下列什么设备可以隔离ARP广播帧

要隔离ARP广播帧，通常需要使用一些网络设备或配置来限制ARP广播的传播范围。以下是一些可以用来隔离ARP广播帧的设备和技术：

1. 交换机（Switch）

- **VLAN (虚拟局域网)**：通过将网络划分为不同的VLAN，可以在不同的VLAN之间隔离ARP广播帧。每个VLAN是一个独立的广播域，ARP广播只会在同一VLAN内传播。如果交换机支持VLAN功能，可以通过划分VLAN来限制ARP广播的范围。
- **Private VLAN**：某些高级交换机支持Private VLAN（PVLAN）功能，可以进一步隔离VLAN内部的ARP广播。这样，虽然设备处于同一VLAN内，但它们之间的ARP请求仍然不会互相广播。

2. 路由器（Router）

- **子网划分**：路由器通过将网络划分为多个子网来隔离不同的广播域，每个子网内的ARP广播只会影响同一子网内的设备。路由器会将ARP广播限制在每个子网内，而不会在不同子网之间传递。

3. ARP Proxy

- **ARP代理（ARP Proxy）**：在某些网络设备（如路由器或专用的ARP代理设备）中，可以启用ARP代理功能来替代真实设备响应ARP请求。ARP代理可以响应ARP请求，而不需要直接让ARP广播传播到网络的其他部分。

4. 防火墙（Firewall）

- **ARP过滤**：一些高级防火墙或网络安全设备可以设置规则来阻止或过滤ARP请求或应答，从而限制ARP广播帧在网络中的传播。这通常是在高安全要求的环境中使用。

5. ARP静态配置

- **静态ARP表**：在网络中的设备（如交换机、路由器）上，配置静态ARP表可以防止设备发送ARP请求。当设备已知某个IP地址对应的MAC地址时，ARP请求不再需要广播。

6. 网络隔离设备

- **网络隔离器（Network Isolation Device）**：这类设备可以通过硬件或软件手段将不同的网络区域进行隔离，防止广播、ARP等流量跨区域传播。

ICMP报文

ICMP 询问报文有 4 种类型：回送请求和回答报文、时间戳请求和回答报文、掩码地址请求和回答报文、路由器询问和通告报文，最常用的是前两类。

ICMP 的两个常见应用是分组网间探测 PING（用来测试两台主机之间的连通性）和 Traceroute（UNIX 中的名字，在 Windows 中是 tracert，可以用来跟踪分组经过的路由）。其中 PING 使用了 ICMP 回送请求和回答报文，Traceroute（Tracert）使用了 ICMP 时间超过报文。

注意：PING 工作在应用层，它直接使用网络层的 ICMP，而未使用传输层的 TCP 或 UDP。Traceroute/Tracert 工作在网络层。

与CSMA/CD网络相比，令牌环网更适合的环境是

与**CSMA/CD**（载波监听多路访问/冲突检测）网络相比，**令牌环网**更适合以下环境：

1. 高数据传输要求的环境

- **令牌环网**采用令牌传递机制（Token Passing），可以确保网络中只有一个设备在某一时刻发送数据，从而避免冲突。而**CSMA/CD**在高负载时容易发生冲突，并且每次冲突都需要重发数据，导致性能下降。因此，在需要高吞吐量、低延迟的环境中，令牌环网具有更好的性能。

2. 流量较为均衡的环境

- 在令牌环网中，令牌在环路中按顺序传递，确保了每个设备都有平等的机会发送数据。相比之下，**CSMA/CD**在网络繁忙时，设备可能会竞争发送，尤其是当网络中有很多设备时，冲突频繁发生，导致性能不稳定。因此，令牌环网适合那些流量比较均衡、不会有太多设备争夺带宽的环境。

3. 实时性要求较高的环境

- 由于令牌环网通过令牌机制控制访问，可以为每个设备提供公平的传输机会，因此适用于对实时性有较高要求的网络环境（如语音、视频等应用），而**CSMA/CD**网络容易受到冲突的影响，无法保证稳定的传输延迟，适应实时应用的能力较差。

4. 固定网络拓扑的环境

- 令牌环网通常需要一个固定的拓扑结构（环形拓扑），而且环内每个节点必须严格连接。相比之下，**CSMA/CD**可以在任意拓扑下工作，尤其适用于灵活性较高的环境。然而，如果环境中设备较为固定且拓扑要求严格，令牌环网的稳定性和效率通常更好。

