟到五种基本情况。

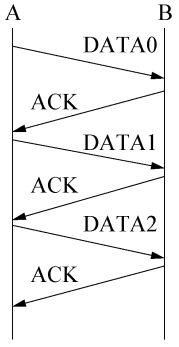


图 1－16(a)　无差错情况

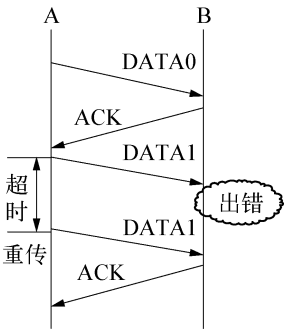


图 1－16(b)　报文出错

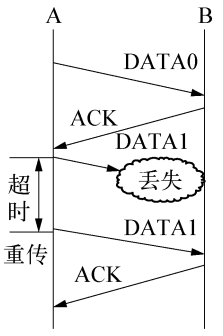


图 1－16(c)　报文丢失

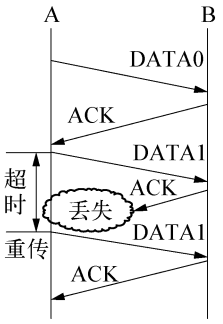


图 1－16(d)　确认报文丢失

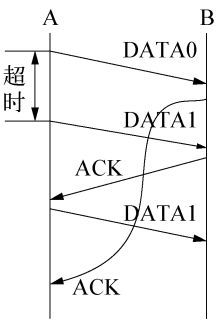


图 1－16(e)　确认报文迟到

提示

可靠传输协议常称为自动重传请求（ARQ）。ARQ 表明重传的请求是自动进行的。接收方不需要请求发送方重传某个出错的分组。因为停止等待协议一次只发一个报文，相当于发送窗口为 1，协议优势是简单、易于实现，缺点是信道利用率低。

为了提高信道利用率，使用连续 ARQ 协议和选择 ARQ 协议，在此协议中，允许发送端可以连续发送多个报文。使用一个确认报文对多个接收报文进行确认，确认报文携带下一次期望的报文序号。一次性连续发送报文的数量叫发送窗口。

TCP 在保证数据传输可靠性的同时，还提供了多路复用、最大报文段（MSS）协商、窗口机制等功能。

多路复用是指多个应用程序允许同时调用传输层，从而为不同的应用建立各自的连接通道。传输层把上层发来的不同应用程序数据分成段，按照先到先发（FIFO）的原则发送数据段，可以去往同一目的地，也可以去往不同目的地。

MSS 表示 TCP 传给另一端的最大报文段长度。当建立一个连接时，连接的双方都要通告各自的 MSS，协商得到 MSS 的最终值，以此提高网络利用率和提升应用性能。

TCP 滑动窗口技术通过动态改变窗口大小来调节两台主机间的数据传输。每个 TCP/IP 主机支持全双工数据传输，因此，TCP 有两个滑动窗口：一个用于接收数据，另一个用于发送数据。

当网络连接的两端速度不匹配时，源主机的发送速度快于目的主机的处理能力时，便会出现快速的源主机将慢速的目的主机淹没的现象，导致数据丢失。为了防止由于主机之间的不匹配而引起数据丢失，TCP 采用滑动窗口进行流量控制。TCP 滑动窗口面向字节流，即以字节为单位进行控制。

二、UDP 协议

UDP 协议提供无连接的服务，即通信双方并不需要建立连接，这种业务是不可靠的。正是由于无连接的服务，所以 UDP 简单，数据传输速度快、开销小。具体来说：

（1）无需建立连接和释放连接，从而减少了连接管理开销，而无需建立连接也减少了发送数据之前的时延。

(2) UDP 数据报只有 8 个字节的报头开销,比 TCP 的 20 个字节的报头要短得多。

(3) 由于 UDP 没有拥塞控制,因此,UDP 的传输速度很快,即使网络出现拥塞也不会降低发送速率。

UDP 更适合于对传输效率要求高的应用,如 SNMP、Radius 等。SNMP 监控网络并断续发送告警等消息,如果每次发送少量信息都需要建立 TCP 连接,无疑会降低传输效率,所以更注重传输效率的应用程序都会选择 UDP 作为传输层协议。

图 1-17　UDP 数据报格式

UDP 的报文格式由两部分构成:报头和数据区。报头各字段意义如下:

(1) 源端口:本主机应用进程的端口号,16 比特。

(2) 目的端口:目的主机应用进程的端口号,16 比特。

(3) 长度:UDP 用户数据报的长度,16 比特。

(4) 检验和:用于检验 UDP 用户数据报在传输中是否出错,16 比特。

1.2.5　ARP 协议

ARP 是一个非常重要并经常使用的地址解析协议,将网络层地址(IP 地址)解析为数据链路层(MAC 地址)的协议。在局域网网络中存在大量的 ARP 报文,多数是以广播形式出现。

一、ARP 报文格式

ARP 是一个独立的三层协议,所以 ARP 报文在向数据链路层传输时不需要经过 IP 协议的封装,而是直接生成自己的报文,其中包括 ARP 报头,到数据链路层后再由对应的数据链路层协议(如以太网协议)进行封装。

ARP 报文分为 ARP 请求报文和 ARP 应答报文两种。它们的报文格式可以统一为如图 1-18 所示。

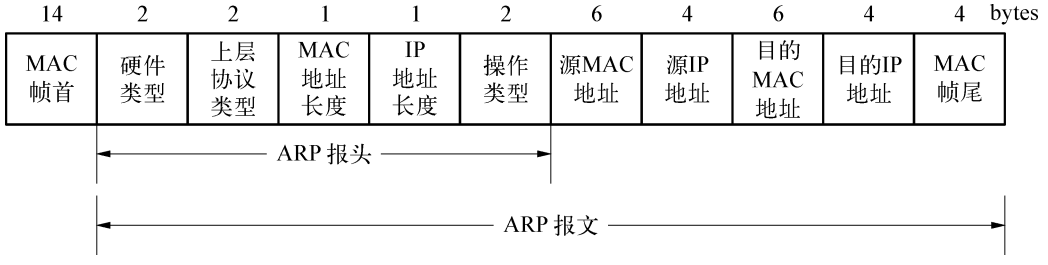


图 1-18　ARP 报文格式

二、ARP 表

无论是主机、交换机还是路由器，都设有一个 ARP 高速缓存(ARP Cache)，缓存着本局域网上设备的 IP 地址到 MAC 地址的 ARP 表，用于数据帧的转发。

设备通过 ARP 解析到目的 MAC 地址后，将会在自己的 ARP 表中增加这条 IP 地址到 MAC 地址的记录，以用于后续到同一目的地数据帧的转发。

提示

ARP 高速缓存中的每一个映射地址项目都设置生存时间(Live Time)，例如，10～20 分钟，凡超过生存时间的项目就从高速缓存中删除掉。设置这种地址映射项目的生存时间是很重要的，主要应对主机移动位置、更换网卡和关机等情况的发生。

三、ARP 地址解析原理

1. 两主机位于相同的局域网

在图 1－19 的示例中，现假设主机 A 和 B 在同一个局域网，主机 A 要向主机 B 发送信息。这时主机 A 只知道主机 B 的 IP 地址，想要获得主机 B 的 MAC 地址。

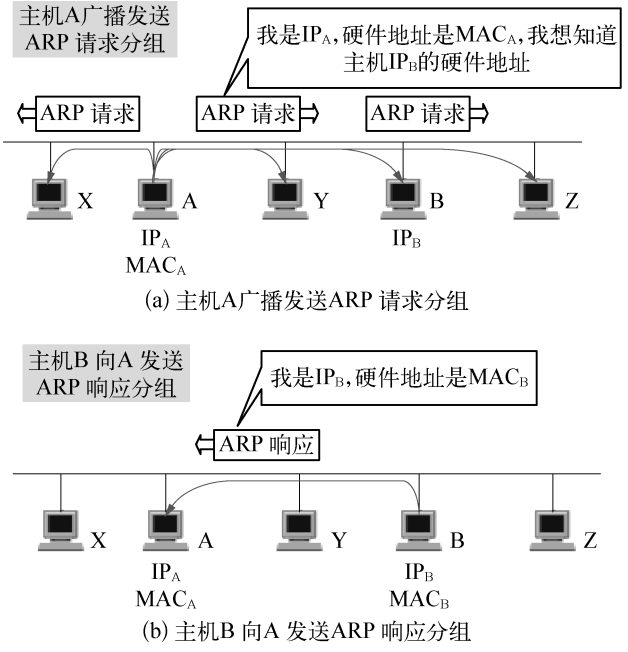


图 1－19　地址解析协议 ARP 的工作原理

具体的地址解析过程如下：

(1) 主机 A 广播发送 ARP 请求分组，ARP 请求分组的主要内容是表明“我的 IP 地址是 IP_A，硬件地址是 MAC_A，我想知道 IP 地址是 IP_B的主机硬件地址 MAC_B”。

（2）在本局域网上的所有主机上运行的 ARP 进程都收到此 ARP 请求分组。

（3）主机 B 在 ARP 请求分组中见到自己的 IP 地址，就向主机 A 单播发送 ARP 响应分组，并写入自己的硬件地址。ARP 响应分组的主要内容是“我的 IP 地址是 IP_B，我的硬件地址是 MAC_B”。

（4）主机 A 收到主机 B 的 ARP 响应分组后，就在其 ARP 高速缓存中写入主机 B 的 IP 地址到硬件地址的映射。

2. 两主机位于不同的局域网

如图 1－20 所示，两主机不在同一局域网又是如何通信的呢？具体步骤如下：

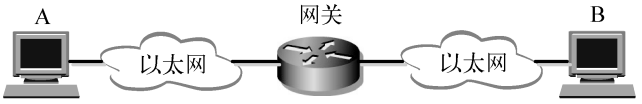


图 1－20　两主机不在同一局域网中 ARP 的工作原理

（1）主机 A 向本网段发出一个 ARP 请求广播，ARP 请求分组中的目的 IP 地址为网关 IP 地址（$IP_{网关}$），其目的是想获得网关的 MAC 地址（$MAC_{网关}$）。如果 A 已知网关的 MAC 地址，则略过此步。

（2）网关收到 ARP 广播包后，同样会向主机 A 发回一个包含自己硬件地址（$MAC_{网关}$）的 ARP 应答包。

（3）当主机 A 获得 $MAC_{网关}$后，在主机 A 向主机 B 发送的原分组的目的 MAC 地址字段填上 $MAC_{网关}$后发送给网关。

（4）如果网关的 ARP 表中已有主机 B 对应的 MAC 地址（MAC_B），则网关直接将在来自主机 A 的分组中的目的 MAC 地址字段填上 MAC_B后转发给主机 B。

（5）如果网关的 ARP 表中没有 MAC_B，网关会再次向主机 B 所在的网段发送 ARP 广播请求，此时目的 IP 地址为主机 B 的 IP 地址（IP_B）。

（6）当网关从收到来自主机 B 的应答报文中获得 MAC_B后，就可以将由主机 A 发来的报文重新在目的 MAC 地址字段填上 MAC_B后发给主机 B。

提示

网关这类设备支持直接连接的多个网段，那每个网段连接在一个端口上。通过网关本身即可实现互通，但是不提供到达非直接连接网络的路由功能。要注意的是，终端设备上配置的网关 IP 地址必须指定为三层设备的接口，如位于网络边缘的路由器、多层交换机的接口地址。

