

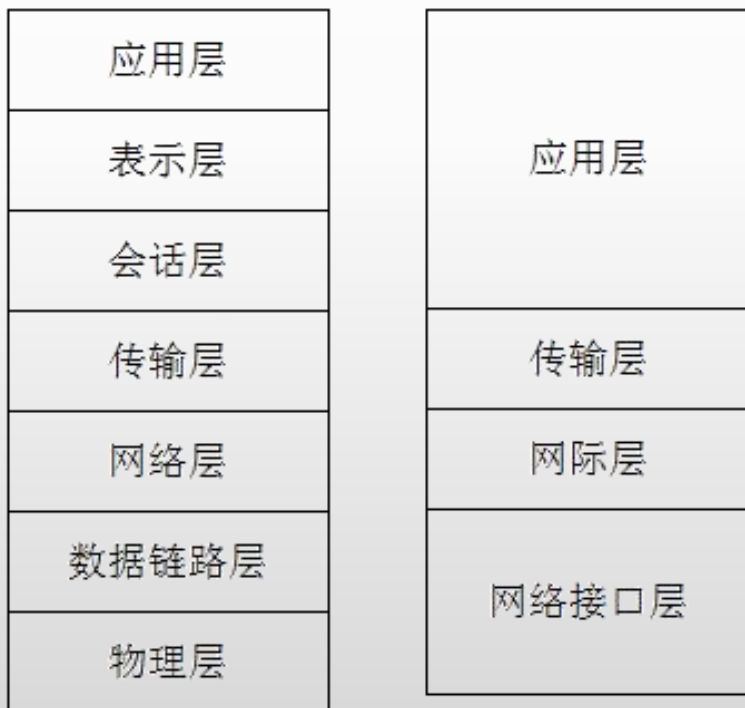
计算机网络基础

51CTO学院：邹月平

网络互联模型

- 1977 年，国际标准化组织为适应网络标准化发展的需求，制定了开放系统互联参考模型（Open System Interconnection/Reference Model, **OSI/RM**），从而形成了网络架构的国际标准。OSI/RM 构造了由下到上的七层模型，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。口诀：“**巫术忘传会鸢鹰**”。
- 互联网协议（Internet Protocol Suite）是一个网络通信模型，以及一整个网络传输协议家族，为互联网的基础通信架构。它常被通称为**TCP/IP协议族**（英语：TCP/IP Protocol Suite，或TCP/IP Protocols），简称TCP/IP。因为该协议家族的两个核心协议：TCP（传输控制协议）和IP（网际协议），为该家族中最早通过的标准。

- **TCP/IP提供点对点的链接机制，将数据应该如何封装、定址、传输、路由以及在目的地如何接收，都加以标准化。它将软件通信过程抽象化为四个抽象层，采取协议堆栈的方式，分别实现出不同通信协议。协议族下的各种协议，依其功能不同，被分别归属到这四个层次结构之中，常被视为是简化的七层OSI模型。**



层的名称	主要功能	详细说明
应用层	处理网络应用	直接为端用户服务，提供各类应用过程的接口和用户接口。例如HTTP、Telnet、FTP、SMTP、NFS等
表示层	数据表示	使应用层可以根据其服务解释数据的涵义。通常包括数据编码的约定、本地句法的转换。例如JPEG、ASCII、GIF、DES、MPEG等
会话层	互连主机通信	负责管理远程用户或进程间的通信，通常包括通信控制、检查点设置、重建中断的传输链路、名字查找和安全验证服务。例如：RPC、SQL等
传输层	端到端连接	实现发送端和接收端的端到端的数据分组传送，负责保证实现数据包无差错、按顺序、无丢失和无冗余的传输。其服务访问点为端口。代表性协议有TCP、UDP、SPX等
网络层	分组传输和路由选择	通过网络连接交换传输层实体发出的数据，解决路由器选择、网络拥塞、异构网络互联的问题。服务访问点为逻辑地址（网络地址）。代表性协议有IP、IPX等
数据链路层	传输以帧为单位的信息	建立、维持和释放网络实体之间的数据链路，把流量控制合并在一起。为MAC（媒介访问层）和LLC（逻辑链路层）两个子层。服务访问点为物理地址（MAC地址）。代表性协议有IEEE802.3/2、HDLC、PPP、ATM等
物理层	二进制为传输	通过一系列协议定义了通行设备的机械的、电气的、功能的、规程的特征。代表性协议有RS232、V.35、RJ-45、FDDI等

常见的网络协议

1. 应用层协议

在应用层中，定义了很多面向应用的协议，应用程序通过本层协议利用网络完成数据交互的任务。这些协议主要有 FTP、TFTP、HTTP、SMTP、DHCP、Telnet、DNS 和 SNMP 等。

FTP (File TransportProtocol, 文件传输协议) 是网络上两台计算机传送文件的协议，运行在 **TCP** 之上，是通过 Internet 将文件从一台计算机传输到另一台计算机的一种途径。FTP 的传输模式包括 Bin (二进制) 和 ASCII (文本文件) 两种，除了文本文件之外，都应该使用二进制模式传输。FTP 在客户机和服务器之间需建立两条 TCP 连接，一条用于传送控制信息 (使用 **21** 号端口)，另一条用于传送文件内容 (使用 **20** 号端口)。

TFTP (Trivial FileTransfer Protocol, 简单文件传输协议) 是用来在客户机与服务器之间进行简单文件传输的协议, 提供不复杂、开销不大的文件传输服务。TFTP 建立在 **UDP** (User Datagram Protocol, 用户数据报协议) 之上, 提供不可靠的数据流传输服务, 不提供存取授权与认证机制, 使用超时重传方式来保证数据的到达。

HTTP (Hypertext TransferProtocol, 超文本传输协议) 是用于从 WWW 服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效, 使网络传输减少。HTTP 建立在 **TCP** 之上, 它不仅保证计算机正确快速地传输超文本文档, 还确定传输文档中的哪一部分, 以及哪部分内容首先显示等。

2. 传输层协议

传输层主要有两个传输协议，分别是 TCP 和 UDP（User Datagram Protocol，用户数据报协议），这些协议负责提供流量控制、错误校验和排序服务。

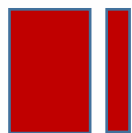
TCP 是整个 TCP/IP 协议族中最重要的协议之一，它在 IP 协议提供的不可靠数据服务的基础上，采用了重发技术，为应用程序提供了一个**可靠的、面向连接的、全双工**的数据传输服务。TCP 协议一般用于传输**数据量比较少**，且对可靠性要求高的场合。

UDP 是一种**不可靠的、无连接**的协议，可以保证应用程序进程间的通信，与 TCP 相比，UDP 是一种无连接的协议，它的错误检测功能要弱得多。可以说，TCP 有助于提供可靠性，而 UDP 则有助于提高传输速率。UDP 协议一般用于传输**数据量大**，对可靠性要求不是很高，但要求速度快的场合。

3. 网络层协议

网络层中的协议主要有 IP、ICMP (Internet Control Message Protocol, 网际控制报文协议)、IGMP (Internet Group Management Protocol, 网际组管理协议)、ARP (Address Resolution Protocol, 地址解析协议) 和 RARP (Reverse Address Resolution Protocol, 反向地址解析协议) 等, 这些协议处理信息的路由和主机地址解析。

IP 所提供的服务通常被认为是无连接的和不可靠的, 它将差错检测和流量控制之类的服务授权给了其他的各层协议, 这正是 TCP/IP 能够高效率工作的一个重要保证。网络层的功能主要由 IP 来提供, 除了提供端到端的分组分发功能外, IP 还提供很多扩充功能。例如, 为了克服数据链路层对帧大小的限制, 网络层提供了数据分块和重组功能, 这使得很大的 IP 数据包能以较小的分组在网络上传输。

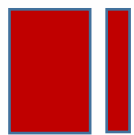


IP地址及其表示方法

IP (IPV4) 地址是一个32位的二进制数的逻辑地址，为了表示方便，将32位二进制数划分成4个字节，每个字节间以 “.” 区分。例如，IP地址11000000 10101000 11001000 10000000，用十进制表示就是192.168.200.128

IP地址由两个部分组成，**网络号+主机号**

	0	1	2	3	4	8	16	24	31			
A类 1~126	0	网络号				主机号						
B类 128~191	1	0	网络号					主机号				
C类 192~223	1	1	0	网络号					主机号			