5. 冲突较为敏感的环境

- **令牌环网**通过令牌机制消除了冲突的可能性，因为每次只有持有令牌的设备能够发送数据。而**CSMA/CD**在网络中存在冲突的可能，冲突会导致数据重传和延迟，适用于网络中设备较少或流量较轻的环境，但对于大型、繁忙网络可能导致性能下降。因此，令牌环网更适合对冲突敏感的环境，如数据中心、金融系统或需要高可靠性的大型企业网络。

6. 需要高可靠性的环境

- 令牌环网具有内置的可靠性机制，例如，当一个设备失败或网络中断时，环路的其他部分可以继续工作，令牌可以绕过故障节点继续传递。**CSMA/CD**网络在出现设备故障或网络问题时，可能会导致整个网络的冲突和性能下降。因此，令牌环网适用于需要高可靠性和容错的环境，如工业控制系统和军事通信。

7. 小型、封闭式的网络环境

- 令牌环网通常不适用于扩展性较强、动态变化的网络环境，因为它依赖于固定的物理环路结构。然而，在一个封闭的小型网络中，令牌环网可以较为高效地工作，特别是在设备数量不多且拓扑固定的情况下。对于这些环境，令牌环网的优势在于网络中数据传输的公平性和无冲突性。

总结

令牌环网相较于**CSMA/CD**网络，适用于需要高稳定性、高可靠性、实时性和公平性的数据传输环境，尤其在设备较为固定、拓扑稳定且对冲突敏感的场景下表现更为出色。尽管令牌环网的扩展性和灵活性不如CSMA/CD，但在特定的高要求环境下，它仍然是一个非常合适的选择。

无线局域网不适用CSMA/CD而是用CSMA/CA的原因

CSMA/CD 协议已经成功地应用于使用有线连接的局域网，但在无线局域网的环境下，却不能简单地搬运 CSMA/CD 协议。
主要有两个原因：
（1）接受信号的强度往往会小于发送信号的强度，且在无线介质上信号强度动态变化范围很广。因此若要实现碰撞检测，在硬件上的花费就会过大；
（2）在无线通信中，并非所有的站点都能够听见对方。而“所有站点都能够听见对方”正是实现 CSMA/CD 协议必备的基础。
CSMA/CD 协议的特点是：先听再发，边听边发，冲突停发，随机重发；
CSMA/CA 协议的特点是：发送数据时先广播告知其他结点，让其他结点在某段时间内不要发送数据，以免发生碰撞；

CSMA/CA和CSMA/CD对比

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 和 **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** 是两种用于多设备共享网络介质的访问控制

机制，它们的主要区别在于如何处理冲突。下面是这两种技术的对比：

1. 工作原理

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**:
  - **载波监听多路访问与冲突检测**：在CSMA/CD中，设备首先监听信道是否空闲（载波监听），如果信道空闲，设备就开始发送数据。如果多个设备在同一时刻发送数据，会发生**冲突**。当冲突发生时，设备能够检测到冲突信号，然后会停止发送数据，并等待随机的回退时间后再重新尝试发送。这种方式需要设备能够检测到冲突并采取适当的措施。
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:
  - **载波监听多路访问与冲突避免**：CSMA/CA是CSMA/CD的扩展，尤其用于无线网络。在CSMA/CA中，设备同样会监听信道是否空闲。如果信道空闲，设备会在发送数据前执行“冲突避免”步骤，通常通过发送一个小的控制帧（如**RTS**（请求发送）和**CTS**（清除发送））来通知网络其他设备自己即将发送数据。通过这种方式，设备可以避免冲突的发生。CSMA/CA的关键特点是，它**避免**冲突的发生，而不是像CSMA/CD那样在冲突发生后进行检测和处理。

2. 适用环境

- **CSMA/CD**:
  - CSMA/CD主要用于**有线网络**，如传统的以太网（Ethernet）。它适用于共享介质的有线网络环境，例如同轴电缆或早期的以太网环境。
  - 在有线网络中，由于信号传播速度较快，冲突检测可以实现得较为高效，即使发生冲突，设备可以通过检测冲突信号迅速停止发送数据。
- **CSMA/CA**:
  - CSMA/CA主要用于**无线网络**（如Wi-Fi）。在无线通信中，信号传播的物理特性使得**冲突检测**变得非常困难，因为无线信号在传播过程中会受到衰减、多径效应等因素的影响，设备无法像有线网络那样可靠地检测到冲突。
  - 由于无线设备通常不能同时发送和接收数据，因此无法检测冲突。因此，CSMA/CA采用了“冲突避免”的机制，避免在发送前就知道可能的冲突。