1.2.6　Wireshark 软件操作

微课：
数据包抓包

Wireshark 是网络包分析工具，其主要作用是对接口实时捕捉网络包，并详细显示包的协议信息。Wireshark 可以捕捉多种网络接口类型的包，可以

打开多种网络分析软件捕捉的包，能够支持多个协议的解码。网络管理人员一般用它来检测网络安全隐患、解决网络问题，也可以用它来学习网络协议、测试协议执行情况等。

值得注意的是，Wireshark 不会处理网络事务，它仅仅是“测量”（监视）网络，具有以下主要特性：

① 在接口实时捕捉包；

② 能详细显示包的详细协议信息；

③ 可以打开/保存数据包；

④ 创建多种统计分析，可以采用多种方式过滤；

⑤ 可以导入导出其他捕捉程序支持的数据包格式；

⑥ 多种方式查找包。

一、网络数据流的监测部署

监测部署是通过设置监测接入点，即在监测设备上安装 Wireshark 软件，可以分为三种情况：一是在被监测主机上直接捕获，二是利用集线器将被监测接口的数据分为多路进行捕获（如图 1－21(a)），三是利用交换机的接口数据映射功能进行捕获（如图 1－21(b)）。

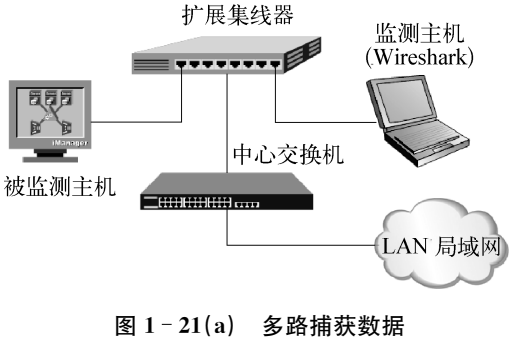


图 1－21(a)　多路捕获数据

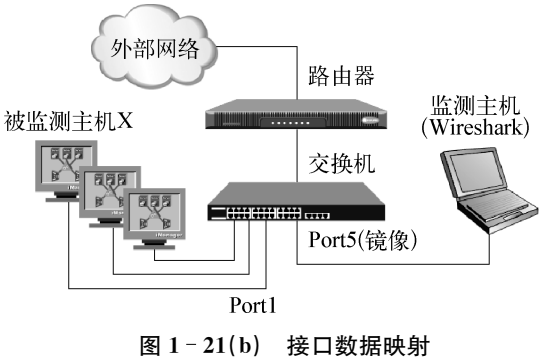


图 1－21(b)　接口数据映射

二、Wireshark 软件抓包

(1) Wireshark 软件用于捕获主机上某一个网卡的收发网络包，当主机有多个网卡时，需要选择其中的一个网卡。点击菜单栏中的“捕获-选型”，选择正确的网卡，然后点击“捕获-开始”，出现如图 1－22 所示的对话框，即开始抓包。

(2) 使用过滤是非常重要的，Wireshark 抓包时会得到大量的冗余信息，在几千甚至几万条记录中，很难找到网络管理员需要的部分。过滤器会帮助我们在大量的数据中迅速找到需要的信息，一般可以分为两种：

一种是显示过滤器，在图 1－22 的抓包界面中所示，用来在捕获的记录中找到所需要的记录；

另一种是捕获过滤器，点击菜单栏中“捕获-捕获过滤器”中设置，用来过滤捕获的数据包，以免捕获太多的记录。

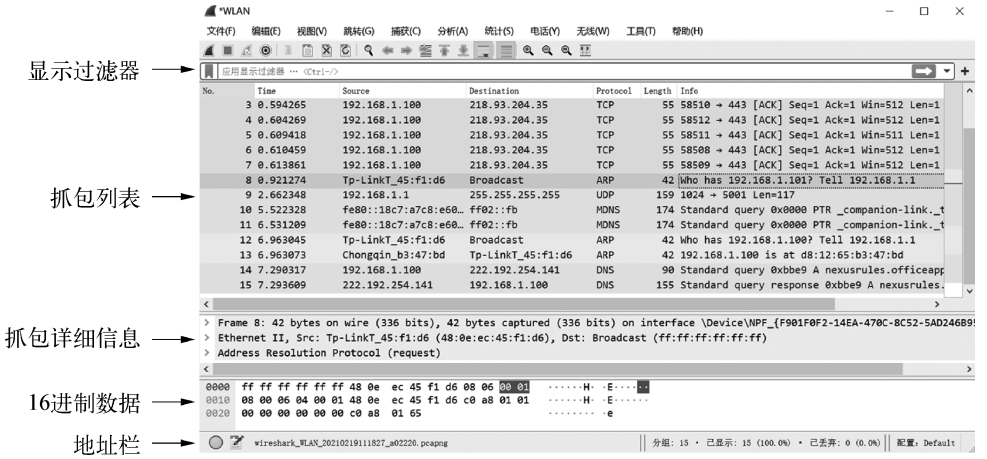


图 1－22　Wireshark 抓包界面

过滤表达式的规则可定义为：① 协议过滤，比如只显示 TCP 协议；② IP 地址过滤，比如 ip.src、ip.dst 限制源主机和目的主机的 IP 地址；③ 端口过滤，比如 tcp.port＝80 是只显示端口号为 80 的 TCP 协议包等等。

(3) 抓包列表。抓包列表的表项中显示了编号、时间戳、源地址、目标地址、协议、长度以及抓包信息。这里可以看到不同的协议用了不同的颜色显示。

(4) 抓包详细信息。这个面板是最重要的，用来查看协议中的每一个字段。各行信息分别为：

① Frame：物理层的数据帧概况；

② Ethernet II：数据链路层以太网帧头部信息；

③ Internet Protocol Version 4：互联网层 IP 包头部信息；

④ Transmission Control Protocol：传输层协议的数据段头部信息，此处是 TCP；

⑤ Hypertext Transfer Protocol：应用层的信息，此处是 HTTP 协议。

操作练习

【操作一】利用 Wireshark 捕获发生在 ping 过程中的 ARP 报文，加强对 ARP 协议的理解，掌握 ARP 报文格式，掌握 ARP 请求报文和应答报文的区别。

【操作二】利用 Wireshark 实际分析一下三次握手的过程。具体操作步骤如下：

第一步　打开 Wireshark，打开浏览器输入 www.163.com；

第二步　在 Wireshark 中输入 http 过滤，选中 HTTP/1.1 的那条记录，然后点击右键，对话过滤器→“F5 TCP”。

1.3 IP 协议与配置管理

需求分析

A、B 为两台位于不同地点的计算机，现在 A 机准备发送 20 个数据给 B 机，然而网络上有成千上万的其他网络终端，A 机如何保证这 20 个数据准确无误地到达 B 机？回想一下“写信”这个行为，只有在信封上写了正确的目的地址，邮递员才可能把信件正确无误地送到目的地。同样的道理，网络数据必须有一个目的地址。赋予网络数据包目的地址的这个行为，正是 IP 协议的作用之一。

目前的数据通信网络，特别是 TCP/IP 网络，使用最多的是数据报分组交换方式，而 IP 协议是用于将多个分组交换网络连接起来的最典型通信协议。它成为 TCP/IP 互联网设计中最基本的部分，有时都称 TCP/IP 互联网为基于 IP 技术的网络。网络数据包不仅有目的地址，还有源地址，即发送这个数据的终端地址，这个地址有一个专业的术语：IP 地址。

知识学习

目前的数据通信网络，特别是 TCP/IP 网络，使用最多的是数据报分组交换方式，而 IP 协议是用于将多个分组交换网络连接起来的最典型通信协议。它成为 TCP/IP 互联网设计中最基本的部分，有时都称 TCP/IP 互联网为基于 IP 技术的网络。

IP 提供了不可靠、无连接的数据报传送服务，不可靠的意思是它不能保证 IP 数据报能成功地到达目的地。IP 仅提供尽最大努力(Best-effort)投递的传输服务。如果发生某种错误时，如某个路由器暂时用完了缓冲区，IP 有一个简单的错误处理算法：丢弃该数据报，然后发送 ICMP 消息报给发送端。任何要求的可靠性必须由上层来提供(如 TCP)。

无连接的意思是 IP 并不维护任何关于后续数据报的状态信息。每个数据报的处理是相互独立的。这也说明，IP 数据报可以不按发送顺序接收。举个例子，如果发送端向相同的接收端发送两个连续的数据报(先是 A，然后是 B)，每个数据报都是独立地进行路由选择，可能选择不同的路径，因此，B 可能在 A 到达之前先到达。

由于 IP 协议的第 4 版本(IPv4)在网络中仍广泛使用，本节所有内容都以 IPv4 标准为主，但是，下一代网络技术中所采用的 IPv6 也在我国逐步推广当中。

1.3.1　IP 报文及转发过程

一、IP 报文

IP 报文是网络通信的基本传送单元，包括报头和数据两部分。图 1－23 表示 IPv4 报文格式，普通的 IP 头部长度为 20 个字节，不包含 IP 选项字段。下面是部分字段的简单说明。

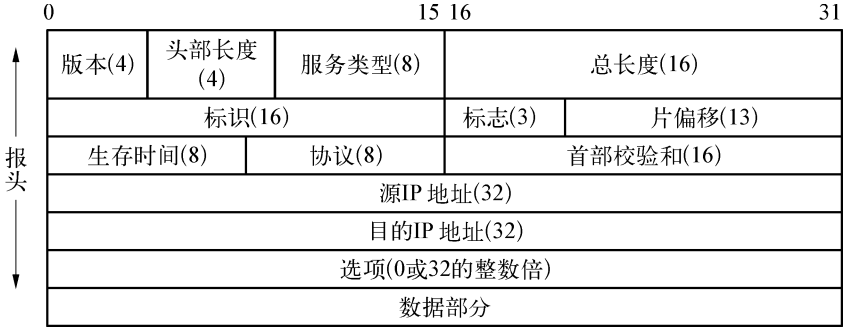


图 1－23　IPv4 报文格式

1. 服务类型

占 8 bit，服务类型字段指明 IP 报文将被如何处理，其中 3 位用来标识由发送者指定的优先权或重要程度。因此，该字段提供了 IP 数据报路由的优先权机制。

2. 总长度

指整个 IP 报文的长度，以字节为单位。利用报头长度字段和总长度字段，就可以知道报文中数据内容的起始位置和长度。由于该字段长 16 比特，所以 IP 报文最长可达 65 535 字节。而对于一个长达 65 535 字节的 IP 报文，大多数链路层都会对它进行分片。

3. 标识(与分片相关)

IP 报文长度如果超过最大传送单元(MTU)则需要分片，分片可以发生在原始发送端主机上，也可以发生在中间路由器上。

把一份 IP 报文分片以后，只有到达目的地才进行重新组装。重新组装由目的端的 IP 层来完成，即使只丢失一片数据也要重传整个报文。

标识字段占 16 bit，是由计数器产生的一个数字，该值会被复制到所有的数据报片的标识字段中。相同的标识字段的值使分片后的各数据报片最后能正确地重装成原来的报文。

4. 标志(与分片相关)

占 3 bit，标志字段用其中一个比特来表示“更多的片”，除了最后一片外，其他每片都要把该比特置 1；另一个比特称作“不分片”位。如果将这一比特置 1，IP 协议将不对报文进行分片。如果在网络传输过程中遇到 MTU 小于报文长度时，将报文丢弃并发送一个 ICMP 差错报文。

5. 片偏移(与分片相关)