IP地址及其表示方法

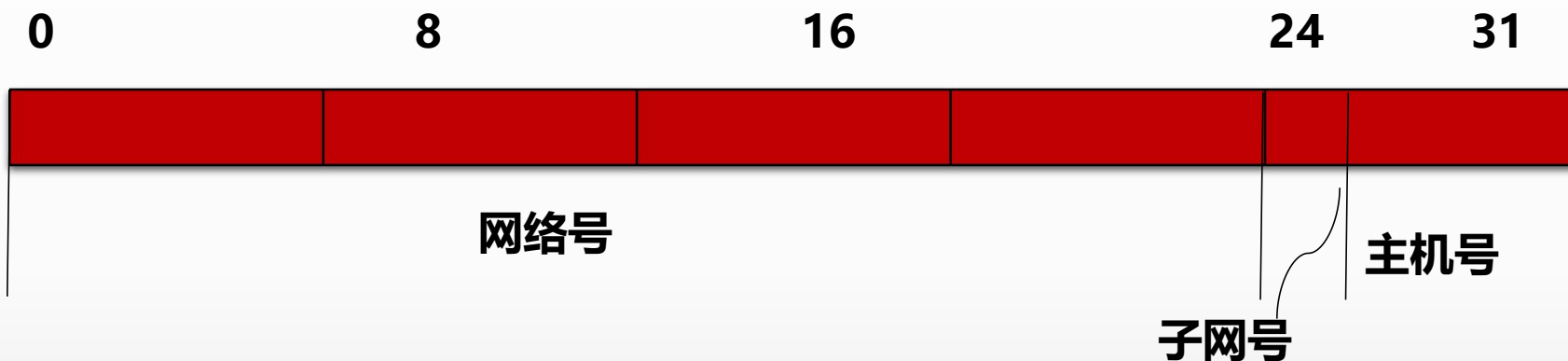
0 1 2 3 4 8 16 24 31

D类 224~239	1	1	1	0	组播地址																										
---------------	---	---	---	---	------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

E类 240~255	1	1	1	0	保留																										
---------------	---	---	---	---	----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

子网与子网掩码

三级IP地址：网络号+子网号+主机号



子网掩码也是32位二进制数，网络与子网标识全为1，主机标识全部为0。

A类地址的子网掩码：255.0.0.0

B类地址的子网掩码：255.255.0.0

C类地址的子网掩码：255.255.255.0

子网与子网掩码

将IP地址和其对应的子网掩码逐位进行“与”运算，可得到对应的子网的网络地址。

例如：某主机的IP地址为136.34.5.56，子网掩码为255.255.255.0。进行与运算后，得出该主机所在子网的网络号为136.34.5.0

因此路由器在相互之间交换信息的时候，除了要给出目的地址和下一跳地址外，还需要给出该目的网络的子网掩码。

例如：IP地址：131.1.123.24/27与IP地址：131.1.123.43/27是否在同一网段？

解析：/27代表前27位都是网络号，主机号是5位，因此将24与43 分别转换成二进制：

000 11000

001 01011

典型真题

与地址220. 112. 179. 92匹配的路由表的表项是 （ ） 。

A. 220. 112. 145. 32/22

B. 220. 112. 145. 64/22

C. 220. 112. 147. 64/22

D. 220. 112. 177. 64/22

典型真题

试题分析

因为都是/22因此我们只看前22位既可，又因为选项中前两个数（16位）一样，因此我们直对比第三个数，将第三个数转换位二进制，对比其前6位。

179→ 1011 0011

145→ 1001 0001

147→ 1001 0011

177→ 1011 0001

22 位掩码，除去前2组16位，还剩余6位，从左向右匹配177一致。

参考答案：D

典型真题

某公司网络的地址是 192.168.192.0/20, 要把该网络分成 32 个子网, 则对应的子网掩码应该是 () , 每个子网可分配的主机地址数是 () 。

A. 255.255.252.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

A. 62

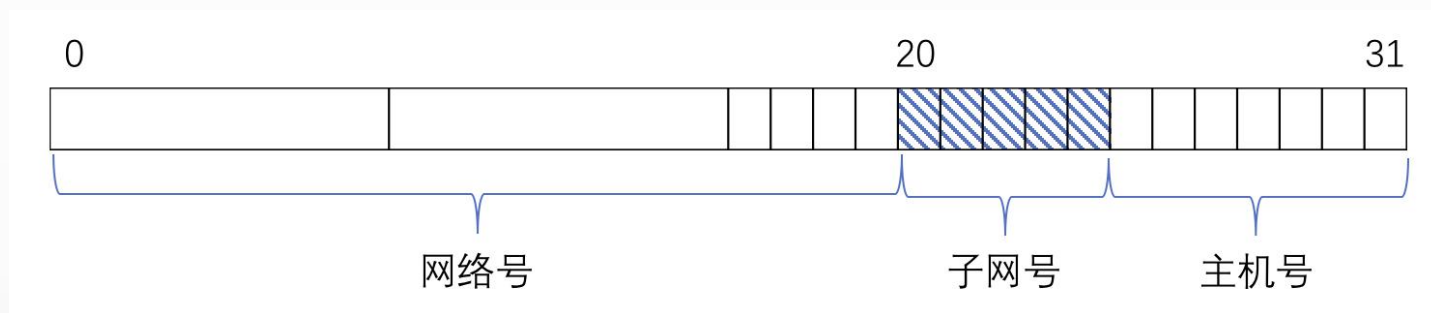
B. 126

C. 254

D. 510

典型真题

试题分析



IPv4地址用4个字节即32位表示，前20位作为网络地址，第21至第24位为子网号（占5位），剩余第25至31位为主机号（占7位）。

因此子网掩码占25位，最后一个字节的左边第一位是1，即 $2^7=128$ ，子网掩码为255.255.255.128。主机号占7位，去掉全是0和全是1，实际为126。

