物理层概念　　数据层　 网络层　 介质访问控制子层 传输层（期中会考 期末重点）

多看作业（今年作业） 知识点总结主要看HTML PPT上重点

填空　概念　定义

**TCP的头部某些段含义 PPT**

URG：紧急指针

ACK：响应字段

PSH：迅速推送信号

RST：困难重启信号

SYN：建立连接字段

FIN：断开连接字段

**什么层上面是什么**

OSI(7层)：物理——数据链路——网络——传输——会话——表示——应用

比特 帧 分组 TPDU SPDU PPDU APDU

TCP/IP(3层)：互联网————传输————应用

邮政系统、IP TCP/UDP

**数据链路层的功能**

1.向网络层提供一个定义良好的接口

2.处理传输错误（差错控制）

3.调节数据流，确保慢速的接收方不会被快速的发送方淹没（流控制）

**英文缩写全称**

TCP transport control protocol 传输控制协议

UDP user datagram protocol 用户数据报协议

DHCP dynamic host configuration protocol 动态主机配置协议

WWW World Wide Web 万维网

PDU protocol data unit 协议数据单元

MAC medium access control 介质访问控制子层

CDMA code division multiple access 码分复用

TDM time division multiplexing 时分复用

ARP address resolution protocol 地址解析协议

DNS协议（应用层）Domain Name System

TCP/UDP协议（传输层）Transport Control Protocol User Datagram Protocol

IP/ARP/OSPF/BGP协议（网络层） Internet Protocol Address Resolution Protocol Open Shortest Path First Border Gateway Protocol

MAC子层协议（数据链路层）Medium Access Control

**命令**

Ifconfig：查看网卡的IP地址、掩码、广播地址、网关等。

route：用于查看IP路由表

ping：检查网络是否连通

traceroute：用来侦测主机到目的主机之间所经路由情况

netstat：显示网络连接、路由表和网络接口信息。不带参数显示TCP连接

**滑动窗口协议（重点）**2 看HTML PPT（数据链路层）

1位 回退N 选择重传

* Please illustrate the principle of the sliding window protocol using selective repeat.

发送方和接收方各自维持一个窗口，该窗口分别包含可发送或已经发送但未被确认的和可接受的序号（窗口的最大尺寸不超过序号空间的一半）每当到达一帧接收方检查它的序号，看是否落在窗口内。如果落在窗口内并且以前没有接收过该帧，则接受该帧，并保持在缓冲区。

* 请说明使用选择性重传方法的滑动窗口协议的基本工作原理。

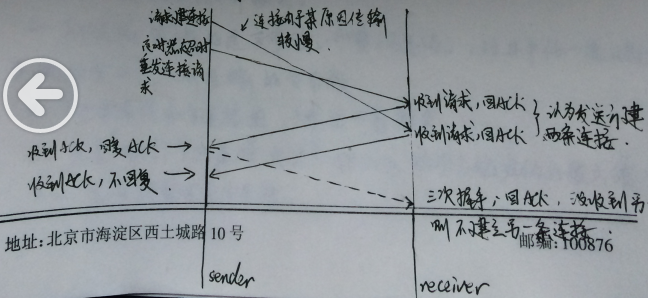
P176-189 必考

发送方和接收方各自维持一个窗口，该窗口分别包含可发送或已发送但未被确认的和可接受的序号。发送方的窗口大小从0开始，以后可以增大到某一个预设的最大值。相反，接收方的窗口总是固定不变，其大小等于预先设定的最大值。接收方为其窗口内的每个序号保留一个缓冲区。与每个缓冲区相关联的还有一个标志位，用来指明该缓冲区是满的还是空的。每当到达一帧，接收方通过between函数检查它的序号，看是否落在窗口内。如果确实落在窗口内，并且以前没有接受过该帧，则接受该帧，并且保存在缓冲区。但该帧只能被保存在数据链路层中，直到所有序号比它小的那些帧都已经按序递交给网络层之后，它才能被传递给网络层。窗口的最大尺寸应该不超过序号空间的一半。

