# 第10课 互联网协议：数据报转发

## 一、单项选择题

1. （　　） is (are) responsible for fragments reassembly.

A. The routers B. The ultimate destination host

C. The source host D. The routers and destination host

答：B。

1. When transmitting frames without setting DF (Don't Fragment) tag, how does a router treat a frame that is larger than the outbound interfaces maximum transmission unit?

A. drops the packet

B. sends a host unreachable message to the sender

C. fragments the packets into units allowed by the outbound interfaces MTU

D. none of these

答：C。

1. 路由器通常采用 （　　） 连接以太网交换机。
2. RJ-45端口 B. Console端口 C. 异步串口 D. 高速同步串口

答：A。路由器通常使用RJ-45端口连接以太网交换机。RJ-45是一种标准化的网络接口连接器，用于以太网连接。路由器的以太网接口使用RJ-45端口与以太网交换机进行连接，这些端口通常标记为LAN或以太网端口。

1. 以下关于三层交换机的叙述中，正确的是 （　　） 。（很多同学选D）

A. 三层交换机包括二层交换和三层转发，二层交换由硬件实现，三层转发采用软件实现

B. 三层交换机仅实现三层转发功能

C. 通常路由器用在单位内部，三层交换机放置在出口

D. 三层交换机除了存储转发外，还可以采用直通交换技术

答：A。七层协议里，1、2层是硬件、3+层是软件实现的。三层交换机不仅可以实现二层交换功能，还能实现三层路由功能。路由器一般用在出口，三层交换机用在单位内部。三层交换机不采用直通交换技术。

三层交换机结合了二层交换机的高速数据转发能力和路由器的复杂网络功能，如IP路由、VLAN（虚拟局域网）支持等。

直通交换技术（Cut-Through Switching）是一种交换机处理数据包的方式。在这种模式下，交换机在接收到数据帧的源和目的MAC地址后，立即开始转发数据帧，而不需要等待整个数据帧的接收完成。这样做可以减少数据帧的传输延迟，提高交换机的转发效率。但是，直通交换技术也有其局限性，主要是在处理错误数据包时可能会引入一些问题，因为它没有对数据包进行完整的检查。

三层交换机在处理数据包时，除了考虑MAC地址之外，还需要考虑IP地址和相关的路由协议。这是因为三层交换机工作在OSI模型的第三层，即网络层，需要处理跨网络的数据传输。三层交换机通常使用一种称为"IP路由"的技术来转发数据包，这需要对数据包进行更深层次的检查，包括检查IP地址和相关的协议信息。

在实际应用中，三层交换机可以采用类似于直通交换技术的方法来提高转发效率，但这通常被称为"快速转发"或"硬件转发"。这种方法利用了交换机的专用硬件来加速数据包的处理和转发。

通过这种方式，三层交换机可以在保持高效转发的同时，也能够处理复杂的网络层功能。因此，虽然三层交换机并不直接采用直通交换技术，但它使用了类似的原理，并通过硬件优化来实现快速、准确的数据包转发。

## 二、简答题

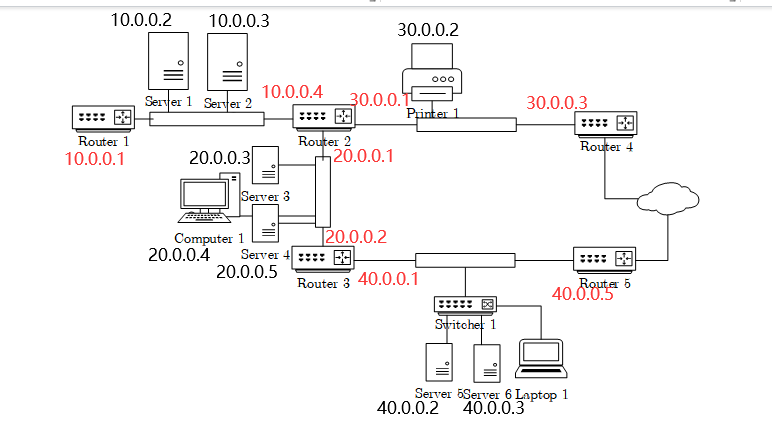
1. 请画出图10‑1 (a)所有路由器设备的路由表，其IP配置如图(b)所示。标明：目的地、网络掩码、下一跳。



(a) 网络架构图

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device** | **IP** | **Device** | **IP** | **Device** | **IP** |
| Router 1 | 10.0.0.1 | Server 1 | 10.0.0.2 | Net 1 | 10.0.0.0/8 |
| Router 2 | 10.0.0.4, 20.0.0.1, 30.0.0.1 | Server 2 | 10.0.0.3 | Net 2 | 20.0.0.0/8 |
| Server 3 | 20.0.0.3 | Net 3 | 30.0.0.0/8 |
| Server 4 | 20.0.0.5 | Net 4 | 40.0.0.0/8 |
| Router 3 | 20.0.0.2, 40.0.0.1 | Server 5 | 40.0.0.2 | Laptop 1 | 40.0.0.4 |
| Server 6 | 40.0.0.3 |  |  |
| Router 4 | 30.0.0.3 | Computer 1 | 20.0.0.4 |  |  |
| Router 5 | 40.0.0.5 | Printer 1 | 30.0.0.2 |  |  |

(b) 设备与IP地址对照表

图10‑1 网络架构图

答：

R1：

目的地 掩码 下一站

10.0.0.0 255.0.0.0 直接传递

20.0.0.0 255.0.0.0 10.0.0.4

30.0.0.0 255.0.0.0 10.0.0.4

40.0.0.0 255.0.0.0 10.0.0.4

R2：

目的 地掩码 下一站

10.0.0.0 255.0.0.0 直接传递

20.0.0.0 255.0.0.0 直接传递

30.0.0.0 255.0.0.0 直接传递

40.0.0.0 255.0.0.0 20.0.0.2

R3：

目的 地掩码 下一站

20.0.0.0 255.0.0.0 直接传递

40.0.0.0 255.0.0.0 直接传递

10.0.0.0 255.0.0.0 20.0.0.1

30.0.0.0 255.0.0.0 20.0.0.1

R4：

目的地 掩码 下一站

30.0.0.0 255.0.0.0 直接传递

10.0.0.0 255.0.0.0 30.0.0.1

20.0.0.0 255.0.0.0 30.0.0.1

40.0.0.0 255.0.0.0 30.0.0.1

R5：

目的地 掩码 下一站

40.0.0.0 255.0.0.0 直接传递

10.0.0.0 255.0.0.0 40.0.0.1

20.0.0.0 255.0.0.0 40.0.0.1

40.0.0.0 255.0.0.0 40.0.0.1

1. 如图10‑2 (a)所示，从C1向C5发送一个IP报文（报文总长24KB），其中MTU如图(b)所示。请写出此IP报文经N1、N2、N3、N4、N5，在R6处每个分片的大小及其偏移量。（提示：IP报头为20B。）



**(a) 网络拓扑图**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Net** | **Type** | **MTU** | **Net** | **Type** | **MTU** | **Net** | **Type** | **MTU** |
| N1 | FDDI | 4325B | N2 | 802.11n | 2346B | N3 | Ethernet | 1500B |
| N4 | TokenRing | 4464B | N5 | 802.11n | 2346B |  |  |  |

**(b) 网络号、类型、MTU对照关系**

图10‑2 网络结构示意图

答：(1480,0), (840,185), (1480, 290), (504, 475), (1480,538), (840,723), (1480,828), (504,1013), (1480,1076), (840,1261), (1480,1366), (504,1366), (1480,1614), (840,1799), (1480,1904), (504,2089), (1480,2152), (840,2337), (1480,2442), (504,2627), (1480,2690), (840,2875), (716,2980)。

规律为：共23分片，设第分片的头部长度为、数据长度为、偏移量为，单位为字节。则：，

，。

解答：报文头部20B，报文数据24556B。

在第N1处，按20B+4304B划分。(大小,偏移)为(4304,0), (4304,538), (4304,1076), (4304,1614), (4304,2152), (3036,2690)。

在第N2处，按20B+2320B划分。(大小,偏移)为(2320,0), (1984, 290), (2320,538), (1984,828), (2320,1076), (1984,1366), (2320,1614), (1984,1904), (2320,2152), (1984,2442), (2320,2690), (716,2980)。

在第N3处，按20B+1480B划分。(大小,偏移)为(1480,0), (840,185), (1480, 290), (504, 475), (1480,538), (840,723), (1480,828), (504,1013), (1480,1076), (840,1261), (1480,1366), (504,1366), (1480,1614), (840,1799), (1480,1904), (504,2089), (1480,2152), (840,2337), (1480,2442), (504,2627), (1480,2690), (840,2875), (716,2980)。

在N4、N5处，同N3的情况。

# **第11课 ICMP、ARP和支撑协议**

## 一、单项选择题

1. PING command can （　　） .

A. manipulates network routing tables

B. trace route to a remote host

C. test if a host is reachable across an IP network

D. displays and modifies the IP-to-physical address translation tables

答：C。

1. PING command uses （　　） .

A. TCP B. UDP C. raw IP D. IGMP

答：C。

1. Pinging （　　） with all packets received successfully CANNOT tell the network interface card (NIC) is working properly.

A.0.0.0.0 B. 59.77.7.25 C. 127.0.0.1 D. 192.168.1.1

答：C。

A. 0.0.0.0：通常表示无效地址或默认路由，无法作为有效 Ping 目标，与网卡无关。

B. 59.77.7.25 和 D. 192.168.1.1：均为实际网络中的地址（公网或局域网）。若能 Ping 通，表明网卡能正常收发数据，可间接验证其功能。

选项 C（127.0.0.1） 是本地环回地址（Loopback Address），用于测试主机自身的网络协议栈。Ping 127.0.0.1 仅验证本地 TCP/IP 协议栈是否正常，数据包不会经过物理网卡（NIC）。即使网卡损坏或未启用，只要系统协议栈正常，Ping 仍会成功。

1. When you execute the command line "ping （　　） " with all packets received successfully, network interface card (NIC) may NOT work.