参考答案：D B

典型真题

分配给某公司网络的地址块是220.17.192.0/20，该网络被划分为_____个C类子网，不属于该公司网络的子网地址是_____。

A. 4 B. 8 C. 16 D. 32

A. 220.17.203.0

B. 220.17.205.0

C. 220.17.207.0

D. 220.17.213.0

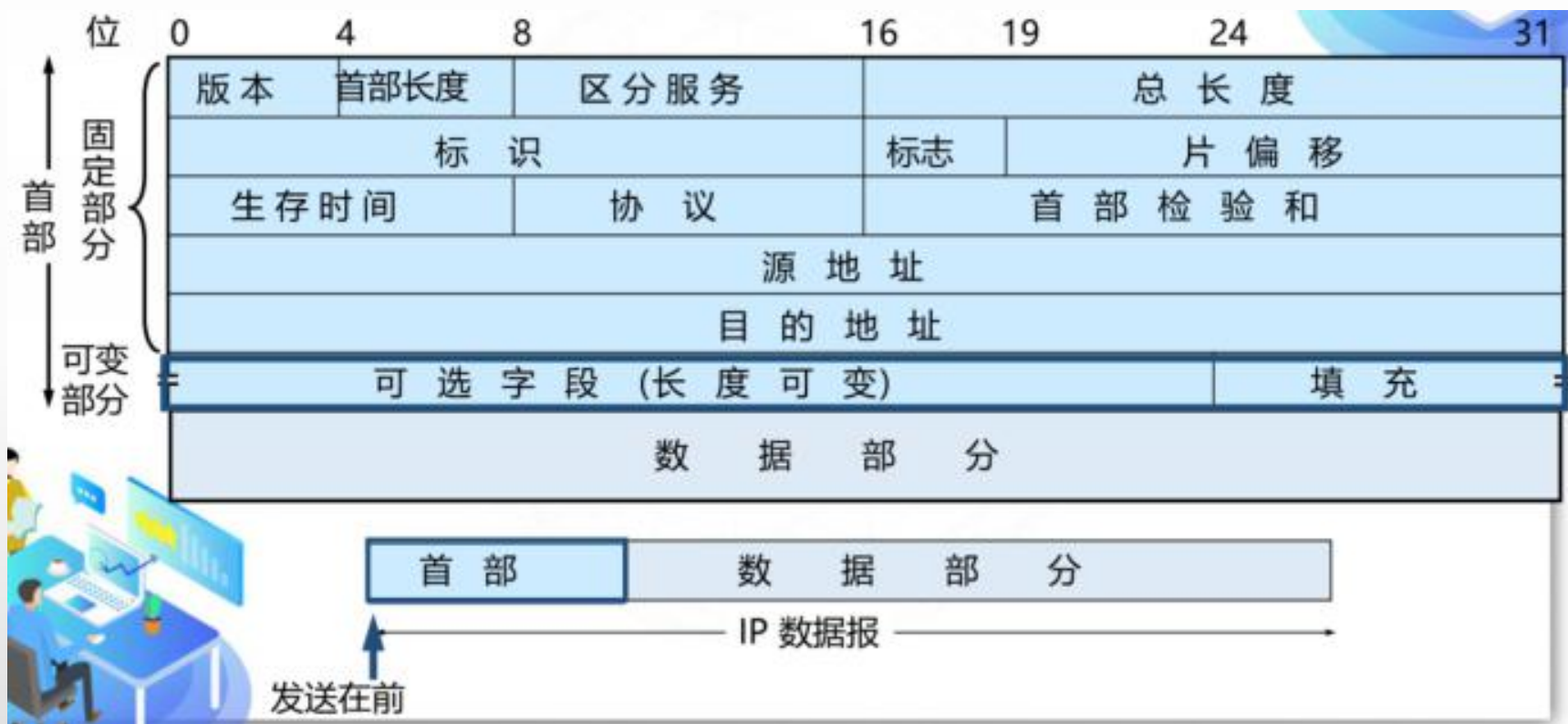
典型真题

解析：

220. 17. 192. 0是一个C类网络地址，应该有24位子网掩码，现在仅采用20位子网掩码，少了4位，所以被划分成了 $2^4=16$ 个子网。16个子网号的第三个字段范围为192~207，因此D不属于该公司网络的子网地址。

参考答案：C、D

IPV4数据报



IPV4数据报

版本	IP协议的版本。这里版本号为4。
首部长度	可表示的最大数值是15个单位（4 字节为一个单位）， 60字节。
区分服务	不同优先级服务质量不同，只有在使用区分服务（DiffServ）时有效。
总长度	首部与数据之和的长度，最大长度为 $2^{16}-1=65535$ 字节。
标识	唯一标识数据报的标识符。
标志	DF：不分片位，MF：片未完位。
片偏移	指明该段处于原来数据报中的位置。
生存时间	记为TTL（Time To Live），指示数据报在网络中可通过的路由器的最大值。
协议	数据报携带的协议（TCP、UDP、IGMP等）
首部检验和	只检验首部，不检验数据。采用16位二进制反码求和算法。
可选字段	可记录时间戳，通过路径，安全信息等。
填充	填充为4的倍数。

典型真题

IETF定义的区分服务（DiffServ）模型要求每个IP分组都要根据IPv4协议头中的（ ）字段加上一个DS码点，然后内部路由器根据DS码点的值对分组进行调度和转发。

- A. 数据报生存期
- B. 服务类型
- C. 段偏置值
- D. 源地址

典型真题

试题分析

Diffserv体系模型的核心思想是：在网络边界将数据流按QoS要求进行简单分类，不同的类别在内部节点的每次转发中实现不同的转发特性。

Diffserv体系使得ISP能够提供给每个用户不同等级和质量的服务。用户(或网络边界节点)通过设置每个数据包的DS字段(IPV4首标中的服务类型(ToS)字段或IPV6首标中的通信类(Traffic Class)字段)的值要求特定的服务等级。其中，被设置的DS字段被称为区分服务码点(DSCP)。这样就维持了现有的IP分组格式不变。

参考答案：B

IPv6

互联网络能发展到当前的规模，IPv4 协议的建立功不可没。但同时它的缺点也已经充分显现出来，如地址空间耗尽、路由表急剧膨胀、缺乏对 QoS 的支持、本身并不提供任何安全机制、移动性差等问题。尽管采用了许多新的机制来缓解这些问题，如 DHCP 技术、NAT 技术、CIDR 技术等，但都不可避免地要引入其他新的问题，问题没有得到根本解决。于是 IETF 从 90 年代起就开始积极探讨下一代 IP 网络，经过几年努力，在广泛听取业界和专家意见的基础上，终于在 1995 年 12 月推出了下一代网络的 RFC 文档——IPv6 协议，该协议最早叫做下一代 IP(IP Next Generation, IPng)。现在它的全称是“互联网协议第 6 版”，即下一代的网际协议。

IPv6

下一代IP地址，共128位，以16位为一段，共为8段，每段的16位转换为一个4位的十六进制数，没段之间用 “:” 分开。例如，
2001:0da8:d001:0001:0000:0000:0000:0001，

还可以表示为：2001： da8： d001： 1： 0： 0： 0： 1与2001： da8： d001：
1： : 1

与IPv4比， IPv6的优势：

IPv6有更大的地址空间
IPv6使用更小的路由表
IPv6增加了组播支持与对流支持
IPv6加入了自动配置的支持
IPv6具有更高的安全性

IPv6

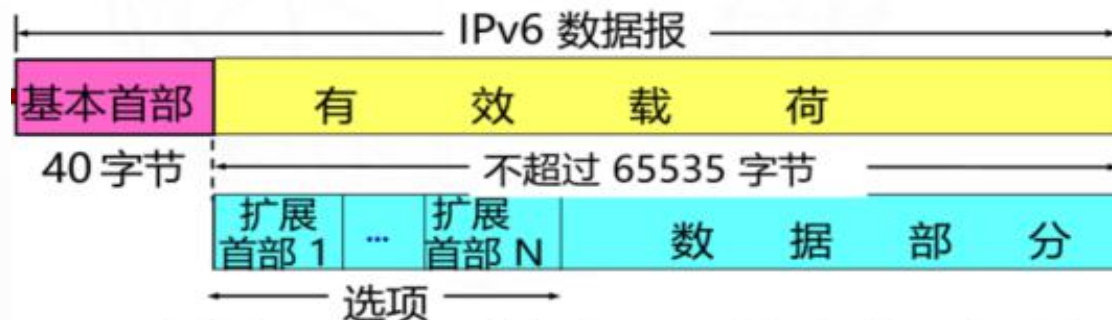
IPv4 / IPv6 过渡技术有：

(1) 双协议栈技术：双栈技术通过节点对 IPv4 和 IPv6 双协议栈的支持，从而支持两种业务的共存。

(2) 隧道技术：隧道技术通过在 IPv4 网络中部署隧道，实现在 IPv4 网络上对 IPv6 业务的承载，保证业务的共存和过渡。具体的隧道技术包括：6to4 隧道；6over4 隧道；ISATAP 隧道。

(3) NAT-PT 技术：NAT - PT 使用网关设备连接 IPv6 和 IPv4 网络。当 IPv4 和 IPv6节点互相访问时，NAT - PT 网关实现两种协议的转换翻译和地址的映射。

IPv6数据报



版本 (4)	流量分类 (8)	流标签 (20)	
有效负载 (16)		下一头部 (8)	跳数限制 (8)
源 IP (128)			
目的 IP (128)			

Ipv6 首部结构

IPV6数据报

版本	IP协议的版本。这里版本号为6。
流量分类	通信类型，相当于IPV4服务类型字段。
流标签	从源点到终点的一系列数据报，同一个流上的数据报标签相同，保证服务质量。
有效负载长度	除基本首部以外的字节数（所有扩展首部都算在有效负载内），最大值64KB
下一头部	相当于IPV4的协议字段或可选字段。
跳数限制	用于检测路由循环，路由器在转发数据报时对这个字段减1，变成0丢弃该数据报。

IPv6数据报的目的地址可以是以下三种基本类型地址之一：

- （1）单播（unicast）：传统的点对点通信。
- （2）多播/组播（multicast）：一点对多点的通信。
- （3）任播（anycast）：这是 IPv6增加的一种类型。任播的目的站是一组计算机，但数据报在交付时只交付其中的一个，通常是距离最近的一个。

TCP与UDP

在TCP/IP协议簇中有两个传输协议，即传输控制协议（Transmission Control Protocol, TCP）和用户数据报协议（User Datagram Protocol, UDP）。TCP是面向连接的，而UDP是无连接的。

