

期末真题终点

17年

4. ASDL which divides available bandwidth uses _____ division multiplexing. D

A. time B. wave C. code D. frequency

翻译：

4.非对称数字用户线路（ASDL）划分可用带宽时使用_____复用技术。【答案：D】

A. 时分B. 波分C. 码分D. 频分

（解析：ASDL 通过频分复用（FDM）技术将电话线路的高频段和低频段划分，分别用于数据传输和语音通信，实现带宽的非对称分配。）

6. The mechanism of _____ created to establish label switched paths was so cumbersome that it was not used. B

A. ARPANET B. ATM C. Frame relay D. X. 25

用于建立标签交换路径的_____机制因过于繁琐而未被采用。【答案：B】

A. 阿帕网（ARPANET）

B. 异步传输模式（ATM）

C. 帧中继（Frame Relay）

D. X.25 协议

解析：

- **ATM（异步传输模式）**：通过虚拟路径标识符（VPI）和虚拟信道标识符（VCI）建立标签交换路径（类似现代 MPLS 中的标签概念），但需依赖复杂的信令协议（如 PNNI）来动态创建和管理连接，配置和维护成本高，机制繁琐。尽管 ATM 曾用于骨干网络，但其复杂性限制了广泛应用，尤其在 IP 网络兴起后逐渐被更简单的技术取代。

- **其他选项排除：**

- **ARPANET**：早期分组交换网络，未涉及标签交换或复杂连接机制。
- **帧中继（C）**：基于数据链路连接标识符（DLCI）的简化分组交换，机制轻量，无需复杂信令。
- **X.25（D）**：早期分组交换协议，基于虚电路（VC），但协议层处理较多（如错误校验），但连接建立机制不如 ATM 繁琐。

因此，ATM 因标签交换路径建立机制的复杂性而未被广泛采用，故选 B。

8. Which of the following can be a source address of an IP datagram? A

A. 0.0.0.0 B. 218.193.0.0 C. 224.1.0.2 D. 255.255.255.255

选项分析：

1. A. 0.0.0.0

- **含义：**代表“未知地址”或“所有地址”，常用于主机启动时尚未获取有效 IP 地址的场景（如 DHCP 申请过程中）。
- **作为源地址：**合法。例如，主机在未配置 IP 时发送 DHCP 请求，源地址会暂时使用 **0.0.0.0**，表示“本主机”。
- **限制：**不能作为目的地址，且仅在特定初始化场景中作为源地址使用。

2. B. 218.193.0.0

- **类别：**属于 C 类 IP 地址的网络地址（前 24 位为网络号，最后 8 位为 0）。
- **用途：**网络地址用于标识一个网段（如 **218.193.0.0/24**），不能分配给具体主机。
- **结论：**不能作为源地址，因为源地址必须是主机的有效 IP 地址。

3. C. 224.1.0.2

- **类别：**D 类多播地址（224.0.0.0~239.255.255.255），用于组播通信（如视频会议、路由器协议）。
- **用途：**只能作为目的地址，标识一组接收者，不能作为单播通信的源地址。
- **结论：**禁止作为源地址。

4. D. 255.255.255.255

- **含义：**受限广播地址，用于向本地网络（同一子网）的所有主机发送广播包。
- **用途：**只能作为目的地址，且仅在本地网络内有效（路由器不会转发）。
- **结论：**不能作为源地址，因为源地址必须是唯一标识发送者的单播地址。

11. Which of the following statements about WAN store and forward is TRUE? D

A. A system that uses the store and forward paradigm can keep each data link busy, and thus, decrease overall performance.

B. The forward operation occurs when a packet arrives: I/O hardware inside the packet switch places a copy of the packet in memory.

C. The store operation occurs once a packet has arrived and is waiting in memory,

D. The processor examines the packet, determines its destination, and sends the packet over the I/O interface that leads to the destination.

