==========应用层==========

Q1 什么是应用层协议？举例说明其作用。

答案：负责为用户提供各种网络应用服务。常见的应用层协议包括 HTTP（用于 Web 浏览）、SMTP（用于电子邮件传输）、FTP（用于文件传输）和 DNS（用于域名解析）。

Q2 什么是域名系统（DNS），它的主要功能是什么？

答案：域名系统（DNS）是一种分布式数据库系统，它的主要功能是域名解析，工作原理上，当用户在浏览器中输入一个域名时，浏览器会向 DNS 服务器发送一个查询请求；DNS 服务器根据域名的层次结构逐级查询，最终找到与该域名对应的 IP 地址，并将其返回给浏览器；浏览器根据返回的 IP 地址与对应的服务器建立连接，完成网页的加载。

Q3 什么是 Cookie，HTTP Cookie 的主要用途是什么？

答案：Cookie 是一小段数据，由服务器发送并存储在客户端浏览器中。由于 http 是 stateless 的，所以其主要功能是帮助服务器回忆与该用户曾经的链接状态，Cookie 的主要用途包括会话管理（如用户登录状态）、个性化设置（如语言选择）、和跟踪用户行为（如广告投放）。

Q4：请解释 HTTP 请求中的 GET 和 POST 方法的区别。

Q4: Please explain the difference between the GET and POST methods in HTTP requests.

答案：GET 方法用于请求获取指定的页面信息，而 POST 方法用于提交表单数据，数据包含在请求体中，如网页里的留言板。HEAD 的应用之一是搜索引擎，例如一个搜索引擎发出爬虫请求各食品网页，返回的包的头部里的信息，就可以用作未来搜索引擎展示给用户的搜索结果。

Q5 应用程序需要什么样的运输服务?

Q5 What transport service does an app need?

data integrity 例如，文件传输，网络交易等 app。需要 100%可靠的数据传输
Throughput 如有些应用需要高吞吐量服务，即保证最大化单位时间内的数据传输量，如大文件传输、视频点播服务。
Timing 如语音电话需要 delay 要小
Security 如安全加密，数据没被篡改

Q6 CDN 是什么？

Content Delivery Network，内容分发网络）是一种分布式网络基础设施，用于提高互联网内容的传输速度和可靠性。它通过将内容缓存到靠近用户地理位置的服务器上，使用户可以更快地访问网站、视频、图片等资源。

Q7 简单描述 Socket 在网络编程中的作用及其基本工作流程？

Q7 Briefly describe the role of Socket in network programming and its basic workflow?

答案：

创建 Socket： 在客户端和服务器上创建 Socket 对象。

绑定地址和端口（服务器端）： 服务器将 welcome Socket 绑定到一个指定的地址和端口。

监听连接（服务器端）： 服务器开始监听来自客户端的连接请求。

发起连接（客户端）： 客户端尝试连接到服务器的地址和端口。

接受连接（服务器端）： 服务器接受客户端的连接请求，并会产生一个 connection socket。

数据传输： 客户端通过第一步里创建的 Socket 进行通信，服务器用 connection socket 跟对应的客户进行通信

关闭连接： 通信完成后，客户端和服务器关闭 Socket 以释放资源。

Q8 HTTP 和 HTTPS 的区别是什么？

答案：HTTP（HyperText Transfer Protocol）和 HTTPS（HyperText Transfer Protocol Secure）的主要区别在于安全性。HTTP 数据以明文形式传输，而 HTTPS 使用 SSL/TLS 协议加密数据，确保数据的保密性和完整性。

Q9 简述一下网络中 5 层结构中每一层数据在封装后的叫法及组成。

Q9 Briefly describe the name and composition of each layer of data in the 5-layer structure in network after encapsulation.

答案：

Application-layer message

Transport layer segment

Network-layer datagram

Link-layer frame

每一层中，一个分组都是由两个类型的字段组成，1.首部字段（header field）2.载荷字段（payload field）,有效载荷都是来自于上一层的分组。

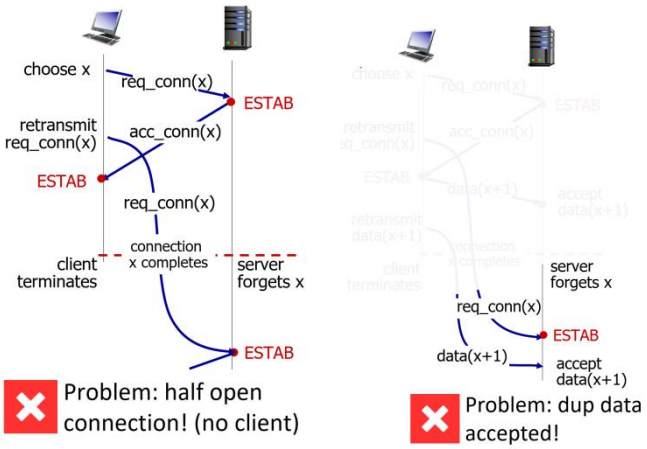
Q10 电子邮件协议有哪些？

Q10 What are the email protocols?

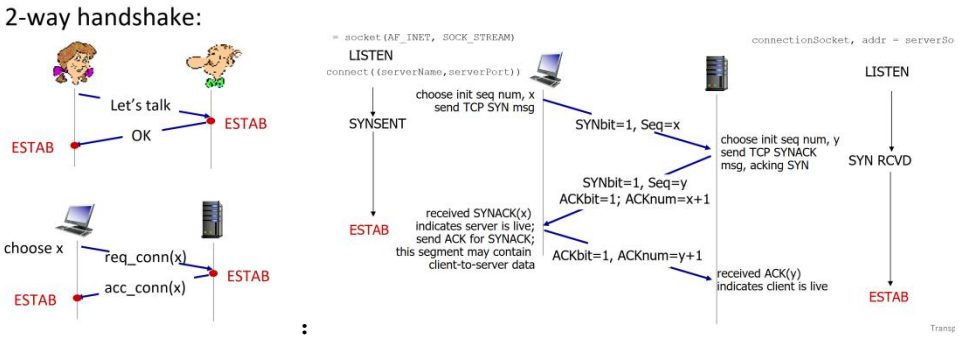
答案：常见的有 SMTP、POP3 和 IMAP

==========**传输层**==========

解决了两次握手中的：



两次握手：　　三次握手



：

Q1：请简述传输层的主要功能是什么？

Q1: What are the main functions of the transport layer?