➤ 传输控制协议（Transmission Control Protocol, TCP）是一种可靠的、面向连接的字节流服务。

TCP建立在无连接的IP基础之上，因此使用了3种机制实现面向连接的服务。

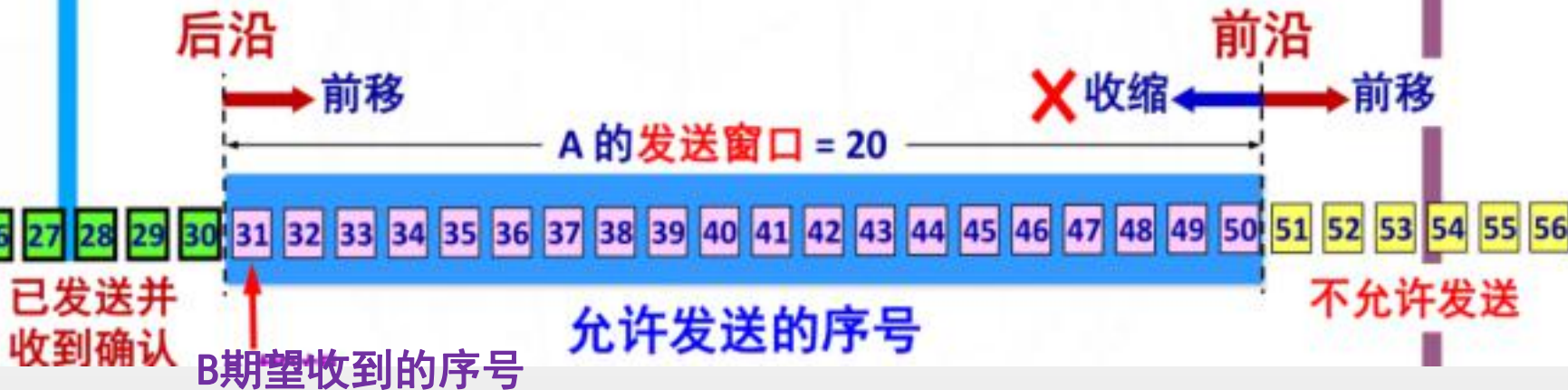
1) 使用序号对数据报进行标记。

这种方式便于TCP接收服务在向高层传递数据之前调整失序的数据包。

2) TCP使用确认、校验和定时器系统提供可靠性。当接收者按照顺序识别出数据报未能到达或发生错误时，接收者将通知发送者；当接收者在特定时间没有发送确认信息时，那么发送者就会认为发送的数据包并没有到达接收方，这时发送者就会考虑重传数据。

3) TCP使用窗口机制调整数据流量。并且窗口的大小并不是固定的，而是会随着网络的情况进行调整。

TCP与UDP



TCP 协议

- TCP只有一种类型的PDU，叫作TCP段，段头（也叫TCP头或传输头）的格式如图6-21 所示，其中的字段如下。

源端口				2^16				目标端口				2^16																			
固定				发送顺序号				首部大																							
20字节				接收顺序号				60字节																							
偏置值		保留		URG		ACK		PSH		RST		SYN		FIN		可变 窗口															
校验和				所有				紧急指针				总长度最大																			
可变40字节				任选项+补丁				65535字节																							
MTU=1500-20(IP报头)																用户数据 - 20(TCP报头)=1460字节															

TCP 传输头格式

UDP 协议

用户数据报协议 (User Datagram Protocol, UDP) 是一种不可靠的、无连接的数据报服务。源主机在传送数据前不需要和目标主机建立连接。

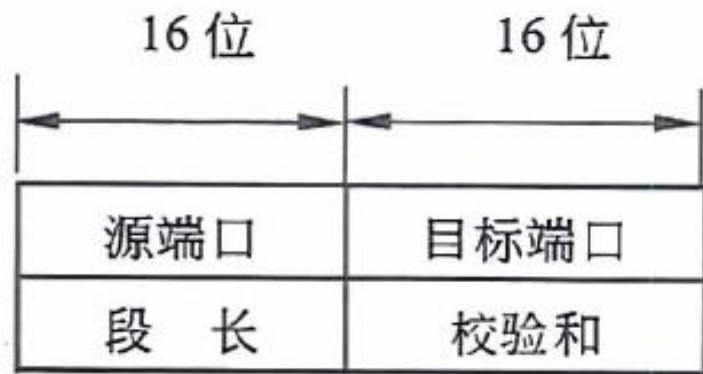


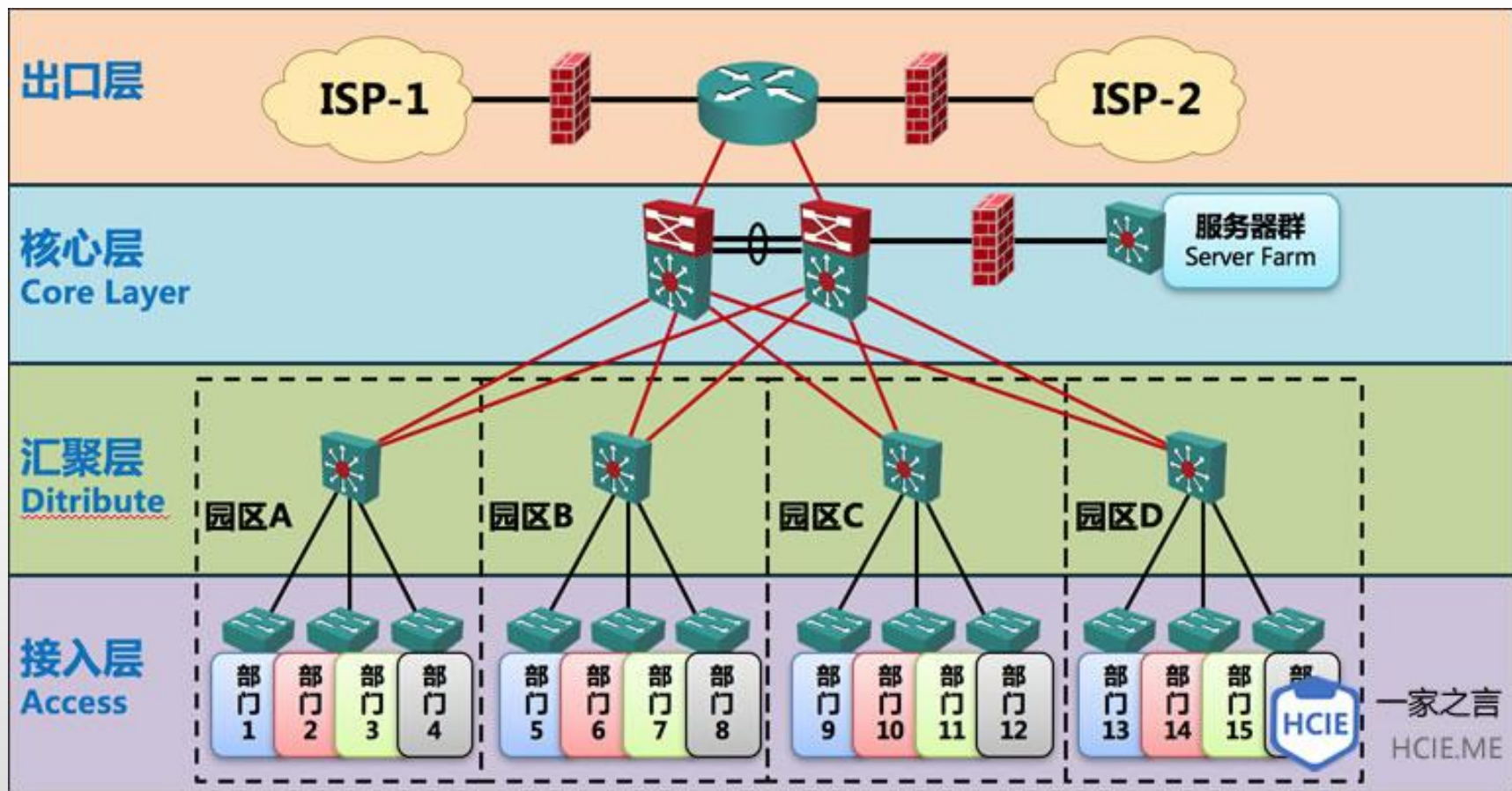
图 6-26 UDP 头

TCP与UDP

➤ 用户数据报协议（User Datagram Protocol，UDP）是一种不可靠的、无连接的数据报服务。源主机在传送数据前不需要和目标主机建立连接。

- （1）UDP是无连接的，发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延。
- （2）UDP使用尽最大努力交付，即不保证可靠交付，因此主机不需要维持复杂的连接状态表。
- （3）UDP是面向报文的。UDP对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。UDP一次交付一个完整的报文。
- （4）UDP没有拥塞控制，因此网络出现的拥塞不会使源主机的发送速率降低。这对某些实时应用是很重要的。很适合多媒体通信的要求。
- （5）UDP支持一对一、一对多、多对一和多对多的交互通信。
- （6）UDP的首部开销小，只有8个字节，比TCP的 20个字节的首部要短。