选项分析

- A. 使用存储转发范式的系统可以让每个数据链路保持忙碌，从而降低整体性能。

错误。存储转发机制通过暂存数据包并优化路径转发，理论上可提高链路利用率（而非“降低性能”）。若链路持续忙碌，通常意味着资源利用率高，性能应提升而非下降。

- B. 当数据包到达时，转发操作发生：分组交换机内的 I/O 硬件将数据包的副本存入内存。

错误。“存储（Store）”操作是指数据包到达时先存入内存，而“转发（Forward）”是后续的处理步骤（如查找路由后再转发）。此选项混淆了“存储”和“转发”的顺序，将存储误称为转发。

- C. 当数据包到达并在内存中等待时，存储操作发生。

错误。存储操作在数据包到达时立即执行（将数据存入内存），而“在内存中等待”是存储后的状态，并非存储操作的触发条件。此选项逻辑颠倒。

- D. 处理器检查数据包，确定其目的地，并通过通向目的地的 I/O 接口发送数据包。

正确。这是存储转发的核心流程：

- a. 设备先接收并存储数据包；
- b. 处理器解析数据包的目的地址（如 IP 地址），通过路由表确定转发路径；
- c. 将数据包从对应的 I/O 接口（如网卡）转发到下一跳。

此选项准确描述了“转发”操作的关键步骤。

总结：存储转发机制的核心是“先存储、后处理、再转发”，选项 D 完整体现了这一逻辑，其他选项均存在概念混淆或逻辑错误。

12. Pinging _____ with all packets received successfully CANNOT tell the network interface card is working properly. B

A. 0.0.0.0 • B. 127.0.0.255 C. 192.168.1.0 D. 255.255.255.255

翻译：ping哪个地址并且所有数据包都成功接的情况下，不能说明网络接口卡工作正常

关键知识点：环回地址（Loopback Address）的特性

- 环回地址范围：127.0.0.0/8（即 127.0.0.0 到 127.255.255.255）是预留的本地环回地址，用于测试本地 TCP/IP 协议栈的连通性。

- 核心逻辑：

当向环回地址发送数据包时，数据包不会经过物理网卡，而是直接在操作系统内部的协议栈中“环回”（Loop Back），即从发送端直接返回接收端。因此，ping 环回地址成功只能证明：

- a. 本地协议栈（如 IP、ICMP 协议）正常工作；
- b. 操作系统与协议栈的交互正常。

但无法验证网卡硬件是否正常（因为数据包未触达网卡）。甚至数据包完全不会离开本地主机，也够不到任何网卡、交换机之类的。

所以：A代表未分配的本地地址、不能作为目标被ping通，直接无响应，而C是网络地址而非主机地址，通常不可ping通，若ping通可能表示网络配置异常，而且与网卡测试无关，D是受限广播地址，若成功接收响应，说明网卡能正常发送接收广播包，可以证明网卡硬件工作正常

14. Each entry in a ____ advertisement consists of a pair (destination network, distance), A

A. RIP B. OSPF C. IS-IS D. BGP

翻译：哪个协议的每个条目都由（目标网络，距离）组成

解析：

A. RIP（路由信息协议）

- 协议类型：距离矢量路由协议（Distance-Vector Routing Protocol）。
- 更新内容：
每个路由条目包含（目标网络，距离）两个核心信息：
 - 目标网络：标识目的网络地址（如 192.168.1.0/24）。
 - 距离：以 跳数（Hop Count） 为度量值，表示到达目标网络的距离（最大 15 跳，16 跳视为不可达）。
- 结论：符合题意。

B. OSPF（开放最短路径优先）

- 协议类型：链路状态路由协议（Link-State Routing Protocol）。
- 更新内容：
通过 链路状态通告（LSA） 传播信息，包含：
 - 本地接口的 IP 地址、子网掩码、链路类型（如广播型、点到点）。
 - 相邻路由器的 ID、链路开销（Cost）等链路状态信息，而非直接的“距离”值。
- 结论：不包含“距离”字段，不符合题意。