答案：传输层的主要功能是为两台主机上的应用程序提供端到端的通信服务。具体来说，传输层将来自应用层的数据分割成合适大小的数据段，并在接收端进行重组；同时，它还通过一系列机制确保数据的可靠传输，防止数据丢失或乱序。

Q2：请解释 TCP 和 UDP 的主要区别。

答案：TCP 是面向连接的协议，提供可靠的数据传输服务，通过确认和重传机制确保数据的完整性和顺序；而 UDP 则是无连接的协议，不保证数据的可靠传输，但具有较低的传输延迟。

Q3：TCP 的三次握手过程是怎样的？

Q3: What is the 3-wave handshake of TCP?

答案：TCP 的三次握手过程是为了在客户端和服务器之间建立可靠的连接。首先，客户端向服务器发送一个 SYN 包，请求建立连接；服务器收到 SYN 包后，回复一个 SYN+ACK 包，表示同意建立连接并请求客户端确认；最后，客户端再发送一个 ACK 包，确认收到服务器的 SYN+ACK 包，至此三次握手完成，连接建立成功。

Q4：TCP 的四次挥手过程是怎样的？

Q4: What is the four-wave handshake of TCP?

答案：TCP 的四次挥手过程用于关闭一个已经建立的连接。首先，客户端向服务器发送一个 FIN 包，请求关闭连接；服务器收到 FIN 包后，回复一个 ACK 包，表示收到客户端的关闭请求；然后，服务器发送一个 FIN 包给客户端，表示自己也准备关闭连接；最后，客户端回复一个 ACK 包给服务器，确认收到服务器的 FIN 包，至此四次挥手完成，连接关闭。

Q5：TCP 是如何保证数据传输的可靠性的？

Q5: How does TCP ensure the reliability of data transmission?

答案：

1. 使用序列号对数据包进行编号，以便在接收端进行重组和排序；
2. 使用确认和重传机制确保每个数据包都被正确接收；
3. 使用流量控制机制防止发送方发送过多数据导致接收方缓冲区溢出；
4. 使用拥塞控制机制避免网络拥塞导致的数据丢失。

Q6：请解释 TCP 的流量控制机制。

Q6: Explain the TCP flow control mechanism.

答案：TCP 的流量控制机制是通过滑动窗口来实现的。发送方和接收方各维护一个窗口，窗口的大小表示接收方当前可用的缓冲区空间。

发送方在发送数据时，会检查接收方的窗口大小，确保发送的数据量不会超过接收方的处理能力。

接收方在缓冲区空间不足时，它会缩小窗口大小并通知发送方，发送方则根据新的窗口大小调整发送速率，从而实现了流量控制。

Q7：什么是 TCP 的拥塞控制？

Q7: What is congestion control in TCP?

答案：TCP 的拥塞控制是为了防止过多的数据包注入网络导致拥塞，

例如

1. 当发送方连续收到多个重复确认，即冗余 ack 时，它会认为网络发生了拥塞并降低发送速率；
2. 当发送方检测到超时事件，即 time out 时，它会认为网络拥塞严重并大幅度降低发送速率。这些措施有助于维护网络的稳定性和性能。

Q8：请简述 UDP 的应用场景。

Q8: Please describe the application scenarios of UDP.

答案：UDP 主要适用于那些对实时性要求较高而对数据完整性要求相对较低的应用场景。例如，在线视频、音频流、实时游戏等应用通常使用 UDP 作为传输层协议。此外，一些简单的服务或查询请求也可能使用 UDP 作为传输层协议，因为它们不需要建立复杂的连接和进行复杂的错误处理。

Q9：在传输层中，如何实现数据的加密和安全性？

Q9: How to implement data encryption and security in the transport layer?

答案：在传输层实现数据的加密和安全性通常依赖于 SSL/TLS 等安全协议。这些协议在传输层和应用层之间建立了一个安全通道，这些协议在握手阶段协商加密算法和密钥，并在后续的数据传输阶段使用这些算法和密钥对数据进行加密和解密。

Q10：假设主机 A 通过 TCP 连接向主机 B 反向发送两个 TCP 段。第一片段的序号为 90;第二种序列号为 110。

a. 第一个段数据是多大?

b.假设第一个报文段丢失了，但是第二个报文段到达了，b 在主机 b 发送给主机 A 的确认中，确认号是多少?

Suppose Host A sends two TCP segments back to back to Host B over a TCP connection. The first segment has sequence number 90; the second has sequence number 110.

a. How much data is in the first segment?

b. Suppose that the first segment is lost but the second segment arrives at B. In the acknowledgment that Host B sends to Host A, what will be the acknowledgment number?

答案：

A.20 bytes 的数据

B.发送确认号为 90 的 ACK 报文

Q11：UDP 和 TCP 怎样做校验和的。举例有 3 个 4 比特的 1100，1010，1001

Q11: How to do the checksum of UDP and TCP. For example, there are three 4-bit 1100s,

答案：

1010,1001

UDP 和 TCP 使用反码作为校验和，首先将上述 3 个 4 比特的求和

1100

1010

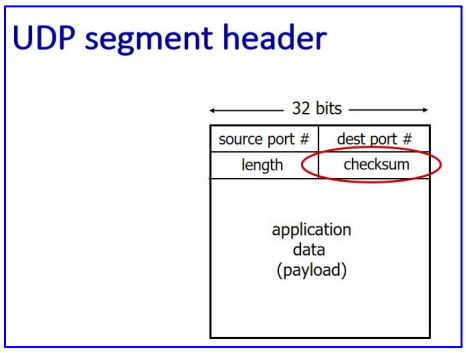
求和结果是 0111，注意最高位有回卷

0111

1001

求和结果是 0001,溢出回卷同理

将 0001 的反码 1110 放入 tcp 和 udp 的 header 的 checksum 字段中，如下图 udp 的 header 结构



最终接收方将全部的 4 个 4 比特字（3 个原始+1 个 checksum 字段）求和，若没出错则为全 1，有 0 出现表明有出错

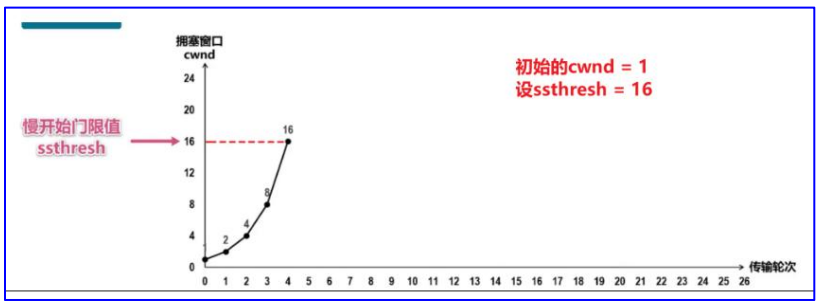
Q12 题：简述 tcp 拥塞算法基本原则，简述 tcp 拥塞算法中的慢启动、拥塞避免、快速重传、快速恢复的意思