网络设计



网络设计

通常将网络中**直接面向用户连接或访问网络**的部分称为**接入层**，将位于接入层和核心层之间的部分称为分布层或汇聚层。目的是允许终端用户连接到网络，主要解决相邻用户之间的互访需求，并且为这些访问提供足够的带宽，接入层还应当适当负责一些**用户管理功能**（如地址认证、用户认证、计费管理等），以及用户信息收集工作（如用户的IP地址、MAC地址、访问日志等）。

网络设计

汇聚层是核心层和接入层的分界面，完成**网络访问策略控制、数据包处理、过滤、寻址**，以及其他数据处理的任务。汇聚层交换机是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路，因此，汇聚层交换机与接入层交换机比较，需要更高的性能、更少的接口和更高的交换速率。

网络设计

网络主干部分称为核心层，**核心层的主要目的在于通过高速转发通信**，提供优化、可靠的**骨干传输**结构，因此，核心层交换机应拥有更高的可靠性，性能和吞吐量。核心层为网络提供了骨干组件或高速交换组件，在纯粹的分层设计中，核心层只完成**数据交换**的特殊任务。需要根据网络需求的地理距离、信息流量和数据负载的轻重来选择核心层技术，常用的技术包括ATM、100Base-Fx和千兆以太网等。在主干网中，考虑到高可用性的需求，通常会使用双星（树）结构，即采用两台同样的交换机，与汇聚层交换机分别连接，并使用链路聚合技术实现**双机互联**。

核心层的设备采用**双机冗余热备份**是非常必要的，也可以使用负载均衡功能来改善网络性能。

典型真题

按照网络分层设计模型，通常把局域网设计为3层，即核心层、汇聚层和接入层，以下关于分层网络功能的描述中，不正确的是（ ）。

- A. 核心层设备负责数据包过滤、策略路由等功能
- B. 汇聚层完成路由汇总和协议转换功能
- C. 接入层应提供一部分管理功能，例如MAC地址认证、计费管理等
- D. 接入层负责收集用户信息，例如用户IP地址、MAC地址、访问日志等

典型真题

试题分析

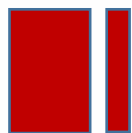
三层模型将大型局域网划分为核心层、汇聚层和接入层，每一层都有特定的作用。

①核心层是因特网络的高速骨干网，由于其重要性，因此在设计中应该采用冗余组件设计。在设计核心层设备的功能时，应尽量避免使用数据包过滤和策略路由等降低数据包转发速率的功能。如果需要连接因特网和外部网络，核心层还应包括一条或多条连接到外部网络的连接。

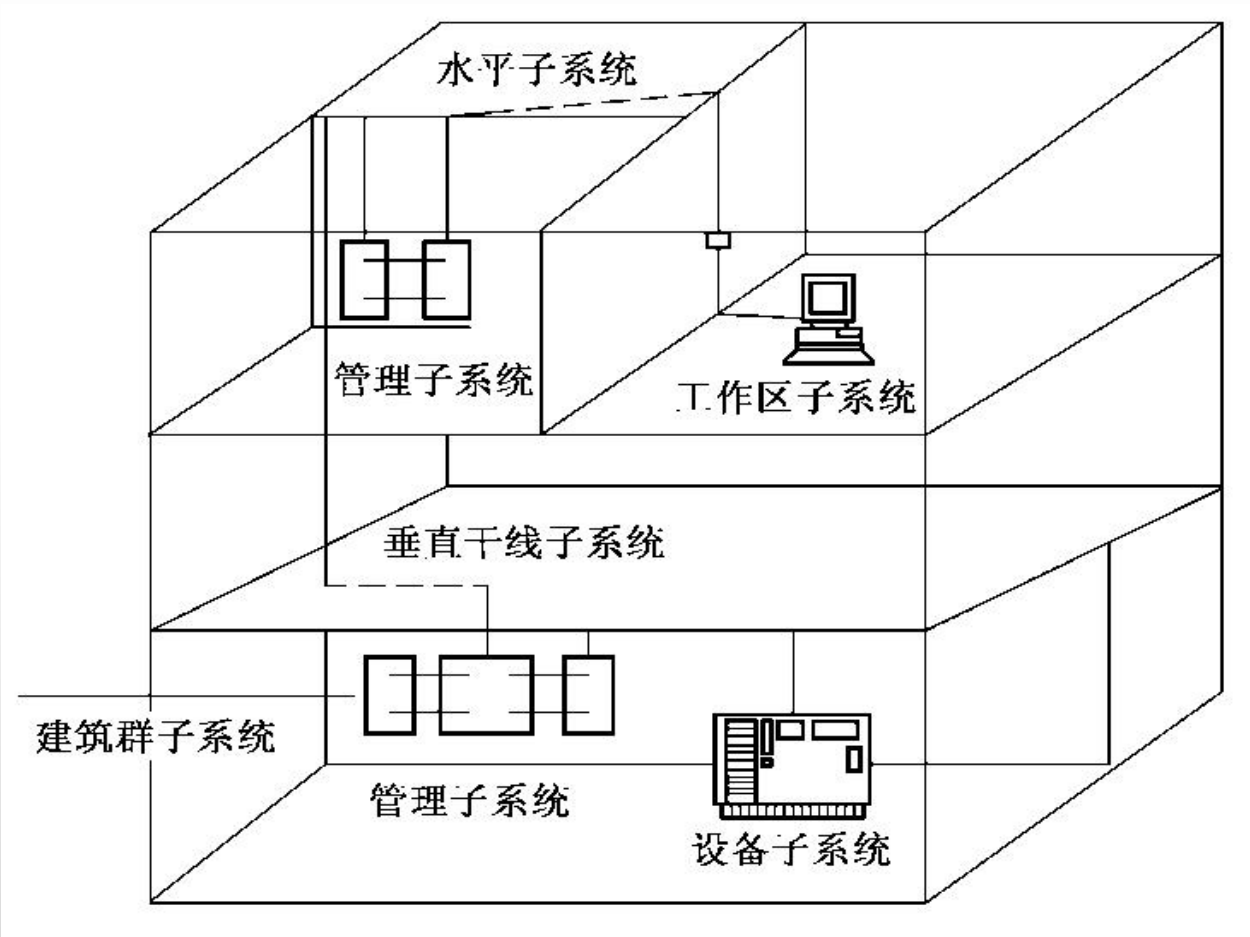
②汇聚层是核心层和接入层之间的分界点，应尽量将资源访问控制、流量的控制等在汇聚层实现。为保证层次化的特性，汇聚层应该向核心层隐藏接入层的细节，例如不管接入层划分了多少个子网，汇聚层向核心层路由器进行路由宣告时，仅宣告由多个子网地址汇聚而成的网络。为保证核心层能够连接运行不同协议的区域网络，各种协议的转换都应在汇聚层完成。

③接入层为用户提供在本地网段访问应用系统的能力，也要为相邻用户之间的互访需求提供足够的带宽。接入层还应该负责一些用户管理功能，以及户信息的收集工作。

参考答案：A



综合布线系统

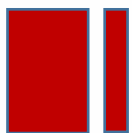


综合布线系统

综合布线系统是一个用于传输语音、数据、影像和其他信息的标准结构化布线系统，是建筑物或建筑群的传输网络，它使语言和数据通信设备、交换设备和其他信息管理系统彼此相连接。综合布线的热物理结构一般采用模块化设计和分层星型拓扑结构。系统结构有6个独立的子系统：

1.工作区子系统：它是工作区内终端设备连接到信息插座之间的设备组成，包括信息插座、连接软线、适配器、计算机、网络集散器、电话、报警探头、摄像机、监视器、音响等。

2.水平子系统：水平子系统是布置在同一楼层上，一端接在信息插座，另一端接在配线间的跳线架上，它的功能是将干线子系统线路延伸到用户工作区，将用户工作区引至管理子系统，并为用户提供一个符合国际标准，满足语音及高速数据传输要求的信息点出口。



综合布线系统

3.管理子系统：安装有线路管理器件及各种公用设备，实现整个系统集中管理，它是干线子系统和水平子系统的桥梁，同时又可为同层组网提供条件。其中包括双绞线跳线架、跳线(有快接式跳线和简易跳线之分)。