**TCP IP三次握手机制 PPT 书（传输层）**

* 为什么TCP连接的建立需要三次握手协议过程

1. 三次握手才能使双方都保留对方的SEQ序号，并确认以保留的序号，使得连接建立之后，通信双方的行为同步
2. 考虑如下的消息顺序图



该情况下，定时器设置时间过短，或者由于网络延迟较大，使得发送方端定时器超时，此时，两次握手则在双方建立两条连接（发送方认为只有一条连接，接收方认为有两条连接），双方出现不同步。关闭连接时，发送方只关闭一条，于是造成接收方资源浪费，端口号、套接字

而三次握手则会发送ACK（图中虚线），接收方只收到一条ACK并建立连接，从而使双方达到同步状态。

**数据链路层和网络层 重点2 PPT 书**

* 数据链路层和网络层的关系
* 数据链路层向网络层提供一个定义良好的服务接口
* 数据链路层向网络层提供服务如下：

1.定义操作连接的程序；

2.封装数据包为数据帧；

3.数据链路建立、维护与释放的链路管理工作；

4.数据链路层服务数据单元帧的传输；

5.差错检测与控制；

6.数据流量控制；

7.在多点连接或多条数据链路连接的情况下，提供数据链路端口标识的识别，支持网络层实体之间建立网络连接；

8.帧接收顺序控制。

* 请说明以太网MAC地址（物理地址）与网络层IP地址有什么不同 PPT

IP地址和MAC地址相同点是它们都唯一，不同的特点主要有：

长度不同。IP地址为32位，MAC地址为48位。

分配依据不同。IP地址的分配是基于网络拓扑（动态分配），MAC地址的分配是基于制造商（静态分配）。

寻址协议层不同。IP地址应用于OSI网络层，而MAC地址应用在OSI数据链路层。 数据链路层协议可以使数据从一个节点传递到相同链路的另一个节点上（通过MAC地址），而网络层协议使数据可以从一个网络传递到另一个网络上（ARP根据目的IP地址，找到中间节点的MAC地址，通过中间节点传送，从而最终到达目的网络）。

一个网卡会有一个全球唯一固定的MAC地址，但可对应多个IP地址。

* 请说明数据链路层协议差错控制的基本方法

在数据链路层中引入计时器。当发送方发出一帧时，启动一个计时器。计时器的超时值应该设置得足够长以保证在正常情况下该帧能够到达接收方，并在接收方进行处理后再将确认返回到发送方。一般情况下，在计时器超时前，该帧应该被正确地接收，并且确认帧也被传了回来，此时计时器被取消。当帧确认被丢失，则计时器被触发，从而警告发送方存在一个潜在的问题。解决方案是重新发送该帧，为避免接收方多次将同一帧传递给网络层，需要给发送出去的帧分配序号，这样接收方可以根据帧的序号来有效区分原始帧和重传帧。管理好计时器和序号，以便保证每一帧最终都恰好一次地被传递给目标机器的网络层，这是数据链路层（以及上层）工作的重要组成部分。

* 请说明链路层协议是如何进行差错控制和流量控制的？

差错控制：通过引入定时器，当发送方发出一帧时，启动一个计时器。一般情况下，在计时器超时前，该帧应该被正确地接收，并且确认帧也被传了回来，此时计时器被取消。当帧确认被丢失，则计时器被触发，从而警告发送方存在一个潜在的问题。解决方案是重新发送该帧，为避免接收方多次将同一帧传递给网络层，需要给发送出去的帧分配序号，这样接收方可以根据帧的序号来有效区分原始帧和重传帧。

流量控制：基于反馈的流控制，接收方给发送方送回信息，允许发送更多数据，或者告诉发送方它的情况。

基于速率的流控制，限制发送方传输数据的速率，无需利用接收方的反馈信息。

* 在数据链路层已经有差错控制了，为什么在提供可靠传输服务的传输层协议中还需要有差错控制功能

1. 数据链路层的数据传输为点到点，传输层协议控制传输为端到端，因此数据链路层的校验是保护一个穿过单条链路的帧，而传输层校验保护跨越整个网络路径的段，故数据链路层差错控制只保护一条链路上经过的数据包，没有考虑路由器内部出错的情况。即使每条链路校验正确，该数据包仍可能被不正确传递
2. 数据链路层主要针对单一帧，或字节本身的对错，而传输层是对所有传输内容的总体控制。

**7层结构 基本概念 每层干嘛 （物理层概念）2**

* Please illustrate the function of protocol in each layer in the OSI reference model.