Q12: Briefly describe the basic principles of tcp congestion algorithm, and briefly describe the meaning of slow start, congestion avoidance, fast retransmission, and fast recovery in tcp congestion algorithm

tcp 拥塞算法是通过对拥塞窗口（cwnd）的控制，基本原则是，通过收到 3 个冗余 ack 和丢失报文段来判断是否产生拥塞，通过带宽探测，不断试探 cwnd 的合理值。

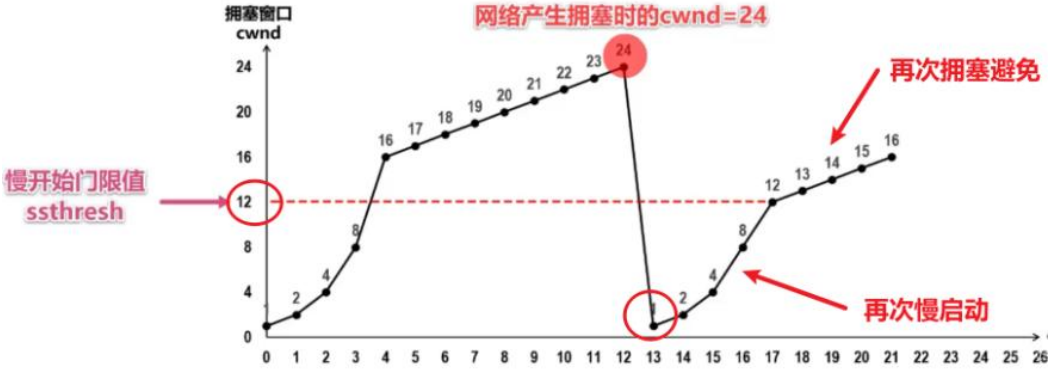
慢启动（Slow Start）：

慢启动是 TCP 连接刚开始发送数据时采用的一种策略，以指数方式增加速率，1，2，4，8....，以便探测网络的可用带宽。



拥塞避免（Congestion Avoidance）：

其目的是在网络出现拥塞时，减缓数据包的发送速率，避免进一步加剧拥塞。Cwnd 为上次遇到拥塞时的一半，此时缓缓试探，即此时 cwnd 的值为 1 个 mss 的速度增加。



快速重传

让发送方尽快重传，而不是等待超时重传计时器超时再重传。

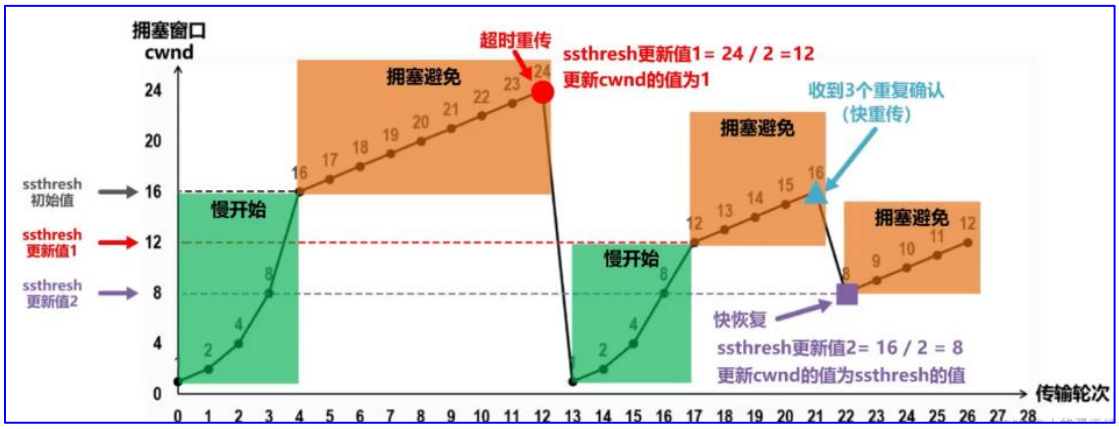
即发送方一旦收到 3 个连续的重复确认，就将相应的报文段立即重传，而不是等待该报文的重传计时器超时再重传。

快速恢复（Fast Recovery）

如果发送方收到了 3 个冗余 ack，就执行快恢复算法

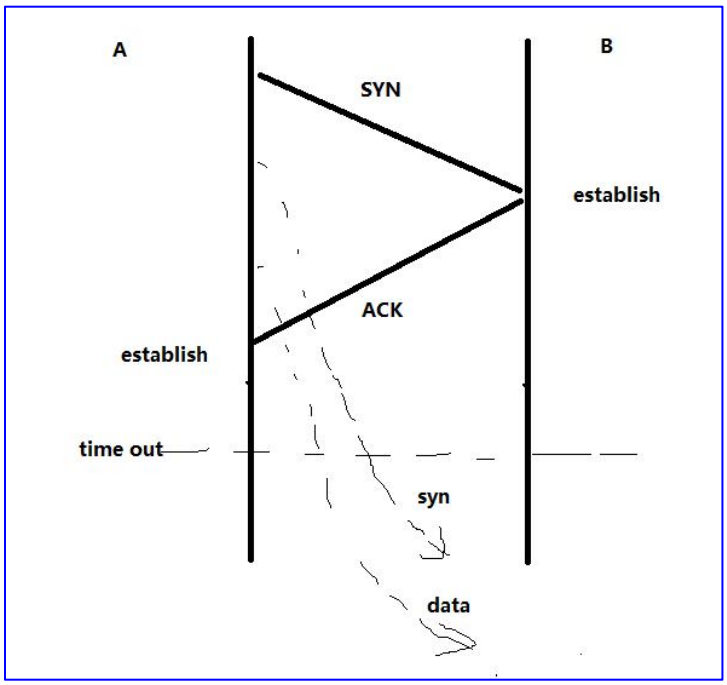
将 sstresh 和 cwnd 都设置为当前拥塞窗口的一半，然后执行拥塞避免算法.

综合图例



Q13：请画出 2 次握手的时序图，并说出它的缺点是什么，且简述三次握手。

Q13: Please draw the timing diagram of the 2-way handshake, and say what its disadvantages are, and briefly describe the 3-way handshake.



缺点及三次握手如前面几题的描述

Q14：什么是端口号？在 TCP 和 UDP 中如何使用？

Q14: What is a port number? How is it used in TCP and UDP?