4.垂直（干线）子系统：通常它是由主设备间至各层管理间，特别是在位于中央点的公共系统设备处提供多个线路设施，采用大对数的电缆馈线或光缆，两端分别端接在设备间和管理间的跳线架上，目的是实现计算机设备、程控交换机(PBX)、控制中心与各管理子系统间的连接，是建筑物干线电缆的路由。

综合布线系统

5.设备间子系统：该子系统是由设备间中的电缆、连接跳线架及相关支撑硬件、防雷电保护装置等构成。可以说是整个配线系统的中心单元，因此它的布放、造型及环境条件的考虑适当与否，直接影响到将来信息系统的正常运行及维护和使用的灵活性。电话交换机、计算机主机设备及入口设施也可与配线设备安装在一起。

6.建筑群子系统：它是将多个建筑物的数据通信信号连接成一体的布线系统，它采用架空或地下电缆管道或直埋敷设的室外电缆和光缆互连起来，是结构化布线系统的一部分，支持提供楼群之间通信所需的硬件。

典型真题

结构化布线系统分为六个子系统，其中水平子系统（ ）。

- A. 由各种交叉连接设备以及集线器和交换机等设备组成
- B. 连接了干线子系统和工作区子系统
- C. 由终端设备到信息插座的整个区域组成
- D. 实现各楼层设备间子系统之间的互连

典型真题

试题分析

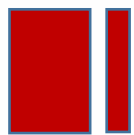
结构化布线系统分为6个子系统：工作区子系统、水平子系统、管理子系统、干线(或垂直)子系统、设备间子系统和建筑群子系统。其中水平子系统是指各个楼层接线间的配线架到工作区信息插座之间所安装的线缆系统，其作用是将干线子系统与用户工作区连接起来。

参考答案： B

域名和地址

Internet 地址分为3级，可表示为“网络地址·主机地址.端口地址”的形式。其中，网络和主机地址即 IP地址；端口地址就是TCP 或UDP 地址，用于表示上层进程的服务访问点。TCP/IP 网络中的大多数公共应用进程都有专用的端口号，这些端口号是由 IANA (Internet Assigned Numbers Authority) 指定的，其值小于1024，而用户进程的端口号一般大于1024。

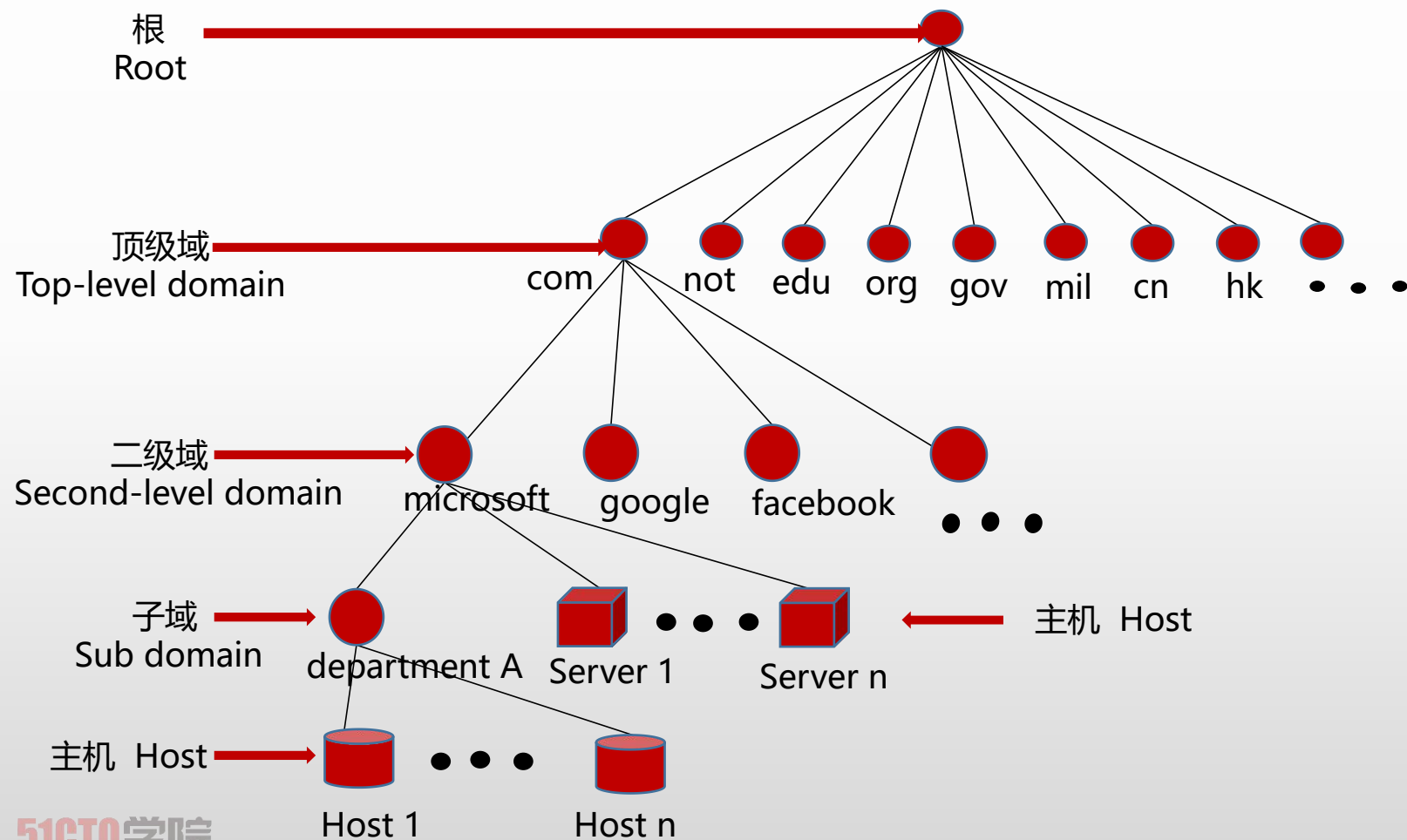


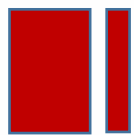


域名系统 (DNS)

域名系统 (Domain Name System, DNS) 是把主机域名解析为IP地址的系统, 解决了IP地址难记的问题。该系统是由解析器和域名服务器组成的。**DNS使用UDP协议, 较少情况下使用TCP协议, 端口号均为53。域名系统由三部分构成: DNS名字空间、域名服务器、DNS客户机。**

域名系统 (DNS)



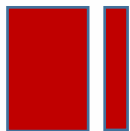


域名系统 (DNS)

(1) 根域：根域处于Internet上域名空间结构树的最高端，是树的根，提供根域名服务。根域用 “.” 来表示。

(2) 顶级域名 (Top Level Domain, TLD)：顶级域名在根域名之下，分为三大类：国家顶级域名、通用顶级域名和国际顶级域名。

(3) 主机：属于最低层域名，处于域名树的叶子端，代表各类主机提供的服务。



域名系统 (DNS)

通用顶级域名	
域名	使用对象
com	商业机构等盈利性组织
edu	教育机构、学术组织和国家科研中心等
gov	美国非军事性的政府机关
mil	美国的军事组织
net	网络信息中心 (NIC) 和网络操作中心 (BIC) 等
org	非盈利性组织、例如技术支持小组、计算机用户小组等
int	国际组织

域名系统 (DNS)

顶级域下面是二级域，这是正式注册给组织和个人的唯一名称，例如 `www.microsoft.com` 中的 `microsoft` 就是微软注册的域名。

在二级域之下，组织机构还可以划分子域，使其各个分支部门都获得一个专用的名称标识，例如 `www.sales.microsoft.com` 中的 `sales` 是微软销售部门的子域名称。划分子域的工作可以一直延续下去，直到满足组织机构的管理需要为止。但是标准规定，一个域名的长度通常不超过63 个字符，最多不能超过255个字符。