物理层：关注在一条通信信道上传输的原始数据，实现数据可以通过介质传输。

数据链路层：将原始的传输设施转变成一条没有漏检传输错误的线路。保证在链路传输过程中没有传输错误。向网络层提供一个定义良好的服务；处理传输错误；调节数据流，确保慢速的接收方不会被快速的发送方淹没。

网络层：控制子网的运行，将分组（数据包）通过路由寻址从源端沿着网络路径送达目标端。同时进行流量控制和拥塞控制。

传输层：传输层是真正端到端的层。保证端到端的正确传输。接收来自上一层的数据，必要时将数据分割成较小的单元然后传递给网络层。

会话层：建立会话。实现对话控制，令牌管理，同步功能等。

表示层：解释所传递数据的语法和语义。

应用层：包括了用户常用需要的各种各样的协议。

**计算机网络协议、协议分层**

* 请说明您对计算机网络协议分层的理解？为什么计算机网络协议需要分层？

理解：

a) 为了降低网络设计的复杂性，绝大多数网络都组织成一堆相互叠加的层，每一层都建立在其下一层基础之上。

b) 一台机器上的第n层与另一台机器上的第n层进行对话。在对话中用到的规则和约定合起来称为第n层协议

c) 协议是指通信双方关于如何进行通信的一种约定

d) 不同机器上包含对应层的实体称为对等体

e) 每一对相邻层之间是接口

f) 层和协议的集合称为网络体系结构

g) 一个特定系统所使用的一组协议称为协议栈

原因：

a) 降低了网络设计的复杂性

b) 分层设计协议有助于各个部件的开发、设计和故障排除。

c) 各层之间相互独立，某一层只要了解下一层通过接口所提供的服务,而不需了解其实现细节.

d) 灵活性好，若某一层的内容发生变化,只要接口关系不变,上下层均不受影响.同时,也便于程序的实现,调试和维护.

e) 标准化程度高，由于结构上分割成较小部分,各层都可以选择最适合的实现技术.此外,各层的功能和所提供的服务都有精确说明,便于人们理解与实现.

* 请说明你对计算机网络协议的理解？要定义一个计算机网络协议，需要定义哪些内容？

网络协议是网络上所有设备（网络服务器、计算机及交换机、路由器、防火墙等）之间通信规则的集合，它规定了通信时信息必须采用的格式和这些格式的意义。大多数网络都采用分层的体系结构，每一层都建立在它的下层之上，向它的上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。一台设备上的第 n层与另一台设备上的第n层进行通信的规则就是第n层协议。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。常见的协议有：TCP/IP协议、IPX/SPX协议、NetBEUI协议等。

三要素：语义（做什么）：规定了需要发出何种控制信息，以及完成的动作与做出什么样的响应

语法（怎么做）：用户数据与控制信息的结构与格式，以及数据出现的顺序

时序（顺序）：对事件发生顺序的详细说明。

* 协议数据单元与协议服务原语之间有某种关联性吗？为什么？

没有关联。

所谓协议数据单元就是在不同站点的各层对等实体之间，为实现该层协议所交换的信息单元。通常将第N层的协议数据单元记为NPDU。它通常是将SDU分成若干段，每一段加上报头，作为单独协议数据单元PDU在水平方向上传送。

服务原语=服务动作+原语类型，一个服务由一组原语操作来描述，进程通过原语操作访问该服务。

服务和协议截然不同，他们完全分离。服务涉及层之间的接口，协议涉及到不同机器上对等实体发送的分组。…….书31，所以PDU与服务原语也没有关联

**从校园网到外网过程的大图（网络层） 图在哪？**

* 请描述校园网内的一台主机使用URL访问校外一个web网站主页所涉及到的协议和协议过程

这一请求过程应该涉及DNS协议（应用层）、TCP/UDP协议（传输层）、IP/ARP/OSPF/BGP协议（网络层）、MAC子层协议（数据链路层）、物理层协议。下面详细讲解这一系列过程：

