

思考练习参考答案

1.5 思考与练习

1. 填空题

- (1) 现场勘查、阅读招标文件、技术交流会、答疑会
- (2) 核心层、汇聚层和接入层。
- (3) RIP、IGRP、EIGRP、OSPF、IS-IS、BGP
- (4) 威胁评估、分布式控制、编写网络安全策略

2. 选择题

- (1) ABCDEF
- (2) A
- (3) ABCDEFG

3. 问答题

(1) 在实施网络安全防范措施时要考虑的问题。

答：在实施网络安全防范措施时要考虑以下几点：

- 要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；
- 要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补；
- 从路由器到用户各级建立完善的访问控制措施，安装防火墙，加强授权管理和认证；
- 利用数据存储技术加强数据备份和恢复措施；
- 对敏感的设备 and 数据要建立必要的物理或逻辑隔离措施；
- 对在公共网络上传输的敏感信息要进行数据加密；安装防病毒软件，加强内部网的整体防病毒措施；建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

(2) 什么是网络的逻辑三层结构。

答：所谓的逻辑三层结构为接入层、汇聚层、核心层，其含义分别如下：

- 接入层为用户提供了网络设备的接入，它通常包括实现局域网的设备（例如工作站和服务器）互联的第二层交换机。在广域网环境中，同广域网的接入点就为接入层的节点。
- 汇聚层有可称为分布层，它汇聚了配线架，并且使用第二层和第三层交换进行工作组分段、实施安全策略、限制带宽和隔离各种网络故障等等。这些措施能够直接防

止汇聚层和接入层造成对核心层的影响。

- 核心层主要是用来快速交换的，因为核心层是连通的关键环节，所以必须采用高速传输交换技术才能满足网络的快速有效的传输。

2.5 思考与练习

1. 选择题

- (1) d
- (2) b
- (3) c
- (4) a
- (5) a

2. 填空题

- (1) LLC。
- (2)
- (3) 应用层、传输层、网络层和数据链路层。
- (4): 网络 ID 号，主机部分。

3. 问答题

(1) 任何两台计算机都可以使用相同的网络接口卡连接到网络上。对还是错？为什么？

答：错。因为网络接口卡标识了此接口的第二层 MAC 地址，它是唯一的，如果两台机器使用相同的 MAC 地址的话，那么在同一个网络就会出现 MAC 地址不唯一的情况，从而就无法进行数据传输。

(2) IP 地址和 MAC 地址都可以标识网络中的一台计算机，两者之间有什么区别和联系？

答：IP 地址是指 Internet 协议使用的地址，而 MAC 地址是 Ethernet 协议使用的地址，IP 地址与 MAC 地址之间并没有什么必然的联系。

MAC 地址是 Ethernet NIC（网卡）上带的地址，为 48 位长。每个 Ethernet NIC 厂家必须向 IEEE 组织申请一组 MAC 地址，在生产 NIC 时编程于 NIC 卡上的串行 EEPROM 中。因此每个 Ethernet NIC 生产厂家必须申请一组 MAC 地址。任何两个 NIC 的 MAC 地址，不管是哪一个厂家生产的都不应相同。Ethernet 芯片厂家不必负责 MAC 地址的申请，MAC 地址存在于每一个 Ethernet 包中，是 Ethernet 包头的组成部分，Ethernet 交换机根据 Ethernet 包头中的 MAC 源地址和 MAC 目的地址实现包的交换和传递。

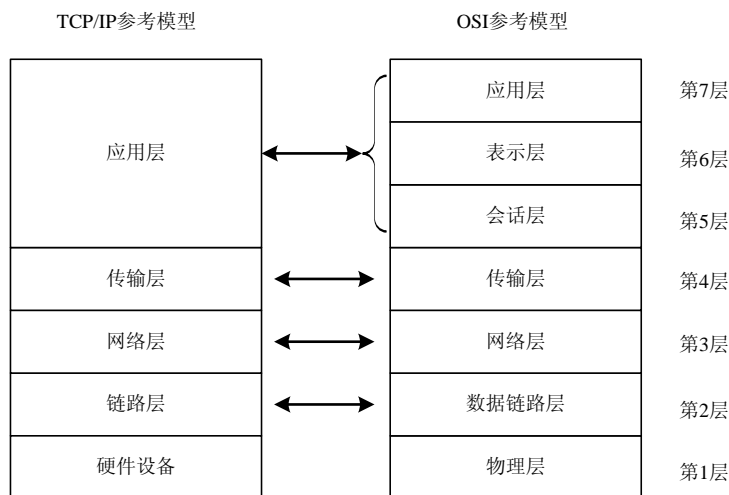
IP 地址是 Internet 协议地址，每个 Internet 包必须带有 IP 地址，IP 地址现是 32 位

长，正在扩充到 128 位。IP 地址与 MAC 地址无关，因为 Ethernet 的用户，仍然可通过 Modem 连接 Internet。IP 地址通常工作于广域网，我们所说的 Router（路由器）处理的就是 IP 地址。

MAC 地址工作于局域网，局域网之间的互连一般通过现有的公用网或专用线路，需要进行网间协议转换。可以在 Ethernet 上传送 IP 信息，此时 IP 地址只是 Ethernet 信息包数据域的一部分，Ethernet 交换机或处理器看不见 IP 地址，只是将其作为普通数据处理，网络上层软件才会处理 IP 地址。

(3) 请说明 OSI 模型和 TCP/IP 协议簇的对应关系。TCP/IP 是目前 Internet 上最常用的协议，而 OSI 模型则是国际化的标准，为什么在目前的 Internet 上没有完全实现 OSI 的体系结构？

答：1.OSI 模型与 TCP/IP 协议簇的对应关系如下图所示。



2.OSI 模型仍处在几个关节的结合阶段，并没有完全实现，其原因如下：

a. OSI 模型协议指定的时机较晚，OSI 协议出现时，TCP/IP 协议已大量应用在大学和科研机构，人们不会轻易改动协议的。

b. OSI 模型设计亦有一定缺陷。首先会话层对大多数应用没有用，表示层几乎是空的；而数据链路层和网络层功能太多，因而又把它们分成了几个子层，每个子层都有不同的功能。

c. OSI 模型以及与其相关的服务定义和协议极其复杂，实现起来困难且操作效率不高。

(4) 假如你目前是某大学计算机实验室的一名网络专业人员，一个学生对如何使一个网站出现在他计算机屏幕上感到好奇。在一张纸上，参考 OSI 模型，解释当请求一个网页时，发生在客户机与服务器之间的过程。

答：a. 首先，当输入网址时，其实就是用户直接应用层操作的实例。

b. 表示层会将此网址的信息进行解析和压缩成计算机能够识别的信息。并且将本层的信息添加到数据头上。

c. 数据被传到会话层后，在会话层会建立起一个虚拟的连接。并且将本层的信息添加到数据头上。

d. 数据被传到传输层后，在此层会建立端到端的可靠有效的网络连接。并且将本层的信息添加到数据头上。

e. 数据被传输到网络层后，在此层会把本地机器的第三层地址添加到数据中。并且将本层的信息添加到数据头上。

f. 数据被传输到数据链路层后，在此层把本地机器的 MAC 地址添加到其中。并且将数据打包成帧。

g. 当数据被传输到物理层时后，此时数据会被分解成电信号，通过传输介质传输到服务器上，而在服务器的一端首先会将电信号转换成数据帧，并且会传输到上一层数据链路层。

h. 在数据链路层，数据帧被解封装后，去掉头部相关信息，一层一层网上传输，最后，达到应用层，服务器就获得了客户端发过来的信息，然后，将结果按上面的步骤再返回给客户端。

4. 一个公司，总共有四个部门，分别是技术部、销售部、财务部和客户部。技术部总共有 100 人，销售部有 50 人，财务部有三人，客户部有 20 人。现在有一个 IP 地址段：192.168.0.0/24。请为这家公司合理的进行 IP 地址规划。

答：由于有四个部门，而技术部有 100 人，是所有部门中人数最多的部门，所以，在规划地址的时候，首先考虑技术部。根据 $2^n < 100$ 的原理，计算出 n 的值为 6，所以主机位为 7 位，其子网掩码为 255.255.255.128，根据 192.168.0.0/24 划分为 192.168.0.0/25 和 192.168.0.128/25，在此，为技术部分配 192.168.0.128/25。

接下来考虑销售部，根据 $2^n < 50$ ，计算出 n 为 5，所以主机为 6 位，其子网掩码为 255.255.255.192，根据 192.168.0.0/25 可以划分为 192.168.0.0/26 和 192.168.0.64/26，在此为销售部分配 192.168.0.64/26。