A. 127.0.0.1 B. 0.0.0.0 C. 8.8.8.8 D. 255.255.255.255

答：A。

1. 0.0.0.0：该地址通常表示默认路由或无效地址，无法作为有效 Ping 目标。多数系统会直接报错，与网卡状态无关。
2. 8.8.8.8：这是 Google 的公共 DNS 服务器地址（公网 IP）。若 Ping 成功，表明网卡能够通过物理链路收发数据包，说明网卡工作正常。
3. 255.255.255.255：这是广播地址，用于向本地网络所有设备发送数据。若 Ping 成功，说明网卡至少能发送广播包，但可能因系统限制或安全策略无法正常响应。
4. （　　） forms a conceptual boundary in the protocol stack. Layers above it are realized by software, while layers below it are mainly related to hardware.

A. Internet B. ICMP C. ARP D. DHCP

答：C。

A. Internet网络层（IP协议）负责逻辑寻址和路由，完全由软件实现，属于分界线的上层，并非边界本身。 B. ICMP属于网络层的辅助协议（如Ping工具），仍处于软件层次，与硬件无关。 C. 在TCP/IP模型中，数据链路层（网络接口层） 负责将网络层（Internet层）的数据包封装成帧，并通过物理介质传输。这一层包含 ARP，其作用是将IP地址解析为对应的MAC地址。关键分界点：ARP位于数据链路层，是软件与硬件的交互点。上层（网络层及以上）：完全由软件实现（如IP协议、TCP/UDP）。下层（物理层）：涉及硬件设备（如网卡、电缆）和驱动程序的物理传输。D. DHCP应用层协议，完全由软件实现，与硬件无关。

1. An ARP message is placed in the （　　） area.

A. frame payload B. IP payload C. IP options D. TCP data

答：A。

1. A traceroute application sends a series of （　　） messages with TTL set to 1, 2, 3, etc.

A. Echo Request B. Echo Reply C. Time Exceeded D. Redirect

答：A。

1. An IP Ping utilizes which ICMP control message?

A. Redirect B. Source quench C. Dest. Unreachable D. Echo Request

答：D。

1. FTP protocol is uses （　　） .

A. TCP B. UDP C. raw IP D. ICMP

答：A。

1. ICMP protocol:

A. stands for International Commission on Missing Persons

B. stands for Internal Critical Monitoring Problem

C. uses TCP as transport protocol

D. is used by routers to inform hosts about unexpected events

答：D。

1. In error reporting the encapsulated ICMP packet goes to （　　）

A. the sender B. the receiver C. a router D. any of the above

答：A。

1. 在 Windows中运行route print命令后得到某主机的路由信息如下图所示。则该主机的IP地址为 （　　） ，子网掩码为 （　　） ，默认网关为 （　　） 。

|  |
| --- |
| Active Routes:  Network Destination Netmask Gateway Interface Metric  0.0.0.0 0.0.0.0 114.220.115.254 114.220.115.254 20  127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1  114.220.115.128 255.255.255.128 114.220.115.132 114.220.115.132 20  114.220.115.132 255.255.255.255 127.0.0.1 127.0.0.1 20  114.220.115.255 255.255.255.255 114.220.115.132 114.220.115.132 20  224.0.0.0 224.0.0.0 114.220.115.132 114.220.115.132 20  255.255.255.255 255.255.255.255 114.220.115.132 114.220.115.132 1  255.255.255.255 255.255.255.255 114.220.115.132 2 1  Default Gateway: 114.220.115.254 |

问题1

A. 114.220.115.132 B. 114.220.115.254

C. 127.0.0.1 D. 224.0.0.1

主机的IP地址应该是在接口列中出现，并且属于本地子网的条目。通常，主机在路由表中会有一个指向本地子网的路由，其接口地址就是主机的IP地址。例如，在条目3中，网络目标114.220.115.128/25的网关是114.220.115.132，接口也是这个地址。这说明主机在这个子网中的IP地址是114.220.115.132，因为它作为接口地址来处理该子网的数据包。

1. 问题2
2. 255.0.0.0 B. 255.255.255.0 C. 255.255.255.128 D. 255.255.255.255

子网掩码是255.255.255.128，也就是25位掩码。这个掩码对应的子网是114.220.115.128到114.220.115.255，但其中网络地址是114.220.115.128，广播地址是114.220.115.255。因此，主机的IP地址114.220.115.132属于这个子网，子网掩码是255.255.255.128。

1. 问题3

A. 114.220.115.132 B. 114.220.115.254

C. 127.0.0.1 D. 224.0.0.1

答：A；C；B。

默认网关已经明确给出是114.220.115.254。子网范围是128到255（包括网络地址和广播地址）。因此，网关地址114.220.115.254确实在这个子网内，所以是有效的。

1. IPv4 address exhaustion is one of the motivation of IPv6, （　　） and （　　） overcomes such shortage and extends the life of IPv4.

A. CIDR; NAT B. CDMA; CSMA C. ICMP; ARP D. DHCP; DNS

答：A。

1. Ping command utilizes （　　） ICMP control message.

A. echo request B. echo reply C. time exceeded D. redirect

答：A和B。Ping用于测试网络连通性，其核心机制依赖于 ICMP（Internet Control Message Protocol） 的两种消息：Echo Request（类型 8，代码 0）：由源主机主动发送至目标主机，探测其可达性。Echo Reply（类型 0，代码 0）：目标主机收到Echo Request后返回的响应。

1. The DHCP protocol uses （　　） to send messages.

A. TCP B. UDP C. raw IP D. ICMP

答：B。

1. The ping command uses ICMP to send （　　） message.

A. dest. unreachable B. echo C. redirect D. time exceeded

答：B。

1. We are assigned only one IP 210.34.0.2, but we can use （　　） to enable 3 devices to share the Internet connection.

A. NAT B. DHCP C. DNS D. ARP

答：A。

1. Which of the following statements about ICMP is NOT TRUE?

A. It contains message to report error and information.

B. It encapsulates messages in IP for transmission, and IP uses it to report problems.

C. If a datagram carrying ICMP error message causes an error, an error message is sent.

D. PING uses ICMP to carry echo messages.

答：C。

1. ICMP的核心功能是报告错误和传递控制信息（如目的不可达、超时、回显请求/应答等）。例如，Ping工具依赖的Echo Request/Reply即属于信息类消息。
2. ICMP报文确实封装在IP数据包中传输。IP层在处理数据包时若遇到问题（如无法到达目标），会通过ICMP生成错误消息（如Destination Unreachable）。
3. 若携带ICMP错误消息的数据包本身出错，不会生成新的错误消息。这是为了防止错误消息的无限循环。例如，若一个ICMP Destination Unreachable消息在传输中出错，接收方不会针对此错误再发送另一个ICMP消息。
4. Ping工具通过发送ICMP Echo Request（类型8）并接收ICMP Echo Reply（类型0）来测试网络连通性，完全依赖ICMP协议。
5. Which of the following technologies is NOT used in ARP?

A. Broadcast. B. Cache. C. Look-up table. D. Forward.

答：D。

1. Which protocol translates IP address to a hardware address?

A. DHCP B. NAT C. ARP D. HTTP

答：C。

1. ICMP差错报告报文格式中，除了类型、代码和校验和外，还需加上 （　　） 。

A. 时间戳以表明发出的时间

B. 出错报文的前64比特以便源主机定位出错报文

C. 子网掩码以确定所在局域网

D. 回声请求与响应以判定路径是否畅通

答：B。

ICMP主要分为差错报文和控制报文。我们使用type来code两个标志来确定一个具体的错误。因为需要指出具体是哪个主机上的哪个程序发出的信息没有到达。因此，每一个ICMP的错误消息，应该包含：

1. 具体的错误类型（Type/code 决定）

2. 引发ICMP错误消息的数据包的完全IP包头（哪个主机的数据）

3. 数据报的前8个字节----UDP报头或者TCP中的port部分（主机上的哪个程序）

1. 某客户端可以ping通同一网段内的部分计算机，原因可能是 （　　） 。

A. 本机TCP/IP协议不能正常工作 B. 本机DNS服务器地址设置错误

C. 本机网络接口故障 D. 网络中存在访问过滤

答：D。主机能PING通同一网络的部分主机，说明TCP/IP协议能正常工作，接口也没有故障，综合四个选择最有可能是的网络中存在过滤规则。

1. （　　） 属于第三层VPN协议。

A. TCP B. IPsec C. PPPOE D. SSL

答：B。

1. 以下关于DHCP服务的说法中，正确的是 （　　） 。

A.在一个园区网中可以存在多台DHCP服务器

B.默认情况下，客户端要使用DHCP服务需指定DHCP服务器地址

C.默认情况下，客户端选择DHCP服务器所在网段的IP地址作为本地地址

D.在DHCP服务器上，只能使用同一网段的地址作为地址池

答：A。DHCP服务可以服务于一个网段，也可以通过DHCP中继服务多个子网，所以C和D选项有误。因为客户端要自动获取IP，此时并不知道DHCP服务器在哪，所以B选项有误。在一个网段中可以配置多台DHCP服务器，答案选A。

1. DHCP客户端通过 （　　） 方式发送DHCP discover消息。

A. 单播 B. 广播 C. 组播 D. 任意播

答：B。当DHCP客户机第一次登录网络的时候（也就是客户机上没有任何IP地址数据时），它会通过UDP 67端口向网络上发出一个DHCPDISCOVER数据包（包中包含客户机的MAC地址和计算机名等信息）。因为客户机还不知道自己属于哪一个网络，所以封包的源地址为0. 0. 0. 0，目标地址为255. 255. 255. 255，然后再附上DHCP discover的信息，向网络进行广播。

1. RARP协议的作用是 （　　） 。

A. 根据MAC查IP B. 根据IP查MAC

C. 根据域名查IP D. 查找域内授权域名服务器

答：A。

1. ARP 协议数据单元封装在 （　　） 中传送。

A. IP 分组 B. 以太帧 C. TCP 段 D. ICMP报文

答：B。

1. 使用traceroute命令测试网络时可以 （　　） 。

A.检验链路协议是否运行正常 B.检验目标网络是否在路由表中

C.查看域名解析服务

D.显示分组到达目标路径上经过的各个路由器

答：D。

1. 若主机hostA的MAC地址为aa-aa-aa-aa-aa-aa，主机hostB的MAC地址为bb-bb-bb-bb-bb-bb。由hostA发出的查询hostB的MAC地址的帧格式如下图所示，则此帧中的目标MAC地址为 （　　） ，ARP报文中的目标MAC地址为 （　　） 。

