引　　言

计算机网络，是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统，网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

21 世纪的人类社会是一个信息爆炸的社会，信息膨胀的主要原因，在于 20 世纪后半叶科技发展的一个突出成就——计算机及网络的发展。计算机网络技术的发展深刻影响了人类的文化，为信息的发展带来了新的动力，从本质上引起了一场信息的革命，促生了一种新的信息形态——网络文化。生活在今天人们，已经充分认识到信息的重要性，因此各种信息传播和信息共享的技术就成为非常热门的技术。

在学习了计算机网络的相关基础知识以后，如何设计、规划和组建各种实用的计算机网络，通过网络间的互连为用户提供高效的网络服务和信息共享，就成了一种重要的职业追求。这一类职业有哪些技术素质需求，怎样开展这一类工作呢？

网络在我们生活中随处可见，如下情境中所描述的网络应用，是本引言中所描述的知识发生场景。

情 境 描 述

小明是信息学院新入学的新生。宿舍中有来自各地的 5 名同学。由于大家是计算机专业的学生，因此都购买了计算机。

开学之初，开设了一门设计课程，大家需要在各自的电脑上安装一个 200MB 的软件。由于都没有购买 U 盘、移动硬盘等移动存储介质，而宿舍中只有一台计算机上有这个软件的备份，怎样通过联网，让每一台终端上都拥有这一软件并完成安装呢？

通过以上网络情境的描述，需要理解以下网络知识：如何把多台分立的计算机连接起来组成网络？使用什么样的方式连接？如何共享网络中的计算机资源？

知 识 储 备

1. 将两台终端连接成网络

关于两台计算机的连接，我们比较熟悉，只要接成对等网即可。所谓对等网，就是网络中各台终端的作用和地位是相同的，没有主从之分。其实多台连接的原理也是一样。

知识回顾：两台电脑组成对等网

在先前的算机网络课程学习过程中，应该已经掌握了两台电脑组成对等网的知识。利用这种方式来连接两台电脑时，需要先准备两块有 RJ-45 接口的网卡、两个 RJ-45 水晶接头和一段双绞线。首先，我们需要自己将双绞线制作成一根交叉线，也就是通常所说的 TIA568A 标准线缆。

接下来，我们打开机箱，将网卡安装在计算机主板的插槽上。需要注意的是，由于网卡可能与声卡、显卡互相产生干扰信号，因此需要把网卡安装在远离它们的插槽中。安装好网卡后，盖上机箱，用事先制作好的交叉网线将两台计算机连接好。

2. 多台终端的星型连接

所谓星型连接，就是用一台网络设备将多台计算机连接在一起，形成的一种拓扑结构，如图 1 所示。根据其数据转发方式的不同，又可以分为共享型和交换型，这一概念将在后面做具体说明。采用星型连接，当一台计算机终端需要向另一台计算机终端发送数据时，就可以通过中心网络设备转发。

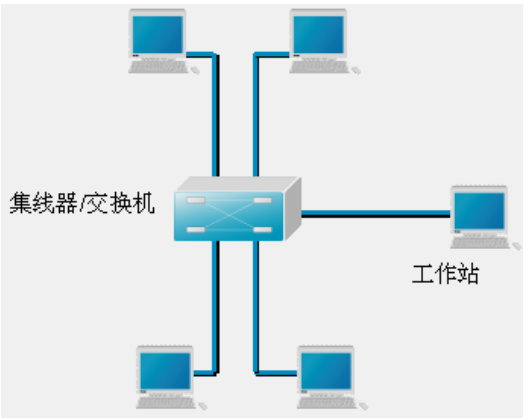

图 1　星型网络拓扑

以星型连接组网时，大都通过交换机(Switch)连接，即以交换机作为中心网络设备。硬件安装方面相当简单，只需每台计算机装有一块带有 RJ-45 接头的网卡，然后用带有 RJ-45 接头的直连网线接到交换机上就可以了。

连接完成后，在所有计算机“网上邻居”的属性中启用相应的协议。其具体操作步骤如下。

(1) 在桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，将弹出图 2 所示的界面。

(2) 双击界面中的“本地连接”图标，弹出图 3 所示的“本地连接状态”对话框。

(3) 单击图 3 对话框中的“属性”按钮，弹出如图 4 所示的“本地连接属性”对话框。直接单击“安装”按钮，在出现的图 5 所示的“选择网络组件类型”对话框中选择“协议”组件，单击“添加”按钮，然后选择要添加的协议。为了完成以上网络情境中所描述的组

建宿舍网络的项目，需添加“TCP/IP 协议”和“NETBEUI 协议”(默认的情况下，Windows XP 操作系统中，这些协议已经安装成功)。

图 2　本机上所具有的网络连接

图 3　“本地连接状态”对话框

图 4　“本地连接属性”对话框

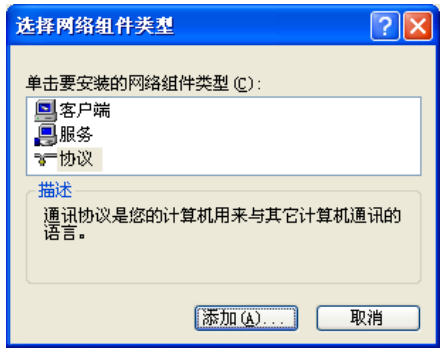

图 5　添加“协议”组件

(4)　按照图 1 所示的网络拓扑，把宿舍中的 5 台终端计算机连接在一起，组建成“情境描述”中所描述的宿舍网络。由于是连接在一起的共享网络，需要把所有计算机的 IP 地址规划在同一网段上。根据地址规划原则，各台计算机的 IP 地址分别规划为 192.168.0.1/24、192.168.0.2/24、192.168.0.3/24、192.168.0.4/24 和 192.168.0.5/24(其中的/24 表示子网掩码的长度，即 11111111 11111111 11111111 00000000，十进制为 255.255.255.0)。

(5)　在图 4 所示的“本地连接属性”对话框中选择“Internet 协议 TCP/IP”列表项后，

单击“属性”按钮。在弹出的图 6 所示的“Internet 协议(TCP/IP)属性”对话框中设置。

完成了上述操作以后，接下来只需要让所有的工作站处于同一工作组，并且具有互相不冲突的计算机名即可。配置计算机名的操作如下。

(6) 从“控制面板”中启动“系统属性”，或从桌面上右击“计算机”，选择 “属性”菜单命令，打开图 7 所示的“系统属性”对话框。

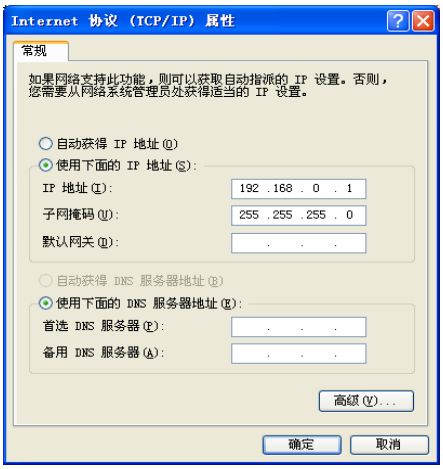

图 6 IP 地址配置

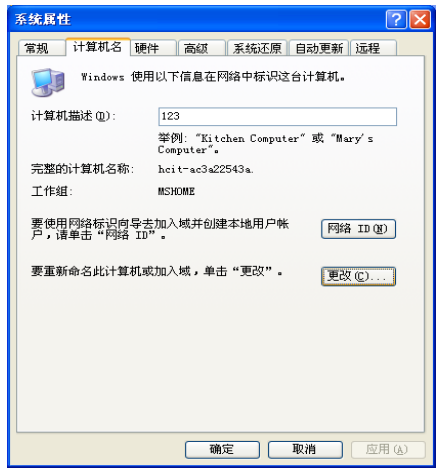

图 7 “系统属性”对话框

(7) 单击“计算机名”选项卡，然后单击“更改”按钮，可以在弹出的如图 8 所示的对话框中，完成计算机名称的更改，同时，也可以完成工作组的更改。

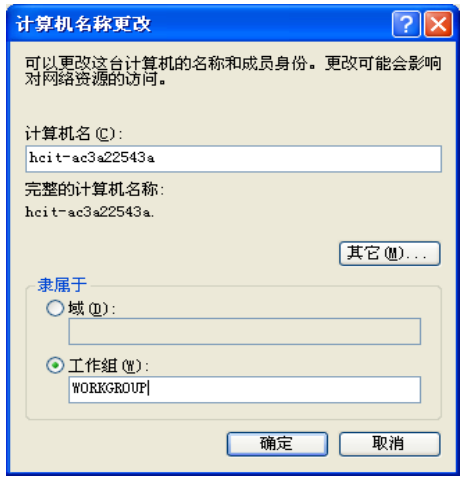

图 8 更改计算机名称

更改的要求就是：使想要进行通信的所有计算机处在同一个工作组中。注意：这里暂时不考虑“域”的问题，否则会带来其他不必要的麻烦。计算机名如果没有一样的，或者说没有冲突，就可以不做处理，工作组的名称在这里就叫 WORKGROUP 即可。

现在可以进行信息共享了。例如，图 1 中标有“工作站”的那台计算机中有所需的应

用软件，将软件所在的文件夹共享，现在别的联网用户就可以从“网上邻居”里找到所需的软件，并传输到自己的计算机中了，从而实现了网络情境描述中的工作任务内容。

自己动手：把以上操作内容自己操作练习一遍。

我不理解：如果有些学习内容还不理解，请复习“计算机网络”基础课程的相关章节。

在本单元所描述的网络情境中，我们通过使用网卡、交换机和直连双绞线等常见的网络设备完成了一个简单的计算机星型局域网的组建，并利用此局域网完成了信息共享网络服务。从这里可以看出，网络就是通过设备和介质将分布在不同地点的计算机终端连接起来，设备是这一工作的关键和灵魂，在本书剩下的部分中，将根据工作情境的不同，分析规划应该使用的网络设备，设计它们的连接方法，实施配置并完成网络的互连。