占 13 bit,指的是某片在原报文中的相对位置。也就是说,相对于用户数据字段的起点,该片从何处开始。

IP 报文分片的工作基本原理如图 1-24 所示。

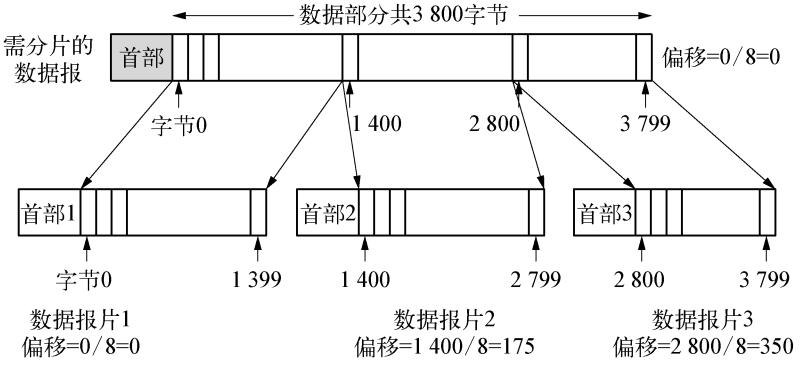


图 1-24　IP 报文分片的工作原理

6. 协议

占 8 bit,指出此报文携带的数据是使用何种协议,以便使目的主机的 IP 层知道应将数据部分交给哪个高层处理进程,表 1-2 表示出一些常用协议与对应的字段值。

表 1-2　常用协议和相应的协议字段值

协议名	ICMP	IGMP	TCP	EGP	IGP	UDP	IPv6	OSPF
协议字段值	1	2	6	8	9	17	41	89

7. 首部校验和

根据 IP 首部计算的检验和码,它不对首部后面的数据进行计算,因为 ICMP、IGMP、UDP 和 TCP 在它们各自的首部中均含有同时覆盖首部的数据校验和码。

8. 源 IP 地址/目的 IP 地址

各占 4 字节。每一个地址代表一个网络或网络中的一台主机。

二、IP 地址和硬件地址的比较

图 1-25 说明了 IP 地址与硬件地址的区别。从层次的角度看,硬件地址(或物理地址、MAC 地址)是数据链路层和物理层使用的地址,而 IP 地址是网络层及以上各层使用的地址。

两种地址的具体差别如下:

① IP 地址放在 IP 报文的首部,硬件地址放在 MAC 帧的首部。

② IPv4 地址为 32 位,硬件地址为 48 位。

③ IP 地址基于逻辑,可以更改;硬件地址基于物理,固化在网卡的 ROM 中,一般不可以修改。

④ IP 地址的寻址范围是运行 IP 协议的广域网,硬件地址的寻址范围是以太局域网。

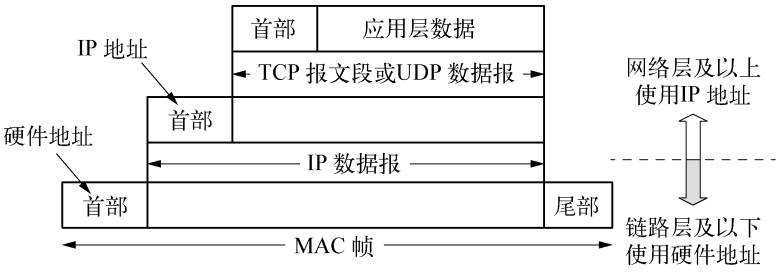


图 1－25　IP 地址与硬件地址的区别

三、IP 报文的转发过程

图 1－26 中画的是三个局域网用两个路由器 R_1 和 R_2 互连起来，现在主机 H_1 和主机 H_2 在通信。这两个主机的 IP 地址分别是 IP_1 和 IP_2，而它们的硬件地址分别是 HA_1 和 HA_2。

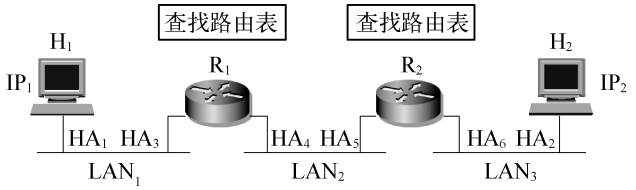


图 1－26　IP 报文的转发过程

转发路径是：$H_1 \rightarrow R_1 \rightarrow R_2 \rightarrow H_2$。路由器有两个端口，因此，它有两个硬件地址。表 1－3 中描述了在数据链路层和网络层上分别观察硬件地址和 IP 地址，确定在两个网络设备之间传递数据所包含的地址信息。

表 1－3　传递数据包含的地址信息

	IP 数据报首部		MAC 帧首部	
	源地址	目的地址	源地址	目的地址
从 H_1 到 R_1	IP_1	IP_2	HA_1	HA_3
从 R_1 到 R_2	IP_1	IP_2	HA_4	HA_5
从 R_2 到 H_2	IP_1	IP_2	HA_6	HA_2

这里要指出的几点是：

① IP 数据报中的源地址和目的地址在整个传送过程中，包括经过路由器，都不会发生任何改变。

② 当 IP 数据报经过路由器时，路由器会根据目的 IP 地址的网络号进行路由选择。

③ 在具体的链路中，同一网络内的设备（主机或路由器）是根据 MAC 地址寻址。例如，在图 1－26 中，MAC 帧在不同网络上传送时，其 MAC 帧首部中的源地址和目的地址

要发生变化。

思考

还有两个重要问题没有得到解决：

(1) 主机或路由器怎样知道向 MAC 帧的首部应填入什么样的硬件地址？

(2) 路由器中的路由表是怎样产生的？

1.3.2 IP 地址和子网掩码

微课：IP 地址规划

一、IP 地址

1. IPv4 地址简介

为了使连入互联网的众多主机在通信时能够相互识别，互联网上的每一台主机和路由器都分配有一个唯一的 32 位地址，即 IP 地址，也称作网际地址。IP 地址一般采用国际上通行的点分十进制表示。

一个 IP 地址由 4 个字节组成，字节之间用点号分隔，每个字节表示为从 0～255 的十进制数(8 位二进制数最大为 11111111，即十进制数 255)，这个表示法称为 IP 地址的点分十进制表示法。例如，IP 地址“10100110 01101111 00000100 01100100”(对应的十六进制数为“A6 6F 04 64”)，用点分十进制表示法就是“166.111.4.100”。

IP 地址被定义为由两个固定长度的字段组成，其中一个字段是网络号(net-id)，它标志主机(或路由器)所连接到的网络，而另一个字段则是主机号(host-id)，它标志该主机(或路由器)。两级的 IP 地址可以记为：

IP 地址::＝｛<网络号>，<主机号>｝

“::＝”代表“定义为”。

一般来说，互联网上的每个接口必须有一个唯一的 IP 地址，因而多接口主机(比如路由器)具有多个 IP 地址，其中每个接口都对应一个 IP 地址，如图 1－27 所示。

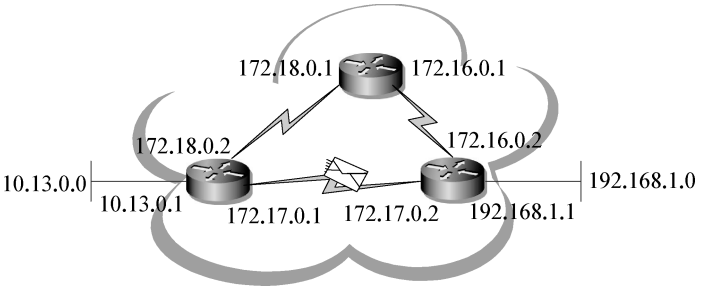


图 1－27　互联网 IP 地址使用示例

IPv4 使用 32 位(4 字节)地址，因此，整个地址空间中有 4 294 967 296(2^{32})个地址，

也就是近 43 亿个地址。不过，其中一些地址是为特殊用途保留的，如局域网专用地址（约 800 万个）、测试地址（约 1 600 万个）和组播地址（约 2 700 万个），这样一来可直接在广域网上使用的、路由的公网 IP 地址数量就更加少了。

提示

公网 IP 地址是指可以在广域网上直接使用，直接被路由，需要向 IP 地址管理机构申请、注册、购买且全球唯一的 IPv4 地址，类似于我们每个公民的身份证号。公网 IP 地址直接分配给互联网的主机、服务器或其他设备，可以通过它在全球范围内找到对应的设备，如各大网站就是直接采用公网 IP 地址。

与公网 IP 地址对应的自然是私网 IP 地址了，又称为专网 IP 地址或者局域网 IP 地址。私网 IP 地址是指仅可以在各用户自己的局域网内部使用，无需向 IP 地址管理机构申请、注册，也无须购买的 IPv4 地址，这就类似于公司内部的员工编号。

图 1－28 给出了各类 IP 地址的网络号字段和主机号字段。

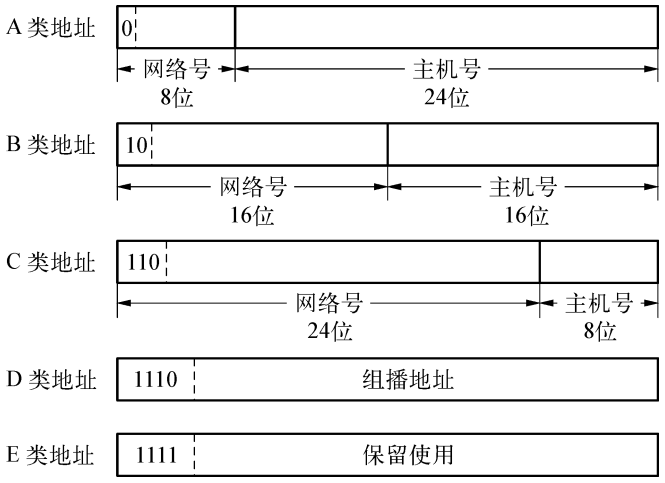


图 1－28　IP 地址分类

A 类地址的最高位为“0”，与其后 7 位作为网络号，剩余 24 位用作主机号。A 类地址共 126 个网，它用于少数主机数量众多的大型网络，主机数可以为 $2^{24}-2=16\ 777\ 216-2=16\ 777\ 214$。

B 类地址的最高位为“10”，与其后 14 位作为网络号，剩余 16 位用作主机号。B 类地址共 16 384 个网，它用于中等规模的网络，每个网络主机数最多为 $2^{16}-2=65\ 536-2=65\ 534$。

C 类地址的最高位为“110”，与其后 21 位作为网络号，剩余 8 位用作主机号。C 类地址共 2 097 152 个网，它用于小型网络，每个网络的主机数只能少于 $2^{8}-2=256-2=254$。

这样我们就可得出如表 1－4 所示的 IP 地址的使用范围。

表 1－4　A、B、C 三类 IP 地址的使用范围

网络类别	最大网络数	第一个可用的网络号	最后一个可用的网络号	每个网络中的最大主机数
A	126 (2^7-2)	1	126	16 777 214
B	16 384 (2^{14})	128.0	191.255	65 534
C	2 097 152 (2^{21})	192.0.0	223.255.255	254

D 类地址为组播(Multicast)地址，它用一个地址代表一组主机。组播地址是到一个“主机组”的 IP 数据报的传送，主机组是由零个或多个用同一 D 类 IP 目的地址表示的主机集合。

E 类地址是实验性地址，设计时保留给将来使用。但在目前由于地址匮乏，也被用于公网寻址分配使用。

2. 网络地址、主机地址和广播地址

在很多资料中，我们经常会看到网络地址、主机地址和广播地址这样的几个概念，那么它们代表什么含义呢?