端口号用于标识传输层的不同应用程序。TCP 和 UDP 都使用端口号来区分不同的应用连接，如区分微信，网页等应用。客户端通常使用动态端口，服务器使用固定端口。

==========网络层==========

Q1：请解释什么是 IP 地址

答案：

传统的 IPv4 地址分为五类：A 类、B 类、C 类、D 类和 E 类。

后出现 CIDR（无类别域间路由），是一种用于分配 IP 地址和构造路由表的 IP 地址分配方法。它消除了传统的 A、B、C 类网络划分的概念，允许更灵活和高效的 IP 地址分配。CIDR 使用斜线记法（如 192.168.1.0/24）来表示网络前缀的长度。

Q2：请描述子网掩码的作用是什么？

Q2: Please describe what a subnet mask does?

答案：子网掩码用于划分 IP 地址中的网络部分和主机部分。它通过与 IP 地址进行逻辑与运算，来确定一个 IP 地址所属的网络地址。即子网掩码也可以说能够帮助确定几个 ip 是否属于同一个局域网。

Q3：什么是 CIDR（无类别域间路由）的工作原理是什么？

Q3: What is CIDR (Classless Interdomain Routing) and how does it work?

答案：

Ip 格式：

在 CIDR 中，IP 地址与子网掩码一起使用，子网掩码决定了网络部分和主机部分的划分。例如：192.168.0.0/24 的子网掩码是 255.255.255.0。

地址块分配：

ISP 可以分配一个较大的地址块（如 192.168.0.0/22），然后再将其划分为多个更小的子网分配给客户（如 192.168.0.0/24、192.168.1.0/24 等）

路由聚合：

路由器可以将多个相邻的子网聚合为一个更大的路由项。例如，192.168.0.0/24 和 192.168.1.0/24 可以聚合为 192.168.0.0/23

Q4：什么是路由？请解释静态路由和动态路由的区别。

Q4: What is routing? Explain the difference between static routes and dynamic routes.

答案：

路由是指数据包在网络中从源节点到目标节点所经过的路径选择过程。

静态路由是手动配置的路由信息，管理员根据网络拓扑结构手动指定每个路由条目,例如我们机房实验中手动配置的吓一跳。

动态路由则是路由器之间通过路由协议（如 OSPF、BGP 等）交换路由信息，自动计算并选择最佳路径。

Q5：请描述 ICMP 协议的主要功能。

答案：其主要功能包括报告 IP 数据包的传输错误（如目的不可达、超时等），以及进行网络探测和诊断（如 ping 命令就利用了 ICMP 协议）。

Q6：什么是 NAT（网络地址转换）？它有什么作用？

答案：NAT（网络地址转换）是一种在 IP 地址私有和公有之间转换的技术。它允许一个私有 IP 地址的网络（如家庭或企业内部网络）通过公共 IP 地址连接到互联网，例如你家的网络，只有一个公有 ip，但是你的 pad，手机，电脑等拥有转换后的私有地址。NAT 有助于缓解 IPv4 地址空间不足的问题。

Q7：什么是 MTU（最大传输单元）？它在网络层中的作用是什么？

Q7: What is MTU (Maximum Transmission Unit)? What is its role in the network layer?

答案：MTU（Maximum Transmission Unit）是网络层可以传输的最大数据包大小。数据报（datagram）如果超过 MTU，需要进行分片。分片是为了适应不同网络链路的 MTU，确保数据包能够传输到目的地而不被丢弃。

Q8：考虑向具有 700 字节 MTU 的一条链路发送一个 2400 字节的数据报。假定初始数据报标有标识号 422。将会生成多少个分片？在生成相关分片的数据报中各个字段的值是多少？

Consider sending a 2400-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are

generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?

最大传输单元(MTU)为 700 字节，其中要包含 20 个字节的 IP 首部，能够存放 680 字节的数据。数据报为 2400 字节，除去 20 字节的 IP 首部，共有 2380 字节的数据。

则分片的个数为 2380/680=4。

四个分片的标识号均为 422，

片偏移字段分别购 0、85、170、255，

标志分别为 1、1、1、0（标志分片是否是最后一片，0 代表是最后一片）

Q9：什么是 OSPF？简述其工作原理。

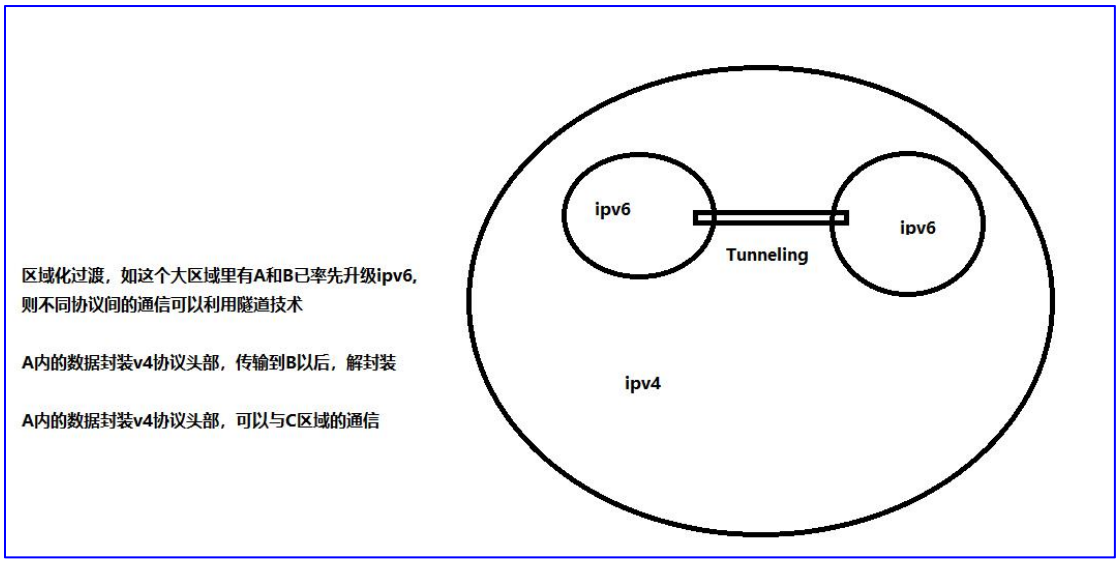
答案： OSPF（Open Shortest Path First）是一种（link state）链路状态路由协议，使用 Dijkstra 算法计算最短路径。

Q10：DHCP 是什么

用于自动分配 IP 地址和其他网络配置参数（如子网掩码、默认网关和 DNS 服务器）给网络中的设备。在宽带路由器上一般有 DHCP 服务，而且在默认情况下是开启的。