【目标MAC | 源MAC | 协议类型 | ARP报文 | CRC】

A. aa-aa-aa-aa-aa-aa B. bb-bb-bb-bb-bb-bb

C. 00-00-00-00-00-00 D. ff-ff-ff-ff-ff-ff

答：D，C。当主机A向本局域网内的主机B发送IP数据报的时候，就会先查找自己的ARP映射表，查看是否有主机B的IP地址，如有的话，就继续查找出其对应的硬件地址，在把这个硬件地址写入MAC帧中，然后通过局域网发往这个硬件地址。也有可能找到不到主机B的IP地址项目，在这种情况下，主机A就要运行ARP协议，广播ARP请求分组，去请求主机B的MAC。

1. 虽然IPv4地址已经告罄，为何IPv6在短时间内无法取代？

A. IPv6不兼容IPv4，更新系统需要花费大量的成本；

B. 无分类地址、DHCP和NAT等技术提高IPv4地址利用率，延续了IPv4的生命；

C. Windows操作系统不能很好地支持IPv6；

D. 更好的协议IPv9已经在部署中。

答：A.不完全兼容。B。NAT（网络地址转换）：允许多台设备共享一个公网IPv4地址，极大缓解地址短缺问题。CIDR（无类别域间路由）：通过可变长子网掩码灵活分配地址块，减少地址浪费。DHCP动态分配：按需分配IP地址，提高地址利用率

C.现代操作系统（包括Windows）已全面支持IPv6。D.目前IPv9并未实际部署。

DDD现代操作系统（包括Windows）已全面支持IPv6。

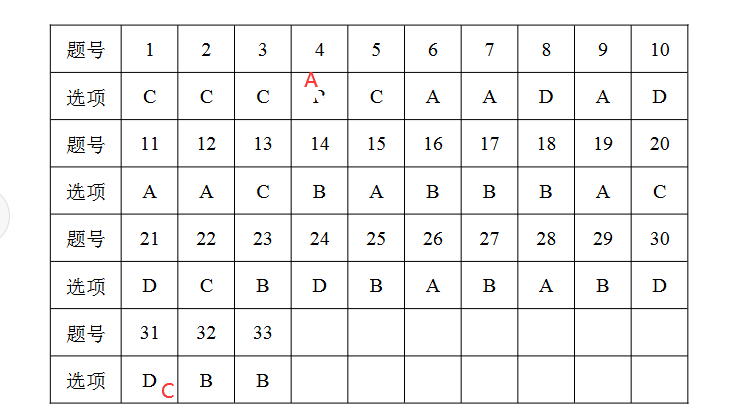
1. 下列说法正确的是：

A. DHCP服务器安装在路由器上；

B. 通过NAPT内网搭建网络服务器，可以映射到外网IP地址和端口，对外网提供服务；

C. 向DHCP服务器请求IP地址时，仅能在局域网内；

D. DHCP是网络层协议。

答：B。 

## 二、简答题

1. 请简要说明TraceRoute和PING的原理。

答： **Traceroute**用于追踪数据包从源设备到目标设备所经过的网络路径。TraceRoute利用ICMP及IP头部的TTL（Time To Live）域得到一连串数据包路径。首先，TraceRoute送出一个TTL是1的IP报文到目的地。该路径上的第一个路由器收到该报文，将TTL减1。此时TTL变为0，该路由器便将此报文丢掉，并送回一个“ICMP time exceeded”超时消息，主机收到该消息后，便知道该路由器存在于该路径上。接着TraceRoute再送出另一个TTL是2的数据报，发现第2个路由器……TraceRoute每次将送出的报文的TTL加1来发现另一个路由器，重复此过程，直到数据包到达目标设备或达到最大跳数（通常为 30 跳），返回“ICMP Echo Reply”。

Ping用ICMP回应请求和回应应答报文来实现。当调用Ping程序时，它发送一个包含ICMP回应请求的报文给目的地，然后等待一段很短的时间。如果没有收到应答，则重新传送请求。如果重传的请求仍没有收到应答（或收到ICMP目的不可达报文），Ping声称该远程机器为不可达。远端主机上的ICMP软件应答该回应请求报文。按照协议只要收到回应请求，ICMP软件必须发送回应应答。

1. 考虑如何利用ICMP协议对一个网络上的时延性能进行监控？

答： ICMP时间戳请求和应答消息都包含初始、接收和传送时间戳。产生ICMP时间戳请求的主机可以使用这三个时间戳估算远程主机的本地时间。往返时间，它的值是收到回答时的时间值减去发送请求时的时间值。

1. 学院的实验楼有上百台主机，而可分配的外网IP地址数量远远不足。

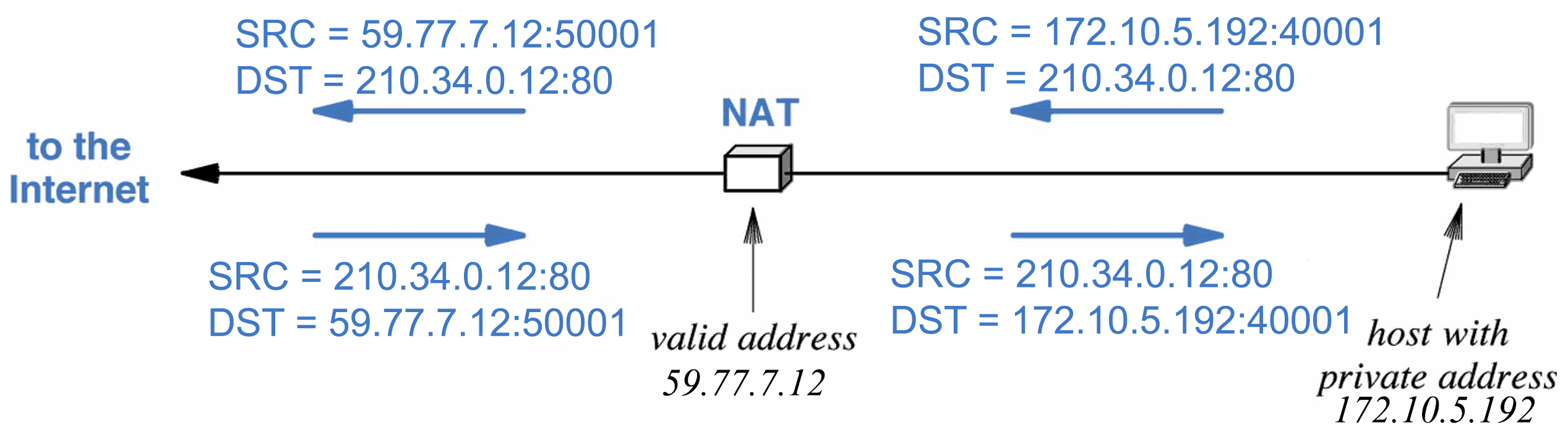
（1） 如何使这些主机连接到Internet？并通过图示说明机房某台主机（IP地址为172.10.5.192，子网掩码为255.255.255.0，在搜索引擎查询“ip”得到59.77.7.12）访问厦大网站（210.34.0.12）时的MAC地址、IP地址和端口号转换过程。

（2） 实验楼主机是否能通过ARP询问厦大网站的MAC地址？并说明原因。

（3） 当主机172.10.5.192（MAC地址：d0:76:e7:10:2f:1d）询问172.10.5.129（MAC地址：d0:76:e7:93:6a:52）对应的MAC地址时，应如何填写其以太网帧的源地址与目的地址？主机172.10.5.129应答时，如何应填写以太网帧的源地址与目的地址？

答：

（1）通过NAT或NATP技术，可使同一站点的多台计算机能共享一个全球有效的IP地址。



（2）不可以。ARP报文不会被路由器转发，而且查询不同局域网络中的MAC地址是没有意义的。

（3）源地址：d0:76:e7:10:2f:1d，目的地址：ff:ff:ff:ff:ff:ff；源地址：d0:76:e7:93:6a:52，目的地址：d0:76:e7:10:2f:1d。

1. 什么是ARP缓存？ARP如何使用其缓存？

答：局域网各主机和路由器的IP 地址到硬件地址的映射表。

当主机A欲向本局域网上的某个主机B发送IP数据报时，就先在其ARP高速缓存中查看有无主机B的IP地址。如有，就可查出其对应的硬件地址，再将此硬件地址写入MAC帧，然后通过局域网将该MAC帧发往此硬件地址。

为了减少网络上的通信量，主机A在发送其ARP请求分组时，就将其IP地址到硬件地址的映射写入ARP请求分组。

当主机B收到A的ARP请求分组时，就将主机A的这一地址映射写入主机B自己的ARP高速缓存中。

1. 某网络拓扑如下图所示，其中路由器内网接口、DHCP服务器、WWW服务器与主机1均采用静态IP地址配置，相关地址信息见图中标注；主机2～主机N通过DHCP服务器动态获取IP地址等配置信息。请回答下列问题：



（1）DHCP服务器可为主机2～主机N动态分配IP地址的最大范围是什么？主机2使用DHCP协议获取IP地址的过程中，发送的封装DHCP Discover报文的IP分组的源IP地址和目的IP地址分别是什么？

（2）若主机2的ARP表为空，则该主机访问Internet时，发出的第一个以太网帧的目的MAC地址是什么？封装主机2发往Internet的IP分组的以太网帧的目的MAC地址是什么？

（3）若主机1的子网掩码和默认网关分别配置为255.255.255.0和111.123.15.2，则该主机是否能访问WWW服务器？是否能访问Internet？请说明理由。

答：（1）子网为 111.123.15.0/24（掩码 255.255.255.0），可用地址为111.123.15.5/24—111.123.15.254/24；客户端（主机2）在未获取IP地址前，发送的DHCP Discover报文为广播报文，0.0.0.0（表示未分配IP）；255.255.255.255；（2）主机2的ARP表为空，需通过ARP协议获取默认网关（路由器内网接口 111.123.15.1）的MAC地址。FF-FF-FF-FF-FF-FF（广播）；主机2访问Internet时，所有外网流量需通过默认网关（111.123.15.1）转发。00-A1-A1-A1-A1-A1（默认网关的MAC地址）；（3）能，同一子网内；当主机1尝试访问Internet时，会向 111.123.15.2 发送数据包，但该地址对应的设备（DHCP服务器）无路由功能，导致流量无法转发到外网。不能，默认网关错误。