1. 校园网内一台主机在浏览器中输入URL，浏览器确定并分析输入的URL，得到协议、主机DNS域名和路径名。我们仔细考虑DNS协议：首先，在校园网内部查找并代理DNS服务器，若该服务器已经缓存了该域名对应的IP地址，则返回。若未找到，则从顶级域名从上往下依次寻找所属的授权DNS服务器，进而查找对应IP地址，得到网站IP后可以选择TCP/UDP协议进行传输
2. 数据进入网络层在路由器之间进行传递时，需要寻找下一跳的ip地址，在此需要使用OSPF协议或者BGP协议。OSPF协议是在网络内部寻找下一跳路由主机，BGP协议在网络外部寻找下一跳路由主机。
3. 找到下一跳主机IP之后，需要得到其MAC地址，网络层把打包好的数据包送到数据链路层后，在此需要使用ARP协议。ARP协议是源主机向网内所有主机广播消息，消息中携带目的主机IP，目的主机收到后，向网内回送消息，包含本机IP和MAC地址，发送到源主机，其他主机则对该消息不作处理。
4. 数据链路层将数据分组组装成帧，送到物理层，物理层根据帧内容，以比特流方式发送到目标主机。

NAT网络地址转换：

* NAT的基本思想：

ISP为每个家庭或公司分配一个ip地址用来传输流量，在客户网内部，每台计算机有唯一的ip地址，用来在客户内部传递流量，然而当一个数据包需要离开数据网络，发向其他的ISP时，它必须执行一个地址转换，把唯一的ip地址转换为共享的公共ip地址。

* 问题：当应答数据包返回时，NAT盒子如何确定是用哪一个地址来替代？

端口是16位整数，它指示了TCP连接从哪里开始到哪里结束，正是这些端口为NAT提供了工作所需的字段。

利用源端口字段，可以完成前面的映射问题。接收时 数据包只含子网的外网地址 (所有外网地址相同无法标识) 只能通过分配的端口号找到之前记录的源端口号找到内网中的计算机（端口号转换）

* NAT设备有什么用

Network address translation 网络地址转换，用途有以下两点：

1. 宽带共享，解决IP地址匮乏的问题。由于局域网内所分配的公有IP地址数量有限，NAT机制将内部多台PC机映射到同一个公有IP，内部PC通过端口号进行标识。端口多路复用（PAT）和动态转换是NAT的两种方式。
2. 提供安全防护。NAT机制对外只公布一个IP地址，即NAT之内PC联机到互联网时，所显示的IP是NAT主机的公共IP，所以客户端PC具有一定的安全。相当于来自外网攻击到来时，隐藏了内部计算机。外界计算机扫描端口，无法找到内部PC。

9?

**ARP(网络层)**

Address Resolution Protocol 地址解析协议

* 主机发送一个广播包到以太网络上请求拥有目标ip地址的主机，该广播包会到达CS网络上的每一台主机，并且每台主机都会检查自己的ip地址，若匹配则给出应答，否则忽略。
* 不管网络层使用的是什么协议，在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。

每一个主机都设有一个 ARP 高速缓存(ARP cache)，里面有所在的局域网上的各主机和路由器的 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。

ARP 是解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。如果所要找的主机和源主机不在同一个局域网上，那么就要通过 ARP 找到一个位于本局域网上的某个路由器的硬件地址，然后把分组发送给这个路由器，让这个路由器把分组转发给下一个网络。剩下的工作就由下一个网络来做。

* Please explain the principle of the ARP protocol.

一个主机发送一个广播包到以太网络上请求拥有某个IP地址的主机。该广播包将会到达主机所在子网上的每一台主机，并且每台主机都会检查自己的IP地址，只有IP为规定IP的主机和连接到该主机的路由器会以自己的MAC地址作为应答。这个过程就是地址解析协议。

**TCP和UDP的区别2（传输层）**

TCP：面向连接、传输可靠(保证数据正确性,保证数据顺序)、用于传输大量数据(流模式)、速度慢，建立连接需要开销较多(时间，系统资源)。

UDP：面向非连接、传输不可靠、用于传输少量数据(数据包模式)、速度快。

运输层需要有两种不同的运输协议，即面向连接的 TCP 和无连接的 UDP。

TCP的特点：

TCP 是面向连接的运输层协议。

每一条 TCP 连接只能有两个端点，每一条 TCP 连接只能是点对点。

TCP 提供可靠的服务。

TCP 提供全双工通信。

面向字节流。

UDP 是面向报文的:

发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付IP层。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。应用层交给 UDP 多长的报文，UDP 就照样发送，即一次发送一个报文。

接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。应用程序必须选择合适大小的报文。

**TCP连接用什么标识，listen socket和connect socket的区别 百度（传输层）**

标识TCP的四个参数：源地址，源端口，目的地址，目的端口。

Listen socket和connect socket的区别

Socket: TCP连接的两个端点

* 如何标识一个TCP连接？如何理解一个TCP连接？

1. TCP/IP通信中一般采用5个信息来识别。源IP地址、目的IP地址、源端口号、目的端口号、协议号。协议号指示采用TCP通信还是UDP通信。其中一项不同，则认为是其他通信。即通过TCP端口加主机IP地址组成一个48位的唯一端点，而通过源端口和目的端口一起标识了一个TCP连接。

2. TCP连接时全双工模式，收发双方都可发送、接收消息

TCP连接时端到端的，通过连接绑定交互双方只有一个主机/端口，不支持组播或广播的传输模式。

TCP连接传输的是字节流，而不是消息流。对其中任一流进行编号时，依据的是之前传输的字节数。

TCP连接是面向连接的，提供可靠服务

流量控制，TCP连接发送方能知道接收方能容纳的最大缓冲区大小，进而调整发送字节数

TCP连接允许通信双方协商参数

TCP连接双方都需为该连接分配缓存和变量

* TCP套接字编程中，套接字和端口号之间的关系，连接套接字与监听套接字

TCP服务由发送端和接收端创建套接字实现。每个套接字有一个套接字编号，由主机IP地址和端口号组成。

在socket编程中，sever端申请套接字，绑定主机IP及端口号，之后处于阻塞监听状态，称之为监听套接字。客户端向服务器发送连接请求，sever收到请求后创建新线程以及新的套接字，成为连接套接字。连接套接字与监听套接字的端口号一致。服务器处理不同套接字可以依据源IP地址和端口号的不同加以区别

* What is the relationship between the TCP port and TCP socket? What’s the difference between them?

TCP 服务由发送端和接收端创建TCP socket 的端点来获得。TCP socket使得应用程序将自己关联到一个本地的TSAP（传输服务访问点）上，而端口号（TCP port）标明该服务的TSAP名字。每个套接字有一个套接字号，它由主机的IP地址以及本地主机局部的16位数值组成的，次16位数值被称为端口。端口是一个TSAP的TCP名字。端口是应用层服务的一种代号，它用来标志应用层的进程。

**建立TCP连接时为何要交换（定义？）初始seq值，TCP怎么进行差错控制（传输层）**

三次握手？

双方保留对方的SEQ序号，并确认以保留的序号，使得连接建立之后，通信双方的行为同步，在出错的时候……

**如何识别一个IP地址使用TCP协议传输（传输层）网上答案？**

协议字段（报头检验和前面那个），其值为6，则为TCP，其值为17，则为UDP。

**MAC layer的概念、作用，在以太网中使用了介质控制哪种算法2（介质访问控制子层）**

概念：medium access control 介质访问控制子层

作用：书 PPT解决当局域网中共用信道的使用产生竞争时，如何分配信道的使用权问题。

算法：经典以太网使用1-坚持CSMA/CD算法：当有需要发送数据时要侦听介质，一旦介质变为空闲立即发送。在它们发送的同时检测信道上是否有冲突，如果有冲突则立即中止传输，并发出一个短冲突加强信号，在等待一段随机时间后重发。

在冲突发生后，时间被分成离散的时间槽，其长度等于最差情况下在以太介质上往返传播时间（2t）

第一次冲突后，每个站随机等待0或1个时间槽，之后再重试发送，再次发生冲突之后，每个站随机选择0，1，2，3，每次冲突之后从0到2^3-1之间随机选择。

随着连续冲突的次数越来越多，随即等待的间隔呈指数增加，算法能保证少量站发送冲突时，确保较低的延迟，许多站发生冲突时，可保证在一个相对合理的时间间隔内解决冲突。

* 为什么需要介质访问控制(MAC)子层？ 书 PPT

　 在只有两个用户之间使用一个信道通信时不存在信道使用者的冲突问题，但是在一个广播网络中当只有一条信道可供使用时，确定下一个使用者十分困难，而介质访问控制子层就包含了确定多路访问信道下一个使用者的协议。。

* Why MAC sublayer is needed? Please explain the principle of CSMA/CD algorithm.