牢记概念：网络就是用设备和介质将计算机终端连接起来形成的系统。

情境 1　组建中小型局域网

在无纸化办公、电子商务、电子政务等诸多领域中，局域网起着非常重要的作用。现在，越来越多的中小企业开始组建局域网以提高办公效率，众多高校和事业单位也建设了自己的计算机网络，以方便学生学习，以及信息获取和信息共享交流。

怎样建成适合部门应用需求的网络？怎样保证它能承担必需的日常工作？怎样组建的网络性价比更高？这些正是这一情境下所要考虑的主要问题。

情 境 描 述

学校为了迎接新生，需要在室外空旷的地方建立一个共公接待处，学院的 8 个系都要设立自己的接待点。为了工作方便，接待点能够上网是基本要求，现在需要计算机网络技术专业的师生帮助建立一个临时网络，可以实现各系接待点之间相互通信，以及与特殊部门的通信，同时，可以访问处于外网的服务器，并能远程解答新生的相关问题。

1.1　知 识 储 备

1.1.1　网络标准化

ISO 的 OSI/RM 是网络标准化的规范性文档，又被称作“网络世界的法律”。成立于 1947 年的国际标准化组织(ISO)是个多国团体，专门为一些国际标准达成世界范围的一致。OSI/RM 是由 ISO 创建的一个有助于开发和理解计算机的通信模型，我们通常称为 OSI 七层参考模型，它最初是在 20 世纪 70 年代后期提出的。

要点讲评：什么是“层”

对于计算机网络的学习者而言，“层”是一个看不见、摸不着，特别不容易理解的概念。其实，只要通俗地把层理解为功能模块就可以，一个层和一个功能模块一样，可以完成一个或一类功能。作为使用者，只需要关心两件事：交给它的输入必须是什么类型的数据，以及这种数据应该是什么格式；从它里面输出的是什么类型的数据，以及输出的数据是什么格式。这样，在设计一个具体的“层”时，工作就会变得简单。

建立 OSI 模型的目的，是为了使单个或多个不同的系统能够较容易地通信，而不考虑其底层体系结构，更不需要改变底层的硬件或软件的逻辑。OSI 模型并不是协议，它是为

了解和设计灵活的、稳健的、可互操作的网络体系结构而提炼的一种模型。

1. 层次化体系结构

OSI 七层参考模型把网络体系自下而上地分为 7 个层次：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。每一层均有自己相应的功能集，帮助上层完成功能，依赖于紧邻自身的下层完成网络信息的传递。在最上层，应用层与计算机用户的软件程序进行交互。

OSI 七层参考模型对网络中两节点之间交互的过程进行了结构化的定义和描述。

在这个模型中，设计者根据发送数据过程中的各种最基本的要素，找出与用途相关的网络功能需求，将其分成不同的组，由这些组构成相应的层次。每一层定义了一簇功能，并严格保证这些功能和其他层的功能不同，从而确保各层功能的局部化。正如现在大家所看到的通信网络，既有丰富的功能，又有很灵活的体系结构。最重要的是，OSI 模型使得本来不兼容的系统变成完全可互操作。

在单台网络设备中，每一个层调用紧挨着它的下一层的服务。例如，第 3 层使用第 2 层提供的服务，同时向第 4 层提供服务。网络设备之间则是在一个网络设备中的第 X 层与另一个网络设备的第 X 层通信。这种通信是由一些协议来控制的，而协议就是事先都同意的一组规则和约定。在每一个网络设备的某个给定层上进行通信的进程，称为对等进程。因此，在网络设备之间的通信，就是使用某个给定层的协议的对等进程之间的通信。

知识库：层是理念上的“模块”

完全把层理解为模块或功能部件是错误的，生活中，我们定义的模块一般都依附于独立的物理实体。以大家熟悉的计算机为例，如“内存”是存储功能部件，在制作时它就是一个物理实体；再如“显卡”是一个用于显示的功能部件，它也是被制作在一个实体上的。“层”则不然，如果你想说网卡是哪一层，就会发现它不仅仅属于一层，而是包含了物理层、数据链路层、网络层的功能，甚至包含了传输层的部分功能。层之所以难理解，就是因为这一点，但只要不试图与物理实体相互对应，也就没有问题了。任意一个网络终端都必须涵盖七个层。

2. 对等进程

物理层的通信是非常直接的：一台设备将二进制位流发送给另一台设备。就像早些年的电报机一样，一台电报机发出“嘀 嘀 嘀嘀”，另一台电报机相应地也会收到“嘀 嘀 嘀嘀”。这两台电报机都不明白(也不必明白)“嘀 嘀 嘀嘀”是什么含义，因为了解这含义是报务员的事。我们说一台电报机和另一台电报机通信，这就是对等进程；我们也可以说报务员和报务员通信，这也叫对等进程，但我们不说报务员和对方的电报机通信，这不合常理，或者说不对等。在高层，通信过程是：必须先通过设备 A 的各层向下移动，到了设备 B 后，再经过各层向上移动。在发送设备的每一层，要在它从紧挨着的上层收到报文时，添加上本层的信息，然后将整个包装好的报文送出，送出报文实际上是传递给紧挨着的下

层，由下层完成剩余的工作。

在第 1 层，整个报文包要转换成可向接收设备传送的形式。在接收机设备上，报文要逐层被打开，每一个进程接收数据，然后取出对该层有意义的数据。例如，第 2 层把对第 2 层有意义的数据单元取走后，把其余的部分传递给第 3 层。第 3 层把对它有意义的数据单元取走后，再把其余部分传递给第 4 层，依次类推。

图 1-1 是对层的一种实例化描述，但问题是，这里的每一个层还是一个实体，容易误会。如果考虑两个人的协同工作，把脑的想法和手的动作都看成层，就更像网络体系结构中的层。这样做的根本目的，是为了让协作双方有统一的规定，这样，即便是两个不同国度的人，甚至是不同物种的生物，也都可以协同工作了(如警犬训练)。

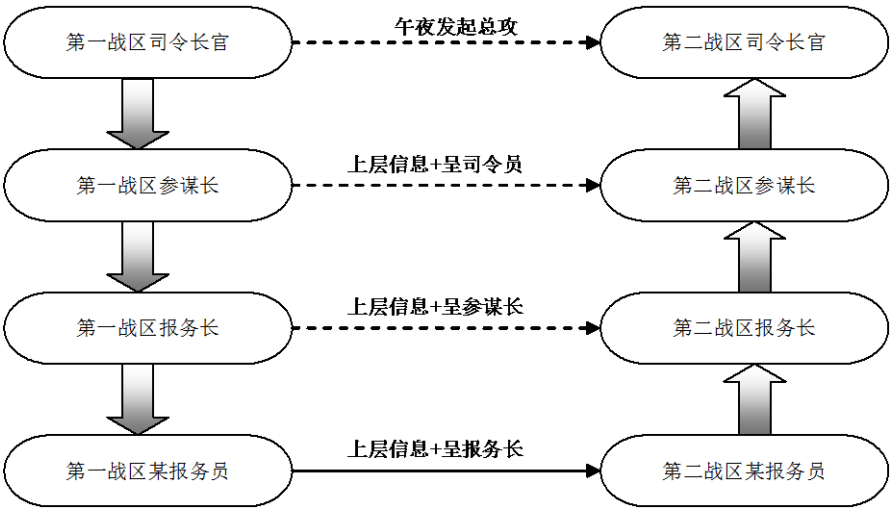

图 1-1　战区联合行动中层的概念

1)　层间的接口

在发送设备中，数据和网络信息通过各层向下传送，而在接收设备中，这些数据和信息通过各层向上传送。这样做之所以是可能的，是因为在各层的每两个相邻层之间有一个接口，每一个接口定义了一个层必须向它的上层提供什么信息和服务，定义清楚的接口和层功能使得网络可以模块化。只要一个层向它的相邻层提供了预期的、规定类型的数据，则这个层是由什么组成或采用什么结构就都是可以允许的，换句话说，升级或替换一个层的软、硬件时，不需要对其他的相关层进行改动。正如生活中我们可以将邮箱看成接口，你将信件投入邮箱，另一侧邮递员是骑自行车来取还是开轿车来取，对于你来说都是无须关注的。

2)　各层的组织

OSI 的 7 个层可看成是属于 3 个组。第 1、2 和 3 层(物理层、数据链路层和网络层)是网络支持层，被称为网络通信的低层；这些层的任务是在物理上将数据从一个设备传送到另一个设备(例如，电气规约、物理连接、物理编址、传输的定时和可靠性)。第 5、6 和 7 层(会话层、表示层和应用层)可以看成是用户支持层，也被称为网络通信的高层；这些层

使得一些无关的软件系统有了互操作性。第 4 层，即传输层，是将上面两个组连接起来，使得低层所发送的是高层可使用的形式。OSI 的上三层总是用软件来实现的；而下三层则是硬件和软件的组合，但物理层除外，它的绝大部分是硬件。

生产者和使用者都遵循以上这些规则，就称为网络标准化。网卡坏了时，只要换一块网卡即可，而不用关心是什么品牌的网卡。

深度点评：网络标准化

在网络发展初期，许多研究机构、计算机厂商和公司都按自己的想法大力发展计算机网络。这种各自为政的发展策略，使得网络在体系结构上差异很大，以至于它们之间互不相容，难于相互连接以构成更大的网络系统。为此，许多标准化机构积极开展了网络体系结构标准化方面的工作，其中最为著名的就是国际标准化组织 ISO 提出的开放系统互连参考模型 OSI/RM。OSI 参考模型最终成为研究如何把开放式系统连接起来的标准，各个厂家都按这个标准进行生产，网络互连和网络部件替换就变得简单易行了。