1. 某单位在内部局域网采用Windows Server 2008R2配置DHCP服务器。可动态分配的IP地址范围是192.168.81.10~192.168.81.100和192.168.81.110~ 192.168.81.240；DNS 服务器的IP地址固定为192.168.81.2。

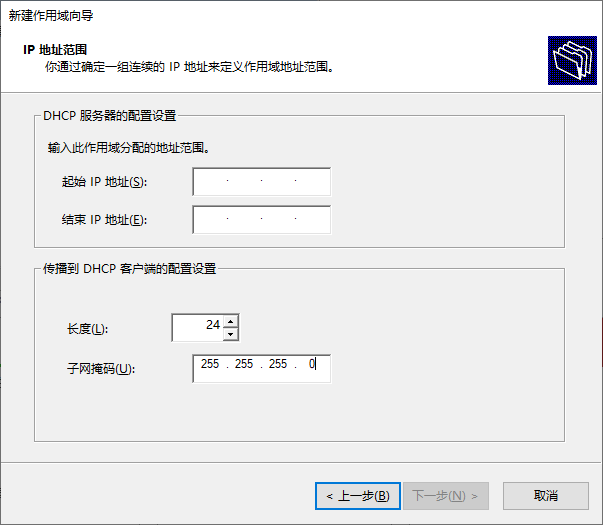
【问题1】在DHCP工作原理中，DHCP客户端第一次登录网络时向网络发出一个（1）广 播包；DHCP服务器从未租出的地址范围内选择IP地址，连同其他TCP/IP参数回复给客户端一个（2）包；DHCP客户端根据最先抵达的回应，向网络发送一个（3）包，告知所有DHCP服务器它将指定接收哪一台服务器提供的IP地址，当DHCP服务器接收到客户端的回应之后，会给客户端发出一个（4）包，以确认IP租约正式生效。

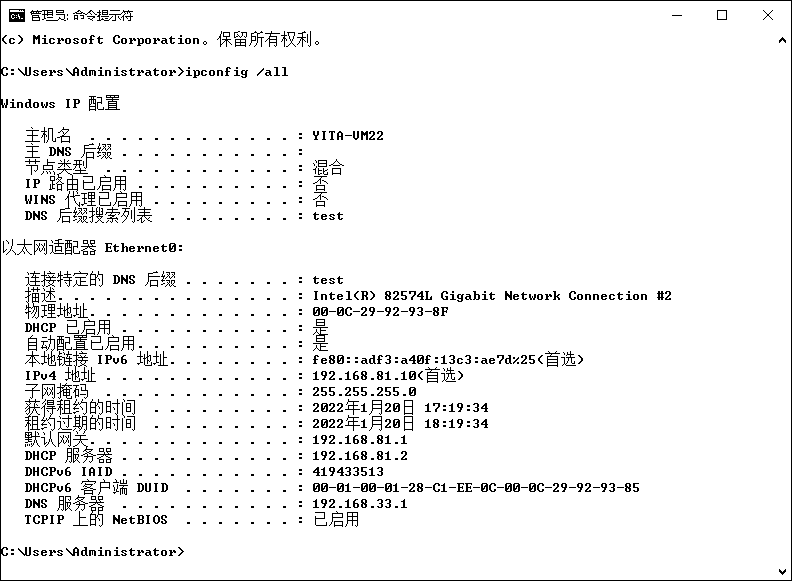
（1）~（4）备选答案：

A. Dhcpdiscover B. Dhcpoffer C. Dhcprequest D. Dhcpack

【问题2】DHCP服务器具有三种IP地址分配方式：第一种是手动分配，即由管理员为少数特定客户端静态绑定固定的IP地址；第二种是（5），即为客户端分配租期为无限长的 IP地址；第三种是（6），即为客户端分配一定有效期限的IP地址，到达使用期限后，客户端需要重新申请IP地址。

【问题3】在Windows Server 2022上配置DHCP服务，图2-1所示配置IP地址范围时“起始IP地址”处应填（7），“结束IP地址”处应填（8）；图2-2所示添加排除和延迟时“起始IP地址”处应填（9），“结束IP地址”处应填（10）。默认客户端获取的IP地址使用期限为（11）天；图2-3所示的结果中实际配置的租约期限是（12）秒。



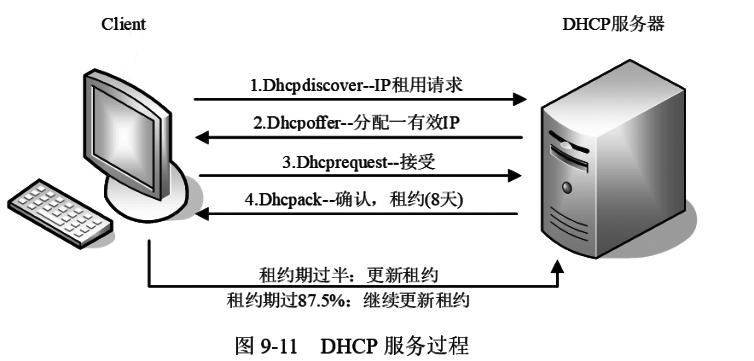
【问题4】通过创建DHCP的IP保留功能，使静态IP地址的设备管理自动化。如果正在为新的客户端保留IP地址，或者正在保留一个不同于当前地址的新IP地址，应验证DHCP 服务器是否租出该地址。如果地址已被租出，在该地址的客户端的命令提示符下键入 ipconfig/（13）命令来释放它；DHCP服务器为客户端保留IP地址后，客户端需在命令提示符下键入ipconfig/（14）命令重新向DHCP服务器申请地址租约。使用ipconfig/（15）命令可查看当前地址租约等全部信息。

（13）~（15）备选答案：

A. all B. renew C. release D. setclassid

答：（1）A；（2）B；（3）C；（4）D；（5）自动分配；（6）动态分配；（7）192.168.81.10；（8）192.168.81.240；（9）192.168.81.101；（10）192.168.81.109；（11）8；（12）3600；（13）C；（14）B；（15）A。

【问题一】DHCP服务器过程如下：



文字解析过程如下：

①DHCP Client以广播的方式发出DHCP Discover报文。

②所有的 Server都能够接收到Client发送的DHCP Discover 报文，并向Client发送一个DHCP Offer报文（并带上可用IP地址）。

③ Client接收并处理最先收到的DHCP Offer报文。并广播一个DHCP Request报文（告知所有DHCP服务器它选择谁分配的IP）。

④Server都会收到DHCP Request报文，但只有选择了它的这个服务器会响应处理。向Client响应一个 DHCP ACK报文，并在选项字段中增加IP地址的租期信息。

⑤ Client收到DHCP ACK报文后，检查DHCP Server分配的IP地址是否能够使用。

如果可以使用，则 Client 成功获得IP地址并根据IP地址使用租期自动启动续延过程;

如果DHCP Client 发现分配的IP地址已经被使用，则向Server 发出DHCP Decline报文，通知Server禁用这个IP地址，然后Client开始新的地址申请过程。

因此可得第一问答案为：ABCD

【问题2】

主机上的IP地址可通过三种方式分配：

①手工分配：由管理员为客户机分配一个静态固定的IP地址。

②自动分配：由DHCP服务器为客户机分配一个永久的IP地址（如在DHCP服务器中设置静态绑定）。

③动态分配：由DHCP服务器，为客户机动态分配一个带一定有租约IP地址，客户机使用完毕后予以回收。

【问题3】

根据题目说明，在DHCP服务器上可动态分配的IP地址范围为：192.168.81.10~ 192.168.81.100和192.168.81.110~ 192.168.81.240。

因此第7空的起始地址为：192.168.81.10，第8空结束地址为：192.168.81.240。

另外要添加地址排除，以排除不能分配的IP地址范围，排除的起始地址第九空为：192.168.81.101，结束地址第十空为：192.168.81.109。

Windows Server 2008 R2配置DHCP服务器时，默认的租约为8天（第11空），租约可改，所以根据图2-3所示我们可知（根据获得租约的时间和租约过期的时间判断），实际租约为1小时，即3600秒（第12空）。

【问题4】

ipconfig是计算机网络的常用命令。结合参数，可查看很多网络参数信息，例如：

ipconfig /all：显示本机TCP/IP配置的详细信息，DHCP分配完成后，我们可以通过这个命令来查看客户主机获得的IP地址、子网掩码、DNS地址、网关地址、租约等相关信息。

ipconfig /release：DHCP 客户端手工释放IP地址；如果要手工释放某个IP可采用这个命令。

ipconfig /renew： DHCP客户端手工向服务器刷新请求；如果要刷新租约信息，可用这个命令实现主动刷新。

而ipconfig /setclassid：主要用于设置网络适配器的DHCP类别。

因此答案为CBA。

# 第12课 传输层：UDP和TCP协议

## 一、单项选择题

1. Which can be a source address in the header in IPv6 datagram?

A. 00:50:56:C0:00:01 B. 2002::87e5:c3dd

C. 7.0.0.3 D. 8080

答：B。

1. Which of the following address uniquely identifies a running application program?

A. MAC address B. IP address C. port number D. host name

答：C。

1. Which does NOT exist in the UDP header?

A. Source port B. Destination port C. Checksum D. ACK Number

答：D。

UDP头部包含以下字段（总长度8字节）：Source Port（源端口，2字节）：标识发送方端口。Destination Port（目的端口，2字节）：标识接收方端口。Length（长度，2字节）：指示UDP报文总长度（头部+数据）。Checksum（校验和，2字节）：用于验证数据完整性（IPv4中可选，IPv6中强制启用）。