在只有两个用户之间使用一个信道通信时不存在信道使用者的冲突问题，但是在一个广播网络中当只有一条信道可供使用时，确定下一个使用者十分困难，而介质访问控制子层就包含了确定多路访问信道下一个使用者的协议。

CSMA/CD：当一个站有数据要发送时，它先侦听信道，如果信道空闲就发送数据。传输时站的硬件继续侦听信道，如果它读回的信号不同于它放到信道上的信号，则知道发生了碰撞，要重新发送数据。

**CDMA是什么（物理层）**

码分多址 code division multiple access

允许每个站利用整个频段发送信号，而且没有任何时间限制。它的关键在于：能够提取出期望的信号，同时拒绝所有其他的信号，并把这些信号当做噪声。

* 请说明复用（Multiplexing）的含义？在计算机网络中，有哪些种类的复用？

频分复用（FDM，Frequency Division Multiplexing）将频谱分成几个频段，每个用户完全拥有其中的一个频段来发送自己的信号，给不同的逻辑信道分配不同的频率，每个频率工作在频谱中的一部分，并且相邻信道之间的频谱间隔足够大以防止干扰，利用通带传输的优势使多个用户共享一个信道。OFDM正交频分复用Orthogonal

时分复用（TDM，Time Division Multiplexing）用户以循环的方式轮流工作。每个用户周期性地获得整个带宽非常短的一个时间，每个输入流的比特从一个固定的时间槽（time slot）取出并输出到混合流。该混合流以各个流速率的总和速度发送。STDM统计时分复用Statistical

码分复用（CDM，Code Division Multiplexing）扩展频谱（spread spectrum）通信的一种形式，把一个窄带信号扩展到一个很宽的频带上。这种方法更能容忍干扰，而且允许来自不同用户的多个信号共享相同的频带。

码分多址（CDMA，Code Division Multiplexing）允许每个站利用整个频段发送信号，而且没有任何时间限制。它的关键在于：能够提取出期望的信号，同时拒绝所有其他的信号，并把这些信号当做噪声。

**路由表有什么用，写出两种路由算法2（网络层） HW2**

所谓路由表，指的是路由器或者其他互联网网络设备上存储的表，该表中存有到达特定网络终端的路径，在某些情况下，还有一些与这些路径相关的度量。供路由选择时使用，表中包含的信息决定了数据转发的策略。

路由表中含有网络周边的拓扑信息。路由表建立的主要目标是为了实现路由协议和静态路由选择。 整理

距离矢量路由算法 链路状态路由算法

* Please explain the meaning of the field Destination, Gateway, and Interface in the routing table.

Destination：目的地址，包要传输到达的最终目标地址

Gateway:下一跳的地址（包括路由器的IP地址，或者网络的ID）

Interface：要到达目的地址分组要转发到路由器的哪一个接口（即使用那个网卡）

* Please explain the concept forwarding, and the concept routing.

Forwarding：转发，当一个数据包到达时该采取什么动作。每个分组到达的时候对它进行处理，它在路由表中查找该分组所对应的输出路线。这个叫转发。

Routing：路由，对使用那一条路径做出决策。负责填充和更新路由表。

* 查找路由表

在路由表中，对每一条路由，最主要的是（目的网络地址，下一跳地址）.

根据目的网络地址就能确定下一跳路由器，这样做的结果是：

IP 数据报最终一定可以找到目的主机所在目的网络上的路由器（可能要通过多次的间接交付）。

只有到达最后一个路由器时，才试图向目的主机进行直接交付。

* Please explain why Exterior Gateway Protocol, such as BGP, is needed in the Internet?