下面考虑规划客户部的 IP 地址，根据 $2^n < 20$ ，计算出 n 的值为 4，所以主机为 5 位，其子网掩码为 255.255.255.224。根据 192.168.0.0/26 可以划分为 192.168.0.0/27 和 192.168.0.32/27，在此为客户部分配 192.168.0.32/27。

最后，考虑规划财务部的 IP 地址，根据 $2^n < 3$ ，计算出 n 的值为 1，所以主机为 2 位，其子网掩码为 255.255.255.252，根据 192.168.0.0/27 可以划分出 192.168.0.0/30、192.168.0.4/30、192.168.0.12/30、192.168.0.8/30、192.168.0.16/30、192.168.0.20/30、192.168.0.24/30、192.168.0.28/30。在此，将 192.168.0.4/30 分配给财务部。其余的 IP 地址段可以作为备用地址段。

3.6 思考与练习

1. 填空题

- (1) CISC 架构服务器、VLIW 架构服务器
- (2) 光纤、光发送机和光接收机
- (3) 中继器
- (4) MAC
- (5) 存储转发模式
- (6) 下一跳、标志

2. 选择题

- (1) ACD
- (2) C
- (3) A
- (4) C

3. 问答题

- (1) 简述网桥的基本工作原理。

答：当网桥收到一个数据帧后，首先将它传送到数据链路层进行差错校验，然后再发送到物理层，通过物理层传输机制再将它传送到另一个子网上，在转发帧之前，网桥对帧的格式和内容不作或只作很少的修改。网桥一般都设有足够的缓冲区，有些网桥还具有一定的路由选择功能，通过筛选网络中一些不必要的传输来减少网上的信息流量。

局域网网段与网桥相连的接口称为网桥端口。基本网桥只有两个端口，而多口网桥具有多个连接局域网的端口。

每个网桥端口都是由与特定局域网类型相匹配的 MAC 集成电路芯片以及相关端口管理软件组成。端口管理软件在加电时负责对 MAC 集成电路芯片进行初始化，并对缓冲器进行管理。一般情况下，可供使用的存储器在逻辑上被分成若干固定尺寸和单位，称为缓冲器。缓冲管理将空闲缓冲器指针传递到集成电路芯片，以便准备好接收帧，同时将帧缓冲器指针传递给芯片，以便准备好接收帧。

所有网桥都以不加选择的方式进行操作，这意味着网桥在其每个端口都将外入的帧接收下来，并进行缓冲。当帧由 MAC 芯片在一个端口接收并将其置入分配的缓冲器时，端口管理软件便使芯片准备好接收新的帧，随后便将包括接收帧的缓冲器的指针传递给网桥协议实体进行处理。如果在网桥端口处有两个或多个帧同时到达，并需要将这些帧从同一端口转发出去，端口管理软件和网桥协议实体软件间的缓冲器指针的传递就通过一组队列实现。

当网桥收到一个帧时，便可通过查找转发数据基来确定是将帧滤除还是转发。由于网

桥操作是在数据链路层的 MAC 子层，通过对 MAC 帧中站地址的检查便可建立起这种转发数据基。根据 MAC 帧地址建立转发数据基的过程称为“自学习”过程。

(2) 交换和路由的主要区别有哪些？

答：交换和路由的主要区别：

a. 工作层次不同

最初的交换机是工作在 OSI / RM 开放体系结构的数据链路层，也就是第二层，而路由器一开始就设计工作在 OSI 模型的网络层。由于交换机工作在 OSI 的第二层（数据链路层），所以它的工作原理比较简单，而路由器工作在 OSI 的第三层（网络层），可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

b. 数据转发所依据的对象不同

交换机是利用物理地址或者说 MAC 地址来确定转发数据的目的地址。而路由器则是利用不同网络的 ID 号（即 IP 地址）来确定数据转发的地址。IP 地址是在软件中实现的，描述的是设备所在的网络，有时这些第三层的地址也称为协议地址或者网络地址。MAC 地址通常是硬件自带的，由网卡生产商来分配的，而且已经固化到了网卡中去，一般来说是不可更改的。而 IP 地址则通常由网络管理员或系统自动分配。

c. 传统的交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域

由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第三层以上交换机具有 VLAN 功能，也可以分割广播域，但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

d. 路由器提供了防火墙的服务

路由器仅仅转发特定地址的数据包，不传送不支持路由协议的数据包传送和未知目标网络数据包的传送，从而可以防止广播风暴。

交换机一般用于 LAN-WAN 的连接，交换机归于网桥，是数据链路层的设备，有些交换机也可实现第三层的交换。路由器用于 WAN-WAN 之间的连接，可以解决异性网络之间转发分组，作用于网络层。他们只是从一条线路上接受输入分组，然后向另一条线路转发。这两条线路可能分属于不同的网络，并采用不同协议。相比较而言，路由器的功能较交换机要强大，但速度相对也慢，价格昂贵，第三层交换机既有交换机线速转发报文能力，又有路由器良好的控制功能，因此得以广泛应用。

(3) 简述交换机和集线器的主要区别。

答：交换机和集线器区别如下：

a. 结构上

集线器属于 OSI 的物理层设备，对数据的传输起到同步、放大和整形的作用，对数据传输中的短帧、碎片等无法进行有效的处理，不能保证数据传输的完整性和正确性。交换机属于 OSI 的数据链路层设备，不仅可以对数据的传输做到同步、放大和整形，而且可以过滤短帧、碎片等。

b. 数据传输方式上

利用集线器连接的局域网叫共享式局域网，利用交换机连接的局域网叫交换式局域网。共享式网络当数据和用户数量超出一定的限量时，会造成碰撞冲突，使网络性能衰退。交换式网络则可避免共享式网络的不足，交换技术的作用便是根据所传递信息包的目的地地址，将每一信息包独立地从端口送至目的端口，避免了与其它端口发生碰撞，提高了网络的实际吞吐量。

c. 带宽占用方式上

集线器不管有多少个端口，所有端口都是共享一条带宽，在同一时刻只能有二个端口传送数据，其他端口只能等待，同时集线器只能工作在半双工模式下。而交换机每个端口都有一条独占的带宽，这样在速率上对于每个端口来说有了根本的保障，当二个端口工作时并不影响其他端口的工作，同时交换机不但可以工作在半双工模式下而且可以工作在全双工模式下。

d. 传输模式上

集线器只采用半双工方式进行传输，在上行通道上集线器一次只能传输一个任务，要么是接收数据，要么是发送数据。而交换机则不一样，采用全双工方式来传输数据的，因此在同一时刻可以同时进行数据的接收和发送，这不但令数据的传输速度大大加快，而且在整个系统的吞吐量方面交换机比集线器至少要快一倍以上。

(4).什么是智能输入/输出技术？

答：智能输入/输出技术吧任务分配给智能 I/O 系统，在这些子系统中，专用的 I/O 处理器将承担中断处理、缓冲存取以及数据传输等繁琐的任务，从而使得系统的吞吐能力得到的很大的提高。

这个系统中的 I/O 子系统完全独立于网络操作系统，并不需要外部设备的支持，这样就减轻了操作系统的负担，另一方面也提高了 I/O 通信效率。

4. 实践题

假如你的一位朋友是一家公司的老板，拥有员工 50 多人，并设立了 6 个部门。目前公司希望建立自己的网络系统，在公司的各部门之间形成不同的子网，同时公司又要建立共享的 Mail 和文件服务器。请你运用本章的知识，向你的朋友解释要实现这样的网络所需要的主要设备有哪些，如何选择合适的设备。请你针对这些问题给你的朋友写封邮件，谈谈你的建议。

答：

首先，由于需要上互联网，所以必须要求拥有一台第三层的网络设备，可以是第三层交换机，也可以是路由器。

其次，由于整个公司有六个部分，所以，可以设立六个子网，或者也可以按照部门分成六个虚拟局域网，那么，如果来实现虚拟局域网的话，所使用的交换机设备就必须是具备 VLAN 功能的交换机。

最后，由于整个公司有五十多个人，所以，所需的服务器必须保证硬盘容量大，内存大的特色，另外，由于需要设置文件服务器和共享 Mail 服务器，文件服务器必须要作冗

余 CPU、RAM、PCI 适配器、电源、风扇等，可以在单个部件失效时自动切换到备用设备上，保证系统运行。

4.9 思考与练习

1. 填空题

- (1) 计算机、传输媒体、网络适配器和网络连接设备
- (2) CSMA/CD。
- (3) 同步的包 异步的 同步 异步
- (4) 基于端口、基于硬件 MAC 地址和基于网络层。
- (5) 无线网卡、无线访问接入点、 无线网桥。