3. 冲突处理

- **CSMA/CD**:
  - **冲突检测**：在CSMA/CD中，当两个设备同时发送数据时，会发生冲突。冲突发生后，设备会停止发送，并通过回退算法（如**二进制指数回退**）等待随机的时间后重新尝试发送。这种方法能够有效减少冲突，但并不能完全避免冲突，尤其是在网络负载较高时，冲突的发生频率会增加。
- **CSMA/CA**:

- **冲突避免**：CSMA/CA采用不同的方式避免冲突。在发送数据前，设备会发送一个小的请求发送（RTS）控制帧，如果信道空闲，接收方会发送清除发送（CTS）帧，通知发送方可以开始发送数据。其他设备在收到CTS帧后，会避免在此时间段内发送数据，从而避免冲突的发生。CSMA/CA通过这种方式避免了冲突的发生，而不是通过检测冲突来进行处理。

4. 效率与性能

- **CSMA/CD**:
  - **优点**：在有线网络中，CSMA/CD能够高效地检测和处理冲突，适用于负载较低或中等的网络环境。在负载较低的情况下，冲突发生的概率较小，网络性能较好。
  - **缺点**：随着设备数量增加或网络负载增大，冲突发生的频率会显著增加，从而导致性能下降。每次发生冲突时，设备都需要回退并重新尝试发送，浪费了网络带宽。
- **CSMA/CA**:
  - **优点**：CSMA/CA在无线网络中非常有效，因为它通过避免冲突来提高网络效率。尤其是在有多个设备共享无线信道的环境中，CSMA/CA能够减少冲突，提供更稳定的网络性能。
  - **缺点**：由于采用了冲突避免机制，CSMA/CA在高负载情况下的延迟可能较高。特别是在设备数量众多时，为了避免冲突，设备可能会频繁地发送RTS/CTS控制帧，从而增加额外的开销。

5. 适用的网络技术

- **CSMA/CD**:
  - 主要应用于有线局域网（**Ethernet**）。例如，传统的以太网（10BASE-T、100BASE-TX等）使用CSMA/CD来控制数据传输和冲突。
- **CSMA/CA**:
  - 主要应用于无线局域网（**Wi-Fi**）。例如，Wi-Fi标准（如802.11）使用CSMA/CA来避免无线设备之间的冲突。

6. 冲突避免的机制

- **CSMA/CD**:
  - **冲突检测**：CSMA/CD通过监听和检测冲突来处理冲突。一旦检测到冲突，设备停止发送数据，等待随机时间后重新尝试。
- **CSMA/CA**:
  - **冲突避免**：CSMA/CA通过控制帧（RTS/CTS）来避免冲突。在无线环境中，由于设备无法同时发送和接收数据，设备事先通过RTS/CTS交换信号，确保在数据发送期间不会发生冲突。

7. 比较总结

特性	CSMA/CD	CSMA/CA
主要适用环境	有线局域网（Ethernet）	无线局域网（Wi-Fi）
冲突处理	冲突检测：冲突发生后停止发送并回退重试	冲突避免：通过RTS/CTS机制避免冲突
设备数量影响	高负载时冲突频繁，性能下降	更适合设备多、干扰较大的无线环境
性能与效率	适用于低到中等负载的有线网络，较高负载时性能下降	在无线环境中能有效避免冲突，提供较为稳定的性能
延迟	在发生冲突时会增加延迟	通过控制帧避免冲突，但可能增加额外延迟
冲突检测/避免机制	冲突检测和回退	冲突避免（RTS/CTS）
适用的网络技术	以太网（Ethernet）	Wi-Fi（802.11）

总结：

- **CSMA/CD**适用于有线网络，能够高效地处理冲突，但随着网络负载增加，性能会受到影响。
- **CSMA/CA**则适用于无线网络，通过避免冲突来提高效率，在设备多和信号干扰较大的环境中表现更好。由于无线信道的特殊性，CSMA/CA不使用冲突检测，而是通过控制帧（如RTS/CTS）来减少冲突的概率。