在独立运营商网络之间的路由问题和域间路由问题需要外部网关协议。域内协议和域间协议的目标不同。域内协议所需做的只是尽可能有效地将数据包从源端传送到接受方，不用考虑政治方面的因素。而域间路由必须考虑大量涉及政治，安全或者经济方面的因素。

BGP：边界网关协议 Border Gateway Protocol

**解释一下路由算法2 HW2**  PPT 书概念

路由算法，又名选路算法，可以根据多个特性来加以区分。算法的目的是找到一条从源路由器到目的路由器的“好”路径（即具有最低费用的路径[1] ）

* Please tell the difference between the distance vector routing algorithm and the link state routing algorithm.

distance vector routing algorithm：距离矢量路由算法每个路由器维护一张表，表中列出了当前已知的到每个目标的最佳距离，以及所有使用的链路。这些表通过邻居之间的交换信息不断被更新，最终每个路由器了结到达每个目的地址的最佳路径。

link state routing algorithm：链路状态路由算法发现他的邻居，设置到每个邻居节点的距离，构造一个包含这些数据的包，将这个包发给所有的其他路由器，并接受所有其他路由器的信息包，然后计算出到每个其他路由器的最佳路径。

比较：距离矢量路由算法只发送消息给相邻的路由器，而链路状态路由算法是将消息分组发给其他所有的路由器；链路状态路由算法每个路由器知道整个网络的拓扑结构，而另一个不知道。

**纠错码 验错码 海明距离 书 PPT**

纠错码：在每一个被发送的数据块中包含足够多的冗余信息，以便接收方能据此推断出被发送的数据是什么。适用于较多错误

验错码：只包含一些冗余信息，但这些信息只能让接收方推断是否发生了错误，之后可以请求重传。适用于较少错误

海明距离：两个码字中不相同的位的个数

为了检测d个错误，需要一个距离为d+1的编码方案

为了纠正d个错误，需要一个距离为2d+1的编码方案

每个码字有m个消息位，r个校验位，纠正所有单个错误

n个非法码字：n=m+r

2^r>=m+r+1

即(n+1)2^m<=2^n

**单工协议 停-等协议 书 PPT**

（1）一个乌托邦式的单工协议

（2）无错信道上的单工停-等协议（stop and wait） 确认帧的存在

（3）有错信道上的单工停-等协议：

增加一个计时器，发送方发出一帧，接收方只有在正确接收到数据之后才返回一个确认帧，如果是损坏帧则丢弃，重发

问题：确认帧丢失，会导致接收方重复接受数据包，因此需要区分到达的帧是新帧还是旧帧

解决办法：发送方在发送的每帧的头部放一个序号，一位序号（0，1）足以解决问题

**其他**

* Please explain the meaning of the following concepts: modulation, multiplexing.（物理层）

Modulation：调制，我们用模拟信号来表示比特，而比特与代表它们的信号之间的转换过程称为数字调制。

Multiplexing：复用，信道被多个信号共享

* Please tell why flow control is needed in the data link layer protocol.（数据链路层）

当发送方发送帧的速度超过了接受方机器对帧的接受速度时会导致帧的丢失。所以需要流量控制。

* TCP 的流量控制——利用滑动窗口实现

流量控制(flow control)就是让发送方的发送速率不要太快，既要让接收方来得及接收，也不要使网络发生拥塞。

利用滑动窗口机制可以很方便地在 TCP 连接上实现流量控制。

* 计算机网络协议向上层协议或上层应用程序提供的服务可分为面向连接的服务和无连接的服务。请说明面向连接的服务是怎样的含义？无连接的服务是怎样的含义？

对于无连接的服务(邮寄), 发送信息的计算机把数据以一定的格式封装在帧中, 把目的地址和源地址加在信息头上, 然后把帧交给网络进行发送. 无连接服务是不可靠的.

对于面向连接的服务(电话), 发送信息的源计算机必须首先与接收信息的目的计算机建立连接. 这种连接是通过三次握手(three hand shaking)的方式建立起来的. 一旦连接建立起来, 相互连接的计算机就可以进行数据交换. 与无连接服务不同, 面向连接的服务是以连接标识符来表示源地址和目的地址的. 面向连接的服务是可靠的, 当通信过程中出现问题时, 进行通信的计算机可以得到及时通知

1、面向连接的服务：就是通信双方在通信时，要事先建立一条通信线路，其过程有建立连接、使用连接和释放连接三个过程。TCP协议就是一种面向连接服务的协议，电话系统是一个面向连接的模式。

2、无连接的服务：就是通信双方不需要事先建立一条通信线路，而是把每个带有目的地址的包（报文分组）送到线路上，由系统选定路线进行传输。IP、UDP协议就是一种无连接协议，邮政系统是一个无连接的模式。

面向连接与无连接的优缺点：

面向连接优点：实时通信 / 可靠信息流 / 信息回复确认；

面向连接缺点：占用通信道；

无连接优点：不占用通信信道；

无连接缺点：非实时通信 / 信息流可能丢失 / 信息无回复确认

P27

面向连接的服务

Modeled after the telephone system基于电话系统

to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then release the connection

无连接的服务

Modeled after the postal system基于邮件系统

Each message carries the full destination address, and each one is routed through the system independent of all the others.