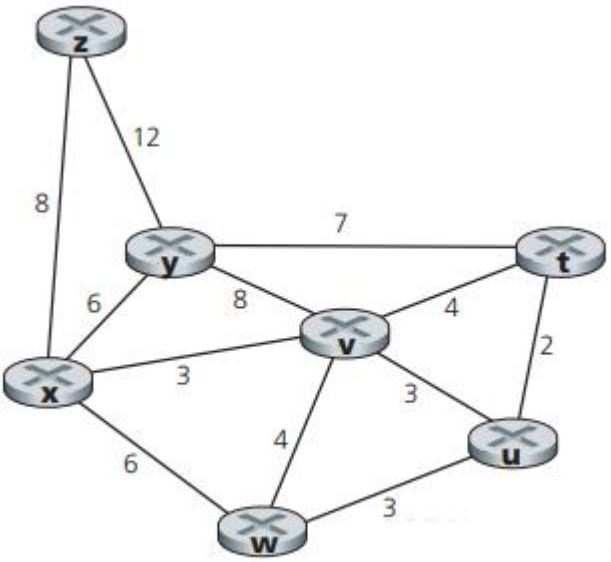
Q11：全球范围内，是如何利用隧道协议将 ipv4 过渡成 ipv6 的？

Q11: How is the transition from ipv4 to ipv6 using the tunneling protocol globally?



Q12：下图拓扑图使用 dijkstra 计算从 x 到所有网络节点的最短路径。

Q12The following topology uses dijkstra to calculate the shortest path from x to all network nodes.



解:

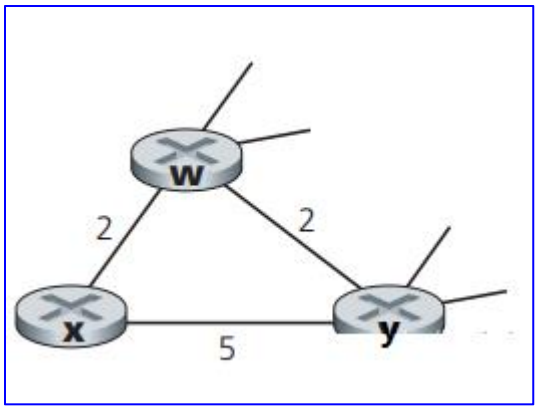
步骤	N'	$D(t),p(t)$	$D(u),p(u)$	$D(v),p(v)$	$D(w),p(w)$	$D(y),p(y)$	$D(z),p(z)$
0	x	∞	∞	3,x	6,x	6,x	8,x
1	xv	7,v	6,v		6,x	6,x	8,x
2	xvu	7,v			6,x	6,x	8,x
3	xvuw	7,v				6,x	8,x
4	xvuwy	7,v					8,x
5	xvuwyt						8,x
6	xvuwytz						

Q13：下面拓扑图，x 只有两个相连邻居 w 与 y。w 有一条通向目的地 u(没有显示）的最低开销路径，其值为 5， y 有一条通向目的地 u 的最低开销路径，其值为 6。从 u 与 y 到 u(以及 w 与 y 之间）的完整路径未显示出来。

注意：拓扑中所有链路开销皆为正整数值，更新后若代价相同不通知。

Q13: In the following topology, x has only two neighbors w and y. w has a lowest-cost path to destination u(not shown) with a value of 5, and y has a lowest-cost path to destination u with a value of 6. The full path from u and y to u(and between w and y) is not shown.

Note: All link costs in the topology are positive integer values. If the cost is the same after the update, no notification is given.



a. 给出 **x** 对目的地 **w**、**y** 和 **u** 的距离向量。

b. 给出对于 **c(x，w)**使得执行了距离向量算法后，**x** 将通知其邻居有一条通向 **u** 的新最低开销路径。

c. 给出对 **c(x,y)**的链路开销的变化，使得执行了距离向量算法后，**x** 将不通知其邻居有一条通向 **x** 的新最低开销路径。

答案：

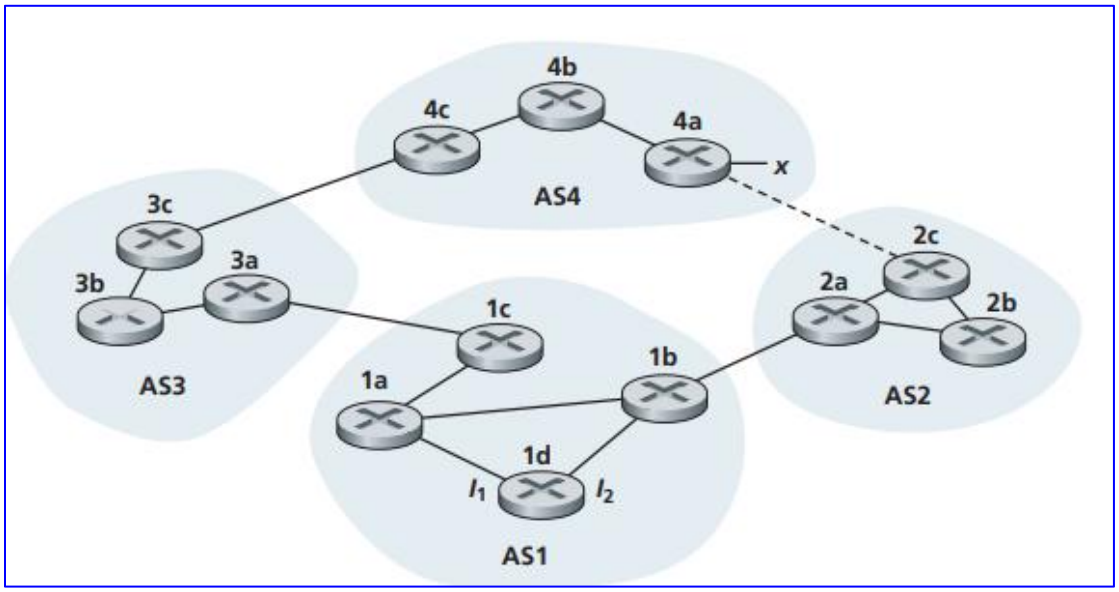
a) $D_x(w) = 2, D_x(y) = 4, D_x(u) = 7$
b) 对于c(x,w)，c(x,w)>6

c) c(x,y)变为任意值，都不能改变最低开销路径

Q14：拓扑图如下，现位于 AS1 中的 1d 想要取 AS4 中的 X
a. 若虚线位置不通，请问 3a 是用什么协议将通往 x 的路由信息告诉 1c 的？
b. 1c 如何是用什么协议将通往 x 的路由信息告诉 1d 的？
c. 若 AS2 与 AS4 之间的虚线接通了，则决定 1d 到 x，到底是通过 1c 还是 1b，取决于什么？
d. 若 c 题里，对 1c 和 1b 的出口端评估是一样的话，则应该选 1c 还是 1b 呢？
e. 若 1c 和 1b 是连着的，且之前所有评估都是均衡的，现已确定我们需要从 1c 端口出去，则在 1d 中，我们应该选择 I1 还是 I2？

Q14: The topology is as follows, 1d now in AS1 wants to take X in AS4
a. If the dotted line is unavailable, what protocol does 3a use to tell 1c the routing information to x?
b.1c How does the protocol Used to tell 1d about the route to x?
c. If the dotted line between AS2 and AS4 is connected, what determines whether 1d to x passes through 1c or 1b?
d. If the exit evaluation of 1c and 1b in question c is the same, should 1c or 1b be chosen?
e. If 1c and 1b are connected, and all previous evaluations have been balanced, and it has been

determined that we need to exit the 1c port, should we choose l1 or l2 in 1d?