(1) 网络地址

网络地址是用来标识一个网络的地址，可以是分类地址，也可以是后面介绍的无分类地址。对应的格式如图 1－29 所示，正常 IP 地址中的网络号部分保持不变，主机号部分全为 0。

网络层设备(例如路由器等)使用网络地址来代表本网段内的主机，大大减少了路由器的路由表条目。

(2) 主机地址

主机地址是用来标识指定网络中所包含的主机，它的格式用得比较少，如图 1－30 所示。其中主机号部分保持不变，网络号部分全部为 0。

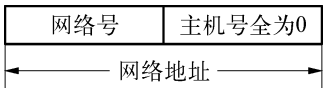


图 1－29　网络地址结构

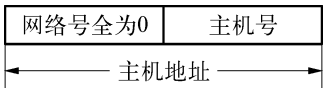


图 1－30　主机地址结构

(3) 广播地址

广播地址则是一个有类或无类网络中的最后一个 IPv4 地址，即主机号部分全为 1 的 IPv4 地址，可通过这个地址向对应网络或子网以广播方式发送数据包(也就是广播通信)，让本地网络或子网的所有节点都可收到同一数据包。

提示

根据所使用的 IPv4 地址通信用途来划分的三种方式：

单播(Unicast)是指一台源 IP 主机仅与一台目的 IP 主机进行通信的方式。单播通信中所使用的 IPv4 地址，主要是指除广播地址或保留地址外的 A 类、B 类、C 类地址，这些全是常规的单播地址。

组播(Multicast)是指一台源 IP 主机同时与网络中多台 IP 主机进行通信的方式，又称多播。组播通信所用的 IPv4 地址就是 D 类的组播地址，通过这类地址就可以把一个数据包发送到多个指定的节点上。

广播(Broadcast)是指一台源 IP 主机同时与本地网络或子网中所有其他节点进行通信的方式。上述介绍的广播地址就是广播通信所需的 IPv4 地址。

(4) 可用主机地址数量计算

下面让我们来计算一下可用的 IP 地址，假定这个网段的主机部分位数为 n，每一位都可以有 0 或 1 这两个值的选择，所以主机地址一共有 2^n 个。但是如上所述，每一个网段会有一些 IP 地址不能用作主机 IP 地址，那么可用的主机地址个数为 2^n-2 个。如图1－30 所示例子。

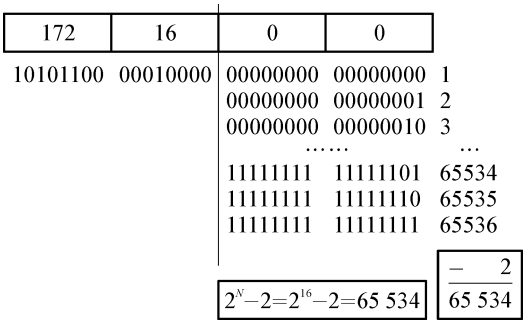


图 1－31　可用主机地址数量计算示例

例如网段 172.16.0.0，有 16 个主机位，因此，有 2^{16} 个 IP 地址，去掉一个网络地址 172.16.0.0，一个广播地址 172.16.255.255 不能用作标识主机，那么共有 $2^{16}-2$ 个可用地址。再如网段 192.168.1.0，有 8 个主机位，共有 $2^8=256$ 个 IP 地址，去掉一个网络地址 192.168.1.0，一个广播地址 192.168.1.255，共有 254 个可用主机地址。

3. 几类特殊的 IPv4 地址

IP 地址用于唯一的标识一台网络设备，但并不是每一个 IP 地址都是可用的，一些特殊的 IP 地址被用于各种各样的用途，不能用于标识公用网络设备。

(1) 私网 IP 地址

校园网或企业网如果是与因特网连接的，则要向因特网编号管理局(IANA)的有关机构申请网络号。例如，中国教育科研网的用户向 CERNET 的网络中心申请网络号，然后再安排网上主机地址。如果只是内部的互联网，则可自己规定网上各主机的 IP 地址，一般使用在 RFC 1918 中推荐的为私有网络保留的 IP 地址空间(见表 1－5)：

表 1－5　三类私网 IP 地址

网络个数	起始地址	结束地址
1	10.0.0.0	10.255.255.255
32	172.16.0.0	172.31.255.255
256	192.168.0.0	192.168.255.255

(2) 127.0.0.1 地址

在配置网络设备或者进行系统主机测试时，经常用到 127.0.0.1 这个地址，被称为回环地址(Loopback)。其实不仅是该地址，所有 127 开头的地址段都属于保留测试地址。它不能分配给主机使用，但却可以用来进行各种地址管理操作，如 Ping 操作。在 IP 网络

中可用来测试主机 TCP/IP 协议、网卡驱动是否工作正常。

(3) 全 0 地址

全“0”的 IP 地址 0.0.0.0 代表所有的主机，在路由器上用 0.0.0.0 地址指定默认路由。

(4) 全 1 地址

全“1”的 IP 地址 255.255.255.255，也是广播地址，但 255.255.255.255 代表所有主机，用于向网络的所有节点发送数据包。这样的广播不能被路由器转发。

4. IP 地址的重要特点

(1) IP 地址是一种分等级的地址结构。分两个等级的好处是：

第一，IP 地址管理机构在分配 IP 地址时只分配网络号，而剩下的主机号则由得到该网络号的单位自行分配。这样就方便了 IP 地址的管理。

第二，路由器仅根据目的主机所连接的网络号来转发分组(而不考虑目的主机号)，这样就可以使路由表中的项目数大幅度减少，从而减小了路由表所占的存储空间。

(2) 实际上 IP 地址是标志一个主机(或路由器)和一条链路的接口。

当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号必须是不同的，这种主机称为多归属主机。由于一个路由器至少应当连接到两个网络(这样它才能将 IP 数据报从一个网络转发到另一个网络)，因此，一个路由器至少应当有两个不同的 IP 地址。

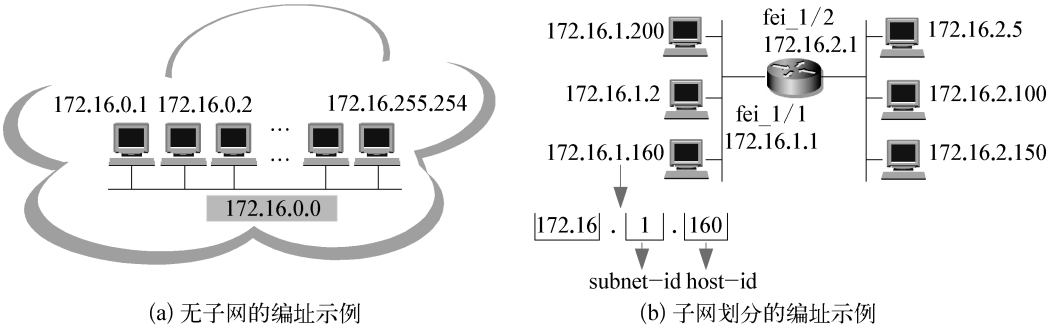
(3) 用转发器或网桥连接起来的若干个局域网仍为一个网络，因此，这些局域网都具有同样的网络号。

(4) 所有分配到网络号的网络，无论是范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的。


微课：子网与子网划分

二、子网掩码

对于使用以上分类 IPv4 地址的组织，外部将该组织看作单一网络，不需要知道内部结构。例如，所有到地址 172.16.X.X 的路由被认为同一方向，不考虑地址的第三和第四个字节，这种方案的好处是减少路由表的项目。如图 1-32(a)所示，这是没有进行子网划分的编址方案。



(a) 无子网的编址示例　　(b) 子网划分的编址示例

图 1-32　子网与子网划分情况

但这种方案无法区分一个大网络内不同的网段，而把这个网络看成一个整体。这使得网络内所有主机都能收到广播包，会降低网络的性能，另外也不利于管理。

这就需要一种方法将这种网络分为不同的网段，按照各个子网段进行管理，这就是子网划分。在图 1－32(b)中，网络 172.16.0.0 被划分为两个子网，即 172.16.1.1 和 172.16.2.1。两个子网之间要通过路由器相互连接，而对外两个子网作为一个整体，都是由出口路由器进行数据转发。

那么，究竟有多少位是网络地址呢？主机地址范围又有多大呢？在网络中必须有这样一个参数来说明以上问题，这就是子网掩码。

IP 地址在没有相关的子网掩码的情况下存在是没有意义的。

子网掩码定义了构成 IP 地址的 32 位中的多少位用于子网位，由连续位个“1”与连续位个“0”组成，如图 1－33 所示。

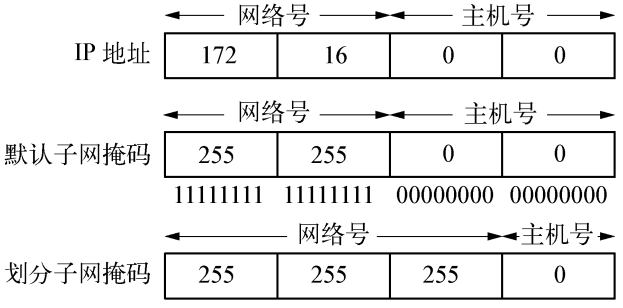


图 1－33　子网掩码示例

子网掩码中的二进制位构成了一个过滤器，它通过“按位求与”的逻辑运算，标识哪一部分是标志网络的部分，哪一部分是标志主机的部分。按位求与是对 IPv4 地址的每一位与子网掩码对应的每一位进行二进制逻辑“与”运算(AND)，如图 1－34 所示。

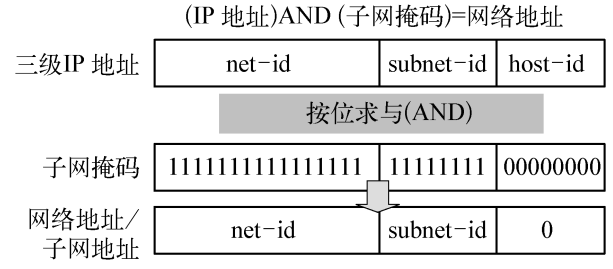


图 1－34　子网掩码的与运算

提示

对于传统分类 IP 地址，在没有进行子网划分的情况下，也具有子网掩码，称为默认子网掩码。在表 1－6 中，A、B、C 类地址中的主机号部分，可以借作子网号的位数最多为 22 位、14 位和 6 位(原因可以自行分析)。

表 1－6　A、B、C 三类地址的默认子网掩码

网络类别	网络地址位数	子网掩码
A	8	255.0.0.0
B	16	255.255.0.0
C	24	255.255.255.0

三、可变长子网掩码

为了解决 IPv4 的不足，提高网络划分的灵活性，诞生了两种非常重要的技术，那就是可变长子网掩码（VLSM）和无分类域间路由选择（CIDR），把传统的标准 IPv4 有类网络演变成一个更为高效、更为实用的无类网络。

VLSM 用于 IPv4 子网的划分，也就是把一个大的网络划分成多个小的子网；而 CIDR 则用于 IPv4 子网的聚合，当然主要是指路由方面的聚合，也就是路由汇总。下面主要讨论的是可变长子网掩码技术。

依据上述内容，VLSM 运用了子网划分技术，包括子网、子网掩码、网络地址等概念。VLSM 可以更灵活地依据实际所需的地址数来调整所划分的子网大小，可以说其就是子网划分的最典型应用。

因为在定义子网掩码的时候，我们做出了假设，在整个网络中将一致地使用这个掩码。在许多情况下，这导致浪费了很多主机地址。比如我们有一个子网，它通过串口连接了 2 个路由器。在这个子网上仅仅有两个主机，每个端口一个，但是我们已经将整个子网分配给了这两个接口。这将浪费很多 IP 地址。

如果我们使用其中的一个子网，并进一步将其划分为第 2 级子网，将有效地“建立子网的子网”，并保留其他的子网，则可以最大限度地利用 IP 地址。“建立子网的子网”的想法构成了 VLSM 的基础。