1990 年以前，在数据通信和联网的文献中占主导地位的是开放系统互联(OSI)模型。那时，人们大都坚信 OSI 模型将是数据通信的最终标准，然而这种情况并未发生。现在 TCP/IP 协议栈成为占主导地位的商用体系结构，因为它已在 Internet 中应用，并且通过了广泛的测试，而 OSI 模型从来没有被真正完全实现过。

3. OSI 模型中的层次

由于 OSI 模型层的概念比较虚幻，下面将通过对每一层次及其作用进行介绍，帮助理解掌握网络体系结构和各层中网络数据流的格式及简单时序。通过理顺网络数据流向及时序关系的方法来理解 OSI 模型是十分高效、科学的学习方法。

1)　应用层

应用层位于 OSI 模型的最顶端，通常被称为第 7 层。应用层的作用主要是为应用软件提供接口，从而使得应用程序能够使用网络服务，这里的应用软件也被称为应用代理。

在应用层中包含了各种各样的协议，运行在应用层上的大部分协议提供的服务是直接面对客户，例如，最常用的协议 HTTP，是我们享受 WWW 服务的基础。此外，常用的协议还包括 FTP、Telnet、DNS、DHCP、SMTP、POP3 等。

2)　表示层

表示层位于应用层的下方，通常称其为第 6 层。表示层考虑的是两个系统所交换的信息的语法和语义，或者说是信息的格式(表示方法)。

表示层的作用主要包括以下几个方面。

(1)　数据的编码和解码。两个系统中的进程所交换信息的形式通常都是字符串、数字、图、表等。这些信息在传送之前必须转变为位流。由于不同的计算机使用的编码系统可能不同，所以表示层的责任，就是在这些不同的编码方法之间提供转换。发送端的表示层将

信息从发送端有关的格式转换为一种公共的格式，接收的机器上的表示层将此公共格式转换为接收端能够理解的格式。按照通俗的理解，文件的格式(DOC、XLS、GIF 等)就属于表示层。

(2) 数据的加密与解密。为安全起见，发送前要对数据进行加密处理，数据到达目的端后，网络另一端节点的表示层将对收到的数据进行解密，变成用户能识别的信息。

(3) 数据的压缩与解压。数据压缩就是对信息中所包含的位数进行压缩。在传输多媒体信息(如文本、声音和视频)时，数据压缩就特别重要。

一言以蔽之，表示层是各节点应用程序、文件传输的翻译官。任务是将应用层产生的交互信息表示成各地计算机终端都熟悉并认可的格式。

3) 会话层

会话层位于表示层的下方，即第 5 层。会话层的作用主要是在不同用户中、节点之间建立和维护通信通道，同步两个节点之间的会话，决定通信是否被中断以及中断时决定从何处重新发送。

例如从互联网中下载文件，就与我们想要下载的文件所在地(提供下载的网站)建立了联系，也就是说，建立了一个会话，这个下载的通道是由会话层来控制的，下载的时候网络如果由于某种原因断掉了，等网络恢复正常后，仍然可以通过会话层这个控制来执行断点续传，所以业内人士形象地把会话层比喻为网络中的“交通警察”。

4) 传输层

传输层处于七层模型中的第 4 层，作为承上启下的一层，是 OSI 模型中相当重要的一层。传输层负责将报文准确、可靠、顺序地从源端传输到目的端(端到端)，而且这两个节点既可以在同一网段上，也可以在不同的网段上。当通信双方处在很遥远的地理位置时，一般不会在同一网段上。

网络层监督单个分组的端到端传输，但并不考虑这些分组之间的关系。网络层独立地处理每个分组，就好像每个分组属于独立的报文那样，而不管是否真的如此。但传输层要确保整个报文原封不动地按序到达，完成从源端到目的端的差错控制和流量控制。

传输层主要负责以下功能。

(1) 服务点编址(端口号)：计算机往往在同一时间运行多个程序。因此，从源端到目的端的传输并不仅是从某个计算机传输到下一个计算机，同时，还指出从某个计算机上的特定进程(运行着的程序)传输到另一个计算机上的特定进程(运行着的程序)。因此，传输层的首部必须包含某一特定地址，叫作端口地址。网络层将每一个分组送到正确的计算机；传输层将完整的报文送到该计算机上正确的进程。

(2) 分段与重组：一个报文要划分成若干个可传输的报文段，每个报文段应包括序号。这些序号使传输层能够将报文在它到达目的端时重组，对在传输时丢失的分组能够识别并替换为正确的分组。传输层能够智能地根据网络的处理能力把一些大的数据包强制分割成小的数据单元，然后为每个数据单元(也称数据段)安排一个序列号，保证数据单元到达接收方的时候能够正确排序。

(3)　连接控制：传输层可以是无连接的，也可以是面向连接的。无连接的传输层将每个报文段看成是独立的数据报，并将此报文段传输给目的机器的传输层。面向连接的传输层在发送分组之前，先要与目的机器的传输层建立一条连接(可以理解为全程应答关系)。当全部数据都传送完毕后，再通过一定的机制断开连接。

(4)　流量控制：如果接收端接收数据的速率小于发送端发送数据的速率，那么就可能因过载而无法工作。传输层的流量控制是在端到端的意义上实现的，其意义在于保证发送端的发送速率是接收端可接受的。

(5)　差错控制：为了加强端到端传输的可靠性，在传输层还增加了层间差错控制。发送端的传输层必须保证整个报文到达传输层时是没有差错的(即无损伤、无丢失、无重复)。如果发现差错，通常通过重传来实现纠错。在网络中，如果接收方正确收到了信息，那么接收方的传输层会发送一个 ACK(应答)来通知发送方；如果数据出现了错误，接收方的传输层也会发消息给发送方，要求重新发送出错数据；如果发送方传输数据在一定时间内没有被应答，发送方的传输层也会认为数据丢失，从而重新发送数据。注意，传输层的差错控制也是在端到端意义上的。也就是说，只是收发两端相互协商，与中间节点不进行协商。

5)　网络层

网络层位于 OSI 模型的第 3 层，网络层主要负责将分组从源端传输到目的端，这可能要跨越多个网络(网段)。传输层负责将完整的报文进行端到端的传输，而网络层则确保每一个分组能够从它的源端到达目的端。

如果两个系统连接在不同的网络(网段)上，而这些网络(网段)是由一些连接设备连接起来的，那么通常需要网络层来完成从源端到目的端的传输。

网络层主要负责以下任务。

(1)　逻辑地址：如果分组穿过了网络的边界，就需要一种编址来帮助我们区分开源系统和目的系统。网络层对从上层来的分组添加首部，其中包括发送端逻辑地址和目的逻辑地址。逻辑地址就是通常所说的 IP 地址。

(2)　路由选择：当许多独立的网络或链路互联在一起组成互联网或组成更大的网络时，这些链接的设备(路由器和交换机)就要使用可选择路由或使用交换的方法，把分组送交到它们最后的目的端。网络层的功能之一，就是提供这种路由选择机制。

网络层通过综合地考虑网络拥塞程度，数据发送的优先权，服务质量(包括传输时间、链路抖动、网络延迟等情况)，以及所有可选择的到达目标的路径开销等情况，来决定网络两节点通信的最佳路径。

在网络中，确定数据传输路径的工作(即路由功能)在网络层中完成，而路由器这种网络设备通过对网络编址方案以及网络可达性的判断，指引数据的发送，所以网络设备路由器属于三层设备。

6)　数据链路层

数据链路层位于 OSI 模型的第 2 层，数据链路层的主要作用是把从网络层接收到的数据分割成可以被物理层传输的帧，数据链路层直接控制着网络层与物理层的通信。

帧是一种用来移动数据的结构包，帧的构成类似于火车的结构，一些车厢负责运送旅客和行李(相当于数据)，车头、车尾保证了列车的完整性(帧结构的完整)，还有一些车厢完成其他的工作(对帧信息的校检、标识目的地址和源地址等)。链路层的功能如下。

(1) 组帧：数据链路层把从网络层收到的位流划分成可以处理的数据单元，即帧。

(2) 物理编址：如果这些帧需要发送给网络上的不同系统，那么数据链路层就要把首部加到帧上，以明确帧的发送端或接收端。如果这个帧是要发送给在发送端的网络以外的一个系统，则接收端物理地址就应当是将本网络连接到下一个网络的连接设备的物理地址。

(3) 流量控制：如果接收端接收数据的速率小于发送端产生的速率，那么数据链路层就应使用流量控制机制来预防接收端因过载而无法工作。

(4) 差错控制：数据链路层增加了一些措施来检测和重传损坏或丢失的帧，因而将物理层增加了可靠性。它还采用前导机制来防止出现重复帧。差错控制通常是在帧的最后加上尾部来实现的。

(5) 接入控制：当两个或更多的设备连接到同一个链路时，数据链路层就必须决定哪一个设备在什么时刻对链路有控制权。

在当今广泛使用的以太网中，数据链路层自身又划分了两个子层；逻辑链路控制层(LLC)和介质访问控制层(MAC)。

LLC 层主要负责对各种网络协议进行封装，使得协议能在物理线路上传输。LLC 帧在传输不同网络协议的时候是需要 SAP 来区分的，例如某个节点同时运行着 TCP/IP 和 IPX/SPX 两种协议，数据帧到达时，接收者需要知道将数据帧交给哪个协议来处理。此外，LLC 层为上层提供了一个可靠的公共接口，来进行流量控制。