2. 选择题

- (1) a
- (2) b
- (3) b
- (4) a
- (5) d
- (6) c
- (7) d
- (8) a

3. 问答题

- (1) 列出典型的局域网拓扑结构，并说明他们各自的特点。

答：计算机网络的物理连接形式叫做网络的物理拓扑结构。连接在网络上的计算机、大容量的外存、高速打印机等设备均可看作是网络上的一个节点,也称为工作站。计算机网络中常用的拓扑结构有总线型、星型、环型等。

a. 总线拓扑结构 总线拓扑结构是一种共享通路的物理结构。这种结构中总线具有信息的双向传输功能，普遍用于局域网的连接,总线一般采用同轴电缆或双绞线。 总线拓扑结构的优点是：安装容易,扩充或删除一个节点很容易,不需停止网络的正常工作,节点的故障不会殃及系统。由于各个节点共用一个总线作为数据通路,信道的利用率高。但总线结构也有其缺点：由于信道共享,连接的节点不宜过多，并且总线自身的故障可以导致系统的崩溃。

b. 星型拓扑结构 星型拓扑结构是一种以中央节点为中心,把若干外围节点连接起来的辐射式互联结构。这种结构适用于局域网,特别是近年来连接的局域网大都采用这种连接

方式。这种连接方式以双绞线或同轴电缆作连接线路。星型拓扑结构的特点是：安装容易，结构简单，费用低，通常以集线器(Hub)作为中央节点，便于维护和管理。中央节点的正常运行对网络系统来说是至关重要的。

c. 环型拓扑结构 环型拓扑结构是将网络节点连接成闭合结构。信号顺着一个方向从一台设备传到另一台设备，每一台设备都配有一个收发器，信息在每台设备上的延时时间是固定的。这种结构特别适用于实时控制的局域网系统。环型拓扑结构的特点是：安装容易，费用较低，电缆故障容易查找和排除。有些网络系统为了提高通信效率和可靠性，采用了双环结构，即在原有的单环上再套一个环，使每个节点都具有两个接收通道。环型网络的弱点是，当节点发生故障时，整个网络就不能正常工作。

d. 树型拓扑结构 树型拓扑结构就像一棵“根”朝上的树，与总线拓扑结构相比，主要区别在于总线拓扑结构中没有“根”。这种拓扑结构的网络一般采用同轴电缆，用于军事单位、政府部门等上、下界限相当严格和层次分明的部门。树型拓扑结构的特点：优点是容易扩展、故障也容易分离处理，缺点是整个网络对根的依赖性很大，一旦网络的根发生故障，整个系统就不能正常工作。

(2) 简述当工作站参与 CSMA/CD 时所采取的步骤。

答：在总线上如果工作站有信包要发送，它在向总线上发送信包之前，先检测一下总线是“忙”还是“空闲”，如果检测的结果是“忙”，则发送站会随机延迟一段时间，再次去检测总线，若这时检测总线是“空闲”，这时就可以发送信包了。而且在信包的发送过程中，发送站还要检测其发到总线上的信包是否与其它站点的信包产生了冲突，当发送站一旦检测到产生冲突，它就立即放弃本次发送，并向总线上发出一串干扰串（发出干扰串的目的是让那些可能参与碰撞但尚未感知到冲突的结点，能够明显的感知，也就相当于增强冲突信号），总线上的各站点收到此干扰串后，则放弃发送，并且所有发生冲突的结点都将按一种退避算法等待一段随机的时间，然后重新竞争发送。从以上叙述可以看出，CSMA/CD 的工作原理可用四个字来表示：“边听边说”，即一边发送数据，一边检测是否产生冲突。

(3) 简述令牌环的操作过程。

答：a. 网络空闲时，只有一个令牌在环路上绕行。令牌是一个特殊的比特模式，其中包含一位“令牌/数据帧”标志位，标志位为“0”表示该令牌为可用的空令牌，标志位为“1”表示有站点正占用令牌在发送数据帧。

b. 当一个站点要发送数据时，必须等待并获得一个令牌，将令牌的标志位置为“1”，随后便可发送数据。

c. 环路中的每个站点边转发数据，边检查数据帧中的目的地址，若为本站点的地址，便读取其中所携带的数据。

d. 数据帧绕环一周返回时，发送站将其从环路上撤消。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧，否则释放缓冲区中的待确认帧。

e. 发送站点完成数据发送后，重新产生一个令牌传至下一个站点，以使其它站点获得发送数据帧的许可权。

4. 练习题

在这个练习中,你将创建一个简单的星型总线网络,它是以太网中最典型的网络形式之一。这个项目准备一个以太网 10Mbps 集线器(其中每个集线器至少包括 4 个端口),6 根电缆,4 台工作站(或者是 PC),所有的计算机都带有 10Mbps/100Mbps 网络接口卡(已安装及正确配置)。工作站可以运行 Windows 95/98, Windows 2000 或 Windows XP,并且安装了 TCP/IP 协议。

(1) 将一根电缆的一端插入集线器的连接端口,另一端插入一台工作站(或者是 PC)的网络接口卡,从而将集线器和工作站(或者是 PC)连接起来。

(2) 将工作站(或者是 PC)的电源打开,注意当工作站(或者是 PC)启动时,集线器上的灯会发生什么变化。

(3) 重复上述的过程,即可建立起一个星型拓扑结构的网络。

5.11 思考与练习

1. 填空题

- (1) OSPF、IS-IS、BGP
- (2) DDN 节点、用户环路。
- (3) 576~640Kbps, 1.544Mbps。
- (4) 用户/网络接口(UNI)和网络节点接口(NNI)。
- (5) 采点到点协议 PPP(Point to Point Protocol) HDLC

2. 选择题

- (1) A
- (2) B
- (3) C
- (4) C
- (5) C
- (6) B

3. 问答题

(1) 简述 ATM 交换机转发信元的过程。

答: ATM 交换机接收一个到达的信元,并决定如何选择该信元的路由,使信元到达一个指定的本地 ATM 交换机接口,以便该信元能够正确到达目的地。根据网络结构的

同, 信元可能会途经一个或多个 ATM 交换机, 直到信元到达其路由上的最后一个交换机, 并且在即将到达接收节点的剩余路途中, 该信元被转换到一个包中。该信元的目的地可能是另外一个交换机, 或者是多个交换机, 例如多点传送的传输, 这一信息是从信元头中得知的。在存在多条路径的网络中, 必须使用特定的 ATM 路由协议, 例如私有网络到网络接口(PNNI), 这些协议在交换机之间交换连接表, 这些连接表包含关于多种路径的信息, 这些路径使得每一个交换机能够为每一个传输选择合适的路径。

(2) 简述广域网实施过程中所要考虑的关键因素。

答: a. 传输速率

b. 可靠性

c. 安全性

d. 虚拟私用网络

4. 实践题

现在有一家公司, 在北京、天津、香港有三家分公司, 上海是总公司, 现在需要将四家公司进行连接, 使得公司内部可以相互通信, 请读者选择广域网路由方式、链路通信方式以及整个网络的规划。

答: 针对这个项目, 首先需要考虑的是如何选择广域网路由, 鉴于可以将每个公司都可以看成一个区域, 所以, 选择 OSPF 路由协议。其次, 选择链路通信方式, 由于四家公司距离很长, 所以可以考虑使用 MPLS 方式。其整个网络规划的拓扑如下图 5-18 所示。