ACK Number是TCP头部的一部分，用于实现可靠传输，确保数据按序到达。UDP不保证数据可靠传输，因此无需序列号、确认号等字段。

1. Which can be a source address in the UDP header?

A. C4-19-87-15-C1-8A B. 192.168.1.3 C. 8080 D. 80800

答：C。

1. C4-19-87-15-C1-8A。MAC地址属于数据链路层（如以太网），与UDP无关。UDP头部不包含硬件地址。
2. 192.168.1.3。IP地址属于网络层（IP头部），UDP头部不涉及IP地址。
3. 8080端口号是UDP头部的核心字段，源端口和目的端口均为16位整数（范围：0-65535）。8080是合法端口号，符合UDP头部定义。

D. 80800端口号最大值为65535（2^16 -1），80800超出范围，非法。

1. Which is a client port number?

A. 80 B. 8080 C. 20101 D. 65530

答：D。

端口号的范围是从0到65535。知名端口（Well-Known Ports）：范围从0到1023，这些端口号被IANA（互联网号码分配局）分配给了特定的服务和应用程序。例如：80端口：HTTP服务，443端口：HTTPS服务，21端口：FTP控制连接，22端口：SSH服务，23端口：Telnet服务

注册端口（Registered Ports）：范围从1024到49151，这些端口号可以由用户或组织向IANA申请，用于特定的服务或应用程序。

动态或私有端口（Dynamic or Private Ports）：范围从49152到65535，这些端口号通常不分配给固定的服务，而是由各个应用程序在运行时动态选择。客户端在与服务器建立连接时，通常会使用这些端口号作为源端口。

1. The field （　　） does NOT exist in both TCP and UDP headers.

A. Source Port B. Destination Port C. Checksum D. Header Length

答：D。

1. The field （　　） exists in both IP and TCP headers.

A. version B. window C. total length D. header length

答：D。

1. version：此字段存在于IP头部中，用于指示IP协议的版本（IPv4或IPv6）。
2. window：此字段仅存在于TCP头部中，用于流量控制，指示接收窗口的大小。
3. 总长度在IP首部有，在TCP首部没有。
4. The field （　　） exists in both TCP and IP headers.

A. Fragment offset B. Window

C. Header length D. Checksum

答：C。

A.片偏移在IP头部才有。 B.window：此字段仅存在于TCP头部中，用于流量控制，指示接收窗口的大小。 D.TCP头部才有校验和

1. TCP DOES NOT guarantee that the data sent across a connection will be （　　） .

A. delivered exactly as sent B. delivered completely

C. delivered in same size pieces D. delivered in order

答：C。

1. TCP works on the （　　） layer of the OSI module.

A. data link B. network C. transport D. application

答：C。

1. TCP works on the （　　） layer of the TCP/IP protocol suite.

A. network interface B. physical

C. transport D. application

答：C。

1. The （　　） uses both TCP and UDP to send messages.

A. DHCP B. DNS C. FTP D. ICMP

答：B。

1. Which statement DOES NOT characterize the transport layer protocols?

A. TCP and UDP port numbers are used by application layer protocols.

B. TCP uses port numbers to provide reliable transportation of IP packets.

C. TCP uses windowing and sequencing to provide reliable transfer of data.

D. TCP is a connection-oriented protocol. UDP is a connectionless protocol.

答：B。

1. 端口号的作用是 （　　） 。

A. 流量控制 B. 应用层进程寻址 C. 建立连接 D. ACL过滤

答：B。

1. SNMP协议采用UDP提供数据报服务，原因不包括UDP （　　） 。

A. 数据传输效率高 B. 面向连接，没有数据丢失

C. 无需确认，不增加主机重传负担 D. 开销小,不增加网络负载

答：B。

1. 在TCP协议中，用于进行流量控制的字段为 （　　） 。

A. 端口号 B. 序列号 C. 应答编号 D. 窗口

答：D。TCP协议使用可变大小的滑动窗口协议实现流量控制。

1. TCP协议中，URG指针的作用是 （　　） 。

A.表明TCP段中有带外数据 B.表明数据需要紧急传送

C.表明带外数据在TCP段中的位置 D.表明TCP段的发送方式

答：C。URG指针是指出需要被紧急传送的数据的位置的。当控制位，URG位为1时，URG指针有效。

## 二、简答题

1. 有些需求需要用TCP实现，有些需求则需要UDP实现。请各列举一些应用场景，指出为何需要用这种模式实现。

答：TCP实现：HTTP、FTP、SMTP、POP3等；

UDP实现：DNS、网络校时、IP隧道、远程进程调用、DHCP、TFTP（小文件传输协议）、IPTV、流媒体应用、VoIP、在线游戏、基于实时流协议的协议、广播、路由信息协议。

原因：在一些轻量级的传输，或者允许部分丢包的情况下，可以用UDP节省数据量；在连接过程中需要广播，不具备使用TCP的条件。

1. 请列举TCP段和UDP报文头部格式（不需要按照顺序）。

答：TCP段：源端口、目的端口、序号、确认号、首部长度、保留、标志字段（确认、重置、开始、结束、紧急指针、推送）、选项和填充字节。

UDP报文：源端口、目的端口、数据报长度、校验值。

1. 请简要回答：为什么发送广播不能通过TCP实现？
2. TCP是面向连接的协议，通信前需通过三次握手建立点对点的可靠连接。而广播是一对多的通信方式，要求数据包同时发送给多个不确定的接收方，无法为每个接收方单独建立连接。TCP仅支持单播通信，即一个发送方对应一个接收方。广播要求同一数据包被多个主机接收，TCP的端到端传输机制无法实现多目标同步传输。

# 第16课 客户和服务模式

## 一、单项选择题

1. Which of the following about C/S mode is NOT TRUE?

A. Clients waits for contact from a server.

B. Clients know which server to contact.

C. Clients may stop after interacting.

D. Clients start after the server.

答：A。

A. 错误。客户端不会“等待服务器联系”，而是主动联系服务器。此描述与C/S模式的基本逻辑完全相悖。B. 客户端必须预先知道服务器的地址（IP+端口）才能发起请求（如浏览器需知Web服务器地址）。C. 客户端在完成交互后可能关闭（如关闭浏览器标签）。D. 服务器需先启动并监听，客户端才能后续连接。若服务器未运行，客户端无法通信。

1. The PING command uses \_\_\_ to send messages.

A. TCP B. UDP C. raw IP D. IPv6

答：C。PING（Packet Internet Groper）基于 ICMP（Internet Control Message Protocol） 实现，而ICMP报文直接封装在 IP数据包 中，不依赖传输层协议（如TCP或UDP）。ICMP作为网络层协议，直接通过原始IP数据包（raw IP）传输。

1. TRACEROUTE command uses （　　） to send messages.

A. TCP B. UDP C. raw IP D. None of above.

答：C。TraceRoute命令是追踪数据包从源到目的地经过的路由路的命令。Traceroute使用ICMP协议发送一系列的ICMP报文。因此同上题，使用raw IP。追踪数据包从源到目的地经过的路由路

1. A connection-oriented concurrent server uses \_\_ ports.

A. ephemeral B. well-known C. active D. a and b

答：D。

1. A(n) （　　） address uniquely identifies a running application program.

A. IP B. host C. MAC D. socket

答：D。

1. The （　　） socket is used with a connection-oriented protocol.

A. stream B. datagram C. raw D. remote

答：A。

1. The （　　） socket is used with a connectionless protocol.

A. stream B. datagram C. raw D. default

答：B。

1. The （　　） socket is used with a protocol that directly uses the services of IP.

A. stream B. datagram C. raw D. remote

答：C。

1. Which of the following functions is not used in a message paradigm?

A. socket B. bind C. listen D. send/sendto

答：C。

1. Which of the following socket is used with a protocol that directly uses the services of IP?

A. stream B. datagram C. raw D. remote

答：C。

1. We use （　　） socket with a connection-oriented protocol.

A. stream B. datagram C. raw D. remote

答：A。

## 二、简答题

1. 根据TCP/IP参考模型，归纳写出各层的分层名称、分层传输最小单位的名称、网络设备名、该层主要协议（或标准）、主要协议编址名称和方案、该层其它同类协议、该层主要作用。

答：第5层：应用层，无，七层交换机，HTTP等，无，DNS、POP3等，具体应用服务；第4层：传输层，数据段、数据报，四层交换机，TCP、UDP，端口号，STCP，将网络数据分配到具体的进程；第5层：网络层，数据报，路由器（网关）、三层交换机，IP，IP地址，IPv6，提供统一的网络互联，隐藏底层网络异构的细节；第2层：网络接口层，帧，网桥、交换机，Ethernet，MAC地址，X.25、令牌环、电话网等，网卡竞争、复用传输信道；第1层：物理层，位，中继器、集线器，光，无，电、无线电，位的传输。

1. 请画出流程图说明Socket API在Client-Server模式中的执行模式。注意：分为面向连接和面向无连接的两种情况。

答：Socket接口是应用程序的基本网络接口，由操作系统提供、进程的通信端点。Socket包括一个五元组：协议类型，本地地址，本地端口号，远端地址，远端端口号。Socket-API接口包括：socket()，bind()，listen()，accept()，send()/sendto()，recv()/recvfrom()，close()/closesocket()。

Socket在Client-Server模式中的执行模式主要有两种：面向连接的和无连接的。其中，面向连接的socket过程如下左图，无连接的socket过程如下右图。注意下右图左半部分也可以用下左图的左半部分代替，但须注意此时两种模式下connect函数的作用完全不同

面向连接的：

客户端：

socket() ，创建 TCP Socket。

connect()，向服务器发起连接请求（如 connect(server\_ip:80)）。

send()/recv()，与服务器进行数据传输。

close()，关闭连接。

服务器端：

socket()，创建 TCP 类型的 Socket。

bind()，绑定 Socket 到本地 IP 地址和端口

listen()，设置 Socket 为监听状态，等待客户端连接请求。

accept()，阻塞直到有客户端连接。接受连接后，返回一个新的 Socket 用于与该客户端通信。

send()/recv()，通过新 Socket 与客户端进行可靠的数据传输。

close()，关闭连接，释放资源。

1. 面向连接和面向无连接的两种情况调用Socket API的方式有差异。请说明为何无连接的情况不需要listen（侦听）和accept（接受）的环节？

答：差异在于无连接的情况下服务器端没有侦听和接受环节。因为，listen函数主要目的是为了使套接字变为监听状态，用于监听新来的连接，然后用accept函数获取接受的新连接，而无连接的情况不需要连接建立即直接发送。

1. （思考题）是否所有通信都基于Socket API？如果否，请举反例。

答：网络层绝大部分通信都是基于Socket API的，包括基于TCP、UDP和Raw IP等形式。局域网的通信技术可以不依赖Socket API，例如RS-232通信实验。即便网络层通信，除了Socket API，还有ACE Socket。

# 第18课 电子邮件

## 一、单项选择题

1. An email contains a textual birthday greeting, a picture of a cake, and a song. The order is not important. What is the content-type?