为了使用 VLSM，我们通常定义一个基本的子网掩码，它将用于划分一级子网，然后用二级掩码来划分一个或多个一级子网。在图 1－35 中，我们示意了 VLSM 应用的基本情况。这里“/＊＊”是指子网掩码中有多少位作为网络地址，这是 CIDR 技术的记法，“＊＊”值越小，表示网络规模越大。可以看到，基本的子网掩码是“/16”，划分后的一级是“/24”，二级是“/27”，三级是“/30”。

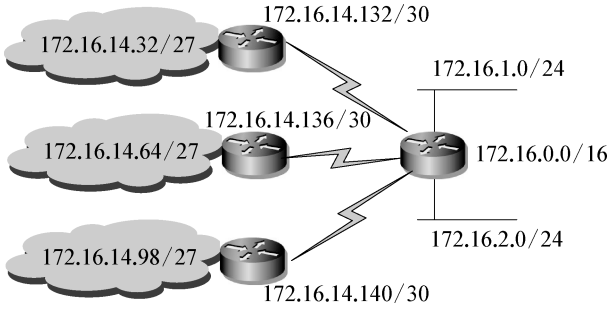


图 1－35　VLSM 示例

VLSM 技术对高效分配 IP 地址（较少浪费）以及减少路由表大小都起到非常重要的作用，这在超网和网络聚合中非常有用。但是需要注意的是使用 VLSM 时，所采用的路由协议必须能够支持它，这些路由协议包括 RIP2，OSPF，EIGRP，IS－IS 和 BGP。

【示例 1】某公司有两个主要部门：市场部和技术部。技术部又分为硬件部和软件部两个部门。该公司申请到了一个完整的 C 类 IP 地址段：210.31.233.0，子网掩码 255.255.255.0。为了便于分级管理，该公司采用了 VLSM 技术，将原主网络划分称为两级子网（未考虑全 0 和全 1 子网）。

市场部分得了一级子网中的第 1 个子网，即 210.31.233.0，子网掩码 255.255.255.192，该一级子网共有 62 个 IP 地址可供分配。

技术部将所分得的一级子网中的第 2 个子网 210.31.233.128，子网掩码 255.255.255.192 又进一步划分成了两个二级子网，其中第 1 个二级子网 210.31.233.128，子网掩码 255.255.255.224划分给技术部的硬件部，该二级子网共有 30 个 IP 地址可供分配。技术部的软件部分得了第 2 个二级子网 210.31.233.160，子网掩码 255.255.255.224，该二级子网共有 30 个 IP 地址可供分配。

【示例 2】从 198.16.0.0 起提供 IP 地址，4 个单位 A、B、C、D 分别要求 4 000、2 000、4 000 和 8 000 个地址，并按照顺序分配。请写出每一个单位的第一个 IP 地址、最后一个 IP 地址及用 W.X.Y.Z/S 形式表示的掩码。

详细规划步骤如下：

（1）设 A、B、C、D 4 个网络的主机位分别为 x、y、z、w（bit），应该满足以下条件：$2^x-2\geqslant 4\ 000$，$2^y-2\geqslant 2\ 000$，$2^z-2\geqslant 4\ 000$，$2^w-2\geqslant 8\ 000$。得到最小值为：x＝12，y＝11，z＝12，w＝13，下面在分配过程中要满足此条件。

（2）按照网络的主机数量从大到小排列，分别为 D、A 和 C、B，下面将按照这个顺序依次进行分配。详细见图 1－36。

（3）D 单位为一级子网 198.16.0000＊/20。

（4）A 单位为二级子网 198.16.00010＊/21，C 单位为二级子网 198.16.00011＊/21。

（4）B 单位为三级子网 198.16.001000＊/22。

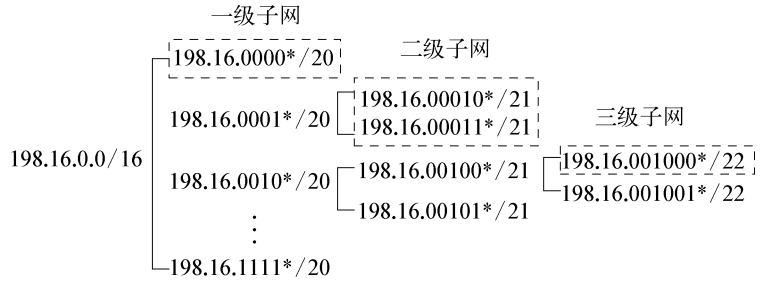


图 1－36　VLSM 子网划分示例 2

1.3.3　小型网络的 IP 参数规划

在对小型网络进行规划时，方案中的 IP 参数设计非常重要，需要考虑 5 个问题，分别是：

① 该网络内将划分几个子网？

② 每个子网有多少台有效主机?

③ 在该子网划分中,网络掩码是什么?

④ 每个子网的网络地址是什么?

⑤ 每个子网的广播地址是什么?

由此,我们提出以下的基本概念和计算方法。包括子网数、每个子网中的主机数、子网掩码、基数和广播地址。

● 子网数=2^x-2。x——子网位的比特数目,减 2——子网位全 0 和全 1,默认是无效的。例如,在 C 类网络的默认掩码中,掩码后 8 位为 1110 0000,能产生 $2^3-2=6$ 个子网。

● 每个子网的主机数=2^y-2。y——主机位的比特数目,减 2——主机位全 0 和全 1,是网络地址和广播地址。例如,在 C 类网络的默认掩码中,掩码后 8 位为 1110 0000,可以得到 $2^5-2=30$,每个子网有 30 台主机。

● 子网掩码——根据网络类型,确定子网位数和位置。根据对应位的权值,计算其十进制数值。例如,在 B 类网络的默认掩码中,掩码后 8 位为 1100 0000,则子网位数为 10 位,该 8 位的十进制为 $2^7+2^6=128+64=192$,子网掩码为 255.255.255.192。

● 基数=256−子网掩码。由此计算,子网地址中对应字节值=N×基数,具体见示例 2。例如,子网掩码为 255.255.255.224,则有效子网基数为 256−224=32。

● 广播地址是所有主机位为 1。

【示例 1】某企业内部有一 IP 地址 172.16.2.160,子网掩码为 255.255.255.192,要求计算该 IP 地址所处的子网网络地址、子网广播地址及可用 IP 地址范围。

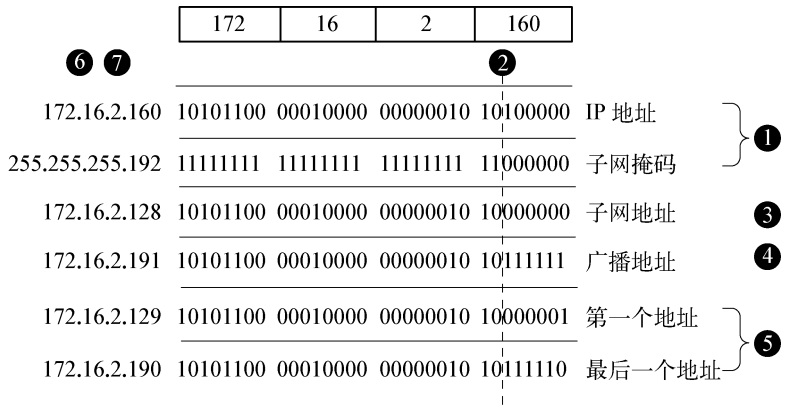


图 1-37　地址计算示例

如图 1-37 所示,详细步骤如下:

第一步　首先将 IP 地址和子网掩码转换为二进制表示。

第二步　在子网掩码的 1 与 0 之间划一条竖线,竖线左边即为网络位(包括子网位),竖线右边为主机位。

第三步　将主机位全部置 0,网络位照写就是子网的网络地址。

第四步　将主机位全部置 1,网络位照写就是子网的广播地址。

第五步　介于子网的网络地址与子网的广播地址之间的即为子网内可用 IP 地址范围。

第六步　将前 3 段网络地址写全。

第七步　最后转换成十进制表示形式。

【示例 2】现有一个网络地址 202.119.200.0，要在此网络中划分 6 个子网，问需要多少位表示子网？子网掩码是多少？每个子网的网络地址是什么？

规划详细步骤如下：

第一步　这是一个 C 类网络，默认子网掩码为 255.255.255.0，表示网络地址为 24 位，主机地址为 8 位。

第二步　子网数＝$2^x-2\geqslant 6$，则 $x\geqslant 3$，取 x＝3，表示用 3 位表示子网。

第三步　其对应十进制数值为 $2^7+2^6+2^5=128+64+32=224$，子网掩码是 255.255.255.224。

第四步　子网基数＝256－224＝32，N＝1～6(6 个子网)，则子网地址为 202.119.200.32，202.119.200.64，202.119.200.96，202.119.200.128，202.119.200.160，202.119.200.192。

第五步　子网内有效主机数 $2^5-2=30$ 个，网络内总的主机数为 30×6＝180 个。

任务布置

1. 等长子网划分

(1) 等分成 4 个子网

假如单位有 4 个部门，每个部门有 60 台网络终端，现使用 192.168.0.0/24 的内网网络地址。规划每个部门的终端位于独立的网段，如何划分子网？每个子网的可用地址范围是什么？

(2) 等分成 8 个子网

假如单位有 8 个部门，现使用 192.168.0.0/24 的内网网络地址。规划每个部门的终端位于独立的网段，如何划分子网？每个子网的可用地址范围是什么？

2. 变长子网划分

如图 1－38 所示，网络地址 192.168.0.0/24 的内网要划分成 5 个网段：三台路由器分别连接三个交换机，每个交换机各自连接 20 台、50 台、100 台计算机，路由器之间也要规划网段，请写出规划的接口地址或地址段(见表 1－7)。

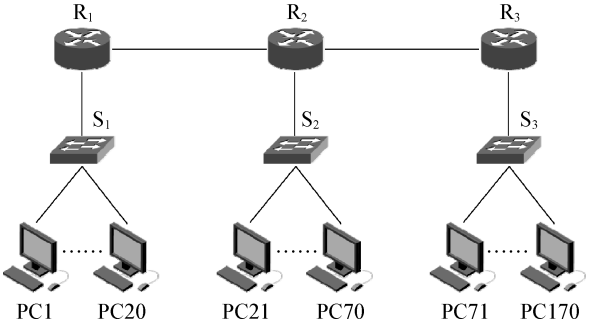


图 1－38　可变长子网示例

表 1-7　地址规划填写

设备	设备接口地址	分配地址段
R_1		/
R_2		/
R_3		/
PC1～PC20	/	
PC21～PC70	/	
PC71～PC170	/	

1.4　园区网组建与业务部署

需求分析

在万物互联时代，随着物联网、云计算、超宽带、大数据和 AI 等技术的成熟，园区将实现完全数字化，园区内万物都会产生数据。这些数据既代表物，也代表物的状态，甚至代表人工定义的各类概念。超宽带技术使网络带宽不再是瓶颈，一切数据皆可实时上云，并实时参与计算。在云计算超强算力和各种数学分析模型的帮助下，AI 系统不断挖掘这些大数据代表的事物之间的复杂联系。园区网要发展成为智慧型、智能性网络，将实现园区内各业务数据共享共用，是各种业务终端和园内外所有数字化系统的信息基础平台。