C. IS-IS（中间系统到中间系统）

- 协议类型：链路状态路由协议（与 OSPF 类似，常用于大型企业网和 ISP 网络）。

- **更新内容：**

通过 **链路状态分组（LSP）** 传播信息，包含：

- 路由器连接的链路、接口地址、度量值（如默认的“延迟”“开销”）等**链路状态细节**，而非简单的“目标网络 + 距离”对。

- **结论：**不包含“距离矢量”结构，**不符合题意**。

D. BGP（边界网关协议）

- **协议类型：**路径矢量路由协议（Path-Vector Routing Protocol，用于自治系统间路由，如互联网）。

- **更新内容：**

每个路由条目包含（**目标网络，路径属性**），路径属性包括：

- **AS 路径（AS Path）**：标识路由经过的自治系统列表（用于防环）。
- **下一跳（Next Hop）**、本地优先级（Local Preference）等，而非“距离”（跳数）。

- **结论：**以“路径属性”替代“距离”，**不符合题意**。

16. FTP can be characterized as: B

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.

总结

- **选项 B 正确**，因 FTP 控制消息在默认情况下为 ASCII 文本，且在扩展配置下可支持非 ASCII 字符。
- 其他选项均存在明显错误：A 否定目录获取功能，C 混淆 FTP 与操作系统的权限机制，D 忽略二进制传输模式的正确性。

17.

17. When a host cannot resolve a domain, a request message will be sent to _____ server.

A A. local B. authority C. top level D. root

解析：

当主机无法解析域名时，首先会向 **本地 DNS 服务器 (Local DNS Server)** 发送请求。本地服务器是**主机配置中指定的首选 DNS 服务器**（如路由器或 ISP 提供的 DNS）。若本地服务器无法解析，**才会逐级向上查询**（根服务器→顶级域服务器→权威服务器）。因此，**初始请求一定先发送到本地服务器**，正确答案为 **A**。

18.

18. During an e-mail is received from the server, _____ is NOT engaged. D

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

解析：

电子邮件接收过程涉及以下协议：

- **POP3/IMAP4 (C 选项)**：用于从服务器下载邮件到客户端（接收协议）。
- **DNS (A 选项)**：解析邮件服务器域名（如 `mail.example.com`）为 IP 地址。
- **IP (B 选项)**：承载数据传输的底层协议。
- **SMTP (D 选项)**：仅用于发送邮件（从客户端到服务器或服务器间中继），**不参与接收过程**。

因此，接收邮件时**不涉及 SMTP**，正确答案为 **D**。

20.

20. IPv4 address exhaustion is one of the motivation of IPv6, _____ and _____ overcomes such shortage and extends the life of IPv4. A A. CIDR; NAT B. CDMA; CSMA C. DHCP; ARP D. ARP; DNS

解析：

IPv4 地址耗尽的两大核心解决方案是 **CIDR** 和 **NAT**：

- **CIDR (无类别域间路由, A 选项)**：通过合并子网减少地址浪费（如将多个 C 类地址聚合为一个超网），提高地址利用率。
- **NAT (网络地址转换, A 选项)**：允许多个内网设备共享一个公网 IP，大幅减少公网地址消耗（如家庭网络中数十台设备共用一个 IPv4 地址）。

其他选项分析：

- **B. CDMA/CSMA**：属于物理层技术（无线通信 / 信道访问控制），与 IP 地址无关。
- **C. DHCP/ARP**：DHCP 用于动态分配 IP 地址，但未解决地址总量不足；ARP 用于 IP-MAC 映射，与地

址耗尽无关。

- **D. ARP/DNS:** ARP 同上；DNS 用于域名解析，与地址扩展无关。

因此，正确答案为 **A**，CIDR 和 NAT 通过地址优化和复用“延长了 IPv4 的寿命”。

简答题：

2. TCP/IP协议族的网络接口层已定义帧格式和物理地址，为何网络层需要定义IP报文 格式并使用唯一的IP地址？

网络接口层的帧格式和物理地址（如 MAC）仅用于本地链路通信，无法跨网络路由。IP 报文格式和唯一 IP 地址提供逻辑寻址，通过网络号 + 主机号结构支持跨网段路由，使数据包能在异构网络间传输，突破物理层局限，实现互联网级通信。