答案：

A. ebgp

B. ibgp

C. 取决于政策，偏向于本地属性偏好，例如经济属性偏好，竞争属性偏好

D. 用 1b，因为 AS 内跳数更少

E. 取决于 l1 和 l2 的 cost 哪个小，基于热土豆原理，烫手早点扔出去。

Q15：TTL，RTT 是什么

答案：

TTL（Time to Live）是一个字段，存在于 IP 包头中，用于限制数据包在网络中的存活时间。它的目的是防止数据包在网络中无限循环，从而避免网络拥塞。例如 ping 包中的 icmp 协议里的 ttl 为 3，则数据包的存活时间为 3 跳。

RTT（Round-Trip Time）从源端到目标端的往返时延。

==========链路层==========

数据链路层

1. 三个基本概念：

封装成帧

透明传输

差错检测

2. 多点接入 csma/cd， csma/ca（主要应用于无线领域）

3. Mac 地址

链路及帧

①链路（link）是一条无源的点到点的物理线路段，中间没有任何其他的交换结点。

A link is a passive point-to-point physical line segment without any other switching nodes in the middle.

一条链路只是一条通路的一个组成部分。

A link is only one component of a path.

②封装成帧(framing)就是在一段数据的前后分别添加首部和尾部,然后就构成了一个帧。

framing is to add a header and a tail before and after a piece of data, and then form a frame.

确定帧的界限。

Determine the bounds of the frame.

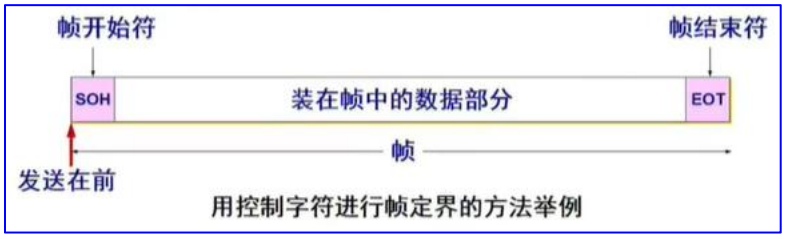
首部和尾部的一个重要作用就是进行帧定界。

控制字符 SOH (Start Of Header)放在一帧的最前面,表示帧的首部开始。

The control character SOH (Start Of Header) is placed at the beginning of a frame, indicating the beginning of the frame header.

另一个控制字符 EOT (End Of Transmission) 表示帧的结束。

Another control character, EOT (End Of Transmission), indicates the end of the frame.



用控制字符进行帧定界的方法举例

③透明传输是啥？

透明传输是指不管所传数据是什么样的比特组合,都应当能够在链路上传送。

Transparent transmission means that no matter what combination of bits the transmitted data is, it should be able to be transmitted over the link.

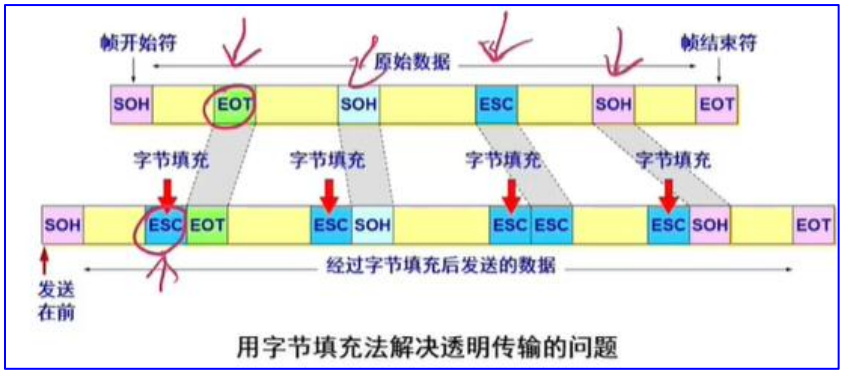
当所传数据中的比特组合恰巧与某一个控制信息完全一样时，就必须采取适当的措施

When the combination of bits in the transmitted data happens to be exactly the same as one control message, appropriate action must be taken

举例如下：如果数据中的某个字节的二进制代码恰好和 SOH 或 EOT 一样，数据链路层就会错误地“找到帧的边界”。

Eg. If the binary code of a byte in the data happens to be the same as SOH or EOT, the data link layer will mistakenly "find the boundary of the frame."

解决透明传输问题解决方法:字节填充(byte stuffing)或字符填充(character stuffing)。
Solution to the transparent transmission problem Solution: byte stuffing or character stuffing.
发送端的数据链路层在数据中出现控制字符



“SOH”或"EOT"的前面插入一个转义字符“ESC” (其十六进制编码是 1B)。
The data link layer on the sending side inserts an escape character "ESC" (whose hexadecimal code is 1B) before the control character "SOH "or "EOT" appears in the data.

怎么恢复数据呢？
接收端的数据链路层在将数据送往网络层之前删除插入的转义字符。
The data link layer at the receiving end deletes the inserted escape character before sending the data to the network layer.

④差错检测在传输过程中可能会产生比特差错：1 可能会变成 0 而 0 也可能变成 1。

error detection in the transmission process may produce bit errors: 1 May become 0 and 0 May also become 1.
在一段时间内，传输错误的比特占所传输比特总数的比率称为误码率 BER（Bit Error Rate)。
The ratio of transmitted Error bits to the total number of transmitted bits over a period of time is called the Bit Error Rate (BER).
误码率与信噪比有很大的关系。
The bit error rate is closely related to the signal-to-noise ratio.
为了保证数据传输的可靠性,在计算机网络传输数据时,必须采用各种差错检测措施。
In order to ensure the reliability of data transmission, various error detection measures must be adopted when transmitting data on computer network.

⑤循环冗余检验 CRC 的检错技术。利用冗余码来实现的校验

cyclic redundancy check CRC error detection technology.