MAC 层管理网络设备的物理地址，物理地址也被称为 MAC 地址。MAC 地址由 48 位构成，前 24 位是分配给厂商的代码，后 24 位是唯一的设备代码，MAC 地址是在设备出厂的时候烧录到设备固件中的，这就使得 MAC 地址不能修改，从而标识了设备的唯一性。

7) 物理层

物理层位于 OSI 模型的最底层，即第 1 层。物理层协调在物理媒体中传送 bit 流所需的各种功能。物理层涉及到接口和传输媒体的机械的和电气的规约。它还定义了这些物理设备和接口为所发生的传输必须完成的过程和功能。

物理层的主要作用，是产生并检测发送和接收的带有数据的电气信号。物理层包括物理上连接网络的媒介，如连接网络的线缆。物理层是不提供数据纠错服务的，但是，在物理层上能对数据的传输速度做一定的控制，并能监测数据的出错率。在物理层传输电气信号的载体，称为位流或比特流。

物理层主要有以下工作。

(1) 定义接口和介质的物理特性：物理层定义在设备与传输介质之间的接口的特性。它还定义传输介质的类型。

(2) 确定位的表示：物理层的数据由位流组成(0 和 1 的序列)，而不需要进行任何解释。要发送时，位必须经过编码变成信号——电信号或光信号。物理层定义编码的类型，即 0

和 1 用什么样的信号来表示。

(3)　数据速率：传输速率(即每秒发送的位数)也在物理层定义。换言之，物理层定义位的持续时间。

(4)　位的同步：发送端不仅要使用同样的位速率，而且还要在位级进行同步，换言之，发送端和接收端的时钟必须是同步的(该收的时候收，该停的时候停，发送方发送的每一位都要被正确地解析为一位)。

(5)　线路配置：物理层要考虑到设备与媒体的连接。在点对点的配置中，两个设备通过专用链路连接在一起。在多点配置中，若干个设备共享一条链路。

(6)　物理拓扑：物理拓扑定义设备是如何连接到网络上的。设备的连接方法可使用网状拓扑、星状拓扑、环状拓扑或总线拓扑。

(7)　传输模式：物理层还定义在两个设备之间的传输方式，单工、半双工或全双工。在单工模式下，一个设备只具备接收或者发送数据的功能。在半双工模式下，设备可以在同一时间内朝某方向单向传输数据。全双工则可同时双向收发数据。

4. 各层间的联系

OSI 七层模型虽然划分了层，但所有的层是为了一个目标协同工作的，一个设备、一次操作可能不会用到所有的层，只要用到就必须相互关联，确保网络通信过程中数据传输的每一时段，每一步的状态都准确无误。

数据的封装及拆封。

1)　数据传输的封装及拆封机制

网络通信过程中，数据的传输可以按着 OSI 七层模型层次顺序来解释，数据在发送过程中通过各层的时候，均被附加一些该层的信息，这些附加的信息被转发方和接收方的对等层作为处理数据的依据，每一层在数据上附加该层的信息时，其实就是组织一个本层的头结构，把上层传来的数据包裹起来，这个过程可以理解为各层对数据的封装。当接收方接收数据的时候，只须在各层上打开相应的封装，获得本层需要的数据，这个封装过程的逆操作我们理解为拆封。封装及拆封的过程主要在传输层、网络层、数据链路层、物理层来实现。

请您思考：把生活中寄信、货物托运等工作的流程与网络传输的工作原理做比对，找出它们的共性。

2)　数据传输的封装及拆封过程

我们用发送电子邮件和接收电子邮件的例子，来仔细讨论数据传输的封装及拆封过程。当写好电子邮件后，提出一个发送到远程邮件服务器的请求，应用层会识别你的请求，并将请求传输到表示层，表示层要判断是否要格式化，是否加密来自应用层的请求。

接下来，表示层间加入需要转换的代码信息，并将请求传递到会话层。会话层接收到表示层处理过的请求后，会给该请求附上一个数据标记符，这个标记符指示你有权限传输数据。

会话层把数据传送到传输层。在传输层，数据(包含上层加在数据上的控制信息)将被分割成可以被管理的数据段，并在每个数据段的头部添加 TCP 报头(包含源端和目的端的端口号，以实现端到端的连接和通信)。传输层的数据到达网络层后，网络层添加逻辑地址信息，在 TCP 报头前面添加 IP 报头(包含数据包的源逻辑地址和目的逻辑地址)。

这时候，我们称数据为数据包，数据包到达数据链路层后，先进入 LLC 子层，加上 LLC 头部，然后进入 MAC 子层，加上 MAC 头部和一个 FCS(帧校验序列)的尾部，数据包在数据链路层被打包成单个的帧。由于在编帧时 LLC 和 MAC 是不加区分的，建议学习者在学习这一段内容时也不要过于细究。

数据帧被传输到物理层后，物理层不做任何解释，也不再添加信息，把数据帧发送到传输介质并以位流的形式传输。在数据到达另一端服务器的物理层时，服务器的数据链路层开始解析你的请求，并反向执行上述过程。

1.1.2 TCP/IP 协议栈

1. OSI 与 TCP/IP 体系结构

为了促进计算机网络的发展，国际标准化组织 ISO 于 1977 年成立了一个委员会，在现有网络的基础上，提出了不基于具体机型、操作系统或公司的网络体系结构，称为开放系统互联模型(OSI 参考模型)。

OSI 的七层协议体系结构概念清楚，理论完整，已经被公认为计算机网络的国际标准。OSI 模型本身不是网络体系结构的全部内容，它并未确切地描述用于各层的协议和服务，仅提出每一层应该做什么。由于其设计太过复杂和繁琐，一直没有研究产生完全符合这一协议的网络系统。

现在网络上流行的协议体系是 TCP/IP，它也被称为计算机网络技术的“事实标准”或“工业标准”。TCP/IP 是随着美国国防部 ARPANET 网络的研发而诞生和独立出来的。由于低成本和可以在多个平台间通信的可靠性，TCP/IP 迅速流行并发展起来。

TCP/IP 协议栈得名于两个最重要的协议：传输控制协议(TCP)和网际协议(IP)。它还有一个鲜为人知的名字，叫作网际协议栈，这是官方的 Internet 标准文档中使用的术语。

TCP/IP 在 OSI 模型出现前就开始开发了，二者之间是各自独立进行的。因此 TCP/IP 协议栈的层次无法准确地与 OSI 模型对应起来。TCP/IP 是一个四层的体系结构，它包括应用层、传输层、互联网络层和网络接口层。

但从实质上讲，TCP/IP 只有三层，即应用层、传输层和互联网络层，因为最下面的网络接口层并没有什么具体内容。

因此，在有些参考资料中，往往采取折中的方法，也就是综合 OSI 和 TCP/IP 的优点，采用一种原理性体系结构，将其概括为五层：应用层、传输层、网络层、数据链路层和物理层。它的下四层与 OSI 的下四层相对应，提供物理标准、网络接口、网际互联以及传输功能。然而 OSI 的上三层在 TCP/IP 中则用应用层来表示。

2. TCP/IP 协议栈——应用层

TCP/IP 协议中的应用层对应于 OSI 模型中的会话层、表示层和应用层。应用层由使用 TCP/IP 进行通信的程序所提供。一个应用就是一个用户进程，通常需要与其他主机上的另一个进程合作。在这一层中定义了很多协议。例如 FTP(文件传输协议)、TFTP(普通文件传输协议)、HTTP(超文本传输协议)、SMTP(简单邮件传输协议)等。所有的应用软件通过该层利用网络。

3. TCP/IP 协议栈——传输层

TCP/IP 协议中的传输层对应于 OSI 模型中的传输层。传输层提供了端到端的数据传输，把数据从一个应用传输到它的远程对等实体。传输层可以同时支持多个应用。这一层包括两个协议：TCP(传输控制协议)和 UDP(用户数据报文协议)，负责数据报文传输过程中端到端的连接，并负责提供流控制、错误校验和报文到达后的排序重组工作。

TCP 提供了面向连接的可靠的数据传送、重复数据抑制、拥塞控制以及流量控制。UDP 提供了一种无连接的、不可靠的、尽力传送的服务。因此，如果用户需要使用 UDP 作为传输协议的应用，必须提供各自的端到端的完整性、流量控制和拥塞控制。通常，对于那些需要快速传输机制并能容忍某些数据丢失的应用，可以使用 UDP，如实时播放的流媒体。

4. TCP/IP 协议栈——网络层

TCP/IP 协议中的互联网络层对应于 OSI 模型中的网络层。互联网络层也称为互联网层或网络层。这一层包括 IP(网际协议)、ICMP(网际控制报文协议)、IGMP(网际组报文协议)以及 ARP(地址解析协议)。IP 是这一层最核心的协议。它是一种无连接的协议，不负责下面的传输可靠性。IP 不提供可靠性、流控或者错误恢复。这些功能必须由更高层提供。IP 提供了路由功能，它试图把发送的消息传输到它们的目的地。IP 网络中的消息单位为 IP 数据报。这是 TCP/IP 网络上传输的基本信息单位。

5. 常用的 TCP/IP 协议

1)　网际协议(IP)

网际协议(IP)位于 OSI 模型的网络层，即 TCP/IP 模型的 Internet 层。IP 是一种不可靠的无连接数据报协议，不保证数据的可靠性。IP 不提供任何校验，所有的传输正确性等问题在 TCP/IP 协议栈的更高层协议加以保证。