3.RIP（路由信息协议）使用何种传输层协议？请简述其工作原理。

RIP 使用**UDP 协议**（端口号 520）传输路由信息。其工作原理为：路由器定期向邻居广播自身路由表，每条路由包含目标网络、跳数等信息；通过比较跳数（最大 15 跳视为不可达）更新路由表；采用水平分割、毒性逆转等机制避免路由环路，实现动态路由发现与维护。

4.请简要说明TraceRoute和PING的原理。

答：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”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，重复到某个报文抵达目的地，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。

5. 简述TCP协议中流量控制机制，并指出流量控制与拥塞控制的区别。

回答：

TCP 流量控制通过**滑动窗口机制**实现：接收方在确认报文中返回“接收窗口”（rwnd）字段，告知发送方当前可用缓冲区大小，发送方据此调整发送速率，避免接收方缓冲区溢出。

区别：

- **流量控制是点对点机制**，解决发送方与接收方间速率匹配问题；
- **拥塞控制是全局机制**，基于网络整体负载调整发送速率，防止全网拥塞；
- 流量控制依据接收方缓冲区状态（rwnd），拥塞控制依据网络拥塞程度（cwnd），发送窗口取两者最小值。

相关知识：

9. 为什么需要进行流量控制？TCP采用何种机制进行流量控制？

答：流量控制主要针对数据段的接收方（由于忙）处理数据长度有限的时候，对发送数据的速度进行控制。TCP 采用接收方不断报告窗口大小的机制进行流量控制，即报告当前可以处理的报文的最大长度。TCP 收到窗口为 0 的时候，停止发送，启动一个计时器，到计时器为零的时候重新发送。

10. TCP已有流量控制，为何还需要拥塞控制？

答：二者的控制目的不同。流量控制是指抑制发送端发送数据的速率，以便使接收端来得及接收。拥塞控制是指防止过多的数据注入到网络中，使网络中的路由器或链路不致过载。

大题：路由表，子网划分，IP分片，socket有连接和无连接的流程图，访问网站的过程

18年

3. 请说明传统以太网的随机接入协议，即如何避免同时使用介质时的冲突。

答：传统以太网使用的随机接入协议是CSMA/CD（Carrier Sense Multiple Access with Collision Detection），它的工作原理如下：

- **载波监听（Carrier Sense）**：设备在发送数据之前先监听传输介质，检测是否有其他设备正在发送数据。
- **多路访问（Multiple Access）**：多个设备共享同一个传输介质，可以同时发送数据。
- **冲突检测（Collision Detection）**：如果多个设备同时发送数据导致冲突，设备会检测到冲突并终止发送。
- **随机退避（Random Backoff）**：设备在检测到冲突后会等待一个随机的时间后再次尝试发送数据，以避免再次发生冲突。

CSMA/CD协议通过以上机制，能够有效地避免同时使用介质时的冲突，提供公平的访问机制和可靠的数据传输。

5. 主机H1向H2 的发送IPv4报文时，请画出路由器R1的路由表，包含目标网络 地址、子网掩码和下一跳。主机H1如何找到默认网关R1的IP地址和MAC地址？

答：图略。主机H1找到默认网关R1的IP地址和MAC地址是通过以下方式进行的：

- 默认网关的IP地址是在主机的网络配置中手动设置的，通常是由网络管理员提供。
- 主机在发送数据时，会先检查目标IP地址是否与其所在子网的地址匹配，如果不匹配，则将数据发送到默认网关的IP地址。
- 主机会使用ARP协议（地址解析协议）将默认网关的IP地址解析为对应的MAC地址，以便在链路层进行数据帧的发送。