A. multipart/mixed B. multipart/parallel

C. multipart/digest D. multipart/alternative

答：A。

1. 适用于邮件中包含多个独立的部分，且这些部分可能是不同类型的内容（如文本、图片、音频等），彼此之间没有依赖关系，顺序也不重要。题目中的邮件包含文本、图片和歌曲，这些内容彼此独立且需要同时存在。符合A的定义。
2. 适用于邮件中的多个部分需要同时呈现（如文本与内联图片、音频同步展示），但大多数邮件客户端不支持自动并行渲染（如自动播放音频）。
3. 将多封邮件内容聚合为一个邮件（如邮件列表的摘要），每个部分本身是一封完整的邮件。
4. 同一内容提供不同格式的替代版本（如纯文本和HTML版本），客户端选择最合适的一种显示。
5. A client machine powers off at the end of the day. It probably needs （　　） to receive email.

A. only SMTP B. only POP

C. both SMTP and POP D. none of the above

答：B。SMTP（Simple Mail Transfer Protocol）简单邮件传输协议，它的主要功能是用于发送邮件。当用户要将邮件从客户端发送到邮件服务器，或者从一个邮件服务器发送到另一个邮件服务器时，会使用SMTP协议。POP（Post Office Protocol）即邮局协议，目前常用的是POP3版本。POP协议的主要作用是允许客户端从邮件服务器上下载邮件到本地。客户端机器在开机后，可以使用POP协议连接到邮件服务器，将存储在服务器上的邮件下载到本地进行查看。即使客户端机器在一天结束时关机，邮件会先存储在邮件服务器上，当客户端再次开机时，就可以通过POP协议接收邮件，所以仅POP协议就可以满足客户端接收邮件的需求，

1. After Alice deletes unwanted e-mails on the mail server, they will NOT vanish on her client after receiving e-mails using （　　） .

A. POP3 B. IMAP4 C. MIME D. SMTP

答：A。

A.当使用POP3协议从邮件服务器接收邮件时，邮件会从服务器下载到客户端，并且默认情况下，邮件会从服务器上删除（也可以设置为保留在服务器上）。一旦邮件被下载到客户端，客户端和服务器上的邮件状态就相对独立了。即使在服务器上删除了某些邮件，这些邮件在客户端上仍然存在，不会因为服务器上的操作而消失。

B.IMAP4（Internet Message Access Protocol - Version 4）即互联网邮件访问协议第4版，也是用于接收邮件的协议。与POP3不同，当在服务器上删除邮件时，客户端会收到相应的更新通知，客户端上对应的邮件也会被删除。

C.MIME（Multipurpose Internet Mail Extensions）即多用途互联网邮件扩展，它并不是一种邮件接收或发送协议，而是对邮件内容格式的一种扩展标准。

D.用于发送邮件的协议。

1. An POP3 server uses port number （　　） by default.

A. 25 B. 80 C. 110 D. 143

答：C。

1. During an e-mail is received from the server, （　　） is NOT engaged.

A. DNS B. IP C. POP3/IMAP4 D. SMTP

答：D。

1. MIME allows （　　） data to be sent through SMTP.

A. audio B. non-ASCII data C. image D. all of the above

答：D。

1. SMTP can be characteristized as:

A. SMTP supports both text and binary messages.

B. A user sends only one copy of a given message if it has multiple recipients.

C. SMTP follows a datagram paradigm.

D. SMTP must be used when the client receives mails.

答：B。

1. When an e-mail is deleted from the ISP, which is NOT engaged?

A. SMTP B. POP/IMAP C. DNS D. IP

答：A。

1. When an e-mail is sent, which is NOT engaged?

A. SMTP B. POP C. DNS D. MTA

答：B。

1. When you receive an e-mail from the server, （　　） is NOT engaged.

A. POP3/IMAP B. SMTP C. DNS D. IP

答：B。

1. Which is the default port number of SMTP protocol?

A. 13 B. 21 C. 25 D. 80

答：C。

1. 下列协议中与电子邮件安全无关的是 （　　） 。

A. SSL B. HTTPS C. MIME D. PGP

答：C。

1. SSL 是一种加密协议，常用于保护电子邮件在传输过程中的机密性和完整性。
2. HTTPS 在 HTTP 基础上添加了 SSL/TLS 加密层的协议，用于安全地传输网页内容。虽然它主要用于网页浏览，但也可以用于安全地访问基于 Web 的电子邮件服务。
3. MIME（Multipurpose Internet Mail Extensions）：MIME 是一种扩展标准，允许电子邮件传输非 ASCII 文本、二进制文件、图像、音频、视频等多媒体内容。不涉及安全性。
4. PGP（Pretty Good Privacy）：PGP 是加密软件，用于加密和解密电子邮件内容，以保护邮件的机密性和完整性。它与电子邮件安全密切相关。

## 二、简答题

1. 下面列出的是使用 TCP/IP 通信的两台主机 A 和 B 传送邮件的对话过程，请根据这个对话回答问题。

|  |
| --- |
| A: 220 beta.gov simple mail transfer service ready  B: HELO alpha.edu  A: 250 beta.gov  B: MAIL FROM:<smith@alpha.edu>  A: 250 mail accepted  B: RCPT TO:<jones@beta.gov>  A: 250 recipient accepted  B: RCPT TO:<green@beta.gov>  A: 550 no such user here  B: RCPT TO:<brown@beta.gov>  A: 250 recipient accepted  B: DATA  A: 354 start mail input; end with <CR><LF>.<CR><LF>  B: Date: Fri 27 May 2011 14:16:21 BJ  B: From: smith@alpha.edu  B: ...  B: ...  B: .  A: 250 OK  B: QUIT  A: 221 beta.gov service closing transmission channel. |

问题：

1. 邮件接收方和发送方机器的全名是什么？发邮件的用户名是什么？
2. 发送方想把邮件发给几个用户？它们的名字各是什么？
3. 哪些用户能收到该邮件？
4. 传送邮件所使用的传输层协议的名称是什么？
5. 为了接收邮件，接收方机器上等待连接的端口号是多少？

答：1)邮件接收方机器的全名是 beta.gov，邮件发送方机器的全名是 alpha.edu，发邮件的用户名是 smith。2) 发送方想把该邮件发给三个用户，它们的名字分别是 jones、green 和 brown。 3) 用户 jones 和 brown 能收到邮件，beta.gov 上不存在用户 green。 4) 传送邮件所用的传输层协议称为 TCP（传输控制协议）。 5) 为了接收邮件，接收方服务器上等待连接的端口号是 25。

1. 某用户向客户发送一封电子邮件，其中有哪些环节需要SMTP协议？

答：用户的客户端程序到电子邮件服务器；源电子邮件服务器到目标电子邮件服务器。

1. MIME支持哪几大类格式的文件？对RAR文件，试着给出其首部。网易或QQ大附件是否为MIME格式？

（提示：将邮件下载为EML格式或以明文模式接受并用Wireshark侦听接收QQ邮件的数据包，观察POP3协议的分组内容。）

答：多用途互联网邮件扩展（MIME，Multipurpose Internet Mail Extensions）支持七大类格式的文件：(1)Text：文本文件；(2)Multipart：用于连接消息体的多个部分构成一个消息，这些部分可以是不同类型的数据；(3)Application：应用程序数据或者二进制数据；(4)Message：用于包装一个E-mail消息；(5)Image：用于传输静态图片数据；(6)Audio：用于传输音频或者音声数据；(7)Video：用于传输动态影像数据，可以是与音频编辑在一起的视频数据格式。

RAR文件的首部：application/octet-stream。

网易或QQ大附件是否为MIME不是格式。可以通过运行监听包的软件校对你的回答，或者在QQ邮箱的扩展菜单里选择“导出为eml文件”，从邮件附件的形式也可以看出来，不是用MIME形式直接发送的，而是将大附件存在存储服务器上，并将下载链接放入HTML块中，附在邮件后。

1. 请写出下列(1)～(8)依次是什么协议或部件，选填MUA，MTA，MDA，SMTP，POP/IMAP。



答：(1) MUA; (2) SMTP; (3).MTA; (4).SMTP; (5) MTA; (6) MDA; (7) POP; (8) MUA。

# 第19课 文件传输协议

## 一、单项选择题

1. During an FTP session the control connection is opened （　　） .

A. exactly once B. as many times as necessary

C. exactly twice D. all of the above

答：A。

1. During an FTP session the data connection is opened and closed （　　） .

A. exactly once B. as many times as necessary

C. exactly twice D. all of the above

答：B。

1. FTP can be characteristized as:

A. Clients can transfer files but they cannot obtain the contents of a directory.

B. Control messages can be sent as either ASCII text or non-ASCII character.

C. FTP allows each file to have ownership and access restrictions.

D. If the FTP server is running on UNIX and a client on Windows is used to download a binary file, a file format error occurs.

答：C。

A. 客户端可以传输文件，但不能获取目录的内容。FTP允许客户端列出目录内容。B.控制消息可以以ASCII文本或非ASCII字符发送。FTP的控制连接通常使用ASCII文本进行通信。C.FTP支持文件的所有权和访问权限设置。正确。D.如果FTP服务器运行在UNIX上，而Windows客户端用于下载二进制文件，会发生文件格式错误。FTP设计时考虑了不同操作系统之间的文件传输，使用适当的传输模式（如二进制模式）可以避免文件格式错误。

1. FTP can be characteristized as:

A. FTP can transfer only textual content.

B. Control messages exchanged between an FTP client and server are sent as ASCII text or non-ASCII character.

C. If an FTP server denies a client to use anonymous login, the server will send use the 3-way handshake to close a connection with FIN segments.

D. If the FTP server is running on UNIX and a client on Windows is used to download a binary file, a file format error occurs.