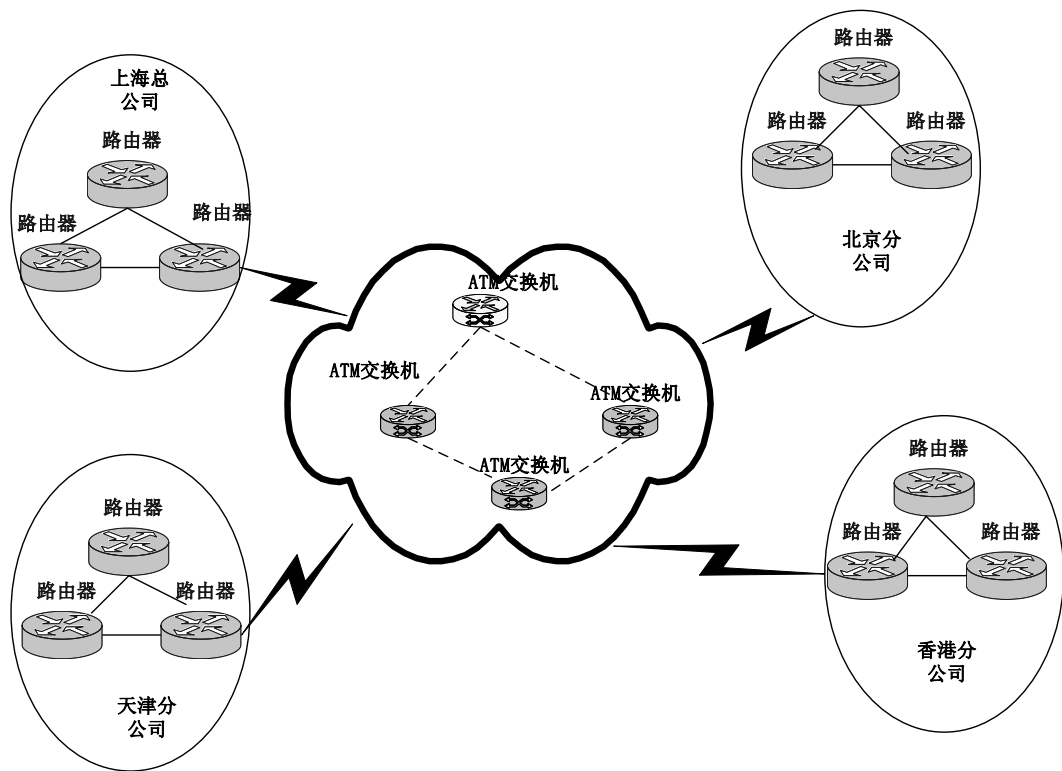


图 5-18 网络规划拓扑图

6.7 思考与练习

1. 填空题

- (1) 网络布线文档和网络系统文档。
- (2) 100
- (3) Microsoft 的 NetBEUI、Novell 的 IPX/SPX，和 TCP/IP。
- (4) 与其他自治域的 BGP 交换网络可达信息。

2. 选择题

- (1) B
- (2) A
- (3) A
- (4) D

3. 问答题

- (1) 网络规划过程中所要考虑的主要因素包括哪些？

答：网络的规划设计工作在整个网络建设中起着举足轻重的作用，一般网络规划需要考虑以下几个方面的问题：

- 采用何种或哪几种网络协议的问题。网络协议是网络规划的基础，每种协议都有自己的优势和特点，例如 Ethernet 协议比较简单，组网灵活，但是 Ethernet 在端对端的性能保证、Qos 等方面有很大的不足，所以，Ethernet 通常用于局域网中。ATM 则可以提供良好的 Qos 保证和端到端的保护，但其技术复杂，设备昂贵，所以通常用于电信级的服务网络中。由此看见，网络协议的选择要根据实际需求决定。
- 采用什么类型的网络拓扑结构。在前面章节介绍过的星型拓扑、环型拓扑和总线拓扑结构中，各有优缺点。在实际网络规划中，不可能简单的决定采用哪种结构，通常需要根据需求采用若干种拓扑结构的组合。
- 采用什么样的应用程序，包括何种类型的操作系统。网络需要提供各种服务，如 FTP、Web、Mail 等，这就需要操作系统和应用程序的支持。从操作系统角度看，可以有 Windows、Unix 等操作系统软件供选择，可以从技术复杂度、成本和稳定性等方面加以考虑。
- 如何加强网络的安全性的问题。安全性是在网络建设过程中所不能忽视的重大问题。安全性的含义很广泛，包括物理安全性、设备安全性、信息安全性等多方面。
- 选择什么样的网络速度。网络速度的提高往往是以成本的提高和技术复杂度的提高

为代价的,所以在选择网络速度时,要综合考虑系统成本和实现的复杂度等要素。

- 如何在满足网络需求的基础上减少建设费用,这也是非常重要的,用户总是希望以最低的代价获得最高的收益。

在网络规划过程中必须解决如上所述的问题,因此我们需要考虑的因素包括:首先需要明确整个网络的需求状况,也就是明确有哪些用户,并需要提供哪些服务。这是建设局域网的基础。在此基础上,再确定需要哪些资源来构建这个网络,然后确定合适的网络协议,并确定网络拓扑结构,保证网络的安全性和可靠性。

在网络设计中还要特别注意以下几个因素:

- 网络的可扩展性:因为网络在未来可能需要扩充,因此必须在网络设计时考虑网络的可扩展性。
- 冗余性:也就是网络在某些资源出现故障时,还能够找到其他的替代资源,以维持网络运行的能力。
- 容错性:指网络对不可避免的各种突发事件的处理能力。

(2) 简述在网络设计过程中,IP 地址分配的基本原则。

答:分配 IP 地址时需要遵循以下原则:

- 惟一性:一个 IP 网络中不能有两个主机采用相同的 IP 地址。
- 简单性:地址分配应简单且易于管理,降低网络扩展的复杂性,简化路由表项。
- 连续性:连续地址在层次结构网络中易于进行路径叠合,极大地缩减路由表,提高路由算法的效率。
- 可扩展性:地址分配在每一层次上都要留有余量,在网络规模扩展时能保证地址叠合所需的连续性。
- 灵活性:地址分配应该具有灵活性,以满足多种路由策略的优化,充分利用地址空间。

(3) 评价一个网络的主要性能指标有哪些,简述各指标的含义。

答: a. 延迟(Latency)

通常情况下,延迟指的是等待某动作发生所需的时间。对很多种网络通信而言,一个数据包(或一组数据包)一旦从一台主机发送到另一台主机,发送主机就必须等待直到收到一个应答包。网络延迟的确定需要测量往返时间(round-trip time, RTT),即一个数据包在客户机和服务器之间往返所需的时间间隔。

b. 丢包率(Packet Loss)

网络丢包率指的是在一特定的时间间隔中,从客户机到服务器往返过程中丢失的数据包所占所发送数据包的百分比数。数据包丢失一般是由于网络拥塞引起的。丢包率一般在 0%~15%(严重拥塞)间变化。更高的丢包率可能导致网络不可用。

少量的丢包率并不一定表示网络故障,很多业务在少量丢包的情况下也能继续进行。例如:一些实时应用或流媒体业务,如 VoIP,就可以忍受少量的丢包,并且不重发所丢失的包;另外,TCP 协议正是靠检测丢包率来发现网络拥塞的,这时它会以更低的速率重发

被丢失的包。

c. 吞吐量(Throughput)

吞吐量一般指的是链路上所有通信数据的总传输速率，有时也可以用于表示某特定业务的数据传输速率。吞吐量指的是数据在网络上的传输速率，一般以 bps(位/秒)、Bps(字节/秒)或 pps(包/秒)表示。

吞吐量通过监测某特定时间间隔内所传输的字节数来测量。需要注意选择适当的测量时间间隔。过长的时间间隔会平滑掉突发速率，过短的时间间隔又会夸大突发速率。折中的办法是选择 1~5 分钟的时间间隔。

d. 链路使用率(Link Utilization)

互联网业务通常是通过若干条物理链路接入的。简单地说，链路使用率指的是特定时间间隔内的吞吐量占链路接入速率的百分比。

e. 可用性(Availability)

可用性是指在某特定时间段内，系统正常工作的时间段占总时间段的百分比，例如，业务的可用性、主机的可用性、网络的可用性等。

对于可用性指标，可以通过发送相应的数据包并检测响应包进行测试，例如：

- Web 业务可用性测试：用 Web 浏览器(例如 Windows 系统中的 IE)从目标服务器下载指定页面，测量其响应时间、丢包率和吞吐量。
- 主机可用性测试：在 Windows 环境下，可以 ping 目标主机，确认该主机对 ICMP 包是否有响应。

网络可用性测试：对目标主机进行路由跟踪(tracert)，以确定目标主机与目标网络之间的连通性。

4.实践题

有一家外贸公司，在全国拥有三家分公司，其中在上海地区的为总公司，每家公司拥有四个部门，分别为财务部、技术部、销售部和市场部，而在总部拥有五个部门，分别为领导办公室、财务部、技术部和市场部，接下来，希望读者能够为其公司做一个合理的网络规划。

答：首先，考虑这家公司的广域网接入，由于分公司之间是相隔比较远的，从成本上考虑，所以可以采用 MPLS 或者帧中继的接入方式。

其次就是考虑所使用的路由协议，因为路由协议决定了整个网络的拓扑，由于存在总公司和分公司之间的关系，所以建议使用 OSPF 的路由协议。将每个分公司作为一个 Area，他们只要与总公司相连即可以彼此通信。这样也避免了全网链接的高费用。

在每家分公司的内部，做好 IP 地址的策划，策划方法，可以参考本章的最后实例。

最后，所需要策划的就是为了能够使得分公司之间相同的部门可以相互通信，所以在整体上可以采用 VLAN 技术。

具体的策划内容，请读者详细的进行分析。

7.6 思考与练习

1. 填空题

- (1) 通信自动化系统(CA)、办公室自动化系统(OA)
- (2) 基本型综合布线系统、增强型综合布线系统
- (3) 设备间
- (4) 梯式桥架
- (5) “随装随测” 接线图、衰减和近端串扰(NEXT)