知识学习

1.4.1　园区专网

园区专网是指园区内部的专用网络，融合网络资源一张网包括核心骨干网络、有线网络、无线网络、物联网络四个部分：

一、核心骨干网络

实现一网多用，是园区的骨干网络，作为多网融合的承载，需要具备如下能力：

1. 具备 SDN 自动化部署

网络通过控制器实现全网设备资源云化管理机构，有线无线，物联网关设备统一运维，全网设备，即插即用，全自动化部署，替换免配置。

2. 超宽架构

接入至汇聚采用 10GE 链路双上行互联；汇聚至核心采用 100GE\40GE 链路互联，实

现 GE 到桌面，满足 10G Wi-Fi 上行接入、POE＋＋供电，保障未来 5～10 年网络业务扩容需求。

3. 全智能化

支持全智能网络，通过 AI 技术搭建智能化联接、运维、学习的三层 AI 架构网络，实现网络运维智能化网络运维；用户体验智能感知，用户接入网络全旅程感知；业务智能化保障，可以实现加密流量与私有定制业务的智能匹配，满足关键业务的 SLA 保障；网络安全态势智能感知，防止加密流量攻击与内网攻击横向扩散。

4. 一网多用，按需定义

实现办公、物联、安防等网络的统一承载，通过 VXLAN 或者其他虚拟网络技术对个专网进行虚拟化隔离。面向未来快速发展的 ICT 业务，通过虚拟网络可以在不改变物理网络架构基础上，实现业务网络的“快速任意重定义”，支撑数字化快速创新。

5. 弹性扩展，权限随人或物而行

通过多种接入方式全面覆盖的一张物理网络，在提供无处不在的网络连接基础上，通过云化网络架构实现网络边界的弹性扩展，让网络随时跟随园区物理世界的延伸而延伸。面向各种类型的终端及物联传感器、仪表接入。终端从园区任意接入，不影响其网络访问权限、体验，并保证不同类型的终端与业务的相互隔离与安全性。

6. 全网高可靠性

从接入到汇聚到核心均可支持双上行，网络可靠性高。

二、无线网络

无线 WiFi 网络是当今移动终端接入采用的最广泛的技术，直接影响用户互联的体验。室内外的全面覆盖能够真正实现终端无缝接入的体验。同时考虑到高速、高密度的用户接入能力应采用当前最新的 WiFi6 技术进行部署。WiFi6 AP 可以提供高达 10Gbps 的吞吐量，有线回传推荐使用支持 MultiGE 技术的大容量接入交换机。结合物联及传输对象，也存在蓝牙、RFID、红外、UWB、Zig-Bee、LoRa、NB-IoT、NFC 等多种协议。

三、有线网络

有线网络从功能覆盖区域来看，可以分为两类：办公以太网络，主要是服务于办公设施，满足桌面千兆接入；住宅网络，考虑到流量主要以南北向的互联网接入为主，且房间密度较高，运维环境复杂，可选 POL 网络 或敏捷分布式 AP 部署；POL 网络技术也可广泛应用于出(售)租办公、医院、小商铺等建筑类型。

四、物联网络

作为智慧园区的基础承载，涉及到室内外数千的传感节点的互联，根据不同的部署环境、供电情况，考虑基于 Hi-PLC(宽带电力线载波)、WiFi 与 IoT 融合的无线近场接入结合智能终端匹配以太网络，与边缘计算物联网关一起，实现室内外的全面覆盖，满足物联设备的智能匹配，安全准入，传感信息的实时回传，边缘计算等园区物联网联接需求。

1.4.2 园区网络的分类

园区网络是一个在连续的、有限的地理区域内相互连接的局域网。园区是一个连续的有限区域，不连续区域的网络会被视作不同的园区网络。很多企业和校园都有多个园区，园区之间通过广域网技术进行连接，如图 1－39 所示。

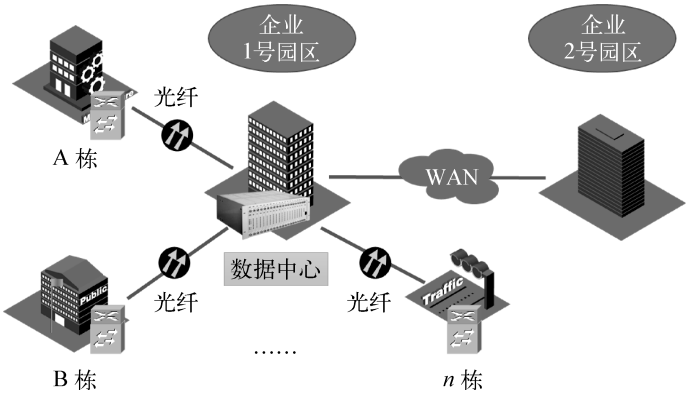


图 1－39　企业园区网络的基本架构

园区网络的规模可大可小，小的有 SOHO(家居办公室)，大的有校园、企业、公园、购物中心等。园区的规模是有限的，一般的大型园区，例如高校园区、工业园区，规模依然限制在几平方千米以内，在这个范围内，可以使用局域网技术构建网络。超过这个范围的“园区”通常被视作一个“城域”，需要用到城域网技术，相应的网络会被视作城域网。园区网络使用的典型局域网技术包括遵循 IEEE802.3 的以太网技术(有线)和遵循 IEEE802.11的 WLAN 技术(无线)。

一、按照规模大小分类

按照终端用户数量或者网元数量，可将园区网络分为小型园区网络、中型园区网络和大型园区网络，见表 1－8 所示。

表 1－8　园区网络规模大小分类

园区网络分类	终端用户数量(个)	网络数量(个)
小型园区网络	＜200	＜25
中型园区网络	200～1 000	25～50
大型园区网络	＞1 000	＞50

一般来说，大型园区网络需求和结构复杂，管理维护的工作量很大，因此，会有专业的运维团队负责整个园区的 IT 管理，包括园区网络的规划、技术和故障处理。同时运维团队会构建完善的管理维护平台，协助完成运维工作。

二、按照承载业务分类

从网络承载的业务来看，园区网络可以分为单业务园区网络和多业务园区网络。承载业务的复杂程度决定了园区网络架构的复杂性。

早期的园区网络通常只承载数据业务，园区的其他业务有其他专网承载。现在的多数中小企业网络业务单一，因此，企业的园区网络仅需要承载内部的数据通信业务，单业务园区网络的架构会趋于简单化。

先进的大型网络通常服务于独立的大型园区。园区需要提供各种基础服务，比如视频监控、车辆管理、能耗控制和身份识别等。如果在大型园区内为每种服务各自部署专门的网络，成本会很高，且管理维护非常麻烦。因此，这些基础服务的技术逐步转向数字化和以太化，以便使用成熟的以太网承载。园区网络逐渐多业务化，一个网络要承载多种不同的业务，不同的业务间需要实施隔离和保障，园区网络架构也开始复杂化和虚拟化。

三、按照接入方式分类

从接入方式看，园区网络可以分为有线园区网络和无线园区网络。当前园区网络多数为有线和无线的混合网络。无线园区网络不受端口位置和线缆的限制，网络使用自由，部署灵活。

传统的园区网络是有线园区网络，每台接入网络的设备都需要通过线缆连接到网络上，不同连接之间基本不存在相互的影响。因此，有线网络的架构通常是结构化、层次化的，逻辑清晰，管理简单，故障易于排查。

无线园区网络和有线园区网络的特征差异很大。无线园区网络通常基于 IEEE802.11 标准(WLAN)，网络部署和安装质量会决定网络覆盖的效果，且需要定期针对网络业务情况实施网络优化，才能保证网络质量。

四、按照不同行业分类

典型的行业园区网络包括企业园区网络、校园网、政务园区网络、商业园区网络和住宅小区网络，下面简单介绍其中的几种：

① 企业园区网络：企业园区网络范畴很大，可以按照不同行业再往下细分。这里介绍的企业园区网络实际上特指的是基于以太网交换设备组建的企业办公网。企业办公网的组网架构一般与企业内部组织架构相对应，如图 1－40 所示。

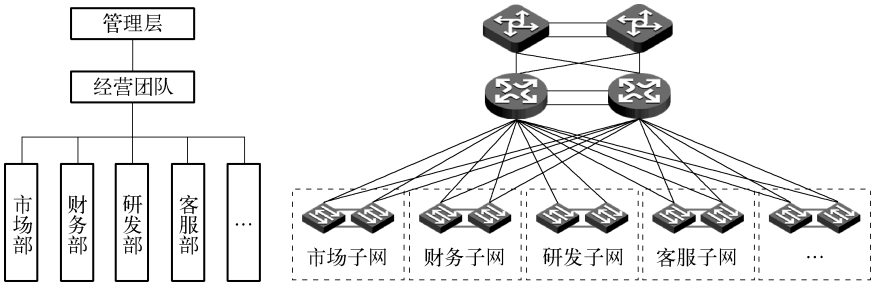


图 1－40　企业园区网络架构

② 校园网：根据教育对象的不同，校园可以分为普教园区和高教园区。普教园区面向的是中小学生和教师，内部网络结构和功能更接近企业园区网络。高教园区网络要复杂得多，不但有并行的教研网和学生网，同时还有运营性的宿舍网络，对网络的部署方式和可管理性有特别高的要求。网络不仅承担数据传输的功能，还需要承担一定的研究和教学功能，因此，对其先进性有较高要求，同时需要对在校学生的上网行为进行管理，避免出现偏激出位的行为。

③ 政务园区网络：一般指政府相关机构的内部网络，对安全性要求极高，通常采用内网和外网隔离的措施保障涉密信息的绝对安全。

1.4.3 园区网络的构成

园区网络虽然多种多样，但是园区网络按业务架构可以抽象成具有不同层次部件的统一模型，如图 1－41 所示。无论未来园区技术发生何种变化甚至革新，都可以归结为这种统一模型。

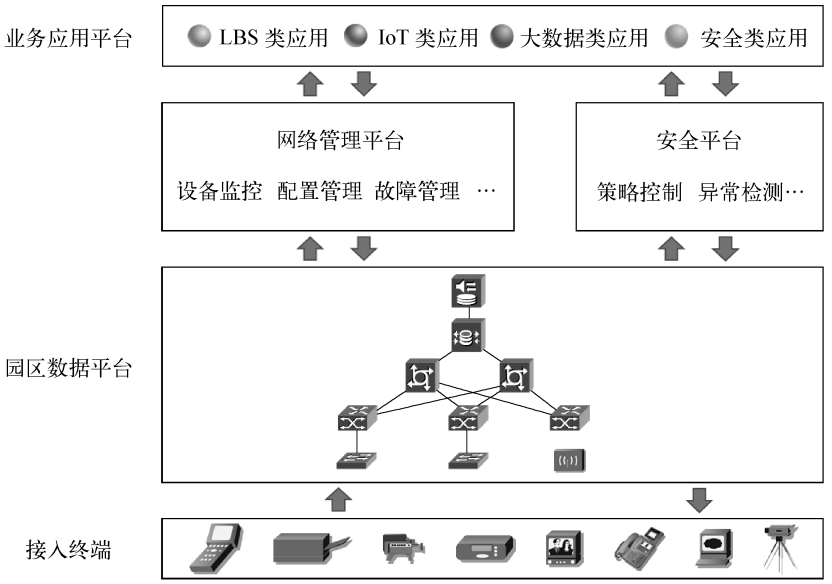


图 1－41 园区网络的统一模型

一、数据网络

园区数据网络是基于以太网技术或者 WLAN 技术构建而成的，由园区内部所有数据通信设备构成，包含各类以太网交换机、AP（接入点）、WAC（无线接入控制器）和 FW（防火墙）等，所有的内部数据流量都会经过园区数据网络进行转发。

园区数据网络通常由多个子网构成，用于承载不同的业务，比如所有园区都会有的办公子网，用于日常员工办公；很多园区内部会保留独立的视频会议子网，并通过专门的子网和链路保证视频会议的质量；园区数据网络会接入 IoT 设备，会有专门承载物联网业务