答：C。

1. FTP不仅可以传输文本文件，还可以传输二进制文件（图片、压缩文件等）。
2. B.FTP的控制消息通常是以ASCII文本形式发送的。
3. FTP服务器拒绝匿名登录时，断开连接是通过三次挥手。
4. 同上。
5. In FTP, to begin a control connection, the server issues （　　） open.

A. An active B. A passive C. An ephemeral D. None

答：B。FTP使用控制连接（默认端口21）和数据连接（端口20或其他）。

控制连接：始终由客户端主动发起，服务器在端口21上被动监听。

数据连接：根据模式不同，建立方式不同：主动模式（Active Mode）：服务器从端口20主动连接到客户端。被动模式（Passive Mode）：服务器开放随机端口，客户端主动连接。

1. Which is the default port number of FTP control in plain text?

A. 20 B. 21 C. 25 D. 110

答：B。

1. Which is the default port number of FTP data transmission?

A. 13 B. 20 C. 21 D. 25

答：B。

1. Which of the following about FTP is true?

A. An FTP reply consists of a three digit number followed by some text.

B. Anyone can download the files which he or she just uploaded.

C. The data connection needs to exist all of the time.

D. When opening a data connection in passive mode, the client acts like a server.

答：A。

1. FTP协议规定，服务器对客户端的每个命令必须返回一个三位数字的状态码，后接描述性文本。例如：200 Command okay. 550 Permission denied.第一位数字表示响应类型（如2表示成功，5表示错误），后两位细化具体状态。这是FTP协议的核心规范，符合RFC 959定义。
2. 能否下载上传的文件取决于服务器权限配置。例如：匿名FTP服务器可能允许上传但不开放下载权限。服务器可能限制文件访问需管理员审核。
3. FTP的数据连接仅在传输文件或目录列表时临时建立，完成后立即关闭。控制连接（端口21）才在整个会话期间保持打开。数据连接无需持续存在。
4. 被动模式（Passive Mode）中，服务器开放随机端口并告知客户端，客户端主动连接该端口传输数据。客户端始终是数据连接的主动发起方，服务器是被动监听方。
5. Which of the following protocols listens on port 25?

A. SMTP B. POP3 C. HTTP D. FTP

答：A。

1. Which of the following statements about FTP is TRUE?

A. FTP can transfer only text file, and files with textual content.

B. FTPS (FTP over SSL) prevents others from intercepting the content of FTP.

C. If an FTP server denies a client to use an invalid login, the client will close the connection with FIN segments.

D. If the FTP server and client are running on different operating system, a file format error occurs.

答：B。

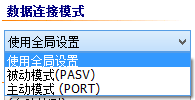
## 二、简答题

1. 为什么FTP客户发出的控制连接时，客户作为客户端？在哪些情况FTP客户作为服务器端，而FTP服务器却作为客户端？

（提示：客户端和服务器端的定义与客户和服务器的定义之间的区别和联系。服务器并不经常作为Socket连接的服务器端。）

答：服务器端被动等待来自客户的连接请求，而客户端主动发起连接请求。当需要传输数据时，FTP新开通数据连接，专门用于传输文件数据。此时，客户起到像服务器（等待数据连接）那样的作用，原来的服务器却起到像客户（发起数据连接）那样的作用。

1. 客户端进行数据连接有主动和被动模式（PASV和PORT模式）两种，比较其优劣。（提示：使用FTP客户端，如FlashFXP，用Wireshark试验。）



答：FTP的控制连接有验证功能，而数据连接却没有。数据连接接受用户的访问是基于服务器控制连接的验证结果。服务器可以从控制连接知道客户端的IP地址，如需标识用户程序，还需要知道客户的端口号。客户唯有做服务器端使用，才能确定其端口号。此时，服务器端用20号端口连接它。

但是，一些简单轻便的FTP客户端没有实现该功能，因此，FTP还提供了一种PASV模式（发数据也是主动打开），客户提出数据连接的请求并通过服务器验证后，客户机器上任意程序如果监听到服务器打开的端口号，它们都能够往该端口接收或发送数据。

（以上过程可以用Omnipeek验证。）

1. 主机H登录FTP服务器后，向服务器上传一个大小为18000B的文件F。假设H传输F建立数据连接时，选择的初始序号为100，MTU=1000B，拥塞控制初始阈值为4MSS，RTT=10ms，忽略TCP的传输时延；在F的传输过程中，H均以MSS段向服务器发送散据，且未发生差错、丢包和乱序。

（1）FTP的控制连接是持久的还是非持久的？FTP的数据连接是持久的还是非持久的？H登录FTP服务器时，建立的是控制连接还是数据连接？

（2）H通过数据连接发送F时，F的第一个字节序号是多少？在断开数据连接的过程中，FTP发达的第二次挥手的ACK序号是？

（3）F发送过程中,当H收到确认序号为2101的确认段时，H的拥塞窗口调整为多少？收到确认序号为7101的确认段时，H的拥塞窗口调整为多少？

（4）H从请求建立数据连接开始，到确认F已被服务器全部接收为止，至少需要多长时间期间应用层数据平均发送速率是多少？

答：（1）控制连接是持久的；数据连接是非持久的；控制连接。（2）101；18102；（3）3000；5000；（4）6个RTT，需要60ms；18000B/24ms=24Mbps。

具体原理为：初始阶段（慢启动）：cwnd=1 MSS，发送段1（1000B）。收到段1的ACK后，cwnd=2，发送段2、3。收到段2的ACK（确认号2101），cwnd=3。拥塞避免阶段：当cwnd达到阈值4 MSS后，进入线性增长。收到段7的ACK（确认号7101），累计确认7100B（7个段），cwnd增长到5 MSS。

# 第20课 万维网

## 一、单项选择题

1. Which is the default port number of HTTP protocol?

A. 20 B. 80 C. 110 D. 443

答：B。

1. HTTP works on the （　　） layer of the TCP/IP reference module.

A. network interface B. physical

C. transport D. application

答：D。

1. Which can be a valid destination address in the packet of HTTP stream?

A. 00-FF-F1-00-25-12 B. 0.0.0.0

C. 00:50::00:01 D. 127.0.0.1

答：D。

1. 00-FF-F1-00-25-12：这是MAC地址（数据链路层地址），用于局域网内设备通信。HTTP作为应用层协议，其数据包的目标地址应为网络层（IP地址）或传输层（端口），而非MAC地址。无效。
2. 0.0.0.0：IPv4地址0.0.0.0表示“任意地址”或默认路由，通常用于服务器监听所有接口，但不能作为目标地址用于实际通信。无效。
3. 00:50::00:01：这是IPv6地址的简写形式，但写法不规范：IPv6每组为4位十六进制数，允许省略前导零。
4. 127.0.0.1：这是IPv4的本地回环地址，用于本机测试。HTTP请求发送到127.0.0.1时，目标地址合法且常用于本地服务访问
5. Which is NOT the major request types of HTTP?

A. GET B. PUT C. POST D. DATA

答：D。

1. Which is NOT the major request types of HTTP?

A. SET B. GET C. PUT D. POST

答：A。

1. HTTP status code （　　） denotes an internal error.

A. 200. B. 301. C. 403. D. 500.

答：D。

1. HTTP status codes which begin with （　　） denote request error on the client side.

A. 2. B. 3. C. 4. D. 5 or 6.

答：C。

1. The HTTP status code beginning with 5 is used for （　　） .

A. redirection B. server error C. client error D. success

答：B。

1. The status code 200 means （　　） for HTTP.

A. redirection B. internal error C. not found D. OK

答：D。

1. The status code 404 means （　　） for HTTP.

A. OK B. not found C. internal error D. redirection

答：B。

1. The status code 500 means （　　） for HTTP.

A. OK B. not found C. internal error D. redirection

答：C。

1. Which is present in both a HTTP request line and a HTTP status line?

A. HTTP version B. URL C. status code D. status phrase

答：A。

1. 使用Telnet协议进行远程登录时需要满足的条件不包括 （　　） 。

A.本地计算机上安装包含Telnet协议的客户端程序

B.必须知道远程主机的IP地址或域名

C.必须知道登录标识与口令

D.本地计算机防火墙入站规则设置允许Telnet访问

答：D。

1. Web 页面访问过程中，在浏览器发出HTTP请求报文之前不可能执行的操作是 （　　） 。

A. 查询本机DNS缓存，获取主机名对应的IP地址

B. 发起DNS请求，获取主机名对应的IP地址

C. 使用查询到的IP地址向目标服务器发起TCP连接

D. 发送请求信息，获取将要访问的Web应用

答：D。

1. 通过代理服务器（Proxy Server）访问Internet的主要功能不包括 （　　） 。

A. 突破对某些网站的访问限制 B. 提高访问某些网站的速度

C. 避免来自Internet上病毒的入侵 D. 隐藏本地主机的IP地址

答：C。

参考解析： 代理服务器主要功能如下：

（1）设置用户验证和记账功能，可按用户进行记账，没有登记的用户无权通过代理服务器访问Internet网。并对用户的访问时间、访问地点、信息流量进行统计。

（2）对用户进行分级管理，设置不同用户的访问权限，对外界或内部的Internet地址进行过滤，设置不同的访问权限。

（3）增加缓冲器(Cache)，提高访问速度，对经常访问的地址创建缓冲区，大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区（可能高达几个GB或更大），当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息，传给用户，以提高访问速度。

（4）连接Intranet与Internet，充当防火墙（Firewall）：因为所有内部网的用户通过代理服务器访问外界时，只映射为一个IP地址，所以外界不能直接访问到内部网；同时可以设置IP地址过滤，限制内部网对外部的访问权限。

（5）节省IP开销：代理服务器允许使用大量的伪IP地址，节约网上资源，即用代理服务器可以减少对IP地址的需求，对于使用局域网方式接入Internet ，如果为局域网（LAN）内的每一个用户都申请一个IP地址，其费用可想而知。但使用代理服务器后，只需代理服务器上有一个合法的IP地址，LAN内其他用户可以使用10.\*.\*.\*这样的私有IP地址，这样可以节约大量的IP，降低网络的维护成本。