2. 选择题

- (1) C
- (2) B
- (3) C
- (4) A

3. 问答题

- (1) 简述综合布线系统的主要特点。

答：1. 兼容性

综合布线的首要特点是它的兼容性。所谓兼容性指的是它自身是完全独立的，与应用系统相对无关，可以适用于多种应用系统。

2. 开放性

综合布线由于采用的是开放式体系结构，符合国际上多种现行的标准，因此它对所有著名厂商的产品几乎都是开放的，例如计算机设备、交换机设备等；并支持所有的通信协议，例如 ISO/IEC8802-3，ISO/IEC8802-5 等协议。

3. 灵活性

传统的布线方式是封闭的，其体系结构是固定的，如果需要迁移设备或增加设备非常困难甚至是不可能。综合布线采用标准的传输线缆和相关的连接硬件以及模块化设计。因此所有的通道都是通用的。每条通道都可以支持终端、以太网工作站和令牌环网工作站。所有设备的开通和更改均不需要改变布线，只需增减相应的应用设备和在配线架上进行必要的跳线管理即可。

4. 可靠性

综合布线由高品质的材料和组合压接的方式构成一套高标准的信息传输通道。所有的线槽和相关连接部件均需通过 ISO 认证，每条通道都要采用专用仪器测试链路阻抗及衰减率，以保证其电气性能。应用系统布线全部采用点到点端接，任何一条链路出现故障均不影响其他链路的运行，为链路的运行维护及故障检修提供了方便，确保了应用系统的可靠运行。各应用系统往往采用相同的传输媒体，因而可互

为备用,提高了备用冗余。

5. 先进性

所有布线均采用目前世界上最新的通信标准,链路均按八芯双绞线配置。5类双绞线带宽可达 100MHz,6类双绞线带宽可达 200MHz。对于用户的特殊需求,可把光纤引到桌面(Fiber To The Desk)。语音干线部分用钢缆,数据部分用光缆,为同时传输多路实时多媒体信息提供了足够的带宽容量。

6. 经济性

综合布线比传统布线经济,综合布线可适应相当长时间的需求,传统布线改造很费时间,因耽误工作而造成的损失更大。

(2) 综述综合布线工程分析和设计的过程和注意事项。

答:综合布线工程分析和设计的过程:

a. 可以选用产品全面、技术成熟、性能优越的综合布线系统。数据系统从端到端采用全 5 类连接硬件产品,以保证信息传输速率达到 155Mbps,并支持 ATM、多媒体等宽带传输技术;语音系统选用能够传输 10Mbps 速率的产品,以保证低速网络信息的传输和通信;监控系统采用 5 类产品,以保证高品质图像的传输。

b. 从功能上看,综合布线系统包括工作区子系统、水平子系统、管理子系统、垂直干线子系统、设备间子系统和建筑群子系统 6 个部分。

(1) 工作区子系统

工作区由各个办公区域构成,每个工作区根据具体的需求分设 1 孔至 4 孔信息插座,其中,选用 5 类信息插座(RJ45 接口)以支持 100Mbps 高速数据通信和图像通信,同时设置 3 类信息插座以连接电话线。

此外,每一信息插座均可通过 400K 分插座支持一部低速数据终端或两部电话(终端),使综合布线具有极强的可扩充性。

(2) 水平子系统

数据传输选用优质的 5 类 4 对非屏蔽双绞线电缆,数据传输速率可达 155Mbps,可支持目前及未来的数据系统和监控系统的需求。结合具体土建结构的特点、弱电间的位置和信息出口的位置,并考虑到端接富裕量,以确定水平子系统的电缆长度。

(3) 垂直干线子系统

干线子系统的数据干线采用 6 芯 62.5/125 μ m 室内多模光缆,传输速率可达 600Mbps,最大限度地满足了高速率传输的需求。采用 3 类 100 对大对数双绞电缆作为语音传输干线,每层由楼层配线间配出一条线缆,可支持 10 兆传输速率,既满足了目前的需求,又为多媒体技术的应用打下了坚实的基础。

(4) 管理间子系统

根据大楼的具体特点,在每层设置一个配线间,在配线间内分别设有综合布线的弱电间。每个配线间设 110 型电缆配线架、光纤配线架和必要的网络互联设备,110 型电缆配线架由两部分组成:一部分用来端接干线(大对双绞电缆);另一部分用来端接水平干线。光纤配线架则用来端接干线光纤。

各层管理配线架通过大对数电缆连接到程控交换机房，与电话交换机相连接，构成大楼内部和外部的通信，保证大楼内的信息畅通。

(5) 设备间子系统

设备间子系统是一个集中化的设备区，用于连接系统公共设备和通过垂直干线子系统连接到管理子系统。设备间安装机柜式光纤配线架，端接各层汇集的光纤并与大楼核心交换机连接，通过主机管理整个大楼的局域网，构成大楼内高速信息系统。通过简单的跳线管理，可以很方便地配置楼内的计算机网络的拓扑结构。

注意事项：

- (1) 带宽与传输速率
 - (2) 传输介质选择
 - (3) 要选用成熟的产品
 - (4) 关于质量保证的问题
- (3) 光纤布线系统测试的主要内容包括哪些？

答：对光纤或光纤系统进行测试的基本内容有：连续性和衰减/损耗，测量光纤的输入功率和输出功率，分析光纤的衰减/损耗，确定光纤的连续性和发生光损耗的部位等。

4.实践题

有一个有两层楼的网吧，现将互联网接入的设备放到二楼的总机房中，服务器也放在二楼总机房中去，现在需要读者来为这个网吧作一个网络综合布线的规划。

答：其实两层楼可以看成是两个一层楼的网吧，分别将每一层楼的布线完成，由一台交换机同楼上的主交换机相连即可完成。

(1) 设备间

在网吧的二楼必须寻找一个空间来作为主设备间，在主设备间中放置路由器和主交换机以及电源系统等等。无论是主交换机还是普通交换机，在选择安放位置时，一定要把它放到节点的中间位置，这样可以节约网线的使用量，另外还可以将网络的传输距离减少到最小，从而可以提高网络传输质量。分设备间的为止最好根据网吧的占地形状来规划，例如如果是方形，则是一个角落一个分设备间，如果是圆形，则是在内切正方形的四个角落。

(2) 强电和弱电布线

在布线时，把双绞线放在 PVC 管或者专业的线槽中，在双绞线经过的地方，尽量避免有强大磁场或者大功率的电器、电源线等等，这样会大大降低网络传输质量。但是如果真的在实际中遇到强电的情况，要学会如何处理，首先要尽量保证强电和弱电线路交叉，这样可以抵消强电对于网线的干扰，但是当平行的时候，最好让强电和弱电能够相聚 30mm 左右。

(3) 两层楼的主干连接

两层楼相连是通过一根五类线或者是一根光纤来连接，无论是通过哪种传输介质相连，都必须使用套管或者 PVC 管道来保护主干线路。

(4) 备份线路的建立

由于在网吧中设备或者线缆的使用率非常之高，所以比较容易老化或损坏。在这种情

况下，建议布线工程师要为所有的线路建立一条备份线路，这样的话，在紧急情况下，可以使用备份线路，而不影响正常的使用。

(5) 线缆的标记

在布线的过程中，一定要把每条双绞线与交换机以及交换机与主交换机之间端口对应起来，并且要使用线标，以备维护方便。

(6) 测试

布线完毕后，布线工程师要使用网络测试仪逐个的测试每一个节点的接通情况，建议使用 FLUCK，因为它能够提供足够多的参数，让工程师清楚整个布线系统的具体情况，包括损耗、最长距离、每对线缆的接通率等等。

此处的拓扑图只需将 7-12 作为网吧的第二层，而第一层只需将 7-12 图中的主设备间处改为一根通向二楼主设备间的主干线路即可。

8.10 思考与练习

1、填空题

- (1) 存储器管理、设备管理、文件管理
- (2) 面向任务型网络操作系统和通用型网络操作系统。
- (3) 网络驱动器接口规范(NDIS)和传输驱动器接口(TDI)标准
- (4) 网络性能分析、网络状态监控

2. 选择题

- (1) C
- (2) B
- (3) A
- (4) D

3. 问答题

- (1) 简述网络操作系统的主要特点。

答：网络操作系统是网络用户与计算机网络的接口。当今的网络操作系统具有如下特点：

a. 从体系结构的角度来看，当今的网络操作系统具有一般操作系统的所有职能，如任务管理、缓冲区管理、文件管理，以及磁盘、打印机等外设管理。

b. 从操作系统的角度看，大多数网络操作系统都是围绕核心调度的多用户共享资源的操作系统，包括磁盘处理、打印机处理、网络通信处理等面向用户的处理程序和面向多用户系统的核心调度程序。

c. 从网络的角度看,可以将网络操作系统与标准的网络层次模型作比较:在物理层和链路层上,网络操作系统支持多种网络接口卡,例如 Novell 公司、3Com 公司以及其他厂家的网卡,其中有基于总线的网卡,也有基于令牌环的网卡以及支持星型网络的 ARCNET 网卡。

(2) 局域网的主要服务有哪些?