* 请说明对一个协议实体的输入有哪些？

P23，31

服务，数据包，报文。

* 请说明Ethernet网中的介质访问控制算法的基本原理 书PPT

经典以太网：1-坚持CSMA/CD算法：站有需要发送数据时要侦听介质，一旦介质变为空闲立即发送。在它们发送的同时检测信道上是否有冲突，如果有冲突则立即中止传输，并发出一个短冲突加强信号，在等待一段随机时间后重发。

交换式以太网（交换机）：CSMA/CD算法

以太网的介质访问控制（MAC）技术称为：载波监听多路存取和冲突检测（CSMA／CD），下面我们分步来说明其原理：

　　 1、载波监听：当你所在的网站（包括服务器和工作站）要向另一个网站发送信息时，先监听网络信道上有无信息正在传输，信道是否空闲。

　　 2、信道忙碌：如果发现网络信道正忙，则等待，直到发现网络信道空闲为止。

　　 3、信道空闲：如果发现网络信道空闲，则向网上发送信息。由于整个网络信道为共享总线结构，网上所有网站都能够收到你所发出的信息，所以网站向网络信道发送信息也称为“广播”。但只有你想要发送数据的网站识别和接收这些信息。

　　 4、冲突检测：网站发送信息的同时，还要监听网络信道，检测是否有另一台网站同时在发送信息。如果有，两个网站发送的信息会产生碰撞，即产生冲突，从而使数据信息包被破坏。

　　 5、遇忙停发：如果发送信息的网站检测到网上的冲突，则立即停止该此网络信息发送，并向网上发送一个“冲突”信号，让其它网站也发现该冲突，从而摈弃可能一直在接收的受损的信息包。

　　 6、多路存取：如果发送信息的网站因“碰撞冲突”而停止发送，就需等待一段时间，再回到第一步，重新开始载波监听和发送，直到数据成功发送为止。

以太网规范具体规定了如何在临近的物理区域，即局域网内，实现计算机之间的数据传送。如果希望将一台计算机接入局域网成为整个网络的一部分，该计算机需要具备一个用于分割和包装数据的网络接口以及一个用于连接线缆的连接端口。连接端口一般被集成到系统的主板上或做为内置网卡将数据发送到网络上，同时接收来自网络上其它计算机的数据。

* 在Ethernet网的帧中是否可以携带IPv6分组？如果可以的话，接收方怎样识别所接收到的帧是否携带Pv6的分组（Packet）？

能？ Ipv6特点？

* TCP的下层IP协议与数据链路层的下层物理层协议，在数据传输的特征性上有哪些不同？

1. 传输数据的形式不同，物理层协议传输0 1原始比特串，IP协议传输IP分组
2. 差错控制。物理层协议向上提供可靠服务，接收方可以准确无误的接收数据及其顺序。IP协议提供不可靠服务，没有相应的差错控制、流量控制等机制。

* 请说明TCP协议实体在接收到上层协议提交的需要发送的数据后，是如何确定怎样将这些数据发送到TCP连接的对方协议实体？

1. 每台支持TCP的机器都有一个TCP传输实体。TCP实体可以是一个库过程、一个用户进程、或是内核的一部分。在所有这些情况下，TCP实体管理TCP流，以及与IP层之间的接口。
2. TCP传输实体接受上层传来的用户数据流之后，将其分段，每个分段以单独的IP数据报形式发送。接收端收到数据报之后，将其重构为原始字节流，查看收到的序列号是否连续，若发送数据全部到达且正确，会在下一次向发送方回应数据响应，其中ACK字段会+1，则发送方知道自己发送的数据已被正确接收。