（6）监控和限制用户的上网行为。

但没有阻止企业网络感染病毒的能力，要实现此功能需要利用企业版杀毒软件。

1. 代理服务器为局城网用户提供Internet访问时，不提供 （　　） 服务。

A. 地址共享 B. 数据缓存 C. 数据转发 D. 数据加密

答：D。

1. 下面的安全协议中， （　　） 是替代SSL协议的一种安全协议。
2. PGP B. TLS C. IPSec D. VPN

答：B。

1. PGP：用于电子邮件和文件的端到端加密与签名，与SSL/TLS的应用场景（传输层加密）无关。
2. SSL（Secure Sockets Layer） 是最初用于加密网络通信的协议，广泛应用于Web安全（如HTTPS）。TLS（Transport Layer Security） 是SSL的标准化升级版本。TLS被明确设计为SSL的替代协议，目前SSL已因安全性问题被弃用，TLS成为主流。
3. IPSec：工作在网络层，保护IP数据包的安全（如VPN中），与SSL/TLS（传输层/应用层）属于不同协议层次，无替代关系。
4. VPN：是一种通过加密通道实现远程安全连接的技术，依赖具体协议（如IPSec、SSL/TLS等），本身并非协议。

## 二、简答题

1. 某Web网站因访问量大而变得很卡，请列出一些方法提高用户体验。

答：负载均衡、内容缓存加速、内容分发网络（CDN）、购置处理能力更高的服务器。

1. 超文本传输协议（HTTP），统一资源定位符（URL）和超文本标记语言（HTML）是万维网（WWW）服务使用的三个标准，请分别写出每个标准的用途。

答： HTTP：用于规范浏览器如何与Web服务器交互传输数据的传输协议；URL：用于规范网页识别符的格式和含义的表示标准，或：用一个字符串构成对网络上文本、图像和视频等资源的引用；HTML：用于规范网页内容和排版布局的表示标准。

1. 某主机的MAC地址为00-15-C5-C1-5E-28，IP地址为10.2.128.100（私有地址）。图a是网络拓扑，图b是该主机进行Web请求的1个以太网数据帧前80B的十六进制及ASCII码内容。



图18-1(a) 网络拓扑

|  |
| --- |
| 0000 00 21 27 21 51 ee 00 15 c5 c1 5e 28 08 00 45 00 .!|!Q... ..^(..E.  0010 01 ef 11 3b 40 00 80 06 ba 9d 0a 02 80 64 40 aa ...:@... .....d@.  0020 62 20 04 ff 00 50 e0 c2 00 fa 7b f9 f8 05 50 18 b ...P.. ..{...P.  0030 fa f0 1a c4 00 00 47 45 54 20 2f 72 66 63 2e 68 ......GE T /rfc.h  0040 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 41 c3 tml HTTP /1.1..Ac |

图18-1(b) 以太网数据帧（前80B）

请参考图中的数据回答以下问题：

（1）Web服务器的IP地址是什么？该主机的默认网关的MAC地址是什么？

（2）该主机在构造题47-b图的数据帧时，使用什么协议确定目的MAC地址？封装该协议请求报文的以太网帧的目的MAC地址是什么？

（3）假设HTTP/1.1协议以持续的非流水线方式工作，一次请求-响应时间为RTT，rfc.html页面引用了5个JPEG小图像，则从发出题47-b图中的Web请求开始到浏览器收到全部内容为止，需要多少个RTT？

（4）该帧所封装的IP分组经过路由器R转发时，需修改IP分组头中的哪些字段？

答：

(1)从题47-b图可知，该数据帧所封装的IP分组的目的地址就是Web服务器的IP地址，即64.170.98.32(40aa62 20H);(1分)该数据帧的目的MAC地址就是该主机的默认网关MAC地址，即00-21-27-21-51-ee。(1分)

(2)该主机在构造题47-b图的数据帧时，使用ARP协议确定目的MAC地址;(1分)因为ARP协议请求报文需要进行广播，所以封装ARP协议请求报文的以太网帧的目的MAC地址是ff-ff-ff-ff-ff-ff。(1分)

(3)根据持续的非流水线方式HTTP/1.1协议的工作原理，每个RTT传输一个对象，共需要传输6个对象(1个htm1页面和5个JPEG小图像)，所以共需要6个RTT。(2分)

(4)该帧所封装的IP分组经过路由器R转发时，需要修改IP分组头中的字段有：源IP地址、TTL和头部校验和。(3分)

1. 阅读以下说明，回答问题1至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某公司有两个办事处，分别利用装有Windows Server 2008 的双宿主机实现路由功能，此功能由Windows Server 2008中的路由和远程访问服务来完成。管理员分别为这两台主机其中一个网卡配置了不同的IP地址，如图3-1所示。

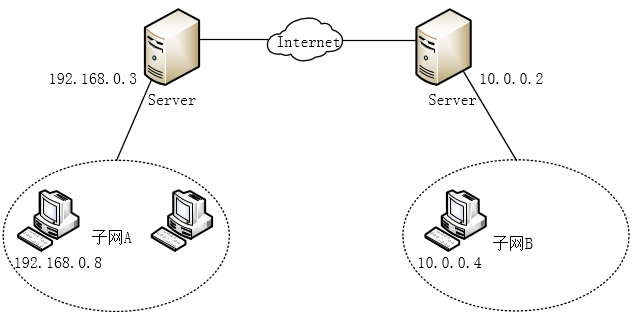


图3-1

【问题1】在“管理您的服务器”中点击“添加或删除角色”，此时应当在服务器角色中选择（1）来完成路由和远程访问服务的安装。在下列关于路由和远程访问服务的选项中，不正确的是（2）。

（1）备选答案：

A. 文件服务器 B. 应用程序服务器（IIS,ASP.NET）

C. 终端服务器 D. 远程访问/VPN服务

（2）备选答案：

A. 可连接局域网的不同网段或子网，实现软件路由器的功能

B. 把分支机构与企业网络通过Intranet连接起来，实现资源共享

C. 可使远程计算机接入到企业网络中访问网络资源

D. 必须通过VPN才能使远程计算机访问企业网络中的网络资源

【问题2】（4分）

两个办事处子网的计算机安装Win7操作系统，要实现两个子网间的通信，子网A和子网B中计算机的网关分别为（3）和（4）。子网 A 中的计算机用ping命令来验证数据包能否路由到子网B中，图3-2中参数使用默认值，从参数（5）可以看出数据包经过了（6）个路由器。

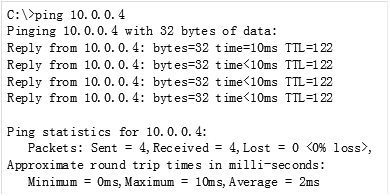


图3-2

（3）备选答案：

A. 192.168.0.0 B. 192.168.0.1 C. 192.168.0.3 D. 无须配置网关

（4）备选答案：

A. 10.0.0.0 B. 10.0.0.1 C. 10.0.0.2 D. 无须配置网关

（5）备选答案：

A. bytes B. time C. TTL D. Lost

【问题3】Windows Server 2008支持RIP动态路由协议。在RIP接口属性页中，如果希望路由器每隔一段时间向自己的邻居广播路由表以进行路由信息的交换和更新，则需要在“操作模式”中选择（7）。在“传出数据包协议”中选择（8），使网络中其它运行不同版本的邻居路由器都可接受此路由器的路由表；在“传入数据包协议”中选择（9），使网络中其它运行不同版本的邻居路由器都可向此路由器广播路由表。

（7）备选答案：

A. 周期性的更新模式 B. 自动--静态更新模式

（8）备选答案：

A. RIPv1广播 B. RIPv2多播 C. RIPv2广播

（9）备选答案：

A. 只是RIPv1 B. 只是RIPv2 C. RIPv1和v2

D. 忽略传入数据包

为了保护路由器之间的安全通信，可以为路由器配置身份验证。选中“激活身份验证”复选框，并在“密码”框中键入一个密码。所有路由器都要做此配置，所配置的密码（10）。

（10）备选答案：

A. 可以不同 B. 必须相同

【问题4】由于在子网A中出现病毒，需在路由接口上启动过滤功能，不允许子网B接收来自子网A的数据包，在选择入站筛选器且筛选条件是“接收所有除符合下列条件以外的数据包”时，如图3-3所示，由源网络IP地址和子网掩码得到的网络地址是（11），由目标网络IP地址和子网掩码得到的网络地址是（12），需要选择协议（13）。如果选择协议（14），则会出现子网A和子网B之间ping不通但是子网B能接收来自子网A的数据包的情况。

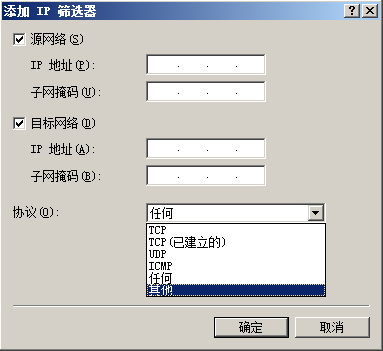


图3-3

（11）备选答案：

A. 192.168.0.0 B. 192.168.0.1 C. 192.168.0.3 D. 192.168.0.8

（12）备选答案：

A. 10.0.0.0 B. 10.0.0.1 C. 10.0.0.3 D. 10.0.0.4

（13）~（14）备选答案：

A. ICMP B. TCP C. UDP D. 任何

答：1、D；2、D；3、C；4、C；5、C；6、6；7、A；8、A；9、C；10、B；11-14 A A D A。

参考解析： 通过文字及图形说明，可知子网A连接在192.168.0.0网段，而子网B处在10.0.0.0网段，对应的网关地址分别为网段连接的服务器IP。Ping命令通常用于测试连通性，利用的ICMP的回送请求或回答报文，其中TTL值代表跳数，WIN7实际TTL默认是64，WINXP是128，这里由于题目有点问题，我们以128跳开始，每经过一个路由器，就会减1。

为支持RIP动态路由协议，可自己相应配置，RIP有两个版本，V1只支持有类路由信息，并以广播的方式发送整个路由表给邻居，V2支持无类别路由，以组播的方式发送整个路由表信息进行路由收敛。默认情况下是发送版本1报文，接收任意版本报文。

为了确保路由器之间的安全通信，可在路由器和路由器之间增加身份验证，并且相互连接的双方密码信息要一致。