广播地址与子网地址

计算方法：广播地址是通过将网络地址的主机部分（即子网掩码为`0`的部分）设置为全`1`来计算的。例如：

- 网络地址：`192.168.1.0/24`
- 子网掩码：`255.255.255.0`
- 广播地址：`192.168.1.255`

子网的**网络地址**是由子网掩码确定的，其主机部分全为0。

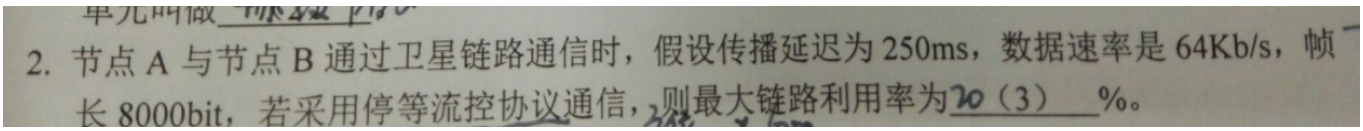
FTP和TFTP区别

1. 交互使用 FTP。 TFTP 允许仅单向传输的文件。
2. FTP 提供身份验证。而 TFTP 不。
3. FTP 使用已知 TCP 端口号： 20 的数据和 21 用于连接对话框。 TFTP 用于 UDP 端口号 69， 其文件传输活动。
4. 因为 TFTP 不支持验证 WindowsNT ， 所以 FTP 服务器服务不支持 TFTP。
5. FTP 依赖于 TCP，是面向连接并提供可靠的控件。 TFTP 依赖 UDP，需要减少开销, 几乎不提供控件。

IPV4路由器收到哪些数据包会丢弃

- IPV6格式的包
- TTL为0
- 目的不可达
- 首部检验和出错
- 路由器中队列长度超过最大门限
- 受限广播

信道利用率


2. 节点 A 与节点 B 通过卫星链路通信时，假设传播延迟为 250ms，数据速率是 64Kb/s，帧长 8000bit，若采用停等流控协议通信，则最大链路利用率为 20（3） %。

2、【20】
8Kb/64Kbps=125ms
125ms / (125+250+250)ms

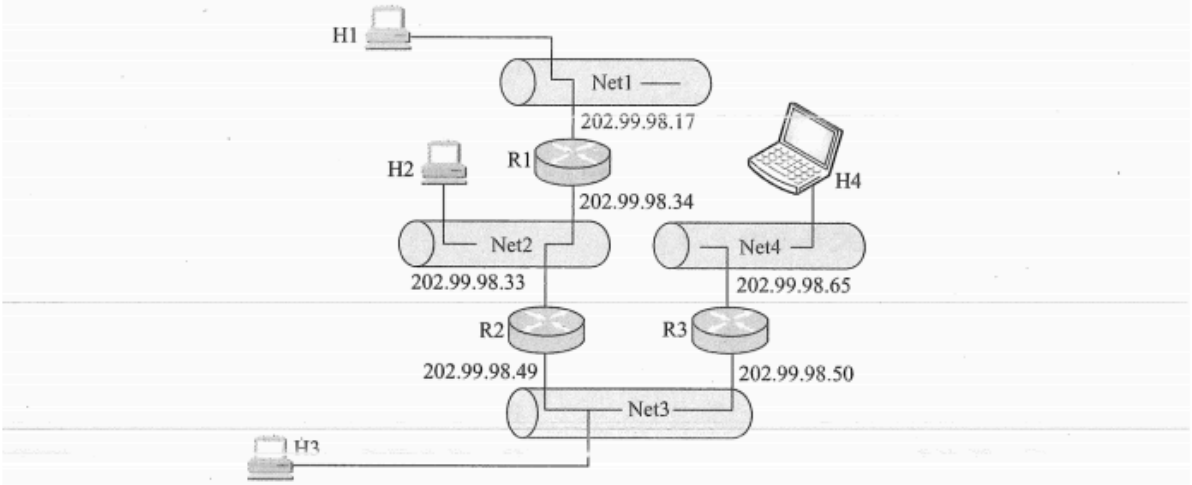
信道利用率。指出某一信道有百分之多少的时间是有数据通过的，即信道利用率 = 有数据通过时间 / (有+无) 数据通过时间。

路由器转发表大题

目的地址要写网络地址，不要写成具体地址了，写好过程

【例题】

1. 某个单位的网点由 4 个子网组成，结构如下图所示，其中主机 H1、H2、H3 和 H4 的 IP 地址和子网掩码见下表。



主　机	IP 地址	子 网 掩 码
H1	202.99.98.18	255.255.255.240
H2	202.99.98.35	255.255.255.240
H3	202.99.98.51	255.255.255.240
H4	202.99.98.66	255.255.255.240