数据的子网，而且由于提供不同业务的物联网技术不同，往往存在多个并行的物联网子网；另外，一般园区会有内部的数据中心，承载数据中心内部转发的子网被称为数据中心网络。

二、接入终端

在园区网络中，终端的所有者可能是网络管理者，也可能不是网络管理者，但可以通过管理手段获得权限，从而对园区内部的终端实施管理。这样，园区数据网络和接入终端可以充分互动，形成端到端的网络，提供更为优质的服务。例如，指定终端安装防病毒软件，接入网络前进行检查，在降低病毒对网络威胁的同时，也简化了网络的防病毒解决方案。

办公、医疗、商场、场馆……当前有越来越多的业务是通过手机、平板等移动端设备进行应用，还有很多五花八门的物联网设备也被部署在网线无法触达的边缘地带，它们所产生的数据也自然只能由 5G、Wi-Fi 等无线网络来进行承载。也正是因为部署灵活、接入便利的无线网络普及，才可以让海量数据被统一收集、分析、处理，从而促进了智慧园区的产生，促使企业由信息化向着数字化的方向转变。

三、网络管理平台

网络管理平台是一个传统的部件，但在最新的园区网络架构中，网络管理平台的定位和它的动能都发生了质的变化，新一代的网络管理平台不但具有网管的全部功能，而且能够对常用场景或者流程实施自动化管理。该平台可以实现物理网络与业务虚拟网络的分离，物理位置的变化不会影响到虚拟网络，当物理位置发生变化时，业务与用户对应的资源（如 IP 地址、安全资源、隔离通道等）和策略（如网络策略、安全策略等）可以动态跟随，从而实现管理员零干预，大大提高了运维管理的效率。

四、安全平台

基于新一代的网络管理平台还可以构建新一代的安全平台，通过调用管理平台提供的南北向接口，再结合采集到的网络大数据，提供智能化的安全管理。在海量设备接入之后，园区的网络中既有需要移动办公的内部用户，也有需要接入控制的外来人员，还有需要获得更高权限的管理者以及海量的物联网设备。因此，能够针对不同场景提供灵活、安全的接入认证方式，并且对于接入的员工、用户和设备提供不同层级的安全防护，就成为智慧园区网络安全统一管理的新挑战。

能够针对不同场景提供灵活的安全的接入认证方式，并且对于接入的员工、用户和设备提供不同层级的安全防护。只有已授权用户，才可以接入网络，通过局域网进行浏览、审批、收发邮件等移动办公应用。支持多种无线安全防护手段，可以抵御常见的无线网络安全威胁，如钓鱼 AP 等。

提示

园区网络经历了几个阶段的演进，在带宽、规模以及业务融合等几个方面都有了长

足的发展。然而，随着行业数字化转型的推进，园区网络在连接、体验、运维、安全、生态等几个方面又面临新的挑战，例如，IoT 业务园区连接无处不在；高清视频、AR(增强现实)/VR(虚拟现实)等业务需要高品质的网络支撑；海量的设备需要极简的业务部署和网络运维等。

为了应对上述挑战，业界厂家也逐步将 AI、大数据等新技术引入园区网络，并推出一系列新的解决方案，例如管理全面 SDN 化、架构全面虚拟化、接入全面无线化、业务全面自动化等。园区网络进入新一轮令人激动的技术创新演进阶段，这一阶段的园区网络逐步具备了智能化的特征。

1.4.4 园区网络设计

园区的建设是一个系统工程，它涉及多个设计细节和执行环节，需要从园区整体的高度全盘考虑，并经历一个酝酿、启动、发展的过程。系统规划既要从时间上、发展上进行纵向的考虑，又要从各个部门协调运作的横向关系上考虑；既要考虑信息基础设施建设、软件系统的建设、安全保障系统的建设等建设项目的分步实施，又要考虑这些建设项目的协调发展，最终达到以园区各类应用和信息资源建设为基础，以公众、企业为核心，面向园区管理、园区文化建设、园区生活等多层次的信息化应用，提供综合的信息资源共享和业务协同服务，构建信息化环境。

一、网络设计流程

网络设计是根据用户的网络环境和业务需求，设计合理的网络架构和技术方案的过程。不同场景对网络的要求是多种多样的，比如可靠性、安全性、易用性等。做好网络设计的前提是了解网络需求及网络现状。网络设计的流程如图 1-42 所示，简要来说首先进行需求调研，然后根据调研结果进行需求分析，最后根据需求分析的结果进行方案设计。

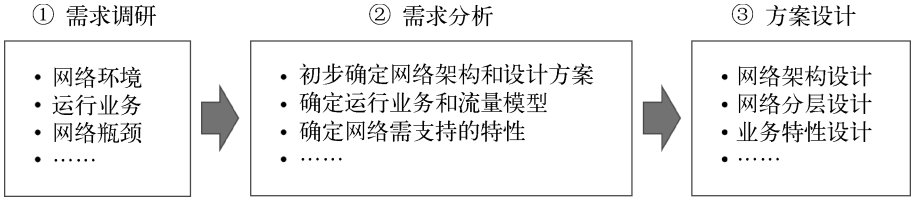


图 1-42 网络设计流程

二、网络需求调研与分析

网络需求调研与分析一般从网络环境、网络瓶颈、网络业务、网络安全、网络规模、终端类型等 6 个方面展开，下面从总体需求和其中 3 个方面的细分需求进行详细说明。

表 1-9　园区网络的总体需求

编号	需求分类	主要调研内容	调研的主要目的
1	网络环境	网络的建设、部署和使用情况，明确是改造网络还是新建网络	初步确定网络架构和设计方案
2	网络瓶颈	现有网络的瓶颈问题（改造场景），或者对网络的更高要求	确定网络建设的要求和目标，初步确定网络需支持的特性
3	网络业务	网络中需要部署的业务及其特性，明确网络的业务和流量模型	确定网络带宽和业务特性
4	网络安全	业务是否需要隔离以及相应的隔离要求（可选），网络安全建设的要求	确定业务隔离和网络安全防御系统的建设方案
5	网络规模	网络的用户规模以及 3～5 年内的增长态势	最终确定网络架构与设计方案
6	终端类型	终端类型及接入要求	确定网络接入方案

表 1-10　需求 1：网络环境调研

编号	调研分类	调研目的	调研内容
1.1	建设类型	明确是新建网络还是改造网络	如果是改造网络，则网络设计的复杂度增加，需要考虑更多内容，如设备的兼容性和新旧问题、网络如何平滑过渡、业务是否允许中断等
1.2	网络类型	明确是有线、无线还是有线和无线一体化融合	确定是否需要同时建设有线网络和无线网络，是否需要一体化融合
1.3	地理分布	明确园区地理分布是集中还是分散	初步确定基础网络架构，如果地理位置比较集中，可考虑单核心架构；如果地理位置比较分散，位于多个建筑物甚至多个不同地点，且各点流量比较大时，需要部署多个核心或汇聚点
1.4	组织架构	了解客户单位的组织架构，了解园区网络的大致使用情况	包括客户单位各组成机构如何使用网络，其网络如何部署；是否需要根据部门、区域、业务等情况来设置网络隔离；是否需要部署多个核心或汇聚点；是否有分支接入要求；如果有分支接入，需要采用何种线路接入
1.5	弱电分布	了解机房或网络设备弱电间的分布情况	当机房或弱电间比较多时，通常可以将网络各层以分布式的方式部署到各个机房或弱电间，即每个机房或弱电间部署一个汇聚点；此外，还要考虑设备摆放的布局及其间隔的距离等问题

表 1-11　需求 3：网络业务调研

编号	调研分类	调研内容	调研分析
3.1	常用业务	常用业务类型，包括办公、电子邮件、上网等	正常的办公业务对网络带宽的要求不高，通常为 300 kbit/s
3.2	关键业务	关键业务类型，包括数据、VoIP、视频、桌面云等	园区网络属于局域网，基本不考虑网络时延问题；如果有桌面云的需求，部署时需要重点考虑网络的可靠性或可用性；如果有视频直播的需求，部署时要重点考虑带宽要求；如果有 VoIP 的需求，部署时要考虑 VoIP 与数据业务组网方式以及 PoE 供电等

续 表

编号	调研分类	调研内容	调研分析
3.3	特别业务	需要特别关注的业务	优先保障客户重点关注的业务，引入 QoS 设计保证客户体验
3.4	未来业务	未来 3～5 年内新增业务的类型	要考虑 3～5 年内业务发展的可能性，实现业务的平滑升级和扩容，避免资源浪费或无法满足使用需求
3.5	业务环境	现网业务环境	现有网络运行的主要网络协议、网络拓扑和设备类型、数量，了解现有网络的网络质量及其对当前业务的支撑情况

表 1－12 需求 5：网络规模调研

编号	调研分类	调研内容	调研分析
5.1	有线接入	有线用户或接入点规模	确定接入交换机的端口数量及密度，根据业务情况初步确定网络带宽需求
5.2	无线接入	无线网络规模	确定 WAC 的规格和 AP 的数量；确认在一些重点区域是否存在高密度接入
5.3	现有网络情况	现有网络的情况及规格	了解网络改造的工作量，确定网络升级方案，包括设备利旧、兼容性、平滑升级等方面的内容
5.4	未来网络增长	3～5 年后的网络规模或最高增长率	网络设计要满足可扩展性要求，应当考虑园区网络在未来 3～5 年的发展需要，在设计时其网络接口、容量和带宽均需要一定的余量，以便未来平滑扩容
5.5	分支情况	分支机构分布情况	考虑分支的数量，分支与总部的距离、连线方式，链路是否需要备份等

三、智慧校园网部署案例

高等院校的校园网是为学校师生提供教学、科研和综合信息服务的网络平台。校园网的用户人数少则几千人，多则几万人，属于典型的典型园区网络。高校一般会有新老两个校区甚至多个校区，不同校区可能分布在一个城市的不同区域，也有可能在不同城市。

智慧校园项目建设按照“合理新增、充分利旧、整体优化、统一运管”的原则，对老校区已有有线信息点梳理，完成网络融合和优化，对新校区网络进行网络规划与新建。网络建设要求有线、无线一体化校园网，覆盖大学校区的各主要建筑物，构建基于以太网组网架构的广覆盖、统一认证、统一管理的规范化校园网络。

1. 建设目标与需求分析

建设目标大致分为三个方面，列举如下：

① 多网融合：构建能够承载有线网络、无线网络及物联网的综合型网络，使校园网能够满足校园内各种数据终端及传感设备在任意位置接入的需求。

② 架构先进：整体架构在性能、容量、高可靠性及技术运用等方面至少在 5 年内保持

领先性。

③ 按需扩展：整体网络架构能够实现按需扩展，并无需对架构进行调整。

2. 整体网络规划

园区网络一般可以划分为终端层、接入层、汇聚层、核心层等，各层分区模块清晰，模块内部调整涉及的范围小，易于进行问题定位。

图 1－43 是智慧校园网的一般抽象模型。通过构建一个超宽融合的承载网络，接入整个校园所有的业务子系统及终端，实现全联接校园；然后从核心层到接入层，利用虚拟化技术，构建基于不同业务规划的虚拟网络（VN）；最后，SDN 控制器完成网络的自动化部署，实现智慧校园网的目标。具体的规划项和说明见表 1－13 所示。