10• 从输入我系主页网址（<http://software.xmu.edu.cn/View/index.aspx>）到 该主页 完整显示在浏览器的过程中，浏览器软件在后台经过了哪些步骤？上述通信过程中使用 了多种编址方案，包括：以太网MAC地址、IP地址、TCP端口和域名。这4种地址各 有何作用？

解析：过程如下，

1. 浏览器首先通过DNS域名解析到服务器IP地址。
2. 浏览器接着查询ARP缓存，查询服务器IP地址对应的MAC地址。
 - a. 如果缓存命中，则返回结果：目标IP地址——MAC地址；
 - b. 如果没有命中：
 - i. 查看本机维护路由表（见下图），看目标IP地址是否在本地路由表中的某个子网内：是则使用目标IP地址，否则使用默认网关的IP地址；
 - ii. 查询选择的网络接口IP地址的MAC地址：发送一个数据链路层的广播ARP请求分组，该网段内都可以收到这个广播分组，但只有对应网关路由器接口才会返回一个ARP单播响应分组，将MAC地址回传。
3. 找到MAC地址后，便找到了下一跳，数据就可以转发到网关，依此类推，客户机就可以通过TCP/IP协议建立到服务器的TCP连接。
4. 客户端向服务器发送HTTP协议请求包，请求服务器里的资源文档。
5. 服务器向客户机发送HTTP协议应答包，将资源返回给客户端。
6. 客户机与服务器断开，由客户端解释HTML文档，在客户端屏幕上渲染图形效果等。

楼楼注：在二层网络中源MAC地址和目的MAC地址保持不变，在三层网络中源MAC地址和目的MAC地址要发生改变，目的MAC地址指向下一跳路由器的接口MAC地址。IP地址除了在NAT情况下，其他情况源IP和目的IP地址都不变。

在上述通信过程中，不同的编址方案发挥了各自的作用：

- 以太网MAC地址：用于在局域网中唯一标识网络设备，以太网帧使用MAC地址进行 目的地和源地址的标识，用于在局域网中的数据链路层通信。
- IP地址：用于在网络层进行主机之间的寻址和路由选择，确定数据的源和目的地，实现跨网络的通信。

- TCP端口：用于在传输层标识应用程序或服务，TCP报文段中的源端口和目的端口标识了发送和接收数据的应用程序。
- 域名：作为人类可读的网址，用于提供更友好的访问方式。域名通过DNS解析为IP地址，使浏览器能够直接与目标服务器创建连接。

12. 某同学开发了一个博客网站，并运行在其主机H1上。他邀请其它城市的同学前来体验，可是同学却向他反映无法访问。请从计算机网络TCP/IP五层协议模型分析可能有哪些方面原因？除了物理层外的4层，每层至少找出可能的1个原因，并针对其中某个原因提出解决建议。

答：可能导致某同学开发的博客网站无法访问的原因如下：

- 数据链路层：可能是物理层的问题，如网线连接故障、网卡故障等。解决方法是检查物理连接是否正常，更换故障的网线或网卡。
- 网络层：可能是IP地址配置错误或路由设置问题。解决方法是检查主机H1上的IP地址配置是否正确，并确保路由表中有正确的路由信息。
- 传输层：可能是防火墙或安全策略阻止了对特定端口的访问。解决方法是检查主机H1上的防火墙设置，确保允许来自外部的访问请求。
- 应用层：可能是Web服务器软件配置错误或服务未启动。解决方法是检查主机H1上的Web服务器配置文档，确保正确设置并启动相关的服务。

针对网络层的问题，可能的解决建议是：

- 检查主机H1上的IP地址配置，确保与其他主机在同一子网，并且没有重复的IP地址。
- 检查主机H1的路由表，确保有正确的默认网关设置，以便能够访问其他网络。
- 如果使用了网络地址转换（NAT）或代理服务器，确保其配置正确，并且允许通过转换或代理访问主机H1上的博客网站。

这些解决建议可以帮助排除网络层的问题，并确保主机H1上的博客网站能够被其他城市的同学访问。