第一级域名

第二级域名

用户单元名

用户名

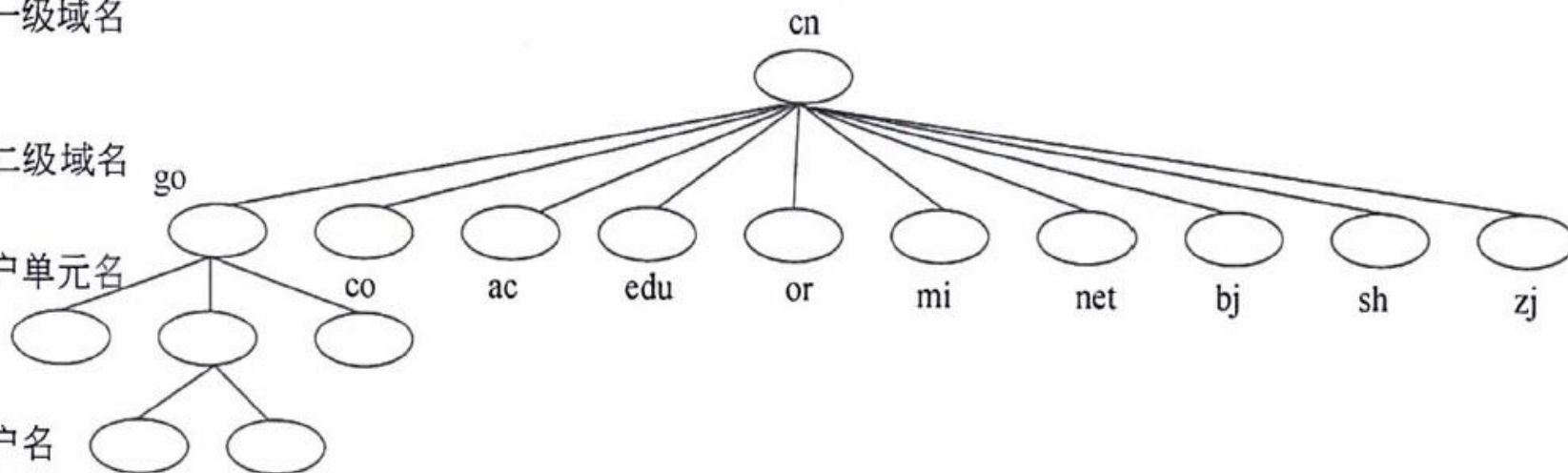


图 6-27 在 cn 域名下的域名树

域名服务器

名称	定义	作用
主域名服务器	维护本区所有域名信息，信息存于磁盘文件和数据库中	提供本区域名解析，区内域名信息的权威。具有域名数据库。一个域有且只有一个主域名服务器
辅助域名服务器	主域名服务器的备份服务器提供域名解析服务，信息存于磁盘文件和数据库中	主域名服务器备份，可进行域名解析的负载均衡。具有域名数据库
缓存域名服务器	向其他域名服务器进行域名查询，将查询结果保存在缓存中的域名服务器	改善网络中DNS服务器的性能，减少反复查询相同域名的时间，提高解析速度，节约出口带宽。获取解析结果耗时最短，没有域名数据库
转发域名服务器	负责非本地和缓存中无法查到的域名。接收域名查询请求，首先查询自身缓存，如果找不到对应的，则转发到指定的域名服务器查询	负责域名转发，由于转发域名服务器同样可以有缓存，因此可以减少流量和查询次数。具有域名数据库

域名查询

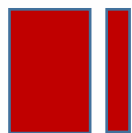
DNS协议：查询过程两种方法：

(1)递归查询

当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果——IP地址或错误信息。

(2)迭代查询

服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器得到的响应可能不是目标的IP地址，而是其他服务器的引用（名字和地址），那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的IP地址或错误信息。



网络互连与常用设备

互 联 设 备	工 作 层 次	主 要 功 能
中继器	物理层	对接收信号进行再生和发送，只起到扩展传输距离的作用，对高层协议是透明的，但使用个数有限（例如，在以太网中只能使用 4 个）
网桥	数据链路层	根据帧物理地址进行网络之间的信息转发，可缓解网络通信繁忙度，提高效率。只能够连接相同 MAC 层的网络
路由器	网络层	通过逻辑地址进行网络之间的信息转发，可完成异构网络之间的互联互通，只能连接使用相同网络层协议的子网
网关	高层（第 4~7 层）	最复杂的网络互联设备，用于连接网络层以上执行不同协议的子网
集线器	物理层	多端口中继器
二层交换机	数据链路层	是指传统意义上的交换机，多端口网桥
三层交换机	网络层	带路由功能的二层交换机
多层交换机	高层（第 4~7 层）	带协议转换的交换机

网络存储技术

目前，主流的网络存储技术主要有三种，分别是直接附加存储（Direct Attached Storage, DAS）、网络附加存储（Network Attached Storage, NAS）和存储区域网络（Storage Area Network, SAN）。

1. 直接附加存储

DAS 是将存储设备通过 SCSI（Small Computer System Interface，小型计算机系统接口）电缆直接连到服务器，其本身是硬件的堆叠，存储操作依赖于服务器，不带有任何存储操作系统。因此，有些文献也把 DAS 称为 SAS（Server Attached Storage，服务器附加存储）。

网络存储技术

DAS 的适用环境为：

- (1) 服务器在地理分布上很分散，通过 SAN 或 NAS 在它们之间进行互连非常困难时；**
- (2) 存储系统必须被直接连接到应用服务器（例如，Microsoft Cluster Server 或某些数据库使用的“原始分区”）上时；**
- (3) 包括许多数据库应用和应用服务器在内的应用，它们需要直接连接到存储器上时。**

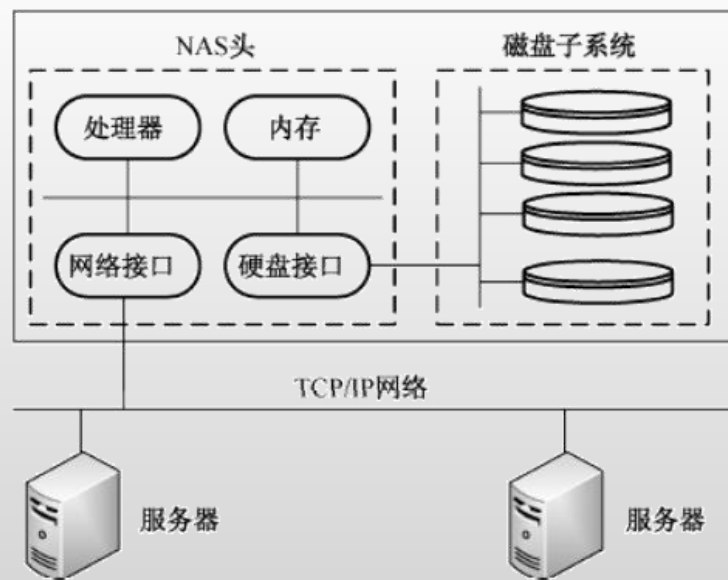
网络存储技术

由于 DAS 直接将存储设备连接到服务器上，这导致它在传递距离、连接数量、传输速率等方面都受到限制。因此，当存储容量增加时，DAS 方式很难扩展，这对存储容量的升级是一个巨大的瓶颈；另一方面，由于数据的读取都要通过服务器来处理，必然导致服务器的处理压力增加，数据处理和传输能力将大大降低；此外，当服务器出现宕机等异常状况时，也会波及存储数据，使其无法使用。目前 DAS 基本被 NAS 所代替。

网络存储技术

2. 网络附加存储

采用 NAS 技术的存储设备不再通过 I/O 总线隶属于某个特定的服务器，而是通过网络接口与网络直接相连，由用户通过网络访问。NAS 存储系统的结构如图所示。



网络存储技术

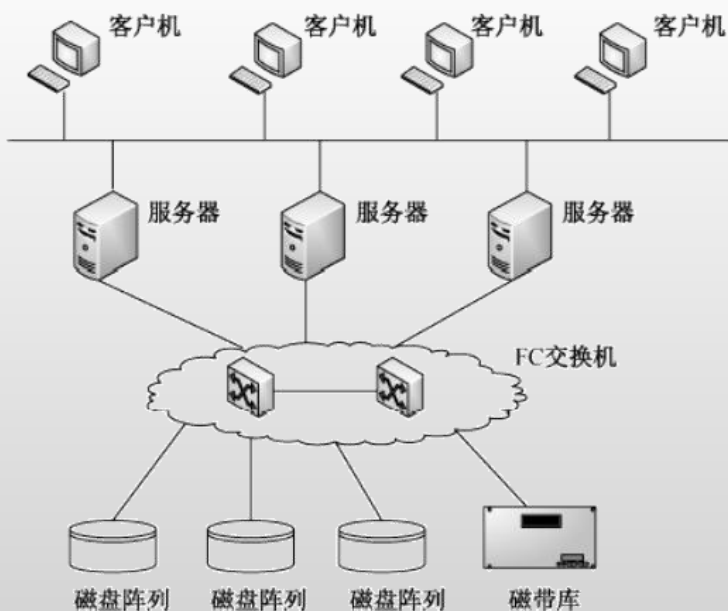
NAS 存储设备类似于一个专用的文件服务器，它去掉了通用服务器的大多数计算功能，而仅提供文件系统功能，从而降低了设备的成本。并且为方便存储设备到网络之间能以最有效的方式发送数据，它专门优化了系统硬件与软件架构。NAS 以数据为中心，将存储设备与服务器分离，其存储设备在功能上完全独立于网络中的主服务器，客户机与存储设备之间的数据访问不再需要文件服务器的干预，同时它允许客户机与存储设备之间进行直接的数据访问，所以不仅响应速度快，而且数据传输速率也很高。