答:局域网操作系统通过文件服务器向网络工作站提供各种有效的服务,这些服务主要包括以下几种:

a. 文件服务(File Service)

文件服务是局域网操作系统中最重要、最基本的网络服务功能。文件服务器以集中方式管理共享文件。网络工作站可以根据所规定的权限对文件进行相应的读、写以及其他各种操作。文件服务器为网络用户的文件安全与保密提供了必要的控制方法。

b. 打印服务(Print Service)

打印服务也是局域网操作系统提供的最基本的网络服务功能之一。共享打印服务可以通过设置专门的打印服务器来完成,或由工作站兼任,也可以由文件服务器担任。通过打印服务功能,在局域网中可以设置一台或几台打印机,这样,网络用户就可以远程共享网络打印机了。通过打印服务实现对用户打印请求的接收、打印格式的说明、打印机的配置、打印队列的管理等功能。网络打印服务在接收到用户打印请求后,按照先到先服务的原则,将多个用户需要打印的文件排队,使用排队队列管理用户的打印任务。

c. 数据库服务(Database Service)

网络数据库服务变得越来越重要,选择适当的网络数据库软件,按照客户端/服务器工作模式,开发出客户端与服务器端数据库应用程序,这样,客户端就可以使用结构化查询语言 SQL 向数据库服务器发送查询请求了,服务器进行查询后将查询结果发送到客户端。客户端/服务器模式优化了局域网系统的协同操作模式,有效地改善了局域网的应用系统性能。

d. 通信服务(Communication Service)

局域网提供的通信服务主要有:工作站与工作站之间的对等通信服务、工作站与主机之间的通信服务等。

e. 信息服务(Message Service)

局域网可以利用存储转发方式或对等的点到点通信方式完成电子邮件服务,目前已经进一步发展为文本文件和二进制数据文件,以及图像、数字视频与语音数据的同步传输服务。

f. 分布式服务(Distributed Service)

局域网操作系统为了支持分布式服务功能,提出了一种新的网络资源管理机制,即分布式目录服务。它将分布在不同地理位置的互联局域网中的资源组织在一个全局性的、可复制的分布数据库中,网中的多个服务器都有该数据库的副本。用户在一个工作站上注册,便可与多个服务器进行连接。对于用户来说,在一个局域网系统中的分布在不同位置的多个服务器资源都是透明的,用户可以使用简单的方法访问一个大型互联局域网系统。

g. 网络管理服务(Network Management Service)

局域网操作系统具有丰富的网络管理服务工具，可以向用户提供网络性能分析、网络状态监控、存储管理等多种管理服务。

h. Internet/Intranet 服务(Internet/Intranet Service)

为了适应 Internet 与 Intranet 的应用，局域网操作系统一般都支持 TCP/IP 协议、提供各种 Internet 服务和支持 Java 应用开发工具，使局域网服务器成为 Web 服务器，全面支持 Internet 与 Intranet 的访问。

9.6 思考与练习

1. 填空题

- (1) Microsoft 网络
- (2) Client/Server
- (3) 网络技术及设备选型

2. 选择题

- (1) A
- (2) C
- (3) B

3. 实践题

根据本章家庭网络组建实例的内容，组建一个家庭局域网环境，并实现接入 Internet，写出网络建设方案，并绘制出网络结构图。

答：根据本章介绍的知识，可以构建出简单的家庭局域网环境，首先需要构建出家庭网络的基本网络设备，由于考虑到价格和性能以及布线的工艺难度，所以，选择无线路由器，另外，为了能够满足在家庭网络中不同地方增加计算机，所以，建议使用交换机。具体的网络拓扑如图 9-13 所示。

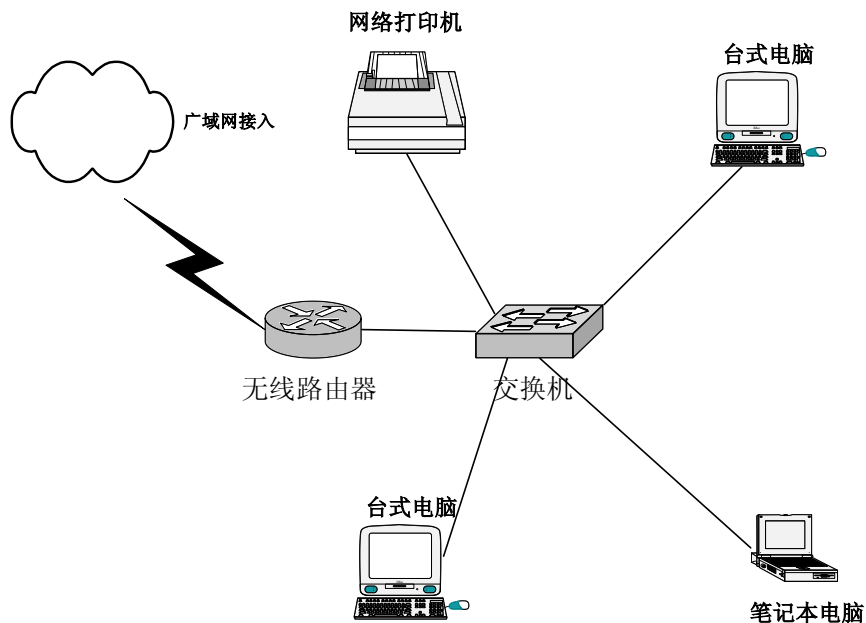


图 9-13 家庭网络拓扑图

10.6 思考与练习

1. 填空题

- (1) 一致性测试、互操作性测试和性能测试。
- (2) 当一条路径(通路)中没有其他背景流量时，网络能够提供的最大吞吐量。
- (3) 功能测试、性能测试、稳定性可靠性测试、一致性测试、互操作性测试和网管测试。
- (4) 入点测试和出点测试。

2. 选择题

- (1) A
- (2) ABCD
- (3) B
- (4) D

3. 问答题

- (1) 根据本章的内容，阐述 3 层交换机测试的主要指标和这些指标的意义。

答：三层交换机其实就是交换和路由的综合，所以要测试三层交换机就必须测试交

换和路由两方面。其分别为如下：

- 吞吐量：作为用户选择交换机和衡量交换机性能的最重要指标之一，吞吐量的高低决定了交换机在没有丢帧的情况下发送和接收帧的最大速率。
- 帧丢失率：帧丢失率可以反映交换机在过载时的性能状况，这对于反映在广播风暴等不正常状态下交换机的运行情况非常有用。
- 背对背(Back-to-Back)：该测试用于测试交换机在不丢帧的情况下能够持续转发数据帧的数量。该测试能够反映出数据缓冲区的大小。
- 延迟：该项指标能够决定数据包通过交换机的时间。延迟如果是 FIFO(First in and First Out)，即被测设备从收到帧的第 1 位达到输入端口开始到发出帧的第 1 位达到输出端口结束的时间间隔。
- 错误帧过滤：该测试项目决定了交换机能否正确地过滤某些错误类型的帧。
- 背压：决定交换机能否阻止将外来数据帧发送到拥塞端口，并且避免丢包。
- 线端阻塞(Head of Line Blocking, HOL)：该测试决定拥塞的端口如何影响非拥塞端口的转发速率。
- 全网状：该测试用于决定交换机在自己的所有端口都接收数据时，所能处理的总帧数。
- 部分网状：该测试在更严格的环境下测试交换机最大的承受能力，通过从多个发送端口向多个接收端口以网状形式发送帧来进行测试。
- 全双工线速转发能力：路由器最基本且最重要的功能是数据包的转发。
- 路由表能力：路由器通常依靠其所建立及维护的路由表来决定如何转发数据包。
- 背板能力：背板指的是输入与输出端口之间的物理通路，背板能力是路由器的内部实现，目前路由器通常采用共享背板技术。
- 丢包率：丢包率指的是测试中所丢失的数据包数量占所发送的数据包数量的比率，通常在吞吐量范围内进行测试。
- 时延：时延指的是数据包第一个比特进入路由器到最后一个比特从路由器输出的时间间隔。
- 时延抖动：时延抖动即时延变化。数据业务对时延抖动不敏感，对于 IP 上多业务，包括语音、视频业务的出现，该指标才有测试的必要性。
- VPN 支持能力：通常情况下，路由器都能支持 VPN。其性能差别一般体现在所支持的 VPN 数量上。一般情况下，专用路由器所支持的 VPN 数量较多。
- 内部时钟精度：拥有 ATM 端口做电路仿真或者 POS 口的路由器互联通常需要
- Qos：Qos 也是路由器测试的一项重要指标。
- 网络管理：网络管理指的是网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，包括配置管理、计费管理、性能管理、差错管理和安全管理。
- 可靠性和可用性：可靠性和可用性包括设备的冗余设计，冗余包括接口冗余、插卡冗余、电源冗余、系统板冗余、时钟板冗余、设备冗余等。