1）请写出路由器 R1 到 4 个子网的路由表。

2）试描述主机 H1 发送一个 IP 数据报到主机 H2 的过程（包括物理地址解析过程）。

1）将 H1、H2、H3、H4 的 IP 地址分别与它们的子网掩码进行“与”操作，可得到 4 个子网的网络地址，分别为 202.99.98.16、202.99.98.32、202.99.98.48、202.99.98.64，因此路由器 R1 到 4 个子网的路由表见下表。

目 的 网 络	子 网 掩 码	下　一　跳
202.99.98.16	255.255.255.240	直接
202.99.98.32	255.255.255.240	直接
202.99.98.48	255.255.255.240	202.99.98.33
202.99.98.64	255.255.255.240	202.99.98.33

2）主机 H1 向主机 H2 发送一个 IP 数据报的过程如下：① 主机 H1 首先构造一个源 IP 地址为 202.99.98.18、目的 IP 地址为 202.99.98.35 的 IP 数据报，主机 H1 先把本子网的子网掩码与 H2 的 IP 地址逐位相与，所得结果不等于 H1 的 网络地址，因此 H1 与 H2 不在同一子网，无法直接交付，然后将该数据报传送给数据链路层。

② 主机 H1 通过 ARP 获得路由器 R1（202.99.98.17）对应的 MAC 地址，并将其作为目的 MAC 地址，将 H1 的 MAC 地址作为源 MAC 地址填入封装有 IP 数据报的帧，然后将该帧发送出去。

③ 路由器 R1 收到该帧后，去除帧头与帧尾，得到 IP 数据报，然后根据 IP 数据报中的目的 IP 地址（202.99.98.35）去查找路由表，得到下一跳地址为直接相连。

④ 路由器 R1 通过 ARP 得到主机 H2 的 MAC 地址，并将其作为目的 MAC 地址，将 R1 的 MAC 地址作为源 MAC 地址填入封装有 IP 数据报的帧，然后将该帧发送到子网 Net2 上。

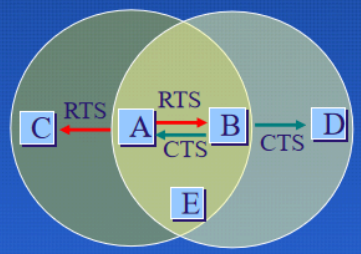
⑤ 主机 H2 将收到的帧，去除帧头与帧尾，并最终得到从主机 H1 发来的 IP 数据报。

RTS和CTS的作用

3-21 (教材习题9-09)：RTS和CTS的作用

- 在发送长数据帧之前先对信道进行预约：
  - 发送方A：先发送请求发送帧 （RTS，Request t
  - 目的方B：响应一个允许发送帧 （CTS，Clear to Send）

选择使用：
✓永远使用
✓永远不使用
✓仅当长数据帧前使用



A的传输范围 B的传输范围

- 附近一些站的反应：

站C：只收到RTS，可以发送数据（不会干扰B）

站D：只收到CTS，在B发送数据的过程中不能发送数据

站E：能同时收到RTS和CTS，因此在A发送数据帧的整个过程中都不能发送数据

滑动窗口

- 主机A数据链路层按滑动窗口协议工作，某时刻A的接收窗口如下图所示，此时收到5号帧和6号帧，则主机A将如何处理5号和6号帧（缓冲还是丢弃）？发出的确认帧的确认号会是什么？（提示：确认号是期望收到的下一帧的序号

- **收到 5 号帧**：
  - 5 号帧在接收窗口范围内，因此主机 A 会 **接受并缓存** 该帧，但如果前面的帧（2、3、4）没有收到，则无法移动窗口。
- **收到 6 号帧**：
  - 6 号帧超出了当前接收窗口的范围（窗口为 2-5），因此主机 A 会 **丢弃 6 号帧。**
- **确认号的定义**：确认号是接收方 **期望收到的下一帧的序号。**
- 当前窗口从 2 开始，但 2 号帧尚未收到，因此确认号仍然是 **2。**

编码方式的同步能力指的是什么?

- **定义**：编码方式的同步能力是指数据传输过程中发送方与接收方在时钟频率和数据边界上的同步能力。它确保接收方能够准确地识别数据流中的比特和帧边界。
- **作用**：良好的同步能力可以减少误码率，保证数据的正确传输。

总线型、星型、环型、网格型拓扑结构中，不能支持点对点通信方式的拓扑结构是哪一种?