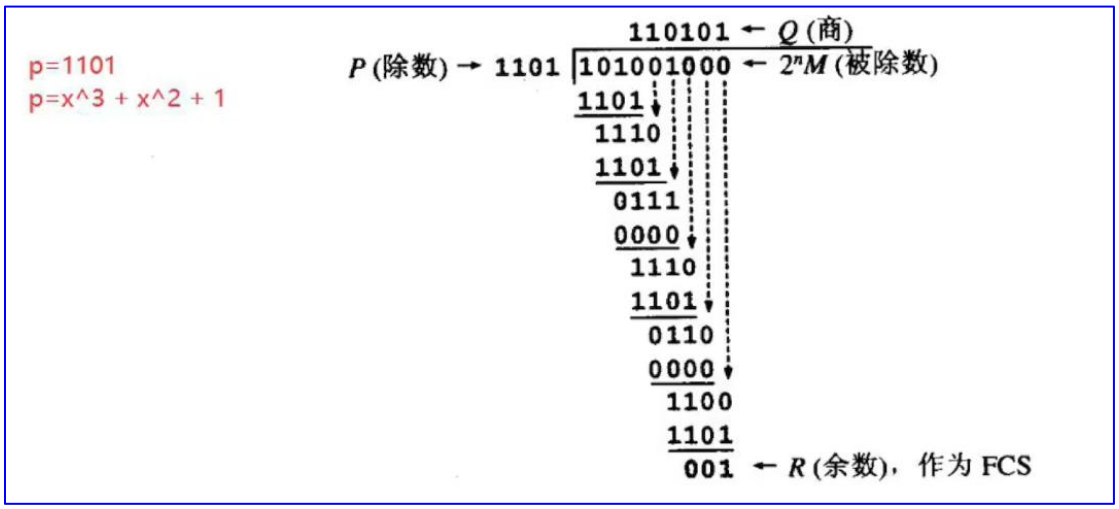
这 n 位冗余码可用以下方法得出。
The n-bit redundancy code can be obtained in the following way.
用二进制的模 2 运算进行 2” 乘 M 的运算，这相当于在 M 后面添加 n 个 0。
Multiply M by 2 "using the binary modular 2 operation , which is equivalent to adding n zeros

after M.

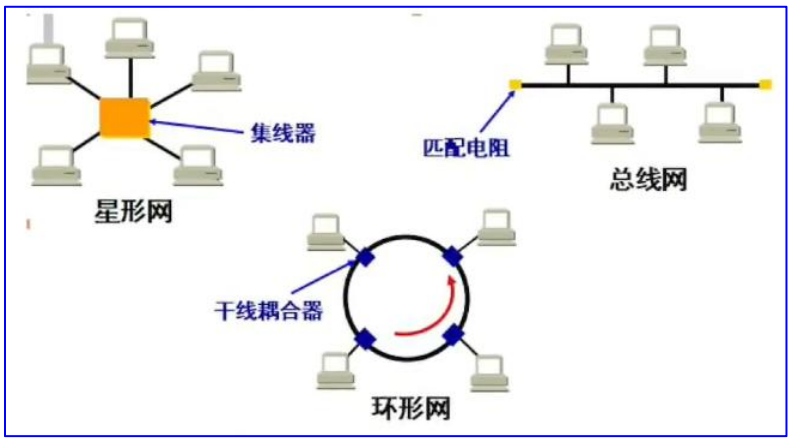
模 2 运算就是异或运算

The modular 2 operation is the xOR operation

具体规则如下：



⑥常见局域网的拓扑结构



⑦CSMA/CD 协议：CSMA/CD 含义：载波监听多点接入 /碰撞检测 Multiple Access with Collision Detection) 。

CSMA/CD protocol: CSMA/CD meaning: carrier monitoring Multiple Access with Collision Detection).

“多点接入”表示许多计算机以多点接入的方式连接在一根总线上。

"Multipoint access" means that many computers are connected to a bus in a multipoint way.

“载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据,如果有,则暂时不要发送数据,以免发生碰撞。

"Carrier monitoring" means that each station must first detect whether other computers on the bus are sending data before sending data, and if so, do not send data for the time being to avoid

collision.

“碰撞检测”就是计算机边发送数据边检测信道上的信号电压大小。

"collision detection" is the computer sends data while detecting the signal voltage on the channel.

在发生碰撞时,总线上传输的信号产生了严重的失真,无法从中恢复出有用的信息来。

In the event of a collision, the signal transmitted on the bus is seriously distorted, and no useful information can be recovered from it.

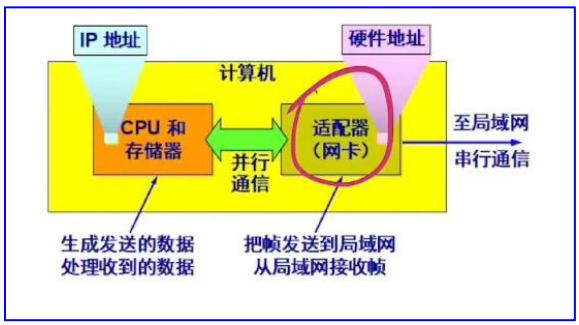
每一个正在发送数据的站,一旦发现总线上出现了碰撞,就要立即停止发送,免得继续浪费网络资源,然后等待一段随机时间后再次发送。

Each station that is sending data, once it finds a collision on the bus, must immediately stop sending, so as not to continue wasting network resources, and then wait for a random period of time to send again.

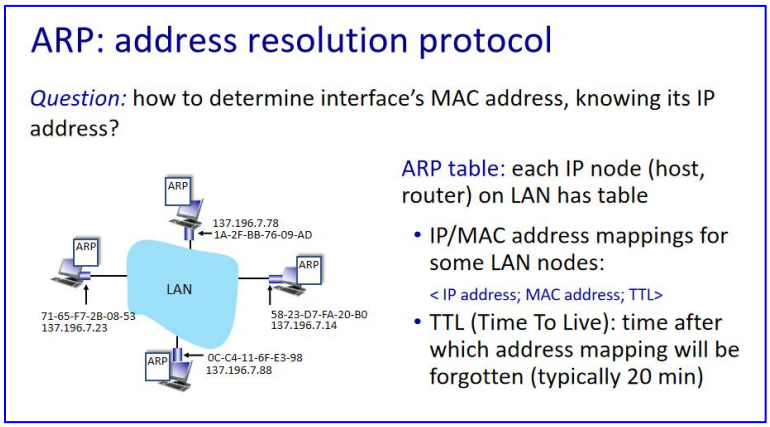
物理地址 mac address

⑧适配器:网络接口板又称为通信适配器(adapter)或网络接口卡 NIC (Network InterfaceCard），或“网卡”。

adapter: The Network interface board is also known as the communication adapter (adapter) or network interface card (NIC) (Network InterfaceCard), or "network card".