IP 是一种不可靠的协议，提供尽力而为的服务。IP 假定了底层是不可靠的，因此尽力而为将数据报传输到目的端，但没有保证；IP 也是一种无连接协议，它是为使用数据报的分组交换网而设计的。这就表示每一个分组独立地进行处理，而每一个分组使用不同的路由传送到终点。这表明如果一个源端向同一个目的端发送多个数据报，那些数据报有可能不按顺序到达。有一些数据报也可能丢失，还有些数据报在传输过程中可能会受到损伤。这时，TCP/IP 要依靠更高层的协议来解决这些问题。网络可靠性要求很高时，IP 必须与可靠的协议(如 TCP)配合起来使用。

2) 地址解析协议(ARP)和反向地址解析协议(RARP)

互联网是由许多物理网络和一些如路由器和网关的联网设备所组成的。从源主机发出的分组在到达目的主机之前，可能经过许多不同的物理网络。

在网络层，主机和路由器通过逻辑地址来标识自己的身份。逻辑地址的作用范围是全局的，并且在一个物理网络中也是唯一的。之所以叫作逻辑地址，是因为逻辑地址是用软件实现的。每一个与互联网打交道的协议都需要逻辑地址，在 TCP/IP 协议栈中，逻辑地址也叫作 IP 地址。

但是，分组都要通过物理网络才能到达这些主机和路由器。在实际物理链路传输时，主机和路由器用它们的物理地址来标志。物理地址是本地地址。它的管辖范围是本地网络。之所以叫作物理地址，是因为物理地址通常(并非永远)是用硬件实现的。物理地址的示例是以太网和令牌环中的 48 位 MAC 地址，它被写入装在主机或路由器的网络接口卡中。最终标志一台计算机的地址是其物理地址，这就表示把报文转发到主机或路由器需要两级地址：逻辑地址和物理地址。这里的两个协议分别将逻辑地址映射为物理地址和将物理地址映射为逻辑地址。

ARP 操作：在任何时候，当主机或路由器有数据报发送给另一个主机或路由器时，它必须有接收端的逻辑地址。但是，IP 数据报必须封装成帧才能通过物理网络。这就表示，发送端必须有接收端的物理地址。因此，需要从逻辑地址到物理地址的映射。此时，它发送 ARP 查询报文，这个报文包括发送端的物理地址和 IP 地址，以及接收端的 IP 地址。因为发送端不知道接收端的物理地址，查询就在网络中广播。

3) Internet 控制信息协议

IP 提供了不可靠的和无连接的数据报发送机制。IP 协议没有差错报告或差错纠正机制。如果出了差错怎么办呢？有可能路由器因找不到可以到达最后目的端的路由，或者因生存时间字段为零而必须丢弃数据报，这时，当然不能只是简单地丢弃。

IP 协议还缺少一种用于主机和管理的查询机制。主机有时需要确定一个路由器或另一个主机是活跃的。有时，网络管理员需要从另一个主机或路由器得到信息。

ICMP 就是为了解决以上两个问题而设计的。它需要配合 IP 协议使用。ICMP 本身是网络层协议。但是，它的报文不是如设想的那样直接传送给数据链路层。实际上，ICMP 报文首先要封装成 IP 数据报，然后再传送给下一层。

IP 数据报究竟携带的是什么内容，由其数据协议字段来表示，IP 报文数据协议中的字段如果是 1，表明其 IP 数据是 ICMP 报文。

ICMP 报文类型：ICMP 报文分为两大类，差错报告报文和查询报文。

差错报告报文是路由器或主机(目的端)用于处理 IP 数据报时可能遇到的一些问题。

查询报文是成对出现的，它帮助主机或网络管理员从一个路由器或另一个主机得到特定的信息。例如，节点能够发现它们的邻居。此外，主机能够发现和知道它们网络上的一些路由器的情况。

4)　传输层协议

TCP/IP 协议栈在传输层采用了两个协议：UDP 和 TCP。IP 负责主机到主机的通信。作为网络层协议，IP 只能将报文传送到目的主机。但是，这是一种不完整的传输。这个报文还必须交给正确的进程。

这正是像 UDP 或 TCP 这样的传输层协议所要做的事情。UDP 就是负责将报文转发给适当进程的。

一个远程计算机在同一时间可支持多个服务，正像许多本地计算机可在同一时间运行一个或多个客户程序一样。对通信来说，我们必须定义本地主机、本地进程、远程主机、远程进程。

本地主机和远程主机是使用 IP 来定义的。要定义进程，我们需要另一个标示符，叫作端口号。在 TCP/IP 协议栈中，端口号是 0~65535 之间的整数。

客户程序使用端口号定义它们自己，这个端口号由运行在客户主机上的 UDP 软件随机选取。这种端口号叫作短暂端口号。

服务器端的应用程序进程也必须用一个端口号来定义自己。但这个端口号不能随机选取。如果在这个服务器上运行服务器程序，并指派一个随机数作为其端口号，那么在客户端想接入这个服务器并使用其服务器的进程时，将不知道这个端口号，无疑，访问需要更多的开销。TCP/IP 决定让服务器使用全局端口号：这样的端口号叫作熟知端口号。

IANA 将端口号划分为 3 个范围——熟知的、注册的和动态的(或私有的)。

熟知端口 0~1023：由 IANA 指派和控制，这些叫作熟知端口。

注册端口 1024~49151：IANA 不指派也不控制。它们只能在 IANA 注册以防止重复。

动态端口 49152~65535：既不指派也不注册。它可以由任何进程来使用，是临时的端口。

5)　TCP/IP 协议中使用的地址

使用 TCP/IP 协议栈的互联网有 3 个等级的地址：物理(链路)地址、互联网(IP)地址以及端口地址，每一种地址都对应着 TCP/IP 体系结构中的特定层。

(1)　物理地址：物理地址也叫作链路地址或 MAC 地址，是节点的地址，它由所在的局域网或广域网定义。物理地址包含在数据链路层使用的帧中。物理地址是最低级的地址。

物理地址用于直接管理网络(局域网或广域网)。这种地址的长度和格式是可变的，取决于网络。例如，以太网使用可卸载网络接口卡(NIC)上的 6 字节(48 位)的物理地址。

(2)　Internet 地址(IP 地址)：Internet 地址对于通用的通信服务是必需的，这种通信服务与底层的物理网络无关。在互联网的环境中，仅使用物理地址是不合适的，因为不同的网络可以使用不同的地址格式。因此，需要一种通用的编制系统，来唯一标示每一个主机，而不管底层是使用什么样的物理网络。

Internet 地址就是为此目的而设计的。目前，Internet 的地址分为 IPv4 和 IPv6 两种，IPv4 是 32 位地址，可以用来表示连接在 Internet 上的每一个主机。在 Internet 上没有 2 个主机具有同样的公网 IP 地址。

(3) 端口地址：对于从源主机将许多数据传送到目的主机来说，IP 地址和物理地址是必须使用的。但是，到达目的主机并不是 Internet 上进行数据通信的最终目的。一个系统若只能从一台计算机向另一台计算机发送某种规定类型的数据，则会失去意义。今天的计算机是多进程的设备，可以在同一时间运行多个进程。Internet 通信的最终目的，是使一个进程能够与另一个进程通信。例如，计算机 A 能够与计算机 B 使用 Telnet 进行通信。与此同时，计算机 A 还与计算机 C 采用 FTP 通信。为了能够同时发生这些事情，我们需要一种方法为不同的进程打上标记。换言之，这些进程需要有地址。在 TCP/IP 体系结构中，给一个进程指派的标号叫作端口地址。TCP/IP 中的端口地址为 16 位长。

1.1.3 IP 地址的使用

MAC 地址是网络设备及网卡在出厂时就烧录确定的，在工作中一般也是不可改变的，但 IP 地址却是终端上网之前才设定的，因此必须有一个设定规则。本小节就讨论怎样给终端设定 IP 地址才能保证通信网络正常运行。

网络通信的概念很像人类社会生活的社区化，每一个城市都坐落于某一地理位置(这相当于一个网络)，不同的城市之间由公路、铁路、航空等交通设施相连(这相当于网络之间的链路)，每一个城市又分成若干个小区(这相当于网络技术中的子网)。为了通信的需要，现在到了给它们取没有歧义名字的时候了。

就以现实世界中的小例子来说明这一问题。某一地名叫“双沟”，这是合理的，但你不能简单地说“把货物送到双沟”，因为仅以江苏省苏北地区为限，就存在淮安市洪泽县的双沟，宿迁市泗阳县的双沟和徐州市铜山县的双沟。这样的重名和命令中的歧义性，使得递送货物的操作无法实现。

网络通信中也是一样，由于这里的信息送达依据是 IP 地址，因此保证 IP 地址与网络及终端的一一对应关系显得格外重要。

在计算机网络的学习过程中，我们知道了 IP 地址(V4 版)被分成了 A、B、C、D、E 五大类，这相当于把地址分成大小不等的许多个区域，以满足不同规模的城市对地址的需求。注意这只是一个类比，或者说，作为工程技术人员的你可以采用这一规则进行地址分配，Internet 的整个地址分配由于起初互连的随机性和地域发展不平衡性，总体 IP 地址的分配并不是严格规范的。

建设一个网络总是需要一定数量的 IP 地址，现在我们可以把获取的一个 IP 地址段看成是给一个城市命名用的，为了让 IP 地址使用更加规范高效，一般情况下会对其做进一步的子网划分，这就是所谓的可变长子网掩码(VLSM)。

在上面关于现实生活递送货物的例子中，如果我们说清楚了是送往“江苏省洪泽县的双沟”，问题就解决了。在计算机网络中传递信息时，也要清楚地表述目的地址属于哪一个网络，只有这样，网络中的设备才能将数据准确送达。

先看一个 IP 地址 210.29.226.85，这是作者个人办公用计算机的网络地址，它属于哪一

个网段呢(类似于现实生活中位于哪个城市)?