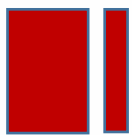
NAS 存储支持即插即用，可以在网络的任一位置建立存储。基于 Web 管理，从而使设备的安装、使用和管理更加容易。NAS 可以很经济地解决存储容量不足的问题，但难以获得满意的性能。

网络存储技术

3. 存储区域网络

SAN 是通过专用交换机将磁盘阵列与服务器连接起来的高速专用子网。它没有采用文件共享存取方式，而是采用块（block）级别存储。SAN 是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统，其最大特点是将存储设备从传统的以太网中分离出来，成为独立的存储区域网络，SAN 的系统结构如图所示。

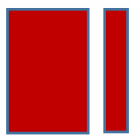




网络系统建设

企业内部网络的建设已经成为提升企业核心竞争力的关键因素。企业网已经越来越多地被人们提到，利用网络技术，现代企业可以在供应商、客户、合作伙伴、员工之间实现优化的信息沟通。这直接关系到企业能否获得关键的竞争优势。企业网络要求具有资源共享功能、通信服务功能、多媒体功能、远程VPN拨入访问功能。所以在进行企业网络的需求分析时，对企业的需求、应用范围、基于的技术等，要从企业应用来进行分析。

先期的网络规划对网络建设和使用至关重要。网络规划的任务就是为即将建立的网络系统提出一套完整的设想和方案，对建立一个什么形式、多大规模、具备哪些功能的网络系统做出全面科学的论证，并对建立网络系统所需的人力、财力和物力投入等做出一个总体的计划。



网络系统建设

1. 网络设计的原则

在网络设计方面，应着重考虑以下几个要素，它们也是网络设计和网络建设的基本原则。

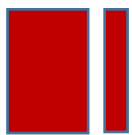
(1) 采用先进，成熟的技术。在规划网络、选择网络技术和网络设备时，应重点考虑当今主流的网络技术和网络设备。只有这样，才能保证建成的网络有良好的性能，从而有效地保护建网投资，保证网络设备之间、网络设备和计算机之间的互联，以及网络的尽快使用、可靠运行。

(2) 遵循国际标准，坚持开放性原则。网络的建设应遵循国际标准，采用大多数厂家支持的标准协议及标准接口，从而为异种机、异种操作系统的互连提供极大的便利和可能。

网络系统建设

(3) 网络的可管理性。具有良好可管理性的网络，网管人员可借助先进的网管软件，方便地完成设备配置、状态监视、信息统计、流量分析、故障报警、诊断和排除等任务。

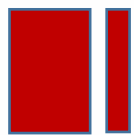
(4) 系统的安全性。一般的网络包括内部的业务网和外部网。对于内部用户，可分别授予不同的访问权限，同时对不同的部门（或工作组）进行不同的访问及连通设置。对于外部的因特网络，要考虑网络“黑客”和其他不法分子的破坏，防止网络病毒的传播。有些网络系统，如金融系统对安全性和保密性有着更加严格的要求。网络系统的安全性包括两个方面的内容：一方面是外部网络与本单位网络之间互联的安全性问题，另一方面是本单位网络系统管理的安全性问题。



网络系统建设

(5) 灵活性和扩充性。网络的灵活性体现在连接方便，设置和管理简单、灵活，使用和维护方便。网络的可扩充性表现在数量的增加、质量的提高和新功能的扩充。网络的主干设备应采用功能强、扩充性好的设备，如模块化结构、软件可升级，信息传输速度快、吞吐量大。可灵活选择快速以太网、千兆以太网、FDDI、ATM网络模块进行配置，关键元件应具有冗余备份的功能。

(6) 系统的稳定性和可靠性。选择网络产品和服务器时，最重要的一点应考虑它们的稳定性和可靠性，这也是我们强调选择技术先进、成熟产品的重要原因之一。关键网络设备和重要服务器的选择应考虑是否具有好的电源备份系统、链路备份系统，是否具有中心处理模块的备份，系统是否具有快速、良好的自愈能力等。不应追求那些功能大而全但不可靠或不稳定的产品，也不要选择那些不成熟和没有形成规范的产品。



网络系统建设

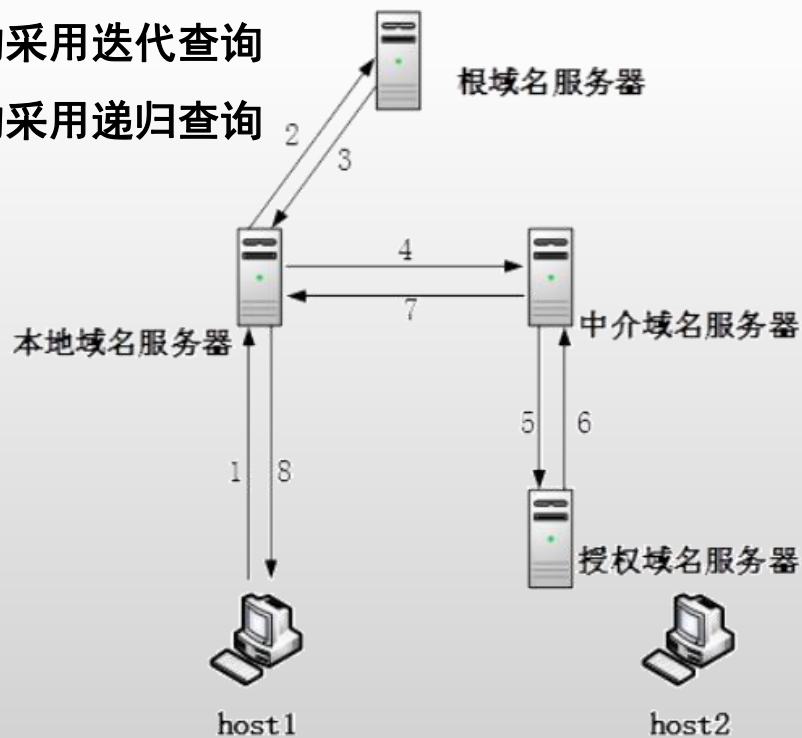
(7) 经济性。网络的规划不但要保质保量按时完成，而且要减少失误、杜绝浪费。

(8) 实用性。网络设计一定要充分保护网络系统现有资源。同时要根据实际情况，采用新技术和新装备，还需要考虑组网过程要与平台建设及开发同步进行，建立一个实用的网络。力求使网络既满足目前需要，又能适应未来发展，同时达到较好的性能/价格比。

典型真题

- 主机host1对host2进行域名查询的过程如下图所示，下列说法中正确的是（ ）。

- A. 根域名服务器采用迭代查询，中介域名服务器采用递归查询
- B. 根域名服务器采用递归查询，中介域名服务器采用迭代查询
- C. 根域名服务器和中介域名服务器均采用迭代查询
- D. 根域名服务器和中介域名服务器均采用递归查询



典型真题

试题分析

本题考查的是网络中DNS的相关知识，在DNS运行的过程中，常常涉及到两种类型的查询：迭代查询和递归查询。

迭代查询的基本思想是：A服务器问B服务器：“host2的IP是多少？”，B服务器回答：“C服务器管这方面的事务，你问问他吧！”，此时A服务器根据B提供的线索找到C服务器，并问他“host2的IP是多少？”，C服务器回答“D服务器管这方面的事务，你问问他吧！”。依据这样的流程，一步步得到host2的地址，是迭代查询方式。

典型真题

递归查询的基本思想是：A服务器问B服务器：“host2的IP是多少？”，B服务器发现自己也不知道，但他知道，这个事情在C服务器管辖范围内，所以B服务器直接找到C服务器问“host2的IP是多少？”，C服务器发现自己也不清楚具体情况，但他辖区内的D服务器应该知道，此时他问D服务器“host2的IP是多少？”，当得到答案后，一层一层回复上去，直到A服务器。这种方式，就是递归查询。

试题答案：A

技术成就梦想