Arp 查询



题：请简述数据链路层的主要功能是什么？

Q: What are the main functions of the data link layer?

答案：数据链路层的主要功能是在物理层提供的服务基础上，向网络层提供可靠的数据传输服务。这包括将网络层交下来的 IP 数据报组装成帧，在两个相邻节点间的链路上透明地传输帧，以及实现差错控制和流量控制等功能。

题：链路和信道有什么区别

Question: What is the difference between a link and a channel

答案：链路是只两个节点之间的一条路径，信道是 A 到 B 的一整条路径，中途可能会经过很多个节点。

题：什么是数据链路层的封装成帧？

Question: What is the encapsulation of the data link layer into frames?

答案：封装成帧就是在一段数据的前后分别添加首部 soh 和尾部 eto，这样就构成了一个帧。首部中包含了帧的一些控制信息，如帧的长度、帧的类型等；尾部则用于标识帧的结束。封装成帧的作用是使得接收端能够准确地识别出一个个完整的数据帧。

题：请解释数据链路层的透明传输是什么意思？

Question: Please explain what is the meaning of transparent transmission at the data link layer?

答案：透明传输是指不管所传数据是什么样的比特组合,都应当能够在链路上传送。当所传数据中的比特组合恰巧与某一个控制信息完全一样时，就必须采取适当的措施,举例：如果数据中的某个字节的二进制代码恰好和 SOH 或 EOT 一样，数据链路层就会错误地“找到帧的边界”。

题：差错控制在数据链路层中是如何实现的？

Question: How is error control implemented in the data link layer?

答案：数据链路层通过差错控制机制来检测和纠正传输过程中可能发生的差错。常见的差错控制方法包括 checksum，奇偶校验，crc 校验等。这些方法通过在数据中添加一些冗余信息，使得接收端能够检测出数据中的错误并进行纠正。

题：请简述 CSMA/CD 协议的工作原理。

Question: Please briefly describe the working principle of the CSMA/CD protocol.

答案：CSMA/CD（载波侦听多路访问/碰撞检测）协议是数据链路层中的一种介质访问控制协议，主要用于以太网中。它的工作原理是：发送方在发送数据前先侦听信道是否空闲，若空闲则发送数据；在发送数据的同时继续侦听信道，若检测到碰撞（即有其他发送方也在发送数据），则立即停止发送并等待一段随机时间后再重新尝试发送。

题：交换机在数据链路层中的作用是什么？

Question: What is the role of the switch in the data link layer?

答案：交换机通过维护一个转发表来记录每个设备所在的网络地址，当接收到一个数据包时，它会根据转发表中的信息将数据包转发到目标设备所在的端口。这个所谓的转发记录表内数据，是通过 self learning 自学习而得到的。

题：什么是以太网？

Question: What is Ethernet?

答案：以太网是一种有线传输技术，是当今现有局域网采用的最通用的通信协议标准

题：什么是 VLAN？它在链路层中的作用是什么？

Question：What is a VLAN? What is its role at the link layer?

答案：虚拟局域网（VLAN）是一种通过软件定义的逻辑分区，使网络中的设备能够像在同一物理局域网中一样进行通信，从而提高网络的灵活性和安全性

题：若按介质进行分类，网络通信手段一般分为几种？以太网是什么？它是属于哪种传输手段？

Question: If classified according to the medium, the means of network communication are generally divided into several kinds? What is Ethernet? Which means of transmission does it belong to?

答案：

按传输介质分类

有线通信：

利用物理线缆传输信号，常见的

双绞线（Twisted Pair）：常用于局域网（LAN）和电话网络。

光纤（Optical Fiber）：传输速度快、距离远，常用于骨干网络。

无线通信：

利用无线电波、红外线或微波传输信号。

Wi-Fi：常用于无线局域网。

蜂窝网络（Cellular Networks）：包括 2G、3G、4G 和 5G，用于移动通信。

蓝牙（Bluetooth）：短距离无线通信，用于个人设备间的数据传输。

红外线（Infrared）：短距离点对点通信，如电视遥控器。

Nfc 等等。

综合讨论：假设您走进一个房间，连接到以太网，并想访问一个网页。

Suppose you walk into a room, connect to Ethernet, and want to download a Web page.

从打开电脑到进入网页，所有的协议步骤都发生了什么？

What are all the protocol steps that take place, starting from powering on your PC to getting the Web page?

答案：

①如果是机房，则需要之前有网络管理员给机房内配置过静态 ip 地址。

若是自己的个人电脑，可以自动获取 ip。使用 dhcp 协议，通常 dhcp 服务器集成在路由器中。

DHCP

您的计算机首先使用 DHCP 动态获取 IP 地址。您的计算机首先在 DHCP 服务器创建一个特定的 IP 数据报，目的地为 255.255.255.255（因为不知道 dhcp 在哪，所以广播），并将其放入以太网帧中并在以太网中广播。然后，按照 DHCP 协议中的步骤，您的计算机能够在给定的时间内获得 IP 地址。

以太网上的 DHCP 服务器还为计算机提供第一跳路由器的 IP 地址列表（因为 DHCP 通常集成在路由器中）、计算机所在子网的子网掩码以及本地 DNS 服务器（如果存在）的地址。

②由于涉及到 dns 的域名解析，所以需要逐级寻找 dns 服务器，第一个要去的 dns 服务器我们现在不知道物理地址，第一跳路由器的物理地址我们也不知道

所以这一步是通过 arp 协议做 arp 查询，获取刚刚提到的两个 mac 地址。

③ ip+mac adress 的 adressing（寻址）方式，是我们做通信的核心，ip 地址帮助我们能够顺利路由到目的地，Mac 地址相当于身份证，帮助我们到达目的地后进行身份认证。

④在做详细的域名解析的过程中，则需要通过 root-->top level Domain -->authoritative DNS servers,这个过程最终解析出域名对应的 ip。

⑤有了域名对应的 ip 地址后，接下来就是正式的向网页发出请求了，使用 http 协议，若是类似登录界面或评论界面，则请求包的 header 里是 POST 类型的请求，若是普通页面，则是 GET 类型的请求。

⑥HTTP 请求消息将被分割并封装成 TCP layer 的 transport segment(因为 http 是可靠性传输，所以这一层使用的是 tcp 协议), 然后进一步封装成 IP layer 的 datagram，最后封装成 link layer 的 ethernet frame(以太网帧)，您的计算机将以太网帧发送到第一跳路由器。

⑦后续在各个路由节点中，经过路由表的查询，能够顺利的将我们的请求发送给网页服务器，最终网页服务器将 html 文件以响应的形式返回给我们的浏览器。