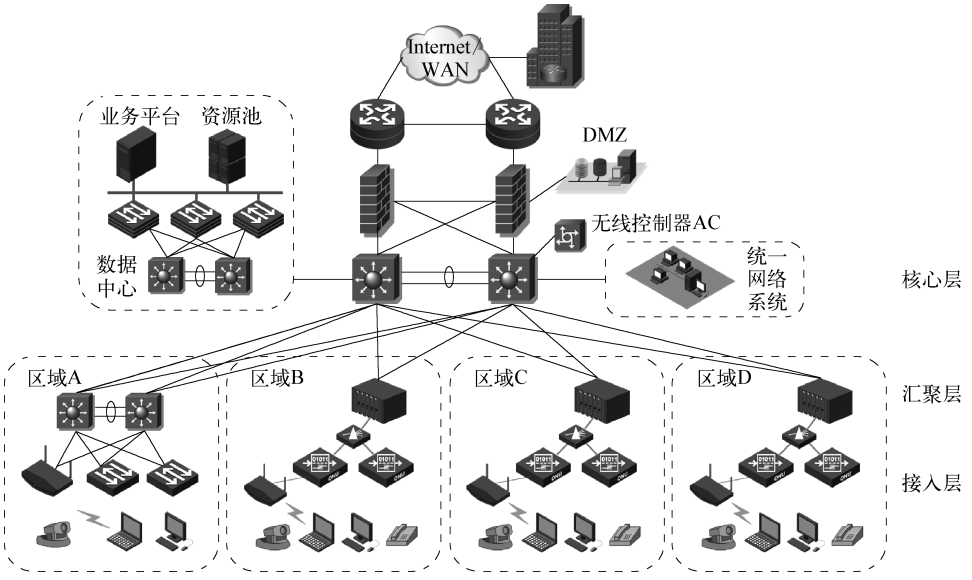


图 1－43　智慧校园网的一般架构

表 1－13　智慧校园网规划项及说明

序号	规划项	规划说明
1	管理网络和开局方式规划	包括管理网络、开局方式
2	物理网络规划	包括设备级可靠性、链路级可靠性、OSPF 路由、BGP 路由
3	逻辑网络规划	包括设备角色及用户网关规划、Border 节点到出口网络规划、VN 及其子网规划、VN 间互访规划
4	出口网络规划	包括防火墙的安全区域规划、防火墙的双机热备及智能选路规划
5	业务部署规划	包括用户接入规划、网络策略规划

3. 管理网络规划

管理网络规划分为带外管理和带内管理两种。带内管理是指使用设备的业务口进行设备管理。带内管理的优势是不需要额外增加管理网络的建设成本，缺点是业务网络如果出现问题，可能会影响管理员登录设备。带外管理是采用设备专用的管理口进行设备

管理，优势是可以实现管控分离，缺点是会增加额外建设管理网络的成本。

举例说明，京华大学出口设备和核心设备都部署在核心机房，地理位置集中，额外建设管理网络代价较小，因此采用带外管理方式。此外，由于设备上运行的业务复杂，开局通常要求网络工程师现场调测，采用命令行或者 Web 网管开局。接入层和汇聚层设备种类、数量众多，部署位置分散，从提高管理效率出发，推荐采用带内管理方式、即插即用开局。管理网络和开局方式规划见表 1－14 所示。

表 1－14　管理网络和开局方式初步规划

区域	设备	管理网络规划	开局方式规划
出口	防火墙	带外管理	本地命令行或 Web 网管
核心层	核心交换机	带外管理	本地命令行或 Web 网管
汇聚层	汇聚交换机	带内管理	即插即用
接入层	接入交换机	带内管理	即插即用
	AP	带内管理	即插即用

4. 物理网络规划

(1) 设备级规划要点

核心层、汇聚层及接入层采用堆叠或集群技术将两台及两台以上的交换机横向虚拟成一台交换机，并提供设备的冗余备份。

交换机设备采用堆叠或集群的方案避免了传统冗余组网时的二层环路，不需要再配置复杂的破环协议。另外，在三层网络中，堆叠或集群的系统内共享相同的路由表，缩短了网络发生故障时路由收敛的时间，堆叠或集群系统的方案使网络更易于管理、维护和扩展。

(2) 链路级规划要点

链路的冗余设计是链路级规划考虑的主要问题。在园区网络中，通常通过设备间采用的双上行链路的冗余设计来提高设备间链路的可靠性，同时对于冗余链路，常用链路聚合技术将多条物理链路通过 LACP(链路聚合控制协议)虚拟成一条逻辑的汇降(Trunk)链路，链路聚合后的接口为 Trunk 接口。链路聚合技术一方面加强了设备间链路的可靠性和链路的冗余备份；另一方面，在不升级硬件的基础上增加了链路的带宽。

(3) OSPF 路由规划

物理网络要为逻辑网络提供路由可达的承载网络，一般采用 OSPF、IS－IS 等 IP 单播路由协议。在园区网络中主要通过 OSPF 路由实现 IP 网络互通，而且 OSPF 路由技术比较成熟，网络建设的运维人员经验丰富，因此，物理网络的路由互通推荐使用 OSPF 协议。

如图 1－44 所示，核心层、汇聚层、接入要规划好互通的 IP 网段，配置 OSPF 路由协议，完成 OSPF 区域管理来实现路由的自动部署，并配合实现 BGP 源接口(Loopback0)之间的互通。

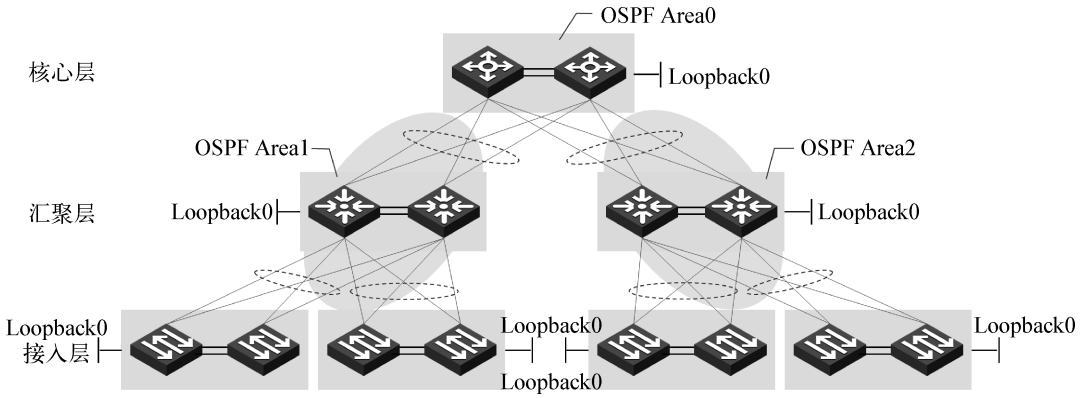


图 1-44　物理网络的 OSPF 路由规划

5. 逻辑网络规划

在逻辑网络规划方案中，每个虚拟网络(VN)是一个 VPN 实例，一个 VN 中可以包含多个子网。同一个 VN 内的用户可以互通，不同 VN 内的用户是路由隔离的。VN 可以依据以下原则进行规划：

① 独立的业务部门作为一个 VN。

② 同一业务部门内用户身份的差异要求可以利用不同 VN 实现，可以通过基于用户角色划分的安全组的组间策略来管控。

根据高校的教学特点，将虚拟网络划分成教学专网、校园一卡通专网、资产管理专网、物联网专网等各种类型专网。因此，在设计网络时，需要先规划好物理网络的 VLAN 和 VN 子网的映射关系，同时配置有线用户和无线用户的 VLAN。

任务布置

➢ 为了打造端到端的智能园区网络解决方案，华为、中兴通讯、新华三等设备厂商提供了从接入层、汇聚层、核心层再到管理层部件的全系列组件。

请列举并分析某一品牌厂商的系列产品，介绍相关组件的应用场景和主要的功能特性，对园区网络做出统一的规划部署。

➢ 业界普遍认为自动驾驶是园区网络未来的发展方向之一。自动驾驶从 L3 开始具备自主意识，到了 L4 级，可以将园区网络作为基础的数字孪生发展到极致，网络自身具有预测性。随着万物互联时代到来，网络也将向 L5 级自动驾驶转变，由此看出整个园区内的所有事物都是数字孪生对象。

请展望和分析未来 L4 级和 L5 级自动驾驶网络的形态。

任务总结

本节工作任务是关于网络规划设计，需要学习并掌握网络基础知识和基本概念，尤其关于规划设计方面的理论和实践是本节任务的重点和难点，希望通过本节任务的学习，能够在这方面打下坚实而稳固的基础。学习完本节内容后，能够掌握网络分类和拓扑结构、OSI 参考模型、IP 地址和子网掩码计算，了解网络性能指标和常见网络设备、TCP/IP 协议体系结构、IP 协议基本概念以及园区网络的分类和构成。在技能操作方面，要能够使用 Wireshark 软件完成数据的抓取、分析等操作，熟练掌握小型网络 IP 参数规划方法。

本节工作任务主要依托“京华大学校园网络建设一期工程”项目，完成以校园网为代表的“园区网络规划与设计”任务。本节从网络组建基础知识出发，包括网络分类和拓扑、性能指标、网络设备等内容，然后到国际标准化组织制定的网络协议架构到常用协议，再到 IP 协议的工作原理以及 IP 参数的规划设计，最后将所学知识应用于园区网络尤其是智慧型园区网络的设计、运维和管理上。

本节内容始终以企业需求为导向，通过实际案例和现网设备的学习和介绍，将企业最新网络技术、工程经验和教育资源融入教学内容中，确保学习者能够掌握到最先进和最实用的网络技术，为将来走向工作岗位打下坚实的基础。

为了把复杂的内容讲解得尽可能通俗易懂，本节采用由理论学习到任务布置，教学方法上建议采用混合教学、翻转课堂和进阶课堂等，并加入国家通信技术专业教学资源库的各类信息化、数字化资源，包括大量微课、课件和动画。

思考与案例

任务思考

1. 数据链路层是由 MAC 和 LLC 两个子层构成，这两个子层分别实现什么功能？
2. 当应用数据从源主机的高层传递到底层时，将会做什么操作？
3. TCP 通过什么机制来保证传输的可靠性？
4. 随着以太网技术发展，早期共享式集线器比起以太网交换机有哪些不足？
5. ARP 是什么协议？它的作用是什么？
6. 某公司被分配了一个 172.16.100.0/20 网段，根据公司需要将设计部、研发部、市场部、客服部 4 个部门进行网段隔离，每个部门内部在一个网段；设计部、研发部可以支持至少 100 个可用 IP 地址，市场部、客服部可以支持至少 50 个可用 IP 地址，请合理规划网段。

工程案例

1. 案例描述

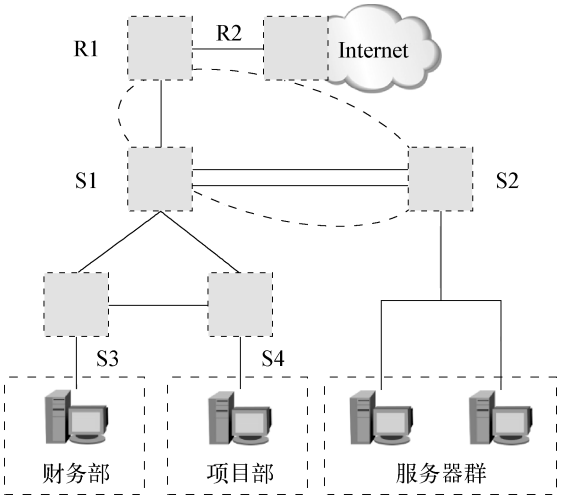
BAT100 公司新建办公大楼网络建设项目实例。

2. 案例要求

(1) 根据拓扑图,填写设备所属区域;

(2) 根据拓扑图的要求,完成网络设备类型、品牌型号选择;

(3) 根据拓扑图的要求,填写接口 IP 地址规划。



设备命名	所属区域	设备类型	建议品牌、型号	IP 规划
R1				
R2				
S1				
S2				
S3				
S4				
Manager				
备注	选项:园区网出口、核心机房、财务部、项目部、服务器群	选项:路由器、三层交换机、二层交换机、网管计算机		