如果是按经典的 IPv4 划分，它属于 210.29.226.0 这个网络。

可能有人仍不明白，没关系，这只是一个命名规定，用多了就明白了。就像我们看很多外国地名不明白一样，用多了也就习惯了，这其实就是一个习惯问题。

计算机和网络设备为了标识具体 IP 地址的网络归属，采用了另外一个数字串，叫掩码，此例中采用的就是经典的 C 类 IP 地址的掩码 255.255.255.0，在计算机及相关设备里，这一串数字被描述成一个二进制串 11111111111111111111111100000000。

当然，在计算机及设备中，IP 地址也会被描述成二进制串，210.29.226.85 转换成二进制就成了 11010010000111011110001001010101，十进制 IP 地址中的点(.)对于计算机和设备是没有意义的，只是为了人类阅读更方便。将两个二进制串相与，得到一个数字串，就是 IP 地址对应的网络号，也称为网络标识：

```
11010010000111011110001001010101
11111111111111111111111100000000
--------------------------------
11010010000111011110001000000000
```

210　　29　　226　　0

知识要点：网络标识符

不论何时，用相应子网掩码与出的地址都是网络标识符，也叫网络号。

同样的例子，当子网掩码变成 255.255.255.192 时，IP 地址 210.29.226.85 所处的网段就发生变化了。此掩码的二进制串是 11111111111111111111111111000000，跟地址对应的二进制串相与，结果如下：

```
11010010000111011110001001010101
11111111111111111111111111000000
--------------------------------
11010010000111011110001001000000
```

210　　29　　226　　64

可见，同样的 IP 地址 210.29.226.85，当掩码为 255.255.255.0 时它属于 210.29.226.0 网络；而当掩码为 255.255.255.192 时，它属于 210.29.226.64 网络，掩码的作用就在于此，我们可以通过使用合适的掩码，将网络合理地进行规划和进一步划分。

1.1.4　局域网中的网关

在引言的图 6 界面中，我们给一台计算机终端配置了 IP 地址，但其后还有一个“默认网关”是空着的，这是一个相当重要的概念，在网络工程中一定要理解清楚。网关可以认

为是一个局域网的出口，或者说未知通信对象的默认送达地。在同一个局域网中，所有的通信对象都属于同一网络(或网段)，它们相互之间是通过广播了解通信路径的(请复习 ARP 协议)，但要是送到外网，广播就无能为力了，必须通过三层设备进行路由，但前提是数据能够准确送到三层设备，所以设定了一个“网关”，确保出网络数据能够到达三层设备，以便进一步传送。

1.2 情境训练：招生临时网络的构建

1.2.1 网络规划

这个案例非常简单，没有太多的规划工作，给出一个适合的拓扑结构，如图 1-2 所示。

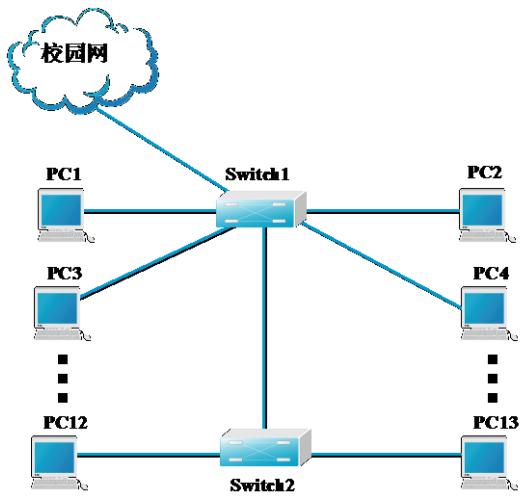

图 1-2 招生接待处的临时网络拓扑

1.2.2 项目实施

从校园网最近的设备上拉一根双绞线到本地的交换机 Switch1，由于现在交换机的接口数都比较多，13 台计算机终端一般够用(各系占 8 台，外加 5 台)，但如果考虑位置关系不好处理，比如位置太远造成线缆太长，或是位置重叠造成线缆太乱，则可以用多台交换机。

拓扑连接完成以后，将每台终端的 IP 地址设置正确，比如说，第一台 IP 地址设为 210.29.226.254、第二台设为 210.29.226.253，以此类推。

子网掩码均设为 255.255.255.0，网关设为本网段的网关，比如 210.29.226.1。

正确设置 DNS 后，网络就可以正常工作了。

1.3　知 识 拓 展

1.3.1　交换机的工作原理

在一个局部的地理范围内(如一个学校、工厂和机关内)，将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网，简称局域网(LAN)。要扩展局域网的规模，就需要用通信线缆连接更远的计算机设备，但当信号在线缆中传输时会受到干扰，产生衰减。如果衰减到一定的程度，信号将不能识别，计算机之间将不能通信。必须使信号保持原样，继续传播才有意义。

当我们安装一个局域网而物理距离又超过了线路的规定长度时，就可以用中继器进行延伸；中继器可以在收到一个网络的信号后，将其放大发送到另一网络，从而起到连接两个局域网的作用。

1. 集线器

由于中继器的连接端口少，因此一种多端口的集线器设备应运而生。集线器也称为Hub，是一种集中完成多台设备连接的专用设备，提供了检错能力和网络管理等有关功能。

局域网早期使用的连接设备是集线器，集线器是中继器的一种形式，区别在于，集线器能够提供多端口的服务，也称为多口中继器。集线器工作在 OSI/RM 中的物理层。

集线器产品发展较快，局域网集线器通常分为五种不同的类型，它对 LAN 交换机技术产生了很多直接的影响，但随着交换技术的发展，集线器产品也基本消失在历史的进程中。

1)　单中继网段集线器

在硬件平台中，第一类集线器是一种简单的中继 LAN 网段，最好的例子是叠加式以太网集线器或令牌环网多站访问部件(MAU)。某些厂商试图在可管理集线器和不可管理集线器之间划一条界线，以便进行硬件分类，但这种考虑后来证明是不切实际的，因为他们忽略了网络硬件本身的核心特性，即它实现什么功能，而不是如何简易地配置它。

2)　多网段的集线器

多网段的集线器是第一类集线器直接派生而来的，采用集线器背板，这种集线器带有多个中继网段，多网段集线器通常是有多个接口卡槽位的机箱系统。然而，一些非模块化叠加式集线器现在也支持多个中继网段。多网段集线器的主要技术优点是可以将用户分布于多个中继网段上，以减少每个网段的信息流量负载，网段之间的信息流量一般要求有独立的网桥或路由器。

3)　端口交换式集线器

端口交换式集线器是在多网段集线器基础上将用户端口的多个背板网段之间的连接过程自动化，并通过增加端口交换矩阵(PSM)来实现的。PSM 提供一种自动工具，用于将任何外来用户端口连接到集线器背板上的任何中继网段上。这一技术的关键是“矩阵”，一

个矩阵交换机是一种电缆交换机，它不能自动操作，要求用户介入。它不能代替网桥或路由器，并不提供不同 VLAN 网段之间的连接性，其主要优点是实现移动、增加和修改的自动化。

4) 网络互连集线器

端口交换集线器为主动端口交换，而网络互联集线器在背板的多个网段之间实际上提供了一些类型的集成连接。这可以通过一台综合网桥、路由器或 LAN 交换机来完成。

5) 交换式集线器

到了集线器发展的后期，集线器和交换机之间的界限已变得模糊。交换式集线器有一个核心交换式背板，采用一个纯粹的减缓系统代替传统的共享介质中继网段。应该指出，集线器和交换机之间的特性几乎没有区别。

2. 交换机

1993 年，局域网交换设备出现；1994 年，国内掀起了交换网络的热潮。其实，交换机是一种具有监护功能的低价格、高性能和高端口密集度特点的交换产品，体现了桥接技术的复杂交换技术在 OSI 参考模型的第二层操作。

与网桥一样，交换机按每一个包中的 MAC 地址，相对简单地决策信息转发，而这种转发决策一般不考虑包中隐藏更深的其他信息。与网桥不同的是，交换机转发延迟很小，远远超过了普通桥接互联网络之间的转发性能。

1) 交换技术的特点

交换技术允许共享型和专用型的局域网段进行宽带调整，以减轻局域网之间信息流通出现的瓶颈问题。以太网、快速以太网、FDDI 和 ATM 技术都有相应的交换产品，但随着以太网技术的成熟，已经形成了大一统的局面。

类似传统网桥，交换机提供了许多网络互联功能。同时，还提供了交互及将网络分成多个小的冲突域，为每个工作站提供更高的带宽。协议的透明性使得交换机在软件配置简单的情况下可直接安装于多协议网络中；交换机使用现有的电缆、中继器、集线器和工作站网卡，不必做高层硬件升级；交换机对工作站来说好像不存在一样，这样管理开销低廉，简化了网络节点增加、移动和网络变化的操作。

利用专门设计的集成电路，可使交换机以线路速率在所有的端口并行转发信息，提供了比传统网桥高得多的操作性能。如理论上，单个以太网对含有 64 个八进制数的数据包，可提供 14880b/s 的传输速率。这意味着一台具有 12 个端口、支持 6 道并行数据流的“线路速率”以太网交换机必须提供 89280b/s 的总吞吐率(6 道信息流×14880bits/s/道信息流)。