(2) 描述路由器性能测试的主要方法。

答：路由器测试一般可以分成以下几类：功能测试、性能测试、稳定性和可靠性测试、一致性测试、互操作性测试以及网络管理测试。

1. 功能测试

路由器功能通常可以划分为如下几个方面：

(1) 接口功能：该功能用于将路由器连接到网络中。可以分为局域网接口和广域网接口两种。局域网接口主要包括以太网、令牌环、令牌总线、FDDI 等网络接口；广域网接口主要包括 E1/T1、E3/T3、DS3、通用串行口等网络接口。

(2) 通信协议功能：该功能负责处理通信协议，包括 TCP/IP、PPP、X.25、帧中继等协议。

(3) 数据包转发功能：该功能主要用于按照路由表内容在各端口(包括逻辑端口)之间转发数据包并且改写链路层数据包的头信息。

(4) 路由信息维护功能：该功能负责运行路由协议，维护路由表。路由协议包括 RIP、OSPF、BGP 等协议。

(5) 管理控制功能：路由器管理控制功能包括 5 个功能：SNMP 代理功能、Telnet 服务器功能、本地管理、远端监控和 RMON 功能。通过多种不同的途径对路由器进行控制管理，并且允许记录日志。

(6) 安全功能：用于完成数据包过滤、地址转换、访问控制、数据加密、防火墙、地址分配等功能。

路由器对上述功能并非必须完全实现，但是由于路由器作为网络设备，存在最小功能集，对最小功能集所规定的功能，路由器必须给予支持。因为绝大多数的功能测试可以由接口测试、性能测试、协议一致性测试和网管测试所涵盖，所以，路由器功能测试一般可以仅对其他测试无法涵盖的功能进行验证性测试。路由器功能测试一般采用远端测试法。

2. 性能测试

路由器是 IP 网络的核心设备，其性能的好坏直接影响到 IP 网网络规模、网络稳定性和网络可扩展性。由于 IETF 没有对路由器性能测试作出专门的规定，一般来说，只能按照 RFC2544 进行测试。但是，路由器区别于一般简单的网络互联设备，因此，在性能测试时还应该加上路由器特有的性能测试。例如：路由表容量、路由协议收敛时间等指标。路由器性能测试应当包括以下指标：

(1) 吞吐量：测试路由器包转发的能力。指的是路由器在不丢包的条件下每秒转发包的极限，一般可以采用二分法查找该极限点。

(2) 时延：测试路由器在吞吐量范围内从收到包到转发出该包的时间间隔。时延测试应当重复 20 次，然后取其平均值。

(3) 丢包率：用于测试路由器在不同负荷下丢弃包占收到包的比例。不同负荷通常指从吞吐量测试到线速(线路上传输包的最高速率)，步长一般为线速的 10%。

(4) 背靠背帧数：测试路由器在接收到以最小包间隔传输时不丢包条件下所能处理的最大包数。该测试实际上是考验路由器的缓存能力，如果路由器具备线速能力(吞吐量=接口媒体线速)，则该测试没有意义。

(5) 系统恢复时间：测试路由器在过载后恢复正常工作所需要的时间。测试方法可以采用向路由器端口发送吞吐量 110% 和线速间的较小值，持续 60 秒后，将速率下降到 50% 的时刻到最后一个丢包的时间范围。如果路由器具备线速能力，则该测试没有意义。

(6) 系统复位：测试路由器从软件复位或关电重启到正常工作的时间间隔。正常工作指的是能以吞吐量转发数据。

3. 一致性测试

路由器一致性测试通常采用“黑箱”方法，被测试设备 IUT 叫做“黑箱”。测试系统通过控制观察点 PCO 与被测试设备接口来进行测试。

不同的测试事件是通过不同的 PCO 来控制 and 观察的，按照其应答是否符合规范，即定时关系和数据匹配限制，测试的结果可分为通过、失败、无结果 3 种。路由器是一种复杂的网络互联设备，需要在各个通信层上实现多种协议。例如，相应接口的物理层和链路层协议、IP/ICMP 等互联网层协议、TCP/UDP 等传输层协议、Telnet/SNMP 等应用层协议和 RIP/OSPF/BGP 等路由协议。

协议一致性测试应当包含路由器所实现的所有协议。由于该测试内容繁多且测试复杂，在测试中，可以选择重要的协议以及所关心的内容进行测试。由于骨干网上的路由器可能影响到全球路由，所以，在路由器测试中，应特别重视路由协议一致性测试，例如 OSPF 和 BGP 协议。由于一致性测试只能选择有限测试例进行测试，一般无法涵盖协议的所有内容。所以，即使已通过测试也无法保证设备能完全实现协议的所有内容，所以最好的办法是在现实环境中进行测试。路由器一致性测试一般采用分布式测试法或远端测试法。

4. 互操作测试

由于通信协议、路由协议非常复杂并且拥有众多的选项，因此，实现同一协议的路由器并不能保证互通、互操作。并且因为一致性测试的能力有限，即使可以通过协议一致性测试也未必能保证完全实现协议，所以，有必要对设备进行互操作测试。

互操作测试实际上是将一致性测试中所使用的仪表替换成需要与之互通、互操作的设备，选择一些重要且典型的互联方式进行配置，观察两台设备是否能按照预期的计划正常工作。

5. 稳定性、可靠性测试

路由器的稳定性和可靠性很难进行测试。一般可以通过两种途径得到：(1) 厂家通过关键部件的可靠性以及备份程度来计算出系统的可靠性；(2) 用户或厂家通过大量相同产品在使用中的故障率来统计产品的稳定性和可靠性。当然，用户也可以通过在一定时间内，对试运行结果的要求来保证路由器的可靠性与稳定性。

6. 网管测试

网管测试一般用于测试网管软件对网络和网络设备的管理能力。由于路由器是 IP 网的核心设备，所以必须测试路由器对网管的支持度。如果路由器附带有网管软件，可以通过使用所附带的网管软件来检查网管软件所实现的配置管理、安全管理、性能管理、计费管理、故障管理、拓扑管理和视图管理等功能。如果路由器不附带有网管软件，则应当测试路由器对 SNMP 协议实现的一致性和对 MIB 实现的程度。由于路由器需要实现的 MIB 非

常多，每个 MIB 都包含有大量的内容，很难对 MIB 实现完全测试。一般可以通过抽测重要的 MIB 项来检查路由器对 MIB 的实现情况。

(3) 简答网络故障分层检测的方法。

答：针对网络的分层结构特点，在分析和排查网络故障时，应充分利用网络这种分层的特点，快速准确地定位并排除故障。

TCP/IP 的层次结构为管理员分析和排查故障提供了非常好的组织方式。由于其各层相对独立，按层排查能够有效地发现和隔离故障，因而一般使用逐层分析和排查的方法。

逐层排查方式通常有两种，一种是从低层开始排查，适用于物理网络不够成熟稳定的情况，例如组建新的网络、重新调整网络线缆、增加新的网络设备；另一种是从高层开始排查，适用于物理网络相对成熟稳定的情况，例如硬件设备没有变动。无论使用哪种方式，最终都能达到目标，只是解决问题的效率有所差别。

具体采用哪种排查方式，可根据具体地情况来选择。例如，遇到某客户端不能访问 Web 服务的情况，如果管理员首先去检查网络的连接线缆，就显得太悲观了，除非明确知道网络线路有所变动。比较好的选择方法是直接从应用层着手，可以按照以下方法进行排查：首先检查客户端的 Web 浏览器是否正确配置，可以尝试使用浏览器访问另一个 Web 服务器，如果 Web 浏览器没有问题，可以在 Web 服务器上测试 Web 服务器是否正常运行；如果 Web 服务器没有问题，再测试网络的连通性。即使是 Web 服务器问题，从底层开始逐层排查也能最终解决问题，只是花费的时间太多了。如果碰巧是线路问题，从高层开始逐层排查也要浪费时间。