- **答案**：**总线型拓扑结构。**
- **原因**：总线型拓扑中所有节点共享一条传输介质，通信以广播的形式进行，不能直接实现点对点通信。

什么是多跳转发网络？给出一个多跳转发通信的例子，并给出保证可靠性的思路。

- **定义**：多跳转发网络是指数据包在发送方和接收方之间，需要经过多个中间节点（路由器或交换机）转发才能到达目的地。
- **例子**：在一个分布式的无线传感器网络中，节点 A 想与节点 D 通信，但两者之间没有直接连接，则数据需要通过节点 B 和 C 的转发才能到达节点 D。
- **保证可靠性的思路**：

1. **确认机制**：每个节点在转发时发送确认信息，确保数据被正确接收。
2. **路径选择**：采用动态路由协议（如 DSR 或 AODV）选择最优路径。
3. **重传机制**：如果某节点未收到确认，则重新发送数据。
4. **冗余路由**：预先规划备用路由，防止单点故障。

两台具有8个端口的HUB通过一根双绞线互连，则它们的冲突域有几个？广播域呢？将HUB换成交换机或路由器以后呢?

- **两台HUB通过双绞线互连**：
  - **冲突域**：两台 HUB 相互连接后，形成了一个共享冲突域。因此整个网络是一个大的冲突域。
  - **广播域**：HUB 是物理层设备，不分割广播域，因此整个网络仍是一个广播域。
- **换成交换机**：
  - **冲突域**：交换机分割冲突域，每个端口是一个单独的冲突域。如果每个端口接一个设备，共有 **16 个冲突域**。
  - **广播域**：交换机工作在数据链路层，不分割广播域，因此整个网络仍是一个广播域。
- **换成路由器**：
  - **冲突域**：路由器的每个接口连接一个网络，因此与交换机类似，也可以分割冲突域。
  - **广播域**：路由器分割广播域，每个接口是一个独立的广播域，因此有 **2 个广播域**。

路由器分割广播域，交换机和路由器分割冲突域，HUB什么都不分割

用流程图的形式说明IEEE802.3协议的工作过程。

只要知道是CSMA/CD就知道怎么答了

IEEE 802.3 是以太网协议，支持 CSMA/CD（载波监听多路访问/冲突检测）机制。流程如下：

1. 监听信道是否空闲：
   - 如果信道空闲，开始发送数据；
   - 如果信道忙，等待信道空闲。
2. 开始发送数据。
3. 检测冲突：
   - 如果发生冲突，停止发送，并发送冲突信号；
   - 等待一段随机时间后重试。
4. 如果无冲突，完成数据发送。
5. 确认发送成功。

(n)PDU加上什么封装成(n-1)PDU?

加上 **控制信息（Header 和 Trailer）** 封装成 (n-1)PDU。
加上协议控制信息PCI

计算机网络的分层结构

在计算机网络的分层结构✦中，第n层的活动元素通常称为第n层实体。
实体指任何可发送或接受信息的硬件或软件进程，通常是一个特定的软件模块。不同机器上的同一层称为对等层✦，同一层的实体称为对等实体。
第n层实体实现的服务为第n + 1层所利用。在这种情况下，第n层称为服务提供者，第n + 1层则服务于用户。
每个报文✦分为两个部分，数据部分SDU，控制信息部分PCI，共同组成PDU。
各层传输数据时，把从第n+1层收到的PDU 作为第n层的SDU，加上第n层的PCI，就变成了第n层的PDU，交给第n - 1层后作为SDU发送，接受法接受时做相反处理。

$$SDN_n + PCI_n = PDU_n = SDU_{n-1}$$

1. 第n层的实体不仅要使用第n-1层的服务来实现自身定义的功能，还要向第n+1层提供本层的服务，该服务是第n层及其下面各层提供的服务总和。
2. 最低层只提供服务，是整个层次结构的基础；中间各层既是下一层的服务使用者，又是上一层的服务提供者；最高层面向用户提供服务。
3. 上一层只能通过相邻层间的接口使用下一层的服务，而不能调用其他层的服务；下一层所提供服务的实现细节对上一层透明。
4. 两台主机通信时，对等层在逻辑上有一条直接信道，表现为不经过下层就把信息传送到对方。

一句话知识点

快速以太网中的“快速”是指数据速率可以达到 100Mbps，是标准以太网数据速率的十倍。

网络协议三要素：语法、语义、同步