专用集成电路技术使得交换机可在更多端口的情况下以上述性能运行，其端口造价低于传统型网桥。

局域网交换机根据使用的网络技术，可以分为以太网交换机、令牌环交换机、FDDI 交换机、ATM 交换机、快速以太网交换机。

2) 二层交换技术

二层交换技术发展比较成熟，二层交换机属于数据链路层设备，可以识别数据包中的

MAC 地址信息，并将这些 MAC 地址与对应端口记录在自己内部的一个地址表中(就是俗称的 MAC 地址表)，根据 MAC 地址表进行转发。具体工作流程如下。

(1)　当交换机从某个端口收到一个数据包时，它先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在交换机的哪个端口上，从而产生 MAC 地址和端口一一对应的 MAC 地址表。

(2)　再去读取包头中的目的 MAC 地址，并根据 MAC 地址表查找相应的转发端口。

(3)　如表中有与该目的 MAC 地址相对应的表项，把数据包直接复制到相应的端口上。

(4)　如果从表中找不到对应的表项，则把数据包广播到所有端口上。当目的终端对源终端回应时，交换机可以学习到此目的 MAC 地址与哪个端口对应，下次再有向这一目的端口发送的数据时，就不再需要对所有端口进行广播了。

不断循环这个过程，对于全网的 MAC 地址信息都可以学习到，二层交换机就是这样建立和维护它自己的地址表的。

从二层交换机的工作原理，可以总结出以下三点。

第一，由于交换机对多数端口的数据进行同时交换，这就要求具有很宽的交换总线带宽，如果二层交换机有 N 个端口，每个端口的带宽是 M，交换机总线带宽超过 N×M，那么，该交换机就可以实现线速交换。

第二，学习端口连接终端的 MAC 地址信息，写入地址表。地址表的大小(一般有两种表示，即 Beffer RAM 和 MAC 表项数值)会影响交换机的接入容量。

第三，一般来说，二层交换机都配有专门用于处理数据包转发的 ASIC(Application Specific Integrated Circuit)芯片，因此，转发速度可以做到非常快。由于各个厂家使用的 ASIC 不同，产品的性能会受到直接的影响。

3)　交换机与集线器的区别

集线器存在的主要问题是其所有用户共享带宽，每个用户的可用带宽随着接入用户数的增加而减少。这是因为当通信比较繁忙时，多个用户可能同时争用信道，而信道在某一时刻只允许一个用户占用，故大量的用户经常处于侦听等待状态，这样会严重影响数据传输效率。

交换机则为每个用户提供专用的信息通道，除了多个源端口企图同时将信息发送到同一个目的端口的情况外，各个源端口与其他目的端口之间可同时进行通信而不会发生冲突，从而可提高数据传输效率。因此，我们也说交换机的每一个端口就是一个冲突域。

1.3.2　交换机的基本配置

对于一般的交换机，我们买回来后直接就可以使用了，但如果你想要划分内网、关闭某个端口什么的，这时就需要对其进行一些配置工作了。要配置就得登录，常见的登录方式有三种：通过 Console 端口直接连接登录、通过 Telnet 方式登录、通过 Web 浏览方式登录。下面主要涉及前两种方式。

这里我们要掌握交换机的基本配置方法及命令行各种操作模式的区别，并能够在各种模式之间进行切换。

交换机的管理方式基本分为两种：带内管理和带外管理。

通过交换机的 Console 口管理交换机属于带外管理，不占用交换机的网络接口，其特点是需要使用配置线缆，近距离配置。需要注意的是，第一次配置交换机时，必须利用 Console 端口进行配置，而在实际工程中这种方式也较多。

另一种方式叫带内管理，这是采用将控制信息从数据端口传入的方式完成的，网络维护工作中则较多使用这种方法。

通常，在交换机买回来第一次进行配置时，都采用通过 Console 端口直接连接登录的方式。首先找到交换机自带的 Console 端口与计算机串口的连接线，然后将两端分别连接到交换机的 Console 控制端口与计算机的串口上。

小提示：有些交换机并不带有这根连接线，那么我们需要自己制作一根这样的连接线，制作时，主要是注意跳线的规则，而这一般在交换机的说明书中都有详细的说明。

通过如下操作来调用 Telnet 工具。

(1) 打开交换机电源，启动好计算机，依次单击“开始”→“程序”→“附件”→“通信”→“超级终端”，打开“超级终端”程序。

小提示：如果没有看到“超级终端”程序，则可以通过“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”把该程序安装上。

(2) 系统自动弹出建立新连接的对话框，在名称栏输入一个连接名称(如“3COM”)，单击“确定”按钮。

(3) 在“连接时使用”下拉列表框中选择与交换机相连的计算机的串口，单击“确定”按钮，弹出如图 1-3 所示的对话框。

图 1-3 “COM1 属性”对话框

(4) 在“每秒位数”(即波特率)下拉列表框中选择 9600，因为这是串口的最高通信速

率，其他各选项都采用默认值，单击“确定”按钮，如果通信正常的话，就会出现类似于如图 1-4 所示的界面了，然后就可以大显身手，对交换机进行一番配置了。

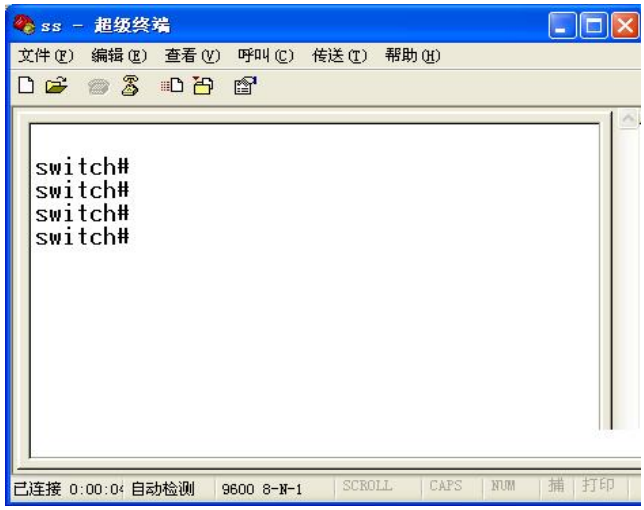

图 1-4　仿真终端连接正常

在交换机的命令行界面下又分为多种操作模式，主要包括用户模式、特权模式、全局配置模式、端口模式等几种。

- 用户模式：这是进入交换机后得到的第一个操作模式，该模式下可以简单查看交换机的软、硬件版本信息，并进行简单的测试。

  用户模式提示符一般为 switch>。
- 特权模式：这是由用户模式进入的下一级模式，该模式下可以对交换机的配置文件进行管理，查看交换机的配置信息，进行网络的测试和调试等。

  特权模式提示符一般为 Switch#。
- 全局配置模式：这属于特权模式的下一级模式，该模式下可以配置交换机的全局参数(如主机名、登录信息等)。在该模式下，可以进入下一级的配置模式，对交换机的具体功能进行配置。

  全局模式提示符一般为 Switch(config)#。
- 端口模式：这属于全局模式的下一级模式，该模式下可以对交换机的端口进行参数配置。

  端口模式提示符一般为 Switch(config-if)#。

任一特定的操作只能在某一特定的模式下完成，在命令行状态下，这些模式是可以相互转换的，进入和退出都有相应的命令，其中退出的常用命令如下：Exit 命令，是退回到上一级操作模式；End(或^Z)命令是指用户从特权模式以下级别直接返回到特权模式。

另外，交换机命令行还支持获取帮助信息、命令的简写、命令的自动补齐、快捷键功能等。

1.4 操 作 练 习

操作与练习 1-1 交换机命令行操作模式的进入

```
Switch> enable                                    ! 进入特权模式
Switch#
Switch# configure terminal                        ! 进入全局配置模式
Switch(config)#
Switch(config)# interface fastEthernet 0/5        !进入交换机 F0/5 的接口模式
Switch(config-if)#
Switch(config-if)# exit                           ! 退回到上一级操作模式
Switch(config)#
Switch(config)# end              ! 直接退回到特权模式
Switch#
```

请您注意：这样的练习是以后学习的基础，要反复操作，越熟悉越好。

操作与练习 1-2 交换机命令行的基本功能

① 显示帮助信息：

```
Switch>?    !显示当前模式下所有可执行的命令
  disable           Turn off privileged commands
  enable            Turn on privileged commands
  exit              Exit from the EXEC
  help              Description of the interactive help system
  ping              Send echo messages
  rcommand          Run command on remote switch
  show              Show running system information
  telnet            Open a telnet connection
  traceroute        Trace route to destination

Switch# co?    !显示当前模式下所有 co 开头的命令
configure      copy
Switch# copy ?
  flash:                Copy from flash: file system
  running-config        Copy from current system configuration
  startup-config        Copy from startup configuration
  tftp:                 Copy from tftp: file system
  xmodem                Copy from xmodem file system
```

② 命令的简写：

```
Switch# conf ter   !交换机命令行支持命令的简写，该命令代表 configure terminal
Switch(config)#
```

③　命令的自动补齐：

```
Switch# con  (按键盘的 Tab 键自动补齐 configure)  !交换机支持命令的自动补齐
Switch# configure
```

④　命令的快捷键功能：

```
Switch(config-if)# ^Z   !Ctrl+Z 退回到特权模式
Switch# ping 1.1.1.1
Sending 5, 100-byte ICMP Echos to 1.1.1.1,
timeout is 2000 milliseconds.
...
Switch#
```

例如，上面在交换机特权模式下执行 ping 1.1.1.1 命令，发现不能 ping 通目标地址，交换机默认情况下需要发送 5 个数据包，如不想等到 5 个数据包均不能 ping 通目标地址的反馈出现，可在数据包未发送 5 个之前，通过按 Ctrl+C 组合键终止当前操作。

【注意事项】

①　命令行操作进行自动补齐命令简写时，要求所简写的字母必须能够唯一区分该命令。如 Switch# conf 可以代表 configure，但 Switch# co 无法代表 configure，因为 co 开头的命令有两个，即 copy 和 configure，设备无法区分。