4. 实践题

假设现在在公司里网络发生了故障导致无法上网，你作为一名网管，应该如何排除故障。

答：根据本章介绍的知识，可以分成以下排错步骤：

(1) 首先，查看无线路由器，LAN 的灯是否亮绿灯，如是则正常，否则说明路由器故障。

(2) 再查看无线路由器的 WAN 灯是否亮且亮绿灯，如是说明正常，否则说明可能是带宽外线故障或者路由器本身故障。

(3) 如果以上可能都排除，接下来需要检测交换机，观察交换机的灯是否闪烁，使用操作系统的网络监视器来查看网络包交换情况，来确认交换机是否故障。

(4) 当交换机故障排除后，下面就要观察是否在局域网内出现 IP 地址冲突，如果是的话，要及时修改。

(5) 当以上可能性排除后，剩下的是网卡故障和操作系统软件故障。

只需按照以上的步骤一步一步的排除，最终就可以找到网络故障的原因。

11.6 思考与练习

1. 填空题

- (1) 配置管理、故障管理、性能管理、安全管理和计费管理。
- (2) 集中式网管和分布式网管
- (3) 被管理设备、代理和网络管理系统(NMS)
- (4) Get、Set 和 Trap。

2. 选择题

- (1) B
- (2) C
- (3) A
- (4) D

3. 问答题

- (1) 简述网络管理系统的 5 大功能。

答：国际标准化组织(ISO)在 ISO/IEC 7498-4 文档中定义了网络管理的 5 大功能：配置管理、故障管理、性能管理、安全性和计费管理。

1. 配置管理

配置管理是一组辨别、定义、控制和监视设备所必需的相关功能，即网络中应有或实际有多少设备，每个设备的功能及其连接关系、工作参数等。

2. 故障管理

故障管理指的是管理功能中的监测设备故障以及与故障设备的监测、恢复或故障排除等措施有关的网络管理功能，其目的是保证网络能够提供可靠的服务。

3. 性能管理

性能管理用于对系统运行和通信效率等系统性能进行评价，包括从被管理设备中收集与网络性能有关的数据，分析和统计历史数据，建立性能分析模型，预测网络性能的长期趋势，并根据分析和预测结果对网络拓扑结构和参数进行调整。性能管理保证了网络资源的最优化利用。

4. 安全管理

安全管理涉及的问题包括保证网络管理工作可靠进行的安全问题，保护网络用户个人隐私和保护网络管理对象的问题。

5. 计费管理

计费管理过程主要用于完成与费用有关的一些信息的收集、处理并给出报告，包括用户对网络资源的使用等，计费管理功能提供了对用户收费的依据。

- (2) SNMP 定义了哪些基本命令？

答：SNMP 实现中的基本命令有 3 个：Get、Set 和 Trap。

- **Get**：管理系统可以读取管理代理包含的对象信息的值。Get 命令是 SNMP 协议中使用率最高的一个命令，因为它是从网络设备中获取管理信息的基本方法。
- **Set**：管理系统可以修改管理代理包含的对象信息的值。Set 命令是一个特权命令，因为通过它可以改变设备的配置或控制设备的运行状态。
- **Trap(陷阱)**：管理代理可以向网络管理软件主动发送一些信息。Trap 命令的功能是在网络管理系统没有明确的要求下，管理代理主动通知网络管理系统网络上有一些特别的情况或特别的问题发生了。

12.8 思考与练习

1. 填空题

- (1) 机密性、完整性、可用性、真实性和不可否认性。
- (2) 物理层安全、系统层安全、网络层安全、应用层安全和安全管理。
- (3) 对称加密算法(私钥密码体系)和非对称加密算法(公钥密码体系)。
- (4) 网络层
- (5) 数据采集子系统、数据分析子系统、控制台子系统和数据库管理子系统。

2. 选择题

- (1) A
- (2) ACD
- (3) A
- (4) D

3. 问答题

1) 简述网络安全防范体系的结构框架。

答：网络安全防范体系的科学性和可行性是其可顺利实施的保障。基于 DISSP 扩展的一个三维安全防范技术体系框架结构，第一维是安全服务，给出了 8 种安全属性(ITU-T REC-X.800-199103-I)，其中包括了对等实体认证、数据源认证、访问控制、机密性、流量机密性、数据完整性、抗否认服务、可用性；第二维是系统单元，给出了信息网络系统的组成，其包括了通信平台、网络平台、系统平台、应用平台、物理环境；第三维是结构层次，给出并扩展了国际标准化组织 ISO 的开放系统互联(OSI)模型，其包括了应用层、传输层、网络层、链路层和物理层。

框架结构中的每一个系统单元都对应于某一个协议层次，需要采取若干种安全服务才

能保证该系统单元的安全。网络平台需要有网络节点之间的认证和访问控制,应用平台需要有针对性用户的认证和访问控制,需要保证数据传输的完整性和保密性,需要有抗抵赖和审计的功能,需要保证应用系统的可用性和可靠性。针对一个信息网络系统,如果在各个系统单元都有相应的安全措施来满足其安全需求,则该信息网络被认为是安全的。

2) 简述入侵检测技术的工作原理。

答:目前,IDS 分析及检测入侵阶段一般通过以下几种技术手段进行分析:特征库匹配、基于统计的分析和完整性分析。其中,前两种方法用于实时的入侵检测,而完整性分析则用于事后分析。为了能够更有效地发现网络受攻击的迹象,网络入侵检测部件应当能够分析网络上所使用的各种网络协议,识别各种网络攻击行为。网络入侵检测部件对网络攻击行为的识别通常是通过网络入侵特征库来实现,这种方法有利于在出现了新的网络攻击手段时,方便地对入侵特征库加以更新,提高入侵检测部件对网络攻击行为的识别能力。

根据 IDS 监控的对象,可以将 IDS 分为以下两大类:

- 基于网络的系统:这种 IDS 放置在网络之上,靠近被检测的系统,它们用于监测网络流量并判断它是否正常。
- 基于主机的系统:这种系统经常运行在被监测的系统之上,用以监测系统上正在运行的进程并判断它是否合法。

利用网络入侵检测技术可以实现网络安全检测和实时攻击识别,但它只能作为网络安全的一个重要安全组件,网络系统的实际安全实现应该结合使用防火墙等技术来组成一个完整的网络安全解决方案,其原因在于,网络入侵检测技术虽然能对网络攻击进行识别并做出反应,但其侧重点在于发现,不能代替防火墙系统执行整个网络的访问控制策略。防火墙系统能够将一些预期的网络攻击阻挡在网络外面,而网络入侵检测技术除了减小网络安全风险之外,还能对一些非预期的攻击进行识别并做出反应,切断攻击连接或通知防火墙系统修改控制准则,将下一次的类似攻击阻挡在网络外部。因此,通过将网络安全检测技术和防火墙系统结合起来,可以实现一个完整的网络安全解决方案。

3) 简述 IPSec 的工作原理。

答:IPSec 的工作原理类似于包过滤防火墙,可以看作是对包过滤防火墙的一种扩展。当接收到一个 IP 数据包时,包过滤防火墙使用其头部在一个规则表中进行匹配,当找到一个相匹配的规则时,包过滤防火墙就按照该规则制订的方法对接收到的 IP 数据包进行处理。这里的处理工作只有两种:丢弃或转发。

IPSec 通过查询 SPD(Security Policy Database 安全策略数据库)决定对接收到的 IP 数据包进行处理。但是,IPSec 不同于包过滤防火墙的是:对 IP 数据包的处理方法除了丢弃和直接转发(绕过 IPSec)外,还有一种即进行 IPSec 处理。正是这个新增添的处理方法提供了比包过滤防火墙更进一步的网络安全性。

进行 IPSec 处理意味着对 IP 数据包进行加密和认证。包过滤防火墙只能控制来自或去往某个站点的 IP 数据包的通过,可以拒绝来自某个外部站点的 IP 数据包访问内部某些站点,也可以拒绝某个内部站点对某些外部网站的访问。但是,包过滤防火墙不能保证从内部网络出去的数据包不被截取,也不能保证进入内部网络的数据包未经篡改。只有在对

IP 数据包实施了加密和认证后，才能保证在外部网络传输的数据包的机密性、真实性、完整性，通过 Internet 进行安全的通信才成为可能。

IPSec 既可以只对 IP 数据包进行加密，或只进行认证，也可以同时实施两者。但无论是进行加密还是进行认证，IPSec 都有两种工作模式：一种是协议工作方式类似的隧道模式；另一种是传输模式。

传输模式只对 IP 数据包的有效负载进行加密或认证。此时，继续使用以前的 IP 头部，只对 IP 头部的部分域进行修改，而 IPSec 协议头部插入到 IP 头部和传输层头部之间。

隧道模式对整个 IP 数据包进行加密或认证。此时，需要新产生一个 IP 头部，IPSec 头部被放置在新产生的 IP 头部和以前的 IP 数据包之间，从而组成一个新的 IP 头部。