②　注意区分每个操作模式下可执行的命令种类，交换机不可以跨模式执行命令。

操作与练习 1-3　交换机设备名称和每日提示信息的配置

①　配置交换机基本信息：

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname 105_switch   !配置交换机的设备名称为 105_switch
105_switch(config)#

105_switch(config)# banner motd &   !配置每日提示信息，&为终止符
2006-07-24 02:37:54  @5-CONFIG:Configured from outband
Enter TEXT message.  End with the character '&'.
Welcome to 105_switch, if you are admin, you can config it.
If you are not admin, please EXIT!       !输入描述信息
&                              !以&符号结束并终止
```

②　验证测试：

```
105_switch(config)# exit
105_switch# exit
Press RETURN to get started!
Welcome to 105_switch, if you are admin, you can config it.
If you are not admin, please EXIT!
```

```
105_switch>
```

【注意事项】

① 配置设备名称的有效字符是 22 个字节。

② 配置每日提示信息时，注意终止符不能在描述文本中出现。如果键入结束的终止符后仍然输入字符，则这些字符将被系统丢弃。

操作与练习 1-4 交换机端口参数的配置

① 配置端口参数：

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fastEthernet 0/3    !进入 F0/3 的端口模式
Switch(config-if)# speed 10     !配置端口速率为 10Mb/s
Switch(config-if)# duplex half    !配置端口的模式为半双工
Switch(config-if)# no shutdown  !开启该端口，使端口转发数据
```

配置端口速率的参数有 100(100Mb/s)、10(10Mb/s、auto(自适应)，默认是 auto。配置模式有 full(全双工)、half(半双工)、auto(自适应)，默认是 auto。

② 查看交换机端口的配置信息：

```
Switch# show interfaces fastEthernet 0/3
Interface   : FastEthernet100BaseTX 0/3
Description :
AdminStatus : up   !查看端口的状态
OperStatus  : down
Hardware    : 10/100BaseTX
Mtu         : 1500
LastChange  : 0d:1h:0m:28s
AdminDuplex : Half     !查看配置的模式(半双工)
OperDuplex  : Unknown
AdminSpeed  : 10    !查看配置的速率
OperSpeed   : Unknown
FlowControlAdminStatus : Off
FlowControlOperStatus  : Off
Priority    : 0
Broadcast blocked        :DISABLE
Unknown multicast blocked :DISABLE
Unknown unicast blocked   :DISABLE
```

【注意事项】

交换机端口在默认情况下是开启的，AdminStatus 是 Up 状态，如果该端口没有实际连接其他设备，OperStatus 是 down 状态。

操作与练习 1-5　查看交换机的端口参数和配置状态

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname 105_switch
105_switch(config)# interface fastEthernet 0/3
105_switch(config-if)# speed 10
105_switch(config-if)# duplex half
105_switch(config-if)# no shutdown

105_switch# show version  !查看交换机的版本信息
System description     : Red-Giant Gigabit Intelligent Switch(S2126G) By
                      Ruijie Network     !系统描述信息
System uptime          : 0d:1h:7m:57s
System hardware version : 3.3      !设备硬件版本信息
System software version : 1.61(2) Build Aug 31 2005 Release
System BOOT version     : RG-S2126G-BOOT  03-02-02
System CTRL version     : RG-S2126G-CTRL  03-08-02   !操作系统版本信息
Running Switching Image : Layer2

105_switch# show mac-address-table      !查看交换机的 MAC 地址表

Vlan         MAC Address          Type      Interface
----------  -------------------- --------  --------------------

105_switch# show running-config    !查看交换机当前生效的配置信息

System software version : 1.61(2) Build Aug 31 2005 Release

Building configuration...
Current configuration : 252 bytes

!
version 1.0
!
hostname 105_switch     !配置的主机名
vlan 1
!
interface fastEthernet 0/3   !针对 F0/3 端口配置的参数
 speed  10
 duplex half
!
banner motd ^C
Welcome to 105_switch, if you are admin, you can config it.
If you are not admin, please EXIT!
```

```
^C
!
end
```

【说明】

查看交换机的系统和配置信息命令要在特权模式下执行。

Show mac-address-table：查看交换机当前的 MAC 地址表信息。

Show running-config：查看交换机当前生效的配置信息。

注：该操作使用两台主机，其中一台用于配置交换机，另一台主机的网卡与交换机的 F0/3 接口相连。注意查看主机连接在交换机的哪个端口，针对该端口进行参数的设置。该试验建立在交换机端口基本配置的基础上。

【注意事项】

Show mac-address-table、show running-config 都是在查看当前生效的配置信息，该信息存储在 RAM(随机存储器里)，当交换机掉电，重新启动时，会重新生成 MAC 地指表和配置信息。

1.5 项 目 总 结

根据前面的情境描述，学院有 8 个系，都要有自己的接待点，再加上财务处、招生处、学工处、团委和院领导，如果每个部门分配一个 IP 地址，则该局域网节点数需要不少于 13 个，找到 2^X-2 大于 13 的最小整数(X=4)，这时能够直接应用的 IP 地址为 $2^4-2=14$(个)。取一个暂时没有应用的网段，比如 210.29.226.240 ~ 210.29.226.254 这段地址暂时没用，我们可以用“/28”的掩码(也就 32 位二进制串的前面 28 位是 1，刚才计算机设备位需要 4 位)，转换成点分十进制数，就是 255.255.255.240。

当一台计算机终端需要向另一台计算机终端发送数据时，就可以通过中心设备转发，这种方式在网络维护方面比较容易，去除掉问题终端时不会影响其他终端通信，在网络扩展上也有其他方式不可比拟的优越性，随时在交换机上插上一台新终端，就可以参与网络通信。这种模式被称为“网络标准化”，不论是从理念上，还是从工程上，都使网络连接变得简单而且高效。

现在大部分局域网都是用双绞线作为传输介质，一般我们还会在局域网组建项目中采用三层构架，即接入层、汇聚层和核心层。这样的架构可以大大降低局域网组建和维护工作的复杂度，究其原因，也是分层带来的好处。

接入层就是连接局域网内各终端机的系统，汇聚层是连接接入层的系统，而核心层则是整个局域网的汇总和出口处。

如果你只是想简单地实现双机互联，就用交叉双绞线直接连接两台计算机，并把它们

的 IP 地址设在同一网段内，把来宾账户打开，简单地共享文件夹或者打印机就行了。

要是你有 10 台以下的计算机，买个小点的交换机，用双绞线连接各终端和交换机，把 IP 地址设在同一网段，也就完成了一个对等网络的搭建。

本项目的实施过程中还有一个操作，就是要将交换机连接到一个和外网相通的路由器上，并将该路由器与交换机连接端口的 IP 地址指定为各台计算机终端的网关，也就是出局域网的各类信息都被默认地传输到这一端口，由路由器处理。

1.6　理 论 练 习

选择填空，选择一个最好的答案。

(1) 考虑线序的问题，主机和主机直连应该用(　　)线序的双绞线连接。

A. 直连线　　B. 交叉线　　C. 全反线　　D. 各种线均可

(2) OSI 是由(　　)机构提出的。

A. IETF　　B. IEEE　　C. ISO　　D. INTERNET

(3) 屏蔽双绞线(STP)的最大传输距离是(　　)。

A. 100 米　　B. 185 米　　C. 500 米　　D. 2000 米

(4) 在 OSI 的七层模型中，集线器工作在哪一层？

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 传输层

(5) 下列哪些属于工作在物理层的网络设备？

A. 集线器　　B. 中继器　　C. 交换机　　D. 路由器

E. 网桥　　F. 服务器

(6) 网络按通信范围分为(　　)。

A. 局域网、城域网、广域网　　B. 局域网、以太网、广域网

C. 电缆网、城域网、广域网　　D. 中继网、局域网、广域网

(7) Internet 中使用的协议主要是(　　)。

A. PPP　　B. IPX/SPX 兼容协议

C. NetBEUI　　D. TCP/IP

(8) IEEE 802.3 标准规定的以太网的物理地址长度为(　　)。

A. 8bit　　B. 32bit　　C. 48bit　　D. 64bit

(9) 关于集线器的叙述中，错误的是(　　)。

A. 集线器是组建总线型和星型局域网不可缺少的基本设备

B. 集线器是一种集中管理网络的共享设备

C. 集线器能够将网络设备连接在一起

D. 集线器具有扩大网络范围的作用

(10) 制作双绞线的 T568B 标准的线序是(　　)。

A. 橙白、橙、绿白、绿、蓝白、蓝、棕白、棕

B. 橙白、橙、绿白、蓝、蓝白、绿、棕白、棕

C. 绿白、绿、橙白、蓝、蓝白、橙、棕白、棕

D. 以上线序都不正确

(11) 理论上讲，100Base-TX 星形网络最大的距离为(　　)米。

A. 100　　B. 200　　C. 205　　D. +∞

(12) 在组建网吧时，通常采用(　　)网络拓扑结构。

A. 总线型　　B. 星型　　C. 树型　　D. 环形

(13) 使用特制的跨接线进行双机互联时，以下(　　)说法是正确的。

A　两端都使用 T568A

B. 两头都使用 T568B

C. 一端使用 T568A 标准，另一端使用 T568B

D. 以上说法都不对

(14) OSI 模型的(　　)负责产生和检测电压，以便收发携载数据的信号。

A. 传输层　　B. 会话层　　C. 表示层　　D. 物理层

(15) 某公司申请到一个 C 类网络，由于有地理位置上的考虑，必须切割成 5 个子网，则子网掩码要设为(　　)。

A. 255.255.255.224　　B. 255.255.255.192

C. 255.255.255.254　　D. 255.285.255.240